MyID PIV

Version 12.13

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: IMP1939-12.13.0-PIV

December 2024

Copyright

© 2001-2024 Intercede Limited. All rights reserved.

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

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

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

Licenses and Trademarks

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

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

Apache log4net

Apache License Version 2.0, January 2004 http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

© You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License. ---

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 describes how to install MyID®, including information on hardware and software requirements, preparing your system, upgrading existing systems, running the installation program, and getting your system up and running.

The MyID Installation Assistant guides you through the process of checking your system requirements, gathering information, running the installation program, and configuring your system. See section 2, *MyID Installation Assistant* for details.

MyID delivers a range of system and security identity management functions. MyID controls card issuance, the day-to-day administration of smart cards and tokens, and supports PKI (Public Key Infrastructure) secured infrastructures.

PKI provides the basis upon which trust can be established between individuals and organizations. Secure deployment of PKI is heavily dependent on the ability of individuals to store and manage their private keys safely.

MyID provides additional components allowing integration with a range of Certificate Authorities. This enhances the security of an existing PKI by enabling the storage and management of digital identities and certificates using smart cards.

1.1 Software bill of materials

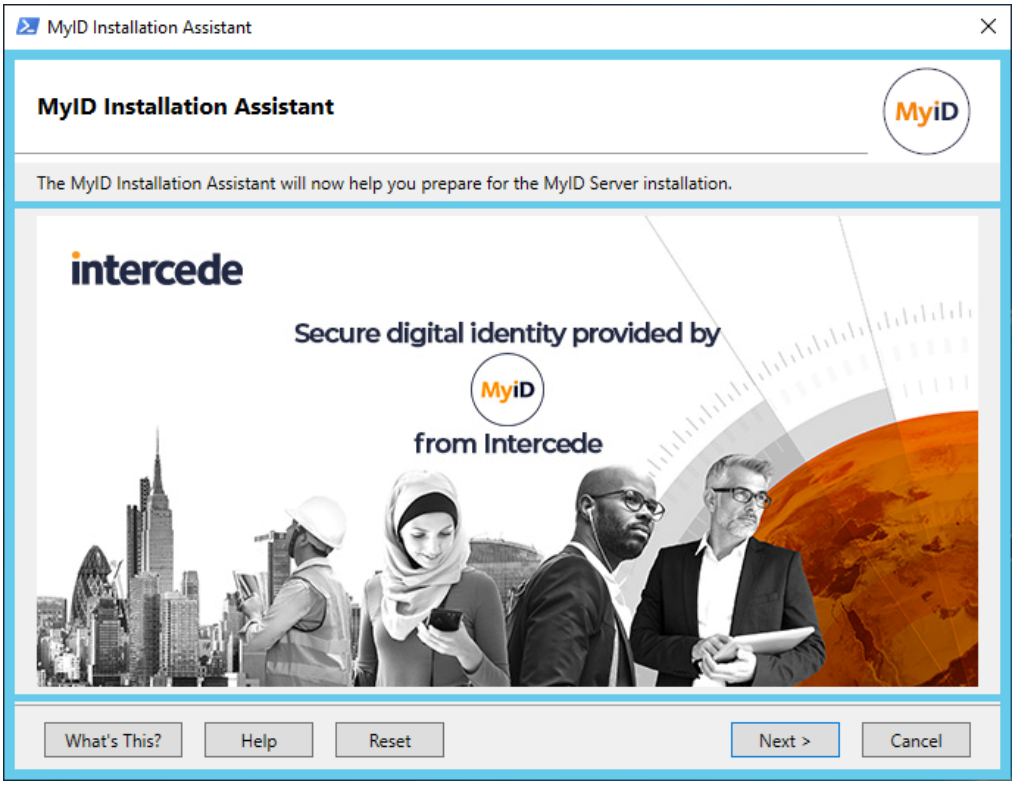
The US President's *Executive Order on Improving the Nation's Cybersecurity* (May 2021) demanded that a Software Bill of Materials is made available for critical software, as part of a range of activities aimed at enhancing software supply chain security.

A software bill of materials (SBOM) is a list of components in a piece of software. Software vendors often create products by assembling open source and commercial software components, in addition to proprietary components they have created. The SBOM describes the components in a product.

An SBOM can be used to perform vulnerability or license analysis, both of which can be used to evaluate risk in a product. Those who operate software can use SBOMs to determine quickly and easily whether they are at potential risk of a newly-discovered vulnerability.

For further information about the MyID SBOM, or to request access, contact Intercede customer support quoting reference SUP-359.

2 MyID Installation Assistant



The MyID Installation Assistant provides a comprehensive way of installing MyID and keeping it updated with the latest software packages. Combining the features of the installation program, a package manager, the System Interrogation Utility, and the Server Diagnostic Report, the MyID Installation Assistant guides you through the process of installing MyID, including:

- Checking your system requirements.
- Checking your network connectivity, including access to specific ports.
- Assisting with https configuration.
- Checking system configuration.
- Gathering information for the installation process.
- Checking pre-install requirements, including the ability to fix issues using PowerShell scripts.
- Running the installation program without further user input.
- Carrying out post-installation configuration.
- Checking post-install requirements, including the ability to fix issues using PowerShell scripts.
- Producing a Server Diagnostic Report .

The MyID Installation Assistant also incorporates a package manager, which means it can install MyID Server (for example, MyID 12.4.0), install an update (for example, MyID 12.4.2), install a server configuration package for custom functionality (for example, CONFIG-9999.1.1) and a hotfix (for example, HOTFIX-12.4.2.1) to install a complete system with the latest software without the need to run multiple installation packages manually in the correct order. You can drop an update or another package into the installation folder of an already-installed system, run the MyID Installation Assistant, and it picks up the available software in the package manager and allows you to update your system.

You can also use the MyID Installation Assistant to carry out upgrades from existing MyID 11 and MyID 12 systems. For upgrades from MyID 11 the Installation Assistant handles the changes from 32-bit to 64-bit software without the need to run a separate upgrade migration script.

At each stage of the process, you can close the MyID Installation Assistant, and when you return to it later it remembers all the details you have already entered. This allows you to carry out your system configuration in stages.

2.1 MyID Installation Assistant use cases

The MyID Installation Assistant allows you to carry out a wide variety of installation procedures for a variety of purposes. This section contains some example use cases.

2.1.1 Checking your system before installation

You can use the MyID Installation Assistant to check that your system is ready to install MyID without selecting any software to install; the MyID Installation Assistant runs through the full series of network connectivity checks, initial server checks, and pre-installation checks, allowing you to set up your infrastructure before you start the MyID installation process.

2.1.2 Installing a quick demo system

You can use the MyID Installation Assistant to set up a single-server demonstration system, with application server, web server, and database server on the same physical machine. The MyID Installation Assistant guides you through the installation process, and allows you to create a self-signed or domain-signed certificate to secure the https connection to the MyID website; this does not provide the same level of security as a certificate from a commercial provider on a production system, but is useful for evaluating the possibilities of MyID.

For more information, see section *2.9*, *Configuring https*.

2.1.3 Installing a secure multiple tier production system

The MyID Installation Assistant handles installing a MyID system across multiple servers where the application components, websites and web services, and database reside on different machines, and checks the infrastructure and communication between these server tiers. You can select a commercial https certificate to secure the https connection to the MyID website, ensuring the highest grade of protection for your production system.

For more information, see section *8.2*, *Split deployment*.

2.1.4 Checking an existing installation

You can run the MyID Installation Assistant to perform checks against your existing system without selecting any software to install; the MyID Installation Assistant runs through the full series of initial server checks, pre-installation checks, and post-installation checks, producing a Server Diagnostic report at the end. Note, however, that these checks are based on the version of MyID provided with the MyID Installation Assistant; for example, if you have MyID 12.3 installed, and run the MyID 12.4 Installation Assistant, it checks whether your system meets the requirements for MyID 12.4.

For more information, see:

- section *2.16*, *Initial server check results*.
- section *2.18*, *Pre-installation check results*.
- section *2.22*, *Post-installation check results*.
- section *2.23*, *Server Diagnostic Report*.

2.1.5 Applying an update, server configuration package, or hotfix

If you add an update installation file, a server configuration package, or hotfix to the package manager, you can use the MyID Installation Assistant to apply these updates to your installed system.

For more information, see:

- section *2.6*, *The Installation Package Manager*.
- section *2.24*, *Applying an update*.
- section *2.25*, *Installing a server configuration package*.
- section *2.26*, *Applying a hotfix*.

2.1.6 Upgrading MyID to the latest version

If you have an existing MyID 11 or 12 system, you can use the MyID Installation Assistant to upgrade your system to the latest version of MyID. The MyID Installation Assistant carries out a full series of checks to ensure that your system meets the latest requirements for the new version of MyID.

For more information, see section *2.27*, *Upgrading MyID*.

2.2 Installing the MyID Installation Assistant

You must install the MyID Installation Assistant on each server on which you want to install MyID. On a single-tier system, where the application, web, and database components are all installed on the same PC, you can install all the MyID components at the same time. To implement a split deployment, where the MyID application, web, and database components are installed on different physical machines, you install the MyID Installation Assistant on different machines, and then follow a strict implementation procedure to ensure the various servers are created in the correct order; see section *8.2*, *Split deployment* for details.

2.2.1 Trusting the signed scripts

The scripts that are used in the installation process are signed to confirm that they were provided by Intercede and have not been altered. If your system is configured to allow only signed PowerShell scripts to be run, you must trust Intercede as a publisher before you run the installation program. If you do not follow these instructions, the scripts will not run.

To trust Intercede as a publisher:

1. In the following folder:

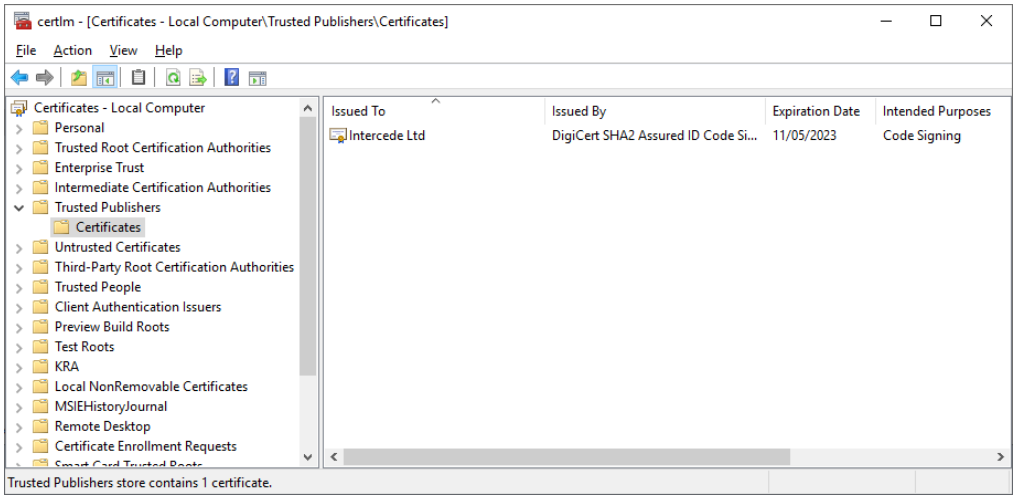
   `<install folder>\Support Tools\MyIDInstallationAssistant`

   right-click the following script:

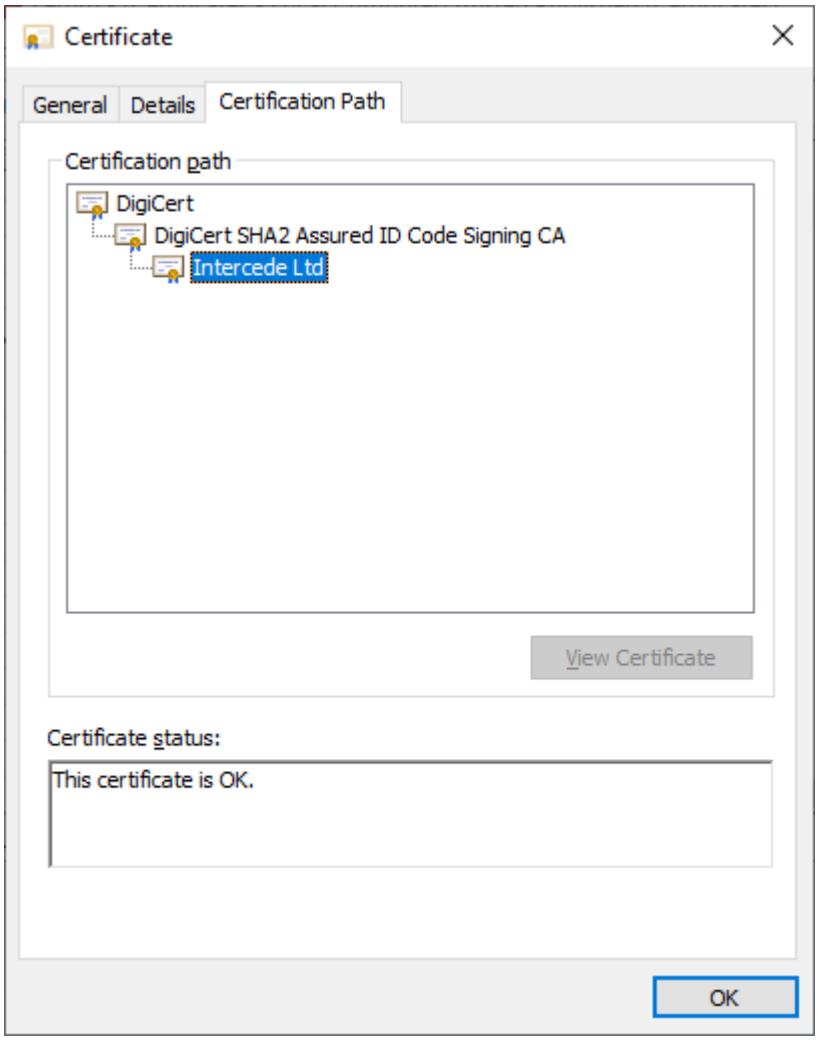
   `MyIDInstallationAssistant.ps1`

2. In the Properties dialog, click the **Digital Signatures** tab.
3. Select the Intercede signature in the signing list, and click **Details**.
4. Click **View Certificate**.
5. Click **Install Certificate**.
6. Select **Local Machine**, and click **Next**.
7. Select **Place all certificates in the following store**, click **Browse**, select the **Trusted Publishers** store, and click **OK**.
8. Click **Next**, then click **Finish**.

   The certificate is now installed to the Trusted Publishers store.



Note: This certificate depends on DigiCert certificates:



You must obtain the DigiCert SHA2 Assured ID Code Signing CA and DigiCert root CA certificates from DigiCert if your server does not already have them.

2.2.2 Running the installation script

Important: The MyID uninstallation process requires PowerShell scripts that are provided as part of the MyID Installation Assistant package. If you move or delete the installation folder, you will be unable to uninstall MyID using the Windows Control Panel **Programs and Features** option; when it is unable to locate the scripts, the uninstallation process displays an error. You are strongly recommended to retain the MyID installation folder in the location from which you originally ran the installation program; this may influence your choice of folder from which to install MyID.

You must also continue to use the same installation folder for any future updates or upgrades; see section *2.2.4*, *Upgrading or updating the MyID Installation Assistant*.

To install the MyID Installation Assistant:

1. Log on to the server as the MyID installation user.

   See section *6.1.1*, *Installation account* for details of the requirements of this user account.

2. Copy the installation package to the server and extract all the files.

   The installation folder contains:

   - The `Installer` folder – this contains the MyID installation program.
   - The `Product Documentation` folder – this contains a copy of the MyID documentation set.
   - The `Support Tools` folder – this contains the MyID Installation Assistant scripts.

   The root of the folder contains a readme and batch files to install and uninstall the MyID Installation Assistant.

3. Open a Windows command window.

   This allows you to see any messages that the installation process produces.

4. Navigate to the installation folder and run the installer batch file:

   ```
   Install-MyIDInstallationAssistant.bat
   ```

   The installation script creates a MyID Installation Assistant icon on the desktop, and sets up the MyID Installation Assistant to access the MyID product documentation. If IIS is installed on the server, you can access the documentation through the following URL:

   ```
   http://localhost:8080/ProductDocs/
   ```

Note: If you see a message similar to the following when running the `Install-MyIDInstallationAssistant.bat` batch file:

```
Do you want to run software from this untrusted publisher?

File C:\Install\Support Tools\MyIDInstallationAssistant\Installer\Install-MyIDInstallationAssistant.ps1 is published by CN=Intercede Ltd, O=Intercede Ltd, L=Lutterworth, C=GB and is not trusted on your system. Only run scripts from trusted publishers.
```

This means that your system is not configured to trust signed scripts from Intercede. You must add the certificate to the Trusted Publishers store; see section *2.2.1*, *Trusting the signed scripts* above.

2.2.3 Uninstalling the MyID Installation Assistant

Note: You are recommended to keep the MyID Installation Assistant installed. The installation folder contains scripts that are required to uninstall the MyID server software, and you can use the MyID Installation Assistant to apply updates, configuration packages, and hotfixes to your installed system. Uninstall the MyID Installation Assistant only when you have uninstalled MyID from your server and have no further use for the software.

To uninstall the MyID Installation Assistant:

1. Log on to the server as the MyID installation user.

   See section *6.1.1*, *Installation account* for details of the requirements of this user account.

2. Open a Windows command window.

3. Navigate to the installation folder and run the uninstaller batch file:

   ```
   Uninstall-MyIDInstallationAssistant.bat
   ```

   The uninstallation script removes the MyID Installation Assistant icon from the desktop, and removes the link to the MyID product documentation, including removing the documentation site from IIS if necessary.

2.2.4 Upgrading or updating the MyID Installation Assistant

Important: If you already have an installation of MyID that was carried out using the MyID Installation Assistant, you *must* prepare the installation folder before you start an upgrade or update process.

You are strongly recommended to retain the MyID installation folder in the location from which you originally ran the installation program. You can then update this installation folder with the new installation files (documentation, installers, PowerShell scripts and so on) from the new installation media, and carry out the update or upgrade from the same folder using the MyID Installation Assistant.

To prepare the installation folder:

1. Back up the `Support Tools\MyIDInstallationAssistant` folder.

   This prevents the loss of any `TestReports` and `TestReportsRedacted` folders or any modified defaults settings.

   You may also want to archive the entire installation folder as a permanent record.

2. Run the uninstallation script for the MyID Installation Assistant.

   See section *2.2.3*, *Uninstalling the MyID Installation Assistant*.

3. Copy the contents of the upgrade or update zip file into the existing installation folder, overwriting any existing files or folders.

   Make sure you copy the files and folders to the same locations; that is, the `Support Tools\MyIDInstallationAssistant\` folder into `Support Tools\MyIDInstallationAssistant\` and so on. The folder structure will be the same for the new installation media, although there may be additional files and folders provided.

4. Run the installation script for the MyID Installation Assistant.

   See section *2.2.2*, *Running the installation script*.

Once you have updated your installation folder, you can carry out the upgrade or update process. See section *7*, *Upgrading MyID* and section *9*, *Updating MyID* for more information.

2.3 Running the Installation Assistant

Once you have installed the MyID Installation Assistant, you can launch it from the icon on the desktop:

You must run the MyID Installation Assistant using an account with the appropriate permissions. See section *6.1.1*, *Installation account* for details of the requirements for this account.

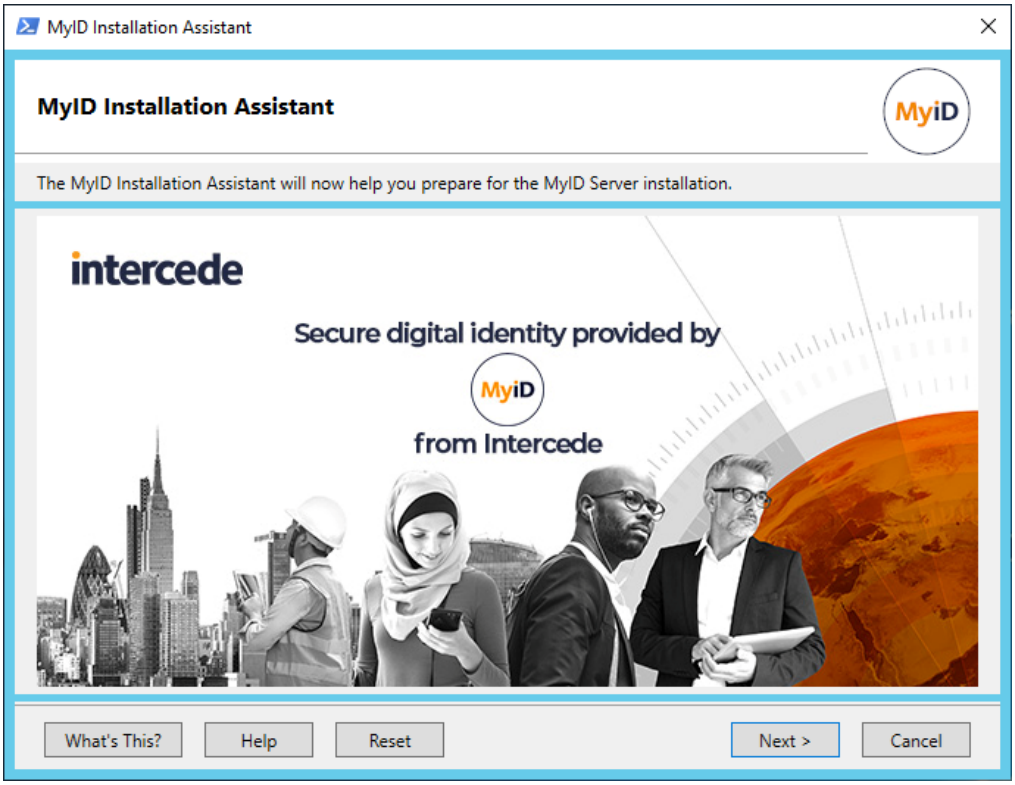
As an alternative to using the desktop icon, you can open a Windows PowerShell command prompt (with elevated permissions) and navigate to the following folder:

```
<install folder>\Support Tools\MyIDInstallationAssistant\
```

Then run the following script:

```
.\MyIDInstallationAssistant.ps1
```

This provides you with some additional debug information in the console.



Click **Next** to move to the first stage.

2.4 Navigating the Installation Assistant

The following buttons are available, depending on the screen.

- **Refresh**

  Appears on check results screens. If you have updated your system configuration, you can use this to run the tests again.

- **What's This?**

  Appears on the first screen, and links to an overview of MyID Installation Assistant in the documentation.

- **Help**

  Provides a context-sensitive link to instructions for working on the current screen in the documentation.

- **Reset**

  Appears on the first screen. Carries out a reset of the information you have added to the MyID Installation Assistant and allows you to start the process again.

  Note: If you are carrying out an upgrade, this option does not delete any information you have added to the MyID Installation Assistant or has been obtained from the previous installation. You can start the process from the first screen but the information is retained; this prevents the loss of information from the previous installation.

- **Back**

  Goes back to the previous screen. You can move backwards and forwards through the screens without losing any information you have added.

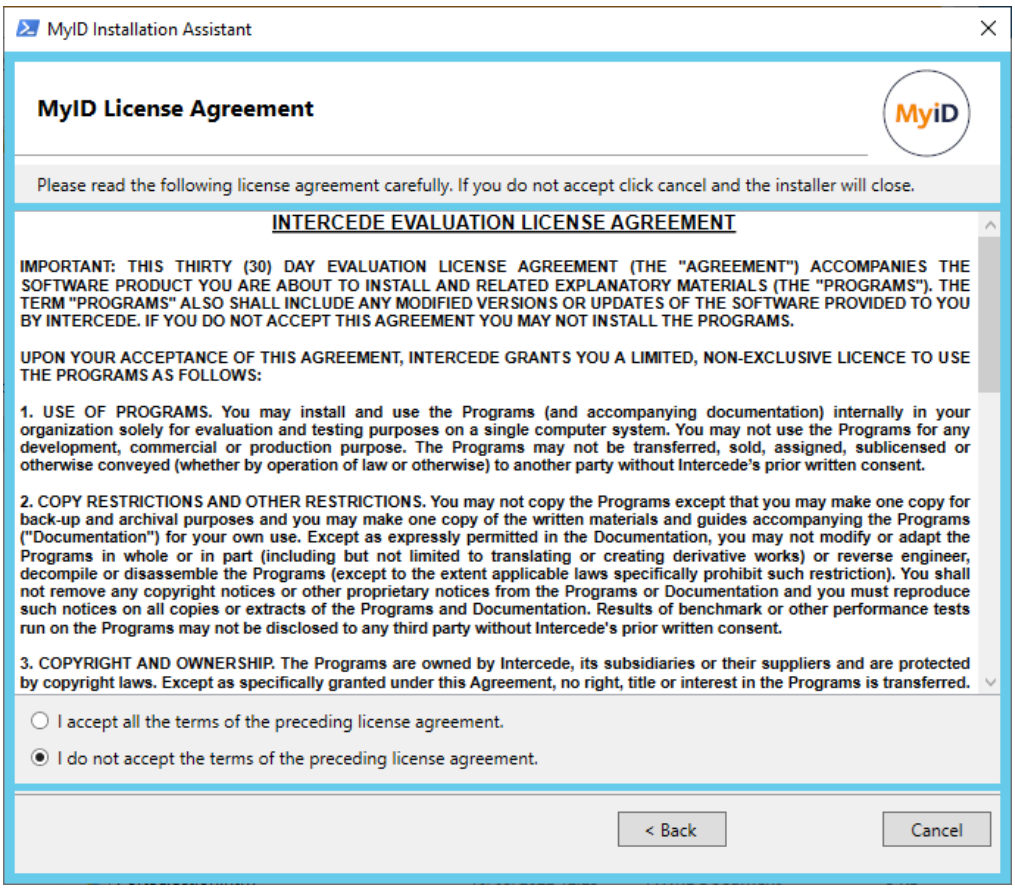
- **Next**

  Goes on to the next screen. You can progress to the next screen once you have provided all the mandatory information on the current screen, and once the MyID Installation Assistant has carried out any checks or processing for the current stage.

- **Cancel**

  At each stage of the process, you can close the MyID Installation Assistant, and when you return to it later it remembers all the details you have already entered. This allows you to carry out your system configuration in stages.

2.5 Accepting the license agreement



1. Read through the license agreement.

   Note: The license details are also available in the `License.rtf` file in the `Installer` folder.

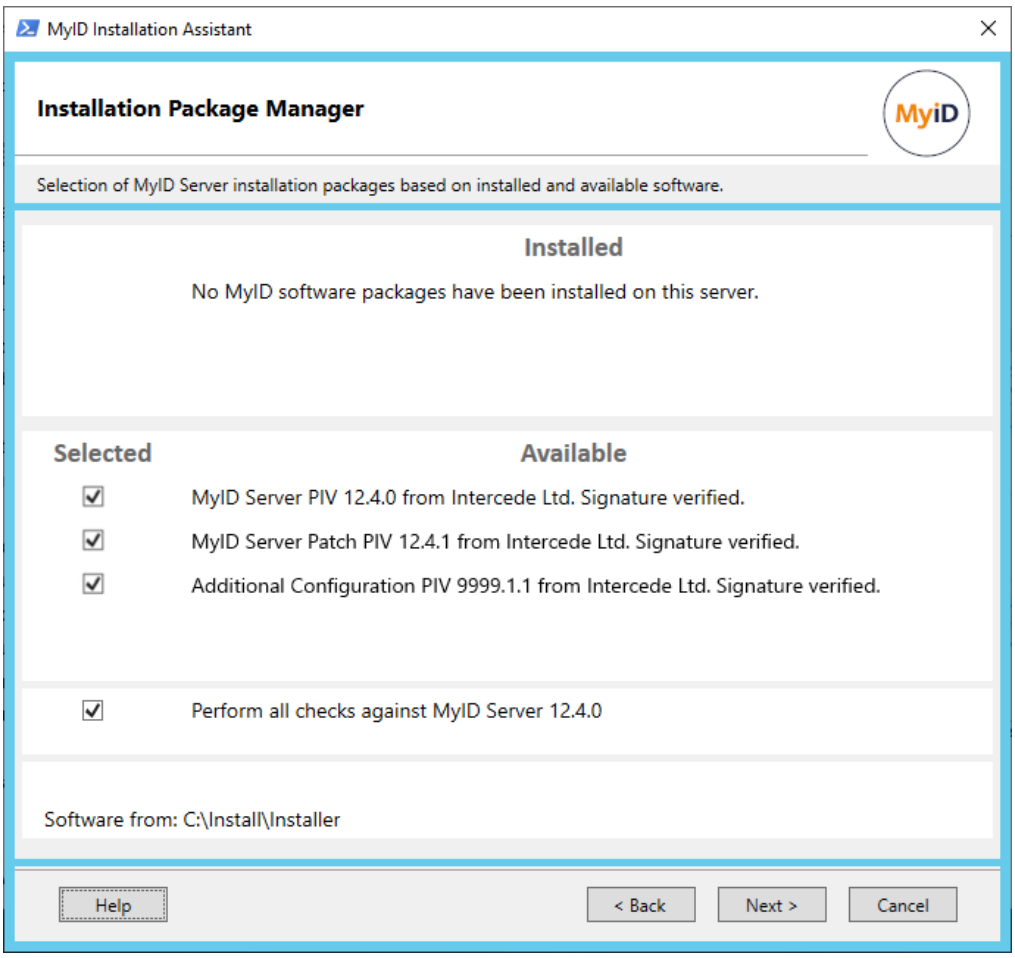
   This agreement covers the 30-day evaluation license provided with your installation of MyID. When you first install MyID, this license allows you to use MyID for up to 30 days, and allows you to add up to 250 user accounts and credentials. Once you have installed MyID, you can request a license from within MyID using the **Licensing** workflow. Full licenses may be subject to additional agreements.

   See the *License management* section of the ***Administration Guide*** for details.

2. If you accept, click **I accept all the terms of the preceding license agreement** and click **Next**.

   If you do not accept, click **Cancel** and the MyID Installation Assistant closes.

2.6 The Installation Package Manager



The Installation Package Manager checks to see what MyID software is installed, scans the `Installer` folder for any MyID software installation packages on the server, and presents a list of the suitable software packages for your installation.

For example, you may have:

- No MyID software currently installed.
- MyID 12.4 available for installation as a new install.
- MyID 12.4.1 available as an update for MyID 12.4.
- Configuration update CONFIG-9999.1.1 available for installation.

As another example, you may have:

- MyID 12.3 already installed.
- MyID 12.4 available as an upgrade for MyID 12.3.
- MyID 12.4.1 available as an update for MyID 12.4.

The package manager recommends base software, upgrades, updates, and additional configuration, as appropriate for your system.

If, for example, you had an installation package for MyID 12.0.1 in the `Installer` folder when you already had 12.3 installed, the Installation Package Manager would not display it in the list, because it is not appropriate for your system.

You also have the option to perform checks that are appropriate for your system. You are strongly recommended to carry out these checks every time you install any MyID server software to ensure that your system is still in the correct state to install MyID. If you want to carry out the checks without installing any software, deselect the software packages in the **Available** list and select only the checks option.

If you have multiple packages available to install, the sequence of installation is:

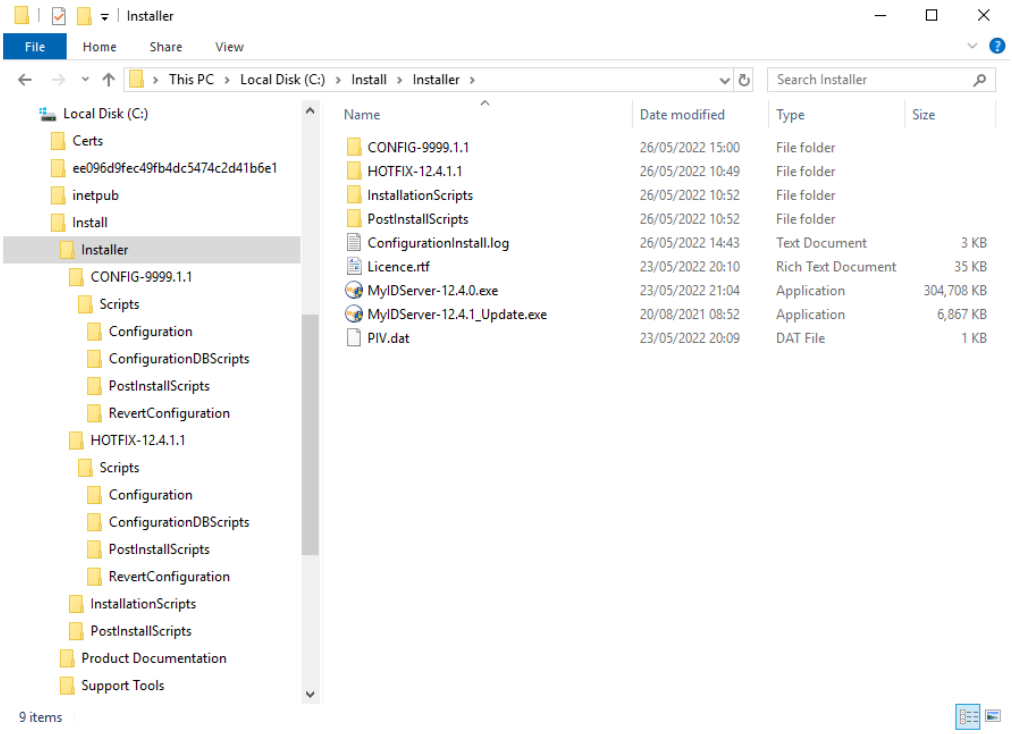
1. Main MyID installation (fresh install or upgrade).
2. Update installation.
3. Server configuration installation.
4. Hotfix installation.

Once you have selected the packages you want to install, click **Next** to move to the next stage.

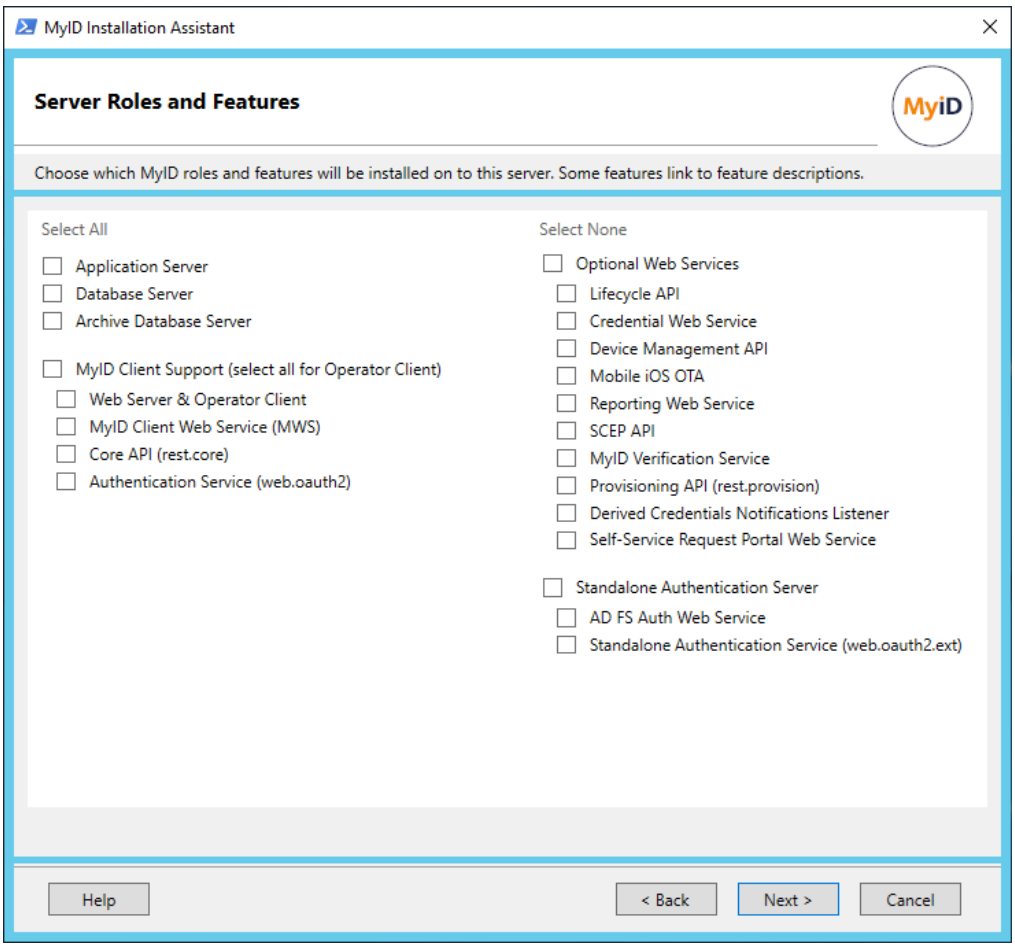
2.6.1 Adding software to the package manager

To make software available to the package manager, you must add the installation materials to the `Installer` folder.

- For updates (for example, `MyIDServer-12.4.1_Update.exe`) copy the installation program into the `Installer` folder, at the same level as the main MyID installation program.
- For server configuration updates (for example, `CONFIG-9999.1.1`) create a folder for the update in the `Installer` folder, then copy the files from the server configuration update zip file into this folder so that the `Scripts` folder is immediately under the folder you created.
- For hotfixes (for example, `HOTFIX-12.4.1.1`) create a folder for the update in the `Installer` folder, then copy the files from the hotfix zip file into this folder so that the `Scripts` folder is immediately under the folder you created.



2.7 Selecting the server roles and features



The Server Roles and Features screen allows you to select which components you want to install on the current server. If you are performing checks against your server without installing any software, you must still select the server components so that the MyID Installation assistant carries out the appropriate checks.

On a single-tier system, where the application, web, and database components are all installed on the same PC, you can install all the MyID components at the same time. To implement a split deployment, where the MyID application, web, and database components are installed on different physical machines, you must follow a strict implementation procedure to ensure the various servers are created in the correct order; see section *8.2*, *Split deployment* for details.

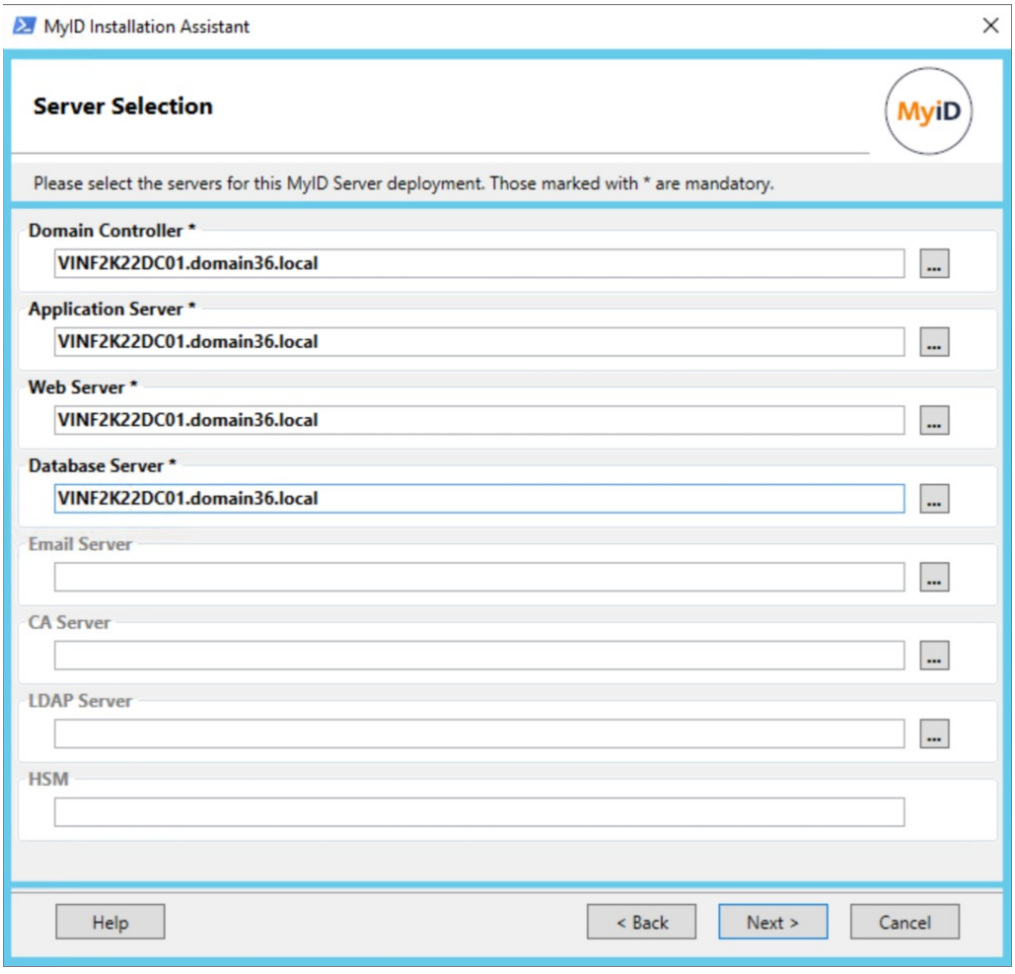
The following components are available:

- **Application Server** – contains the MyID application components.
- **Database Server** – contains the MyID database.
- **Archive Database Server** – contains a database that can contain an archive of some parts of the MyID database. Creating the database does not set up the archiving procedures; the *Database configuration* section in the ***Advanced Configuration Guide*** for details.
- **MyID Client Support** – contains the web server components that the MyID clients use to communicate with the server. This includes:
  - **Web Server & Operator Client** – contains the main MyID web server, including the websites for MyID Desktop and the MyID Operator Client.
  - **MyID Client Web Service (MWS)** – required for MyID Desktop, the Self-Service App, the Self-Service Kiosk, and mobile clients.
  - **Core API (rest.core)** – required for the MyID Operator Client. This contains the rest.core web service that you can also use for your own systems; see the ***MyID Core API*** guide for details.
  - **Authentication Service (web.oauth2)** – required for the MyID Operator Client. This contains the web.oauth2 web service that you can also use for your own systems; see the ***MyID Authentication Guide*** guide for details.
- **Optional Web Services** – contains web services that are required for optional features of MyID.
  - **Lifecycle API** – see the ***Lifecycle API*** guide.
  - **Credential Web Service** – see the ***Credential Web Service*** guide.
  - **Device Management API** – see the ***Device Management API*** guide.
  - **Mobile iOS OTA** – see the *Setting up iOS OTA provisioning* section in the ***Mobile Identity Management*** guide.
  - **Reporting Web Service** – see the ***Reporting Web Service API*** guide.
  - **SCEP API** – see the *Managing devices* section in the ***Administration Guide***.
  - **MyID Verification Service** – see the *MyID Verification Service* section in the ***Mobile Authentication*** guide.
  - **Provisioning API (rest.provision)** – used for issuing mobile credentials, mobile identity documents, and soft certificates. See the *REST API for mobile credentials* section in the ***Implementation Guide***.
  - **Derived Credentials Notifications Listener** – see the ***Derived Credentials Notifications Listener API*** guide.
  - **Self-Service Request Portal Web Service** – see the ***Derived Credentials Self-Service Request Portal*** guide.

- **External Authentication Server** – contains web services for use with external authentication. Select the following options:
  - **AD FS Auth Web Service** – see the *Installing the ADFS Auth web service* section in the ***MyID Authentication Guide***.
  - **Standalone Authentication Service (web.oauth2.ext)** – see the *Setting up the standalone authentication service* section in the ***MyID Authentication Guide***.

Once you have selected the features you want to install or check, click **Next** to move to the next stage.

2.8 Selecting the servers



The Server Selection screen allows you to specify the servers to use for the pre-install connectivity checks; for example, can your web server communicate with your application server; can your application server communicate with your certificate authority; and so on.

In a complex environment, you may have multiple servers carrying out the same role; for example, multiple web servers for load balancing. You may also install some web services on a different server to the main MyID website, or install an archive database on a separate server to the main MyID database. In these cases, you are recommended to specify a representative server for the initial checks, then re-run the MyID Installation Assistant pre-install checks on your servers, selecting your other servers in the appropriate category.

To specify a server, *either*:

- Type the name of the server in the relevant field, *or*
- Click the browse option **...** to browse your Active Directory.

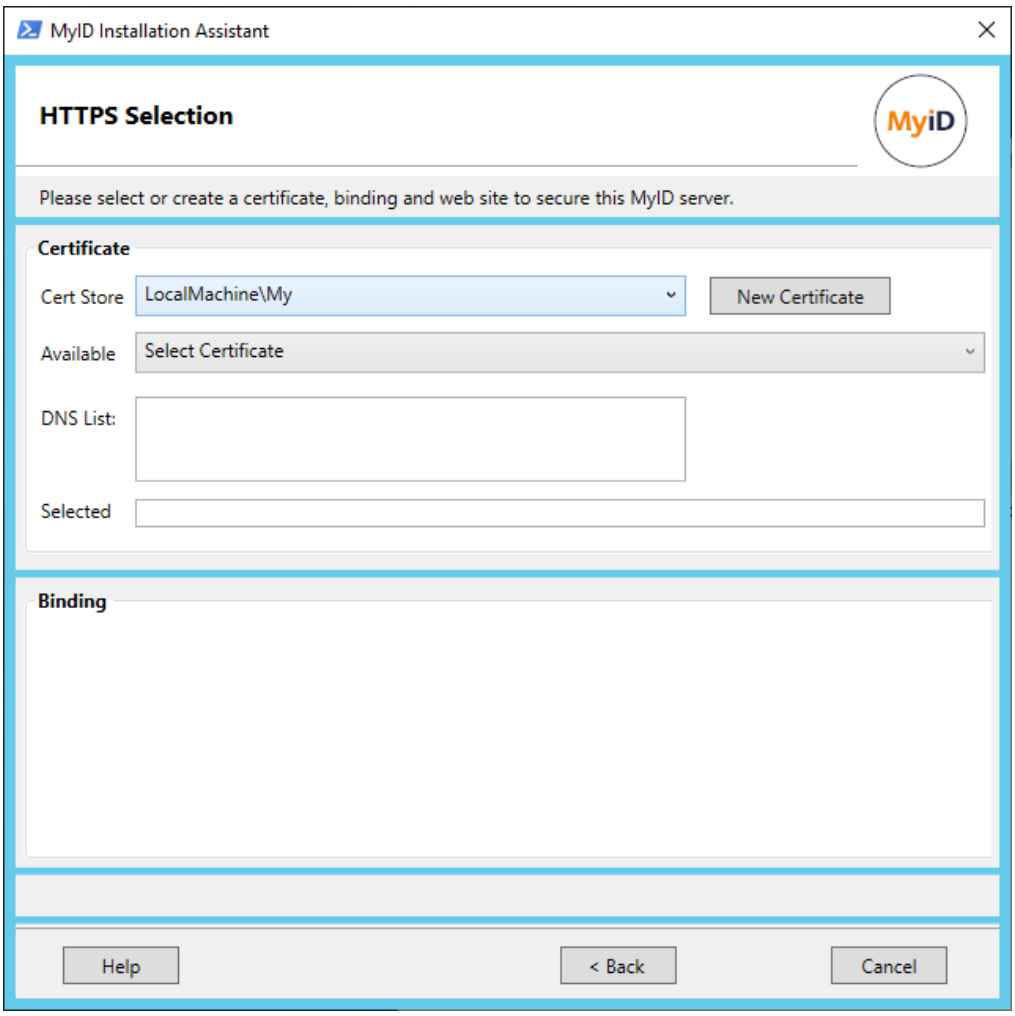
  The initial search of your directory may take some time, but the MyID Installation Assistant caches the details until you close it down, so subsequent browsing of the directory is quicker.

If you are using an HSM, type the IP address or DNS name of the HSM.

Mandatory servers are marked with an asterisk *****.

Once you have provided the details of your servers, click **Next** to proceed to the next stage.

2.9 Configuring https



Using https for communication with your web server is far more secure than using http, and you are strongly recommended to configure this for your system.

Important: The web services used by the MyID Operator Client (`rest.core` and `web.oauth2`) *require* SSL/TLS; if you do not connect through https, you *cannot* use the MyID Operator Client.

The MyID Operator Client helps you set up and test your https configuration. For pre-production systems, the MyID Installation Assistant allows you to create a self-signed certificate, or a domain-signed certificate using a Microsoft CA, to secure your https connection; however, for production systems, you are strongly recommended to obtain a certificate provided by a commercial CA provider, which has the advantage that the root certificate already exists in your certificate store and is trusted in most browsers by default.

Setting up SSL requires the following:

- Protocol – you must use the https protocol to communicate with the website.
- Certificate – the connection is secured by a certificate. This certificate may be self-signed, domain-signed, or obtained from a commercial CA provider; the MyID Installation Assistant allows you to use any of these.
- Binding – the certificate is bound to the website that will contain the MyID web pages and services using a specific port. The MyID Installation Assistant allows you to select an existing binding, or to set up a new binding.

For more information about https and SSL/TLS, see the *Configuring SSL/TLS (HTTPS)* section in the ***Securing Websites and Web Services*** document.

2.9.1 Selecting an existing certificate and binding

If you have already set up IIS with your certificate and bound it to the website, you can select it on this screen.

1. From the **Cert Store** drop-down list, select the certificate store that contains the certificate you are using for https.
2. From the **Available** drop-down list, select the certificate you are using for https.

   The details of the certificate are shown in the **Certificate** section, and the details of the binding are show in the **Binding** section.
3. Click **Next** to proceed to the next stage.

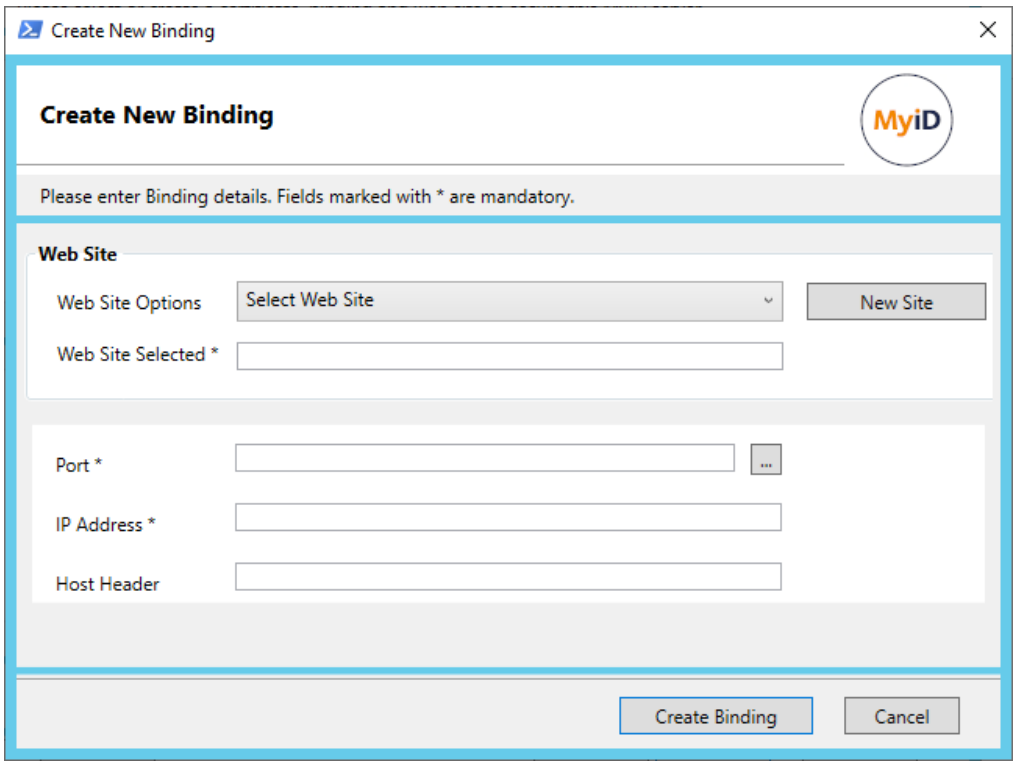
2.9.2 Selecting an existing certificate and creating a new binding

If you have a certificate available to IIS, but have not yet bound it to the website you are going to use for MyID, you can use the MyID Installation Assistant to create a new binding.

1. From the **Cert Store** drop-down list, select the certificate store that contains the certificate you want to use for https.
2. From the **Available** drop-down list, select the certificate you want to use for https.

3. Click **New Binding**.

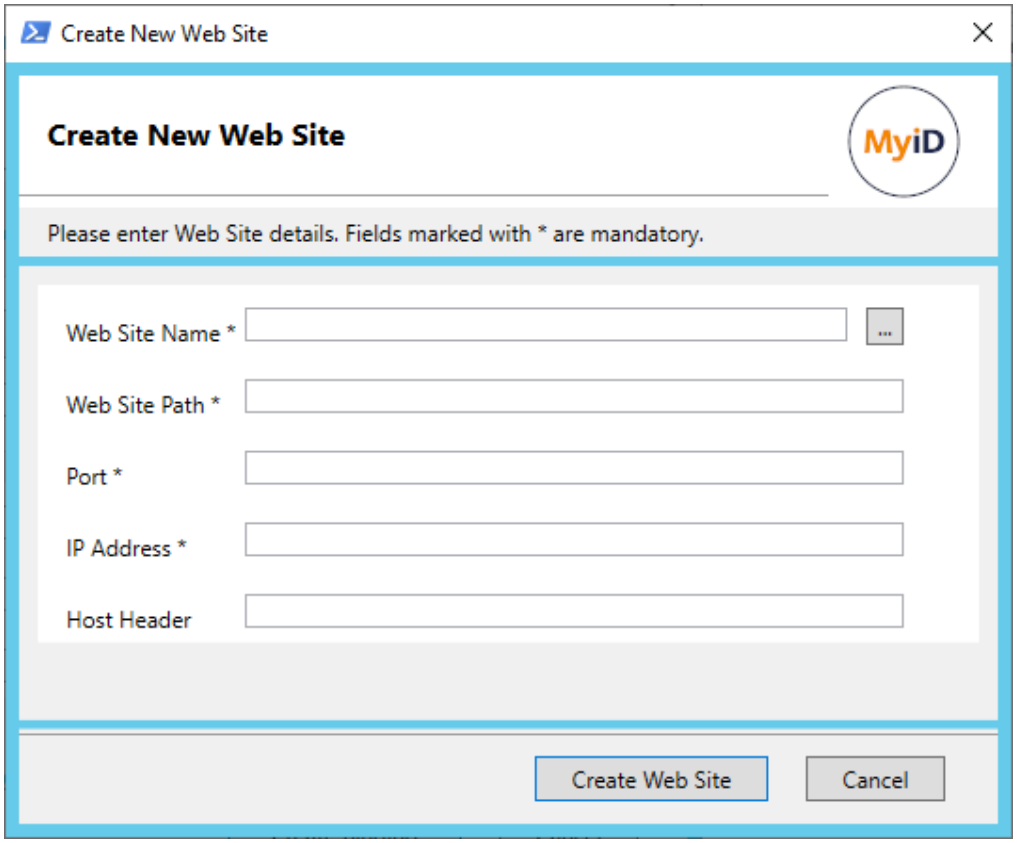
   The Create New Binding screen appears:



4. Select the website you are going to use for MyID from the **Web Site Options** drop-down list.

   If necessary, you can create a new website:

   a. Click **New Site**:



   b. Provide the following details:

      - **Web Site Name** – the site name for the new website.
      - **Web Site Path** – the physical path for the new website.
      - **Port** – the port to be used for the binding.
      - **IP Address** – the IP address for the binding. Type * to specify all unassigned IP addresses.
      - **Host Header** – the host name for the website. This is optional, and allows different bindings to handle different client requests to the same website.

      You can click the **...** button to populate the fields with defaults.

   c. Click **Create Web Site** to add the new website to IIS.

5. If you are using an existing website, provide the following details:

   - **Port** – the port to be used for the binding.
   - **IP Address** – the IP address for the binding. Type * to specify all unassigned IP addresses.
   - **Host Header** – the host name for the website.

6. Click **Create Binding**.
7. If the website **Status** is not **Started**, click **Start Website**.
8. Click **Next** to proceed to the next stage.

2.9.3 Creating a new certificate and binding

For pre-production systems only, the MyID Installation Assistant allows you to create a self-signed certificate or a domain-signed certificate to use for https access to the MyID website.

A self-signed or domain-signed certificate has the following limitations compared to a commercial certificate:

Self-signed certificate	Domain-signed certificate	Commercial certificate
Not created using a CA.	Created from a Microsoft CA only.	Created from any CA.
Can be created on split tier or single tier using the MyID Installation Assistant.	Can be created on a single tier system using the MyID Installation Assistant.	Created outside the MyID Installation Assistant.
Can be set up by a user with Domain or Local Admin permissions.	Must be set up by a user with Domain Admin permissions.	Can be set up by a user with Domain or Local Admin permissions.
The root certificate must be copied into the certificate store manually.	The root certificate must be copied into the certificate store manually.	The root certificate already exists in the certificate store and is already trusted in most browsers by default.

To create a new https certificate:

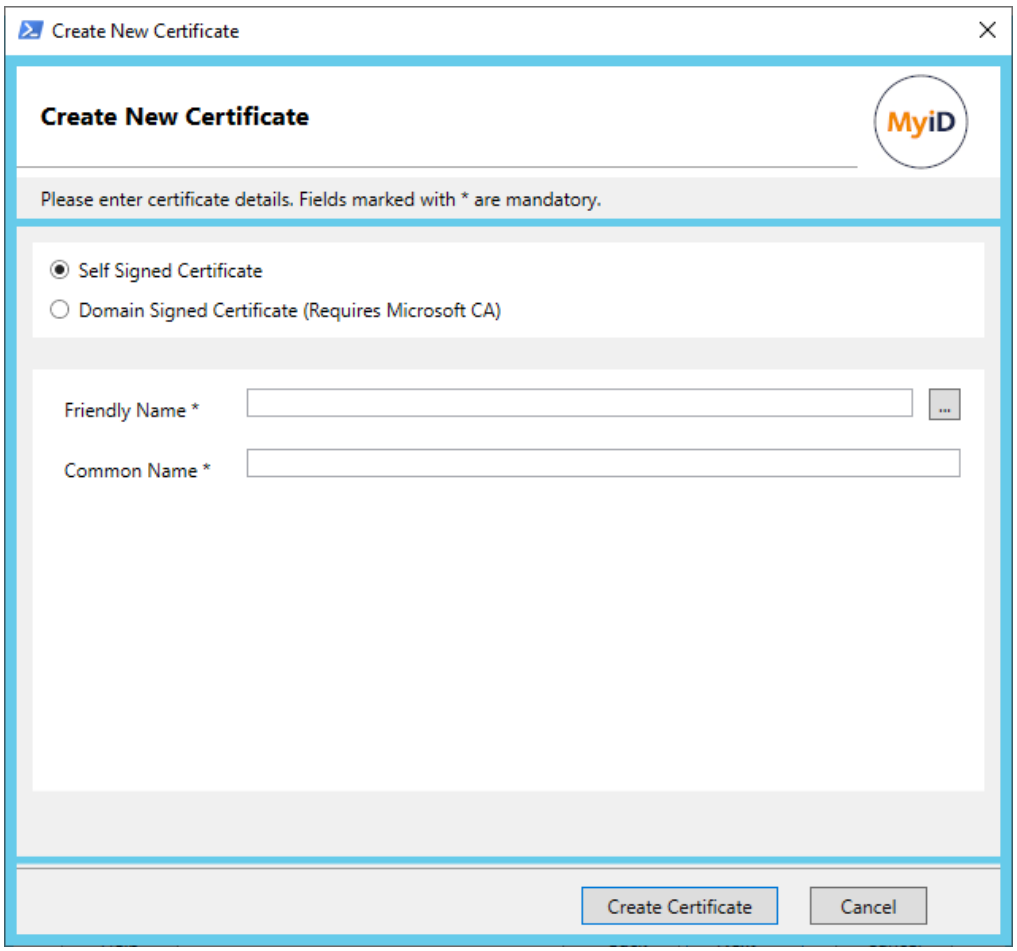
1. Click **New Certificate**.

   The MyID Installation Assistant displays a warning about the limitations of a self-signed or domain-signed certificate. Click **Yes** to continue.

   The Create New Certificate screen appears.

2. Select one of the following options:

   - **Self Signed Certificate**



   Provide the following details for the certificate:

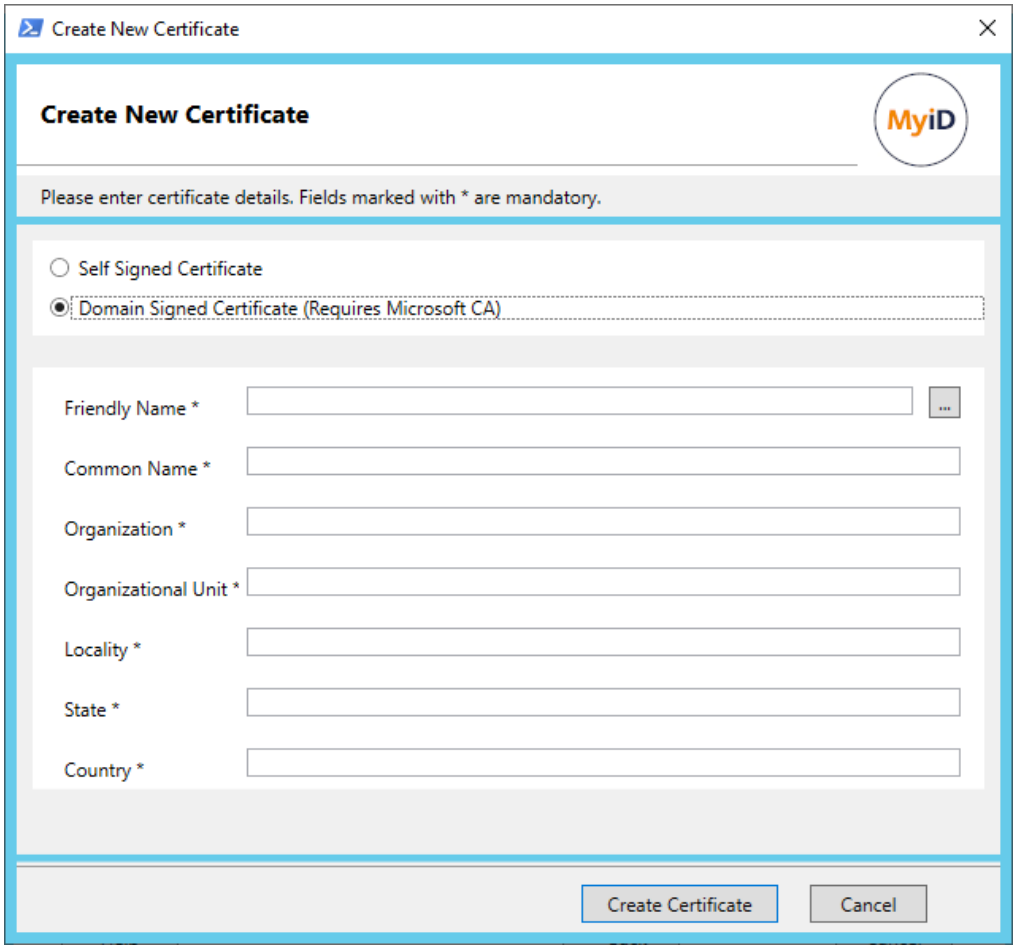
   - **Friendly Name**
   - **Common Name**

   You can click the **...** button to populate the fields with defaults.

   Note: Currently, the MyID Installation Assistant uses the **Common Name** for the Issuer, Subject, and Subject Alternative Name fields in the certificate. If you want to create a self-signed certificate with additional names in the Subject Alternative Name field, see section *2.9.5*, *Specifying subject alternative names in self-signed certificates*.

- **Domain Signed Certificate**

  Important: You must have the correct permissions to create a domain-signed certificate. See section *2.9.4*, *Permissions for domain-signed certificates* for details. If you do not have the correct permissions, this option is disabled.



  Provide the details that will be used to populate the certificate.

  You can click the **...** button to populate these fields with defaults.

3. Click **Create Certificate**.

Once you have created the certificate, you can use it for the binding to the website. Follow the instructions in section *2.9.2*, *Selecting an existing certificate and creating a new binding* above.

2.9.4 Permissions for domain-signed certificates

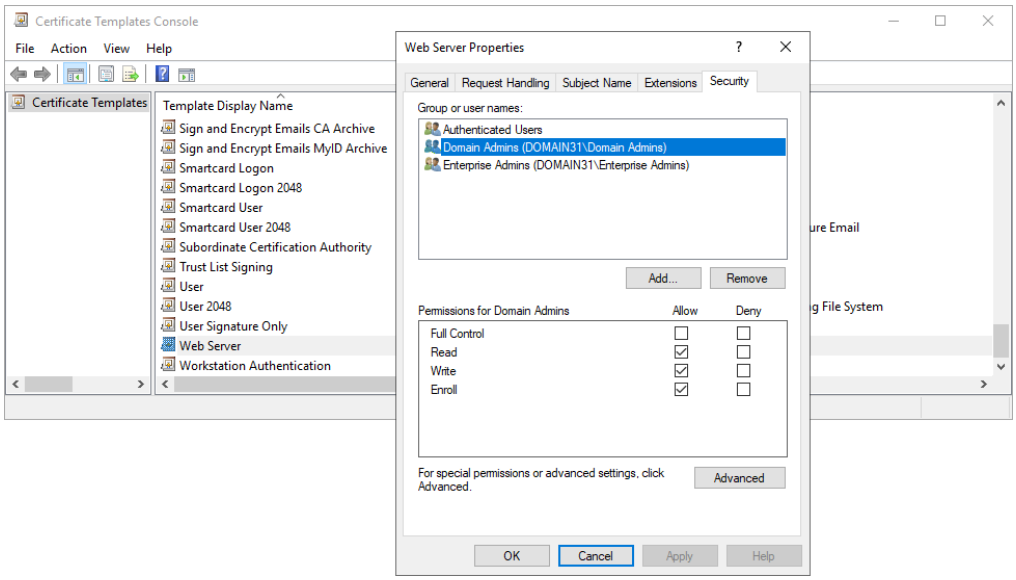
You must have logged on as a domain administrator to create a domain-signed certificate. If necessary, you can close the MyID Installation Assistant, log on as a domain administrator, use the MyID Installation Assistant to create the domain-signed certificate, then log back on as the installation user to continue using the MyID Installation Assistant.

Additionally, the logged-on user must have **Read**, **Write**, and **Enroll** permissions for the **Web Server** certificate template on the Microsoft Certification Authority.

Note: You can create a domain-signed certificate using the MyID Installation Assistant on a single-tier system; you cannot create a domain-signed certificate using the MyID Installation Assistant on a split-tier web server. For split-tier systems, you must create your certificate first before running the MyID Installation Assistant.

To check permissions for the Web Server certificate template:

1. Open the Certification Authority application.
2. Right-click Certificate Templates, then from the pop-up menu select **Manage**.
3. In the Certificate Templates Console, double-click the **Web Server** template.
4. In the Web Server Properties dialog, click the **Security** tab.



5. Verify that the installation user has **Read**, **Write**, and **Enroll** permissions, or belongs to a group that has those permissions.

2.9.5 Specifying subject alternative names in self-signed certificates

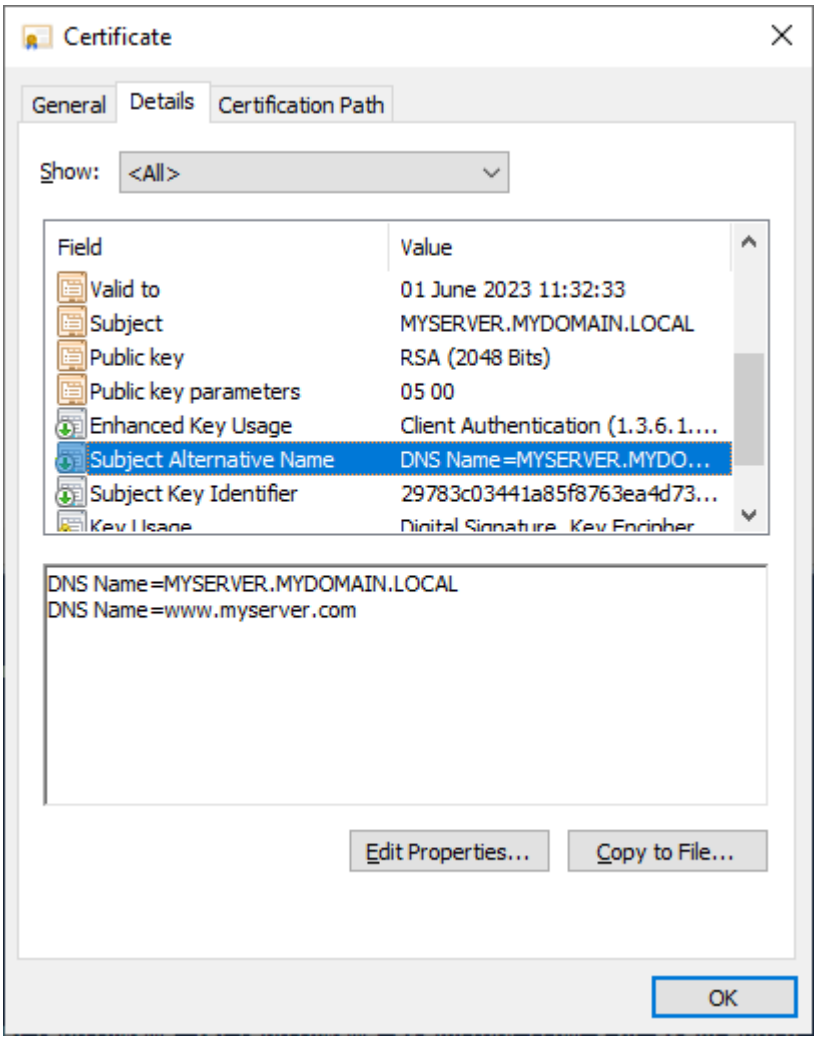
Currently, the MyID Installation Assistant supports only a single name that is used for the Issuer, Subject, and Subject Alternative Name fields in the certificate. If you want to create a self-signed certificate with additional names in the Subject Alternative Name field, you can do so using a PowerShell script, specifying the primary and additional names using the `DnsName` parameter.

For example:

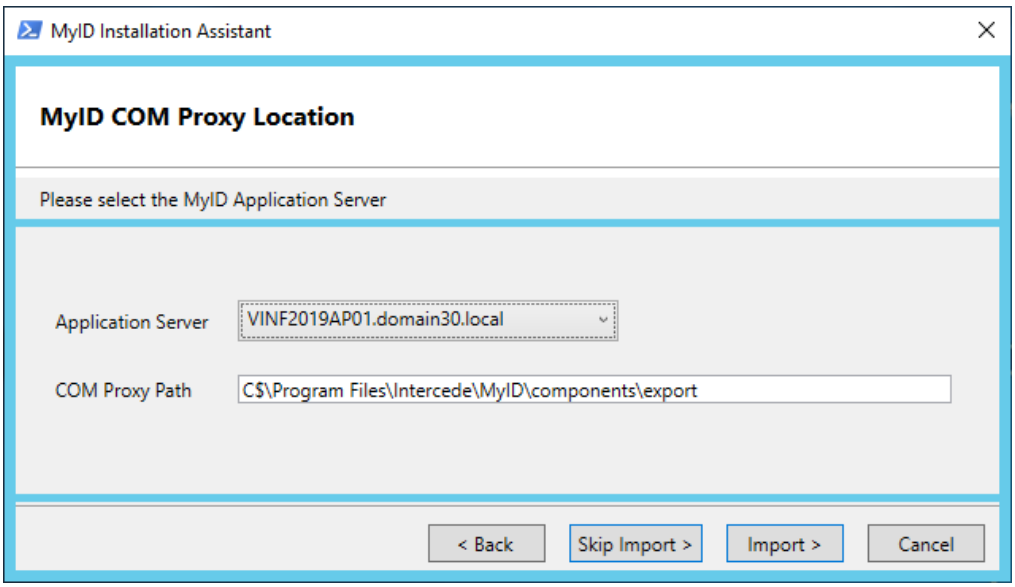
```
$CommonName = "MYSERVER.MYDOMAIN.LOCAL"
$AltName = "www.myserver.com"
$FriendlyName = "Self Signed: MYSERVER.MYDOMAIN.LOCAL"
$temp = New-TemporaryFile
$cert = New-SelfSignedCertificate -CertStoreLocation cert:\LocalMachine\My -DnsName
$CommonName, $AltName -FriendlyName $FriendlyName -KeyAlgorithm RSA -KeyLength 2048
Write-Host "Created Self Signed Certificate"
Export-Certificate -Type CERT -FilePath $temp -Cert $cert | Out-Null
Write-Host "Exported Self Signed Certificate"
Import-Certificate -FilePath $temp -CertStoreLocation cert:\LocalMachine\Root | Out-Null
Write-Host "Imported Self Signed Certificate"
```

This example creates a self-signed certificate that uses `MYSERVER.MYDOMAIN.LOCAL` in the Issuer, Subject, and Subject Alternative Name fields in the certificate, but also adds `www.myserver.com` to the Subject Alternative Name field.

For example:


Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Valid to
01 June 2023 11:32:33
Subject
MYSERVER.MYDOMAIN.LOCAL
Public key
RSA (2048 Bits)
Public key parameters
05 00
Enhanced Key Usage
Client Authentication (1.3.6.1....
Subject Alternative Name
DNS Name=MYSERVER.MYDO...
Subject Key Identifier
29783c03441a85f8763ea4d73...
Key Usage
Digital Signature, Key Encipher
DNS Name=MYSERVER.MYDOMAIN.LOCAL
DNS Name=www.myserver.com
Edit Properties...
Copy to File...
OK

2.10 Installing the COM+ proxies

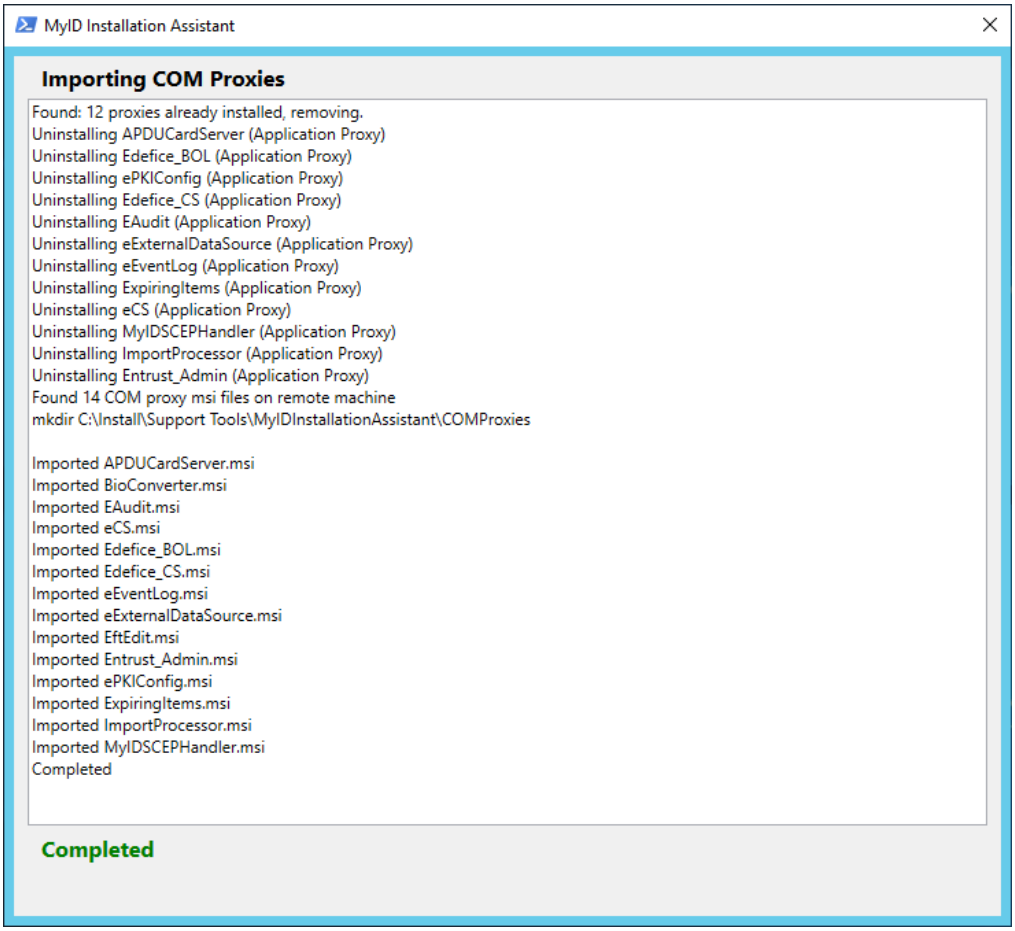


If you are installing on a system where the web server and application server are on different physical machines, you must install COM+ proxies on the web server so that the web server can communicate with the COM+ objects on the application server.

See section *8.2*, *Split deployment* for details.

Important: You must install the application server *before* you install the web server so that the COM+ proxy installers have been created on the application server when you attempt to run them on the web server. This applies to new installations and upgrades.

If you are carrying out an upgrade, the MyID Installation Assistant uninstalls the previous COM+ proxies before installing the new versions from the application server.



2.10.1 Installing the COM+ proxies manually

If you skip this step, you must carry out the import of the COM+ proxies manually before your system will operate. To do this, you must run the .msi files in the following folder on the application server:

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

To run the COM proxy installers, either:

- From the MyID web server, browse to a share on the MyID application server and run the .msi installers directly. For example, browse to:

  ```
  \\<app>\C$\Program Files\Intercede\MyID\Components\Export
  ```

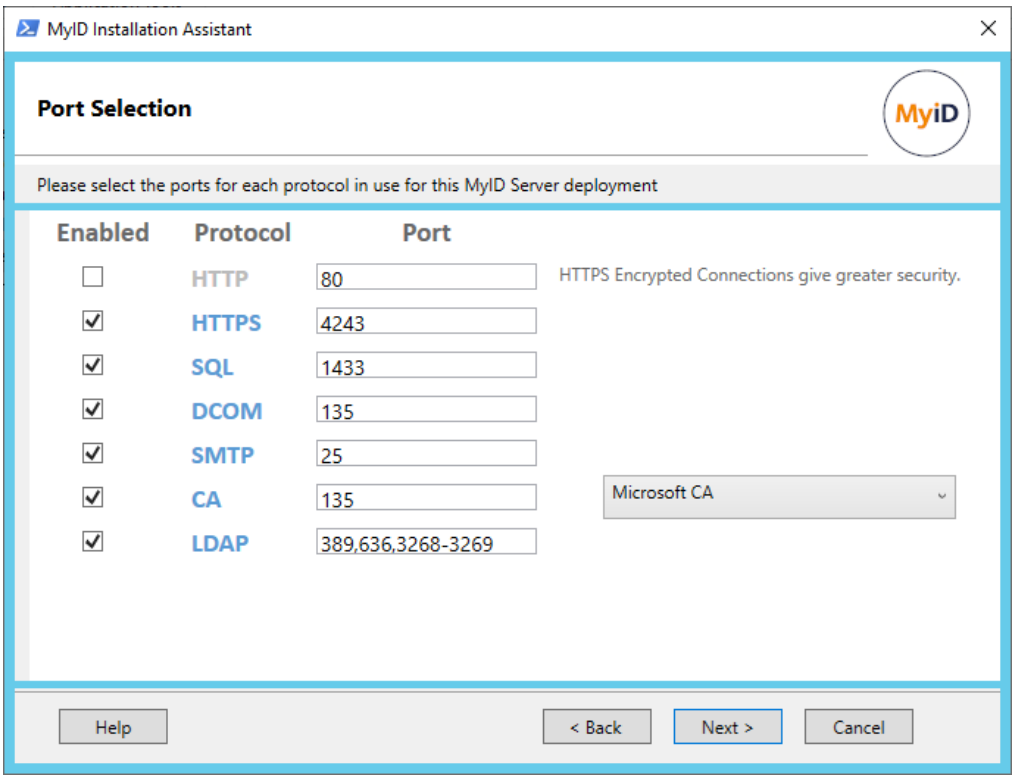
  where `<app>` is the name of your MyID application server. Run the .msi files directly.

  Note: You must add the application server to the list of Trusted Sites on the web server.

or:

- Copy the .msi files to the MyID web server and run the installers from there.

2.11 Selecting the network ports



The Port Selection screen allows you to configure which ports to test.

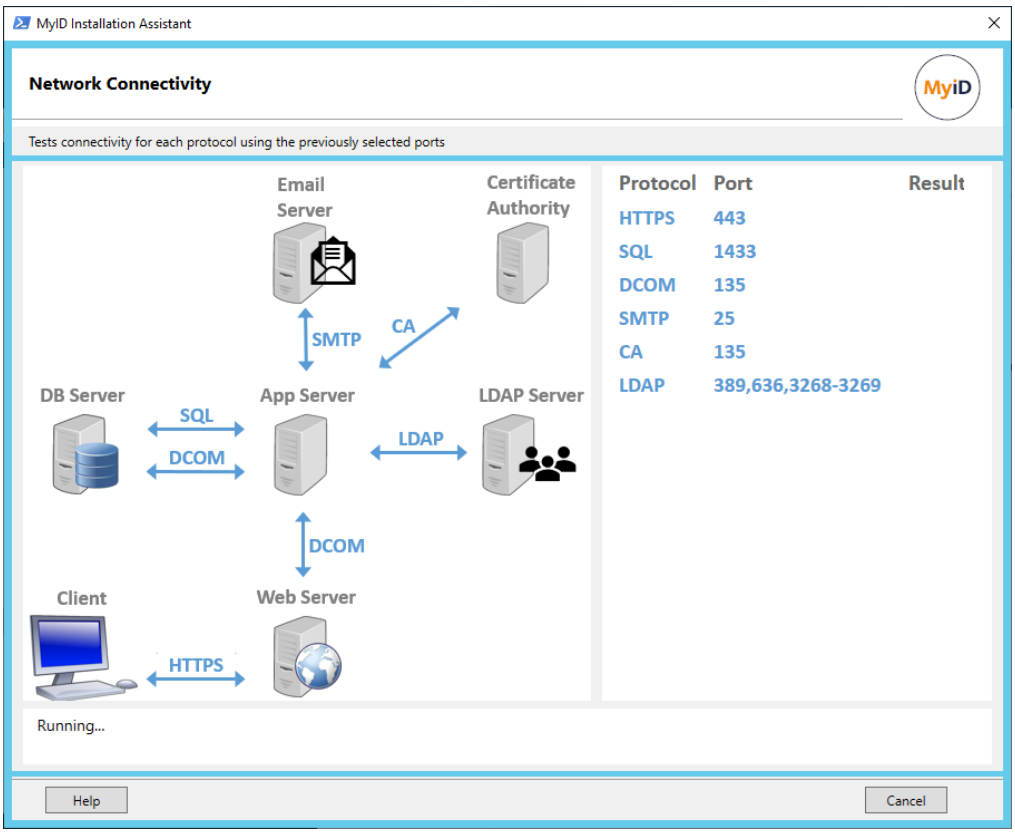
By default, the HTTP port is deselected; you are recommended to test communications with the web server using HTTPS instead. The HTTPS port is set by default to the port used for the binding you selected on the HTTPS Selection screen; see section *2.9*, *Configuring https*.

If you specified servers for the **Email Server**, **CA Server**, and **LDAP Server** options on the Server Selection screen (see section *2.8*, *Selecting the servers*) the MyID Installation Assistant can check those connections, too.

Select the CA you are using from the drop-down list, and the MyID Installation Assistant populates the CA **Port** field with the default ports used for that CA.

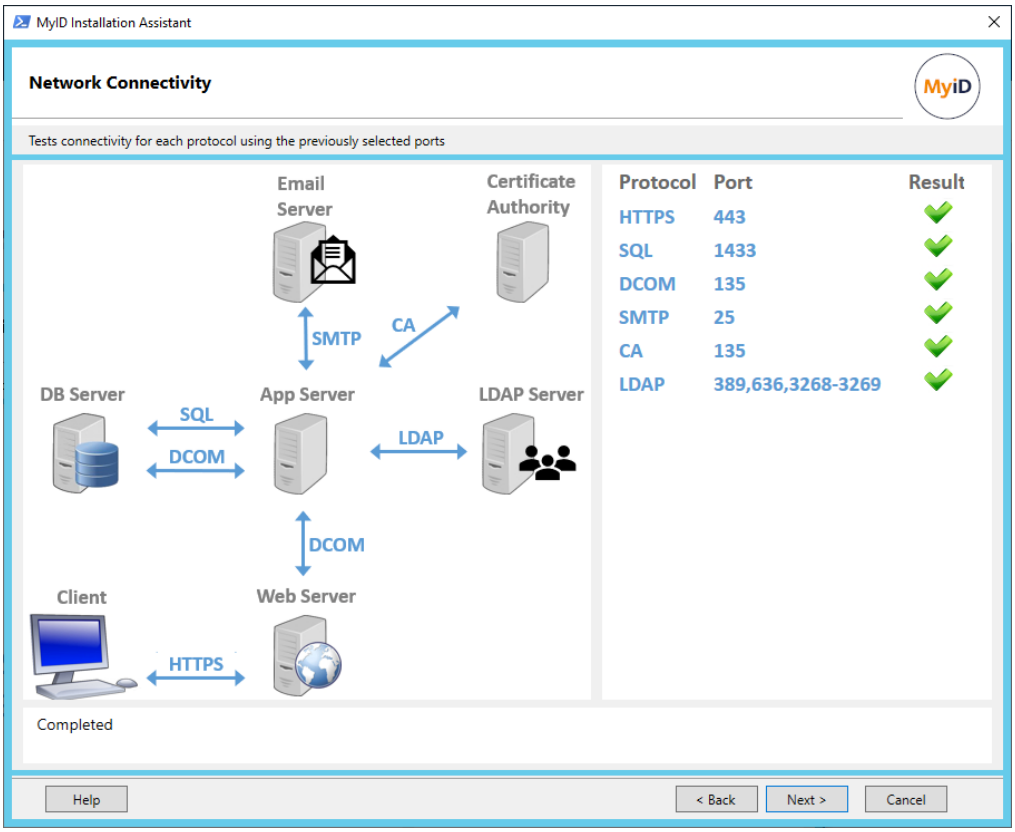
Select the connections you want to check, provide any custom values for the ports used for those connections on your system, then click **Next** to proceed to the next stage.

2.12 Checking network connectivity

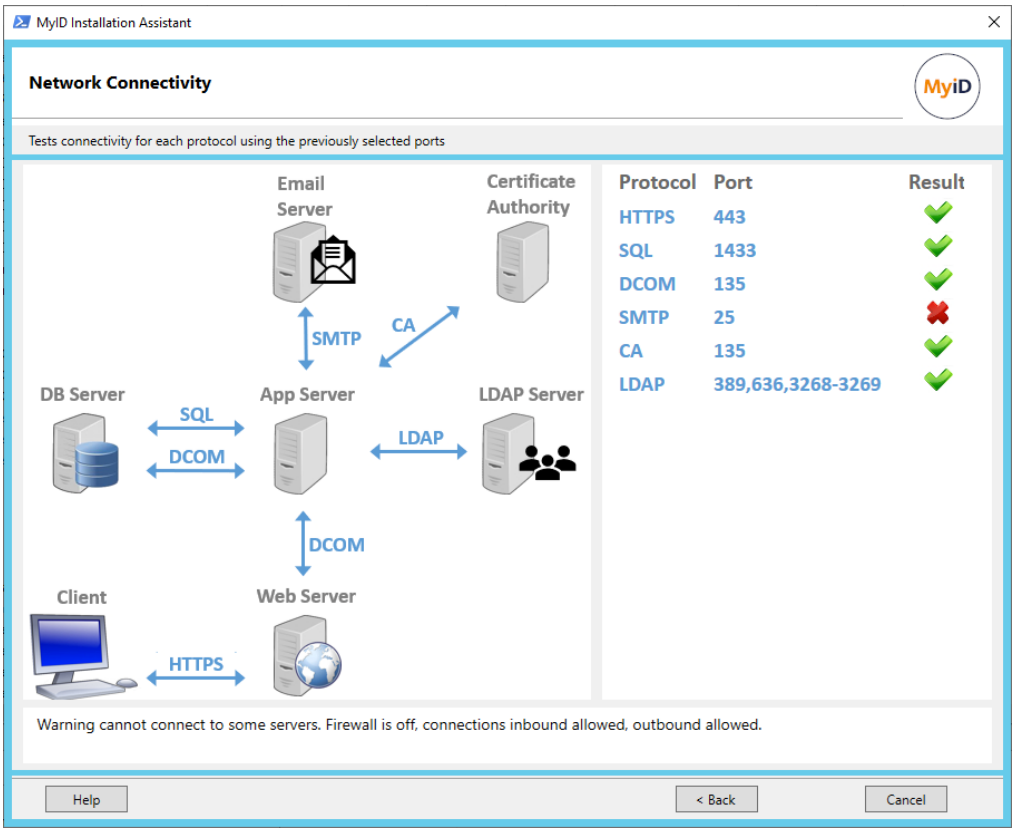


The Network Connectivity screen runs through a series of tests based on the servers and ports you selected on the Port Selection screen; see section *2.11*, *Selecting the network ports* for details.

If all the connections are successful, the screen displays all green ticks, and you can click **Next** to proceed to the next stage.



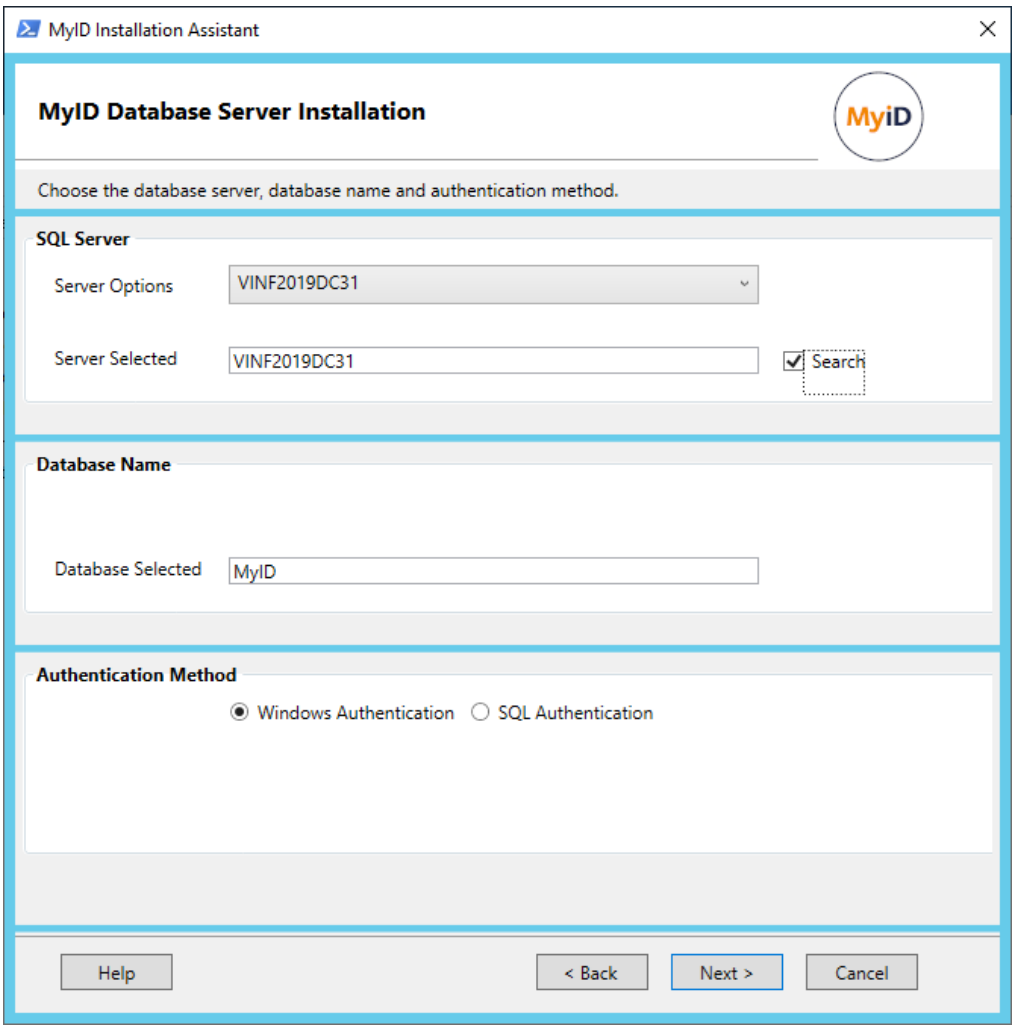
If there are any failures, these are displayed with red crosses:



As much information as possible about the failure is displayed on screen; for example, the status of the firewall, and whether inbound and outbound connections are allowed. If the connection is blocked due a firewall rule that is configured by a Group Policy, the MyID Installation Assistant displays a link to a Resultant Set of Policy report that you can use to justify a request to your network administrator to allow access.

You cannot proceed to the next stage until you have resolved these issues. If necessary, to continue with your system setup, you can click **Back** and deselect the tests that are failing; however, MyID will not work correctly until you have resolved the issues.

2.13 Configuring the databases



You must provide details for the following databases:

- The main MyID database.
- The MyID Authentication database.

  The authentication database contains information on audited authentication attempts. You can use this database for reporting; see the *Reporting on the authentication database* section in the ***MyID Authentication Guide*** for details.

  Note: You must provide the location of the MyID Authentication database on a web-only server if you are installing the MyID Verification Service.
- Optionally, the MyID Archive database.

  The archive database can contain an archive of some parts of the main MyID database. Creating the database does not set up the archiving procedures; the *Database configuration* section in the ***Advanced Configuration Guide*** for details.

To provide the details for a database:

1. Select the database server from the drop-down list.

   This list provides the results of a search for data sources.

Alternatively, you can deselect the **Search** option and type the server's name manually; in this case, the field defaults to the server name you provided on the Server Selection screen (see section *2.8*, *Selecting the servers*).

If your database server uses a named instance, type the name as *server\instance* – for example:

`MYSERVER\myinstance`.

If your database server uses a port other than the default TCP 1433, this is obtained from the details you provided on the Port Selection screen (see section *2.11*, *Selecting the network ports*) – you do not need to provide it here.

2. Type the name of the database.

   The MyID Installation Assistant provides a default name for each type of database:

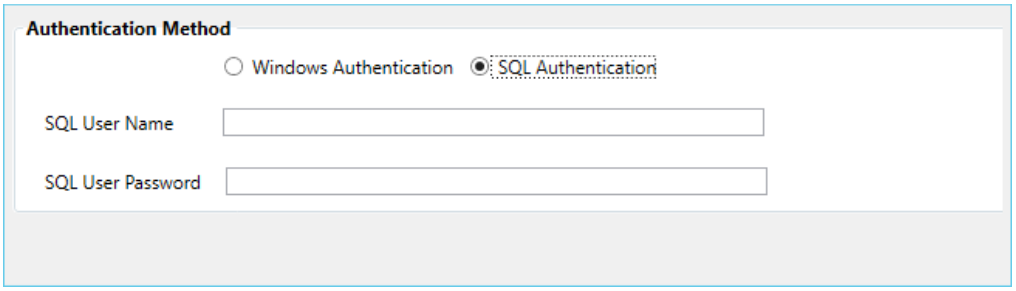
   - `MyID` – the main MyID database.
   - `MyIDAuth` – the MyID authentication database.

     Note: For the MyID authentication database, you can use the same database as the main MyID database; however, you are strongly recommended to use a separate database for your production system. If you are using the web.oauth2.ext standalone authentication web service, security is enhanced by giving the authentication user under which the service runs read-write access to the authentication database, and read-only access to the main MyID database.
   - `MyID_Archive` – the MyID Archive database.

   You can change the database name if necessary. You can type a new name for a database, or the name of an existing database.

3. Select the authentication type:

   - **Windows Authentication** – the user account being used to run the installation program is used to access the SQL Server database.
   - **SQL Authentication** – you must specify the **SQL User Name** and **SQL User Password** for the user you want to use to authenticate to the SQL Server database.

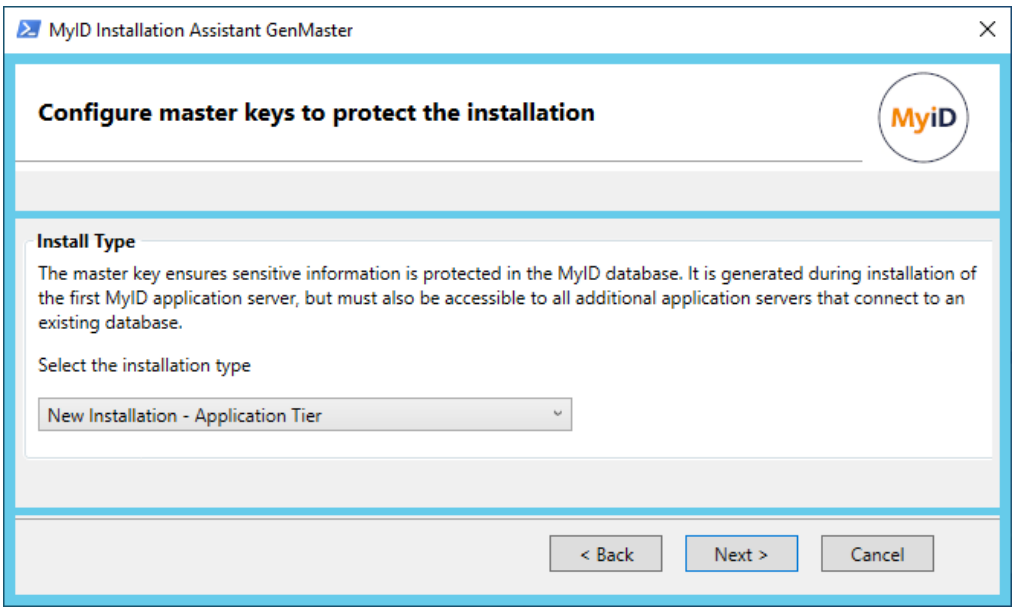
     

     Note: You must create your databases and logins before running the installation program. See section *4.6.6*, *Configuring SQL Server for SQL Authentication* for details.

4. Click **Next** to proceed to the next stage.

   You must repeat the process for each database in your system.

2.14 Configuring the master keys



You must provide the information required for the MyID Installation Assistant to run the GenMaster utility to set up your master keys.

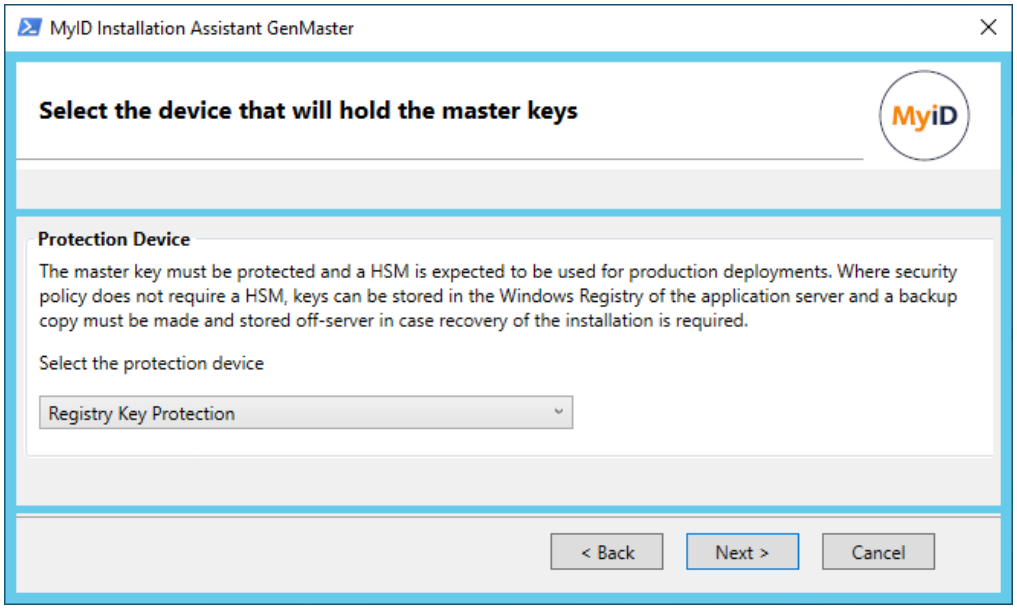
Note: If the generation of master keys fails during the installation, you can run the utility as a standalone program to set your master keys; see section *8.5*, *Using GenMaster*.

To provide details for the master keys:

1. Select one of the following options:
   - **New Installation – Application Tier** – select this option if you are installing the primary (or only) application server.
   - **Existing Installation – Additional Application Tier** – select this option if you have already installed MyID on your primary application server, and are now installing MyID on an additional application server.

     See section *2.14.1*, *Configuring the master keys for an additional application server*.
   - **Existing Installation – Upgrade Application Tier** – select this option if you have already installed MyID and are upgrading your system.

     Because your server is already configured, you do not need to set up your master keys, and can proceed to the next stage.
2. Click **Next**.



3. Select the protection device from the drop-down list.

   You can choose from the following:

   - **Registry Key Protection** – the key is stored in the registry of the MyID application server.
   - **Thales LUNA HSM** – the key is generated and stored in the Thales Luna HSM.
   - **Entrust nShield HSM** – the key is generated and stored in the Entrust nShield HSM.

   To use the **Registry Key Protection** option:

   a. Select **Registry Key Protection** from the drop-down list.

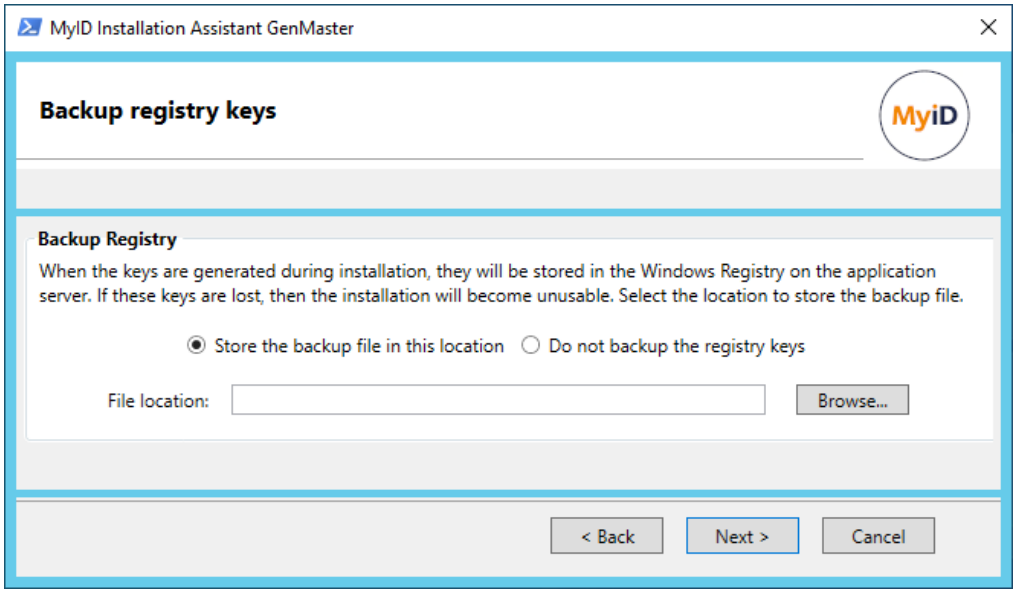
   b. Click **Next**.

   c. Select one of the following options:

      - **Store the backup file in this location** – click **Browse** and provide a location and filename for the backup registry file.

        You are recommended to save this backup file to a secure location.

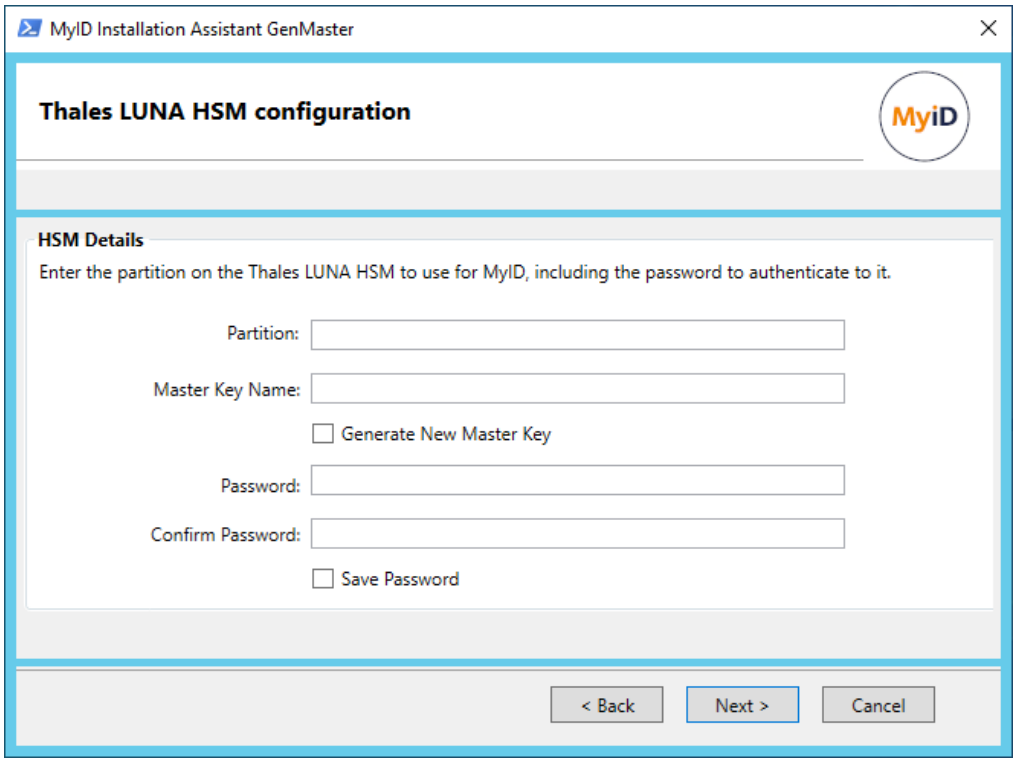
      - **Do not backup the registry keys** – skip the backup step.



To use the **Thales LUNA HSM** option:

a. Select **Thales LUNA HSM** from the drop-down list.

b. Click **Next**.



c. Provide the following information:

- **Partition** – type the name of the partition that you want to use.
- **Master Key Name** – type the name of the key you want to use.

If you have previously generated a master key in Keysafe (for instance if you are operating in FIPS140-1 level 3 mode), type the name of the existing key.

If you have not previously generated a master key in Keysafe, type the new name for the key you want to generate.

- **Generate New Master Key** – select this option if you have not previously generated a master key.

  Note: There must not already be a key of this name installed on the HSM.

- **Password** – type the password for the partition; this is the HSM Partition Administrator password, not the crypto user.
- **Confirm Password** – confirm the password for the partition.
- **Save Password** – select this option to save the password.

  If you do not select the **Save Password** checkbox, you must enter the password in the **Card Manager Startup** dialog box after any machine reboot before the MyID keyserver can start.

  If you choose to save the password, the MyID keyserver starts automatically.

  Note: This password protection is in addition to the HSM client certificate access control, so even if a user obtains the password they cannot use the HSM remotely unless their client has a certificate and has been authorized.

  Important: If you choose to save the password, the password is saved in the registry on the MyID application server for the MyID COM+ user:

  `HKEY_CURRENT_USER\Software\Intercede\Edefice\MasterCard`

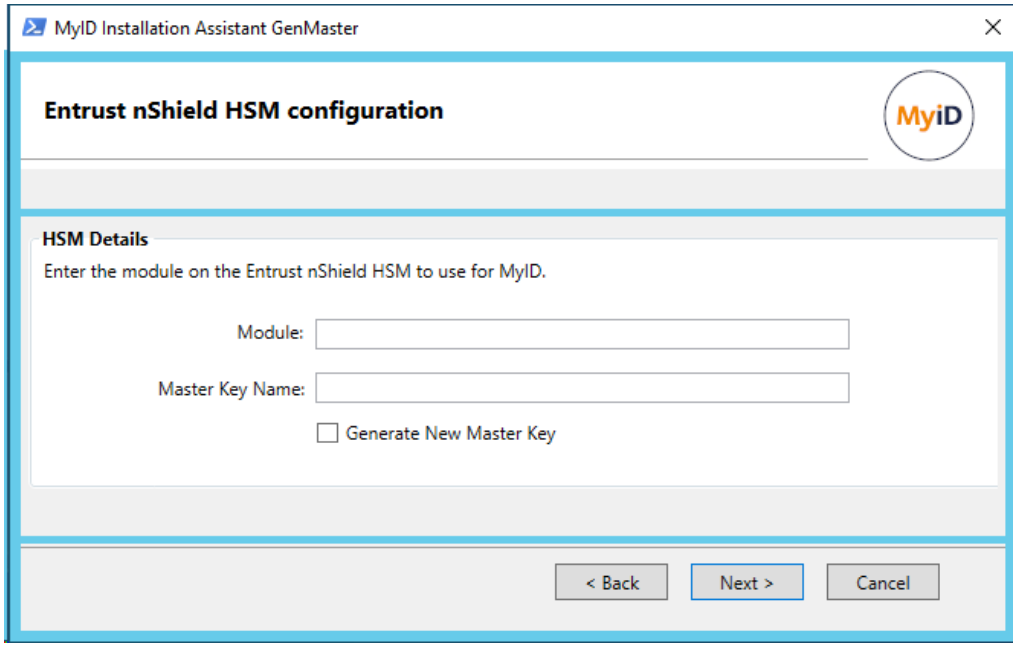
  The password is saved encrypted to the registry; see section *8.6, Setting the HSM PIN*.

For more information, see the ***Thales Luna HSM Integration Guide***.

To use the **Entrust nShield HSM** option:

a. Select **Entrust nShield HSM** from the drop-down list.

b. Click **Next**.



c. Provide the following information:

- **Module** – type the name of the module you want to use.
- **Master Key Name** – type the name of the key you want to use.

  If you have previously generated a master key in Keysafe (for instance if you are operating in FIPS140-1 level 3 mode), type the name of the existing key.

  If you have not previously generated a master key in Keysafe, type the new name for the key you want to generate.

  Generate New Master Key – select this option if you have not previously generated a master key.

  Note: There must not already be a key of this name installed on the HSM.

For more information, see the ***Entrust nShield HSM Integration Guide***.

4. Click **Next** to move to the next stage.

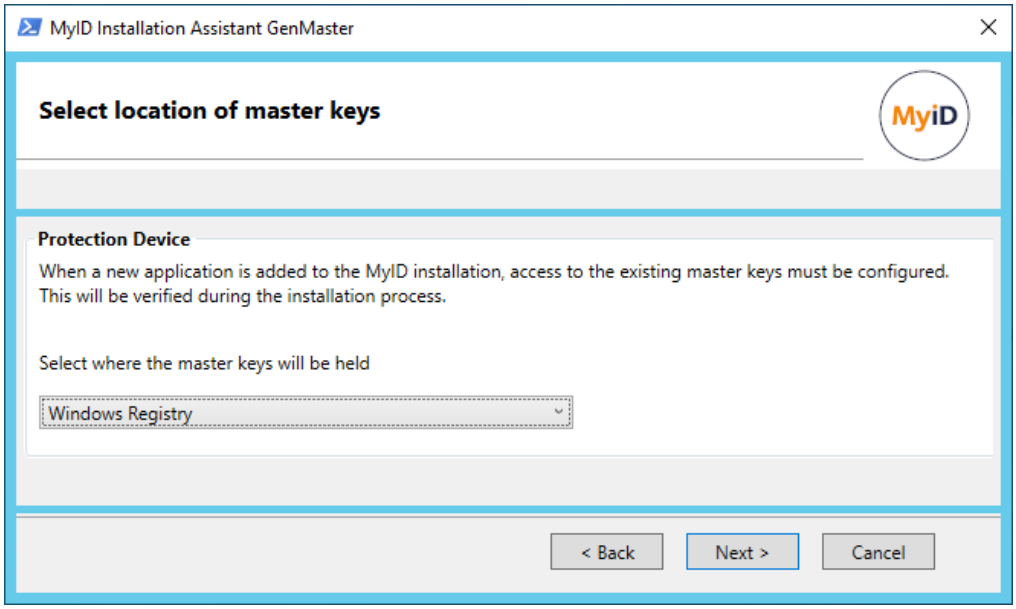
2.14.1 Configuring the master keys for an additional application server

If you have already installed MyID on your primary application server, and are now installing MyID on an additional application server, you do not need to create new keys; you can import the keys from your primary application server, then inform the MyID Installation Assistant, which then checks that the keys are in the correct place.

For detailed information about installing additional application servers, including importing the keys from one server to another, see the *Multiple application servers* section in the ***Advanced Configuration Guide***.

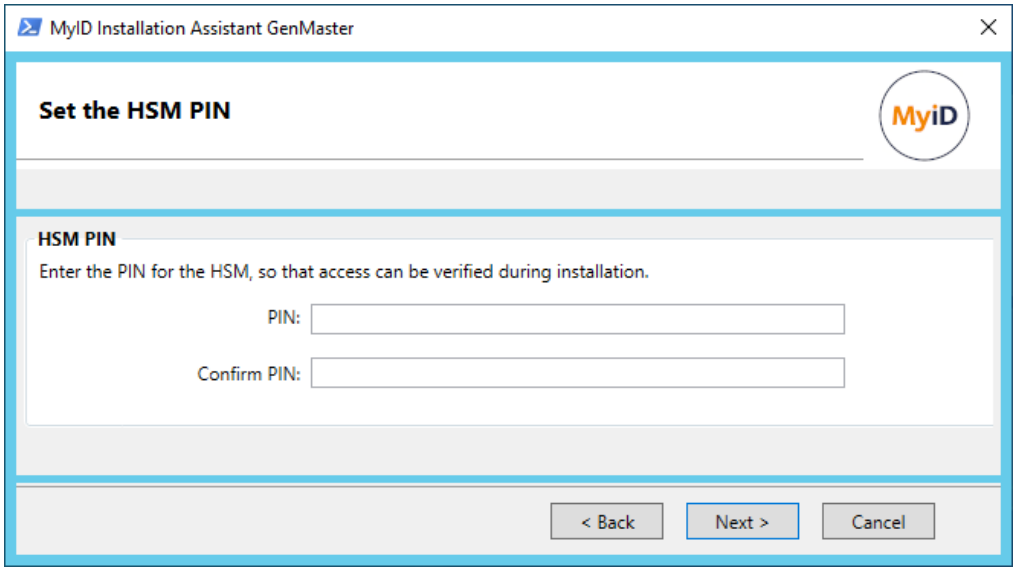
To configure the master keys for an additional application server:

1. From the **Select the installation type** drop-down list, select **Existing Installation - Additional Application Tier** and click **Next**.



2. From the drop-down list, select one of the following options:
   - **Windows Registry** – select this option if you created the master keys in the registry on the primary application server.
   - **Hardware Security Module – Set HSM PIN** – select this option if you created the master keys on an HSM when you installed the primary application server.
3. Click **Next**.

   If you are using an HSM, the PIN screen appears:

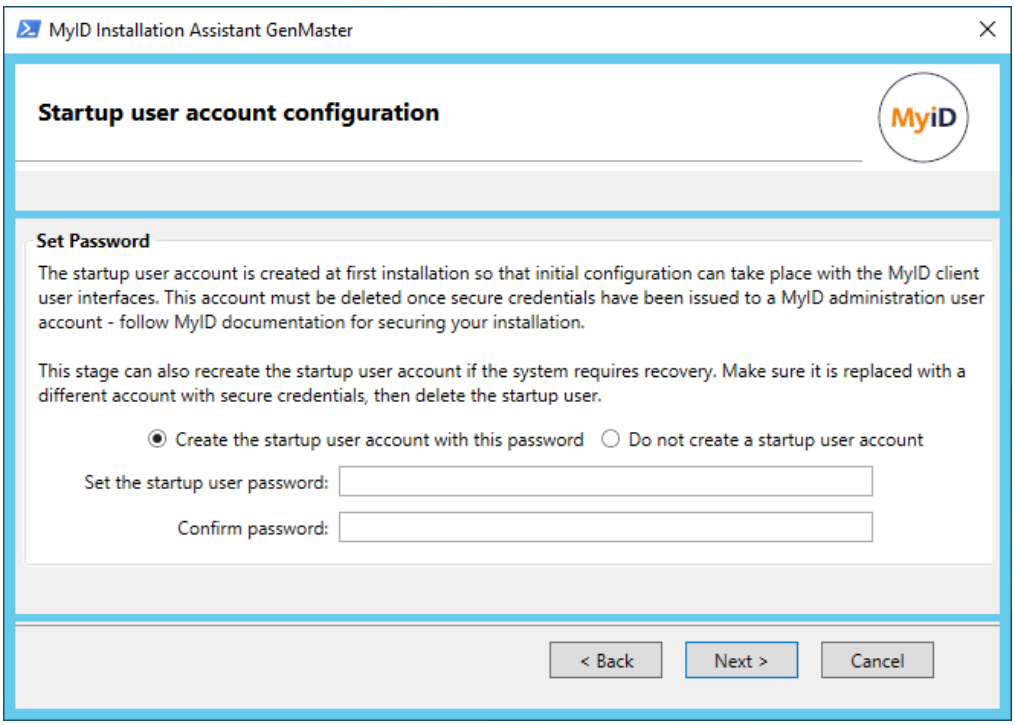


Type and confirm the PIN, then click **Next**.

2.15 Configuring the startup user account

The startup user allows you to access MyID for the first time and complete the setup of your system.

Note: You *must* set up a password for this account when you first install MyID or you will be unable to access the system. If you are upgrading an existing MyID system and already have a smart card or password user that you can use to access the system, you do not have to configure a startup password. If you do not set a password for the startup user when you install MyID, you can run the utility as a standalone program to configure the startup user account if necessary; see section *8.5*, *Using GenMaster*.

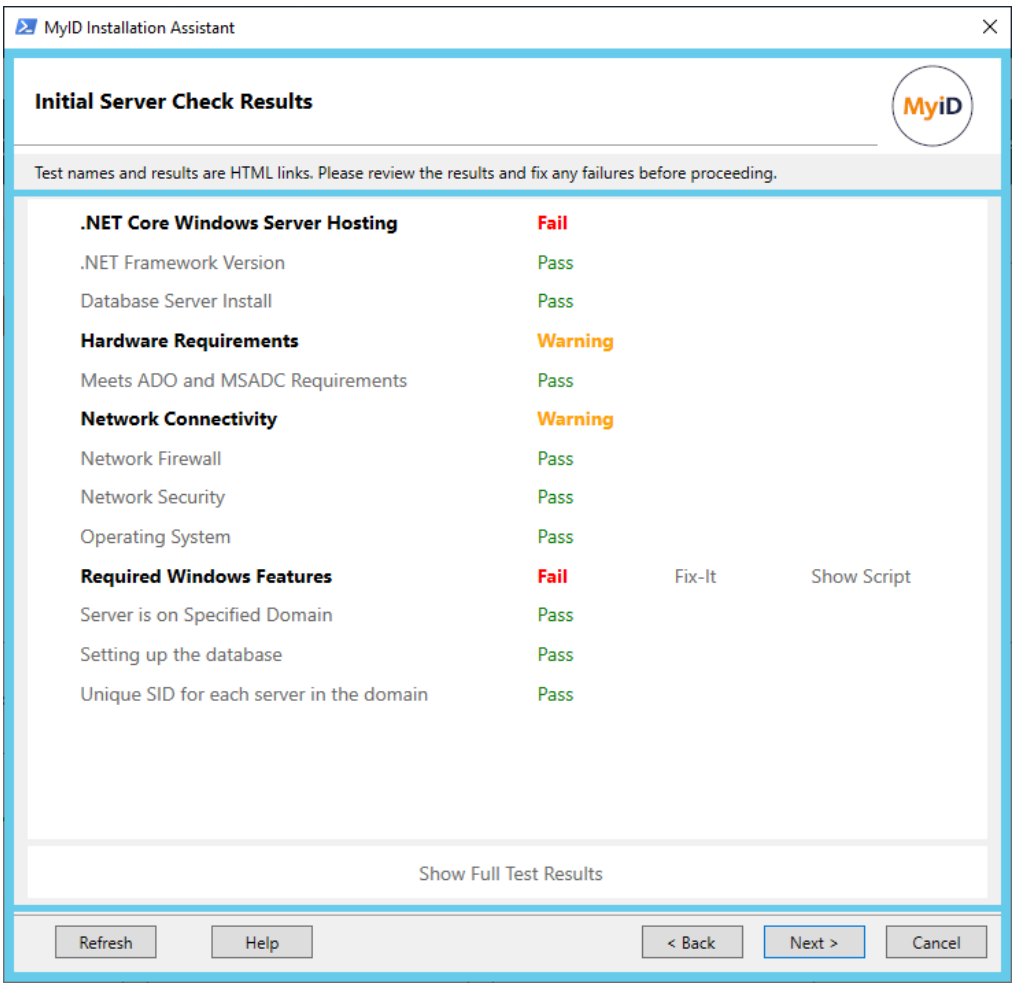


1. Select one of the following options:
   - **Create the startup user account with this password** – type the new password and confirm it.
   - **Do not create a startup user account** – do not create a startup user account.

     Important: If you do not create a startup user account on a new system, you cannot access MyID.

   Note: Startup users are intended only for bootstrapping your system, and are not intended for long-term use. See the *Passwords for startup users* section in the ***System Security Checklist*** guide for details.
2. Click **Next**.

2.16 Initial server check results



The Initial Server Check Results screen runs a series of System Interrogation Utility tests against your system to ensure that your server meets the requirements to install MyID.

The tests are broken down into categories. Click the name of a category to open the relevant section of the MyID documentation.

The results of each category are displayed:

- **Pass** – the system has passed all tests in the category.
- **Warning** – the system did not pass all tests, but the failures relate to issues that may impact performance rather than functionality.
- **Fail** – the system did not pass all tests, and the failures will prevent MyID from operating correctly. You must correct these failures before proceeding.
- **Fatal** – the system did not pass all tests, and the failures will prevent MyID from operating. You cannot click **Next** until you have resolved these failures.

Click the result label to see the test results for that category.

The MyID Installation Assistant cannot fix most of the issues that may be found by these tests (for example, the order in which .NET Core and IIS were installed, or the amount of disk space available) but where it *is* possible, it provides a signed PowerShell script to address the issue; click **Show Script** to display the script in a Notepad window, which you can then review. Once you are happy with the effect of the script on your system, click **Fix-It** to run the script.

Note: If you run the fix-it script to address any failures with the Windows Features category, this may cause a failure in the .NET Core Windows Server Hosting category; this is because .NET Core must be installed after IIS, and the fix-it script may install IIS components. In this case uninstall and reinstall .NET Core after running the fix-it script; see section *5*, *Additional hardware and software requirements* for details of the .NET Core requirements.

If you make a change to your system, click **Refresh** to run the tests again. You can also click **Cancel** to close the MyID Installation Assistant and make changes to your system; then, when you open the MyID Installation Assistant again, it automatically re-runs the tests.

Click **Show Full Test Results** to open the System Interrogation Utility test results page for all of the tests that have been run.

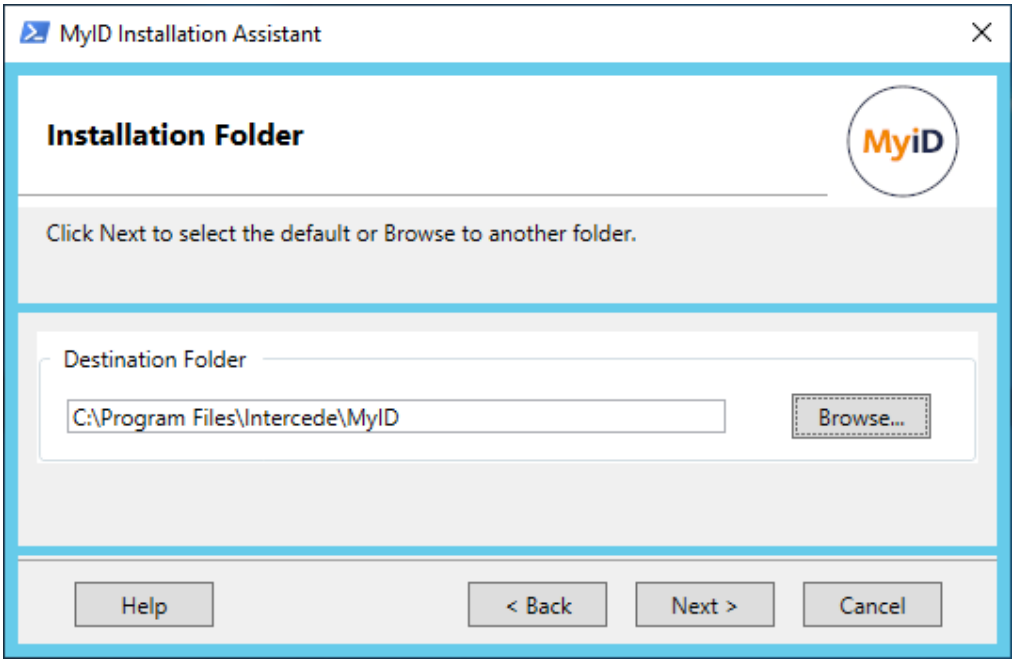
For more information about the tests that are run, see the *Description of derived tests* section in the ***System Interrogation Utility*** guide. Each test has a link to the section in the MyID documentation that describes the requirement being tested. See also section *4*, *Initial server configuration*, which includes the majority of the setup you must carry out before you can start to install MyID.

Once your system passes all the tests, or you are happy to proceed with any warnings, click **Next** to proceed to the next stage.

2.17 Providing the installation details

The next screens allow you to provide the installation details for your system.

2.17.1 Providing the installation location

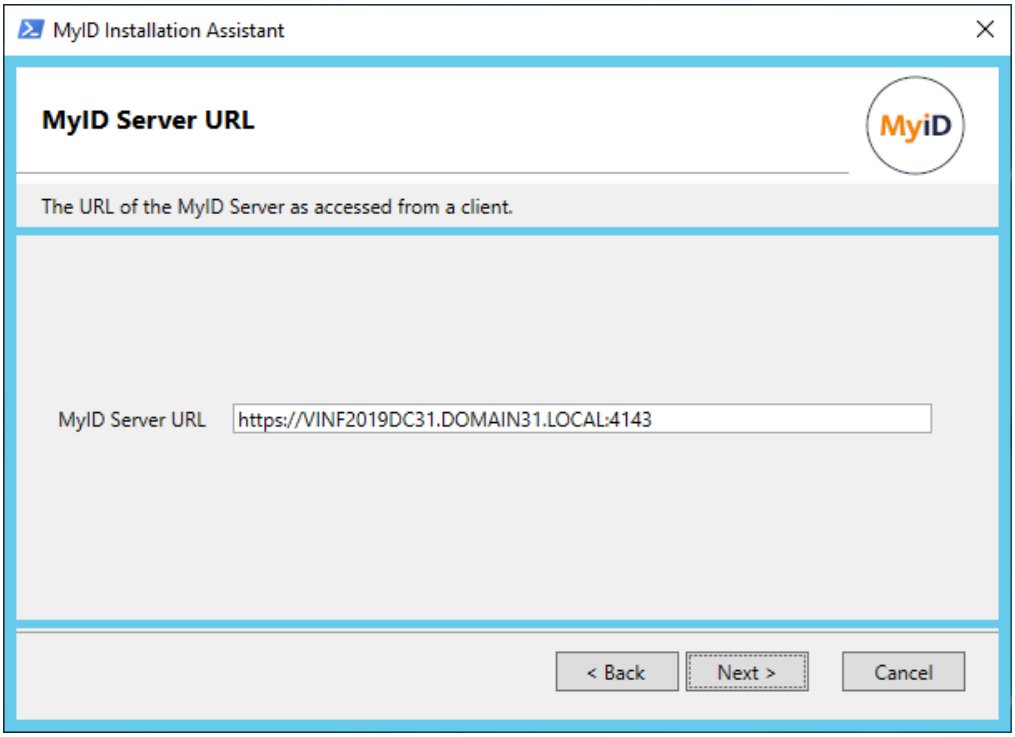


1. Provide the location of the folder into which you want to install MyID. The default is:

   `C:\Program Files\Intercede\MyID`

   Click **Browse** to select a different installation folder.
2. Click **Next** to move to the next stage.

2.17.2 Providing the MyID server URL



1. Provide the URL used to access the MyID web server.

   Important: Specify the URL of the server, but *not* the full MyID Operator Client URL; that is, use an URL similar to:

   `https://myserver.example.com`

   and *not*:

   `https://myserver.example.com/MyID/OperatorClient/`

   This option is case sensitive, and must be consistent with the casing of the DNS Name in the web server's TLS certificate.

   If you are using a non-standard port, specify this; for example:

   `https://myserver.example.com:4143`

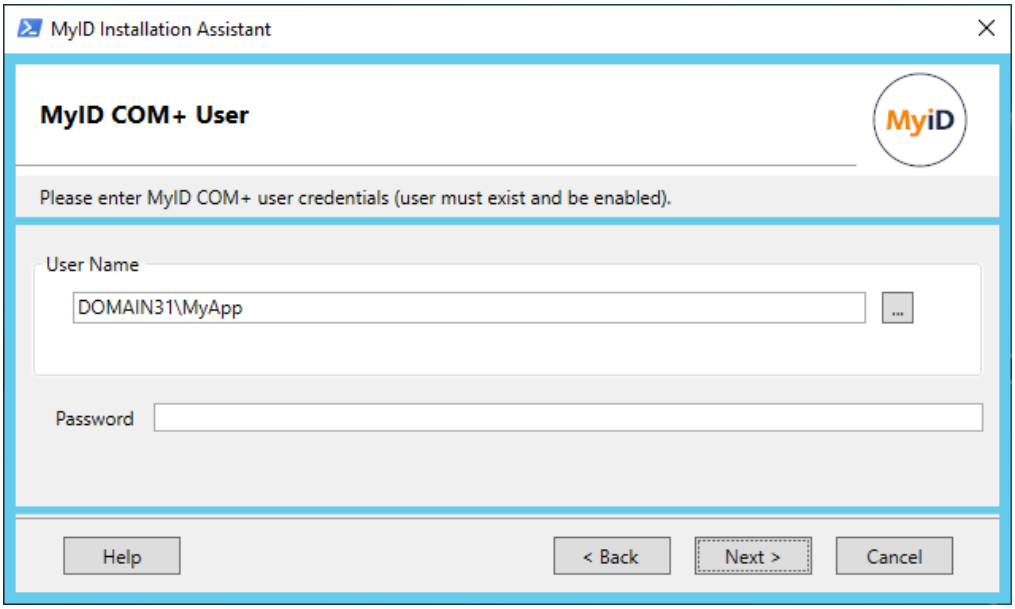
   The MyID Installation Assistant automatically adds a non-standard port if you specified it when setting up the https configuration.

   Note: The web services used by the MyID Operator Client (`rest.core` and `web.oauth2`) require SSL/TLS; if you do not connect through HTTPS, you cannot use the MyID Operator Client. See section *6.5*, *Setting up SSL/TLS* for details.

   If you experience any problems with this URL setting after installation, refer to the *MyID Operator Client advanced configuration* section in the ***MyID Operator Client*** guide for information on troubleshooting connection problems and manually configuring the URL.

2. Click **Next** to move to the next stage.

2.17.3 Providing details of the MyID COM+ user

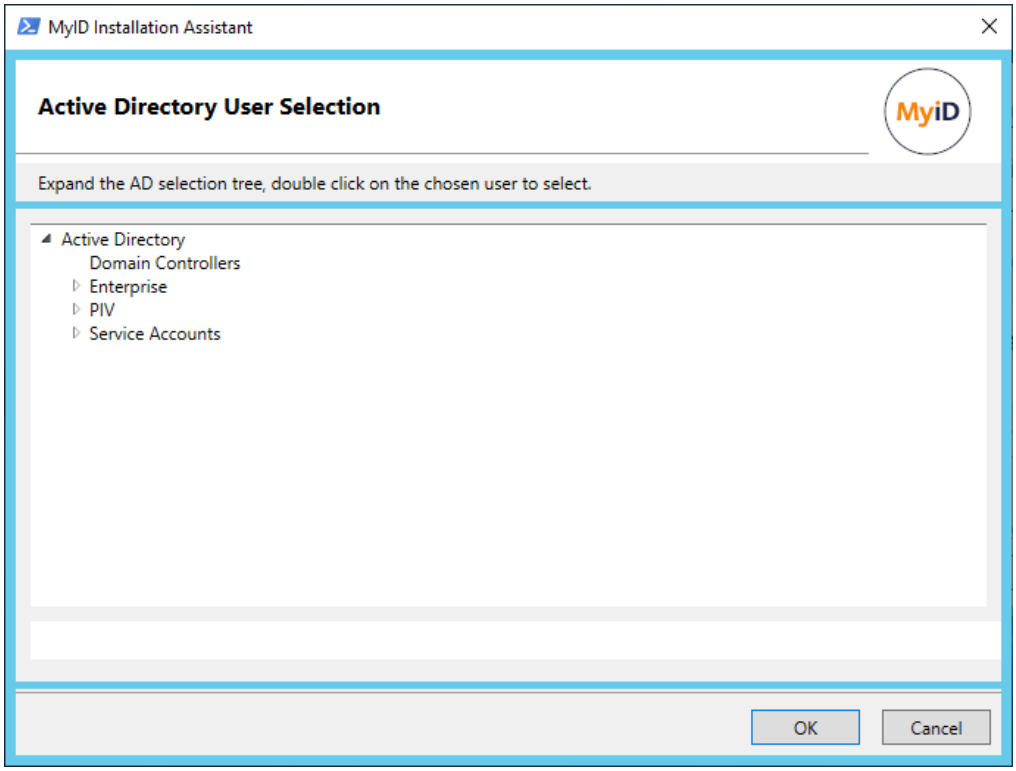


The MyID COM+ user is used to access the MyID COM+ components on the application server.

See section *6.1.2, MyID COM+ account* for details of the requirements for this account.

1. Provide the **User Name** for the MyID COM+ user account.

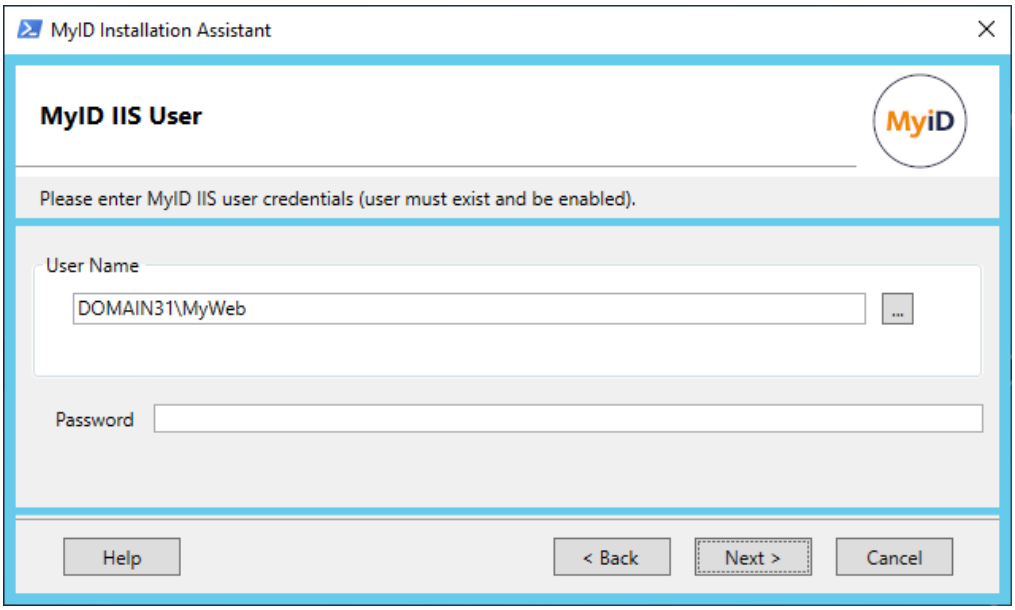
   You can click **...** to browse your Active Directory:



Select the user and click **OK**.

2. Type the **Password** for the user.
3. Click **Next** to proceed to the next stage.

2.17.4 Providing details of the IIS user



The IIS user is used to access the MyID website.

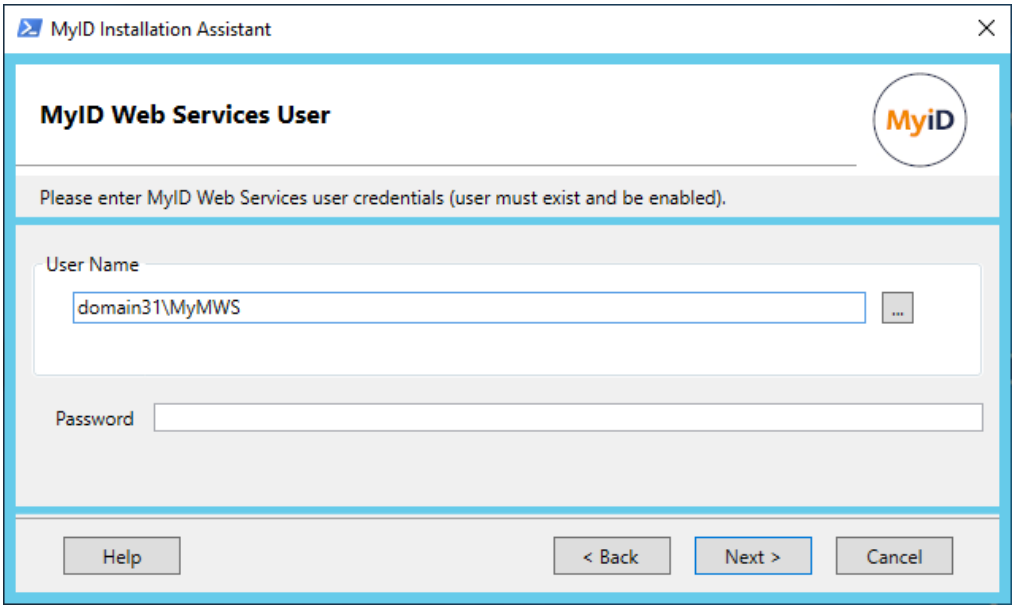
See section *6.1.3, IIS user account* for details of the requirements for this account.

1. Provide the **User Name** for the MyID IIS user account.

   You can click **...** to browse your Active Directory.

   Select the user and click **OK**.
2. Type the **Password** for the user.
3. Click **Next** to proceed to the next stage.

2.17.5 Providing details of the web services user



The web services user is used for the MyID web services.

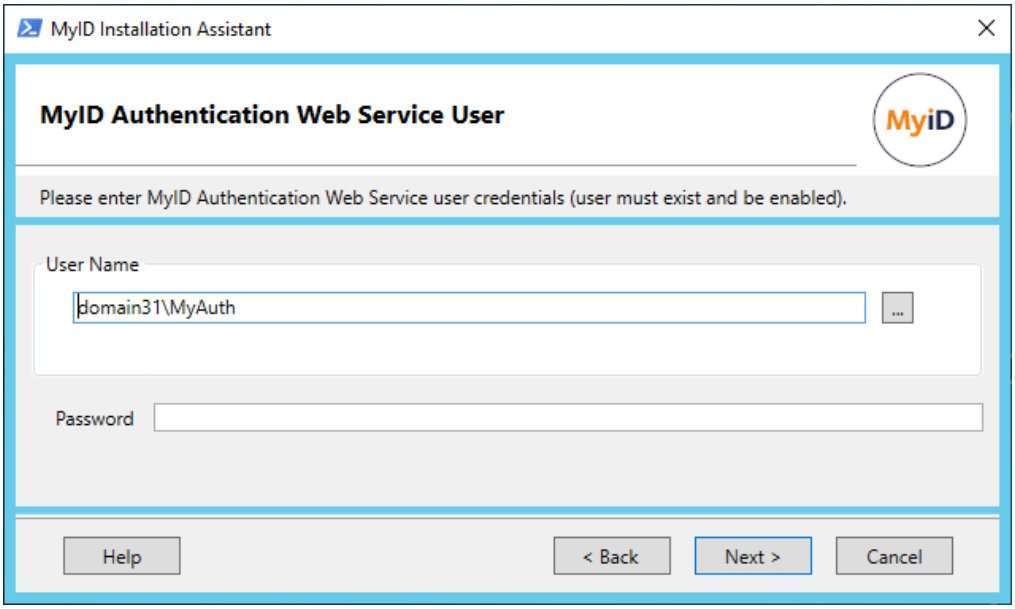
See section *6.1.4*, *Web service user account* for details of the requirements for this account.

1. Provide the **User Name** for the MyID web services user account.

   You can click **...** to browse your Active Directory.

   Select the user and click **OK**.
2. Type the **Password** for the user.
3. Click **Next** to proceed to the next stage.

2.17.6 Providing details of the authentication user



The authentication user is used to access the authentication database and access the authentication web service app pool.

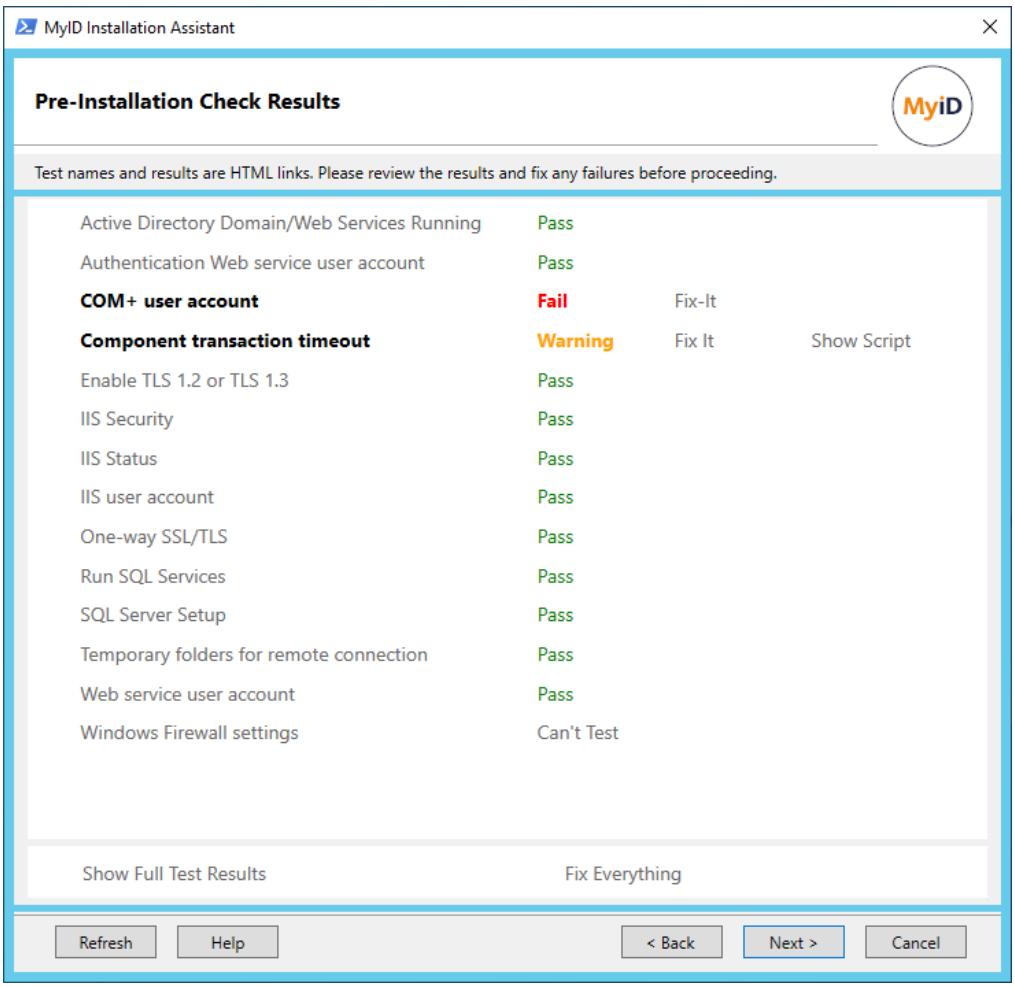
See section *6.1.5*, *MyID Authentication account* for details of the requirements for this account.

1. Provide the **User Name** for the MyID authentication user account.

   You can click **...** to browse your Active Directory.

   Select the user and click **OK**.
2. Type the **Password** for the user.
3. Click **Next** to proceed to the next stage.

2.18 Pre-installation check results



The Pre-Installation Check Results screen runs a series of System Interrogation Utility tests against your system to ensure that your server is ready to install MyID, including checking all the information you have provided (such as user accounts).

The tests are broken down into categories. Click the name of a category to open the relevant section of the MyID documentation.

The results of each category are displayed:

- **Pass** – the system has passed all tests in the category.
- **Warning** – the system did not pass all tests, but the failures relate to issues that may impact performance or security rather than functionality.
- **Fail** – the system did not pass all tests, and the failures will prevent MyID from operating correctly. You must correct these failures before proceeding.
- Can't Test – the test is not appropriate for your system configuration; for example, tests for split-tier systems are not appropriate for single-tier systems.

Click the result label to see the test results for that category.

Where possible, the MyID Installation Assistant provides a signed PowerShell script to address the issue; click **Show Script** to display the script in a Notepad window, which you can then review. Once you are happy with the effect of the script on your system, click **Fix-It** to run the script.

To run all the fix-it scripts, click **Fix Everything**.

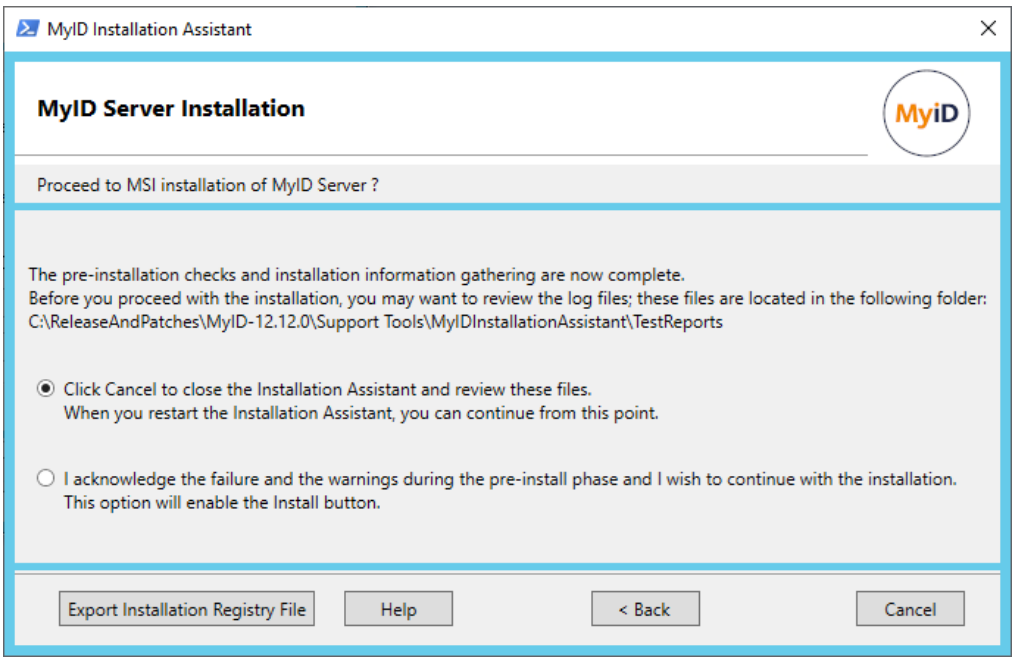
If you make a change to your system, click **Refresh** to run the tests again. You can also click **Cancel** to close the MyID Installation Assistant and make changes to your system; then, when you open the MyID Installation Assistant again, it automatically re-runs the tests.

Click **Show Full Test Results** to open the System Interrogation Utility test results page for all of the tests that have been run.

For more information about the tests that are run, see the *Description of derived tests* section in the ***System Interrogation Utility*** guide. Each test has a link to the section in the MyID documentation that describes the requirement being tested. See also section *6*, *Pre-installation configuration*, which includes the majority of the setup you must carry out before you can start to install MyID.

Once your system passes all the tests, or you are happy to proceed with any warnings, click **Next** to proceed to the next stage.

2.19 Starting the server installation



The MyID Server Installation screen provides you with a decision point. You have now provided all of the information needed to install the MyID server software, and have carried out all the initial server checks and pre-install checks.

If you want to save your configuration to automate running the MyID Installation Assistant, click **Export Installation Registry File**. See section *2.29*, *Automating an installation* for details.

If you want to review your status before proceeding, you can click **Cancel** to close the MyID Installation Assistant. When you restart the MyID Installation Assistant, it returns you to this stage so you can proceed.

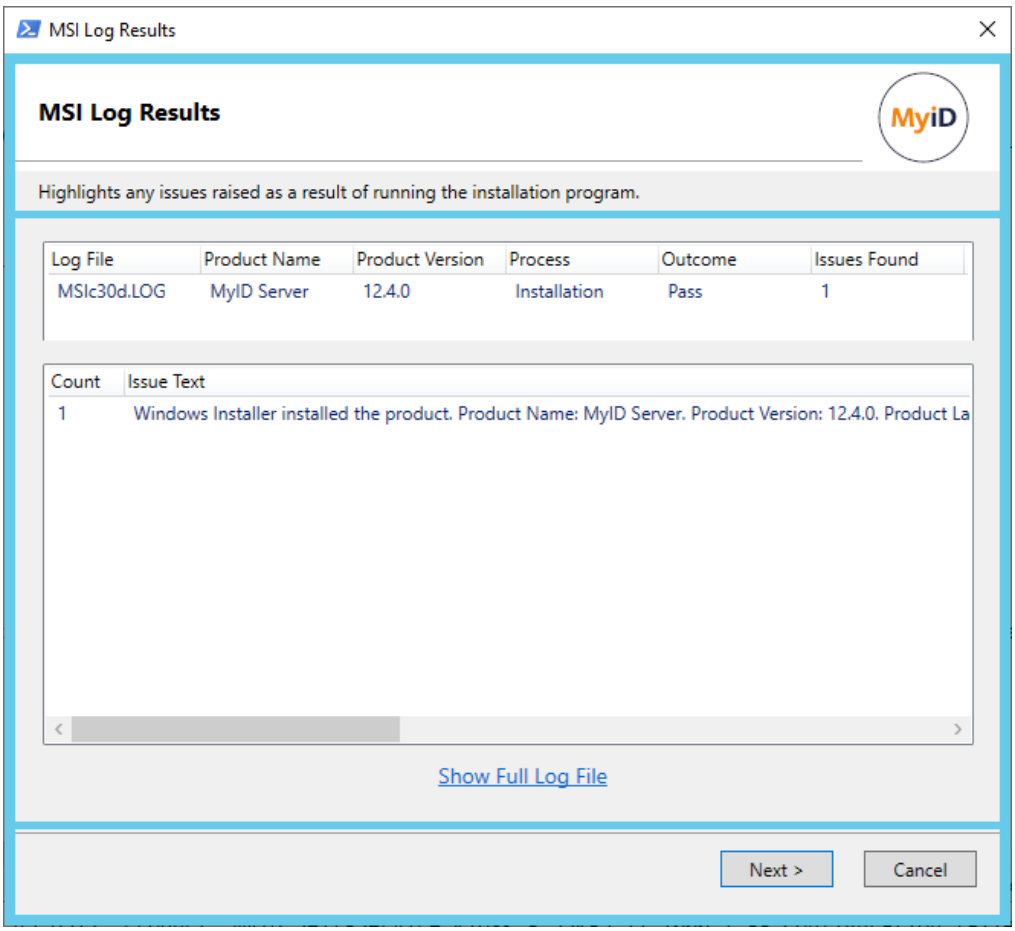
To assist you in making the decision whether to proceed with the installation, the MyID Installation Assistant creates a folder of logs and reports based on the checks it has carried out; see section *2.28*, *Checking the logs and reports* for details.

If you want to proceed with the installation, click the option to enable the **Install** button. If there were any failures or warnings that occurred during the initial server checks or the pre-installation checks, these are mentioned.

Click **Install** to start the MyID installation.

Note: There may be a significant pause between the installer window closing after completing the installation and the log results window appearing in the MyID Installation Assistant; this is expected.

2.20 Checking the installation log results



The MSI Log Results screen displays the result of the installation process, whether it succeeded (the **Outcome** is `Pass`) or failed (the **Outcome** is `Fail`). If there were any issues, the number of issues is displayed, and each one is listed.

Click **Show Full Log File** to open the log file.

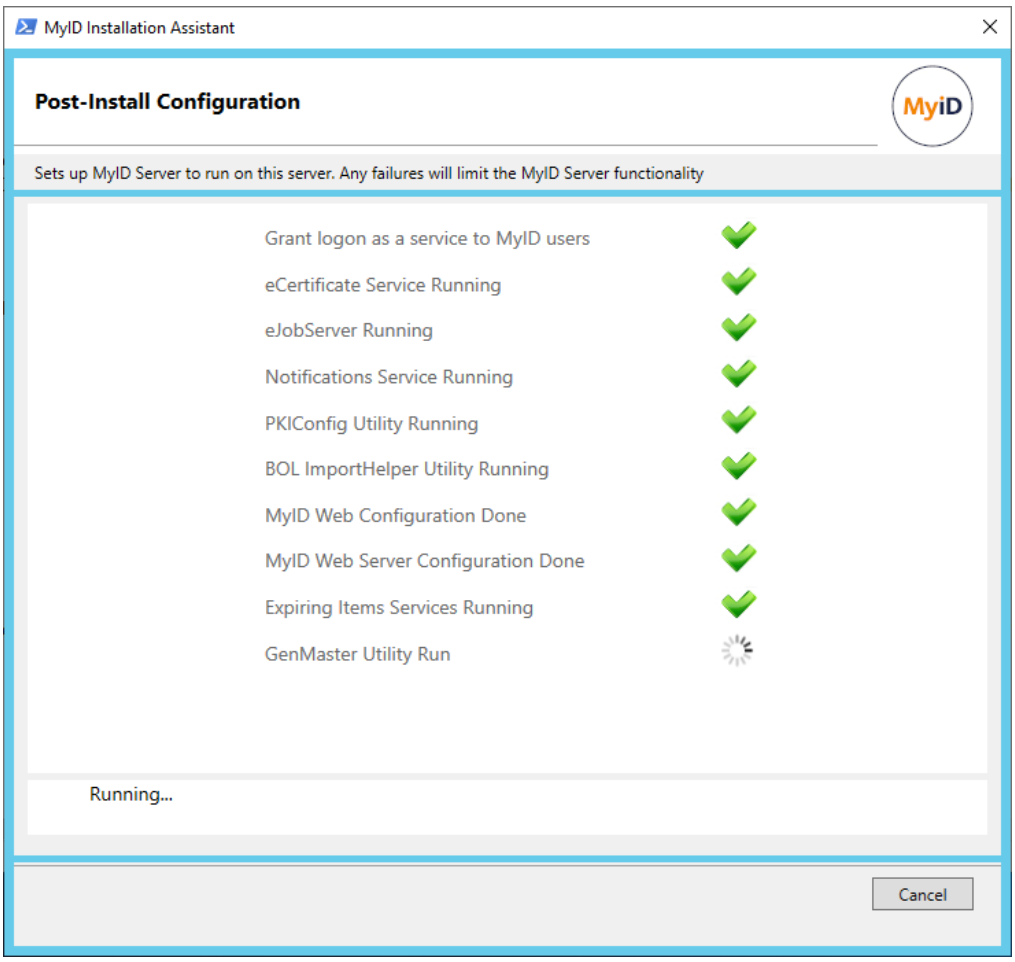
Important: The full log file indicates if a reboot is essential; however, you are strongly recommended to reboot your server at this point in the installation process. Click **Cancel**, reboot your server, then restart the MyID Installation Assistant.

- **IKB-362 – MSI log displays errors on successful install when using SQL Authentication**

  If you use SQL Authentication when installing the database, this may cause errors to be displayed in the MSI installation log.

  The installation has succeeded, but the errors are recorded due to an underlying issue within the database platform.

2.21 Post-install configuration



The Post-Install Configuration screen carries out a series of procedures to ensure that the MyID server is configured correctly, including running utilities and ensuring that required services are running. The procedures depend on the type of server you are installing; for example, a web server needs different procedures to an application server.

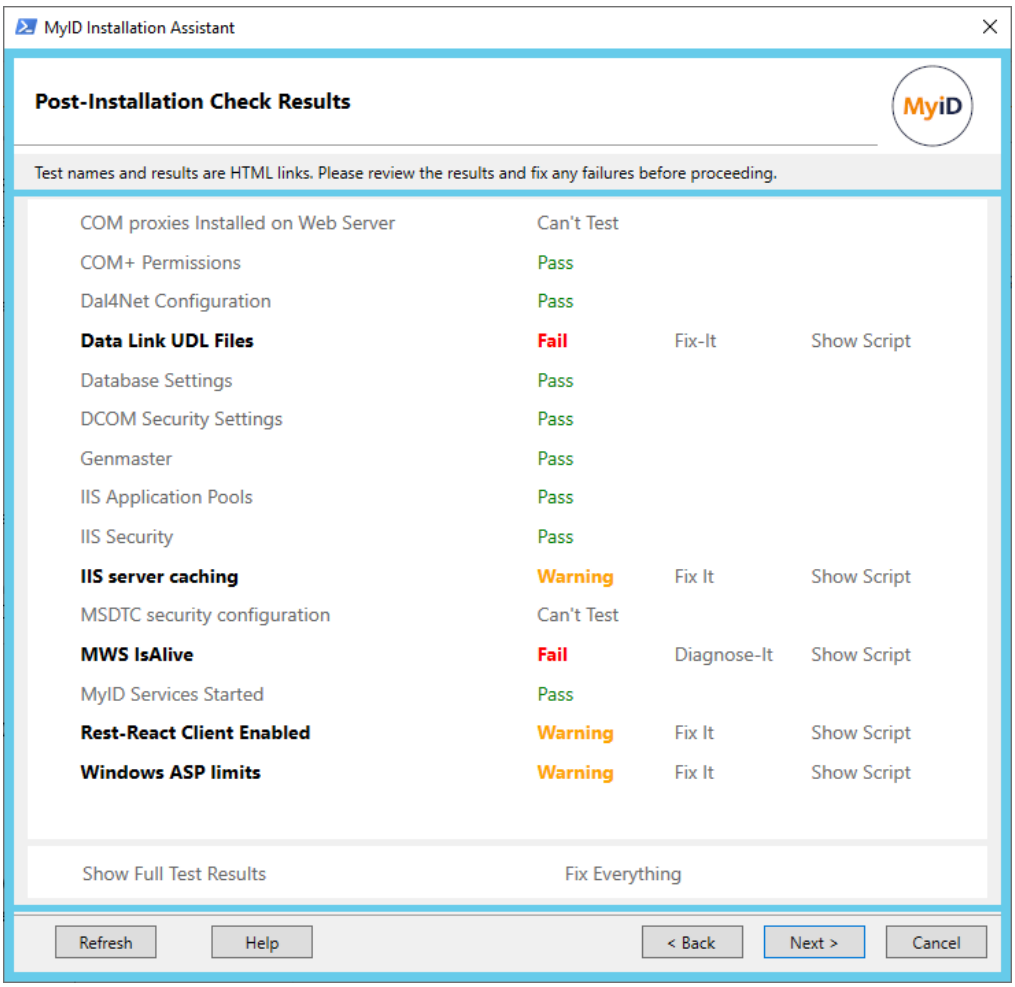
If necessary, for example on new installs on an application server, the MyID Installation Assistant run the GenMaster utility in the background, using the information you provided earlier; see section *2.14*, *Configuring the master keys* and section *2.15*, *Configuring the startup user account*.

GenMaster allows you to secure your MyID installation with a master key, and to set up a startup user that you can use to access the system for the first time.

You can also run the GenMaster utility as a standalone application; see section *8.5*, *Using GenMaster* for details; this allows you to set the master keys if the initial run resulted in a failure, or if you need to reset the startup user password.

Click **Next** to proceed to the next stage.

2.22 Post-installation check results



The Post-Installation Check Results screen runs a series of System Interrogation Utility tests against your system to ensure that your server is ready to run MyID, including carrying out any recommended configuration such as ASP limits.

The tests are broken down into categories. Click the name of a category to open the relevant section of the MyID documentation.

The results of each category are displayed:

- **Pass** – the system has passed all tests in the category.
- **Warning** – the system did not pass all tests, but the failures relate to issues that may impact performance or security rather than functionality.
- **Fail** – the system did not pass all tests, and the failures will prevent MyID from operating correctly. You must correct these failures before proceeding.
- Can't Test – the test is not appropriate for your system configuration; for example, tests for split-tier systems are not appropriate for single-tier systems.

Click the result label to see the test results for that category.

Where possible, the MyID Installation Assistant provides a signed PowerShell script to address the issue; click **Show Script** to display the script in a Notepad window, which you can then review. Once you are happy with the effect of the script on your system, click **Fix-It** to run the script.

To run all the fix-it scripts, click **Fix Everything**.

If the **MWS IsAlive** test fails, you can click **Diagnose-It** to run the system health check on the server; see the *System health check* section in the ***Advanced Configuration Guide*** for details of the information provided by this check.

If you make a change to your system, click **Refresh** to run the tests again. You can also click **Cancel** to close the MyID Installation Assistant and make changes to your system; then, when you open the MyID Installation Assistant again, it automatically re-runs the tests.

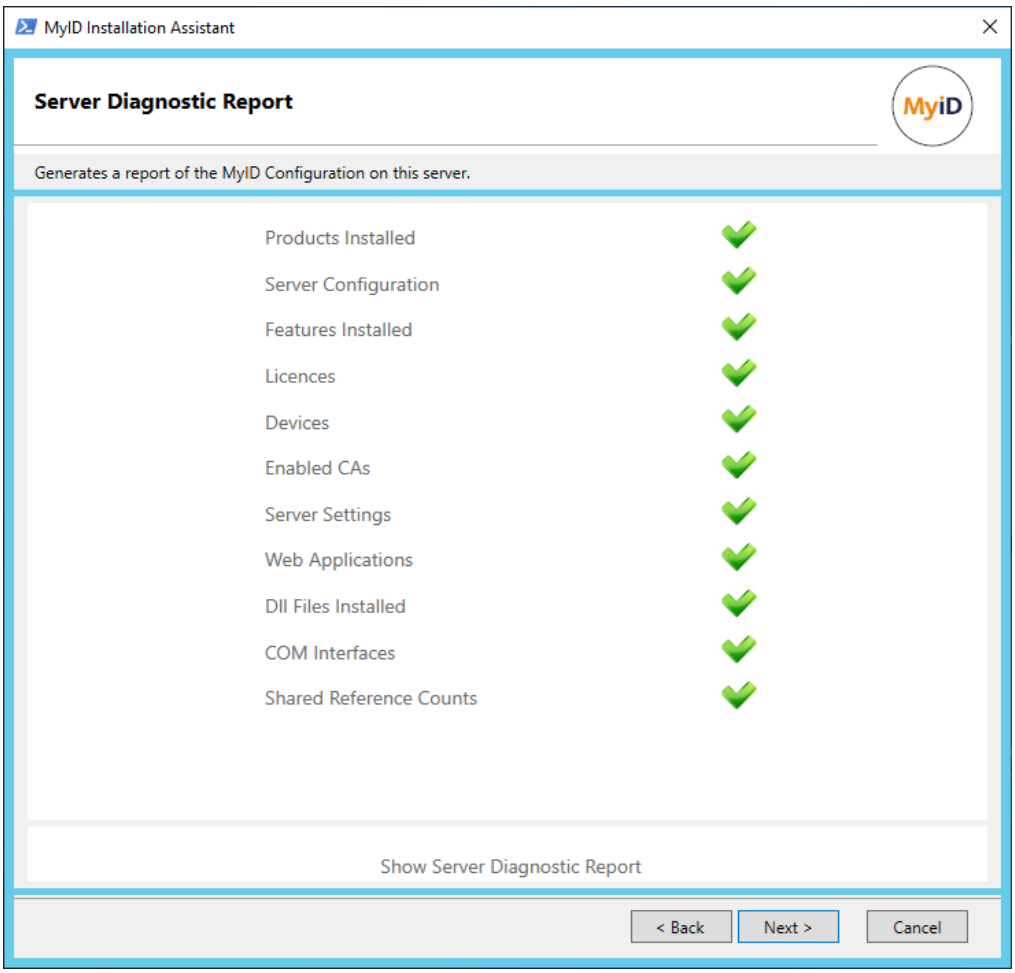
Click **Show Full Test Results** to open the System Interrogation Utility test results page for all of the tests that have been run.

For more information about the tests that are run, see the *Description of derived tests* section in the ***System Interrogation Utility*** guide. Each test has a link to the section in the MyID documentation that describes the requirement being tested.

For information about the web service tests, see section *12.4*, *Checking the web services*.

Once your system passes all the tests, or you are happy to proceed with any warnings, click **Next** to proceed to the next stage.

2.23 Server Diagnostic Report



The Server Diagnostic Report scans your MyID system and produces a report on the following information:

- Products installed.

  Lists the Intercede products installed, including the MyID server along with any installed add-ons, cumulative updates, and hotfixes.
- Server configuration.

  Provides a snapshot of the installation registry, the customization GUID, and non-sensitive data selected or input during installation.
- Features installed.

  Lists all MyID features, and marks each as "Local" (selected during installation) or "Absent" (not selected during installation).
- Licenses.
- Devices.

  Lists all devices supported in this version of MyID.
- Enabled CAs.

  Lists the CAs enabled in your system.

- Server settings.

  Lists the configuration options from the Operation Settings and Security Settings workflows.

  Note: The listing uses the internal database names to prevent any confusion arising from translated options labels.
- Web applications.

  Lists the configuration of websites and applications in IIS.
- DLL files installed.
- COM interfaces.
- Shared reference counts.

  Indicates where installed products share files.

Click **Show Server Diagnostic Report** to open the report in a text editor. This file is available under the name:

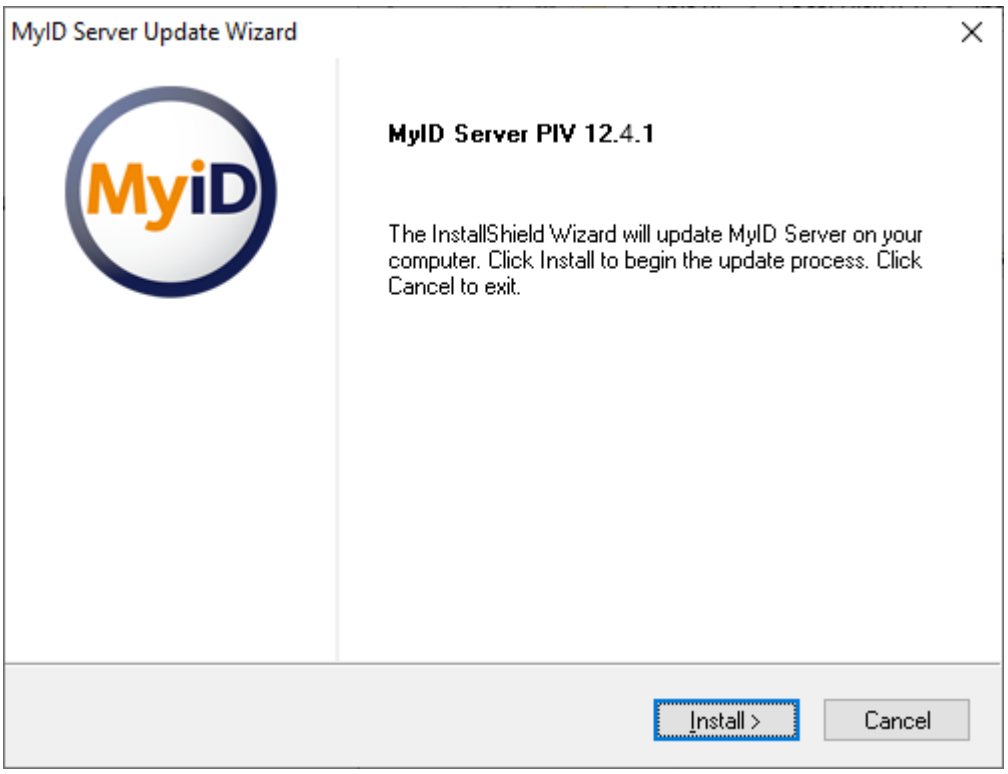
```
ServerDiagnosticsReport.txt
```

in the following folder:

```
<install folder>\Support Tools\MyIDInstallationAssistant\TestReports\
```

Click **Next** to move to the next stage.

2.24 Applying an update



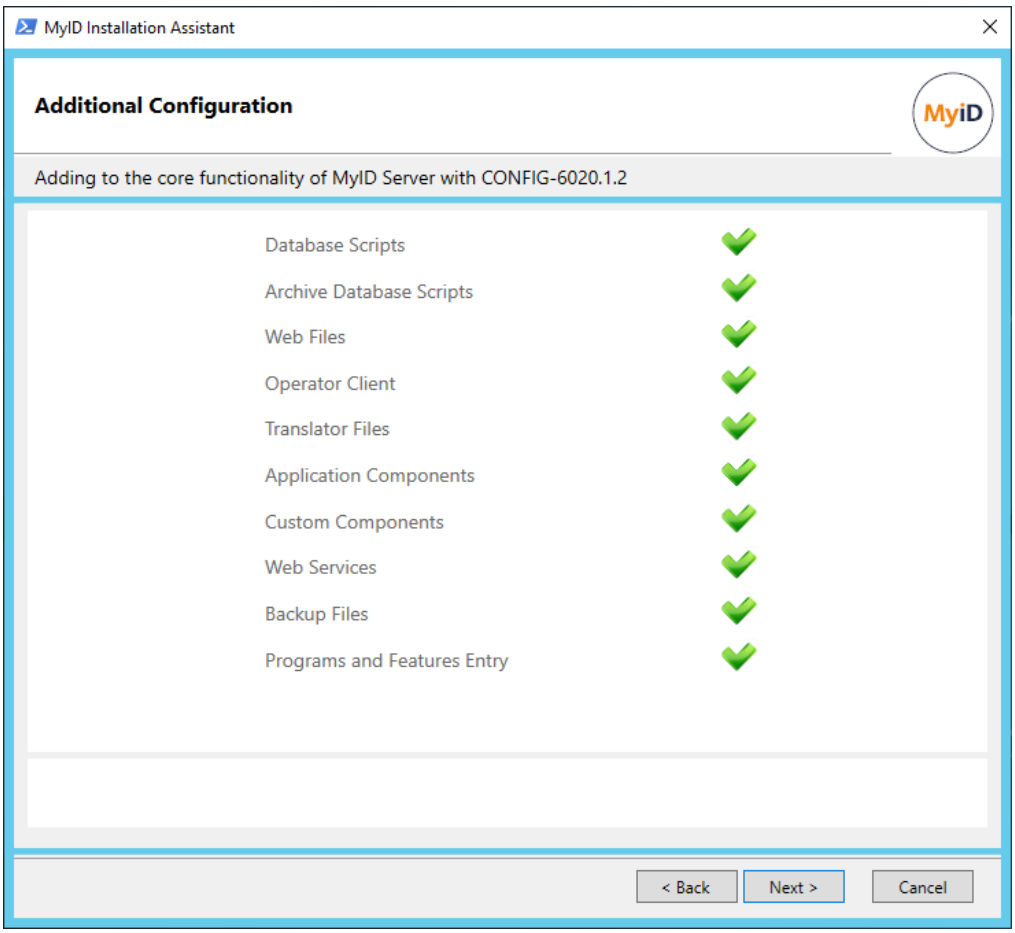
Important: You *must* prepare the installation folder before you start the update process. See section *2.2.4*, *Upgrading or updating the MyID Installation Assistant*.

If you have included an update (`MyIDServer-12.x.x_Update.exe`) in the `Installer` folder, and selected it in the Installation Package Manager, it is installed automatically; see section *2.6*, *The Installation Package Manager*.

If you have selected a main MyID installation (whether a fresh installation or an upgrade), the update is applied after this have been installed.

Once the update has been installed, the MyID Installation Assistant displays the results of the installation process. See section *2.20*, *Checking the installation log results*.

2.25 Installing a server configuration package

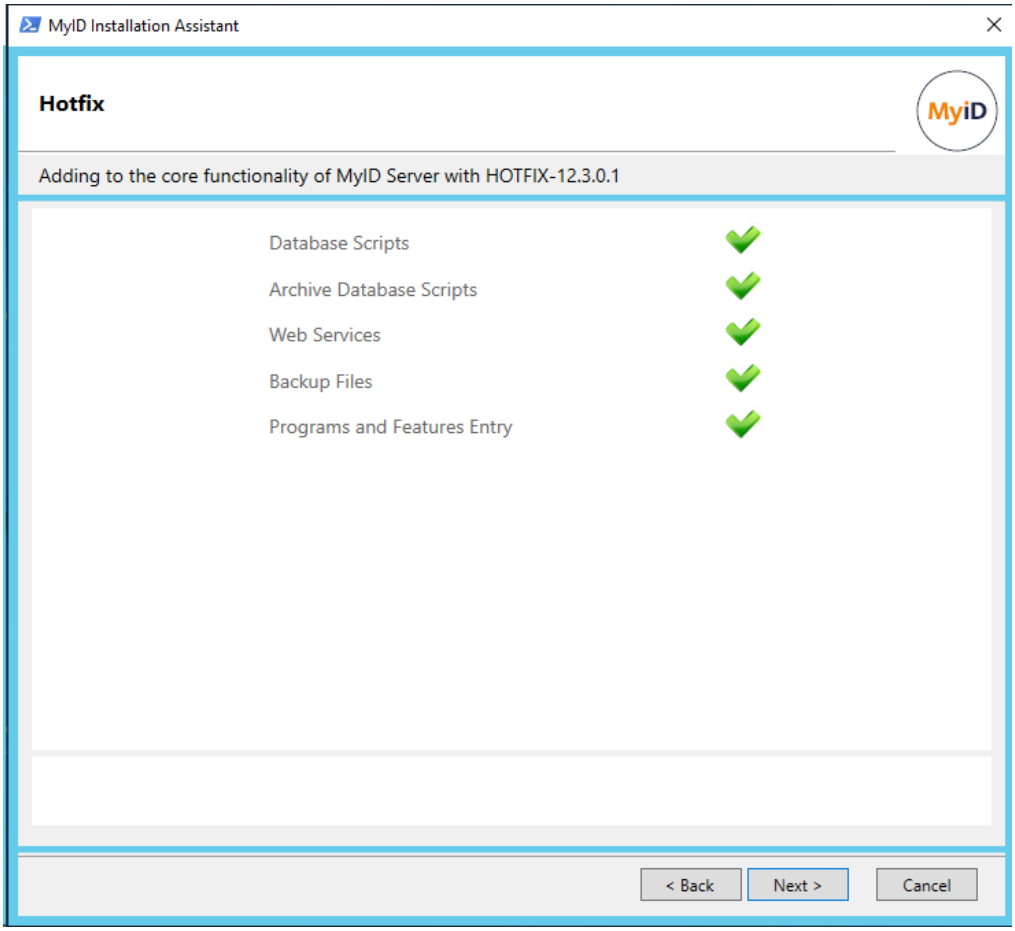


If you have included a server configuration package (`CONFIG-xxxx.x.x`) in the `Installer` folder, and selected it in the Installation Package Manager, it is installed automatically; see section *2.6*, *The Installation Package Manager*.

If you have selected a main MyID installation (whether a fresh installation or an upgrade) or a server update, the server configuration package is applied after these have been installed.

Important: Intercede periodically updates the certificate used to sign its installation PowerShell scripts; the certificate used to sign a configuration package may be newer than the certificate you previously trusted to install the main MyID software. Accordingly, you must make sure that the certificate used for the configuration package is trusted on your MyID servers before starting the installation. See section *2.2.1*, *Trusting the signed scripts* for details; instead of the `MyIDInstallationAssistant.ps1` script in the main MyID release, select the `Install.ps1` script provided in the configuration package.

2.26 Applying a hotfix



If you have included a hotfix (`HOTFIX-x.x.x.x`) in the `Installer` folder, and selected it in the Installation Package Manager, it is installed automatically; see section *2.6*, *The Installation Package Manager*.

If you have selected a main MyID installation (whether a fresh installation or an upgrade), a server update, or a server configuration package, the hotfix is applied after these have been installed.

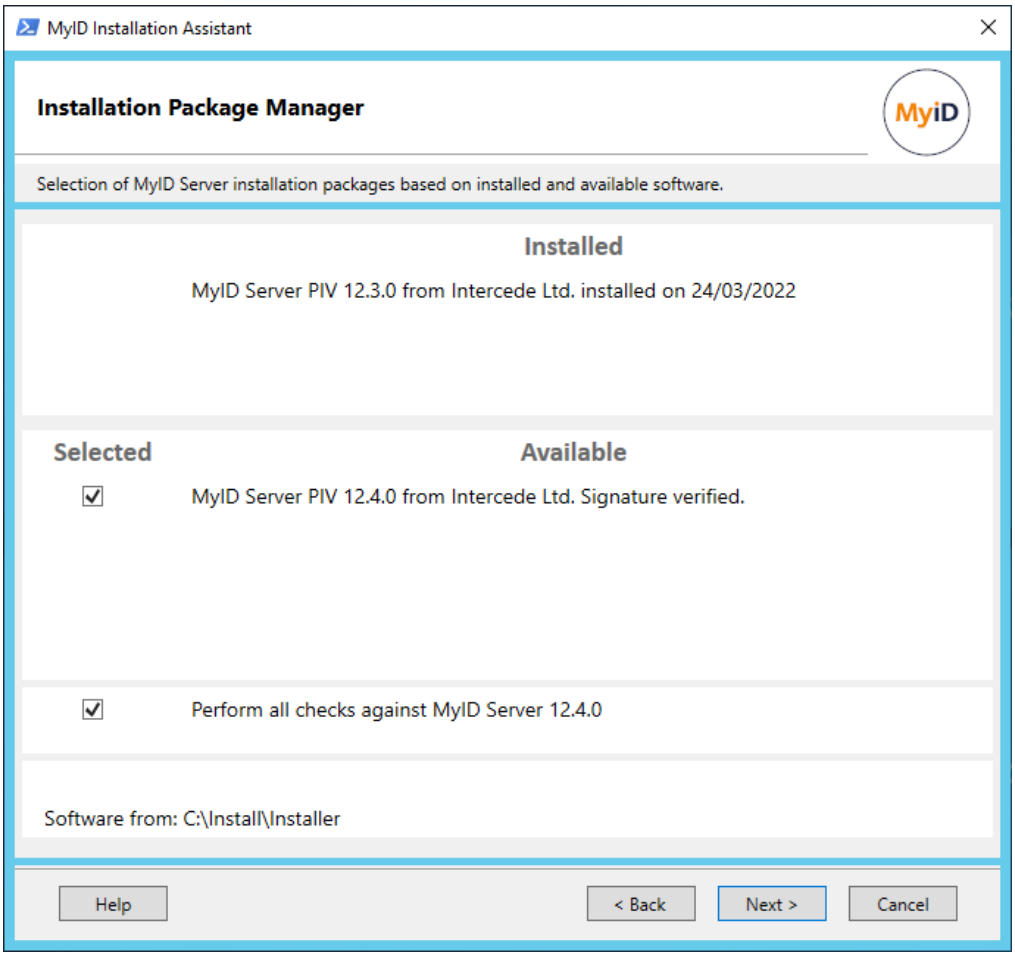
Important: Intercede periodically updates the certificate used to sign its installation PowerShell scripts; the certificate used to sign a hotfix may be newer than the certificate you previously trusted to install the main MyID software. Accordingly, you must make sure that the certificate used for the hotfix is trusted on your MyID servers before starting the installation. See section *2.2.1*, *Trusting the signed scripts* for details; instead of the `MyIDInstallationAssistant.ps1` script in the main MyID release, select the `Install.ps1` script provided in the hotfix.

2.27 Upgrading MyID

The process for upgrading MyID depends on the version of the system from which you are upgrading.

Important: This section contains instructions for running the MyID Installation Assistant as part of an upgrade process; however, an upgrade is a significant change to your system and you must take care to ensure that you follow the appropriate procedures both before and after running the MyID Installation Assistant. See section *7*, *Upgrading MyID* for full details on the upgrade process.

2.27.1 Upgrading from a MyID 12 system



Important: You *must* prepare the installation folder before you start the update process. See section *2.2.4*, *Upgrading or updating the MyID Installation Assistant*.

To upgrade from a MyID 12 system, run the MyID Installation Assistant.

1. On the Intercede Package Manager screen, select the new software to be installed.

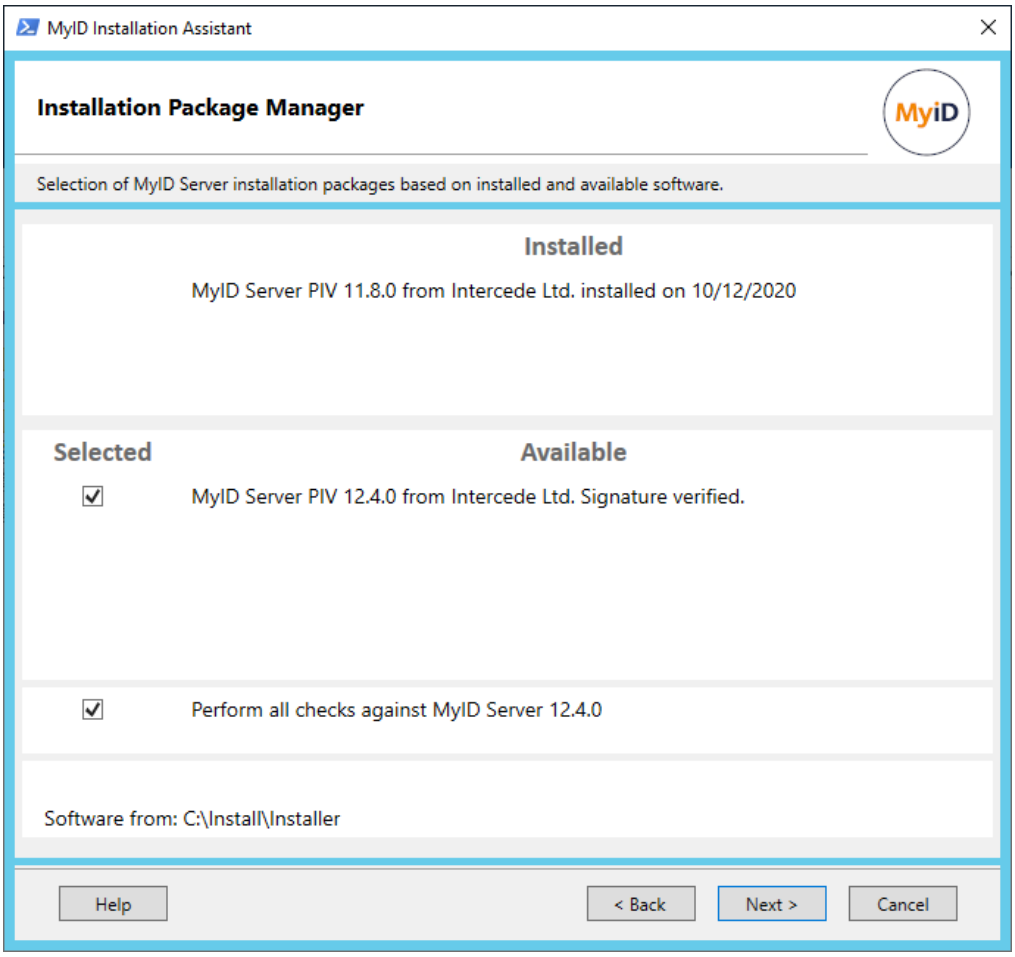
   You are strongly recommended to perform all the checks for the new version. The requirements for MyID may change between versions, and this ensures that your system is suitable for the new version of MyID.

2. Click **Next** to proceed to the next stage.

The upgrade process follows the same process as a fresh installation of MyID.

Note: On the Select Roles and Features screen (see section *2.7*, *Selecting the server roles and features*) make sure that the list of features you want to install is correct. The MyID Installation Assistant interrogates the registry for details of the features that are already installed, but the registry does not contain details of every feature. See section *7.1.1*, *Selecting features when upgrading* for more information.

2.27.2 Upgrading from a MyID 11 system

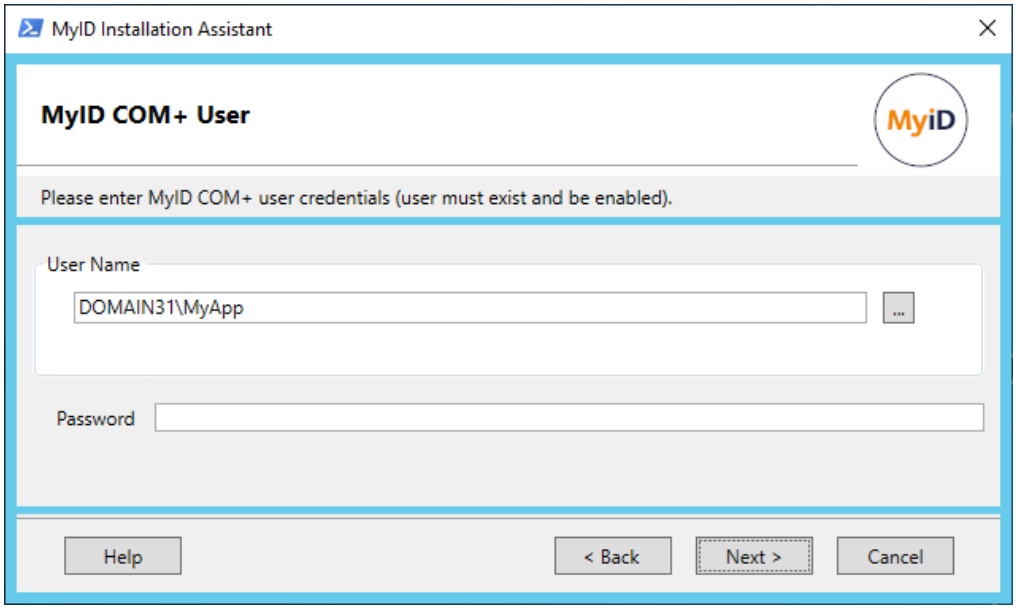


MyID 11 was a 32-bit application, while MyID 12 is a 64-bit application. The MyID Installation Assistant must carry out an additional procedure to back up your configuration, uninstall your previous version of MyID, retaining the database, install the 64-bit version, then restore your configuration to the 64-bit locations on the file system and in the registry.

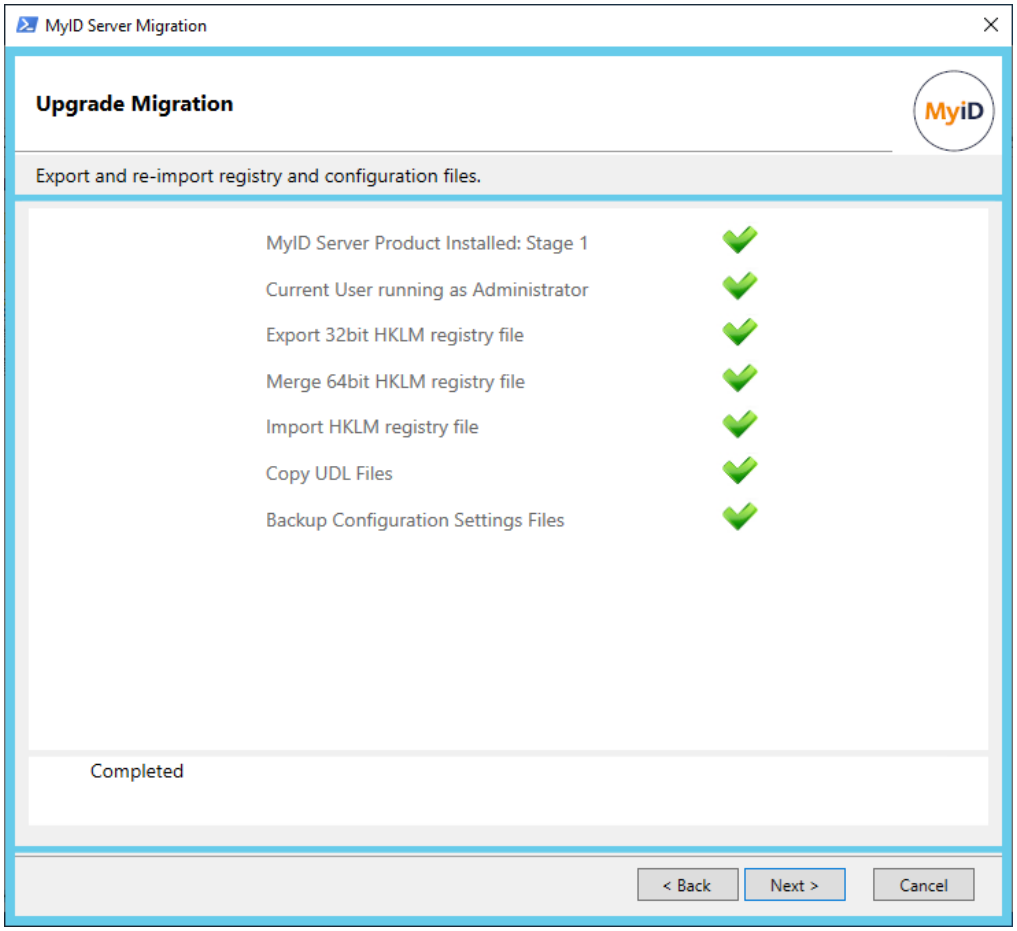
To upgrade from a MyID 11 system:

1. On the Intercede Package Manager screen, select the new software to be installed.

   You are strongly recommended to perform all the checks for the new version. The requirements for MyID may change between versions, and this ensures that your system is suitable for the new version of MyID.
2. Click **Next** to proceed to the next stage.
3. Enter your MyID COM+ user details, and click **Next**.



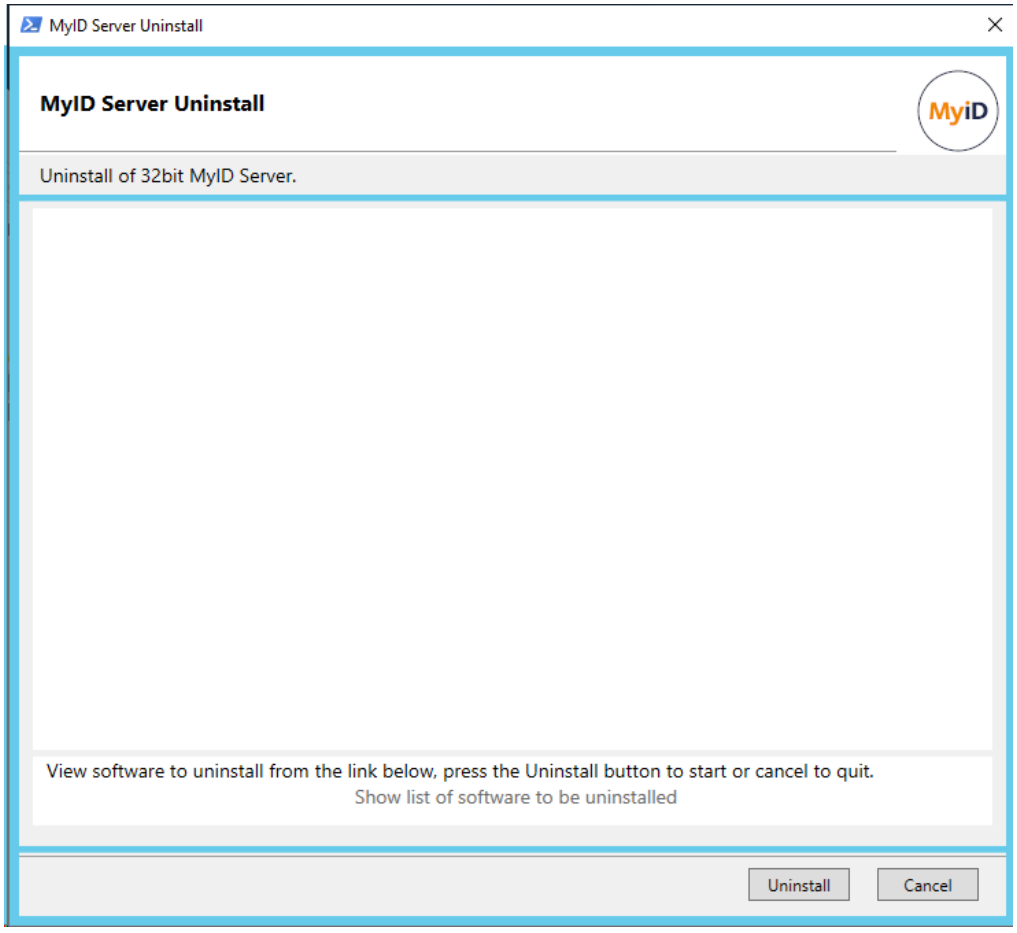
The MyID COM+ user is required to run the upgrade migration process.



4. Click **Next** to proceed to the next stage.

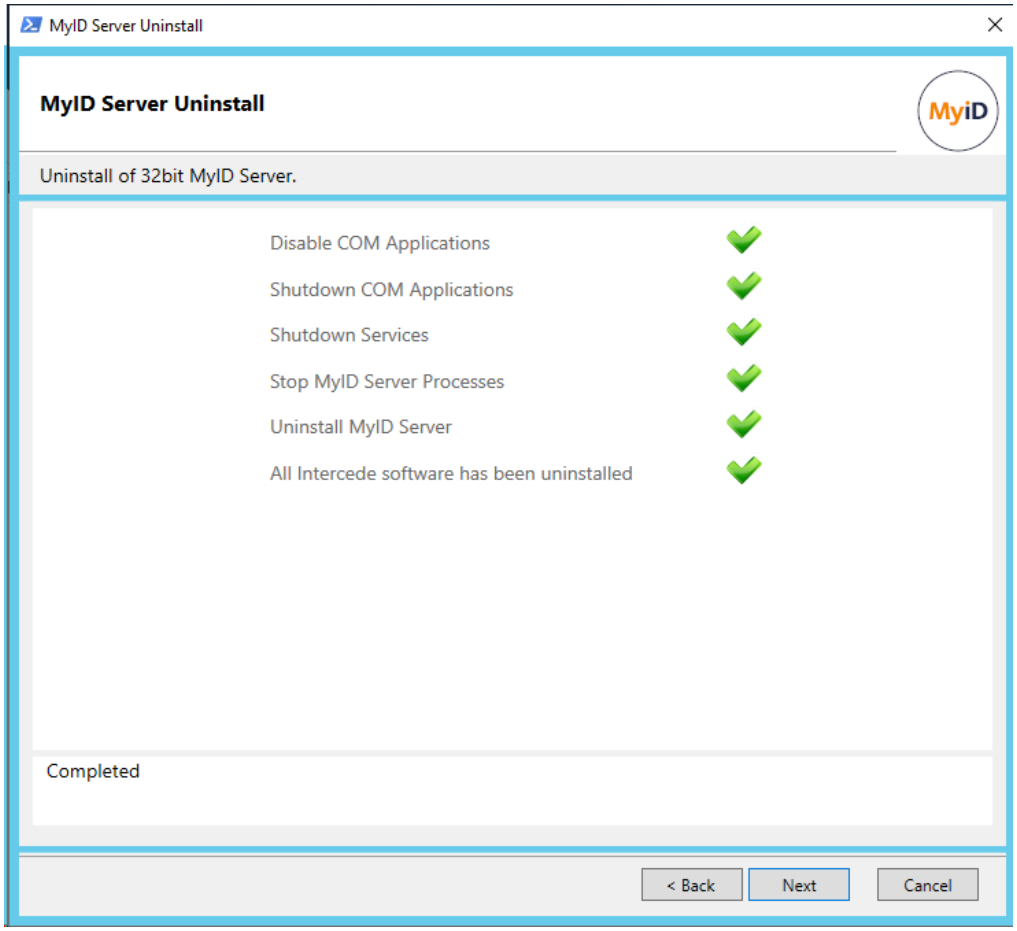
5. On the Select Roles and Features screen (see section *2.7*, *Selecting the server roles and features*) make sure that the list of features you want to install is correct. The MyID Installation Assistant interrogates the registry for details of the features that are already installed, but the registry does not contain details of every feature. See section *7.1.1*, *Selecting features when upgrading* for more information.

   The upgrade process follows the same process as a fresh installation of MyID until the after the Pre-Installation Check Results screen (see section *2.18*, *Pre-installation check results*), when the MyID Server Uninstall screen appears:



6. Click **Show list of software to be uninstalled** to open a text file listing the software that will be uninstalled, then click **Uninstall** to remove this software.

   You must uninstall the old 32-bit software before you can install the new 64-bit software. You cannot upgrade the software in place.



7. When the uninstallation has completed, click Next to view the installation log results.

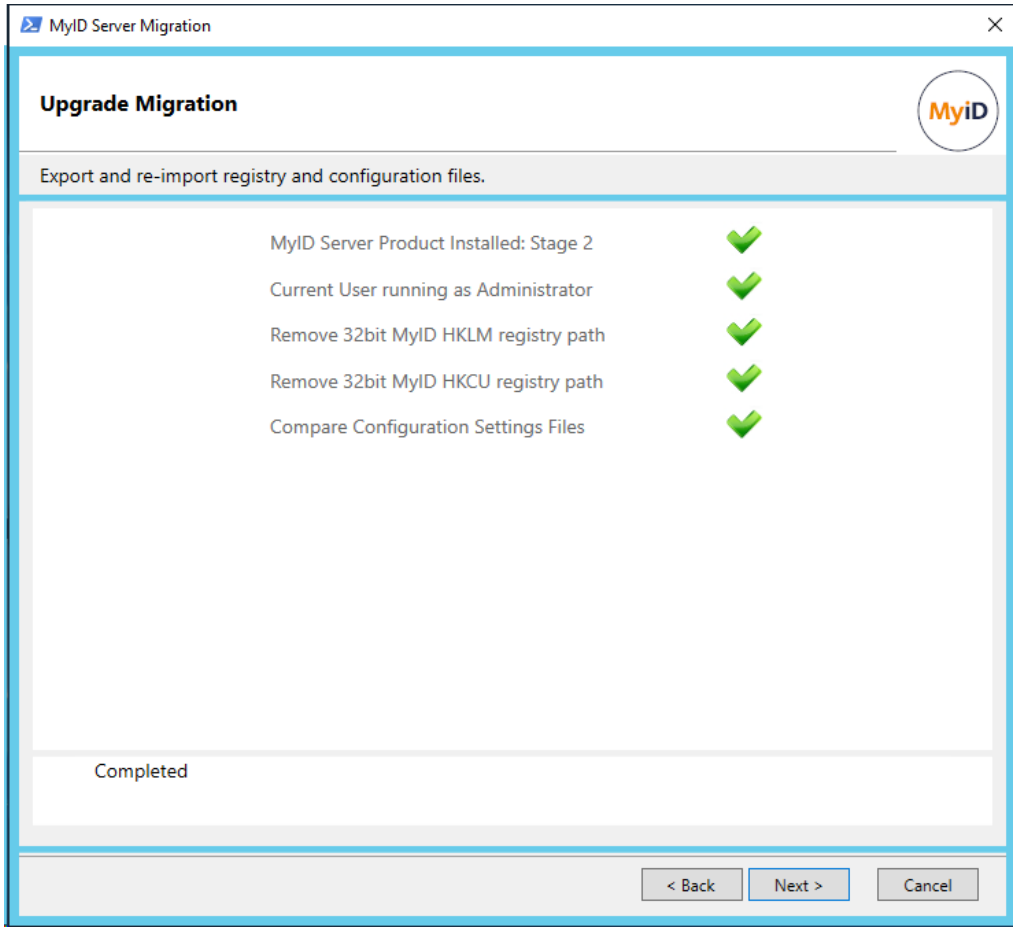
   See section *2.20*, *Checking the installation log results*.

   Click **Next** to proceed to the next stage. If you are asked to reboot, do so, then launch the MyID Installation Assistant again.

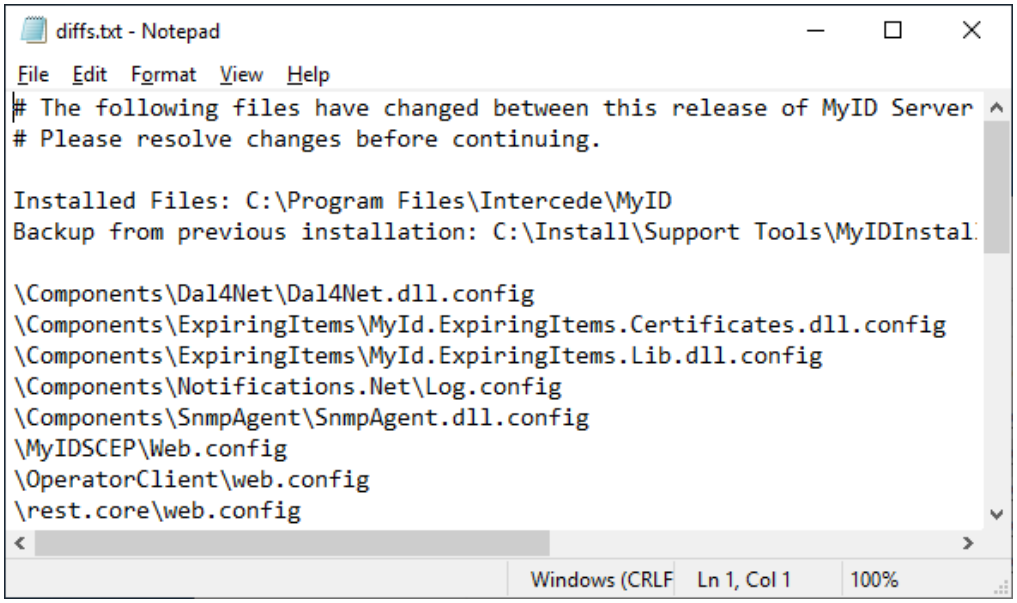
8. Proceed with the installation of the new version.

   See section *2.19*, *Starting the server installation*.

9. After the Post-Installation Check Results screen (see section *2.22*, *Post-installation check results*) the MyID Installation Assistant runs the next stage of the upgrade migration script to import the settings that were backed up.



The MyID Installation Assistant also opens a text file containing a report showing any differences between the configuration files from your previous system and the files installed by the current installation program.



10. Review the changes between the configuration files; if you have made any manual changes to the configuration files, you must implement them in the current versions of the files.

    This file is available under the name:

    ```
    diffs.txt
    ```

    in the following folder:

    ```
    <install folder>\Support Tools\MyIDInstallationAssistant\UpgradeFiles\
    ```

    Note: Some changes in the configuration files may be the result of enhancements to MyID since your previous version was released. If you are unsure about any changes, contact customer support quoting reference SUP-342 for assistance.

11. Click **Next**, and the MyID Installation Assistant runs the Server Diagnostic Report.

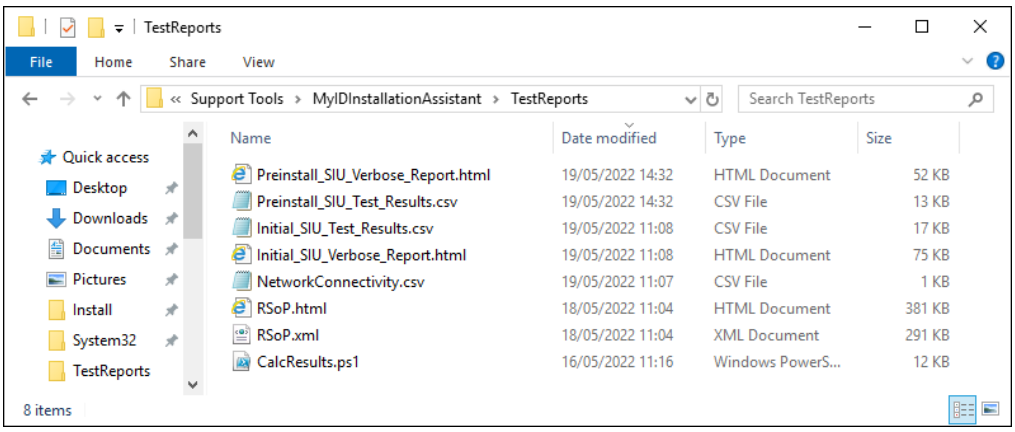
    See section *2.23*, *Server Diagnostic Report*.

12. Click **Next**, and the upgrade is complete.

2.27.3 Upgrading from an earlier system

The MyID Installation Assistant has not been verified for upgrading from MyID 10 or earlier systems. You are recommended to carry out the upgrade process that uses the provided upgrade migration script instead of the MyID Installation Assistant to manage the upgrade process; see section *7.5*, *Upgrading MyID from a 32-bit application to 64-bit* for details. You can use the MyID Installation Assistant to install the new version of MyID as part of the upgrade process.

2.28 Checking the logs and reports



The MyID Installation Assistant creates a folder of logs and reports based on the checks it carries out; you can find this information in the following folder:

```
<install folder>\Support Tools\MyIDInstallationAssistant\TestReports\
```

A redacted and anonymized version of these reports is available in the following folder:

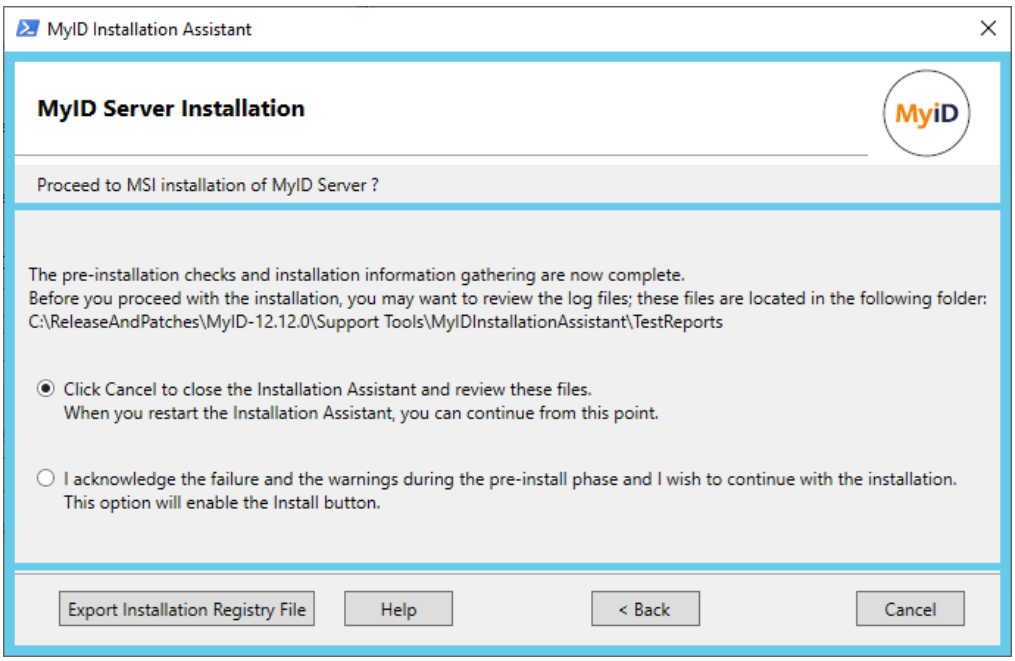
```
<install folder>\Support
Tools\MyIDInstallationAssistant\TestReportsRedacted\
```

You can use the following PowerShell script:

```
CalcResults.ps1
```

to scan the logs and list which ones contain warnings or errors.

2.29 Automating an installation



Once you have reached the MyID Server Installation screen, you can decide to proceed with the installation, or close the MyID Installation Assistant to return to it at a later time and complete the installation; alternatively, you can export all the settings you have entered up to this point as a registry file, and use this file to automate the MyID Installation Assistant process either on the current machine, or on another machine that has the same environment and configuration.

The process is as follows:

1. Export the registry file.

   See section *2.29.1*, *Exporting the registry file*.

2. Update the registry file with the credentials.

   The registry file does not contain any of the usernames or passwords you have provided when going through the MyID Installation Assistant process.

   You must populate the file with the appropriate credentials before you can use it to automate an installation. You can:

   - Provide the credentials interactively.

     See section *2.29.2*, *Populating the credentials in the registry file*.

   - Create a configuration file to store the credentials.

     See section *2.29.3*, *Automating the population of credentials in the registry file*.

3. Enable the automation flag and run the MyID Installation Assistant.

   See section *2.29.4*, *Configuring the automation settings*.

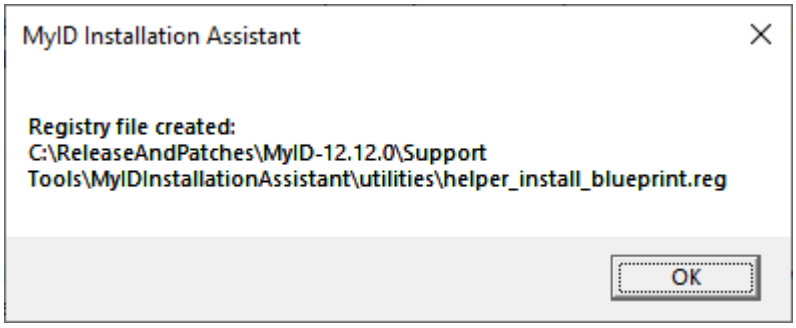
2.29.1 Exporting the registry file

To export the registry file:

1. On the MyID Server Installation screen, click **Export Installation Registry File**.

   The MyID Installation Assistant exports the installation configuration to the `helper_install_blueprint.reg` file in the following folder:

   `<install folder>\Support Tools\MyIDInstallationAssistant\utilities\`



2. Click **OK**.
3. Click **Cancel** to close the MyID Installation Assistant.

2.29.2 Populating the credentials in the registry file

For security reasons, the exported `helper_install_blueprint.reg` file strips out the usernames and passwords for the MyID service accounts (the MyID COM+ user, the MyID IIS user, the MyID Web Services user, and the MyID Authentication user), the database accounts, the HSM credentials, and the password for the MyID startup account.

To allow you to use these credentials when running the MyID Installation Assistant in automation mode, you can use the provided `SetupUsers.ps1` PowerShell script to insert these passwords into the registry file. This script uses DPAPI to encrypt the passwords; this means you must run the script on the machine on which you want to import the registry file, under the user account you will use to run the MyID Installation Assistant.

To store the account passwords:

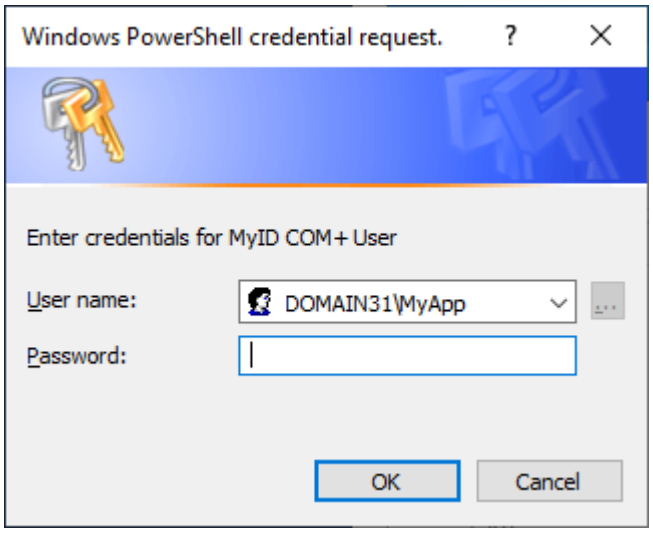
1. Log on using the Windows user account you will use to run the MyID Installation Assistant, on the server on which you will run the MyID Installation Assistant.
2. Open a Windows PowerShell command prompt.
3. Navigate to the following folder:

   `<install folder>\Support Tools\MyIDInstallationAssistant\utilities\`
4. Make sure that there is no file called `SetupUsers.json` in the `utilities` folder.

   This file is used for automating the `SetupUsers.ps1` script; see section *2.29.3*, *Automating the population of credentials in the registry file*. If this file exists, the script does not prompt for passwords, but instead loads the defaults from the file.
5. Run the following script:

   `.\SetupUsers.ps1`
6. Follow the on-screen prompts to provide the user credentials.

   The script prompts for each set of credentials:



   If the script does not prompt for passwords, check to make sure you do not have file called `SetupUsers.json` in the `utilities` folder; if you do, remove it, and run the script again.

When the script is complete, it writes an updated registry file called `helper_install.reg` to the following folder:

```
<install folder>\Support Tools\MyIDInstallationAssistant\
```

2.29.3 Automating the population of credentials in the registry file

In some test environments, you may want to automate running the `SetupUsers.ps1` script so that no user interaction is required to populate the registry file with passwords. To do this, you can provide the passwords in plain text in a file called `SetupUsers.json` in the `utilities` folder.

Note: This file is short-lived. When you run the `SetupUsers.ps1` script, it extracts the passwords from this file, encrypts them, stores them in the `helper_install.reg` file, then (by default) deletes the `SetupUsers.json` file.

To automate the `SetupUsers.ps1` script:

1. Open the `SetupUsers.json` template file in the following folder:

   `<install folder>\Support Tools\MyIDInstallationAssistant\utilities\`

2. Edit the following:

```
[
        {
            "COMUser": "Domain\\ComUser",
            "COMCred": "COMUserCredential",
            "IISUser": "Domain\\IISUser",
            "IISCred": "IISUserCredential",
            "WSUser": "Domain\\WebServiceUser",
            "WSCred": "WebServiceUserCredential",
            "AuthWSUser": "Domain\\AuthenticationWebServiceUser",
            "AuthWSCred": "AuthenticationWebServiceUserCredential",
            "DBUser": "MyIDDBUser",
            "DBCred": "MyIDDBCred",
            "DBArchUser": "MyIDArchDBUser",
            "DBArchCred": "MyIDArchDBCred",
            "AuthDBUser": "MyIDAuthDBUser",
            "AuthDBCred": "MyIDAuthDBCred",
            "HSMPartitionPasswordCred": "HSMPartitionPasswordCred",
            "HSMPINCred": "HSMPINCred",
            "StartupPasswordCred": "StartupPasswordCred"
        }
]
```

where:

- `COMUser` – the domain and user for the MyID COM+ user account.
- `COMCred` – the password for the MyID COM+ user account in plain text.
- `IISUser` – the domain and user for the MyID IIS user account.
- `IISCred` – the password for the MyID IIS user account in plain text.
- `WSUser` – the domain and user for the MyID web service user account.
- `WSCred` – the password for the MyID web service account in plain text.
- `AuthWSUser` – the domain and user for the MyID auth user account.
- `AuthWSCred` – the password for the MyID auth account in plain text.
- `DBUser` – if you are using SQL authentication, the database user name.

- `DBCred` – the database user password in plain text.
- `DBArchUser` – if you are using SQL authentication, the archive database user name.
- `DBArchCred` – the archive database password in plain text.
- `AuthDBUser` – if you are using SQL authentication, the authentication database user name.
- `AuthDBCred` – the authentication database password in plain text.
- `HSMPartitionPasswordCred` – if you are using a Thales LUNA HSM, the HSM partition password in plain text.
- `HSMPINCred` – if you are installing an additional application server that uses an HSM, the HSM PIN in plain text.
- `StartupPasswordCred` – the password for the startup user, in plain text.

Note: Use double slashes for the slashes in the `domain\user` for each username; for example, for the `MYDOMAIN\MyUserName` account, use:

```
MYDOMAIN\\MyUserName
```

You do not need to include any items that you are not using for the current installation; for example, if you are using Windows authentication for database access, you do not need to provide database usernames and passwords, or if you are installing the application server and database server, you do not need to provide the IIS user account or web service account details.

For example:

```
[
  {
    "COMUser": "Domain\\ComUser",
    "COMCred": "MyIDCOMUserPassword123",
    "IISUser": "Domain\\IISUser",
    "IISCred": "MyIDIISUserPassword123",
    "WSUser": "Domain\\WebServiceUser",
    "WSCred": "MyIDWSUserPassword123",
    "AuthWSUser": "Domain\\AuthenticationWebServiceUser",
    "AuthWSCred": "MyIDAuthUserPassword123",
    "StartupPasswordCred": "StartupPassword123"
  }
]
```

3. Save the file.

You can now run the `SetupUsers.ps1` PowerShell script to insert these credentials into the registry file.

Important: By default, the `SetupUsers.ps1` script deletes the `SetupUsers.json` file on completion. If you want to retain the file, you can run the script with the following parameter:

```
.\SetupUsers.ps1 -KeepJsonFile $True
```

Note, however, that the `SetupUsers.json` file is *always* deleted when you run the MyID Installation Assistant. If you want to retain the information in this file, make sure that you

make a secure backup before you run the script; for security reasons, you are not recommended to leave this file with plaintext passwords freely available on the server for longer than is necessary.

2.29.4 Configuring the automation settings

The MyID Installation Assistant automation mode is controlled by a configuration file.

To enable the automation settings:

1. In a text editor, open the following file:

   `<install folder>\Support Tools\MyIDInstallationAssistant\defaults\Automation.js`

2. Edit the following settings:

```
[
        {
            "AUTOSEQ": "0",
            "MANSEQ": "1",
            "ApplyFixItScripts": "0",
            "StopLevel": "None"
        }
]
```

   Set the following:

   - `AUTOSEQ` – set this option to `1` to enable automation mode.

     To disable automation mode, set this option to `0`.

   - `MANSEQ` – set this option to `1` to perform the standard MyID Installation Assistant checks.

     To disable checks, set this option to `0`.

   - `ApplyFixItScripts` – set this option to `1` to apply the fix-it scripts automatically.

     The MyID Installation Assistant runs the scripts up to three times to attempt to fix the issues. If there are still issues after three attempts, the MyID Installation Assistant checks the `StopLevel` configuration to determine its course of action.

     To disable fix-it scripts, set this option to `0`.

   - `StopLevel` – set this option to one of the following:

     - `"None"` – the automation stops only if a fatal issue occurs.
     - `"Error"` – the automation stops if an fatal issue or an error occurs.
     - `"Warning"` – the automation stops if a fatal issue, an error, or a warning occurs.

   For example:

```
[
        {
            "AUTOSEQ": "1",
            "MANSEQ": "1",
            "ApplyFixItScripts": "1",
            "StopLevel": "None"
        }
]
```

   This example enables automation mode, runs all checks, applies all relevant fix-it scripts,

and stops only if it encounters a fatal error.

3. Save the configuration file.

When you run the MyID Installation Assistant in automation mode, it loads the contents of the `helper_install.reg` file into the registry, including the encrypted passwords you added to the file, then starts at the first screen, and automatically moves through each screen without user interaction, until it completes the installation of MyID.

If an error occurs and the MyID Installation Assistant stops, the screen on which the error occurred remains open. You can also view the results of the SIU tests in the `TestReports` folder.

If you experience issues, you are recommended to run the installation from the Windows PowerShell command prompt:

1. Open a Windows PowerShell command prompt with elevated permissions.
2. Navigate to the following folder:

   ```
   <install folder>\Support Tools\MyIDInstallationAssistant\
   ```

3. Run the following script:

   ```
   .\MyIDInstallationAssistant.ps1
   ```

This provides you with some additional debug information in the console.

2.29.5 Checking the imported passwords

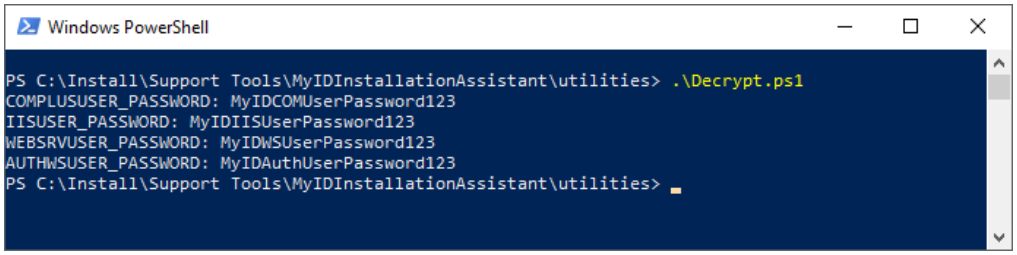
Once the MyID Installation Assistant has started in automation mode and loaded the contents of the `helper_install.reg` file into the registry, you can confirm that you have entered the service account passwords correctly by running the `Decrypt.ps1` script.

To check the values of service account passwords in the registry:

1. Log on using the Windows user account you will use to run the MyID Installation Assistant, on the server on which you will run the MyID Installation Assistant.
2. Open a Windows PowerShell command prompt.
3. Navigate to the following folder:

   `<install folder>\Support Tools\MyIDInstallationAssistant\utilities\`
4. Run the following script:

   `.\Decrypt.ps1`



The user account passwords are obtained from the registry and decrypted using DPAPI with your logged-on user's credentials.

If the passwords do not match, or the script displays an error, make sure that you have logged on to the same machine with the same user account as was used to run the `SetupUsers.ps1` script.

3 The System Interrogation Utility

The System Interrogation Utility (SIU) is a support tool for determining whether the prerequisites stated in the MyID installation documentation have been satisfied. You can run the SIU independently; however, its tests are also integrated into the MyID Installation Assistant, which runs the appropriate tests for the initial server check, the pre-installation check, and the post-installation check at the appropriate stages of the installation process.

The SIU performs a series of automated tests on the hardware, software, and configuration of the server PCs of a MyID installation. You are recommended to run the utility both *before* and *after* the installation of MyID; the MyID Installation Assistant automatically runs the relevant tests at the appropriate stage of the installation process.

Throughout this document are included SIU references; these refer to tests carried out by the System Interrogation Utility. The *Description of derived tests* section in the ***System Interrogation Utility*** guide provides a master list of each test along with a link to the section of the documentation where the requirement is listed.

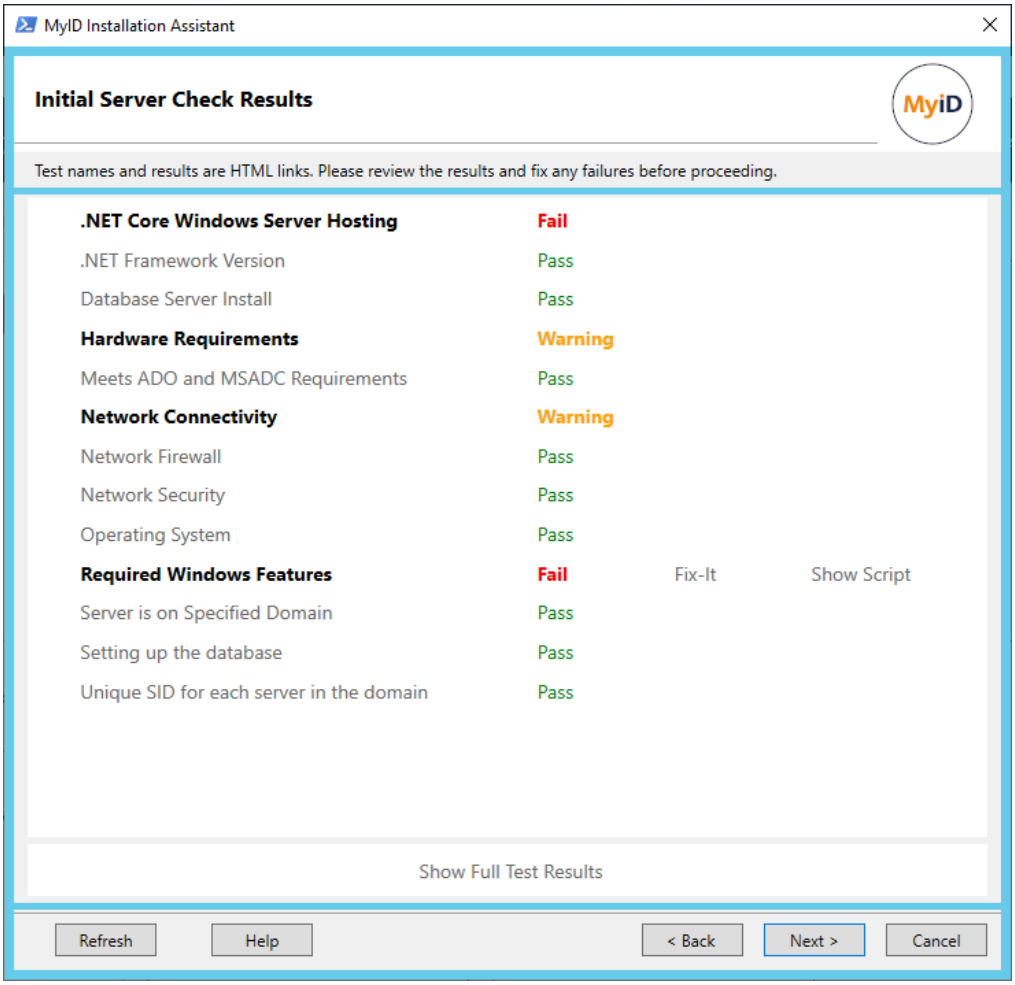
Note: Running the SIU tests does not eliminate the need to consult the core product documentation provided with MyID; it is a useful additional tool that can help prepare your system and confirm that it is appropriately configured for MyID.

The SIU is provided with the MyID installation in the `\Support Tools\System Interrogation Utility\` folder.

See the ***System Interrogation Utility*** guide for details.

4 Initial server configuration

When you run the MyID Installation Assistant, it carries out an Initial Server Check to ensure that you have carried out any initial system configuration, and your servers are ready to start installing MyID; see section *2.16*, *Initial server check results*.



This chapter contains details of the initial server configuration that you must carry out:

- section *4.1*, *MyID server hardware and software requirements*.
- section *4.2*, *Setting up Windows server roles and features*.
- section *4.3*, *Installing .NET Framework and .NET Core*.
- section *4.4*, *Configuring network connectivity*.
- section *4.5*, *Configuring your domain and directory*.
- section *4.6*, *Setting up the database*.

4.1 MyID server hardware and software requirements

This section contains details of the hardware (processor, RAM, display, disk space) and operating system requirements for the MyID servers.

The hardware and software described in this section are the minimum required for MyID. If your system does not match or exceed the requirements outlined in this section, contact Intercede for advice, quoting reference SUP-297.

4.1.1 Hardware requirements

SIU references: SIU-001, SIU-002, SIU-003, SIU-004, SIU-005, SIU-006, SIU-007, SIU-203.

Note: These are the minimum requirements for MyID, excluding operating system, Microsoft SQL Server, third party software, dependencies or drivers. Larger implementations may require faster processors, more memory and more disk space to maintain acceptable levels of performance.

- Processor: 2 GHz
- RAM: 4 GB
- Display resolution: 1024x768
- Hard disk space: 40 GB for the MyID Database server, 2GB for the other MyID servers.

4.1.2 Operating systems

SIU reference: SIU-008.

MyID supports the following server operating systems:

- Windows Server 2019

  MyID has been tested with Windows Server 2019 Standard version 10.0.17763.
- Windows Server 2022

  MyID has been tested with Windows Server 2022 Datacenter version 10.0.20348 (21H2)

4.1.3 Windows PowerShell 5.1

The MyID installation media provides PowerShell scripts that are run as part of the installation process, including post-install PowerShell scripts that run automatically after installing or uninstalling MyID. These scripts require Windows PowerShell 5.1. See for details of post-install PowerShell scripts.

Note: PowerShell Core 6.x or PowerShell 7.x are not supported; you must have Windows PowerShell 5.1 installed.

4.1.4 Additional requirements

SIU references: SIU-034, SIU-035, SIU-036.

- The server's regional setting, as set when you install Windows, is used to determine the date formats displayed on some screens within MyID. This setting must not be changed after installing MyID; make sure that you install Windows with the regional setting appropriate to the date display format you want to use.

  Note: If you are installing on a non-English version of Windows, additional configuration steps may be required.

4.2 Setting up Windows server roles and features

SIU references: SIU-100, SIU-101, SIU-102, SIU-103, SIU-104, SIU-106, SIU-107, SIU-110, SIU-111, SIU-112, SIU-113, SIU-114, SIU-115, SIU-117, SIU-118, SIU-119, SIU-120, SIU-121, SIU-122, SIU-124, SIU-125, SIU-204, SIU-205, SIU-238, SIU-239, SIU-240, SIU-241, SIU-242, SIU-243, SIU-244, SIU-245.

Note: When you install MyID using the MyID Installation Assistant, these requirements are checked on the Initial Server Check Results screen; if you need to add roles and features to your server configuration, you can use the fix-it script provided on that screen. See section *2.16*, *Initial server check results* for details.

4.2.1 Server roles for Windows Server 2019

You must configure the server roles using Server Manager.

4.2.1.1 MyID application server

Make sure the roles include the following:

- File and Storage Services\Storage Services

Set up the following features:

- .NET Framework 4.7 Features\.NET Framework 4.7
- .NET Framework 4.7 Features\WCF Services\TCP Port Sharing
- Windows PowerShell\Windows PowerShell 5.1
- WoW64 Support

4.2.1.2 MyID web server

Make sure the roles include the following:

- File and Storage Services\Storage Services
- Web Server (IIS)\Web Server\Common HTTP Features\Default Document
- Web Server (IIS)\Web Server\Common HTTP Features\HTTP Errors
- Web Server (IIS)\Web Server\Common HTTP Features\Static Content
- Web Server (IIS)\Web Server\Health and Diagnostics\HTTP Logging
- Web Server (IIS)\Web Server\Performance\Static Content Compression
- Web Server (IIS)\Web Server\Security\

  Note: The Security sub-roles required depend on your configuration of MyID and IIS. You are recommended to select all security sub-roles. For example, the following role is required if you are using Integrated Windows Logon:

  - Web Server (IIS)\Web Server\Security\Windows Authentication
- Web Server (IIS)\Web Server\Application Development\.NET Extensibility 4.7
- Web Server (IIS)\Web Server\Application Development\ASP
- Web Server (IIS)\Web Server\Application Development\ASP.NET 4.7
- Web Server (IIS)\Web Server\Application Development\ISAPI Extensions
- Web Server (IIS)\Web Server\Application Development\ISAPI Filters

- Web Server (IIS)\Management Tools\IIS Management Console
- Web Server (IIS)\Management Tools\IIS Management Scripts and Tools

Set up the following features:

- .NET Framework 4.7 Features\.NET Framework 4.7
- .NET Framework 4.7 Features\ASP.NET 4.7
- .NET Framework 4.7 Features\WCF Services\TCP Port Sharing
- Windows PowerShell\Windows PowerShell 5.1
- Windows Process Activation Service\Process Model
- Windows Process Activation Service\Configuration APIs
- WoW64 Support

4.2.1.3 MyID database server

Make sure the roles include the following:

- File and Storage Services\Storage Services

Set up the following feature:

- Windows PowerShell\Windows PowerShell 5.1

4.2.2 Server roles for Windows Server 2022

You must configure the server roles using Server Manager.

4.2.2.1 MyID application server

Make sure the roles include the following:

- File and Storage Services\Storage Services

Set up the following features:

- .NET Framework 4.8 Features\.NET Framework 4.8
- .NET Framework 4.8 Features\WCF Services\TCP Port Sharing
- Windows PowerShell\Windows PowerShell 5.1
- WoW64 Support

4.2.2.2 MyID web server

Make sure the roles include the following:

- File and Storage Services\Storage Services
- Web Server (IIS)\Web Server\Common HTTP Features\Default Document
- Web Server (IIS)\Web Server\Common HTTP Features\HTTP Errors
- Web Server (IIS)\Web Server\Common HTTP Features\Static Content
- Web Server (IIS)\Web Server\Health and Diagnostics\HTTP Logging
- Web Server (IIS)\Web Server\Performance\Static Content Compression
- Web Server (IIS)\Web Server\Security\

Note: The Security sub-roles required depend on your configuration of MyID and IIS. You are recommended to select all security sub-roles. For example, the following role is required if you are using Integrated Windows Logon:

- Web Server (IIS)\Web Server\Security\Windows Authentication

- Web Server (IIS)\Web Server\Application Development\.NET Extensibility 4.8
- Web Server (IIS)\Web Server\Application Development\ASP
- Web Server (IIS)\Web Server\Application Development\ASP.NET 4.8
- Web Server (IIS)\Web Server\Application Development\ISAPI Extensions
- Web Server (IIS)\Web Server\Application Development\ISAPI Filters
- Web Server (IIS)\Management Tools\IIS Management Console
- Web Server (IIS)\Management Tools\IIS Management Scripts and Tools

Set up the following features:

- .NET Framework 4.8 Features\.NET Framework 4.8
- .NET Framework 4.8 Features\ASP.NET 4.8
- .NET Framework 4.8 Features\WCF Services\TCP Port Sharing
- Windows PowerShell\Windows PowerShell 5.1
- Windows Process Activation Service\Process Model
- Windows Process Activation Service\Configuration APIs
- WoW64 Support

4.2.2.3 MyID database server

Make sure the roles include the following:

- File and Storage Services\Storage Services

Set up the following feature:

- Windows PowerShell\Windows PowerShell 5.1

4.3 Installing .NET Framework and .NET Core

MyID requires both .NET Framework and .NET Core.

4.3.1 .NET Framework

SIU references: SIU-037, SIU-038.

The Microsoft .NET framework version 4.8 must be installed on web server, application server, database server, and all client PCs before you install MyID.

Note: MyID is developed and tested using .NET framework 4.8. If you need to use a later version of the .NET framework, contact customer support quoting reference SUP-283.

Note: For Windows Server, you must upgrade your system to .NET 4.8. See the Microsoft website for details.

4.3.2 .NET Core Hosting

SIU references: SIU-299, SIU-300, SIU-321.

The web services server requires ASP.NET Core Runtime 8.0 Hosting Bundle. The application server requires the .NET Runtime 8.0 package. In addition, any client on which you want to run the MyID Operator Client requires the Desktop Runtime version of .NET Core.

To obtain the installation programs, visit the Microsoft .NET download site:

dotnet.microsoft.com/en-us/download/dotnet/8.0/runtime

- For the MyID web services server, download and install ASP.NET Core Runtime 8.0 Hosting Bundle.

  Important: You must install the Core Hosting Bundle *after* installing IIS. If you install the Core Hosting Bundle before IIS, you must repair the installation; run the Core Hosting Bundle installation program again after installing IIS.

- For the MyID application server, download and install the .NET Runtime 8.0 package.

- For each client PC that is going to use the MyID Operator Client or the MyID Client for Windows, download and install the .NET Core Desktop Runtime 8.0.

  Note: On a 64-bit client operating system, you require *both* the x86 and x64 versions of the .NET Core Desktop Runtime 8.0. On a 32-bit client operating system, you require only the x86 version.

  The .NET Core Desktop Runtime (x64 version) is also required on the MyID application server if you want to use the MyID Document Uploader; see the ***MyID Document Uploader*** guide for more information.

Important: Microsoft releases updates for .NET Core that are compatible with the initial release. These updates include security fixes that are essential to the continued safe operation of your system. You are strongly advised to keep your installation of .NET Core up-to-date with the latest third point releases available from Microsoft; for example, 8.0.1 for .NET Core 8.0.

4.4 Configuring network connectivity

SIU references: SIU-023, SIU-024, SIU-025, SIU-026, SIU-027, SIU-028, SIU-029, SIU-030, SIU-152, SIU-235, SIU-236, SIU-322.

The network must be running the TCP/IP protocol.

If there is a firewall between the web server and the workstation, the firewall must allow:

- HTTP requests through port 80.
- HTTPS requests through port 443 (if SSL/TLS is being used).

The MyID installation program uses the bindings and ports for the website as specified in IIS. If a single binding exists, that protocol and port is used. If multiple bindings exist for a website, a port is selected in the following priority:

- Port 80
- Port 443
- The lowest numeric value in the list

Note: If you have CRL checks enabled, and your PowerShell scripts are required to be signed, you must make sure that you have Internet access to allow the server to check the CRL for the signed scripts. If you cannot enable Internet access, server performance will be impacted; you may want to disable CRL checks in this case.

4.4.1 ADO and MSADC requirements on the application server

SIU references: SIU-246, SIU-247.

The MyID application server requires ADO and MSADC to be operational to allow database connectivity. Make sure you do not remove or disable these components on your application server.

4.4.2 NetBIOS computer names

You must make sure that the NetBIOS names of the MyID servers conform to Microsoft's requirements, including allowed characters and length; NetBIOS computer names must contain between 1 and 15 characters. See your Microsoft documentation for details.

4.5 Configuring your domain and directory

SIU references: SIU-031, SIU-032, SIU-269.

Your MyID servers should be in a domain, so that trust can be established between each of the system components.

MyID is preconfigured to operate with Microsoft Active Directory Domain Services. You can integrate other LDAPv3-compliant LDAP directory providers with MyID; this requires additional configuration of MyID. For information on custom LDAP mappings and search filters, contact customer support quoting reference SUP-223.

Note: You must make sure that the following services are running:

- NTDS
- ADWS

4.5.1 Unique SIDs

SIU reference: SIU-200.

You must make sure that every computer on the domain has a unique SID (Security Identifier).

4.6 Setting up the database

This section contains information about setting up your database.

4.6.1 Database versions

SIU references: SIU-009, SIU-010, SIU-279.

MyID has been tested with the following SQL Server versions:

- SQL Server 2022 – CU13 (16.0.4125.3 – May 2024)
- SQL Server 2019 – CU27 (15.0.4375.4 – June 2024)
- SQL Server 2017 – CU31 (14.0.3456.2 – September 2022)

Note: Intercede supports the database versions listed above. If you are going to use different service packs or cumulative updates for these major versions than those listed above, make sure that you carry out additional testing within your environment. For production deployment, SQL Server Enterprise or Standard editions must be used. Do not use major versions that are not listed above (for example, SQL Server 2012) as these are not supported.

If you have multiple MyID application servers, you must have a Client Access License for SQL Server for each MyID application server.

MyID has also been tested using the following databases:

- Microsoft Azure.

  See the ***Microsoft Azure Integration Guide*** for details.
- Amazon RDS for SQL Server.

  See the ***Amazon Web Services Integration Guide*** for details.

4.6.2 Database configuration considerations

SIU references: SIU-097, SIU-098, SIU-126.

If you are creating the MyID database using the installation program, and have selected the Windows authentication option, make sure the account you use to install the software has the correct permissions to create a database on your SQL Server.

If you are using SQL Server authentication, make sure the accounts you specify for the main MyID database and the authentication database have the appropriate permissions on your SQL Server, and that you have created your databases before installing MyID; see section *4.6.6, Configuring SQL Server for SQL Authentication*.

If you are installing MyID into an already-created database (for example, when upgrading an existing system, or installing a new system where your DBA has already created an empty database), you do not need user permissions to create a database; however, you do need permissions to alter the schema. This means that you can remove the `sysadmin` permission

from the installation user, as long as you make sure that the user has database-level `db_owner` permission instead. See section *6.1.1*, *Installation account* for more information about permissions and default schema settings for existing databases.

Note: The SIU test SIU-097 queries the database to ensure that the installation user has the correct permissions. For this to happen, the user running the installation must have either the `sysadmin` role or the `securityadmin` role in SQL Server. If not, the test displays a warning.

Make sure your SQL Server is using English (United States) as the language. MyID supports only English (United States) for the connection to SQL Server. You can view the language used in SQL Server Management Studio – right-click the database, then select **Properties** from the pop-up menu.

See your Microsoft SQL Server documentation for further details.

- **IKB-295 – Database failures may occur when SQL Server user accounts do not use US English as the default language**

  A problem has been identified that causes failure to log on to MyID with the startup user account after first installation of, and subsequent problems to occur with the installation on dates where the day and month components cannot be reversed (for example, day/month 13/12).

  This has been seen to occur when using Windows Server 2019 and SQL Server user accounts created by the MyID installer that have been created with a default language of British English (date format `dmy`).

  To check the user account setting in SQL Server, run the following SQL query when logged in as the MyID Application user:

  ```
  DBCC USEROPTIONS
  ```

  See the Microsoft documentation for details:

  docs.microsoft.com/en-us/sql/t-sql/database-console-commands/dbcc-useroptions-transact-sql?view=sql-server-ver15

  The problem will occur when the `dateformat` value returned by this query is not `mdy`.

  Symptoms may include:

  - Failure to logon after first installation.
  - Failure to carry out certificate operations.

  In these cases, the following entries may be recorded in the `LogEvents` table of the MyID database:

  - `DAL std::exception catch handler Function : Update, catch hander. Error : SQL Error: 01000`
  - `An error occurred inside CBOL_AuthenticationWeb::LogonEx Error: 0x8004600c IDispatch error #24076 An error occurred inside CCommandContext::SetComplete Error: 0x8004600c IDispatch error #24076 AuditCollection - error Commiting Audit Rows In object BOLContext.AuditCollection.1 In object BOLContext.CommandContext.1`

To correct the problem, modify the default language of the MyID COM+ account in SQL Server:

1. Open SQL Server Management Studio as an administrative user
2. Open **Security > Logins**.

   Note: Open the **Security** folder at the top level for the server, not the folder under the MyID database.
3. Right-click, then from the pop-up menu select **New Login**.

   Alternatively, if the login for the MyID COM+ user already exists, double-click the login.
4. Make sure **Windows authentication** is selected, then click **Search** to select the MyID COM+ user account.
5. From the **Default language** drop-down list, select `us_english`.
6. Click **OK**.

If you continue to experience problems after correcting this issue, contact Intercede customer support quoting reference IKB-295.

4.6.3 Installing the database software

SIU references: SIU-092, SIU-093, SIU-096, SIU-296.

To install the database software:

1. Install the following SQL Server packages on the MyID database server:
   - **Database Engine Services.**

     Note: You must install the SQL Server Full Text Search option. To confirm whether Full Text Search is installed, you can run the following query:

     ```
     SELECT FULLTEXTSERVICEPROPERTY('IsFullTextInstalled')
     ```

     If this query returns `1`, Full Text Search is installed. If this returns `0`, you must add the feature before attempting to install MyID.

     Note: Under some circumstances, for example when setting up mirroring, the Full Text Search may stop indexing. See your Microsoft documentation for information on re-indexing the database.
   - **Client Tools Connectivity.**
2. On the MyID application server, install the following:
   - Microsoft OLE DB Driver 19 for SQL Server (MSOLEDBSQL).

     This driver is available from Microsoft.

     Important: From MyID 12.6, you must have the Microsoft OLE DB Driver 19 for SQL Server (MSOLEDBSQL) installed. Previous versions of MyID from MyID 11.0 required Microsoft OLE DB Driver 18 for SQL Server; these versions are not compatible with each other. You must upgrade to Microsoft OLE DB Driver 19 for SQL Server before installing MyID. For more information about supported versions of the Microsoft OLE DB Driver, contact customer support quoting reference SUP-324.

     Note: You must install the Microsoft Visual C++ Redistributable before installing the Microsoft OLE DB Driver 19 for SQL Server.

- SQL Server Native Client 11

  This is available in the SQL Server Feature Pack.

You must also make sure that the OLE DB Driver and Native Client are installed on the PC on which you run the database component of the installation program. For simplicity, you can run the database component of the installation program from the MyID application server.

If you are using the standalone authentication service (web.oauth2.ext) you must make sure that the OLE DB Driver and Native Client are installed on the server onto which you want to install this service.

Note: Install only one instance of the MyID database. You can choose to install the database from the database server or the application server, but do not run the installation from both.

4.6.4 SQL Server services

SIU references: SIU-153, SIU-219, SIU-220, SIU-221, SIU-222.

You must make sure that the following SQL Server services are installed and running on the MyID database server:

- SQLBrowser
- MSSQLSERVER
- MSSQLFDLauncher
- SQLSERVERAGENT

These services are part of an installation of SQL Server.

4.6.5 Running SIU tests against the database

SIU reference: SIU-022

You must have the SqlServer PowerShell module installed on the server from which the database is installed. This module is required to run the SIU tests against the database. If the SqlServer module is not installed, but the SQLPS module is installed, the tests can still run, but as this module is no longer maintained, test SIU-022 displays a warning.

Note: If you are using the SQLPS module, you must make sure that the module is trusted; alternatively, you can run the MyID Installation Assistant from a Windows PowerShell command window to give you the opportunity to run the untrusted module. However, you are recommended to use the SqlServer PowerShell module instead.

4.6.6 Configuring SQL Server for SQL Authentication

If you intend to use SQL authentication rather than Windows authentication to secure the connection to the MyID database, before you begin the MyID installation, you must have:

- Already-created databases to be populated during the installation.

  You must create a database for the main MyID installation, and an additional database for the MyID authentication database. If you are using a separate archive database, you must also create a database for that purpose.

- You must create two logins that can create schema objects:
  - The MyID user – used to control the main MyID database. Also requires permissions to the authentication database.
  - MyID authentication user – used to control the authentication database. Also requires read-only permissions to the main MyID database.

  These logins must have the following permissions on each database:
  - MyID user on the MyID database:
    - `db_datareader` – required for reading data.
    - `db_datawriter` – required for writing data.
    - `db_owner` – required for creating schema objects; for example, temporary tables created by stored procedures.
  - MyID user on the authentication database:
    - `db_datareader` – required for reading data.
    - `db_datawriter` – required for writing data.
    - `db_owner` – required for creating schema objects; for example, temporary tables created by stored procedures.
  - MyID Authentication user on the MyID database:
    - `db_datareader` – required for reading data.
  - MyID Authentication user on the authentication database:
    - `db_datareader` – required for reading data.
    - `db_datawriter` – required for writing data.
    - `db_owner` – required for creating schema objects; for example, temporary tables created by stored procedures.

Note: If you are using Microsoft Azure or Amazon RDS for SQL Server as your database, you *must* use SQL Authentication; you cannot use Windows authentication.

4.6.7 Database installation scripts

You may want to review the scripts used to install the MyID database for troubleshooting purposes. Your Database Administrator may also want to evaluate the database scripts before allowing you to run them on your database.

A copy of the scripts is available in the product installation image in the following location:

```
\Support Tools\Database Scripts\
```

The `Core_Database.zip` archive contains the scripts used to create the MyID database.

The `PIV_Database.zip` archive contains additional scripts that are used to configure your database for the PIV edition of MyID.

Each folder contains multiple individual scripts within that category. When the installation process runs these scripts, it first combines them into a single script for each category; for example, the `Devices` folder contains individual scripts for each type of device, and a combined `devices.sql` script. If you experience an issue when running the installation process, any script line numbers that appear in the log refer to this combined script.

Note: These installation scripts are provided to assist with troubleshooting an installation; do not attempt to use them to install the database, as this is not a supported mechanism for a product installation. Use the MyID Installation Assistant instead.

4.7 Restarting your servers

SIU reference: SIU-099.

Before you begin the MyID installation process, you are recommended to restart your servers to ensure that there are no pending updates that may interfere with the MyID installation.

The MyID Installation Assistant checks whether your server requires a restart as part of the Initial Server Check; see section *2.16*, *Initial server check results*.

5 Additional hardware and software requirements

The hardware and software described in this section are the minimum required for MyID. If your system does not match or exceed the requirements outlined in this section, contact Intercede for advice, quoting reference SUP-297.

This section contains details of the hardware and software requirements for client workstations, peripherals such as card readers, and external systems such as certificate authorities and hardware security modules.

5.1 Deployment considerations

Before starting to install MyID, you need to consider the way in which you intend to deploy it and the third party products that you want to integrate with it.

Warning: If you are upgrading an existing installation of MyID, you must back up your database and any files you have modified before starting.

5.1.1 Deployment strategy

MyID consists of three major components: the web server, the MyID application server and the database server. These can all be installed on a single physical machine or can be distributed across two, three or more machines.

The strategy you select will influence the hardware you require.

5.1.2 Databases

Supported databases are listed in section *4.6.1*, *Database versions*.

5.1.3 Integration with other products

Warning: Many products have to be installed and configured before installing MyID. Further configuration may then be required to enable them to work with MyID. The individual integration guides provide details.

Identify the products that you will be using with MyID. For example, you may want to use a specific directory, a Certificate Authority and smart cards from various vendors.

Integration Guides are provided for those products that have been tested with MyID. Locate those for the products you will be using and check for any special requirements.

5.1.3.1 Directory services

Although MyID can be operated without an LDAP directory present, most installations will include one. All MyID communication with the directory uses the standard LDAP protocol.

5.1.3.2 Certificate authority

If you intend to use MyID with a PKI Certificate Authority, your chosen CA must be installed and operational before installing MyID.

Read the Integration Guide relating to your CA before installing MyID, so that you have the various files, certificates and settings ready.

5.2 Client workstation

This section contains information about the requirements for MyID Desktop, the MyID Client Service, the Self-Service App, and the Self-Service Kiosk.

For information about the MyID Client for Mac, see the *System requirements* section in the ***MyID Client for Mac*** guide.

For information about the MyID Client for Windows, see the *System requirements* section in the ***MyID Client for Windows*** guide.

5.2.1 Hardware requirements

SIU references: SIU-011, SIU-012, SIU-013, SIU-014, SIU-015, SIU-016, SIU-017.

Note: These are the minimum requirements for MyID, excluding operating system, third party software, dependencies or drivers.

- Processor: 1 GHz
- RAM: 2 GB
- Display resolution: Minimum width 1280, minimum height 768.

  Note: If you are using administrative workflows such as the **Card Layout Editor** and **Edit Roles**, you may find it useful to use a higher resolution.
- Hard disk space: 2 GB
- If you are using smart cards, you need a smart card reader and drivers (see section *5.9.1*, *Card readers*)

5.2.2 Operating systems

SIU reference: SIU-018.

MyID supports the following client operating systems:

- Windows 10 version 22H2*.
- Windows 11 version 22H2*.

*Previous versions of the operating systems listed are expected to be compatible with MyID, with a minimum of Windows 10 version 1809. If you require support for earlier versions of Windows 10, contact Intercede customer support for further information, quoting SUP-366.

Important: At the time of release of this version of MyID, many third party device and peripheral vendors have not yet updated their drivers or software to be validated for use on Windows 11. Windows 10 drivers are expected to work, but you must verify integration between MyID and any devices or peripherals. Where issues arise that are due to incompatible drivers or changes to supporting software provided by the vendor, further investigation or changes to MyID may be necessary, which may require an upgrade to a later MyID version.

5.2.3 .NET Framework

You must have .NET Framework 4.8 installed on each client PC on which you want to install MyID Desktop. MyID is developed and tested using .NET Framework 4.8; if you need to use a later version of the .NET framework, contact customer support quoting reference SUP-283.

5.2.4 .NET Core Desktop Runtime

For each client PC that is going to use the MyID Operator Client, download and install the .NET Core Desktop Runtime. See section *4.3*, *Installing .NET Framework and .NET Core* for details.

5.2.5 Internet Options

SIU references: SIU-019, SIU-020, SIU-021.

MyID no longer has dependencies on Internet Explorer; however, there are still some circumstances where Windows Internet Options configuration is still required for some features. See section *10.1*, *Configuring Internet Options* for details.

5.2.6 Microsoft WebView2 Runtime

You must have the Microsoft WebView2 Runtime installed on each client PC where you want to use HTML-based Terms and Conditions or mailing documents. This component allows the client software (MyID Client Service, MyID Desktop, Self-Service App, and Self-Service Kiosk) to display or print the HTML content.

The minimum version supported of the WebView2 Runtime is 109.0.1518.46; however, you are recommended to use the Evergreen installer, which allows Windows to keep the component up to date with the latest features and security updates.

See the Microsoft website for details and to obtain an installer:

- ***developer.microsoft.com/en-us/microsoft-edge/webview2/***

The Microsoft WebView2 Runtime is also required on the MyID application server if you want to use the MyID Document Uploader; see the ***MyID Document Uploader*** guide for more information.

5.3 Virtual environments and remote connections

If you want to deploy MyID on a virtualized server environment (for example, VMware, Microsoft Azure, or Amazon AWS), or make use of a virtualized desktop solution (for example, Citrix or Cisco) you must be aware of the following limitations:

- The MyID Operator Client, MyID Desktop, and the Self-Service App can be used over remote desktop connections for multiple concurrent users. Additional configuration is required for the MyID Operator Client; see or details.
- The Self-Service Kiosk is not supported over remote desktop connections.
- While Intercede will make best endeavors to support all customers, should any issue arise which can be shown to be due to a failing of the virtualized environment and not MyID itself (for example, failure of the virtual environment to connect to an HSM or smart card reader, or other connected peripheral or third party software) this will be deemed 'out of support' and it will be the customer's responsibility to address this issue.
- Support of the virtual environment itself is not covered by Intercede and must be provided from the virtual environment vendor.
- Intercede reserves the right to charge for investigation which shows an issue is due to the use of a virtualized deployment environment and not MyID itself.

5.4 Mobile devices

MyID provides credential issuance features on mobile operating systems, including iOS and Android.

See the *Supported devices* section in the ***Mobile Identity Management*** guide for details of the operating system versions and secure key stores supported.

5.5 Card printers

MyID has been tested with the following makes of printer:

- Fargo
- DataCard
- Magicard
- XID
- Zebra

For more information on printers, including model, driver, firmware, and operating system support, see the ***Printer Integration Guide***.

Card printers require a card reader to allow MyID to write data to the chip on the smart card. Make sure that the card reader used in the printer is compatible with the card type you want to use.

5.6 Image capture

MyID supports webcams for capturing user photographs and scanners for capturing documents.

5.6.1 Webcams

Image capture is supported on all browsers supported by the MyID Operator Client.

However, due to the large number of variations of camera model, operating system, and driver, we recommend that you test the required combination with MyID before purchasing items in bulk for production use. Environmental factors such as camera position and light levels may also affect the performance of webcams with MyID.

- **IKB-5 – Webcam compatibility issues**

  MyID has been tested with a number of webcams across different versions of Windows operating systems. While the cameras used have worked successfully with MyID, some issues have been found. Symptoms include:

  - Live view from camera not displayed in the Image Capture screen.
  - Microsoft LifeCam HD-3000 displays Green Screen on Image Capture.

  These issues cannot be reproduced consistently, and testing with vendor drivers and Microsoft drivers has produced inconsistent results.

  Therefore you must pay attention to testing the combination of webcam, operating system, and driver version before deploying in your production environment. You must also ensure that the cameras you are using have compatible drivers for later versions of Windows operating systems.

5.6.2 Scanning support

MyID supports scanners that use the standard WIA2 method. Scanning using the TWAIN standard is supported in the MyID Operator Client if you have the MyID TWAIN module installed; see the *Scanning documents* section in the ***MyID Operator Client*** guide for details.

5.6.3 Tested scanners

The current release has been tested with the following scanners and drivers:

- Canon CanoScan LiDE 210 – LiDE 210 Scanner Driver Ver. 17.0.4
- Canon CanoScan LiDE 220 – LiDE 220 Scanner Driver Ver. 20.4.0.19
- Epson Perfection V500 Photo – EPSON Scan 3.770
- Epson Workforce DS-1630 – EPSON Scan 1.0.1.0

5.6.4 Signature capture

MyID has been tested with the following signature capture device:

- Topaz SigLite® signature pad, model T-LB460-HSX-R.

Signature capture is supported in the MyID Operator Client from the **Edit PIV Applicant**, **Update PIV Applicant**, and **Initial PIV Enrollment** screens. See the *Capturing signatures* section in the ***MyID Operator Client*** guide for details

5.7 Certificate authorities

The following Certificate Authorities (CAs) are supported in this release of MyID:

- DigiCert ONE
- Entrust JASTK
- Entrust CA Gateway
- Entrust
- Microsoft Windows Server Certificate Services
- PrimeKey EJBCA
- Symantec
- UniCERT

See the integration guide for the relevant CA for full details of the versions supported and procedures for integrating the CA to your MyID installation:

- ***DigiCert ONE Integration Guide***
- ***Entrust JASTK CA Integration Guide***
- ***Entrust CA Gateway Integration Guide***
- ***Entrust CA Integration Guide***
- ***Microsoft Windows CA Integration Guide***
- ***PrimeKey EJBCA Integration Guide***
- ***Symantec (Digicert) Managed PKI Integration Guide***
- ***UniCERT Integration Guide***

Note: If you want to issue certificates to a cardholder, that cardholder needs a Distinguished Name (DN). This means either that the cardholder must have an account in an LDAP to which MyID has access, or that MyID is informed of the DN in another way.

5.7.1 Additional certificate authorities

MyID has supported a wider range of certificate authorities than the limited range included in this release, and in some cases CA vendors have created connectors for MyID.

These include:

- IdenTrust.
- Nexus.
- Exostar.
- GlobalSign.
- Microsoft Standalone Certificate Authority.

For the latest information regarding integration with certificate authorities, contact customer support, quoting reference SUP-88.

5.8 Hardware Security Modules

Hardware Security Modules (HSMs) provide cryptographic operations, such as the storage of sensitive key data, in a very secure fashion.

MyID supports the following HSMs:

- Entrust nShield Connect
- Entrust nShield Solo
- Thales Luna

See the following documents for details:

- ***Entrust nShield HSM Integration Guide***
- ***Thales Luna HSM Integration Guide***

5.9 Supported card readers and card types

5.9.1 Card readers

MyID supports PC/SC compatible smart card readers. For more details about particular models, see the ***Smart Card Integration Guide***.

5.9.2 Supported smart cards and tokens

For details of the smart card manufacturers, model numbers, and middleware versions supported, see the ***Smart Card Integration Guide***.

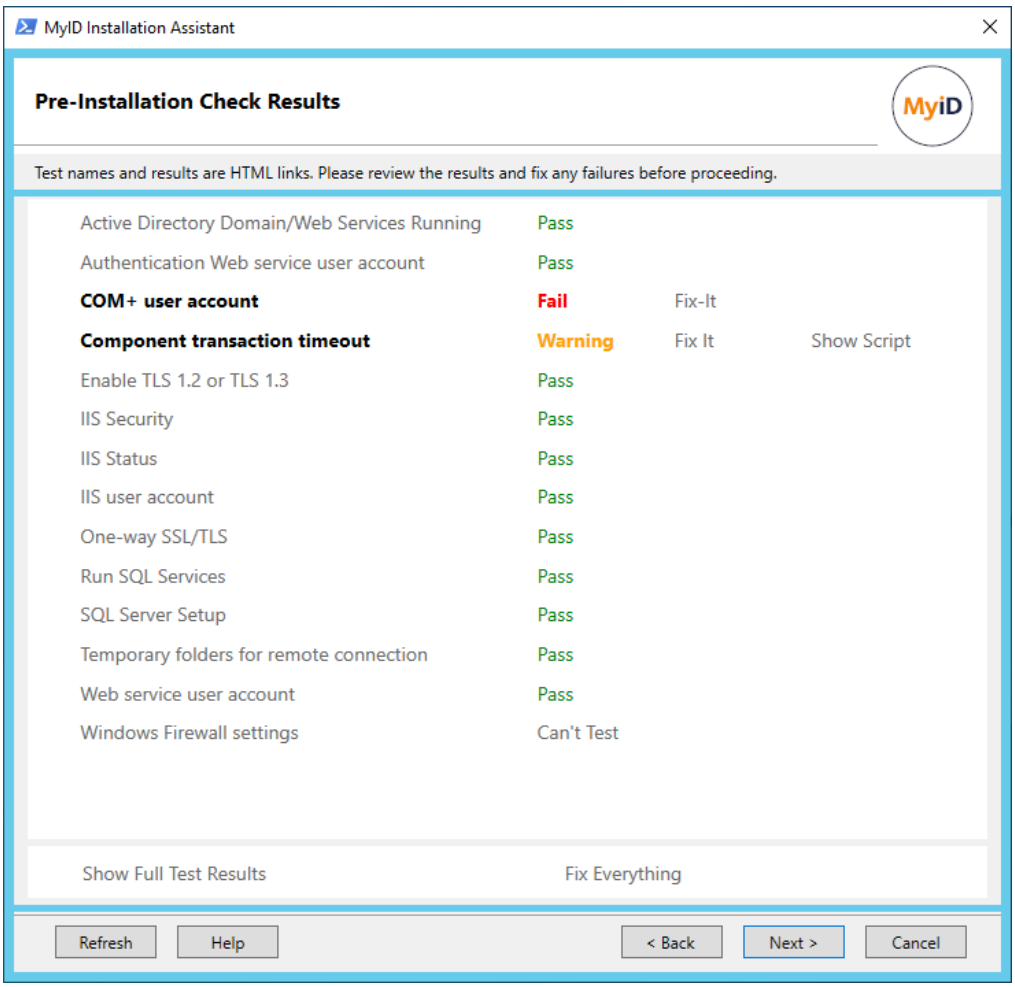
5.9.3 Virtual Smart Cards

MyID supports Microsoft Virtual Smart Cards.

See the ***Microsoft VSC Integration Guide*** for details.

6 Pre-installation configuration

When you run the MyID Installation Assistant, once you have provided the installation details (for example, the installation folder, the server URL, and the user accounts) it carries out an Pre-Installation Check to ensure that you the details you have entered are correct (for example, the user accounts have the appropriate permissions, and the MyID server URL has the appropriate security), and your servers are ready to start installing MyID; see section *2.18*, *Pre-installation check results*.



Note: The Pre-Installation Check also carries out some tests on configuration that is included as part of the initial server configuration; for example, for the initial server configuration you must install an appropriate version of SQL Server, and the pre-installation check ensures that the relevant SQL Server services are running correctly. See section *4*, *Initial server configuration* for details.

This chapter contains details of the pre-installation configuration that you must carry out:

- section *6.1*, *Setting up user accounts*.
- section *6.2*, *Launch and activation permissions*.
- section *6.3*, *Timeouts, limits and other settings*.
- section *6.4*, *Temporary folders for remote connections*.
- section *6.5*, *Setting up SSL/TLS*.
- section *6.6*, *World Wide Web Publishing Service*.

6.1 Setting up user accounts

For details of the procedures needed to set up your user accounts, see your Microsoft documentation.

Note: You are recommended to set up the MyID user accounts so that the passwords do not expire. If your organization's security policy does not allow this, you must make use of MyID's system for monitoring the expiry of system credentials; see the *Monitoring the expiry of system credentials* section in the ***Advanced Configuration Guide*** for details. If you need to change the password for the MyID user accounts, you can use the Password Change Tool; see the ***Password Change Tool*** guide for details.

6.1.1 Installation account

SIU references: SIU-040, SIU-041, SIU-042, SIU-043, SIU-044, SIU-217.

We recommend that your installation is carried out using a domain user that is part of the local Administrator group. This ensures the correct set-up and permissions for your installation.

The account must have the following properties:

- Must be a member of Domain Users.
- Must be a member of the local Administrators group on the application server.
- Must be a member of the local Administrators group on the web server.
- Must be a member of the local Administrators group on the database server, if you intend to carry out any installations directly on the database server, rather than remotely from the application server.
- If the database does not already exist, must have `sysadmin` privileges for their logon to SQL Server.

  This allows you to create databases and add the MyID COM and Authentication users as logins to SQL server.
- If the database *does* already exist (for example, when upgrading an existing MyID system, or installing a new system where your DBA has already created an empty database), and do not need to create any new databases or logins, you can omit the `sysadmin` permission as long as you ensure that the installation user has `db_owner` permissions on all MyID databases (including archive databases).

If the database already exists, the installation user must have the **Default Schema** set to `dbo` for the MyID database. If the default schema is set to something different, an error similar to the following may appear when running the installation program:

```
Error 27506. Error executing SQL script schema.sql. Line 2685. The default schema does not exist. (2797)
```

If you do not want to grant the installation user `sysadmin` privileges, you must also add the MyID COM+ and MyID Authentication users as logins to SQL Server manually.

If you add the MyID COM+ and MyID Authentication users manually, you must do so before running the installation process. The user accounts must have the following roles:

MyID COM+ user on the MyID database:

- `db_datareader`
- `db_datawriter`
- `public`

MyID COM+ user on the authentication database:

- `db_datareader`
- `db_datawriter`
- `public`

MyID Authentication user on the MyID database:

- `db_datareader`
- `public`

MyID Authentication user on the authentication database:

- `db_datareader`
- `db_datawriter`
- `public`

If these users do not exist with the above permissions, or the installation user does not have the `ALTER ANY LOGIN` permission to update SQL Server with the above permissions (as provided by the `sysadmin` privilege), the installation process will display errors, the eCertificate service will be unable to start, and you will be unable to run GenMaster.

You are recommended to use this account for performing all installation and maintenance procedures related to MyID, including subsequent patch installation.

Note: You are recommended to define the MyID user accounts under the organizational unit Service Accounts in the LDAP directory. Create the Service Accounts OU if it does not already exist. If you put the accounts in a different organizational unit, the System Interrogation Utility will be unable to detect the account.

6.1.2 MyID COM+ account

SIU references: SIU-045, SIU-046, SIU-047, SIU-048, SIU-049, SIU-050, SIU-051, SIU-276.

You must have the name and password of the account that will be used to run the MyID service. This information is required during the installation.

- Create the account before installing MyID.
- Set the password for the account so that it does not expire.
- You are recommended to define the user under the organizational unit Service Accounts in the LDAP directory. Create the Service Accounts OU if it does not already exist.
- Set the user as a member of the domain group Domain Users and the local group Distributed COM Users on the web, application, and database servers.
- The account should not be a member of the Domain Admins or the Enterprise Admins domain groups.
- Ensure the account is active (not disabled), unlocked, and does not expire.

Note: When you install MyID using the MyID Installation Assistant, these settings are checked on the Pre-Installation Check Results screen; if you need to change these settings, you can use the fix-it script provided on that screen. See section *2.18*, *Pre-installation check results* for details.

After creating the account, on the MyID application server:

1. Run the Local Security Policy application.
2. Under **Local Policies**, select **User Rights Assignment**.
3. Double-click **Log on as a service**.
4. Add the MyID COM+ user, then click **OK** to save the changes.

Note: When the MyID installation program sets the COM+ user as the COM+ identity for the MyID components, COM+ automatically adds the **Log on as a batch job** privilege. This privilege is required for the correct operation of COM+ components – make sure that the group policy does not remove the privilege.

6.1.3 IIS user account

SIU references: SIU-053, SIU-054, SIU-055, SIU-056, SIU-057, SIU-058, SIU-277.

You will need to enter the name and password of a valid IIS user account during the installation process.

- Create the account before installing MyID.
- You are recommended to define the user under the organizational unit Service Accounts in the LDAP directory. Create the Service Accounts OU if it does not already exist.
- Set the user as a member of the domain group Domain Users and the local group Distributed COM Users on the web, application, and database servers.
- The account should not be a member of the Domain Admins or the Enterprise Admins domain groups.
- Set the password for the account so that it does not expire.

- Ensure the account is active (not disabled), unlocked, and does not expire.
- If the `manualGroupMembership` setting in IIS (available in the Configuration Editor in IIS, in the `system.applicationHost/applicationPools/applicationPoolDefaults/processModel` section) is set to `True` (the default is `False`), you must add the user to the IIS_IUSRS group on both the domain and the local machine.

Note: When you install MyID using the MyID Installation Assistant, these settings are checked on the Pre-Installation Check Results screen; if you need to change these settings, you can use the fix-it script provided on that screen. See section *2.18*, *Pre-installation check results* for details.

After creating the account, on the MyID web server:

1. Run the Local Security Policy application.
2. Under **Local Policies**, select **User Rights Assignment**.
3. Double-click **Log on as a service**.
4. Add the MyID IIS user, then click **OK** to save the changes.

Note: The MyID IIS user account requires the **Log on as a batch job** privilege – make sure that the group policy does not remove the privilege.

6.1.4 Web service user account

SIU references: SIU-059, SIU-060, SIU-061, SIU-062, SIU-063, SIU-064, SIU-278.

You will need to enter the name and password of a valid user account to be used for the MyID web services during the installation process.

- Create the account before installing MyID.
- You are recommended to define the user under the organizational unit Service Accounts in the LDAP directory. Create the Service Accounts OU if it does not already exist.
- Set the user as a member of the domain group Domain Users and the local group Distributed COM Users on the web, application, and database servers.
- The account should not be a member of the Domain Admins or the Enterprise Admins domain groups.
- Set the password for the account so that it does not expire.
- Ensure the account is active (not disabled), unlocked, and does not expire.
- If the `manualGroupMembership` setting in IIS (available in the Configuration Editor in IIS, in the `system.applicationHost/applicationPools/applicationPoolDefaults/processModel` section) is set to `True` (the default is `False`), you must add the user to the IIS_IUSRS group on both the domain and the local machine.

Note: When you install MyID using the MyID Installation Assistant, these settings are checked on the Pre-Installation Check Results screen; if you need to change these settings, you can use the fix-it script provided on that screen. See section *2.18*, *Pre-installation check results* for details.

After creating the account, on the MyID web services server:

1. Run the Local Security Policy application.
2. Under **Local Policies**, select **User Rights Assignment**.
3. Double-click **Log on as a service**.
4. Add the MyID web service user, then click **OK** to save the changes.

Note: The web service user account requires the **Log on as a batch job** privilege – make sure that the group policy does not remove the privilege.

6.1.5 MyID Authentication account

SIU references: SIU-310, SIU-311, SIU-312, SIU-313, SIU-314, SIU-315, SIU-316.

You must have the name and password of the account that will be used to access the authentication database and access the authentication web service app pool. This information is required during the installation.

- Create the account before installing MyID.
- Set the password for the account so that it does not expire.
- You are recommended to define the user under the organizational unit Service Accounts in the LDAP directory. Create the Service Accounts OU if it does not already exist.
- Set the user as a member of the domain group Domain Users and the local group Distributed COM Users on the web, application, and database servers.
- Ensure the account is active (not disabled), unlocked, and does not expire.
- If the `manualGroupMembership` setting in IIS (available in the Configuration Editor in IIS, in the `system.applicationHost/applicationPools/applicationPoolDefaults/processModel` section) is set to `True` (the default is `False`), you must add the user to the IIS_IUSRS group on both the domain and the local machine.

Note: When you install MyID using the MyID Installation Assistant, these settings are checked on the Pre-Installation Check Results screen; if you need to change these settings, you can use the fix-it script provided on that screen. See section *2.18*, *Pre-installation check results* for details.

After creating the account, on the server running the MyID authentication web service:

1. Run the Local Security Policy application.
2. Under **Local Policies**, select **User Rights Assignment**.
3. Double-click **Log on as a service**.
4. Add the MyID authentication user, then click **OK** to save the changes.

6.1.6 SQL Server account

If you are using SQL Authentication, you set up logins with the appropriate permissions in SQL Server before installing MyID. See section *4.6.6*, *Configuring SQL Server for SQL Authentication* for details..

6.2 Launch and activation permissions

SIU references: SIU-065, SIU-067, SIU-071, SIU-075.

You must grant additional permissions to the account used to run MyID. The procedure you follow depends on whether you are going to install the MyID web server software on the same machine as the MyID application server software.

6.2.1 Web server on the same machine as the application server

On the server holding the MyID components (the application server) add the MyID COM+ user account to the Distributed COM Users group on the local machine, then give this group Local Launch, Remote Launch, Local Activation and Remote Activation rights.

1. In the Windows Computer Management tool, expand **System Tools > Local Users and Groups**, then select **Groups**.
2. Right-click the **Distributed COM Users** group and select **Properties** from the menu.
3. The Distributed COM Users Properties dialog is displayed.
   a. Click **Add**.
   b. Find and select the MyID COM+ account.
   c. Click **OK** in the Distributed COM Users Properties dialog.
4. Browse to and open **Component Services**.
   This is in the **Administrative Tools** section of Control Panel.
5. Expand the **Component Services** tree until you can see **My Computer**.
6. Right-click **My Computer** and select **Properties** from the menu.
7. The My Computer Properties dialog is displayed.
   a. Click the **COM Security** tab.
   b. In the **Launch and Activation Permissions** group, click the **Edit Default** button.
   c. Add the **Distributed COM Users** group.
   d. Make sure that the **Allow** options for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation** are selected.

Note: If you do not set these permissions, logon to MyID fails with an error message such as:

```
Unable to perform the requested operation
Solutions:
A problem occurred attempting to process your selection.
Please contact your administrator
```

6.2.2 Web server on a separate machine

If the web server and the MyID application server are installed on different machines, then the MyID IIS account also requires COM Security permissions.

Note: The steps in this section must be followed on both the MyID application server and the web server.

This is done by first adding the IIS, COM, and web service users to the Distributed COM Users group on the local machine and then giving this group Local Launch, Remote Launch, Local Activation and Remote Activation rights.

1. In the Windows Computer Management tool, expand **System Tools > Local Users and Groups**, then select **Groups**.
2. Right-click the **Distributed COM Users** group and select **Properties** from the menu.
3. The Distributed COM Users Properties dialog is displayed.
   a. Click **Add**.
   b. Find and select the MyID IIS account. Click **OK**.
   c. Next, add the MyID COM+ account.
   d. Next, add the MyID web service account.
   e. Click **OK** in the Distributed COM Users Properties dialog.
4. Browse to and open **Component Services**.
   This is in the **Administrative Tools** section of Control Panel.
5. Expand the **Component Services** tree until you can see **My Computer**.
6. Right-click **My Computer** and select **Properties** from the menu.
7. The My Computer Properties dialog is displayed.
   a. Click the **COM Security** tab.
   b. In the **Launch and Activation Permissions** group, click the **Edit Default** button.
   c. Add the **Distributed COM Users** group.
   d. Make sure that the **Allow** options for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation** are selected.

Note: If you do not set these permissions, the following message is displayed when attempting to launch MyID:

```
Unable to perform the requested operation
```

6.3 Timeouts, limits and other settings

6.3.1 Component transaction timeout

SIU reference: SIU-082.

As some operations (for example, PACS operations, Entrust templates, and so on) may take a significant amount of time to complete, you may want to increase the COM+ transaction timeout on the MyID application server.

Note: When you install MyID using the MyID Installation Assistant, these settings are checked on the Pre-Installation Check Results screen; if you need to change these settings, you can use the fix-it script provided on that screen. See section *2.18*, *Pre-installation check results* for details.

To increase the transaction timeout:

1. Start the Windows Component Services.
2. Expand **Component Services** and **Computers**.
3. Right-click on **My Computer**, and click **Properties**.
4. Click the **Options** tab.
5. In the **Transaction Timeout** box, type a number of seconds for the timeout value.

   For example, set the transaction timeout to `180`.
6. Click **OK**.

6.3.2 Windows Firewall settings

SIU references: SIU-085, SIU-086, SIU-260.

The Distributed Transaction Coordinator must be allowed access through the firewall on the web server, application server and database server.

Note: When you install MyID using the MyID Installation Assistant, these settings are checked on the Pre-Installation Check Results screen; see section *2.18*, *Pre-installation check results* for details.

To allow access through the firewall:

1. From the Control Panel, open the Windows Firewall.
2. Select **Allow an app or feature through Windows Firewall**.
3. Make sure the entry for **Distributed Transaction Coordinator** is selected for **Domain** networks.
4. Click **OK** to return to the main screen.
5. Click the **Turn Windows Firewall on or off** option.
6. Make sure the **Block all incoming connections, including those in the list of allowed apps** option is not selected.
7. Click **OK**.

6.3.3 ISA Server connection limit

If you are using Microsoft Internet Security and Acceleration Server (ISA Server), you may experience issues if the connection limit for ISA Server is set too low. The problem may appear with the following symptoms:

- Users lose connection to the MyID server.
- System Event log contains messages similar to:

```
Violation of PRIMARY KEY constraint 'PK_Logons'. Cannot insert
duplicate key in object 'dbo.Logons'.
```

- The `HTTPErr.log` in the Windows `System32\logfiles\HttpErr` folder contains client connections from a limited set of addresses with the comment `Timer_ConnectionIdle`.
- HTTP 500 error messages appearing to clients.

You are recommended to increase the connection limit for the MyID web server.

For example, to set the limit in ISA Server 2004:

1. In the ISA Server Management utility, open the connection limits screen:
   - For ISA Server 2004 Enterprise Edition:

     Expand **Microsoft Internet Security and Acceleration Server 2004 > Arrays > Array_Name > Configuration**, then click **General**.
   - For ISA Server 2004 Standard edition:

     Expand **Internet Security and Acceleration Server 2004 > Server_Name > Configuration**, then click **General**.
2. In the details pane, click **Define Connection Limits**.
3. In the **Custom connection limit** box, type a large number; for example, `1000000`.
4. Click the **Add** button to add the IP address of the MyID web server to the **Apply the custom limit to these IP addresses** list.
5. Click **OK**.

For information on setting the connection limit in other versions of ISA Server or Forefront Threat Management Gateway, see your Microsoft documentation.

6.3.4 Post-installation IIS server caching

After you have installed MyID, you must set up your IIS server caching. See section *11.1*, *IIS server caching* for details.

6.3.5 Shutting down COM+ components

If you attempt to shut down COM+ components manually, you may experience problems, with a message similar to:

```
An error occurred while processing the last operation.
Error code 80004002 - No such interface supported.
```

To prevent this from occurring, you can disable the related Windows User Profile Service feature.

1. On the MyID application server, open the Group Policy editor (`gpedit.msc`).
2. Open **Local Computer Policy > Computer Configuration > Administrative Templates > System > User Profiles**.
3. Set the **Do not forcefully unload the user registry at user logoff** option to **Enabled**.

For more information about this option, see the Microsoft documentation.

6.4 Temporary folders for remote connections

SIU reference: SIU-091.

If you are installing over a remote connection, you must set up your system not to use temporary folders per session before installing MyID.

Note: When you install MyID using the MyID Installation Assistant, these settings are checked on the Pre-Installation Check Results screen; if you need to change these settings, you can use the fix-it script provided on that screen. See section *2.18*, *Pre-installation check results* for details.

To set the temporary folder options:

1. Open the Local Group Policy Editor (gpedit.msc).
2. Expand **Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Temporary folders**
3. Set the **Do not use temporary folders per session** option to **Enabled**.

   You may have to disconnect and reconnect, or restart the server, for this setting to take effect. To find out if the setting is correct, in Windows Explorer, type the following in the address bar, and press Enter:

   ```
   %temp%
   ```

   If this resolves to a path similar to:

   ```
   C:\Users\myapp\AppData\Local\Temp\
   ```

   rather than a path with a number on the end, similar to:

   ```
   C:\Users\myapp\AppData\Local\Temp\1
   ```

   the setting has taken effect correctly. If the path has a number at the end (for example, `/1`), you must reconnect your remote session or restart the server before you start to install MyID.

6.5 Setting up SSL/TLS

SIU references: SIU-251, SIU-274.

For production systems, you are strongly recommended to set up SSL/TLS on all MyID websites and web services. See the *Configuring SSL/TLS (HTTPS)* section in the ***Securing Websites and Web Services*** guide and the *MyID website* section in the ***System Security Checklist***.

The MyID Installation Assistant can help you with the process of securing your web servers. See section *2.9*, *Configuring https* for details.

6.5.1 SSL/TLS for the MyID Operator Client

Important: The web services used by the MyID Operator Client (`rest.core` and `web.oauth2`) require SSL/TLS; if you do not connect through HTTPS, you cannot use the MyID Operator Client. For information on setting this up, see the *Configuring SSL/TLS (HTTPS)* section in the ***Securing Websites and Web Services*** document.

When you install MyID, you must specify the **MyID Server URL**. This must match the URL of the server as accessed by client PCs using the MyID Operator Client, which must in turn match the server name used in the SSL/TLS certificate. The default value provided by the installation program is the fully-qualified domain name of your server, but this may not match the URL used by your clients; for example, you may use a domain name such as `myid.example.com` that is mapped to the web server rather than an internal address.

6.5.2 SSL/TLS for MyID Desktop

For information on configuring MyID Desktop for SSL/TLS, see section *10.3.4*, *One-way SSL/TLS* and section *10.3.5*, *Two-way SSL/TLS*.

6.5.3 Securing MyID with TLS 1.2 or TLS 1.3

SIU reference: SIU-297.

You are recommended to set up your system to use TLS 1.2 or TLS 1.3; this involves configuring the MyID application servers to ensure that they can use TLS 1.2 or TLS 1.3, and configuring the MyID web servers to disable SSL and versions of TLS earlier than TLS 1.2.

For more information, see the *Securing MyID with TLS 1.2 and TLS 1.3* section in the ***System Security Checklist***.

6.6 World Wide Web Publishing Service

SIU reference: SIU-150, SIU-258.

You must make sure that the World Wide Web Publishing Service (W3SVC) is installed and running on the MyID web server. This service is part of IIS.

7 Upgrading MyID

This chapter contains important information on upgrading your MyID system. The upgrade procedure you must carry out depends on what version of MyID you are upgrading.

7.1 Before you upgrade

Note: Before you upgrade your MyID system to the current version of MyID, contact Intercede customer support quoting reference SUP-300 for advice on upgrading your particular configuration; this is essential if your system contains any customizations, or if you are upgrading from a system earlier than version 8.0.

Check section *5*, *Additional hardware and software requirements* to make sure that your system supports the latest version of MyID, and section *6*, *Pre-installation configuration* to make sure that your system has been configured correctly. The MyID Installation Assistant automatically checks that your system meets these requirements; alternatively, you can use the System Interrogation Tool to confirm that your system meets the requirements for the current version of MyID – see the ***System Interrogation Utility*** guide for details.

Make sure that your client workstations are correctly configured; see section *5.2*, *Client workstation*. For example, make sure that the MyID website has not been added to the list of compatibility view sites on any of your client PCs.

MyID 10.7 introduced the requirement to have the SQL Server Full Text Search option installed on your database server.

MyID 10.7 also introduced the web service user account. If you are upgrading a MyID 10.6 or earlier system, you must create this user before you run the installation program; see section *6.1.4*, *Web service user account* for details.

MyID 11.0 introduced the requirement for the MyID COM+ user account, the IIS user account, and the web service user account to have **Log on as a service** rights – if you are upgrading, you must make sure that your accounts have the correct permissions; see section *6.1*, *Setting up user accounts* for details.

Make sure that you complete any outstanding activation jobs before upgrading your system – if you request a card, upgrade MyID, then attempt to activate the card, you may experience problems due to the different requirements for activation between versions of MyID. For more information contact customer support quoting reference SUP-182.

MyID 12.0 introduced the authentication user account. If you are upgrading a MyID 11.8 or earlier system, you must create this user before you run the installation program; see section *6.1.5*, *MyID Authentication account* for details. If you are using SQL Authentication, you must also create an additional login to be used for the authentication database; see section *4.6.6*, *Configuring SQL Server for SQL Authentication*.

MyID 12.6 introduced the requirement to have the Microsoft OLE DB Driver 19 for SQL Server (MSOLEDBSQL) installed – see section *4.6*, *Setting up the database* for details. Previous versions of MyID from MyID 11.0 required Microsoft OLE DB Driver 18 for SQL Server; these versions are not compatible with each other. You must upgrade to Microsoft OLE DB Driver 19 for SQL Server before installing MyID. For more information about supported versions of the Microsoft OLE DB Driver, contact customer support quoting reference SUP-324.

MyID 12.6 also introduced the requirement to have the SqlServer PowerShell module installed on the server from which the database is installed; this is required by the MyID Installation Assistant to run database tests. See section *4.6.5*, *Running SIU tests against the database* for details.

MyID 12.9 updated the required version of .NET Core Hosting from 6.0 to 8.0. You must upgrade your servers and clients with the new version of .NET Core. See section *4.3.2*, *.NET Core Hosting* for details.

7.1.1 Selecting features when upgrading

In the MyID Installation Assistant, on the Select Roles and Features screen (see section *2.7*, *Selecting the server roles and features*) make sure that the list of features you want to install is correct. The MyID Installation Assistant interrogates the registry for details of the features that are already installed, but the registry does not contain details of every feature.

You may also want to install new features that were not available in your previous version of MyID.

If you do not have a record of the features installed on a server, you can run the installation program for the already-installed version of MyID and select the **Modify** option. The Server Roles and Features screen lists what you have installed.

Note: The options in this installation program do not correspond exactly to the options displayed in the MyID Installation Assistant; the MyID Installation Assistant displays a list of options that has been organized to make it clear which options are optional. In addition, the **Web Server** option in the **Modify** process incorporates both the **Web Server** and **Operator Client Web Services** options in the MyID Installation Assistant; this option has been split in the MyID Installation Assistant to allow for greater flexibility when installing MyID.

See section *8.4*, *Modifying the installation* for details of running the modify process.

7.1.2 Upgrading a split-tier system

If you are upgrading a system where the application server and web server are installed on different physical machines, you must upgrade the application server before you upgrade the web server; this allows you to upgrade the web server using the updated COM+ proxies from the application server.

7.1.3 Upgrading systems with edited appsettings.Production.json files

Important: The installation program may uninstall and reset the contents of any `appsettings.Production.json` files you have edited. You must back up any `appsettings.Production.json` files on your system and restore their settings after you have upgraded MyID.

7.1.4 Upgrading systems with custom configuration updates

If you have received an update from Intercede for your pre-MyID 12.0 system that applies custom configurations – for example `CONFIG-9999.1.0` – you must contact customer support quoting reference SUP-318 to receive an updated version of this configuration update.

7.1.5 Upgrading systems with custom LDAP mappings

If the MyID system you are upgrading has custom LDAP mappings, before you upgrade you must set a configuration option to prevent the installation program from overwriting your existing settings.

Note: Product upgrades may provide changes or enhancements to LDAP integration features that require changes to your LDAP mappings; if you set the **Custom LDAP Mappings** option, these updates are not applied. Contact Intercede support quoting SUP-227 for further guidance.

To retain your custom LDAP mappings while upgrading:

1. From the **Configuration** category, select **Operation Settings**.
2. On the **LDAP** tab, select the following:
   - **Custom LDAP Mappings** – set to `Yes`.
3. Click **Save changes**.

- **IKB-150 – Upgrading can reset LDAP mapping**

  If you are upgrading from a system earlier than MyID 10.7 that was connected to another LDAP directory type, the **Custom LDAP mappings** option will not be available, and configuration settings regarding attribute mapping may be reset to the Active Directory values.

  Specifically, if mappings have been removed as the directory does not have an equivalent field, these will be re-added with ADS values. Existing mappings that are modified should remain unchanged, and custom additional field mappings should not be removed.

  For more information on working around this issue, contact customer support, quoting reference IKB-150.

7.1.6 Upgrading systems with a web server outside the domain

If your system has been configured to use a web server outside the domain used for the rest of the MyID system, the custom configuration on the MyID application components presents some complications when upgrading. If your system meets this description, you are recommended to contact customer support quoting reference SUP-242.

7.1.7 Upgrading renewal jobs

If you are upgrading from a MyID 10.4 or earlier system, you are recommended to complete all outstanding renewal jobs before upgrading. If this is not possible, you can use the provided database scripts to cancel the existing jobs and then regenerate them.

The database scripts are provided in the MyID release in the following folder:

```
\Support Tools\Upgrade\Database Scripts\
```

To upgrade your renewal jobs:

1. Before upgrading, run the following script against the MyID database:

   ```
   db_CountPendingCertRenewals.sql
   ```

   This script informs you how many pending renewal jobs are in the MyID database.
2. Carry out the MyID upgrade.

3. After upgrading, run the following script against the MyID database:

   `db_RegeneratecCertRenewalJobs.sql`

   This script cancels the renewal jobs and regenerates them so that they can be processed.

7.1.8 Upgrading card issuance jobs

If you are upgrading from a MyID 8.0 or earlier system, you are recommended to complete all outstanding issuance jobs before upgrading.

You may find that the **Collect Card** workflow has the following issues with jobs that were created before you carried out the upgrade:

- Issuance jobs may not appear using the default filters.
- Issuance jobs will appear when removing the **Allowed Issuer** default filter.
- Listed issuance jobs will display a blank entry for the credential profile.
- Attempting to collect these jobs will present an error.

You can use the provided database script to upgrade these issuance jobs to the latest format.

The database script is provided in the MyID release in the following folder:

`\Support Tools\Upgrade\Database Scripts\`

To upgrade your issuance jobs:

1. After upgrading MyID, run the following script against the MyID database:

   `db_MigrateV8IssueCardJobs.sql`

   This script upgrades the issuance jobs so that you can collect them.

7.1.9 Upgrading systems with customized configuration files

If you have made any changes to configuration files, such as the `myid.config` file for the various MyID web services, you must back up these files before you start the upgrade process, and merge in the changes once you have completed the new installation.

Important: If you have updated the `EndWorkflowUrl` entry in the `myid.config` file for the MyIDProcessDriver web service to provide a specific server address instead of the `{0}` parameter, make sure that when you implement your changes again that you use the latest version of the configuration option as your basis for the substitution; in particular, MyID 12.8 introduces the use of `dest=/EndSession.asp` instead of `dest=/blank.html` in the configuration file, which is essential for signing out all aspects of the session when signing out from the MyID Operator Client. See the *Reverse proxies and load balancing* section in the ***Web Service Architecture*** guide for details of editing the `EndWorkflowUrl` entry in the `myid.config` file.

7.1.10 Upgrading systems with multiple databases

Your MyID system may have multiple databases; for example, a separate audit database, a separate audit archive database, or a binary objects database. You configure MyID to point to the appropriate database by configuring its `.udl` files; you are recommended to back up the MyID `.udl` files in the Windows `SysWOW64` folder (for 32-bit MyID before version 12.0.0) or `System32` folder (for 64-bit MyID from 12.0.0 on) before you upgrade MyID.

7.1.11 Upgrading systems with custom card layout images

If you have custom images that you use for card layouts (see the *Custom image fields* section in the ***Administration Guide***) you must back up these images before you upgrade, then copy them into the new `upimages` folder after you have completed the installation.

7.1.12 Upgrading systems that use the web server to store images

By default, MyID stores images in the database. If your system is configured to store images on the web server instead (see the *Storing images on the web server* section in the ***Operator's Guide***) you must back up your `upimages` folder before upgrading, then copy these files into the new `upimages` folder after you have completed the installation.

You must then set the **File Store Location** option (on the **Video** tab of the **Operation Settings** workflow) to point to this new location.

Note: You cannot use the MyID Operator Client to capture images if your system is configured to store images on the web server. To view images that are stored on the web server in the MyID Operator Client, you must carry out some additional configuration; see the *Displaying images stored on the web server* section in the ***MyID Operator Client*** guide.

7.1.13 Authentication user

The MyID Authentication user is a new user account introduced at MyID 12.0. If you are upgrading from an earlier version, you must set up this authentication user account before you run the installation program.

See section *6.1.5, MyID Authentication account* for details.

7.1.14 Authentication database

The authentication database is a new database introduced at MyID 12.0. This database is used to store authentication information, including details of audited authentication attempts. You can use this database for reporting; see the *Reporting on the authentication database* section in the ***MyID Authentication Guide*** for details.

If you are using SQL Authentication you must create an additional login for this database; see section *4.6.6, Configuring SQL Server for SQL Authentication* for details.

7.1.15 Upgrading systems with multiple instances of the Certificate Server service

If you are upgrading from a 32-bit version of MyID to a 64-bit version of MyID, and your system uses multiple instances of the MyID Certificate Server (eCertificateSrv) service, you must back up your registry before starting the upgrade, then set up your additional service instances again after installing MyID, using the 64-bit Program Files path. See the *Multiple Certificate Server Services* guide (available on request from Intercede customer support).

7.1.16 Upgrading systems with customized services

If you are upgrading from a 32-bit version of MyID to a 64-bit version of MyID, and your system has customizations applied to the services through the registry, you must back up your registry before starting the upgrade, then set up your customizations again after installing MyID.

7.1.17 Upgrading systems with customized banned word lists for PINs

If you have customized the list of banned words for user PINs, whether dynamic views in the database or the static word list file, you must take a backup of your banned word lists and re-apply them after the upgrade has completed.

See the *Enforcing banned words in PINs* section in the ***Administration Guide***.

7.1.18 Upgrading systems with customized card data models

If you have customized card data models, you must take a backup of your card data model files, and re-apply them after the upgrade has completed. Custom data model files are deleted by the upgrade process.

7.1.19 Upgrading systems with customized Self-Service Request Portal features

You can customize various aspects of the Self-Service Request Portal, including terminology, properties, and external identity providers. Make sure you back up all of your customizations before upgrading MyID, and reapply them if necessary once the upgrade has completed.

See the *Customizing the Self-Service Request Portal* and *External identity providers* sections in the ***Derived Credentials Self-Service Request Portal*** for details.

7.2 Running the upgrade installation

The recommended process for upgrading MyID depends on the version you are upgrading from:

- If you are upgrading from MyID 12, use the MyID Installation Assistant.

  See section *7.3*, *Upgrading from MyID 12.0 – 12.12*.

- If you are upgrading from MyID 11, use the MyID Installation Assistant, with additional configuration to handle the change from 32-bit software to 64-bit software.

  See section *7.4*, *Upgrading from MyID 11*.

- If you are upgrading from MyID 10 or earlier, use the upgrade migrate script to carry out the change from 32-bit software to 64-bit software. Use the MyID Installation Assistant only to install the new version of MyID; do not use it to handle the upgrade process.

  See section *7.5*, *Upgrading MyID from a 32-bit application to 64-bit*.

- If you are upgrading to a new server, you must transfer the database and export the registry.

  See section *7.6*, *Upgrading to a new server*.

Important: If you already have an installation of MyID that was carried out using the MyID Installation Assistant, you *must* prepare the installation folder before you start an upgrade or update process. See section *2.2.4*, *Upgrading or updating the MyID Installation Assistant*.

7.2.1 The importance of rebooting during the upgrade process

It is important that you follow the upgrade instructions closely. At various points in the upgrade process, you may be asked to reboot the MyID server; this is important to ensure that your server operating system is in a clean state. If the server has pending changes, this may affect the installation process, causing unexpected errors to occur.

For example, this situation may occur if your server has pending:

- Windows update activity.
- System file changes; for example, location, naming, permissions, or attributes.
- `.exe` modification.
- Component Services changes, including registry, COM+/DCOM.
- Security and deployment tasks, including System Center Configuration Management.

The most effective way to clear these issues is to reboot the server when instructed to by the upgrade process. If rebooting the server is not possible, you must take steps to ensure that there are no pending server changes before continuing with the upgrade process.

7.3 Upgrading from MyID 12.0 – 12.12

Important: Check that you have carried out all of the prerequisite actions before beginning the upgrade installation process. See section *7.1*, *Before you upgrade* for details.

If you are upgrading to a new server, you must transfer the database and export the registry; see section *7.6*, *Upgrading to a new server*.

Note: If you have customized JavaScript hooks in your installation, you must contact customer support quoting reference SUP-300 before you upgrade.

When you are upgrading an existing MyID 12.0 – 12.12 installation to the current version, you are recommended to use the MyID Installation Assistant.

1. Close all MyID clients.
2. Start up a single MyID client, log in to MyID, then log out again without accessing any workflows.

   This ensures that the task numbers are cleared from the database.
3. Back up the MyID registry on the application server.

   This is:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Intercede\`
4. Back up the MyID database and program folder.
5. Uninstall any MyID hotfixes you have applied.

   Note: It is important that you uninstall any hotfixes that have been installed *before* you install any update or upgrade. If you uninstall a hotfix *after* installing the update or upgrade, you may cause your system to experience errors or stop operating. See the *General bug fixes and improvements* section in the ***Release Notes*** for a list of the items that have been incorporated into the current release, if any; if you have been issued any *additional* items that are not incorporated in the release, you must uninstall them before installing the update, but then contact customer support quoting reference SUP-337 before attempting to re-apply them after installing the update.
6. On each client, you are recommended to uninstall the previous version of the MyID client software; for example, MyID Desktop, the MyID Client Service, the Self-Service App, the Self-Service Kiosk, or the BioPack client components.
7. Install or upgrade any pre-requisites for the components you are going to be using.

   See your integration guides for details.

Note: The configuration for your components may have changed for this version of MyID. Make sure you check the integration guides for the latest information.

8. Reboot the MyID server.

   Note: If you do not reboot the MyID server before running the installation program for the latest version, you may see an error similar to the following:

   ```
   Error 1303. The installer has insufficient privileges to access this directory: C:\Program Files\MyID\Components\Devices. The installation cannot continue.
   ```

   If you see this error, click **Cancel**, ignore any errors that appear, then reboot the server. Make sure that MyID is not installed, then attempt to run the installation program for the latest version again.

9. Run the MyID Installation Assistant.

   See section *2.27.1*, *Upgrading from a MyID 12 system*.

   Note: On a split deployment, upgrade the application server before you upgrade the web server.

10. Complete any required post-installation configuration changes to your system.

    See section *11*, *After installing MyID*.

11. On each client:

    a. Install the MyID client software; for example, MyID Desktop, the MyID Client Service, the Self-Service App, or the Self-Service Kiosk.

    b. Clear the browsing history in the Windows Internet Options dialog.

       Note: Make sure you deselect the **Preserve Favorites website data** option, if it is available.

    You are recommended to upgrade the client software on each client. New features of the server software may require the latest client software.

12. Review your security settings.

    For example, when you install MyID, the **Security Officer PIN Type** is set to **Random** rather than whatever it was set to previously – make sure that this suits the security requirements of your system.

    See the ***System Security Checklist*** for details.

13. Follow the instructions for configuring MyID after you complete the upgrade.

    See section *7.7*, *After you upgrade*.

7.4 Upgrading from MyID 11

From MyID 12.0.0, MyID Server is a 64-bit application. All previous versions of MyID were 32-bit, even when installed on 64-bit operating systems.

Accordingly, you cannot upgrade MyID from an earlier version to a 64-bit version by installing over the previous version; the file paths and registry settings have changed. You must back up your configuration, uninstall your previous version of MyID, retaining the database, install the 64-bit version, then restore your configuration to the 64-bit locations on the file system and in the registry.

The MyID Installation Assistant handles this process for you when you are upgrading from MyID 11.

If you are upgrading to a new server, you must transfer the database and export the registry; see section *7.6*, *Upgrading to a new server*.

Important: Check that you have carried out all of the prerequisite actions before beginning the upgrade installation process. See section *7.1*, *Before you upgrade* for details.

Note: If you have customized JavaScript hooks in your installation, you must contact customer support quoting reference SUP-300 before you upgrade.

To upgrade from MyID 11:

1. Close all MyID clients.
2. Start up a single MyID client, log in to MyID, then log out again without accessing any workflows.

   This ensures that the task numbers are cleared from the database.
3. Back up the MyID registry on the application server.

   This is:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Intercede\
   ```
4. Back up the MyID database and program folder.

   By default, the program folder is:

   ```
   C:\Program Files (x86)\Intercede\
   ```
5. Reboot the server.
6. On each client, you are recommended to uninstall the previous version of the MyID client software; for example, MyID Desktop, the Self-Service App, the Self-Service Kiosk, or the BioPack client components.
7. Install or upgrade any pre-requisites for the components you are going to be using.

   See your integration guides for details.

   Note: The configuration for your components may have changed for this version of MyID. Make sure you check the integration guides for the latest information.
8. Reboot the MyID server.

   Note: If you do not reboot the MyID server before running the installation program for the latest version, you may see an error similar to the following:

   ```
   Error 1303. The installer has insufficient privileges to access this
   directory: C:\Program Files\MyID\Components\Devices. The installation
   cannot continue.
   ```

   If you see this error, click **Cancel**, ignore any errors that appear, then reboot the server. Make sure that MyID is not installed, then attempt to run the installation program for the latest version again.
9. Run the MyID Installation Assistant.

   See section *2.27.2*, *Upgrading from a MyID 11 system* for details.

   Note: On a split deployment, upgrade the application server before you upgrade the web server.

10. Complete any required post-installation configuration changes to your system.

    See section *11*, *After installing MyID*.

11. Intercede may have provided you with an update to your system that you must install after running the main MyID installation program.

    See section *9*, *Updating MyID* for details.

12. If you have been provided with a configuration update for your system, install it.

13. Install the 64-bit versions of any modules you previously had installed.

14. On each client:

    a. Install the MyID client software; for example:

    - MyID Desktop
    - MyID Client Service for the MyID Operator Client
    - Self-Service App
    - Self-Service Kiosk

    b. Clear the browsing history in the Windows Internet Options dialog.

    Note: Make sure you deselect the **Preserve Favorites website data** option, if it is available.

    You are recommended to upgrade the client software on each client. New features of the server software may require the latest client software.

15. Review your security settings.

    For example, when you install MyID, the **Security Officer PIN Type** is set to **Random** rather than whatever it was set to previously – make sure that this suits the security requirements of your system.

    See the ***System Security Checklist*** for details.

16. Follow the instructions for configuring MyID after you complete the upgrade.

    See section *7.7*, *After you upgrade*.

7.5 Upgrading MyID from a 32-bit application to 64-bit

From MyID 12.0.0, MyID Server is a 64-bit application. All previous versions of MyID were 32-bit, even when installed on 64-bit operating systems.

Accordingly, you cannot upgrade MyID from an earlier version to a 64-bit version by installing over the previous version; the file paths and registry settings have changed. You must back up your configuration, uninstall your previous version of MyID, retaining the database, install the 64-bit version, then restore your configuration to the 64-bit locations on the file system and in the registry.

The MyID Installation Assistant handles this process for you when you are upgrading from MyID 11; see section *7.4*, *Upgrading from MyID 11*.

If you are upgrading from MyID 10 or earlier, Intercede has provided a utility that automates this process for you.

If you are upgrading to a new server, you must transfer the database and export the registry; see section *7.6*, *Upgrading to a new server*.

Important: Check that you have carried out all of the prerequisite actions before beginning the upgrade installation process. See section *7.1*, *Before you upgrade* for details.

Note: If you have customized JavaScript hooks in your installation, you must contact customer support quoting reference SUP-300 before you upgrade.

To upgrade from MyID 10 or earlier:

1. Take a copy of the list of the updates that have been applied to your system from the **Installation History** tab of the **System Status** report within MyID.
2. Close all MyID clients.
3. Start up a single MyID client, log in to MyID, then log out again without accessing any workflows.

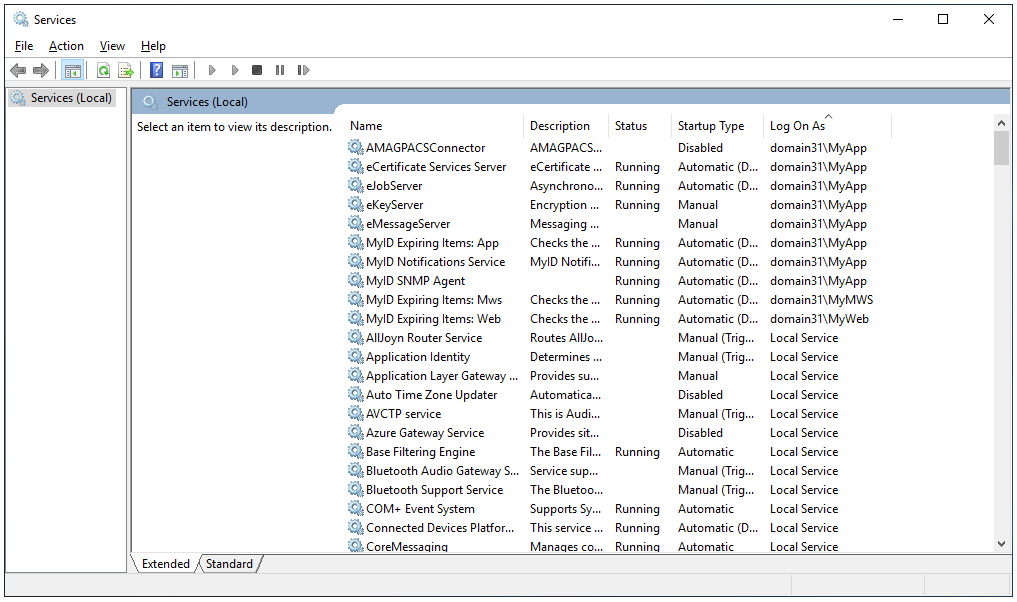
   This ensures that the task numbers are cleared from the database.
4. Back up the MyID registry on the MyID servers.

   This is:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Intercede\`
5. Back up the MyID database and program folder.

   By default, the program folder is:

   `C:\Program Files (x86)\Intercede\`
6. Reboot the server.
7. Shut down all active MyID services.
   a. In the Windows Services tool, locate each service running under one of the MyID accounts.



   Note: You can sort the list of services by clicking the **Log On As** header.

   b. Right-click the service, then from the pop-up menu select **Stop**.
8. Run the upgrade migration script to back up your configuration:

a. Log on to the server as the MyID installation user.

   On a split tier system, you must run the script on both the application server and the web server.

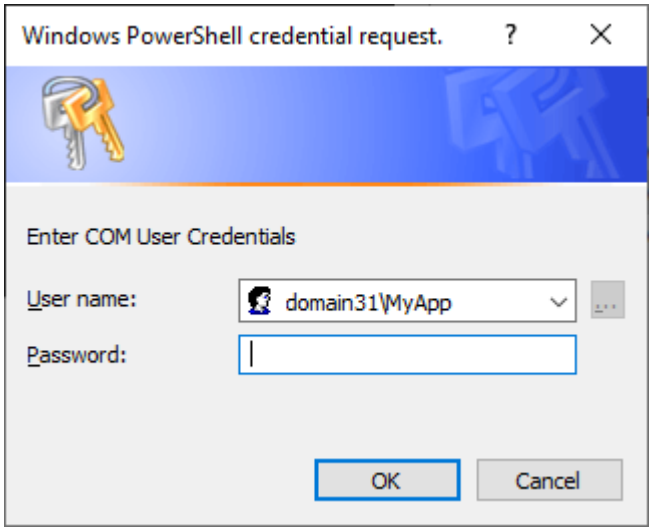
b. Copy the `Scripts` folder from the following location in the MyID release image:

   `Support Tools\Upgrade\Upgrade Data Migration\`

c. Right-click the `UpgradeMigrate.bat` file, then from the pop-up menu select **Run as administrator**.

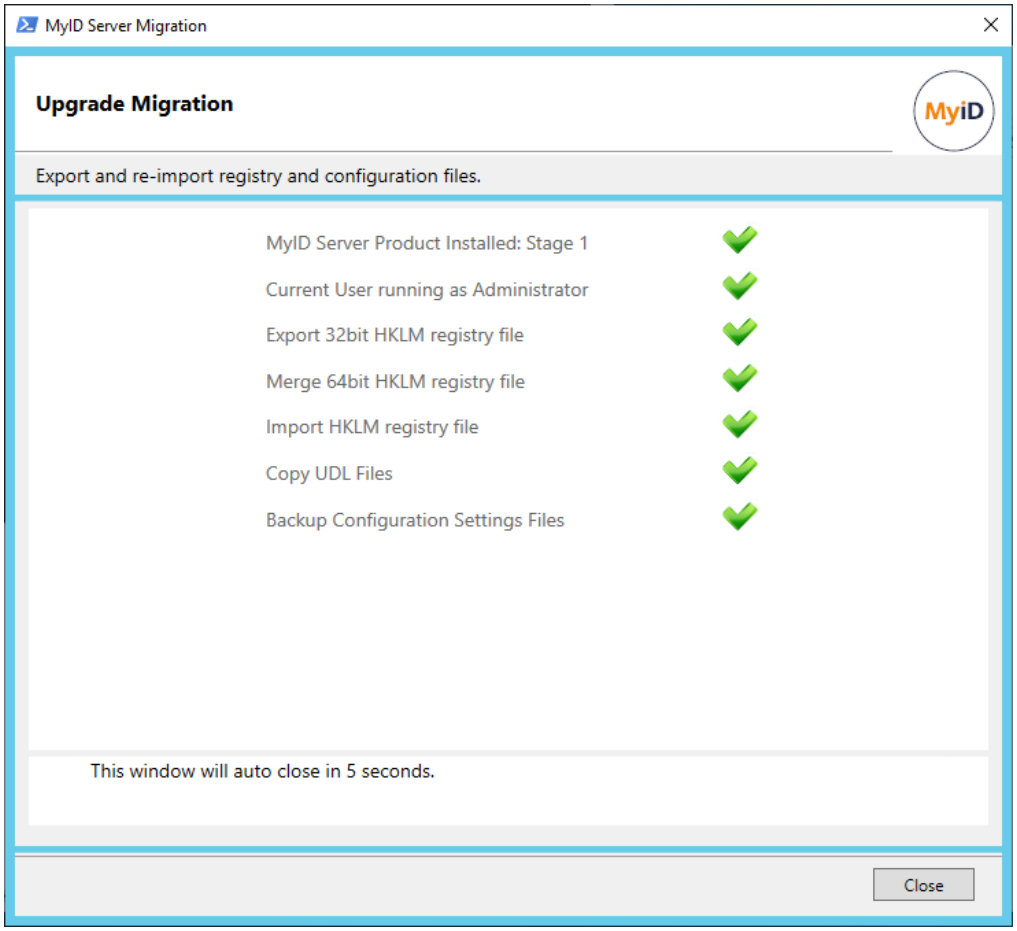
   Enter your administrator credentials if prompted.

   If you are running the script on the application server, the script then requests your MyID COM user credentials:



d. Type the password for the MyID COM user, then click **OK**.

   The MyID Server Migration screen appears, and displays its progress as it backs up your server configuration.



The information backed up depends on your system configuration; for example, in addition to the items in the screenshot, the script may also need to back up your `HKCU` area of the registry.

If there are any problems, you can display the log by clicking the provided link on screen.

e. Click **Close**, or wait for the dialog to close automatically five seconds after a successful run.

9. Uninstall any MyID patches, hotfixes, or modules.

   You must uninstall the patches and modules in the reverse order in which they were applied. See the list of the updates that have been applied to your system that you obtained from the **Installation History** tab of the **System Status** report.

   If you are asked to reboot at any point, do so.

   Note: If you are uninstalling a MyID 10 system, you can used a set of PowerShell scripts that help remove existing patches. See the instructions in the following folder in the current MyID release image:

   `\Support Tools\Upgrade\v10 Patch Removal\`

10. Uninstall MyID:

    a. Using the **Programs and Features** option in the Windows Control Panel, uninstall the following item:

- MyID Server

b. If you have the following item in the list of **Programs and Features**, you must also uninstall the client components:

- MyID Client Components x86

c. Reboot the server.

d. If the MyID program folder still exists, make a backup, then remove it.

The easiest way to do this is to rename the folder.

11. On each client, you are recommended to uninstall the previous version of the MyID client software; for example, MyID Desktop, the Self-Service App, the Self-Service Kiosk, or the BioPack client components.

12. Install or upgrade any pre-requisites for the components you are going to be using.

See your integration guides for details.

Note: The configuration for your components may have changed for this version of MyID. Make sure you check the integration guides for the latest information.

13. Reboot the MyID server.

Note: If you do not reboot the MyID server before running the installation program for the latest version, you may see an error similar to the following:

```
Error 1303. The installer has insufficient privileges to access this
directory: C:\Program Files\MyID\Components\Devices. The installation
cannot continue.
```

If you see this error, click **Cancel**, ignore any errors that appear, then reboot the server. Make sure that MyID is not installed, then attempt to run the installation program for the latest version again.

14. Install the latest version of MyID using the MyID Installation Assistant.

See section 2, *MyID Installation Assistant* for details.

15. Once the installation has completed, run the upgrade migration script to restore your backed-up configuration:

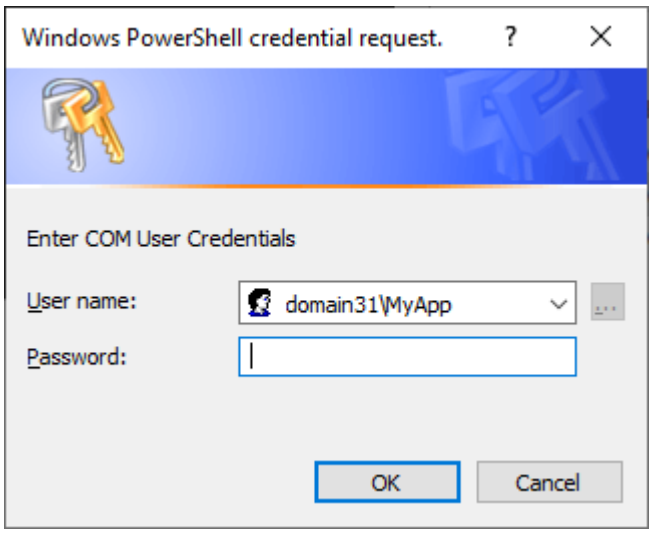
a. Log on to the server as the MyID installation user.

On a split tier system, you must run the script on both the application server and the web server.

b. Right-click the `UpgradeMigrate.bat` file, then from the pop-up menu select **Run as administrator**.

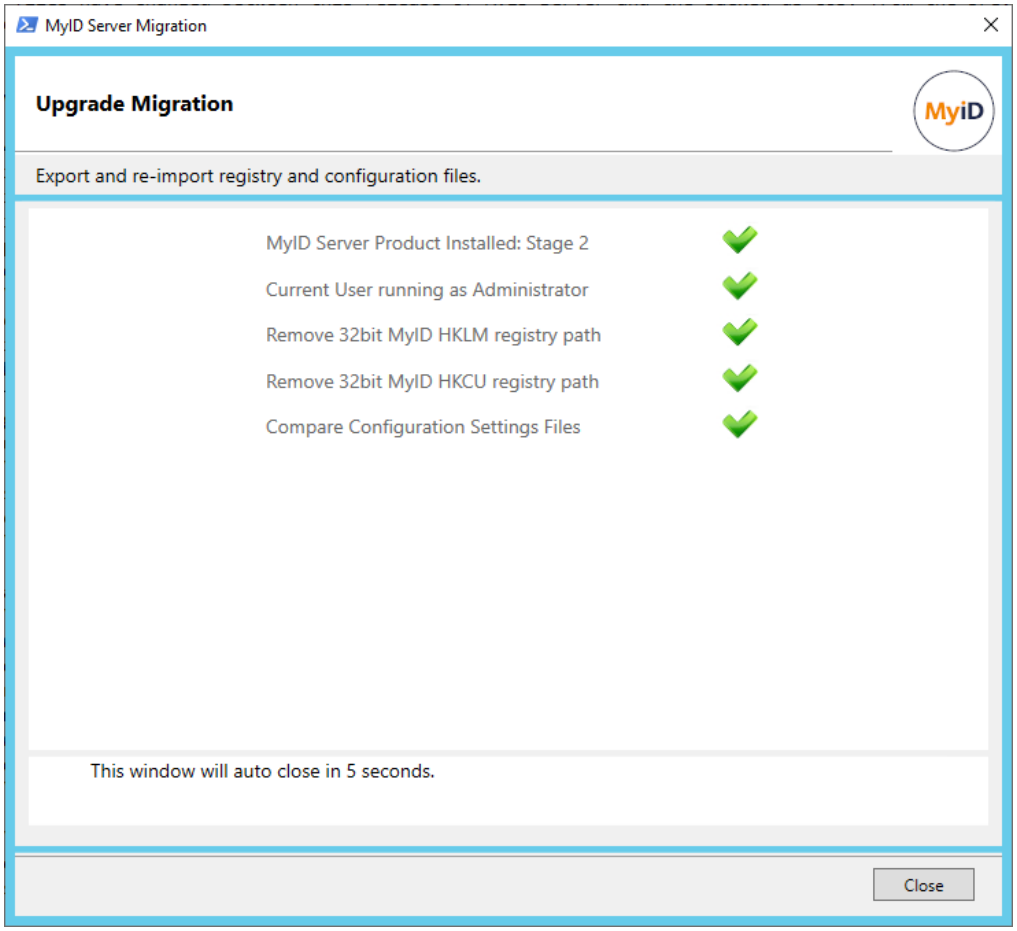
Enter your administrator credentials if prompted.

If you are running the script on the application server, the script requests your MyID COM user credentials:



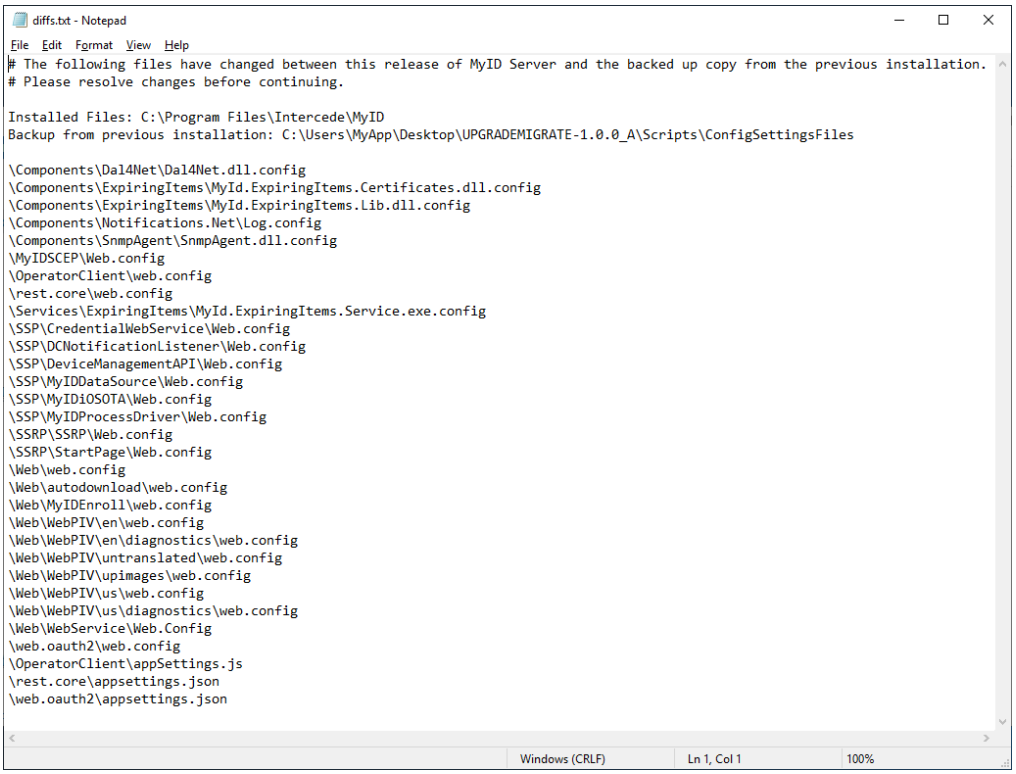
c. Type the password for the MyID COM user, then click **OK**.

The MyID Server Migration screen appears, and displays its progress as it restores your server configuration.



d. Click **Close**, or wait for the dialog to close automatically five seconds after a successful run.

The configuration file change report appears:



This report displays any differences between the configuration files from your previous system and the files installed by the current installation program.

e. Review the changes between the configuration files; if you have made any manual changes to the configuration files, you must implement them in the current versions of the files.

   Note: Some changes in the configuration files may be the result of enhancements to MyID since your previous version was released. If you are unsure about any changes, contact customer support quoting reference SUP-342 for assistance.

16. Complete any required post-installation configuration changes to your system.

    See section *11*, *After installing MyID*.

17. Install the 64-bit versions of any modules you previously had installed.

18. On each client:

    a. Install the MyID client software; for example:

       - MyID Desktop
       - MyID Client Service for the MyID Operator Client
       - Self-Service App
       - Self-Service Kiosk

    b. Clear the browsing history in the Windows Internet Options dialog.

       Note: Make sure you deselect the **Preserve Favorites website data** option, if it is available.

You are recommended to upgrade the client software on each client. New features of the server software may require the latest client software.

19. Review your security settings.

    For example, when you install MyID, the **Security Officer PIN Type** is set to **Random** rather than whatever it was set to previously – make sure that this suits the security requirements of your system.

    See the ***System Security Checklist*** for details.

20. Follow the instructions for configuring MyID after you complete the upgrade.

    See section *7.7*, *After you upgrade*.

7.6 Upgrading to a new server

If you are upgrading MyID from an existing system, you may take the opportunity to upgrade onto a new environment, particularly if you are currently running on an older server operating system.

Important: Check that you have carried out all of the prerequisite actions before beginning the upgrade installation process. See section *7.1*, *Before you upgrade* for details.

The overview of the process is as follows:

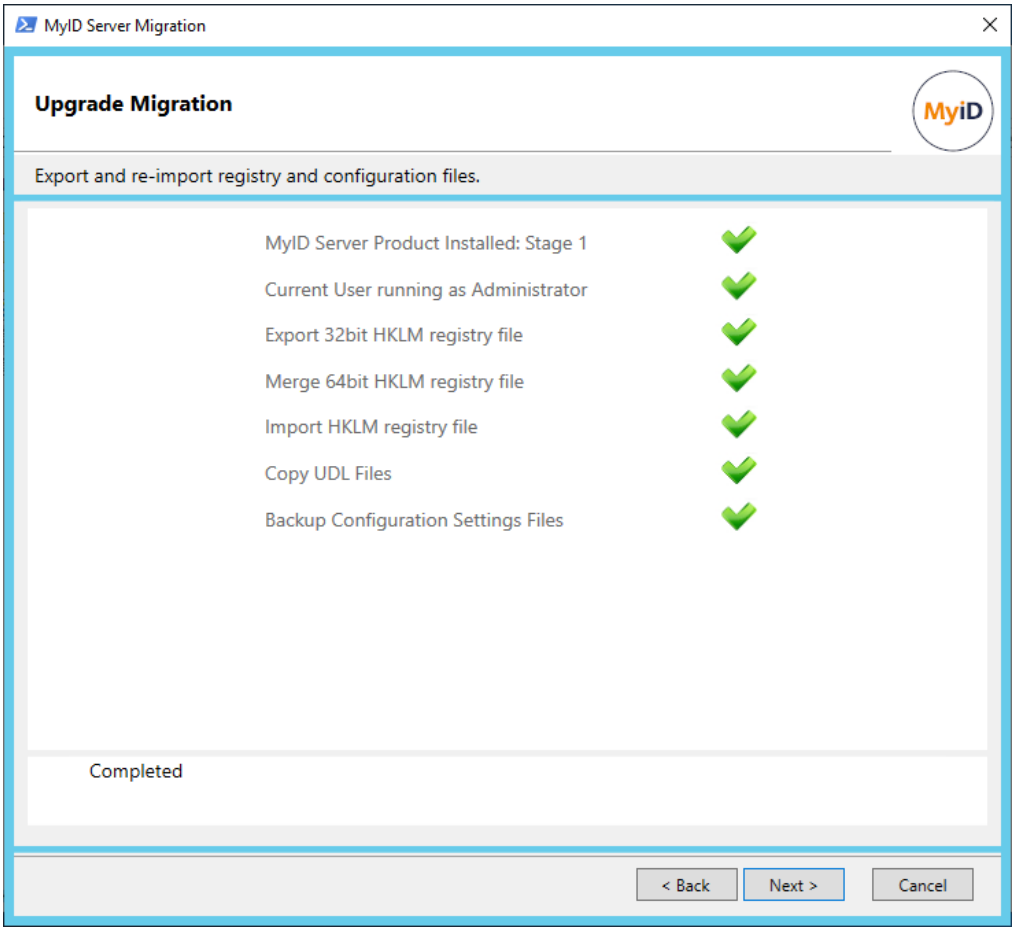
1. Back up your existing system.
2. Make sure your system registry is ready for export.

   This depends on the version of your existing system.

   - For MyID 12 or later, you do not have to do anything to upgrade your registry before you export it.
   - For MyID 11:
     a. Run the MyID Installation Assistant.

        See section *2.27.2*, *Upgrading from a MyID 11 system*.

     b. Complete the process until the Upgrade Migration screen has completed.



c. Click **Cancel** to close the MyID Installation Assistant.

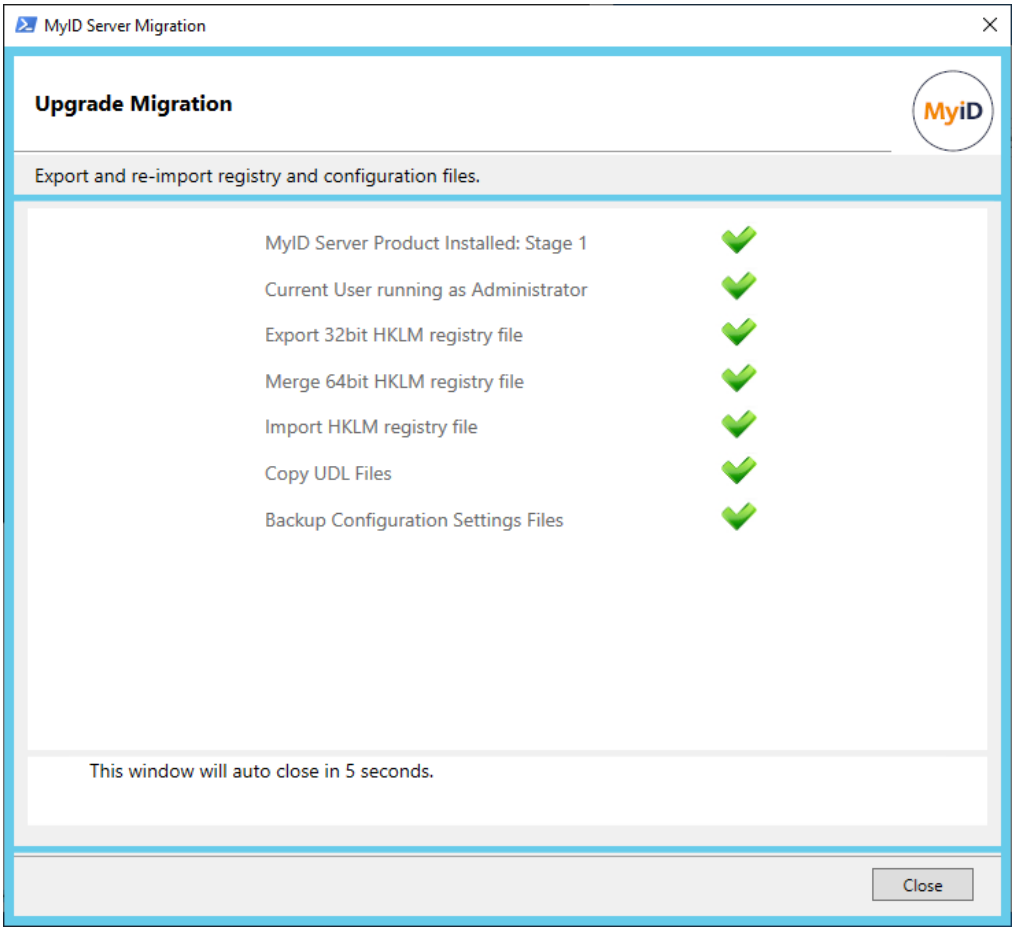
You do not have to proceed further with the installation process on the existing server, as this is a temporary step to upgrade the registry on your existing system before migrating it to the new system.

- If your existing system is earlier than MyID 11:

  a. Run the Upgrade Migration script.

  See section *7.5, Upgrading MyID from a 32-bit application to 64-bit*.

  b. Complete the process until the Upgrade Migration screen has completed.



c. Click **Close**.

You do not have to proceed further with the installation process on the existing server, as this is a temporary step to upgrade the registry on your existing system before migrating it to the new system.

3. Back up the database.

   See the Microsoft SQL Server documentation for details on carrying out a backup and restore of your database.

4. Copy the database backup files to the new server.
5. Restore the backed-up database on the new database server.
6. Repeat the process for any additional MyID databases; for example, archive databases.
7. Export the registry from the old application server.

   The registry is in the following location:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Intercede`

8. Merge the exported registry file into the registry on the new application server.
9. If you are using an HSM, make sure the HSM is accessible from the new server.

   You can use the HSM Test Utility on the new application server to confirm that MyID can access the HSM.

10. Run the MyID Installation Assistant on the new system and install the latest version of MyID.

    The MyID Installation Assistant picks up the key from the registry or HSM, which provides access to the information in the database.

    Make sure you select the database you copied to the new database server.

    Make sure you run all of the checks – initial, pre-install, and post-install – and configure your system accordingly.

11. Follow the instructions for configuring MyID after you complete the upgrade.

    See section *7.7*, *After you upgrade*.

7.7 After you upgrade

After you have completed the installation process for the new version of MyID, you may have to carry out some additional configuration before your system is fully operational.

7.7.1 Reviewing web server security

Upgrading your MyID system may reset some of your IIS configuration, if you have made changes manually or using PowerShell scripts; for example, setting up SSL/TLS on your websites. You must review your IIS settings after upgrade to ensure that everything is configured correctly.

7.7.2 Upgrading your renewal and issuance jobs

If you need to update your renewal and issuance jobs, after you install MyID you must run the appropriate database scripts. See section *7.1.7*, *Upgrading renewal jobs* and section *7.1.8*, *Upgrading card issuance jobs* for details.

7.7.3 Upgrading clients

Note: If you have the MyID Client Components (provided in the UMC package) installed on any PC, uninstall them before you install the latest version of the MyID clients.

You are recommended to upgrade your clients (Self-Service App, Self-Service Kiosk, MyID Desktop, and MyID Client Service) on each client PC when you upgrade MyID. Older versions of the MyID clients may continue to operate with reduced functionality, and may experience problems when attempting to use new functionality.

7.7.4 Upgrading credential profiles

After you have upgraded your system, you must use the **Credential Profiles** workflow to upgrade each credential profile to the latest version.

Note: Credential profiles were previously known as card profiles.

To upgrade a credential profile:

1. From the **Configuration** category, select **Credential Profiles**.
2. From the **Select Profile** drop-down list, select the profile you want to edit.
3. Click **Modify**.
4. Click **Next** on each screen until you complete the workflow.

In most circumstances, you do not have to make any changes. However, see section *7.7.12*, *Upgrading systems with older data models* and section *7.7.13*, *Upgrading systems with customized data models* for considerations relating to upgrading credential profiles and their data models.

The profile is updated to the latest version of the software.

Note: If you are upgrading from a pre-MyID 10.8 system and are using terms and conditions, you must select an HTML template for the terms and conditions in each credential profile. See the *Terms and conditions* and *Customizing terms and conditions* sections in the ***Administration Guide***.

7.7.5 Upgrading security phrase security

MyID now uses SHA256 to store the answers stored for security phrases, providing significantly enhanced security. This feature is enabled by default for new installations. If you are upgrading an existing system prior to version 10.2, you must update the security phrases stored for each user.

The security phrase security setting is controlled by the **Use Security Phrase algorithm version 2** option on the **PINs** tab of the **Security Settings** workflow. You can set the option to one of the following:

- **No** (red cross icon) – The new security phrase algorithm is not used. This means the original security phrase hashing algorithm is used.
- **Ask** (blue question mark icon) – The new security phrase algorithm is used for users on upgraded clients. This setting is for transitioning from the original algorithm to the v2 algorithm.

  While in this mode, logon can be performed using clients that have not been upgraded, using security phrases that were captured using the original security phrase algorithm.

  If a user changes their security phrases while this configuration is set on a client that has not been upgraded, the old password algorithm will be used to store the new security phrases.

  If a user changes their security phrases while this configuration is set on a client that has been upgraded, security phrases will be stored using both the old and the new algorithms. This allows logon on both upgraded and non-upgraded clients.
- **Yes** (green tick icon) – The new security algorithm is used across the board.

  Security phrase logon is allowed only if the client software has been upgraded, and the passphrases have been captured using the new algorithm. Authentication using original security phrase algorithm is no longer allowed. Any passphrases that are changed shall be stored only using the new v2 algorithm.

You are recommended to carry out the following procedure:

1. Set the **Use Security Phrase algorithm version 2** option to **Ask**.
2. Upgrade each client PC.
3. Ask each user to change their security phrases on an upgraded client.
4. Once all users have updated their security phrases, set the **Use Security Phrase algorithm version 2** option to **Yes**.

To get the full benefit of the **Use Security Phrase algorithm version 2** feature, the setting must be **Yes**, and any previously captured passphrases using the original algorithm (while the configuration was set to **No** or **Ask**) must be removed. To remove the old security phrases, a user can change their security phrases while the **Use Security Phrase algorithm version 2** option is set to Yes. If you require assistance with bulk removal of legacy security phrase data, contact Intercede customer support, quoting reference SUP-121.

Note: This feature also affect authentication codes that were issued by MyID 10.1 or earlier. If you want to use authentication codes that were generated before you upgraded, you must set the **Use Security Phrase algorithm version 2** option to **Ask**. If you set the **Use Security Phrase algorithm version 2** option to **Yes**, you must request new authentication codes.

7.7.6 Upgrading roles

The upgrade process can make changes to the roles set up on your system; for example, upgrades from MyID PIV 9 to MyID 10 may result in changes to the PIV Sec Officer role and the workflows it has available. Check that your role assignments are correct after you have completed the upgrade.

When you install MyID, the System role is granted permission to all the workflows in MyID. Make sure you review your security requirements for this role after upgrading MyID.

If you have removed any of the following roles:

- Registrar
- Help Desk
- Applicant
- Adjudicator
- Issuer
- Sponsor
- Security Officer
- Signatory
- Contractor
- Emergency
- Foreign

When you upgrade MyID from any pre-MyID PIV 10.1 system, these roles are added back into your system.

7.7.7 Upgrading email support

Versions of MyID before MyID 10.6 used Database Mail to send email messages.

If you are upgrading an existing system from before MyID 10.6, your Database Mail configuration will continue to work; however, if you want to switch to the new system, carry out the following:

1. Set up a new SMTP server in the **External Systems** workflow.
2. Set the **Database Mail Profile Name** option to empty.

See the *Setting up email* section in the ***Advanced Configuration Guide*** for details.

7.7.8 Upgrading the storage of PINs for HSMs

From version 10.7, MyID stores the PINs for Thales HSMs encrypted in the registry for the MyID COM+ user. If you are upgrading an existing Thales HSM system and want to migrate the PIN, or if you are using an Entrust nShield HSM and want to store the PIN, you can use the SetHSMPIN utility to do this.

See section *8.6*, *Setting the HSM PIN* for details.

7.7.9 Modifying an existing installation

If you want to use the installation program to modify your installation of MyID after the original installation is completed, see section *8.4*, *Modifying the installation*.

7.7.10 Upgrading systems with Virtual Smart Cards

If your system is using server-generated Virtual Smart Cards, note that the server-generated VSC feature has now reached end of support. If you are upgrading from an earlier version of MyID, and are using server-generated VSCs, MyID will continue to support lifecycle management of the issued VSCs. See the ***Microsoft VSC Integration Guide*** for details.

7.7.11 Upgrading systems with a startup user

If you are using a startup user configured using GenMaster, after you upgrade your system to the latest version of MyID you may not be able to use that account to log on to MyID. To reset the startup user, run GenMaster again and select the **Configure startup password** option. See section *8.5*, *Using GenMaster* for details.

Note: Startup users are intended only for bootstrapping your system, and are not intended for long-term use. See the ***System Security Checklist*** document for details.

7.7.12 Upgrading systems with older data models

When you upgrade your system, if your credential profiles use older data models that are no longer supported, you may experience problems with certificates losing their assigned containers. After upgrading, make sure that each of your credential profiles has a valid data model specified, and has the correct settings for each certificate container, if appropriate.

7.7.13 Upgrading systems with customized data models

If you have customized the standard card data models, installing MyID may overwrite your changes. Make sure you back up your customized files and review the changes after installation.

MyID 10.7 increases the size of the Security Object in all standard card data models. This addresses an issue that prevented issuance on systems where the Certificate Authority had a long distinguished name.

If you are upgrading an existing pre-MyID 10.7 system that has custom data models, you must manually update your data model files to increase the size of the Security Object.

For guidance on updating the size of the security object, contact customer support, quoting reference SUP-247.

7.7.14 Upgrading systems with Project Designer customizations

If you are upgrading a MyID system that has had screen layouts customized using Project Designer, you may see some cosmetic differences after you have upgraded your system.

7.7.15 Upgrading hyperlinks for the Self-Service App

In MyID 11.0, the format used for command-line parameters for the Self-Service App has changed. You must make sure that any systems that make use of these arguments – for example, custom email templates – are updated to use the new command-line arguments. For more information, see the *Command line arguments* section in the ***Self-Service App***.

7.7.16 Upgrading customized configuration

If you have made any changes to configuration files, such as the `myid.config` file for the various MyID web services, you must merge in the changes from the backups you made before you installed the new version.

You may also have to re-implement translations. For information about translating the text for all on-screen elements in the client applications, contact Intercede customer support, quoting reference SUP-138.

If you have further customizations on your system and would like assistance with the upgrade process, contact customer support quoting reference SUP-300.

7.7.17 Upgrading systems with multiple databases

Your MyID system may have multiple databases; for example, a separate audit database, an audit archive database, or a binary objects database. You configure MyID to point to the appropriate database by configuring its `.udl` files; you are recommended to back up these files in the Windows `SysWOW64` folder (for 32-bit MyID before version 12.0.0) or `System32` folder (for 64-bit MyID from 12.0.0 on) before you start the upgrade; after you have installed the new version of MyID, you may have to reconfigure each of these files to point to the appropriate database.

For more information about setting up your MyID system to use multiple databases, see the *Database configuration* section in the ***Advanced Configuration Guide***.

7.7.18 Upgrading systems that use Integrated Windows Logon

If your system uses Integrated Windows Logon, you must reconfigure the web services and carry out any configuration in IIS for Integrated Windows Logon. See the *Configuring the MyID web services for Integrated Windows Logon* section in the ***Web Service Architecture*** guide and the *Integrated Windows Logon* section in the ***Administration Guide*** for details.

7.7.19 Upgrading biometric integration

If a change to the biometric devices and software used in your environment is required as part of the upgrade, you must review the configuration options relating to biometrics. For example, you must check the **Biometric matching library** and **Fingerprint enrollment device**.

If you previously used Cross Match as the biometric matching library, you must modify this setting to the new library selected for your environment. For further information, see the *Cross Match legacy fingerprint integration* section in the ***Release Notes***, and the appropriate biometric integration guides provided with MyID.

7.7.20 Upgrading the client suite with MSIX

If you are upgrading to the MyID Client Suite 1.5.0 using MSIX, you must also update some of the optional packages. For more information, see the *Upgrading to the MyID Client Suite 1.5.0* section in the ***MyID Client MSIX Installation Guide***.

7.7.21 Supporting older clients

MyID has an improved envelope mechanism. This provides enhanced security for data transferred between MyID clients and the MyID server. When you install MyID, it is configured to support the new Envelope Version 1.3 instead of the previous Envelope Version 1.2. This affects whether you can use older clients to access MyID:

- Windows clients (MyID Desktop, Self-Service App, and Self-Service Kiosk) that use MyID Client Components version UMC-10.1.1000.14 or later (as provided with MyID 10.1) support the new Envelope Version 1.3.
- Windows clients using older versions of the MyID Client Components support only the previous Envelope Version 1.2.

You can choose which envelope mechanisms to support in MyID; if you need to maintain support for older clients, you must enable support for Envelope Version 1.2.

To select the envelope mechanisms:

1. Install the latest MyID Desktop.
2. Within MyID Desktop, from the **Configuration** category, select **Security Settings**.
3. On the **Server** tab, set the following:
   - **Allow envelope version 1.2** – MyID allows clients to connect using the older envelope mechanism. All clients support this mechanism.
   - **Allow envelope version 1.3** – MyID allows clients to connect using the updated envelope mechanism. Windows clients from MyID 10.1 support this mechanism.

   Note: Do not deselect both options. If you deselect both options, no clients will be able to access MyID, and you will be locked out of the system. If you accidentally deselect both options, contact customer support, quoting reference SUP-140.
4. Click **Save changes**.

Note: If you have enabled envelope version 1.2, then subsequently decide to disable it and use envelope version 1.3 only, you may experience some problems when you set the option in the **Security Settings** workflow. After you click **Save changes** to set **Allow envelope version 1.2** to `No` and **Allow envelope version 1.3** to `Yes`, MyID Desktop cannot communicate with the server through its current connection, and you will see an error similar to:

```
An error occurred on the server when processing the URL. Please contact the
system administrator.
If you are the system administrator please click here to find out more
about this error.
```

Close MyID Desktop (this may present additional errors, which you can safely ignore). When you open MyID Desktop again, it will use envelope 1.3 and work correctly.

7.7.22 Updating the list of identity documents

MyID 12.4 provides an updated list of the identity documents available on the **APPLICATION** tab of the Edit PIV Applicant screen to match the specifications of the section 2.7 of the FIPS-201-3 PIV Identity Proofing and Registration Requirements (***pages.nist.gov/FIPS201/requirements/#s-2-7***).

If you are upgrading from a system earlier than MyID 12.4, the upgrade process does not change the existing list of identity documents. You must use the **List Editor** workflow to update your system to include the latest list of primary and secondary identity documents.

See the *Identity documents* section in the ***PIV Integration Guide*** for details.

7.7.23 Known issues with upgrading

- **IKB-198 – Notifications DLL error when uninstalling MyID**

  If you are upgrading from MyID 10.5 or earlier, you may see an error similar to the following when uninstalling MyID:

  ```
  Failed to unregister Notifications.dll
  ```

  The error occurs when the DLL has become unregistered on the server before the uninstall process begins. You can close the error message with no additional impact.

8 Installing MyID

SIU reference: SIU-033.

The MyID installation program checks your system to see if it has recent versions of some important Microsoft utilities. If the versions on your machine are out of date, the installer will attempt to install these for you.

Warning: If you are running a non-English version of Windows, you must get your own language versions of the Windows scripting components from the Microsoft download center and install them yourself. Do not attempt to install these from the MyID installation media, as you will get a 'mixed language' operating system, which may have unpredictable side effects.

The Windows scripting version 5.6 redistributable component is checked and installed if necessary.

8.1 Overview

The installation and initial configuration of the MyID server can be broken down into the following stages:

1. Install and validate the MyID Windows Server environment.
   - Windows Server (including Internet Information Services)
   - Directory Services.
   - Database.
   - Certificate Authority.
2. Install MyID Server.
   - Install and configure the MyID database.
   - Install and configure the MyID application server.
   - Create a master key using GenMaster.
     - You must create the master key for the database. You can use an HSM to store the key or store the keys in the registry.

       Note: Make sure you have set up your HSM in accordance with the instructions in the relevant integration guide before installing MyID.
     - Set the password for the startup user.
   - Install exported COM+ Components on web server.
   - Install and configure the MyID web and web services servers.
3. Install the latest MyID server update.

   Between major versions of MyID, Intercede also supplies customers with updates that provide improvements and new functionality. If an update exists, it will be provided on the installation media.

   See section *9*, *Updating MyID* for details.
4. Configure and test the Directory Connection, where applicable.

- Active Directory will operate with no additional configuration.
- Other LDAP directories may require configuration to set attribute mapping.
- Advanced features such as LDAP mapped custom attributes will require manual configuration.

5. Configure and test the Certificate Authority connection.
6. Install and test a Client Machine.

   See section *12*, *Testing the installation* for details.
7. Define and test MyID Security Policies.
   - Define User Roles.
   - Define Certificate Policy filters.
   - Construct Credential Profiles.
   - Add a user and test card issuance.

8.2 Split deployment

SIU references: SIU-206, SIU-207, SIU-208, SIU-209, SIU-210, SIU-211, SIU-212, SIU-213, SIU-214, SIU-215.

To implement a split deployment, where the MyID application, web, and database components are installed on different physical machines, you must follow a strict implementation procedure. This ensures the various servers are created in the correct order. An overview of this order is described here.

Make sure that the time and date are synchronized between the servers.

Note: Make sure you have DTC set up to allow the servers to communicate with each other. See section *11.2*, *MSDTC security configuration*.

1. Create the MyID database.
   a. Run the MyID Installation Assistant either locally on the database server, or remotely on the MyID application server for a remote install. If you are installing remotely, you can install the database server and application server at the same time.

      Important: If you run the MyID Installation Assistant on the application server to create the database at the same time as you install the application server components, you must carry out any further modifications, updates, or upgrades to the database from this same server.

   b. Select the **Database Server** option on the Server Roles and Features screen.
2. Create the MyID application server.

   Use the Server Manager to make sure that the server is set up to have the Application Server role. You do not need the Web Server (IIS) Support role.

   Run the MyID Installation Assistant on the application server and select the **Application Server** option on the Server Roles and Features dialog.

   Note: It can be helpful to install both the application server and web server on the same machine initially; this allows you to verify that the installation is working correctly. Once

you have this system set up and working, you can install the web server onto a separate machine and transfer the COM proxies to split the web and application servers onto separate physical machines.

3. Run GenMaster to generate a master key for the database and a startup user.

   This application runs automatically during the MyID application server installation and is used to generate your Master Keys in the registry or in your HSM, as well as to create a startup user that allows you to bootstrap the system. See section *8.5*, *Using GenMaster*.

4. Create the web server.

   Run the MyID Installation Assistant on the web server and select the **MyID Client Support** options on the Server Roles and Features screen.

   Select any or all of the optional MyID services features that you want to use.

   On the MyID COM Proxy Location screen, import the COM+ proxies from the application server. This allows the web server to communicate with the application server components; see section *2.10*, *Installing the COM+ proxies*.

5. Open MyID Desktop or the MyID Operator Client.

6. Log on to MyID with the startup user.

Note: This procedure assumes that you want to keep the MyID website and the MyID web services on the same physical server. If you want to use separate servers for the website and the web services, see the *Setting up the MyID web services on a standalone server* section in the ***Web Service Architecture*** guide for details of the necessary additional configuration.

8.3 Running the installation program

The installation program is run automatically as part of the MyID Installation Assistant process. The MyID Installation Assistant checks your system and gathers all the required information, so that when it needs to run the installation program, it runs silently without any further intervention on your part.

Important: Do not attempt to run the product installation program outside of the MyID Installation Assistant; the installation program is designed to be run from within the MyID Installation Assistant.

See section *2*, *MyID Installation Assistant* for details.

8.3.1 Updates

Intercede may have provided you with an update to your system that you must install after running the main MyID installation program. See section *2.24*, *Applying an update* for details.

8.3.2 Windows Event Viewer messages

You may notice event log messages after the installation. For example:

```
During installation of this component into a COM+ application a registry
value was changed from its original value. If you are experiencing
activation problems with this component then please check the registry
values.
```

This can happen for the `edeficeBOL_PKI.dll`.

You may also see an error in the event log relating to `MsiExec.exe`, which is related to a message in the MSI installer log with a corresponding timestamp and the following text:

```
EEUI - Install failure: Calling shutdown on EEUI DLL
```

These messages are expected and do not affect the installation.

8.4 Modifying the installation

You can use the MyID installation program to modify the installation. This allows you to add features, such as individual web services.

Note: The **Modify** option on the installation program does not allow you to change other aspects of the installation, such as the server user accounts or the website used to host the MyID website and web services. If you need to change the passwords for user accounts, you can use the ***Password Change Tool***; if you need to change the website, you must uninstall the **Web Server** or **Web Services Server** feature and install it again. If both the web server and web services server features are installed on the same physical server, and you need the change the web server where they are installed, you must uninstall *both* features then reinstall them.

Important: You are recommended not to use this feature to remove features. To remove items from an existing MyID server installation, first uninstall the product from the affected server, then reinstall with the required features. You need to do this only on the affected server in your installation; for example, if you want to remove a web service, you can uninstall the web tier, then reinstall with only the required web services; you do not have to uninstall the application server. If you require further assistance with this issue from Intercede, contact customer support, quoting reference SUP-299.

Note: If you have installed MyID to a non-default location, when attempting to modify you may see an error similar to:

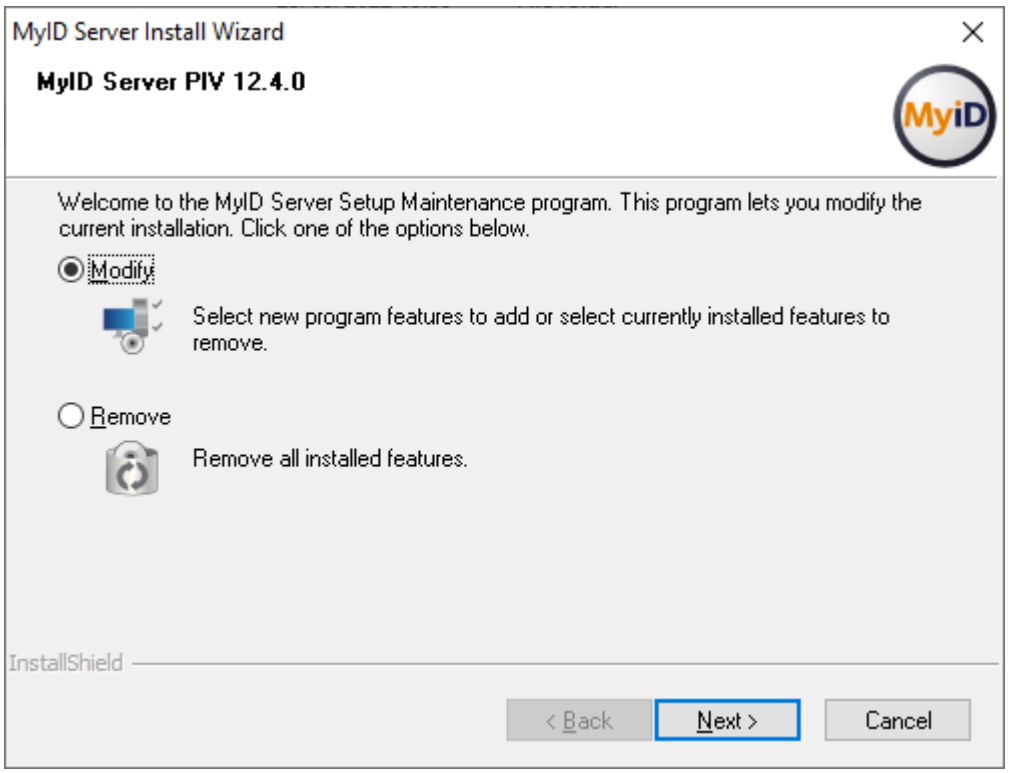
```
Error 1306. Another application has exclusive access to the file
C:Test\Company\MyID\SSP\MyIDDataSource\MyIDDataSource.log. Please shut down
all other applications, then click retry
```

If this error occurs, open a Windows command prompt, type `iisreset` to reset IIS, which clears the file lock, then click **Retry**.

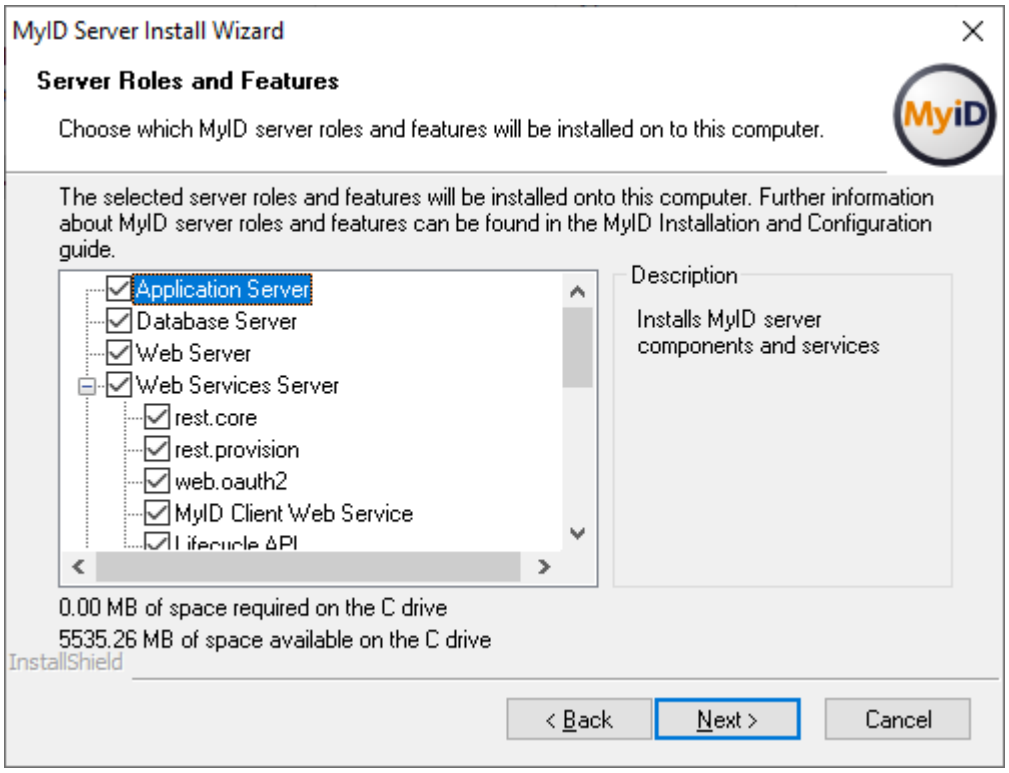
To modify the MyID installation:

1. Log on to the MyID server using the installation account.
2. Close all application windows.

   Note: Once you have started the installation process, do not leave the installer program idle. Windows UAC may cancel the installation if you leave the program idle for too long, depending on your Windows environmental settings.
3. From the MyID `Installer` folder, right-click the installation program – for example, `MyIDServer-12.4.0.exe` – then from the pop-up menu select **Run as administrator**.



4. Make sure the **Modify** option is selected, then click **Next**.



The screen displays the features you currently have installed.

Note: The options in this installation program do not correspond exactly to the options displayed in the MyID Installation Assistant; the MyID Installation Assistant displays a list of options that has been organized to make it clear which options are optional. The options available in this installation program are as follows:

- **Application Server** – contains the MyID application components.
- **Database Server** – contains the MyID database.
- **Web Server** – contains the main MyID web server, including the websites for MyID Desktop and the MyID Operator Client.
- **Web Services Server** – contains the MyID web services. You are recommended to install this on the same server as the Web Server; if you want to install the services on a different server, you must carry out additional configuration. See the *Setting up the MyID web services on a standalone server* section in the ***Web Service Architecture*** guide for details.
  - **rest.core** – required for the MyID Operator Client. This contains the rest.core web service that you can also use for your own systems; see the ***MyID Core API*** guide for details.
  - **rest.provision** – used for issuing mobile credentials. mobile identity documents, and soft certificates. See the *REST API for mobile credentials* section in the ***Implementation Guide***.
  - **web.oauth2** – required for the MyID Operator Client. This contains the web.oauth2 web service that you can also use for your own systems; see the ***MyID Authentication Guide*** guide for details.
  - **MyID Client Web Service** – required for MyID Desktop,the Self-Service App, the Self-Service Kiosk, and mobile clients.
  - **Lifecycle API** – see the ***Lifecycle API*** guide.
  - **Credential Web Service** – see the ***Credential Web Service*** guide.
  - **Device Management API** – see the ***Device Management API*** guide.
  - **Mobile iOS OTA** – see the *Setting up iOS OTA provisioning* section in the ***Mobile Identity Management*** guide.
  - **Reporting Web Service** – see the ***Reporting Web Service API*** guide.
  - **Derived Credentials Notifications Listener** – see the ***Derived Credentials Notifications Listener API*** guide.
  - **SCEP API** – see the *Managing devices* section in the ***Administration Guide***.
  - **MyID Verification Service** – see the *MyID Verification Service* section in the ***Mobile Authentication*** guide.
  - **Self-Service Request Portal Web Service** – see the ***Derived Credentials Self-Service Request Portal*** guide.
- **MyID External Authentication Server** – contains web services for use with external authentication. Select the following options:

- **ADFS Auth Web Service** – see the *Installing the ADFS Auth web service* section in the ***MyID Authentication Guide***.
- **web.oauth2.ext** – see the *Setting up the standalone authentication service* section in the ***MyID Authentication Guide***.

- **Archive Database Server** – contains a database that can contain an archive of some parts of the MyID database. Creating the database does not set up the archiving procedures; the *Database configuration* section in the ***Advanced Configuration Guide*** for details.

5. Select the features you want to add, then click **Next**.
6. Review the installation summary, then click **Install**.
7. Once you have completed the installation, restart the server.

8.4.1 Considerations for modifying your system

Once you have installed the MyID server, its installation configuration settings are preserved in the MSI database and the registry. Subsequent installer actions use these values; if the server configuration has been modified without the use of the installer, actions such as upgrade and update may fail.

In a scenario where you need to change the MyID server configuration, and you have already installed the MyID server components, you must run the installation program and select the Modify option. You may need to deselect features such as web and web services if, for example, you need to change the IIS configuration.

Once you have made your system configuration changes (for example, changing your IIS configuration), you can re-run the installation program, select the Modify option again, and re-add the required features. This ensures future updates or upgrades of the system will function correctly.

8.4.2 Known issues

- **IKB-317 – Issue with modified installations**

  For all 11.x versions of MyID before MyID 11.7, if you install MyID without the Web Server and Web Services Server features, then modify the installation to add these features, you will experience problems when attempting to update, upgrade, or uninstall MyID.

  If this error is encountered, it is present in the MSI log file. The IIS error causes an installer status of 1603.

  As a workaround, you can run the installation program to modify the system and remove the Web Server and Web Services Server features, at which point you can successfully carry out an uninstallation; you can then reinstall MyID with the required features, and subsequently carry out an update or upgrade.

8.5 Using GenMaster

SIU references: SIU-267, SIU-268, SIU-283, SIU-284, SIU-285, SIU-286.

The GenMaster application allows you to do the following:

- Set up the key protection mechanism for the MyID installation.
- Set up a startup user with a password.

The startup user allows you to access MyID for the first time and complete the setup of your system.

- Set up shared secret keys (legacy GenMaster only).

Your choice of key protection mechanism is a compromise between cost, convenience and security.

- Registry secured

  The most convenient but least secure method is to use registry keys, where the database encryption keys are held in the registry. Although access to the keys can be controlled by applying access rights on the relevant branch of the registry, it is still only recommended for test, demonstration or low security installations. It does have the benefits of fast installation, no additional hardware and unattended restart.

- HSM secured

  The most secure option is to use an HSM. In this case, not only is the database key secured, but the HSM also performs on-board decryption, further decreasing the risk of the key being exposed. The choice of HSM and its configuration can affect the ability to perform unattended restarts, as some devices can require a smart card to authorize when rebooting.

  For production environments we recommend the use of an HSM, unless you consider that the physical security of the application server meets your acceptable level of risk.

  For full information on your chosen HSM support, see your HSM integration guide.

MyID provides the following versions of GenMaster:

- GenMasterEx – the current version of GenMaster, fully integrated with the MyID Installation Assistant.
- Legacy GenMaster – the previous version of GenMaster. This version is now deprecated.

8.5.1 Running GenMasterEx

The GenMasterEx utility is started automatically by the installation process using the information you provided earlier in the process; see section *2.14*, *Configuring the master keys* and section *2.15*, *Configuring the startup user account*.

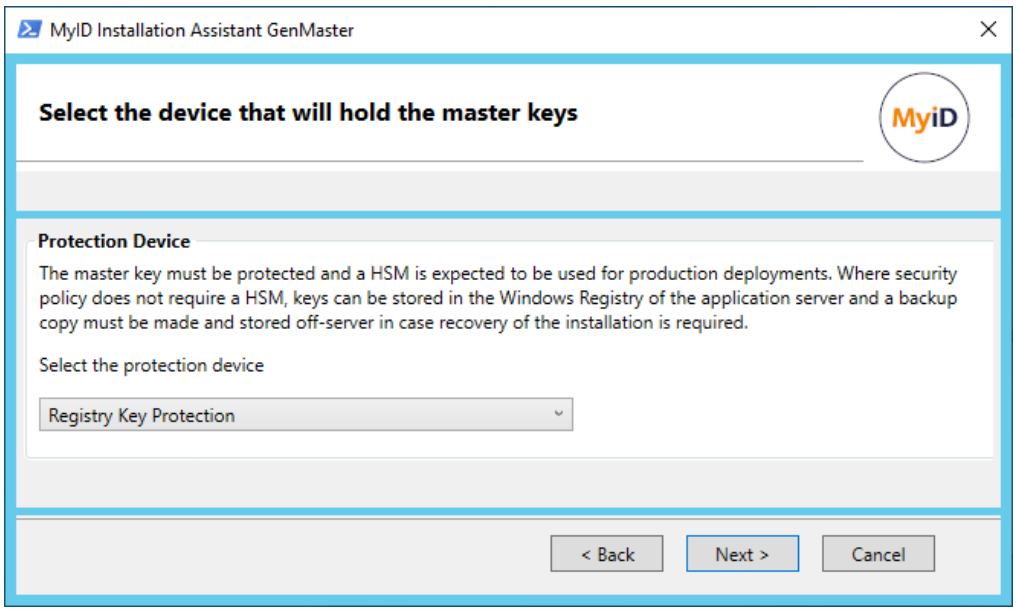
You can also run the utility as a standalone program. If you have already run the GenMasterEx utility as part of the installation, you can use the utility to reset the startup user password.

If the generation of master keys failed during the installation, you can run the utility as a standalone program to set your master keys.

To run GenMasterEx:

1. From the Windows Start menu, select **GenMasterEx**.

   If you have not already generated master keys for your installation, you can do so now.



Otherwise, you can use the utility only to change the startup user password.

2. To set the master keys, select the protection device from the drop-down list.

   You can choose from the following:

   - **Registry Key Protection** – the key is stored in the registry of the MyID application server.
   - **Thales LUNA HSM** – the key is generated and stored in the Thales Luna HSM.
   - **Entrust nShield HSM** – the key is generated and stored in the nShield HSM.

   Note: When you run the utility after installing MyID, only those features that have been detected by the installation process are listed in the drop-down list; for example, if you do not have Thales LUNA HSM software installed, you cannot select that HSM.

   To use the **Registry Key Protection** option:

   a. Select **Registry Key Protection** from the drop-down list.

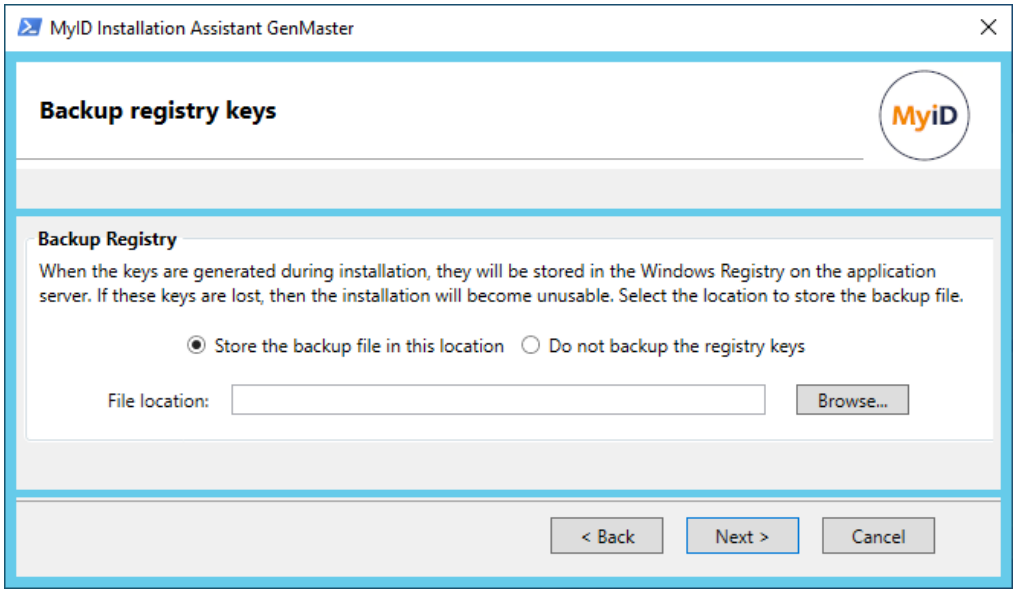
   b. Click **Next**.

   c. Select one of the following options:

      - **Store the backup file in this location** – click **Browse** and provide a location and filename for the backup registry file.

        You are recommended to save this backup file to a secure location.

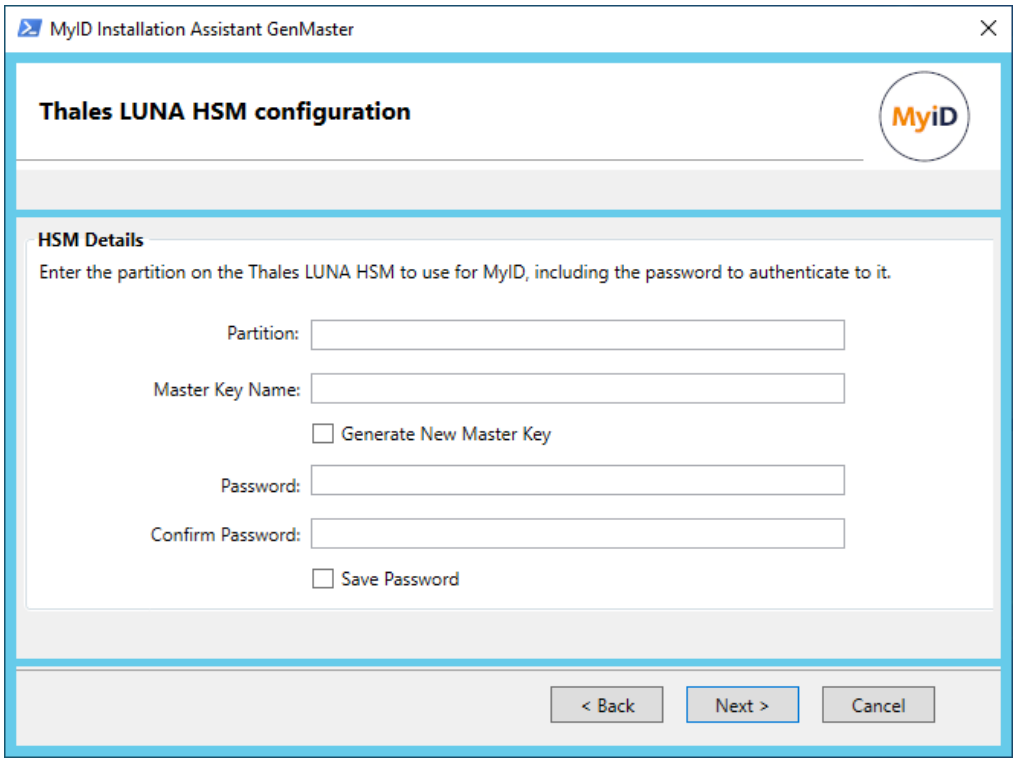
      - **Do not backup the registry keys** – skip the backup step.



To use the **Thales LUNA HSM** option:

a. Select **Thales LUNA HSM** from the drop-down list.

b. Click **Next**.



c. Provide the following information:

- **Partition** – select the partition that you want to use from the drop-down list.
- **Master Key Name** – type the name of the key you want to use.

If you have previously generated a master key in Keysafe (for instance if you are operating in FIPS140-1 level 3 mode), type the name of the existing key.

If you have not previously generated a master key in Keysafe, type the new name for the key you want to generate.

- **Generate New Master Key** – select this option if you have not previously generated a master key and you are not operating in FIPS140-1 level 3 mode.

  Note: There must not already be a key of this name installed on the HSM.

- **Password** – type the password for the partition; this is the HSM Partition Administrator password, not the crypto user.
- **Confirm Password** – confirm the password for the partition.
- **Save Password** – select this option to save the password.

  If you do not select the **Save Password** checkbox, you must enter the password in the **Card Manager Startup** dialog box after any machine reboot before the MyID keyserver can start.

  If you choose to save the password, the MyID keyserver starts automatically.

  Note: This password protection is in addition to the HSM client certificate access control, so even if a user obtains the password they cannot use the HSM remotely unless their client has a certificate and has been authorized.

  Important: If you choose to save the password, the password is saved in the registry on the MyID application server for the MyID COM+ user:

  `HKEY_CURRENT_USER\Software\Intercede\Edefice\MasterCard`

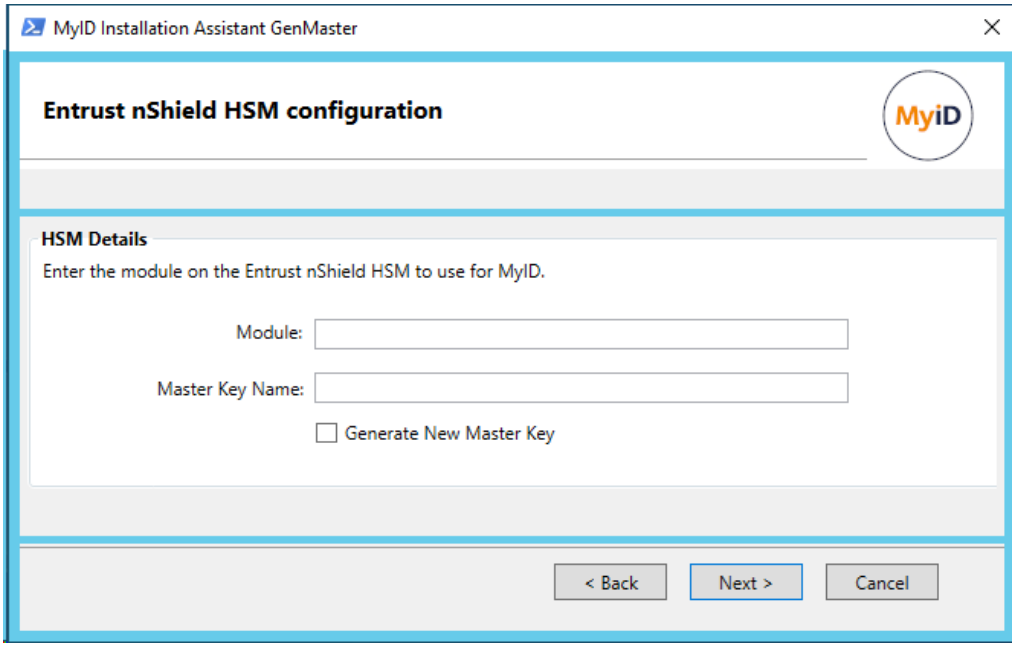
  The password is saved encrypted to the registry; see section *8.6, Setting the HSM PIN*.

For more information, see the ***Thales Luna HSM Integration Guide***.

To use the **Entrust nShield HSM** option:

a. Select **Entrust nShield HSM** from the drop-down list.

b. Click **Next**.



c. Provide the following information:

- **Module** – select the module you want to use from the drop-down list.
- **Master Key Name** – type the name of the key you want to use.

  If you have previously generated a master key in Keysafe (for instance if you are operating in FIPS140-1 level 3 mode), type the name of the existing key.

  If you have not previously generated a master key in Keysafe, type the new name for the key you want to generate.

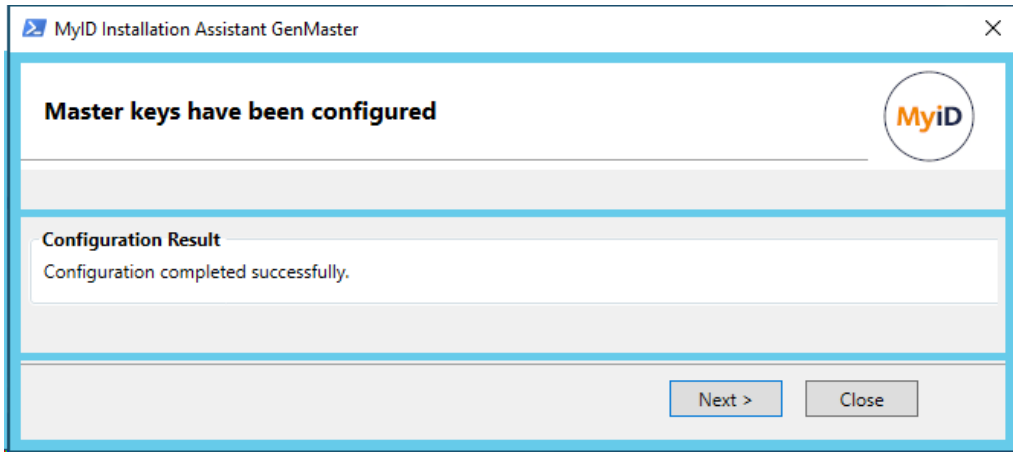
  Generate New Master Key – select this option if you have not previously generated a master key and you are not operating in FIPS140-1 level 3 mode.

  Note: There must not already be a key of this name installed on the HSM.

For more information, see the ***Entrust nShield HSM Integration Guide***.

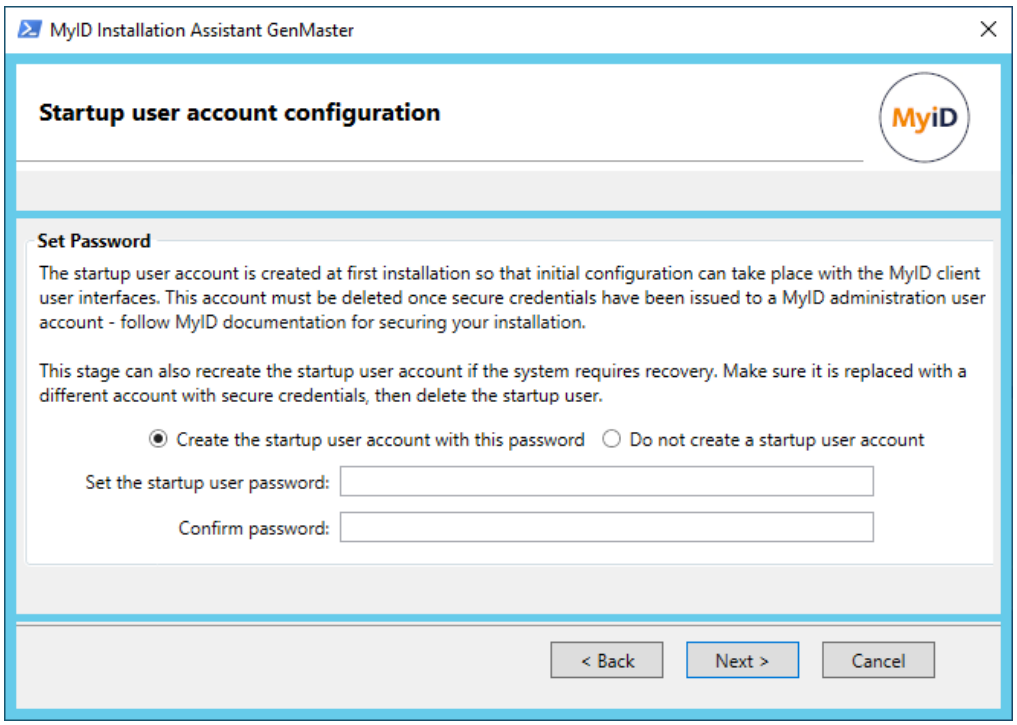
3. Click **Next**.

   The utility configures your system with the master keys.



4. Click **Next**.

   You can now set the startup user password.



5. Select one of the following options:

   - **Create the startup user account with this password** – type the new password and confirm it.
   - **Do not create a startup user account** – do not create a startup user account.

     Important: If you do not create a startup user account on a new system, you cannot access MyID.

   Note: Startup users are intended only for bootstrapping your system, and are not intended for long-term use. See the ***System Security Checklist*** document for details.

6. Click **Next**.

8.5.2 Running legacy GenMaster

The legacy GenMaster utility has been superseded by the GenMasterEx utility, which runs as part of the Installation Assistant installation process. If you have already run the GenMasterEx utility as part of Installation Assistant, you can use the legacy GenMaster utility to reset the startup user password or create new shared secrets.

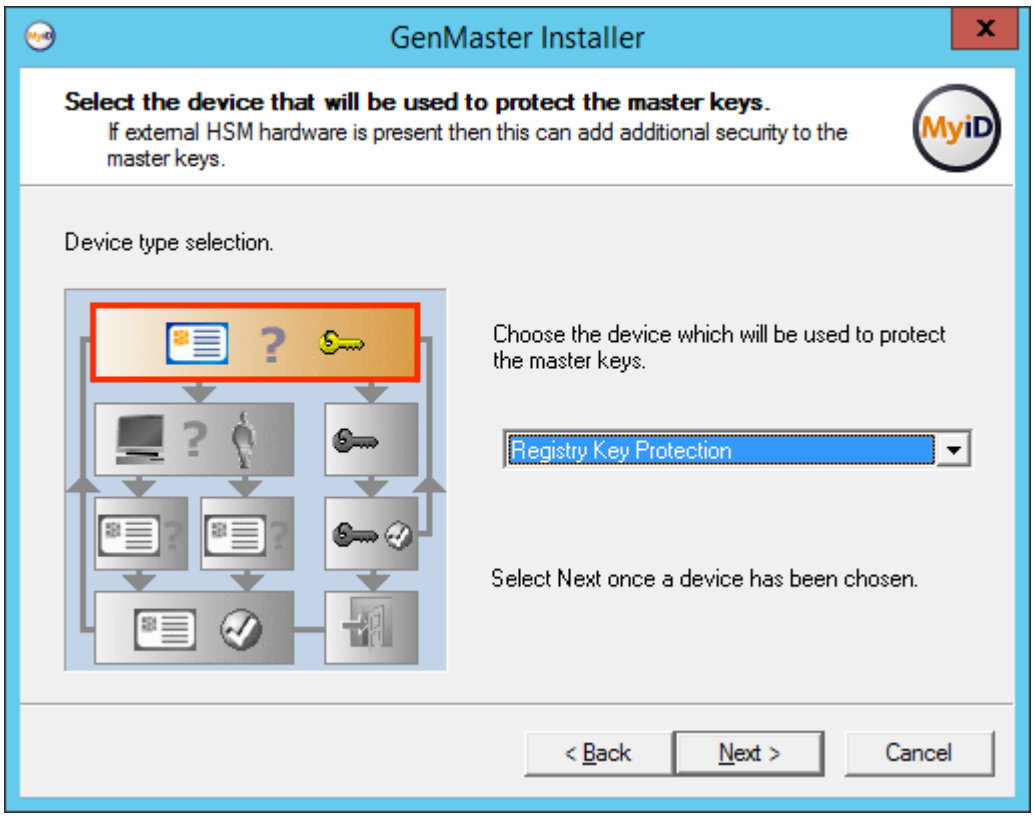
If the generation of master keys failed during the installation, you can run the either utility (GenMasterEx or GenMaster) to set your master keys.

To run the legacy GenMaster utility:

1. From the Windows Start menu, select **GenMaster**.
2. If prompted, enter an admin user name and password.

   The Welcome screen appears.

3. Click **Next**.
4. Select the method of securing the master keys.



Note: The master key is an AES256 key.

Select one of the following options:

- **Registry Key Protection** – the key is stored in the registry of the MyID application server.
- **nCipher HSM key protection** – the key is generated and stored in the nShield HSM.

  Note: Entrust nShield HSMs were previously known as nCipher nShield.
- **LUNA SA HSM key protection** – the key is generated and stored in the Thales Luna HSM.

Note: Entrust nShield and SafeNet Network (LUNA) HSMs are currently supported. Make sure you have set up your HSM according to the instructions in the relevant integration guide before installing MyID:

- ***Thales Luna HSM Integration Guide***
- ***Entrust nShield HSM Integration Guide***

If an HSM is *not* installed, a corresponding entry will not be displayed in the drop-down list.

If an HSM *is* installed and the corresponding entry is not in the drop-down list, then review the instructions in the relevant integration guide and ensure all steps have been followed.

In particular, for the **nCipher HSM**, check that the `CknFast.DLL` has been copied into the `Windows\System32` directory.

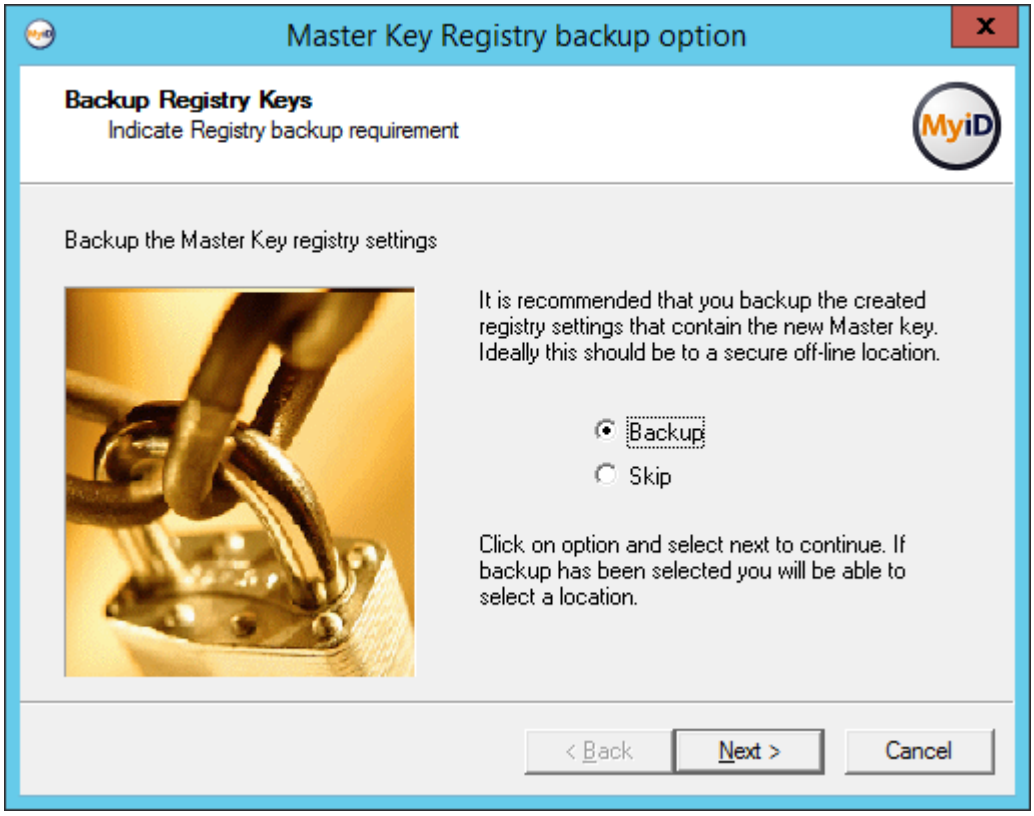
5. Set up the key protection.

To use the **Registry Key Protection** option:

a. Select **Registry Key Protection** from the drop-down list.

b. Click **Next**.

c. Create a backup of the registry key, or skip the backup step.

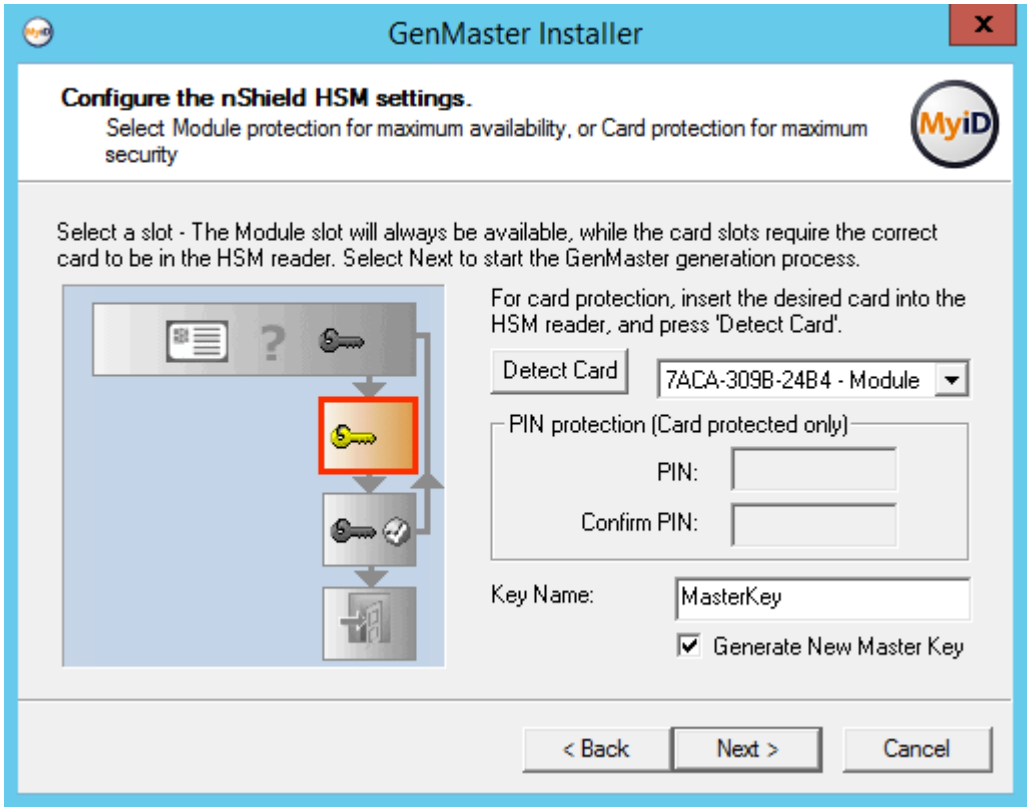


You are recommended to save this backup file to a secure location.

To use the **nCipher HSM key protection** option:

a. Select **nCipher HSM key protection** from the drop-down list.

b. Click **Next**.



c. If a card-set is to be used to protect the key ensure that it is in the HSM card reader. If the card does not appear in the combo box, click **Detect Card** after the card is inserted.

   - If the card-set is PIN protected, enter the PIN.
   - If the key is to be Module protected, select 'Module' in the combo-box.

d. If you have previously generated a master key in Keysafe (for instance if you are operating in FIPS140-1 level 3 mode):

   i. Enter the name of the key in the **Key Name** box.

   ii. Ensure that the **Generate New Master Key** box is cleared.

   If you have *not* previously generated a master key and you are not operating in FIPS140-1 level 3 mode:

   i. Enter a new name in the **Key Name** box.

   ii. Ensure the **Generate New Master Key** box is selected.

   Note: There must not already be a key of this name installed on the HSM.

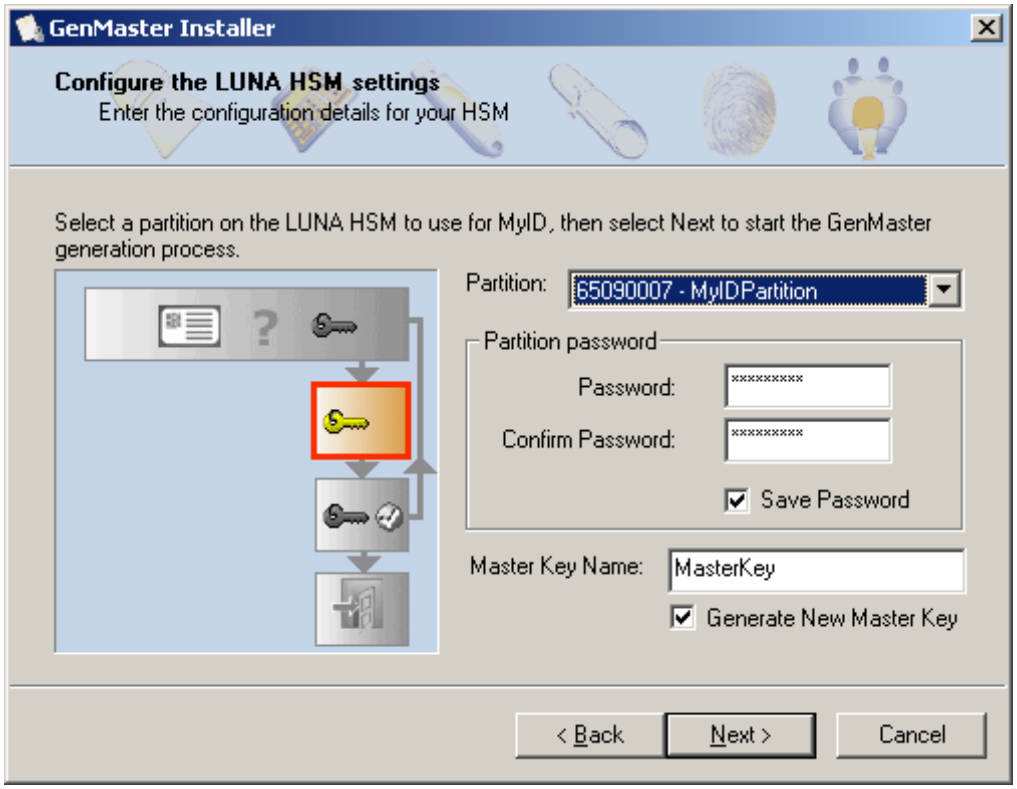
e. Click **Next** to generate the keys – this may take a few seconds.

   For more information, see the ***Entrust nShield HSM Integration Guide***.

To use the **LUNA SA HSM key protection** option:

a. Select **LUNA SA HSM key protection** from the drop-down list.

b. Click **Next**.



c. Select the partition you want to use for MyID from the drop down list.

d. Enter and confirm the password for the partition.

e. If you have previously generated a master key in Keysafe (for instance if you are operating in FIPS140-1 level 3 mode):

   i. Enter the name of the key in the **Master Key Name** box.

   ii. Ensure that the **Generate New Master Key** box is cleared.

   If you have *not* previously generated a master key and you are not operating in FIPS140-1 level 3 mode:

   i. Enter a new name in the **Master Key Name** box.

   ii. Ensure the **Generate New Master Key** box is selected.

   Note: There must not already be a key of this name installed on the HSM.

f. Luna SA HSMs require a password to connect to the partition; this is the HSM Partition Administrator password, not the crypto user.

   - If you do not select the **Save Password** checkbox, you will have to enter the password in the **Card Manager Startup** dialog box after any machine reboot before the MyID keyserver will start.
   - If you choose to save the password the MyID keyserver will start automatically.

   Note: This password protection is in addition to the HSM client certificate access control, so even if a user obtains the password they cannot use the HSM remotely unless their client has a certificate and has been authorized.

Important: If you choose to save the password, the password is saved in the registry on the MyID application server for the MyID COM+ user:

```
HKEY_CURRENT_USER\Software\Intercede\Edefice\MasterCard
```

The password is saved encrypted to the registry; see section *8.6, Setting the HSM PIN*.

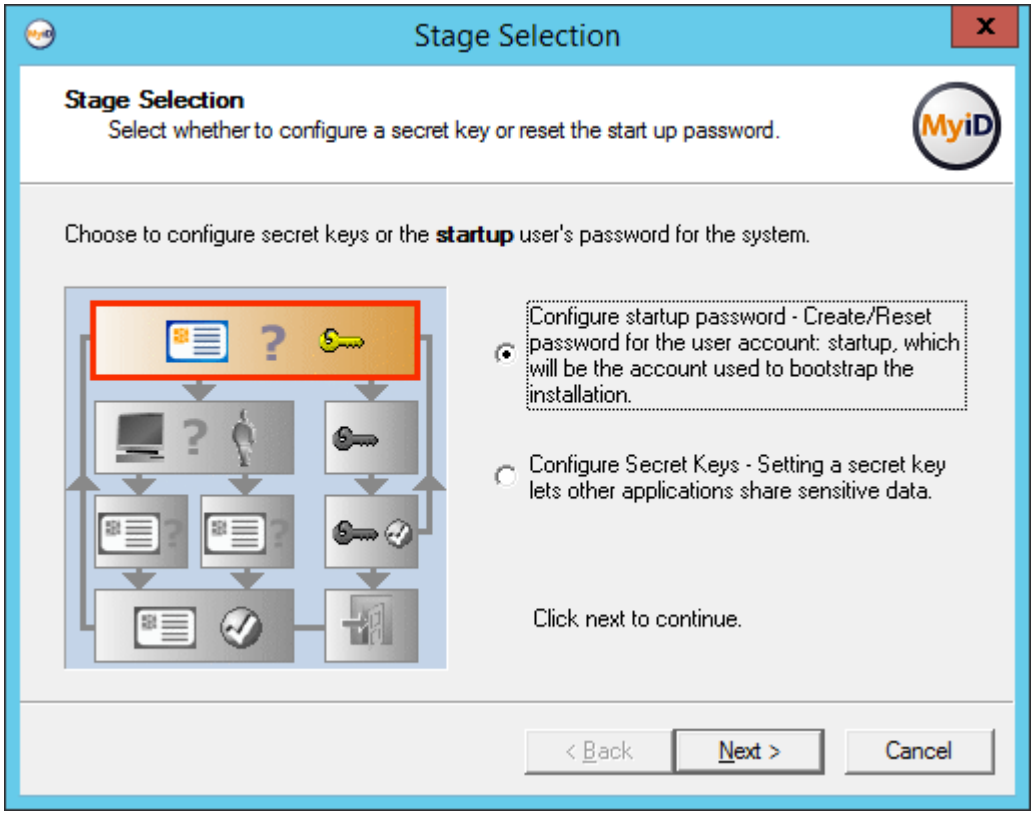
g. Click **Next** to generate the keys – this may take a few seconds.

For more information, see the ***Thales Luna HSM Integration Guide***.

6. You can now select one of the following options:

- **Configure Secret Keys** – this option allows you to set up secret keys that allow other applications to share sensitive data.
- **Configure startup password** – this option allows you to set the password for the startup user account.

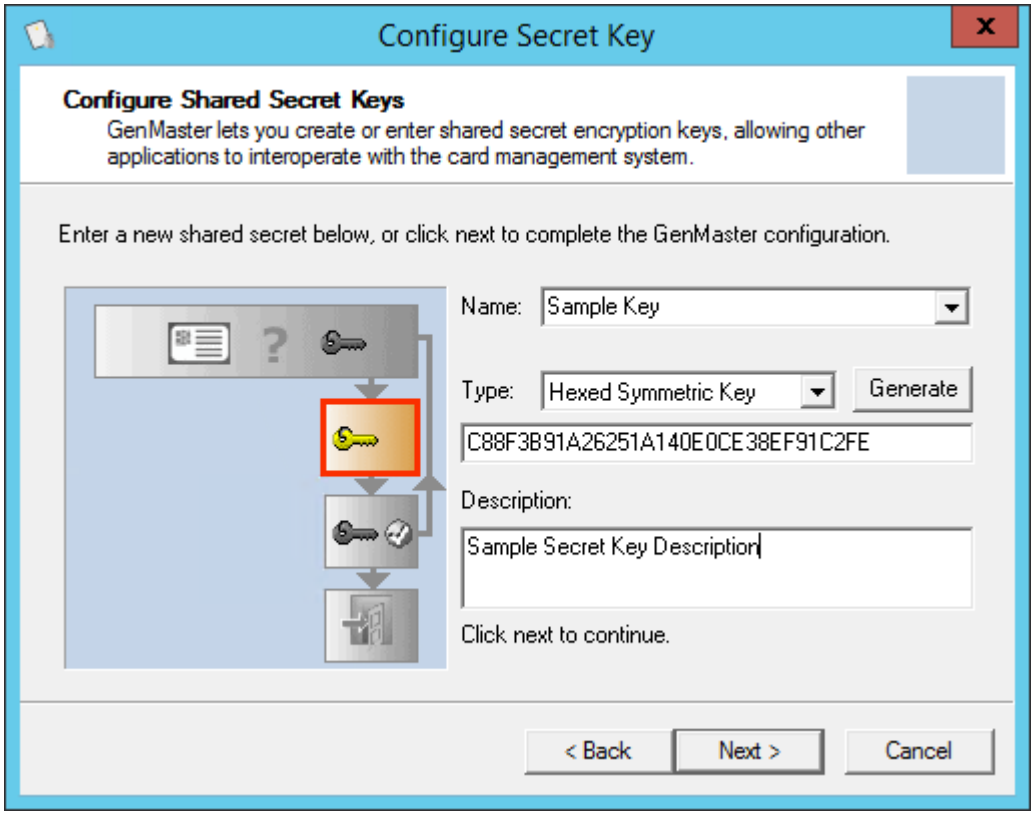
Note: You *must* set up a password for this account when you first install MyID or you will be unable to access the system. If you are upgrading an existing MyID system and already have a smart card or password user that you can use to access the system, you do not have to configure a startup password.



7. To configure secret keys:

a. Select **Configure Secret Keys**.

b. Click **Next**.

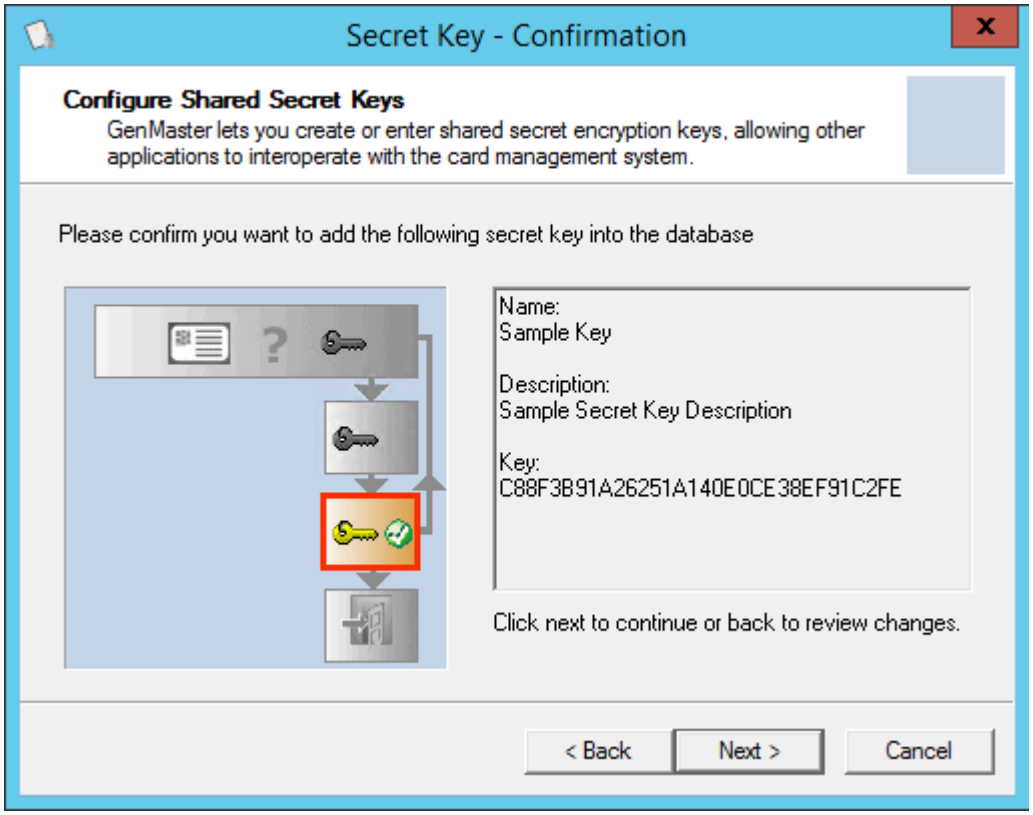


c. Enter the **Name** and **Description**.

d. Click **Generate**.

   This will populate the **Hexed Symmetric Key** box.

e. Click **Next** to continue.



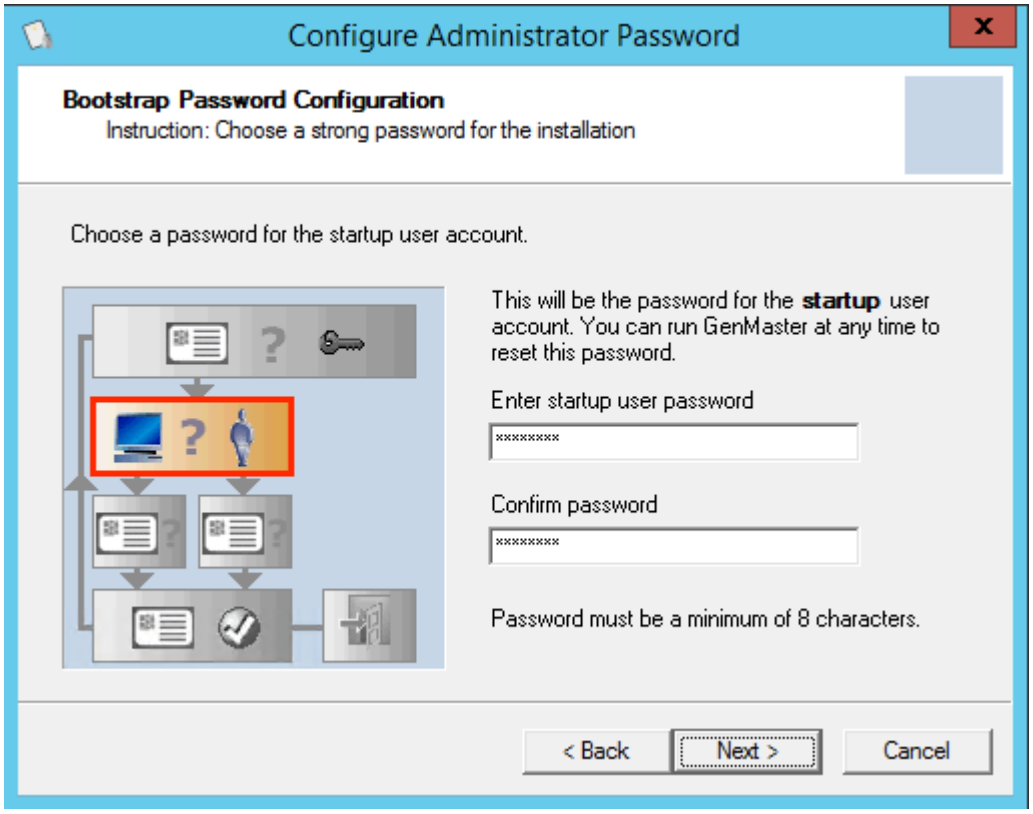
f. Click **Next** to confirm the details of the shared secret key.

8. To set the startup user password:

   Note: If you have upgraded from an earlier version of MyID, or have removed the startup account as part of locking down the installation, the startup user does not exist, and you will be unable to configure the startup password. If you need to recover this startup user account, you can use the Recover Startup User utility; see the *Recover Startup User* section in the ***Implementation Guide***.

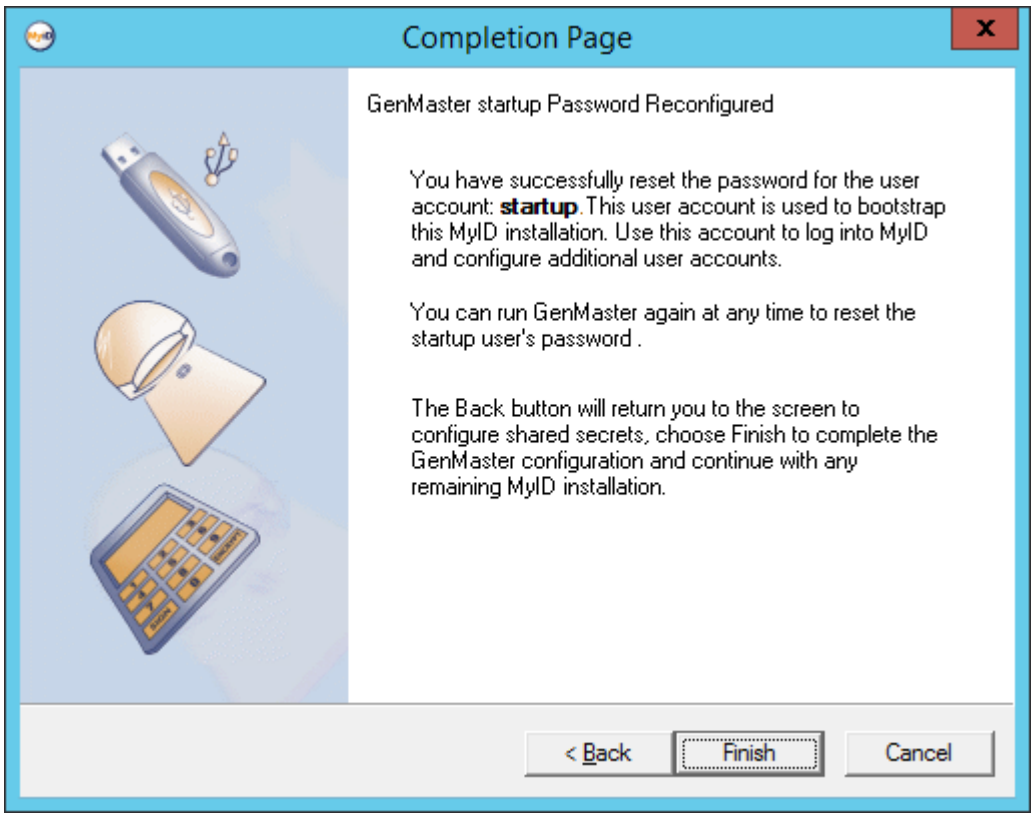
   a. Select **Configure startup password**.

   b. Click **Next**.



c. Type the password, and type it again to confirm it.

d. Click **Next**.



Note: If you enter the startup user password incorrectly three times, the startup user account becomes locked. To unlock the startup user account, run GenMaster again, and create a new password for the startup user.

9. Click **Finish**.

If you are running GenMaster as part of the initial installation, GenMaster returns control to the main MyID installation program, which completes its setup.

8.6 Setting the HSM PIN

When you save the PIN for a Thales HSM using GenMaster, it is stored in the registry of the application server in the following location for the MyID COM+ user:

`HKEY_CURRENT_USER\Software\Intercede\Edefice\MasterCard\LUNA\PINenc`

The PIN is stored using the Windows Data Protection API (DPAPI) which encrypts the PIN.

By default, PINs for nShield HSMs are not stored in the registry by GenMaster.

In previous versions of MyID, the PIN for Thales HSMs was stored in the `HKEY_LOCAL_MACHINE` part of the registry, and was not encrypted.

The SetHSMPIN utility allows you to:

- Change the PIN stored for an HSM.
- Store the PIN for an nShield HSM.
- Add the PIN to the registry of an additional application server.
- Move and encrypt the PIN for an upgraded system.
- Clear the HSM PIN from the registry.

To use the SetHSMPIN utility:

1. Log on to the MyID application server as the MyID COM+ user.

   Note: If you have multiple application servers, you must run the utility on each server.

2. Navigate to the MyID utilities folder.

   By default, this is:

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

3. To set the PIN, run the utility using the following command line:

   ```
   SetHSMPIN <pin>
   ```

   where:

   - `<pin>` – the PIN for the HSM.

   For example:

   ```
   SetHSMPIN 123456
   ```

   Note: If you are running the utility from a PowerShell prompt, you must escape any $ characters using the ` symbol. For example, if the PIN is `123$567`, use the following:

   ```
   SetHSMPIN 123`$567
   ```

4. To clear the PIN, run the utility using the following command line:

   ```
   SetHSMPIN /ClearPIN
   ```

   This removes the HSM PIN from the registry. If you have cleared the PIN, you must either set it again, or set it temporarily using the Startup utility; see the *MyID startup* section in the ***Advanced Configuration Guide***.

5. If prompted, enter an admin user name and password.

9 Updating MyID

Intercede may supply you with an update to your MyID system. If you have already installed MyID, you must install this update. If you have not yet installed MyID, you must first install MyID, then install this update.

The update installation program is located in the same folder as the main MyID installation program, and has a name similar to:

```
MyIDServer-12.4.1_update.exe
```

If there is an appropriate update in this folder, it is listed in the Package Manager in the MyID Installation Assistant; see section *2.6*, *The Installation Package Manager*.

If you do not have an update installation program in the same folder as the main installation program, there are no updates available for your version of MyID.

9.1 Running the update installation program

You must install the update on all of your MyID servers. The MyID Installation Assistant automatically updates the same components that you originally installed using the main MyID installation program – you do not have to select the components to update.

For example, if you have a split deployment across three servers, with a separate application server, web server, and database server, and you originally ran the main MyID installation program first on the application server to install the application components and the database components, and then on the web server to install the web server components and web services, you must apply the update twice – once on the application server to update the application components and the database, and once on the web server to update the web server components and the web services.

Important: You *must* prepare the installation folder before you start the update process. See section *2.2.4*, *Upgrading or updating the MyID Installation Assistant*.

To apply the update to your system:

1. Back up your MyID system, including the database.
2. Log on to the MyID server using the installation account.
3. Uninstall any MyID hotfixes or patches you have applied.

   Note: You may have been supplied with separate hotfixes, patches, or other software changes for your installation that have now been incorporated into this product release. It is important that you uninstall these items *before* you install any update or upgrade. If you uninstall them *after* installing the update, you may cause your system to experience errors or stop operating. See the *General bug fixes and improvements* section in the ***Release Notes*** for a list of the items that have been incorporated into the current release, if any; if you have been issued any *additional* items that are not incorporated in the release, you must uninstall them before installing the update, but then contact customer support quoting reference SUP-337 before attempting to re-apply them after installing the update.
4. Close all application windows.
5. Add the update installation program to the `Installer` folder.

   See section *2.6.1*, *Adding software to the package manager*.

6. Run the MyID Installation Assistant.

   You are recommended to carry out the tests against your server when applying the update to ensure that your system still meets all the requirements.

   See section *2.24*, *Applying an update* for details.

9.1.1 Installation log

For information on viewing the installation log, see section *11.7*, *Checking the installation log*.

9.1.2 COM surrogate error

You may see an error when installing the update similar to the following:

```
The following applications are using files that need to be updated by this
setup. Close these applications and click Retry to continue.

COM Surrogate
```

This error occurs when the installation cannot replace a component because it is in use. To resolve this issue, on the MyID application server:

1. Open Windows Component Services.
2. Expand **Component Services > Computers > My Computer > COM+ Applications**.
3. Select each component that is running under the MyID COM user.

   The user is listed in the **Account** column.
4. Right-click, then from the pop-up menu click **Shut down**.
5. On the installation program dialog, click **Retry**.

9.1.3 .NET files location

If you see an error when running MyID that the MyID IIS, COM, or web service user does not have permission to write to the temporary .NET files location, you must add write permissions for the MyID IIS, COM, and web service users to the appropriate folder; for example:

```
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Temporary ASP.NET Files\
```

9.2 Uninstalling updates

It is not possible to uninstall all updates; if your update cannot be uninstalled, to remove the changes supplied in the update you must uninstall MyID, then reinstall the base version of MyID.

Note: Uninstalling the server components of an update does not remove the database changes. To remove the changes to the main or archive database, you must restore the database from the backup you made before installing the update. If you do this, any data added since you installed the update (for example, data imports or card requests) will be lost. For more information, contact customer support, quoting reference SUP-147.

If you want to uninstall an update, you must uninstall it from all of your MyID servers.

To uninstall an update:

1. On the MyID server where you installed the update, open the Windows Control Panel.
   a. Open the **Programs and Features** option.
   b. Click **View installed updates**.

c. Right-click the MyID update, then from the pop-up menu select **Uninstall**.

   Note: If there is no **Uninstall** option available, it is not possible to uninstall this update.

d. Follow the on-screen instructions.

2. After uninstalling the update, you may have to uninstall some or all of your COM proxies from the web server, and reinstall new versions. Intercede will provide a list of the affected components.
3. If the installation program does not require the MyID web server to be restarted, in Internet Information Services (IIS) Manager on the MyID web server, you must recycle the application pools used for MyID.
4. If the installation program does not require the MyID application server to be restarted, you must restart the Edefice_BOL component.
   a. On the MyID application server, open Windows Component Services.
   b. Expand **Component Services > Computers > My Computer > COM+ Applications**.
   c. Right-click **Edefice_BOL**, then from the pop-up menu click **Shut down**.

      The component will restart automatically the next time it is needed.
5. On each client, clear the browsing history in the Windows Internet Options dialog.

   Note: Make sure you deselect the **Preserve Favorites website data** option, if it is available.

10 Installing MyID clients

MyID supports the following clients:

- MyID Operator Client

  This web-browser client does not require any additional software to be installed for basic operations, but does support the use of the MyID Client Service, which allows the browser to access smart cards, capture images, issue soft certificates, print mailing documents, or access features of MyID Desktop or the Self-Service App
- MyID Desktop
- Self-Service App
- Self-Service Kiosk
- MyID Client for Mac
- MyID Client for Windows

For information on installing the Self-Service App, Self-Service Kiosk, the MyID Client for Mac, or the MyID Client for Windows, see the following installation guides:

- ***Self-Service App***
- ***Self-Service Kiosk***
- ***MyID Client for Mac***
- ***MyID Client for Windows***

MyID also supports a credential unlock provider that allows you to unlock PIV cards at the Windows logon prompt.

This chapter contains information on installing and configuring MyID Desktop, the MyID Client Service, and the credential unlock provider.

Before you start to install MyID Desktop, refer to section *5.2*, *Client workstation* for details of the hardware and software requirements, and section *10.1*, *Configuring Internet Options* for details of configuring your client's Internet Options to support MyID Desktop.

Note: You are recommended to install client software using a software distribution system such as group policy. In some circumstances, for example if you unzip software on a remote drive then copy to the local PC for installation, you may see Windows Defender warnings; while you can safely ignore the warnings and continue to install the software, using a group policy to install your client software prevents this issue.

10.1 Configuring Internet Options

Microsoft have announced that Internet Explorer is being retired and will not be available on future Windows versions, including updates to Windows 10. MyID no longer has dependencies on Internet Explorer; however there are still some circumstances where Windows Internet Options configuration is still required.

10.1.1 ActiveX support for embedded web pages

MyID Desktop uses embedded web pages for some basic features; for example, the **Edit Roles** workflow. You must make sure that the following options are enabled in the Internet Options on the client PC:

- **Run ActiveX controls and plugins**
- **Script ActiveX controls marked safe for scripting**

You can access these settings from the **Security** tab of the Internet Options control panel. By default, these options are enabled on the **Medium-high** security settings, but are disabled on the **High** security setting. If you are using the **High** security setting, you must set a custom level that enables these options.

10.1.2 Additional configuration for specific features

Some features of MyID Desktop require additional configuration.

The table below lists the affected areas, and describes the configuration required and alternatives available that do not require the configuration changes specified. The affected features are used only as part of MyID Desktop – other MyID clients for Windows (the MyID Operator Client, the Self-Service App, and the Self-Service Kiosk) do not make use of these technologies. If you do not use the affected features, then you do not need to make the relevant configuration changes to the Internet Options.

MyID Desktop Feature	Internet Options Configuration	Alternative (Internet Options not required)
Exporting MI Reports to Microsoft Excel	• Adding the MyID website to the Trusted sites or Local intranet group • Disabling the pop-up blocker • Exceptions (**Initialize and script ActiveX controls not marked as safe for scripting**)	Download report results as CSV from the MyID Operator Client and open in Excel.
Collecting a device using the **Collect My Card** workflow	• Adding the MyID website to the Trusted sites or Local intranet group • Disabling the pop-up blocker	
Image Capture using the **Edit Person** workflow	• Adding the MyID website to the Trusted sites or Local intranet group • Disabling the pop-up blocker • Exceptions (**Initialize and script ActiveX controls not marked as safe for scripting** and **Only allow approved domains to use ActiveX without prompt**)	Image Capture using the Edit Person or PIV applicant editing screens in the MyID Operator Client.
Print Mailing Document using Microsoft Word Mail Merge	• Adding the MyID website to the Trusted sites or Local intranet group • Disabling the pop-up blocker • Exceptions (**Initialize and script ActiveX controls not marked as safe for scripting**)	None
Issue Card	• Adding the MyID website to the Trusted sites or Local intranet group • Disabling the pop-up blocker	Request a device using the MyID Operator Client, then use **Collect Card** in MyID Desktop.
Card Layout Editor (layout preview)	• Adding the MyID website to the Trusted sites or Local intranet group • Disabling the pop-up blocker	None

MyID Desktop Feature	Internet Options Configuration	Alternative (Internet Options not required)
Print Badge (layout preview)	• Adding the MyID website to the Trusted sites or Local intranet group • Disabling the pop-up blocker	None
Fingerprint verification during the **Update Card** workflow	• Adding the MyID website to the Trusted sites or Local intranet group • Disabling the pop-up blocker	Self-Service App
Fingerprint verification during the **Identify Card** workflow	• Adding the MyID website to the Trusted sites or Local intranet group • Disabling the pop-up blocker • Exceptions (**Initialize and script ActiveX controls not marked as safe for scripting**)	None

10.1.3 Adding the MyID website to the Trusted sites or Local intranet group

SIU references: SIU-144, SIU-145.

To add the MyID website to the Trusted sites or Local intranet security group in the Internet Options:

1. Double-click **Internet Options** in the Control Panel.
2. Click the **Security** tab.
3. Add the MyID site to the list of **Trusted sites** or **Local intranet**:
   a. Click the **Trusted Sites** or **Local intranet** icon, then click **Sites**.
   b. For the **Local intranet zone**, click **Advanced**.
   c. Add the web address of the MyID Web Server to the list of sites.

      If the MyID website does not use https, make sure the **Require server verification (https:) for all sites in this zone** option is not selected.

      Note: Do not use wildcards in the **Trusted Sites** list. Also, make sure you use the same URL as you are going to use when you access MyID; for example, do not add the IP address to the list if you are using the domain name to access MyID. Make sure you use the correct protocol – http or https.
   d. Click **Close**.
4. Click **OK**.

You can also set these options using Group Policies rather than setting up each client PC individually.

10.1.4 Disabling the pop-up blocker

SIU reference: SIU-146.

MyID requires the ability to display pop-up windows.

To disable the pop-up blocker for the MyID website:

1. Double-click **Internet Options** in the Control Panel.
2. Click the **Privacy** tab.
3. If the **Turn on Pop-up Blocker** option is selected, click **Settings**.
4. Type the address of the MyID Web Server and click **Add**.
5. Click **Close**, then click **OK**.

10.1.5 Exceptions

SIU references: SIU-147, SIU-148.

This version of the client components allows you to use MyID website using the default level of security for the Trusted sites or Local Intranet zones. However, some features do not operate correctly with the default settings.

If you intend to use the following features, you must carry out some additional configuration:

- Exporting MI Reports to Excel – requires the **Initialize and script ActiveX controls not marked as safe for scripting** option in Internet Options.
- Mail Merge – requires the **Initialize and script ActiveX controls not marked as safe for scripting** option in Internet Options.
- Image Capture – requires the **Initialize and script ActiveX controls not marked as safe for scripting** option in Internet Options. You must also disable **Only allow approved domains to use ActiveX without prompt**.
- Fingerprint verification in the **Identify Card** workflow – requires the **Initialize and script ActiveX controls not marked as safe for scripting** option in Internet Options.

Note: For some customized systems, you may experience problems when printing from MyID. If you experience problems printing (for example, if the list of printers does not appear), set the **Initialize and script ActiveX controls not marked as safe for scripting** option in Internet Options.

10.1.6 Performance improvements for client PCs without internet access

SIU reference: SIU-149.

If your client PC has no internet access, you may experience a delay when performing some actions within MyID for the first time in a browser session. This is because Windows is attempting to verify the certificate that was used to sign the MyID .NET components, or checking Windows Update. You may want to consider disabling these checks or allowing internet access. Contact your network administrator.

To disable the certificate revocation check:

1. Double-click **Internet Options** in the Control Panel.
2. Click the **Advanced** tab.
3. In the Security section, disable the **Check for publisher's certificate revocation** option.

   Note: This setting affects the security of all .NET components on the client PC that are accessed by browser. Do not set this option if your PC has internet access.
4. Click **Close**, then click **OK**.

10.1.7 Compatibility mode on the web server

SIU reference: SIU-295.

The installation program sets up the compatibility mode on the web server to be appropriate for MyID. You may experience problems if another system changes this mode. To ensure that the web server is correctly configured, after installing MyID check the following:

1. In Internet Information Services (IIS) Manager, select **Default Web Site > MyID**.
2. Double-click **HTTP Response Headers**.
3. Ensure that the **X-UA-Compatible** option is set to the following:

   `IE=edge`

10.2 Installing MyID Desktop

SIU reference: SIU-140.

Note: MyID Desktop version 2.0.1000.1 and later can be used only against a MyID server version 10.6 or later. If the versions are not compatible, a message similar to the following appears:

```
MyID Desktop is incompatible with MyID Server.
```

The MyID Desktop installation program is located in the MyID release in the `MyID Clients\Desktop Client` folder.

The installation program is provided as a `.msi` file that you can install directly or run from a command-line to install silently on each client PC.

Note: Intercede also provides MSIX versions of the installation programs for MyID Desktop, the Self-Service App, and the MyID Client Service. These are intended for an administrator to create an installation package that combines all of the necessary client software and administrator-controlled configuration. See the ***MyID Client MSIX Installation Guide*** for details of working with these installation programs.

Note: You must have .NET Framework 4.8 installed on each client PC on which you want to install MyID Desktop. MyID is developed and tested using .NET Framework 4.8; if you need to use a later version of the .NET framework, contact customer support quoting reference SUP-283.

To install MyID Desktop:

1. Copy the installation program to a local drive.

   If you do not run the installation program from a local drive, you may experience problems with the application running slowly due to certificate checks.

2. Run the installation program, then click **Next**.

3. Select the destination location, then click **Next**.

   By default, MyID Desktop installs to the following folder:

   ```
   C:\Program Files (x86)\Intercede\
   ```

4. Select the desired shortcuts to be installed.

   By default, a desktop shortcut is created.

5. Click **Next**.

6. In the **Server URL** box, type the location of the server on which the MyID web services are installed.

   For example:

   ```
   https://myserver
   ```

   Note: Make sure you use the correct protocol: `http` or `https`. Use `https` if you have configured SSL/TLS. See section *10.3.4*, *One-way SSL/TLS* and section *10.3.5*, *Two-way SSL/TLS* for details.

   If you want to configure MyID Desktop to be able to connect to multiple servers (for example, if you have a test server and a production server) you can specify multiple servers in the **Server URL** box separated by commas; for example:

   ```
   https://productionserver, https://testserver, https://testserver2
   ```

   By default, MyID Desktop connects to the first server in this list. If you want to connect to any of the other servers, you can specify the server address on the command line using the `/server` option; see section *10.4*, *Launching MyID Desktop* for details.

7. In the **Client Certificate Issuer DN (for 2 way TLS)** box, type the Issuer DN of the client-side certificate used to authenticate the client to the server for two-way SSL/TLS.

   This is optional.

8. Click **Next**.

9. Click **Install**.

10. When the installer has completed, click **Finish**.

To install silently on a client PC, you can use the `.msi` installer with the following command-line parameters:

```
msiexec /i "<msi path>" /lv <LogFile> /q SSA_SERVERNAME=<ServerURL>
SSLCERTIFICATEDN=<sslcertdn> INSTALLDIR=<InstallationFolder>
```

where:

- `<msi path>` is the path to the .msi file.
- `<LogFile>` is the name of the file to which you want to write a verbose log. This is optional.
- `<ServerURL>` is the Server URL; for example `https://webserver2.example.com/`
- `<sslcertdn>` is the Issuer DN of the client certificate used to authenticate the client to the server for two-way SSL. This is optional.
- `<InstallationFolder>` is the name of the folder to which you want to install the application. This is optional.

Note: The installation program requires administrative privileges. Open the command prompt using **Run as administrator**.

Note: Do not put a space character on either side of the = signs in the command line.

For example:

```
msiexec /i "C:\install\<installer>.msi" /lv msilog.txt /q SSA_
SERVERNAME=https://webserver2.example.com INSTALLDIR="C:\temp\desktop"
```

Note: Installing MyID Desktop automatically installs the MyID Client Components for its own use. If you intend to run any other MyID clients that use the Client Components on the same PC as MyID Desktop, you may experience problems. If you uninstall the Client Components after installing MyID Desktop, you will have to reinstall MyID Desktop to restore its own copies of the Client Components.

For more information, contact customer support, quoting reference SUP-139.

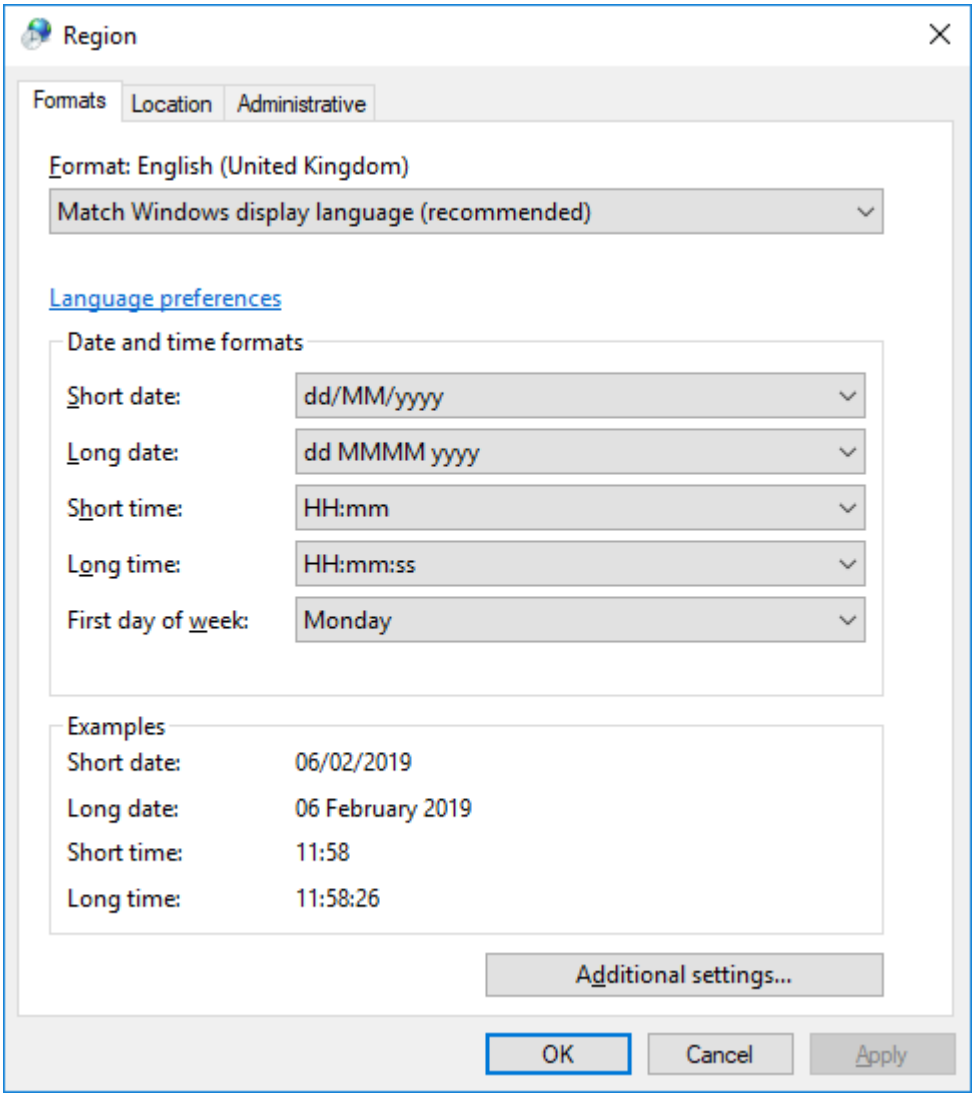
10.3 Configuring MyID Desktop

10.3.1 Specifying the language for MyID Desktop

MyID Desktop uses the language setting of the client PC's Windows installation to determine the language to use.

Note: MyID differentiates between English (United States) and English (United Kingdom).

In the Windows Control Panel, under **Clock and Region** select the **Change date, time or number formats** option, then from the **Format** drop-down list select the language in which you want to display the user interface.



Note: It is possible to override this setting for the MyID workflows that are displayed using an embedded web browser control – make sure the setting in **Internet Options > General tab > Languages** matches the language set for Windows.

If you need to set the language to a different one from the language specified in Windows, contact customer support quoting reference SUP-138.

10.3.2 Communication between MyID Desktop and the MyID server

SIU references: SIU-248, SIU-249.

To allow your clients to communicate with the MyID server, your PC must be able to communicate with the URLs of the MyID 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.

10.3.3 Server location

SIU reference: SIU-250.

MyID Desktop is configured to communicate with the MyID Web Services server when you install the MyID Desktop application. If you want to change the server, you can edit the configuration file.

Note: You must have the appropriate permissions to edit this file.

To edit the configuration file:

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

   `C:\Program Files\Intercede\MyIDDesktop\`

   On a 64-bit system, this is:

   `C:\Program Files (x86)\Intercede\MyIDDesktop\`

2. Using a text editor, open the `MyIDDesktop.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="Server" value="http://myserver.example.com"></add>
   ```

   For example:

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

   If you want to configure MyID Desktop to be able to connect to multiple servers (for example, if you have a test server and a production server) you can specify multiple servers.

   For example:

   ```
   <add key="Server" value="https://productionserver, https://testserver,
   https://testserver2"></add>
   ```

   By default, MyID Desktop connects to the first server in this list. If you want to connect to any of the other servers, you can specify the server address on the command line using the `/server` option; see section *10.4.1, Launching MyID Desktop with a specific server* for details.

4. Save the configuration file.

The server URL must have the following format:

- Protocol – `http://` or `https://`

  Note: Make sure you use the correct protocol: `http` or `https`. Use `https` if you have configured SSL/TLS.

- Server address – the address of the server. For example:

  `myserver.example.com`

For example:

`https://myserver.example.com`

10.3.4 One-way SSL/TLS

You must configure IIS to use SSL/TLS for your production environment. You can either use one-way (standard) SSL/TLS or two-way (client authenticated) SSL/TLS.

To configure MyID Desktop to use SSL/TLS for its communications with the MyID Web Services server, you must ensure that the client trusts the server SSL certificate. This requires that the issuing root CA is a trusted certificate, and that CRL/OCSP locations are accessible from the client for the entire certificate chain.

10.3.5 Two-way SSL/TLS

MyID Desktop supports two-way SSL/TLS.

10.3.5.1 Configuring MyID for 2-way SSL/TLS

There are incompatibility issues using MyID Desktop with SSL 2.0; however, SSL 2.0 is an old protocol and for security reasons should be disabled. If you do not disable SSL 2.0, you may experience errors when attempting to access certain workflows.

SSL has been superseded by TLS, which is supported by MyID Desktop. For more information on disabling old versions of SSL/TLS, see the ***System Security Checklist***.

To set up the web server, you can use the `Configure2WaySSL.ps1` PowerShell script; this is installed on the MyID web server in the `Utilities` folder.

The script takes the following optional parameters:

- `webSiteName` – This is the name of the website that is hosting the MyID web service. By default, this is:

  `Default Web Site`

- `installationPath` – This is the folder where MyID was installed. By default, this is:

  `C:\Program Files\Intercede\MyID`

  If you do not specify this parameter, the script reads the installation folder from the registry.

- `enable` – If this is `$true` it will enable 2-way SSL/TLS; if it is `$false` it will disable 2-way SSL/TLS. The default is `$true`.

When enabled, the script ensures that Anonymous Authentication with the Require SSL and Require Client Certificate options is set for the MyID website and web services:

- MyIDDataSource
- MyIDProcessDriver
- MyID
- MyIDEnroll
- MyIDWebService
- upimages

The script will also turn off SSL for the `images` folder in MyIDDataSource, and `GetImage.aspx` and `WindowsAuth.asmx` in MyIDProcessDriver.

When disabled, the script turns off SSL/TLS for the MyID website and web services.

Warning: If you run the `Configure2WaySSL.ps1` PowerShell script, this enables 2-way SSL/TLS for the MyID Operator Client website; this is not supported for the MyID Operator Client or the MyID Client Service. Do not use 2-way SSL/TLS if you intend to use the MyID Operator Client.

10.3.5.2 Setting up SSL/TLS on the client

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

Note: MyID Desktop does not support two-way SSL/TLS using a certificate stored on a smart card.

To use two-way SSL/TLS 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:

   `MyIDDesktop.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:

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

Note: If you copy the serial number from the **Details** tab of the certificate properties dialog, you may inadvertently copy a non-printing character at the start of the serial number. You must make sure that you delete this character from the MyID Desktop command line. (Position the cursor before the : in the command line. Press the right-cursor key once. The cursor appears after the colon. Press the right-cursor key again. If the cursor does not move to after the first number in the serial number, there is a non-printing character present; press the Backspace key to delete it.)

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.

Note: When you start a legacy web-based workflow for the first time, MyID prompts you again for a certificate, and displays a list of the available certificates; this is because these workflows use an embedded browser. If you select the wrong certificate, you must restart MyID Desktop and try again.

10.3.5.3 Specifying two-way SSL in the configuration file

As an alternative to specifying `/ssl` and `/sslsn` on the command line each time you run MyID Desktop (for example, if you are launching MyID Desktop using a hyperlink, and therefore cannot specify `/ssl` or `/sslsn`) you can add settings to the `<appSettings>` node of the configuration file:

To edit the configuration file:

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

   `C:\Program Files\Intercede\MyIDDesktop\`

   On a 64-bit system, this is:

   `C:\Program Files (x86)\Intercede\MyIDDesktop\`

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

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

3. In the `<appSettings>` node, add the following lines:

   ```
   <add key="TwoWaySSL" value="true"/>
   ```

   ```
   <add key="SSLCertificateSN" value="YourCertificateSerialNumber"/>
   ```

   If you want to stop using two-way SSL, you can set the `TwoWaySSL` value to `false` or remove the line. If you set this value to false, but include `/ssl` on the command line, the command line takes precedence, and MyID Desktop attempts to use SSL. If you specify a value for `SSLCertificateSN` but also include `/sslsn` on the command line, the command line takes precedence.

4. Save the configuration file.

10.3.5.4 Setting up client certificate hinting

If you have 2-way SSL/TLS set up, and start MyID with a smart card inserted, you may find that MyID is unresponsive until you remove the smart card from the reader. This is because more than one certificate meeting the client certificate requirements is available.

As a workaround, you can set up client certificate hinting on the MyID web server. This ensures that MyID looks for certificates from the correct certificate authority, and ignores the certificates issued to the smart card.

Note: This requires that your smart card certificates are issued from a different CA to your SSL/TLS client certificate.

To set up client certificate hinting:

1. On the MyID web server, run the Microsoft Management Console (mmc).

   Note: If you have multiple MyID web servers, you must carry out this procedure on each one.

2. Add the **Certificates** snapin for the **Computer account**.

3. Add the CA certificate that issued the client authentication certificate to the **Client Authentication Issuers** certificate store.
4. Set the following registry DWORD value to 1:

   ```
   HKEY_LOCAL_
   MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Sen
   dTrustedIssuerList
   ```

   If the registry key does not exist, you must create it.
5. Open a Windows command prompt as an administrator, and run the following command:

   ```
   netsh http show sslcert
   ```
6. Take a note of the `ApplicationID` and `certhash` it returns.
7. In the administrator command prompt, run the following commands, substituting in your own values for the `ApplicationID` and `certhash`:

   ```
   netsh http delete sslcert ipport=0.0.0.0:443
   netsh http add sslcert ipport=0.0.0.0:443
   certhash=f27cc86a95570505dd5cffcbd670e65091f14620
   appid={4dc3e181-e14b-4a21-b022-59fc669b0914}
   sslctlstorename=ClientAuthIssuer clientcertnegotiation=enable
   ```
8. Restart IIS.
9. Ensure the website is set to require SSL and a client certificate.

10.3.6 Logging

You can set up your MyID Desktop application to write debug information to a log file. You may need to provide this information to Intercede customer support.

See the *Windows clients* section in the ***Configuring Logging*** guide for details.

10.3.7 Troubleshooting connection problems

If MyID Desktop fails to connect to the MyID server, a message similar to the following appears:

```
Unable to connect to the required MyID Web Service in a timely fashion
Possible reasons for this include:-
- Invalid application connection
- Server Expects a Secure Connection (SSL)
- Firewall blocking
- No internet / intranet connection
Because of the nature of this problem the application is unable to continue
until the problem has been resolved.
Please contact your system administrator
```

If you experience any other errors, check the ***Error Code Reference*** document to see if it provides any suggestions to solve the connection problem.

If you cannot connect, try the following:

- Make sure MyID Desktop is configured for the appropriate MyID server.
- If your system is configured to use SSL, make sure that SSL is set up correctly. Make sure your SSL certificate is trusted.
- Make sure your firewall is not blocking HTTP or HTTPS communication between your client PC and the MyID web services server.
- Make sure you are connected to a network that has access to the MyID server.

If you see a message similar to the following:

```
Unable to access MyID
Unable to authenticate to MyID
Solutions:
Please contact your administrator
```

There may be a problem with the database configuration. On the MyID database server, open Microsoft SQL Server Management Studio, and check that the MyID COM+ user has the correct permissions. In particular, under **Security > Logins**, open the **Properties** for the MyID COM+ user, and check the **User Mapping** section. Make sure the user has `public`, `db_datareader`, and `db_datawriter` role memberships for the MyID database, and ensure that the **Default Schema** is set to `dbo` or another appropriate setting; a default schema of `sys` will cause connection problems.

10.3.8 Signature validation

MyID Desktop performs signature validation at startup to ensure that all components are properly signed by Intercede and have not been tampered with. These checks are performed using the native Windows APIs, and may require the client to connect to the Internet to retrieve the latest Certificate Revocation Lists (CRLs) for revocation checks of the Intercede signing certificate. If the client is permanently running in an isolated environment without access to the Internet, the CRLs cannot be retrieved, which can cause signature verification to fail. Under these circumstances, you may see an error similar to the following:

```
Failed to verify signature for running application. Error Code: 128
```

This error usually indicates that the client is unable to perform its revocation checks; to continue, you must disable these checks by adding an option to the application configuration file.

To edit the configuration file:

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

   ```
   C:\Program Files\Intercede\MyIDDesktop\
   ```

   On a 64-bit system, this is:

   ```
   C:\Program Files (x86)\Intercede\MyIDDesktop\
   ```

2. Using a text editor, open the `MyIDDesktop.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="ComponentVerificationSkipRevocationChecks"
   value="TRUE"></add>
   ```

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

4. Save the configuration file.

When this option is enabled, the client performs all of its normal validation, but does not perform the revocation check. As the client does not need to retrieve the CRLs, it does not need to be connected to the Internet.

Note: This reduces the integrity of the signature validation, as the client will 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.

10.3.8.1 Installing the required certificates for offline operation

If you have disabled the revocation check, you must also ensure that you have the appropriate certificates in the store of the client PC. On a PC with internet access, these certificates are obtained automatically; on a PC without internet access, you must obtain and install these manually.

To determine which certificates are required:

1. On a PC with internet access and MyID Desktop installed, locate the MyID Desktop program file in Windows Explorer.

   By default, this is:

   ```
   C:\Program Files (x86)\Intercede\MyIDDesktop\MyIDDesktop.exe
   ```

2. Right-click the file, and from the pop-up menu select **Properties**.
3. Click the **Digital Signatures** tab, then select the **Intercede Ltd** item in the **Signature list** and click **Details**.

   This is the code signing certificate.
4. Click **View Certificate**, then click **Certification Path**.
   - The certificate at the top is the root certificate – you must ensure that this certificate is in the trusted root store of the client PC. This is normally carried out by Windows Update, but a completely unpatched and disconnected PC may not have this certificate.
   - In the certificate chain, all certificates except the top and bottom certificates are intermediate certificates – you must ensure that these certificates are present in the intermediate certificate store on the client PC. These certificates are normally downloaded on demand, but may not be available on a disconnected PC.
5. Close the certificate dialog, then select the timestamp certificate in the **Countersignatures** list and click **Details**.
6. Obtain the root and intermediate certificates for this certificate, as you did for the code signing certificate.

10.3.9 Configuring timeouts

MyID Desktop is configured to time out after 30 seconds on some stages. This ends the current activity after that period of inactivity.

The default timeout for MyID Windows clients (MyID Desktop, the MyID Self-Service Kiosk, and the MyID Self-Service App) is controlled by the **Page Timeout for Windows Clients** configuration option (on the **General** page of the **Operation Settings** workflow).

If you want to change the timeout for a particular installation of MyID Desktop, you can edit the configuration file. This overrides the configuration option in **Operation Settings**.

To edit the configuration file:

1. Shut down MyID Desktop.
2. On the client PC, back up the `MyIDDesktop.exe.config` file in the following folder:

   `C:\Program Files\Intercede\MyIDDesktop\`

   On a 64-bit system, this is:

   `C:\Program Files (x86)\Intercede\MyIDDesktop\`
3. Using a text editor, open the `MyIDDesktop.exe.config` file.

   Note: Make the changes to the config file exactly as shown. The case is important.
4. 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.
5. Save the configuration file.
6. Restart MyID Desktop.

10.3.10 Ignoring cards inserted before running Batch Collect Card

When you run the **Batch Collect Card** workflow, MyID Desktop ignores any cards that you inserted before you ran the workflow.

If you want MyID Desktop to include already-inserted cards when running **Batch Collect Card**, you must disable this behavior by adding an option to the application configuration file.

To edit the configuration file:

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

   `C:\Program Files\Intercede\MyIDDesktop\`

   On a 64-bit system, this is:

   `C:\Program Files (x86)\Intercede\MyIDDesktop\`

2. Using a text editor, open the `MyIDDesktop.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="BatchIgnoreCardsInsertedBeforeWorkflow" value="false"/>
   ```

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

4. Save the configuration file.

10.4 Launching MyID Desktop

You can launch MyID Desktop from the shortcut installed by the installation program, from the command line, or from a hyperlink. You can also specify various options on the command line or hyperlink.

10.4.1 Launching MyID Desktop with a specific server

When you install MyID, you can specify multiple servers in the list of allowed server addresses; see section *10.2*, *Installing MyID Desktop*. For information on changing the server address *after* installation, see section *10.3.3*, *Server location*. This feature allows you to configure MyID Desktop to be able to connect to multiple servers (for example, if you have a test server and a production server).

By default, MyID Desktop connects to the first server in this list. If you want to connect to any of the other servers, you can specify the server address on the command line using the `/server` option.

```
MyIDDesktop.exe /server:<address>
```

where:

- `<address>` is one of the allowed server addresses.

For example:

```
MyIDDesktop.exe /server:https://testserver
```

10.4.2 Launching MyID Desktop with a specific workflow

You can launch MyID Desktop using a workflow ID on the command line:

```
MyIDDesktop.exe /opid:<value>
```

where:

- `<value>` is the ID of the workflow you want to launch.

See section *10.4.8*, *Workflow IDs* for a list of workflow IDs.

Note: The user must have access to the specified workflow.

10.4.3 Launching MyID Desktop for credential activation

You can launch MyID Desktop to start up at the credential activation screen:

```
MyIDDesktop.exe /activate /sn:<serial> /dt:<device>
```

where:

- `<serial>` is the serial number of the credential you want to activate.

  Note: If the serial number contains alphabetical characters, you must ensure that the case matches the case of the serial number stored in the MyID database.

- `<device>` is the type of the credential you want to activate. If the type contains spaces, enclose the name in quotes.

For example:

```
MyIDDesktop.exe /activate /sn:123456789 /dt:"Oberthur ID-One PIV"
```

10.4.4 Launching MyID Desktop for credential unlocking

You can launch MyID Desktop to start up at the credential unlocking screen:

```
MyIDDesktop.exe /unlock /sn:<serial> /dt:<device>
```

where:

- `<serial>` is the serial number of the credential you want to unlock.

  Note: If the serial number contains alphabetical characters, you must ensure that the case matches the case of the serial number stored in the MyID database.

- `<device>` is the type of the credential you want to unlock. If the type contains spaces, enclose the name in quotes.

For example:

```
MyIDDesktop.exe /unlock /sn:123456789 /dt:"Oberthur ID-One PIV"
```

10.4.5 Launching MyID Desktop with a logon code

If a user has been provided with a one time logon code for logging into MyID Desktop, you *must* start the program using the `/lc` command-line option.

You must also specify a workflow using the `/opid` command-line option.

See section *10.4.8*, *Workflow IDs* for a list of workflow IDs.

For example:

```
MyIDDesktop.exe /opid:216 /lc
```

10.4.6 Launching MyID Desktop with automatic Windows Logon

You can configure MyID Desktop to attempt to log on using Integrated Windows Logon when it starts up, instead of having to select the option on the logon screen:

```
MyIDDesktop.exe /lw
```

You can optionally specify a workflow using the `/opid` command-line option.

See section *10.4.8*, *Workflow IDs* for a list of workflow IDs.

For example:

```
MyIDDesktop.exe /lw /opid:216
```

See the *Integrated Windows Logon* section in the ***Administration Guide*** for details of setting up your system to allow Integrated Windows Logon.

10.4.7 Launching MyID Desktop from a hyperlink

When you install MyID Desktop, it registers the `myiddsk:` protocol – this means that you can click on hyperlinks on web pages and email messages to launch MyID Desktop.

Using the hyperlink mechanism, you can specify the following:

- Launch a workflow using the `/opid` option.

  See section *10.4.8*, *Workflow IDs* for a list of workflow IDs.

  Note: The user must have access to the specified workflow.
- Launch the activation mechanism for a specific credential using the `/activate` option with the `/sn` and `/dt` options to specify the serial number and device type of the credential to be activated.
- Launch the unlock process for a specific credential using the `/unlock` option with the `/sn` and `/dt` options to specify the serial number and device type of the credential to be unlocked.
- Allow the user to log on with a logon code using the `/lc` option.
- When using a logon code, you must also specify a workflow using `/opid`.
- Allow the user to attempt to log on with Integrated Windows Logon using the `/lw` option.
- When using the `/lw` option, you can optionally specify a workflow using `/opid`.
- Launch MyID Desktop with a specific server using the `/server` option.

Examples:

```
myiddsk://
myiddsk:///opid:216
myiddsk:///activate+/sn:123456789+/dt:Oberthur+ID-One+PIV
myiddsk:///unlock+/sn:123456789+/dt:Oberthur+ID-One+PIV
myiddsk:///lc+/opid:216
myiddsk:///lw
myiddsk:///lw+/opid:216
myiddsk:///server:https:%2F%2Ftestserver
```

Note: Make sure you replace spaces in the URL with `+`. Do not enclose the device type name in quotes. You must encode the forward slashes in the server address with `%2F` codes.

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.

10.4.8 Workflow IDs

The following table contains a list of the MyID operation IDs; this includes, but is not limited to, the workflows available in MyID. You can use this, for example, when launching a MyID client with a specific workflow.

Note: Not all workflow IDs will be available within your implementation of MyID. For example, there are some workflows that have been superseded by newer versions; make sure you test your implementation to ensure you are using the correct version of, for example, the **Print Card** workflow. Also, some IDs are used for additional permissions within workflows, rather than workflows themselves.

The master list of workflow IDs is available in the `Operations` table in the MyID database.

ID	Name
245	Activate Card
841	Add Asset
102	Add Group
101	Add Person
105	Amend Group
2967	Approve Erase
727	Approve Key Recovery
295	Assign Card
253	Assisted Activation
405	Audit Reporting
814	Audited Items
124	Authenticate Person
50010	Authentication Code
2979	Authentication Codes
255	Auto Unlock My Card
5003	Batch Collect Card
252	Batch Encode Card
221	Batch Request Card
282	Bio Unlock My Card
50011	Bypass Authentication
2985	Bypass Authentication
299	Cancel Credential
1405	Cancel Device Identity
280	Card Disposal

ID	Name
810	Card Layout Editor
2978	Card PIN
811	Certificate Authorities
702	Certificate Requests
110	Change Passwords
202	Change PIN
117	Change Security Phrases
5002	Collect Card
5005	Collect Card Updates
705	Collect Certificates
724	Collect Device Identity
728	Collect Key Recovery
216	Collect My Card
706	Collect My Certificates
730	Collect My Key Recovery
242	Collect My Updates
2384	Confirm Details
1441	Confirm Cancel Device Identity
2122	Confirm Details
2152	Confirm Details
13012	Confirm Details
807	Credential Profiles
820	Credential Stock
2172	Decision mode
274	Deliver Card
831	Directory Management
842	Edit Asset
108	Edit Groups
103	Edit Person
806	Edit Roles
834	Email Templates
224	Enable / Disable Card
1324	Enable / Disable ID
296	Erase Card
5006	Erase Unused VSCs
837	External Systems
10000	Full Access to Manager Lists

ID	Name
404	General
234	Identify Card
50006	Identity Documents
2974	Identity Documents
1244	Identity Documents
832	Import Device
215	Issue Card
288	Issue Device
260	Issue Temporary Card
261	Issue Temporary Card (Part 2)
701	Issued Certificates
815	Job Management
836	Key Manager
823	Licensing
819	List Editor
141	Manage Additional Identities
1001	Manage Applets
1002	Manage Global Platform Keys
142	Manage My Additional Identities
289	Manage VSC Access
1243	Match Enrolled Fingerprints
410	MI Reports
721	Mobile Certificate Recovery
843	Notifications Management
816	Operation Settings
1245	Operator Approval
2975	Operator Approval
50007	Operator Approval
13197	Operator Approval
236	Print Badge
298	Print Card
243	Print Mailing Document
709	Recover Certificates
710	Recover My Certificates
266	Reinstate Card
50009	Reject Authentication
2977	Reject Authentication

ID	Name
106	Remove Group
109	Remove Person
277	Replace My Card
270	Reprovision Card
269	Reprovision My Card
254	Request Auth Code
212	Request Card
218	Request Card Update
1306	Request Derived Credentials
1307	Request Derived Credentials (part 1)
1308	Request Derived Credentials (part 2)
723	Request Device Identity
1302	Request ID For My Phone
1301	Request ID For Phone
726	Request Key Recovery
278	Request My Temporary Card
217	Request Replacement Card
1317	Request Replacement ID
297	Reset Card PIN
279	Return Temporary Card
703	Revoked Certificates
1246	Security Questions
2976	Security Questions
13198	Security Questions
50008	Security Questions
813	Security Settings
13173	Select Person
409	System Status
1501	Universal Search
5000	Unlock Credential
1319	Unlock ID
122	Unlock My Security Phrases
121	Unlock Security Phrases
290	Unlock VSC Temporary Access
237	Update Card
238	Update Card
291	Update VSC

ID	Name
731	Upload PFX Certificates
708	Validate Certificate Request
1413	Validate Device Identity Request
213	Validate Request
10003	View Device Details
10001	View Full Audit
729	View Key Recovery
113	View Person
10002	View User Audit
2994	Witness Cancel Card
2156	Witness Create Card

10.5 MyID Desktop version number

If you need to find the version of MyID Desktop you are running (for example, if you need to contact customer support) you can obtain the version from the list of installed programs in the Windows Control Panel.

10.6 Installing the MyID Client Service

The MyID Operator Client is a browser-based system that allows operators to work with people and requests in the MyID system; see the ***MyID Operator Client*** guide for details of using the client.

To allow the browser to access smart cards, capture images, issue soft certificates, print mailing documents, or access features of MyID Desktop or the Self-Service App, you must install the MyID Client Service on each Windows PC on which you want to use the MyID Operator Client.

The MyID Client Service installation program is located in the MyID release in the `MyID Clients\MCS` folder.

The installation program is provided as a `.msi` file that you can install directly or run from a command-line to install silently on each client PC.

Note: Intercede also provides MSIX versions of the installation programs for MyID Desktop, the Self-Service App, and the MyID Client Service. These are intended for an administrator to create an installation package that combines all of the necessary client software and administrator-controlled configuration. See the ***MyID Client MSIX Installation Guide*** for details of working with these installation programs.

Note: The MyID Client Service requires .NET Core; see section *4.3*, *Installing .NET Framework and .NET Core* for details of how to obtain the correct version of .NET Core. Make sure this is installed before you attempt to install the MyID Client Service.

Important: The web services used by the MyID Operator Client (`rest.core` and `web.oauth2`) require SSL/TLS; if you do not connect through HTTPS, you cannot use the MyID Operator Client. For information on setting this up, see the *Configuring SSL/TLS (HTTPS)* section in the ***Securing Websites and Web Services*** document.

To install the MyID Client Service:

1. Copy the installation program to a local drive.

   If you do not run the installation program from a local drive, you may experience problems with the application running slowly due to certificate checks.

2. Run the installation program, then click **Next**.

3. Select the destination location, then click **Next**.

   By default, the MyID Client Service installs to the following folder:

   ```
   C:\Program Files (x86)\Intercede\
   ```

   Note: You do not need to have administrative privileges to install the MyID Client Service. However, you must make sure that you have the correct permissions to install software to the program folder; for example, your system administrator may not permit you to install software to the default folder. In this case, choose a different destination location.

4. Click **Next**.

5. In the **Server URL** box, type the location of the server on which the MyID web services are installed.

   For example:

   ```
   https://myserver
   ```

6. In the **Access Control URL(s)** box, type one or more URLs that point to websites that are permitted to access the MyID Client Service. Use commas to separate the URLs.

   For example:

   ```
   https://myserver,https://myserver2
   ```

7. Click **Next**.

8. Click **Install**.

9. When the installer has completed, click **Finish**.

To install silently on a client PC, you can use the `.msi` installer with the following command-line parameters:

```
msiexec /i "<msi path>" /lv <LogFile> /q REACT_SERVERNAME=<ServerURL>
ACCESS_CONTROL_URLS=<accessurls> INSTALLDIR=<InstallationFolder>
```

where:

- `<msi path>` is the path to the .msi file.
- `<LogFile>` is the name of the file to which you want to write a verbose log. This is optional.
- `<ServerURL>` is the address of the MyID web services server; for example `https://myserver/`
- `<accessurls>` is a comma-delimited list of URLs of websites that are allowed to access the MyID Client Service.
- `<InstallationFolder>` is the name of the folder to which you want to install the application. This is optional.

Note: Do not put a space character on either side of the = signs in the command line.

For example:

```
msiexec /i "C:\install\MCS-1.x.x.x.msi" /lv msilog.txt /q REACT_
SERVERNAME=https://myserver
ACCESS_CONTROL_URLS=https://myserver INSTALLDIR="C:\temp\desktop"
```

10.6.1 Using the MyID Client Service on a PC with multiple users

If you have a PC with multiple simultaneous users, you must install an additional client software package to allow multiple instances of the MyID Client Service to work through a single WebSocket port.

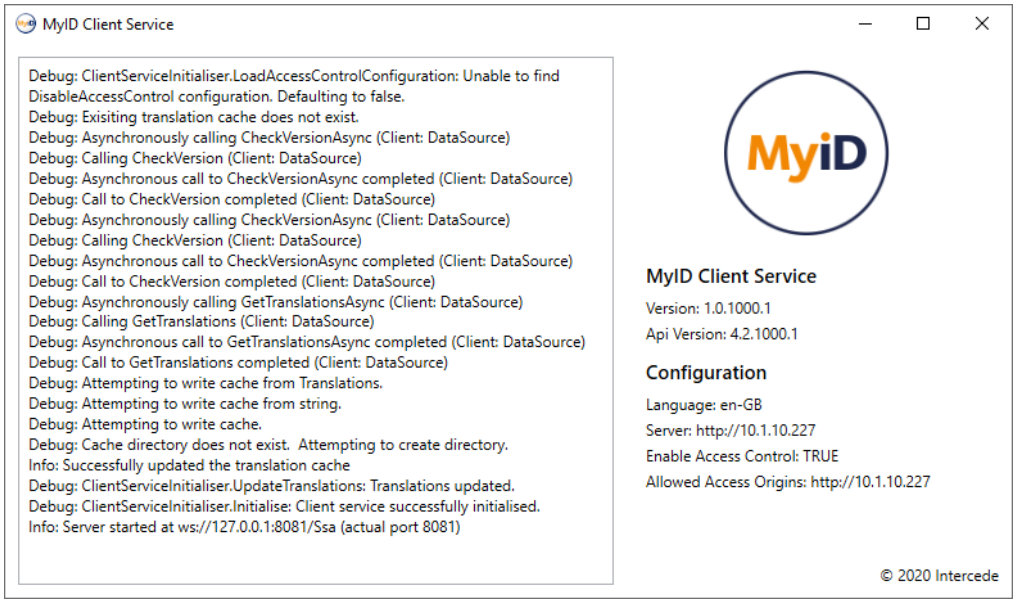
See section *10.7*, *Installing the MyID Client WebSocket Service*.

10.6.2 Running the MyID Client Service

The MyID Client Service must be running for the MyID Operator Client to use its capabilities to communicate with smart cards. You can run the **MyID Client Service App** from the Windows Start menu; however, as an administrator, you are recommended to set the `MyIDClientService.exe` application to run automatically at Windows logon.

When running, the MyID Client Service runs as an icon in the system tray. Right-click the icon and select one of the following options:

- **Show** – displays information about the service.



  The scrolling windows displays the most recent 1000 lines of log entries. This is displayed whether or not you have configured logging, but is not saved to a file. For details of configuring logging for the MyID Client Service, see the *Windows clients* section in the ***Configuring Logging*** guide.

  The following additional information is displayed:

  - **Version** – the version of the MyID Client Service that you are running.
  - **API Version** – This is the version of the MyID Web Service Architecture (MWS) to which the MyID Client Service is connected.
  - **Language** – the language that the MyID Client Service requests for its translations. If this is not available on the MyID server, it will use `en-US`.

    For information about translating the MyID interface, contact customer support quoting reference SUP-138.
  - **Server** – the server to which the MyID Client Service is connected.
  - **Enable Access Control** – Indicates whether or not access control is enabled. If it is disabled, the MyID Client Service will accept connections from any client origin rather than only from origins specified in the `AccessControlAllowOrigin` configuration.
  - **Allowed Access Origins** – the list of origins in the `AccessControlAllowOrigin` configuration from which the MyID Client Service will accept incoming connections.

    For information on access control and allowed access origins, see the *Specifying the server for the MyID Client Service* section in the ***MyID Operator Client*** guide.

- **Exit** – closes the MyID Client Service.

10.6.3 Installing the Aware PreFace software for facial biometrics

If you are using the MyID Operator Client to capture facial biometrics, you must install the Aware PreFace software to the same location as the MyID Client Service.

This software is available from Intercede. If you want to purchase the Aware PreFace software, contact customer support and request a copy of the PreFace software installer.

When you install the Aware PreFace software, on the Destination Folder screen, make sure you select the `MyIDClientService` folder that was created beneath the folder you selected when installing the MyID Client Service; by default, this is:

```
C:\Program Files (x86)\Intercede\MyIDClientService\
```

If you are using Canon EOS cameras, you must also install the Canon SDK, which is also available from Intercede.

When you install the Canon SDK software, you must ensure that the two DLLs are put into the following folder:

```
C:\Program Files (x86)\Intercede\MyIDClientService\MyIDImageCapture
```

- **IKB-403 – Installation program places the Canon DLLs in the wrong location**

  If you have set the Canon MSI Installer to the default location, they are installed to the following location:

  ```
  C:\Program Files (x86)\Intercede\MyIDClientService\Aware
  ```

  You must move the Canon SDK DLL files to the following folder:

  ```
  C:\Program Files (x86)\Intercede\MyIDClientService\MyIDImageCapture
  ```

  Note: The MSIX installation program installs the Canon SDK files correctly.

For more information about using Aware PreFace for the capture of facial biometrics in the MyID Operator Client, see the *Capturing facial biometrics* section in the ***MyID Operator Client*** guide.

10.7 Installing the MyID Client WebSocket Service

If you have a PC with multiple simultaneous users, you must install the MyID Client WebSocket Service to allow multiple instances of the MyID Client Service to work through a single WebSocket port.

Note: As this is client software, you must install all prerequisite client software, including the .NET Framework and the .NET Core Desktop Runtime; see section *5.2*, *Client workstation* for details of the client hardware and software requirements.

10.7.1 Installing the MyID Client WebSocket Service

The MyID Client Service installation program is located in the MyID release in the following folder:

```
MyID Clients\Client Web Socket Service\
```

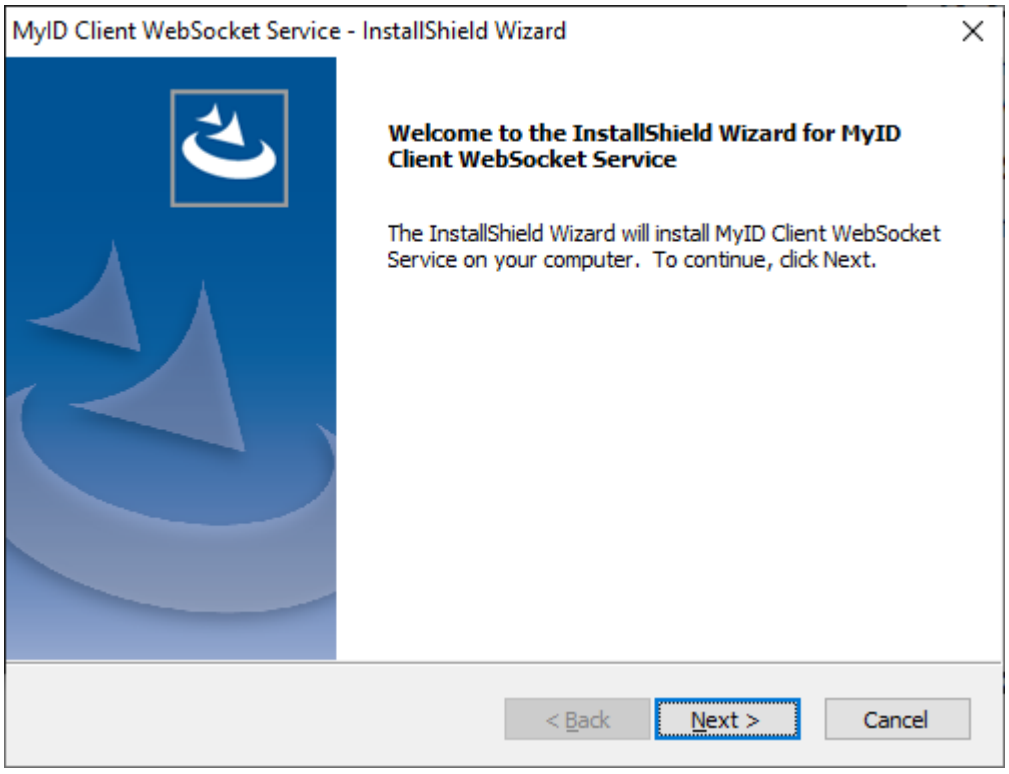
To install the MyID Client WebSocket Service on the client PC:

1. Copy the msi installation program to a local drive.
2. Run the installation program as an administrator.

For example, open a Windows command prompt as an administrator, navigate to the folder containing the msi file, then run the following command:

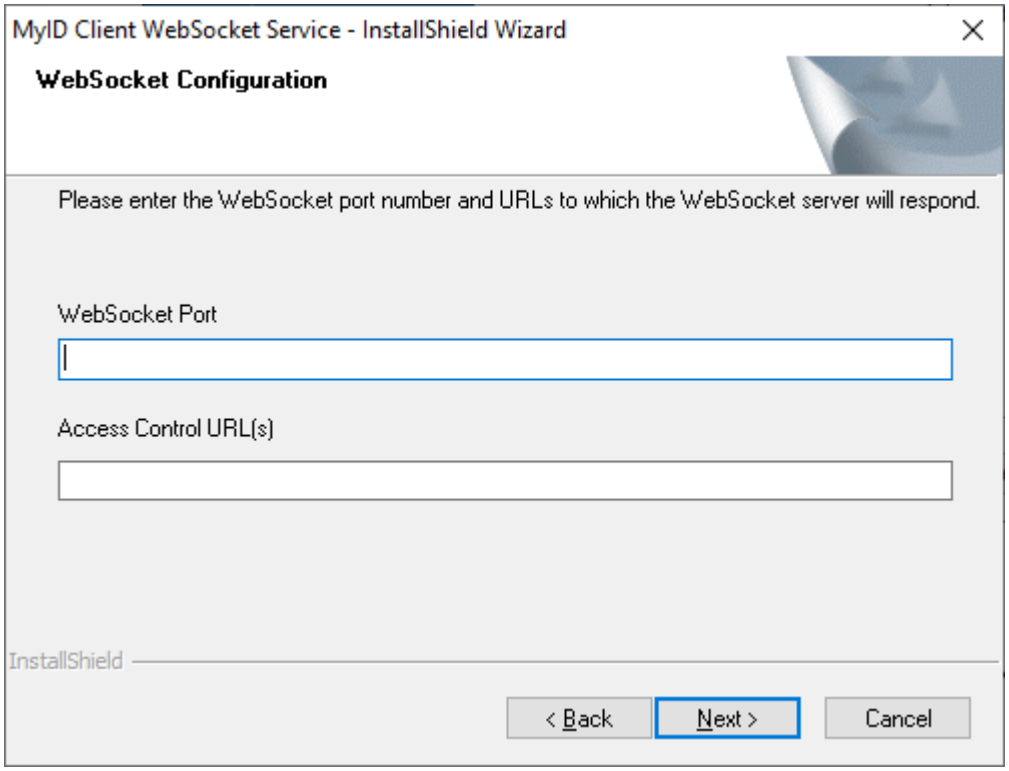
```
msiexec /i CLIENTWSSERVICE-<version>.msi
```

The installer starts.



3. Click **Next**.

   The WebSocket Configuration screen appears.



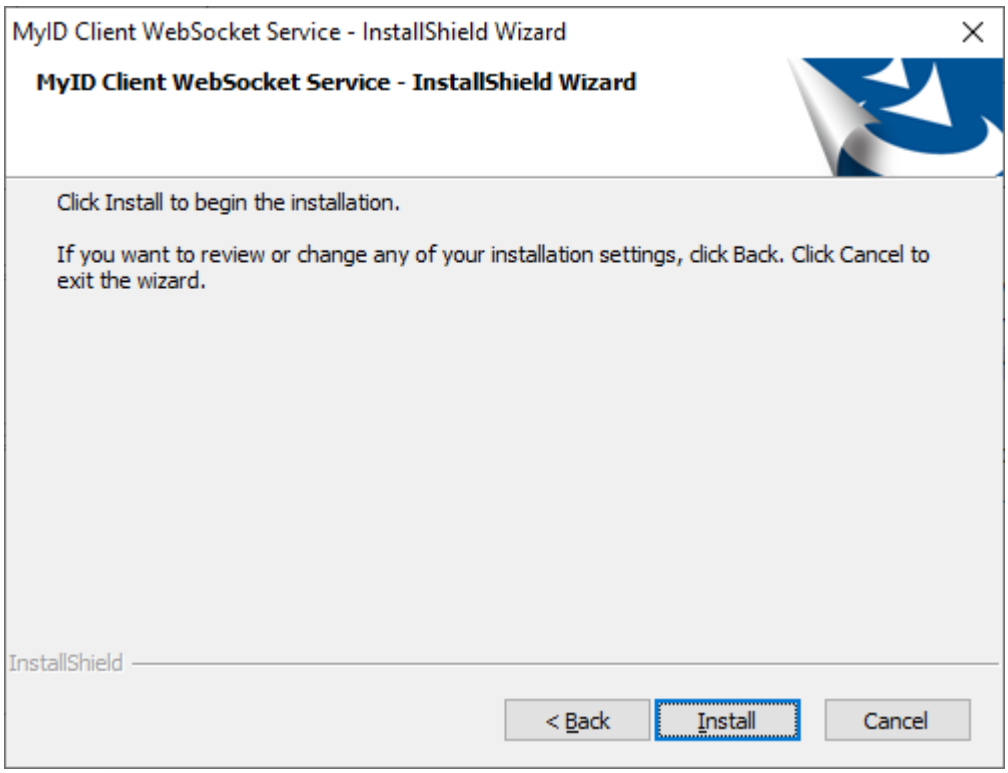
4. Provide the following details:
   - **WebSocket Port** – type the number of the port you want to use. By default, the MyID Operator Client and its web service use port 8081. If you use a different port, you must also configure the MyID Client Service to use the same port; see the *Changing the port* section in the ***MyID Operator Client*** guide for details.
   - **Access Control URL(s)** – type one or more URLs that point to websites that are permitted to access the MyID Client Service. Use commas to separate the URLs.

     For example:

     ```
     https://myserver,https://myserver2
     ```

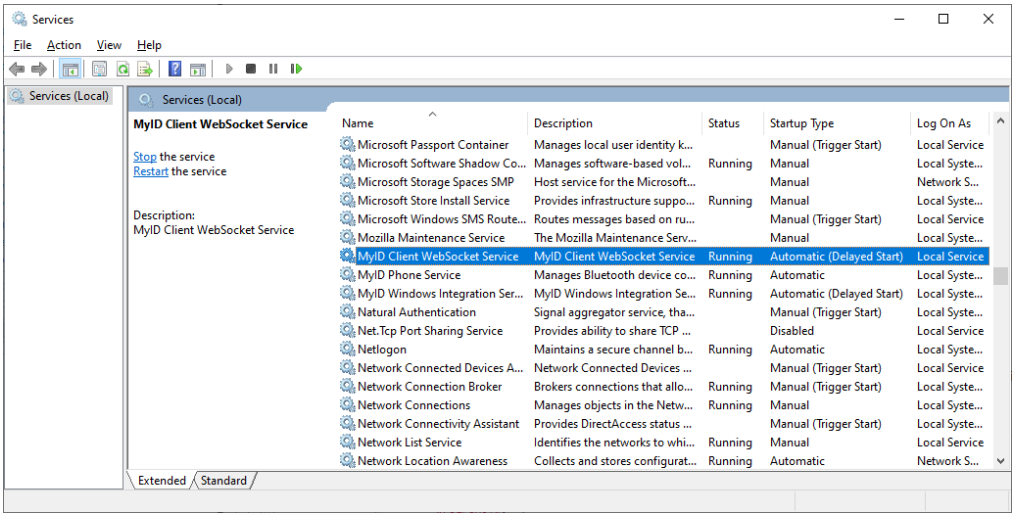
     Note: If you want to allow access to *any* websites, you can use a wildcard:

     ```
     *
     ```
5. Click **Next**.



6. Click **Install**.
7. When the installation has completed, click **Finish**.

The MyID Client WebSocket Service is installed as a Windows Service, and runs automatically.



Important: Once you have installed the MyID Client WebSocket Service, you must configure the MyID Client Service to use it. See section *10.7.3, Enabling or disabling the MyID Client WebSocket Service*.

10.7.2 Configuring the MyID Client WebSocket Service

You can configure the MyID Client WebSocket Service by editing the service's `appsettings.json` file. By default, this file is installed in the following location:

`C:\Program Files (x86)\Intercede\MyIDClientWebSocketService`

```
{
  "Logging": {
    "EventLog": {
      "LogLevel": {
        "Default": "None"
      }
    }
  },
  "Timeouts": {
    "ClientConnectionTimeoutSeconds": 5,
    "ConfirmedSessionTimeoutSeconds": 5,
    "StaleClientTimeoutSeconds": 30,
    "UnconfirmedSessionTimeoutSeconds": 60
  },
  "WebSocket": {
  "Port": 8081,
  "AccessControlAllowOrigin": "https://myserver.example.com"
  }
}
```

10.7.2.1 Configuring logging

The `Logging` section controls whether the service produces log information. See the *MyID Client WebSocket Service* section in the ***Configuring Logging*** guide for details of setting up logging for the MyID Client WebSocket Service.

10.7.2.2 Setting timeouts

You can set the following timeouts in the `Timeouts` section:

- `ClientConnectionTimeoutSeconds` – Once an instance of the MyID Client Service has been matched to a session ID, this is the period that the MyID Client WebSocket Service will wait when attempting to connect to it.

  If you are receiving an `UnresponsiveSessionClient` error, increasing this value will increase the time the service will wait for the client to respond.

  The default is `5` seconds.

- `ConfirmedSessionTimeoutSeconds` – The maximum time the service will wait for a client to be associated with a session ID after having previously successfully communicated with it.

  If a client has been closed after the MyID Operator Client has used it, this is the maximum period of time it will have to wait before receiving an error from the service that will cause it to launch a new instance of the MyID Client Service.

  The default is `5` seconds.

- `StaleClientTimeoutSeconds` – At the interval defined by this configuration, the service will check for and remove any session ID registrations whose associated MyID Client Service instance is no longer running.

  The default is `30` seconds.

- `UnconfirmedSessionTimeoutSeconds` – The maximum time the service will wait for a client to be associated with a session ID that has never previously been communicated with.

  If a client is still starting up when a request is made, this is the maximum period of time a caller will have to wait before receiving an error from the service.

  You are recommended to increase this value to accommodate the time required if the MyID Client Service takes longer than 60 seconds to start in your environment.

  The default is `60` seconds.

10.7.2.3 Updating the port and server details

If you need to update the port number or the list of allowed servers, set the following options in the `WebSocket` section:

- `Port` – type the number of the port you want to use. By default, the MyID Operator Client and its web service use port 8081. If you use a different port, you must also configure the MyID Client Service and the MyID Operator Client website to use the same port; see the *Changing the port* section in the ***MyID Operator Client*** guide for details.

- `AccessControlAllowOrigin` – type one or more URLs that point to websites that are permitted to access the MyID Client Service. Use commas to separate the URLs.

  For example:

  ```
  https://myserver,https://myserver2
  ```

  Note: If you want to allow access to *any* websites, you can use a wildcard:

  ```
  *
  ```

10.7.3 Enabling or disabling the MyID Client WebSocket Service

Once you have installed and configured the MyID Client WebSocket Service, you must configure the MyID Client Service to use this service by editing the MyID Client Service configuration file.

1. Open the `MyIDClientService.dll.config` file in a text editor.

   This file is located in the MyID Client Service program folder. By default, this is:

   ```
   C:\Program Files (x86)\Intercede\MyIDClientService
   ```

2. Edit the following line in the `appSettings` section:

   ```
   <add key="UseGlobalService" value="true"/>
   ```

   Set the value to `true` to enable the use of the MyID Client WebSocket Service, and `false` to disable it.

   If this line does not exist in the configuration file, you can add it to the `appSettings` section.

   If you are using the MSIX version of the MyID Client Service installation program, you can use the **MyID Client Service** tab on the **Client Configuration** page of the MyID Client Configurator to set this option.

3. Save the configuration file.

4. Restart the MyID Client Service.

Note: If you disable the use of the MyID Client WebSocket Service, make sure you stop the MyID Client WebSocket Service before attempting to restart the MyID Client Service; the MyID Client WebSocket Service will retain control over the WebSocket port and the MyID Client Service will be unable to use it. If the MyID Client WebSocket Service is running, you may see an error similar to the following:

```
10000228 - Failed to bind to local web-socket port. Make sure another
application is not running and consuming your port.
```

You are recommended to disable or uninstall the MyID Client WebSocket Service if you are not going to use it.

10.7.4 Connected devices and peripherals

MyID has been tested with connected smart cards and virtual smart cards with Microsoft Remote Desktop Services. Other peripherals, for example cameras, printers, scanners, fingerprint readers, and their associated software from the device vendors, will require special configuration in your environment, which is outside of the scope of MyID software. For example, issues may be seen establishing device connectivity to Windows, and virtualized environments are likely to introduce additional latency which will affect use.

For this reason, support for connected devices and peripherals with MyID in virtualized environments is limited; see section *5.3*, *Virtual environments and remote connections* for further details.

10.8 Installing the unlock credential provider

MyID provides an unlock credential provider that allows a user to unlock their PIV card from the Windows logon screen.

See the *Unlock credential provider* section in the ***Operator's Guide*** for details of using the unlock credential provider to unlock a PIV card.

10.8.1 Prerequisites

The credential unlock provider is supported on Windows 10, build 1709 or later.

To unlock a card, it must be a PIV card or other device that has a PIV applet, and it must have been issued by your MyID system.

10.8.2 Configuring Windows for Integrated Unblock

You must set the `AllowIntegratedUnblock` policy in the Credential Security Support Provider in Windows to allow the unlock credential provider to operate.

See your Microsoft documentation for details of configuring this through group policy or the registry.

10.8.3 Installing the unlock credential provider

You must install the unlock credential provider on each PC on which you want users to be able to unlock their PIV cards at the Windows logon screen.

The installation `.msi` file is provided in the following folder on the MyID installation media:

`\MyID Clients\Unlock Credential Provider\`

The installation package filename is `UNLOCKCREDPROV-x.x.x_x.msi`.

10.8.4 Customizing the unlock credential provider

You can customize the text displayed on the unlock credential provider screen by editing the registry; for example, you could change the "Please contact your help desk" message to include a phone number.

Note: Back up your registry before making any changes.

The text strings are stored as String values in the registry in the following location:

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Intercede\MyIDUnlockCredentialProvider`

If the `MyIDUnlockCredentialProvider` key does not exist, you can create it.

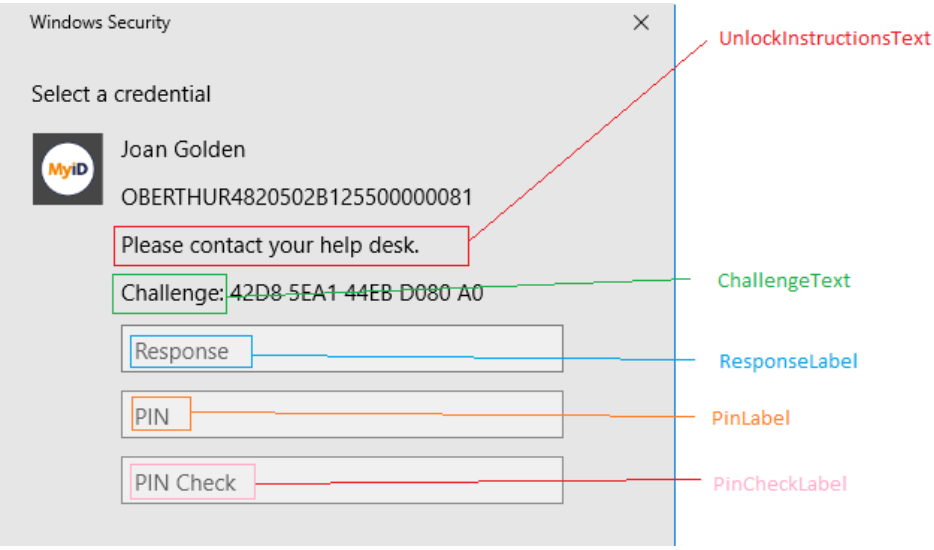
You can edit the following text:

String Value	Default Text	Type
`ChallengeText`	Challenge:	Label
`ChangePinText`	Change PIN	Label
`PinCheckLabel`	PIN Check	Label
`PinLabel`	PIN	Label
`PinResetText`	PIN reset	Label
`ResponseLabel`	Response	Label
`UnlockInstructionsText`	Please contact your help desk.	Label
`EmptyResponseText`	Response code is empty	Prompt
`FailedToUnlockText`	Unlock failed	Prompt

String Value	Default Text	Type
InvalidResponseText	Invalid response code	Prompt
PINLengthWrongText	PIN length is incorrect	Prompt
PINMismatchText	PINs do not match	Prompt

Text of type Label is static text displayed on screen.

Text of type Prompt is displayed in response to a user action.



Other labels available are:

- PinResetText – the message shown when a card is successfully unlocked.
- ChangePinText – reserved for future use.

10.8.5 Troubleshooting

Whenever a card is unlocked, or an unlock procedure fails, a message is written to the Windows application event log.

An error will indicate a card communication issue – for example, the card may be SO PIN locked. In this case, the APDU response is logged. These are industry standard response codes for smart card operations, not specific MyID errors.

10.9 Setting up client software

10.9.1 Cards and card readers

Warning: Install the middleware for your cards and your chosen reader before installing MyID. Check that these are working correctly using the vendor's tools.

MyID supports various brands of card readers, specified in the ***Smart Card Integration Guide***. Although other PC/SC compliant readers may operate with MyID, they may not have been tested.

Note: Only some combinations of card readers can be installed on the same machine because of limitations of the device drivers. Contact customer support for specific advice, quoting reference SUP-298.

10.9.2 JAWS screen reader

If you are using the JAWS screen reader, you must set up the following in the JAWS personal site settings:

- **Form Fields Identify Prompt Using** – set this option to **Alt Attribute**.

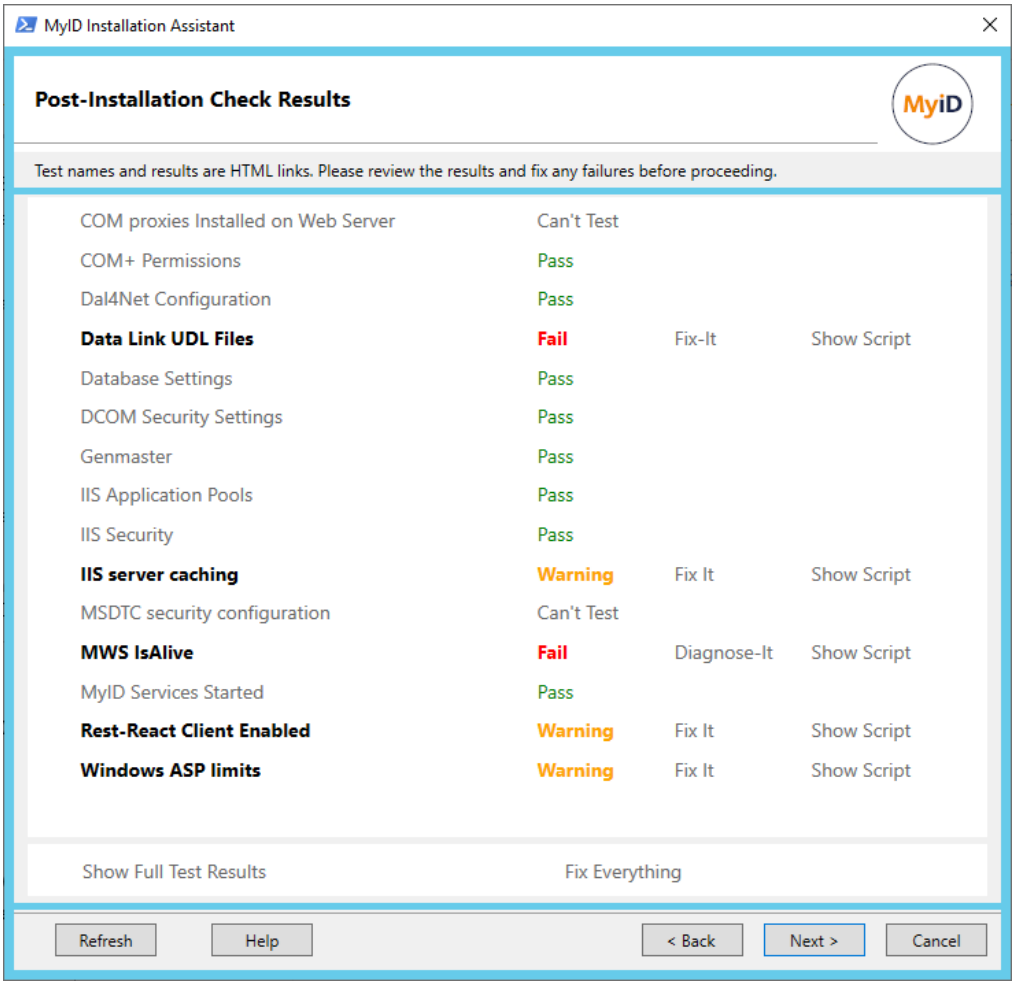
Set the software to use alt tags for buttons and graphics.

The following options are also recommended:

- **Frame Update** – set to **Move to Frame**
- **Frame show start and end** – set to **Off**
- **Voice rate** – set to **>45%**

11 After installing MyID

When you run the MyID Installation Assistant, once it has installed the server software, it carries out an Post-Installation Check, which confirms that the software has been installed correctly, and also provides an opportunity to carry out post-installation configuration.



For example, you can use the Fix-It scripts to set up your IIS server caching, MSDTC security configuration, and Windows ASP limits.

When you have your servers configured, you can test the installation by logging on for the first time; see section *12*, *Testing the installation*. Once you can log on to the system, you can request your licenses; see section *13*, *Licensing*.

You are also recommended to review the ***Advanced Configuration Guide***, which covers topics such as archiving databases and configuring email notifications, and implementing any features that are appropriate to your implementation of MyID.

This chapter contains details of the post-installation configuration that you must carry out:

- section *11.1*, *IIS server caching*.
- section *11.2*, *MSDTC security configuration*.
- section *11.3*, *Windows ASP limits*.
- section *11.4*, *Application recycling*.
- section *11.5*, *HSM concurrency*.
- section *11.6*, *Securing the application*.
- section *11.7*, *Checking the installation log*.
- section *11.8*, *Microsoft system event messages*.

11.1 IIS server caching

SIU references: SIU-087, SIU-088.

Make sure that no server-side caching occurs on the MyID website.

You must carry out this configuration after you have installed MyID.

Within IIS, for each MyID website (for example, MyID, MyIDDataSource, MyIDEnroll, MyIDProcessDriver, MyIDWebService) open **Output Caching > Edit Feature Settings**, deselect the **Enable Cache** and **Enable Kernel Cache** options, then restart the web server.

Note: When you install MyID using the MyID Installation Assistant, these settings are checked on the Post-Installation Check Results screen; if you need to change these settings, you can use the fix-it script provided on that screen. See section *2.22*, *Post-installation check results* for details.

11.2 MSDTC security configuration

SIU references: SIU-083, SIU-084, SIU-218.

Important: Microsoft is making changes to DCOM security over the course of releases in 2021 to 2023. See article ***KB5004442*** on the Microsoft support site (***support.microsoft.com***) for details. These changes affect your Windows DCOM Server Security configuration, including future updates. You are recommended to follow the instructions in this section carefully, and to use the MyID Installation Assistant to check that your system is configured correctly.

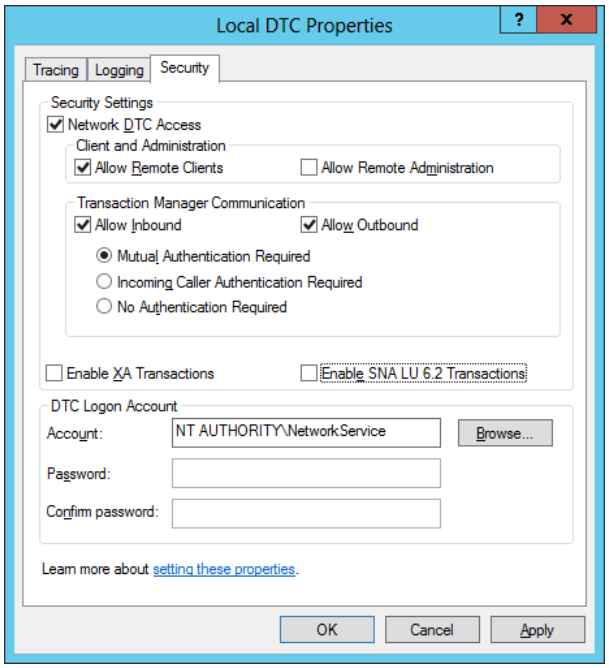
If your system is split across more than one server you must set up your MSDTC security on the web server, application server and the database server to allow access. If you experience an error similar to the following, you may have to check either your MSDTC or Windows Firewall configuration:

```
Unable to perform the requested operation
Set up your MSDTC settings on the application and database tiers.
```

Note: When you install MyID using the MyID Installation Assistant, these settings are checked on the Post-Installation Check Results screen; if you need to change these settings, you can use the fix-it script provided on that screen. See section *2.22*, *Post-installation check results* for details.

To set up the MSDTC security:

1. Within Component Services, expand **Component Services** and **Computers**.
2. Right-click on **My Computer**, and click **Properties**.
3. Click the **MSDTC** tab.
4. Make sure that **Use local coordinator** is selected.
5. Click **OK**.
6. Expand **My Computer > Distributed Transaction Coordinator**.
7. Right-click **Local DTC** and select **Properties**.
8. Click the **Security** tab.



9. To ensure that MyID works correctly, set the following options:
   - **Network DTC Access**.
   - **Allow Remote Clients**.
   - **Allow Inbound**.
   - **Allow Outbound**.
   - **Mutual Authentication Required**.

     Note: If you are using SQL Server authentication, select **No Authentication Required** instead.

     You specify whether to use SQL Server authentication or Windows authentication when installing MyID.
10. Click **OK**.

Note: You may experience an error similar to the following when using mutual authentication:

```
Unable to perform the requested operation
```

For a workaround, see the Microsoft Knowledge Base article KB2172085.

11.3 Windows ASP limits

SIU references: SIU-079, SIU-080.

The following ASP errors may be generated:

```
Request object error 'ASP 0104 : 80004005' Operation not Allowed.
ASP 0251~Response Buffer Limit Exceeded
```

This can occur when submitting large amounts of data to an ASP page. By default Windows allows only a small amount of data to be processed by an ASP request. For example, you may encounter the error when importing large numbers of users from a file.

Note: When you install MyID using the MyID Installation Assistant, these settings are checked on the Post-Installation Check Results screen; if you need to change these settings, you can use the fix-it script provided on that screen. See section *2.22, Post-installation check results* for details.

To increase the ASP limits:

1. In IIS Manager, select the MyID website under **Default Web Site**, then double-click the **ASP** icon.
2. Expand the **Limits Properties** section.
3. Increase the values of the following fields to `1073741824` (1 GB):
   - **Maximum Requesting Entity Body Limit**
   - **Response Buffering Limit**

   These can be set to a lower value depending on the amount of data transferred; for example, 524288 (512KB) or 1048576 (1MB).
4. In IIS Manager, select the **upimages** website under **Default Web Site**, then double-click the **ASP** icon.
5. Expand the **Limits Properties** section.
6. Increase the values of the following fields to a minimum of `524288`:
   - **Maximum Requesting Entity Body Limit**
   - **Response Buffering Limit**
7. Click **Apply**.
8. Restart IIS.

11.4 Application recycling

SIU references: SIU-173, SIU-174, SIU-175, SIU-176, SIU-177, SIU-178, SIU-179, SIU-180, SIU-181, SIU-182, SIU-183.

Application recycling works by creating a duplicate of the Dllhost process associated with an application. This duplicate Dllhost process services all future object requests, which leaves the old Dllhost to finish servicing the remaining object requests. The old Dllhost process is shut down when it detects the release of all external references to objects in the process or when the expiration time-out value is reached. Through this behavior, application recycling ensures that a client application does not experience a service interruption.

This section provides guidelines for settings for the MyID COM+ components to implement application recycling.

11.4.1 Settings for COM+ components

If you are experiencing performance problems, you can set the **Lifetime Limit** and **Memory Limit** for all of the MyID components.

The Edefice_BOL component is installed with a default lifetime limit of 120 minutes; the Edefice_DAL component is installed with a default lifetime limit of 30 minutes; the other MyID components are installed with a lifetime limit of 0. The Edefice_DAL component is installed with a default memory limit of 1000000KB; the other MyID components are installed with a memory limit of 0.

1. Shut down all MyID clients.
2. On the MyID application server, in the Windows Control Panel's **Administrative Tools**, open the **Component Services**.
3. Expand **Component Services > Computers > My Computer > COM+ Applications**.
4. You must make the following changes for each of the MyID components.

   This may include some or all of the following components, depending on the features you have installed on your MyID application server:

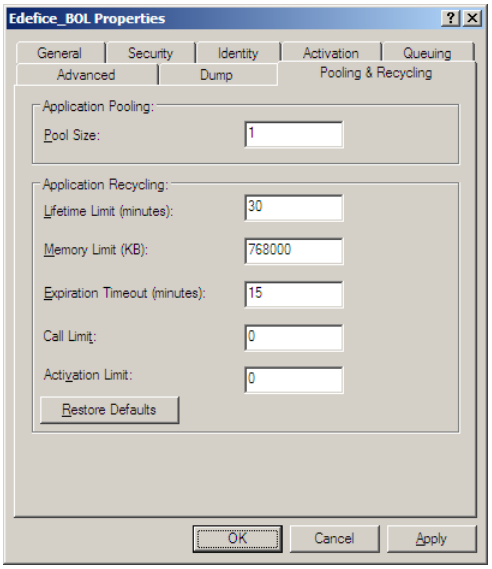
   - `APDUCardServer`
   - `EAudit`
   - `eCS`
   - `Edefice_BOL`
   - `Edefice_CS`
   - `Edefice_DAL`
   - `eEventLog`
   - `eExternalDataSource`
   - `Entrust_Admin`
   - `ePKIConfig`
   - `ExpiringItems`
   - `ImportProcessor`
   - `MyID SNMP Agent`
   - `MyIDSCEPHandler`

   a. Right-click the MyID component and select **Properties** from the pop-up menu.

   b. Click the **Pooling & Recycling** tab.

   c. Set the **Lifetime Limit** to `30` (30 minutes).

   d. Set the **Memory Limit** to `768000` (750MB).



Leave the rest of the settings at their default values: leave the **Pool Size** at `1`, the **Expiration Timeout** at `15`, the **Call Limit** at `0`, and the **Activation Limit** at `0`

e. Click **OK**.

f. To ensure that the component uses the new settings, right-click the component, and select **Shut down** from the pop-up menu.

The component will automatically restart when it is needed.

11.5 HSM concurrency

You can control the multithreading behavior of eKeyServer (the MyID key server service) using registry settings on the MyID application server.

11.5.1 Concurrent sessions

`HKEY_LOCAL_MACHINE\SOFTWARE\Intercede\Edefice\MasterCard\KeyProviderMaxConcurrentSessions`

This option controls the number of HSM sessions that will be created by the key server; this acts as a cap on the number of concurrent operations, and any additional operations beyond this will be queued for execution until a session becomes available. Setting this value too high may cause excessive load on the HSM and degrade performance.

You can also set this key to `0` to disable support for concurrent sessions. Concurrent sessions are also disabled if this key is missing from the registry.

The installer sets the default value for `KeyProviderMaxConcurrentSessions` in the registry to `10`.

11.5.2 Retries

`HKEY_LOCAL_MACHINE\SOFTWARE\Intercede\Edefice\MasterCardKeyProviderMaxRetries`

This option defines the maximum number of times a failed operation will be retried by the key server, not inclusive of the initial attempt.

The default for `KeyProviderMaxRetries` is `5`.

Retries are possible only when a PIN is either not required, or is saved in the registry.

11.6 Securing the application

When you first set up MyID, you may not want to lock down the system completely, allowing you to complete the initial test and setup more easily. Accordingly, the security features have not been made mandatory within MyID. However, it is extremely important that you secure your MyID system before using it for production purposes.

The ***System Security Checklist*** contains information about securing PINs, keys, and web servers; follow the recommendations in this document to secure your system.

11.7 Checking the installation log

If you experience any problems when installing MyID or an update to MyID, you can check the installation log for errors.

Note: If you are using the MyID Installation Assistant, the installation log is checked automatically and any issues highlighted; see section *2.20*, *Checking the installation log results* for details.

Installation logs are created in a file in your temporary folder with a name in the format `MSIxxxxx.LOG`; for example, `MSId149a.LOG`. To check the location of your temporary folder, at a command prompt type:

```
echo %TEMP%
```

Important: If you installed MyID over a remote connection, and did not set up your system not to use temporary folders per session before installing MyID, you cannot check the installation log, as they have been automatically deleted by the operating system. See section *6.4*, *Temporary folders for remote connections*.

Note: This installation log may, under some circumstances, contain the MyID COM, IIS, and web service usernames and passwords entered during installation. If the Microsoft Installer Debug Policy value on the PC is set to 7, any values entered on the command line, including passwords, are written to the log. You are recommended to check this log immediately after installation and delete it if necessary.

11.8 Microsoft system event messages

After installing MyID, you may see messages similar to the following in your system events:

```
Source: Microsoft-Windows-DistributedCOM

Event ID: 10016

Description: The application-specific permission settings do not grant
Local Activation permission for the COM Server application with CLSID

{D63B10C5-BB46-4990-A94F-E40B9D520160}

and APPID

{9CA88EE3-ACB7-47C8-AFC4-AB702511C276}
```

```
to the user MYDOMAIN\MyID_User SID (S-1-5-21-3850267927-4167700666-
3837966660-1117) from address LocalHost (Using LRPC) running in the
application container Unavailable SID (Unavailable). This security
permission can be modified using the Component Services administrative
tool.
```

These 10016 events are recorded when Microsoft components try to access DCOM components without the required permissions. Microsoft's guidance is that "These events can be safely ignored because they do not adversely affect functionality and are by design. This is the recommend action for these events."

For more information, see: ***support.microsoft.com/en-gb/help/4022522/***

12 Testing the installation

Once you have installed MyID (see section *8*, *Installing MyID*) and at least one client (see section *10*, *Installing MyID clients*), you can test the installation by opening MyID Desktop and connecting to your MyID server.

To test basic operation, use the following sequence:

1. Log on to MyID with the startup user.
2. Add a new user – check the connection to LDAP to import a user, if you are using an LDAP directory.
3. Check the certificate authority configuration and (if present) enable at least one certificate policy for issuance.
4. Create a credential profile with MyID logon and a certificate (if a CA is present).
5. Issue a card to the user you created.
6. Check the certificate is on the card.
7. Verify logon to MyID with the newly issued card.
8. Cancel the card.
9. Check the certificate has been revoked.

See:

- section *12.1*, *Configuring and testing the directory connection*.
- section *12.2*, *Configuring and testing the Certificate Authority connection*.
- section *12.3*, *Problems with connecting to the web server*.
- section *12.4*, *Checking the web services*.

12.1 Configuring and testing the directory connection

You can test the connection to the directory.

- Active Directory will operate with no additional configuration.
- Other LDAP directories may require configuration to set attribute mapping.
- Advanced features such as LDAP mapped custom attributes will require manual configuration.

See the *Using an LDAP directory* section of the ***Administration Guide*** for full details.

12.2 Configuring and testing the Certificate Authority connection

This varies between different PKI vendors. See the corresponding CA integration guide provided with MyID for details.

12.3 Problems with connecting to the web server

If you experience problems connecting to the web server, check that you have the correct version of .NET Core Hosting installed on the web services server. If you do not have the correct version installed, you may experience some or all of the following issues:

- Clients cannot connect to the MyID server.
- Application pools in IIS do not start.
- You cannot perform an `iisreset` on the web server – when you attempt it, you get an error similar to:

```
Attempting stop...
Internet services successfully stopped
Attempting start...
Restart attempt failed.
The IIS Admin Service or the World Wide Web Publishing Service, or a
service dependent on them failed to start. The service, or dependent
services, may had an error during its startup or may be disabled.
```

If you experience these issues, you are recommended to uninstall MyID, install .NET Core, then reinstall MyID.

Alternatively, as a workaround, you can edit the `applicationHost.config` file on the web server and remove the following lines:

```
<system.web>
  <authentication mode="Windows" />
</system.web>
```

If you then install the correct version of .NET Core, you should be able to proceed.

See section *5*, *Additional hardware and software requirements* for details of obtaining and installing .NET Core.

12.4 Checking the web services

SIU references: SIU-323, SIU-324, SIU-325, SIU-326, SIU-327, SIU-328, SIU-329, SIU-330.

The MyID Installation Assistant carries out a series of checks on the MyID web services as part of its post-installation check.

This ensures that the services have been installed and are running. It does not confirm that the optional web services have been configured fully and are available for use, however; as these web services are secure by default you must review the documentation for each service to ensure that you have configured them correctly and the correct authentication is in place for you to be able to make use of them.

The following web services are checked:

- rest.core – the core MyID REST API, used for the MyID Operator Client.
- rest.provision – the MyID REST API used for mobile identities, mobile identity documents, and soft certificates.
- web.oauth2 – the MyID authentication server.

- Derived Credentials Notifications Listener – see the ***Derived Credentials Notifications Listener API*** guide for details.
- iOS OTA – see the *Setting up iOS OTA provisioning* section in the ***Mobile Identity Management*** guide.
- Credential Web Service – see the ***Credential Web Service*** guide.
- Device Management API – see the ***Device Management API*** guide.
- Lifecycle API – see the ***Lifecycle API*** guide.

13 Licensing

Each installation of MyID requires licensing. Licenses are provided for up to a specific number of user accounts and credentials and may be time-limited.

MyID can be configured to warn system administrators in advance of a license limit being reached; see the *License management* section of the ***Administration Guide*** for details on how to configure this feature.

Warning: To give enough time for the completion of the commercial and administrative processes required to issue a new license prior to a license limit being reached, it is strongly advised that you configure the warning mechanism appropriately.

13.1 Demo licenses

When you first install MyID, your demo license allows you to use MyID for up to 30 days, and allows you to add up to 250 user accounts and credentials. Once you have installed MyID, you can request a license from within MyID using the **Licensing** workflow.

Note: If you upgrade a demo system, your 30 days counts from the first installation of MyID. If you installed your original demo system more than 30 days ago, your license will expire immediately.

13.2 Licensed features

Some features in this release are controlled by your MyID license. Once you have installed the system, you must request a license to ensure that you have access to all the features in this release.

14 Uninstalling MyID

Important: The MyID uninstallation process requires a folder of PowerShell scripts that is located next to the MyID server installation program. If you have moved or deleted this folder, you cannot uninstall MyID using the Windows Control Panel **Programs and Features** option; when it is unable to locate the scripts, the uninstallation process displays an error. To remedy this, you can either put a copy of the original installation program (complete with scripts folder) back in the location from which you originally ran the installation, or uninstall MyID by running the a copy of the originally-installed MyID installation program using **Run as administrator** and selecting the **Remove** option.

Before uninstalling MyID, make sure that you have removed any hotfixes or diagnostic patches from your servers.

To uninstall MyID, log on as the MyID installation user and uninstall MyID through the **Programs and Features** option in the Windows Control Panel. (Note that, due to an issue with Windows, you cannot use the Windows **Apps & Features** screen to uninstall MyID.) Alternatively, you can uninstall MyID by running the MyID installation program using **Run as administrator** and selecting the **Remove** option.

Note: If you have installed MyID to a non-default location, when attempting to uninstall you may see an error similar to:

```
Error 1306. Another application has exclusive access to the file
C:Test\Company\MyID\SSP\MyIDDataSource\MyIDDataSource.log. Please shut down
all other applications, then click retry
```

If this error occurs, open a Windows command prompt, type `iisreset` to reset IIS, which clears the file lock, then click **Retry**.

14.1 Completely removing MyID

When you remove MyID, some files and settings are left behind; this allows you to reinstall MyID when you are upgrading to a new version, for example.

To remove MyID completely:

1. On the database server, delete the MyID database.
2. On the web servers, delete the MyID program folder.

   For example, `C:\Program Files\Intercede\MyID`
3. On the application servers, reboot the PC, then delete the MyID program folder.

   For example, `C:\Program Files\Intercede\MyID`

   Note: If you do not reboot the PC before attempting to remove this folder, you may be unable to remove some of the subfolders.
4. On the application server, delete any MyID `.udl` files from the Windows `System32` folder.

   The uninstallation process may not remove all of these database connection files. These files start with the name you provided for the MyID database; for example, `MyID.udl`, `MyIDaudit.udl` and `MyIDarchive.udl`.
5. On all servers on which MyID has been installed, delete the MyID section of the registry.

You must delete the following section:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Intercede
```

15 Running post-install PowerShell scripts

MyID provides trigger points that allow you to customize your MyID server installation procedure by running post-install PowerShell scripts.

Note: These PowerShell scripts require Windows PowerShell 5.1; see section *4.1.3, Windows PowerShell 5.1*

You can use the following PowerShell command to confirm the installed version:

```
Get-Host | Select-Object Version
```

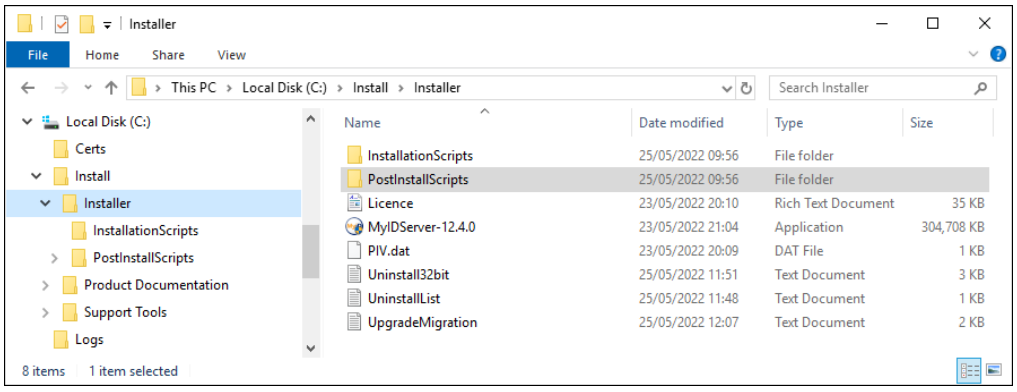
The MyID Installation Assistant can run a PowerShell script automatically at the end of the installation procedure for the following operations:

- Installation
- Uninstallation

15.1 Adding scripts to the installation media

To configure your MyID server installation program to run a PowerShell script automatically:

1. Locate the folder called `PostInstallScripts` in the `Installer` folder that contains the MyID server installation program:



2. In the `PostInstallScripts` folder, the following scripts are provided by default:
   - `Install.ps1` – run automatically at the end of an installation procedure.
   - `Uninstall.ps1` – run automatically at the end of an uninstallation procedure.

   Several PowerShell modules (`.psm1` files) are provided to support the scripts.

   These scripts run automatically at the end of the installation or uninstallation, and configure your system with custom components, web files, translation dictionaries, and database scripts located in the following folders:
   - `Configuration`
   - `ConfigurationDBScripts`

   By default, these folders are empty; if you want to provide your own custom MyID configuration components, files, and database scripts, contact customer support quoting reference SUP-351.

   Alternatively, you can replace these PowerShell scripts with your own scripts.

Note: If Intercede subsequently provides you with configuration updates, these will also use the same filenames – make sure that you merge the changes; if you overwrite the files, you may lose important configuration tasks.

When the provided scripts are run on installation or uninstallation, a log file named `ConfigurationInstall.log` is generated.

15.2 Configuring the provided scripts for non-standard SQL port

When the scripts run, they obtain their connection information from the UDL database connection file. If you have set up a non-standard SQL port, the port number is normally included in the UDL connection.

However, you may require additional configuration if your application and database tiers are on the same physical server; if you have the Shared Memory protocol enabled for SQL Server, the installation program uses that protocol instead of TCP/IP, which means that the UDL file does not contain the TCP/IP connection details, including the port. If you are using the standard port, the PowerShell scripts will connect correctly; however, if you are using a non-standard SQL port, you must edit the `Sql.psm1` module to set the `$SQLPortTCP` variable to the appropriate value.

15.3 Determining which components are installed

You may want to carry out different operations based on which MyID components are installed; for example, you may want to run a database script if the server is being used to install the database components, or to modify web files if the installation is running on the web server.

To do this, you can check the MyID registry in your PowerShell script. For example:

```
$TiersRoot = "HKLM:\SOFTWARE\Intercede\Edefice\Installation"
$AppTier    = Test-Path -Path (Join-Path -Path $TiersRoot -ChildPath "ApplicationTier")
$WebTier    = Test-Path -Path (Join-Path -Path $TiersRoot -ChildPath "WebTier")
$DBTier     = Test-Path -Path (Join-Path -Path $TiersRoot -ChildPath "DatabaseTier")
$ArchDBTier = Test-Path -Path (Join-Path -Path $TiersRoot -ChildPath
"ArchiveDatabaseTier")
$AuthTier   = Test-Path -Path (Join-Path -Path $TiersRoot -ChildPath "ExternalAuthTier")

Write-Output "Checking which MyID server components are installed..."

if ($AppTier)
{
Write-Output "Application server components installed."
}

if ($WebTier)
{
Write-Output "Web server components installed."
}

if ($DBTier)
{
Write-Output "Database server components installed."
}

if ($ArchDBTier)
```

```
{
Write-Output "Archive database components installed."
}

if ($AuthTier)
{
Write-Output "External Authentication Server components installed."
}


if (-Not ($AppTier -or $WebTier -or $DBTier -or $ArchDBTier -or $AuthTier))
{
Write-Output "No MyID server components installed."
}
```