



MyID

Version 10.8 Update 2

Installation and Configuration Guide

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

Copyright

© 2001-2018 Intercede Limited. All rights reserved.

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

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

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

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

Licenses and Trademarks

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

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

Conventions Used in this Document

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

- **Bold** is used for menu items and for labels.
For example:
 - ♦ “Record a valid email address in ‘**From**’ email address”
 - ♦ Select **Save** from the **File** menu

- *Italic* is used for emphasis and to indicate references to other sections within the current document:
For example:
 - ♦ “Copy the file *before* starting the installation”
 - ♦ “See *Issuing a Card* for further information”

- ***Bold and italic*** are used to identify the titles of other documents.
For example: “See the ***Release Notes*** for further information.”
Unless otherwise explicitly stated, all referenced documentation is available on the installation CD.

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

- **Notes** are used to provide further information, including any prerequisites or configuration additional to the standard specifications.
For example:
Note: This issue only occurs if updating from a previous version.

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

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

Contents

| | |
|--|-----------|
| Installation and Configuration Guide | 1 |
| 1 Introduction..... | 8 |
| 1.1 Change history..... | 8 |
| 1.2 System Interrogation Utility | 8 |
| 2 Hardware and Software Requirements | 9 |
| 2.1 MyID server | 9 |
| 2.1.1 Hardware requirements | 9 |
| 2.1.2 Operating systems | 9 |
| 2.1.3 Database | 9 |
| 2.2 Client workstation | 10 |
| 2.2.1 Hardware requirements | 10 |
| 2.2.2 Operating systems | 10 |
| 2.2.3 Internet Explorer | 10 |
| 2.3 Virtual environments and remote connections..... | 11 |
| 2.4 Mobile devices | 11 |
| 2.5 Network..... | 11 |
| 2.6 Card printers | 12 |
| 2.7 Image capture | 12 |
| 2.7.1 Webcams..... | 12 |
| 2.7.2 Scanning support in MyID 10.7 and later | 12 |
| 2.7.3 Tested scanners | 13 |
| 2.7.4 Signature capture | 13 |
| 2.8 Directories..... | 13 |
| 2.9 Certificate authorities | 13 |
| 2.9.1 Additional certificate authorities | 14 |
| 2.10 Other security products..... | 14 |
| 2.10.1 HSM (Hardware Security Modules) | 14 |
| 2.11 Supported card readers and card types..... | 14 |
| 2.11.1 Card readers..... | 14 |
| 2.11.2 Supported smart cards and tokens | 14 |
| 2.11.3 Virtual Smart Cards | 14 |
| 3 Getting Started..... | 15 |
| 3.1 Basic concepts..... | 15 |
| 3.1.1 Personnel account management | 15 |
| 3.1.2 Role separation..... | 15 |
| 3.1.3 Groups and Directory Organizational Units..... | 15 |
| 3.1.4 Scope and multiple roles | 16 |
| 3.1.5 Extended attributes..... | 16 |
| 3.1.6 Credential personalization | 16 |
| 3.1.7 Issuance models..... | 17 |
| 3.2 Quick start system check | 18 |
| 3.3 Suggested configuration sequence..... | 18 |
| 3.3.1 Roles | 19 |
| 3.3.2 Groups..... | 19 |
| 3.3.3 Certificate templates | 19 |
| 3.3.4 Card layouts..... | 20 |
| 3.3.5 GlobalPlatform keys..... | 20 |
| 3.3.6 Applets..... | 20 |
| 3.3.7 Licensing..... | 20 |
| 4 Preparation and Setup | 21 |
| 4.1 Licensing..... | 21 |
| 4.1.1 Demo licenses | 21 |
| 4.1.2 Licensed features | 21 |
| 4.2 Preparation | 21 |
| 4.2.1 Deployment strategy | 21 |

| | | |
|----------|--|-----------|
| 4.2.2 | Prerequisites | 22 |
| 4.2.3 | User accounts | 22 |
| 4.2.4 | Integration with other products | 24 |
| 4.2.5 | Launch and activation permissions | 24 |
| 4.2.6 | Web server on a separate machine | 25 |
| 4.3 | Timeouts, limits and other settings | 26 |
| 4.3.1 | Windows 32KB ASP process limit | 26 |
| 4.3.2 | Component transaction timeout | 26 |
| 4.3.3 | MSDTC security configuration | 27 |
| 4.3.4 | Windows Firewall settings | 28 |
| 4.3.5 | Setting up email | 28 |
| 4.3.6 | ISA Server connection limit | 28 |
| 4.3.7 | Post-installation IIS server caching | 29 |
| 4.3.8 | ADO and MSADC requirements on the application server | 29 |
| 4.4 | Temporary folders for remote connection | 29 |
| 4.5 | Database setup | 30 |
| 4.5.1 | Additional database configuration considerations | 30 |
| 4.6 | Setting up server roles | 31 |
| 4.6.1 | Server roles for Windows Server 2012 R2 | 31 |
| 4.6.2 | Server roles for Windows Server 2016 | 32 |
| 4.7 | Client software | 33 |
| 4.7.1 | Cards and card readers | 33 |
| 4.7.2 | JAWS screen reader | 34 |
| 4.8 | Configuring Internet Explorer | 34 |
| 4.8.1 | Adding the MyID website to the Trusted sites or Local intranet group | 34 |
| 4.8.2 | Disabling the pop-up blocker | 34 |
| 4.8.3 | Exceptions | 35 |
| 4.8.4 | Performance improvements for client PCs without internet access | 35 |
| 5 | Installing MyID | 36 |
| 5.1 | Overview | 36 |
| 5.2 | Split deployment | 37 |
| 5.3 | Upgrading | 38 |
| 5.3.1 | Before you upgrade | 38 |
| 5.3.2 | Upgrading clients | 39 |
| 5.3.3 | Upgrading systems with custom LDAP mappings | 39 |
| 5.3.4 | Upgrading from MyID 10.0 or earlier | 39 |
| 5.3.5 | Upgrading from MyID 10.1 – 10.6 | 41 |
| 5.3.6 | Upgrading from MyID 10.7 | 43 |
| 5.3.7 | Installing the latest updates | 44 |
| 5.3.8 | Upgrading credential profiles | 44 |
| 5.3.9 | Upgrading security phrase security | 45 |
| 5.3.10 | Upgrading roles | 46 |
| 5.3.11 | Upgrading email support | 46 |
| 5.3.12 | Upgrading the storage of PINs for HSMs | 46 |
| 5.3.13 | Modifying an existing installation | 46 |
| 5.3.14 | Upgrading systems with Virtual Smart Cards | 47 |
| 5.3.15 | Upgrading SQL Server configuration | 47 |
| 5.3.16 | Upgrading the web service user account | 47 |
| 5.3.17 | Upgrading systems with a startup user | 47 |
| 5.3.18 | Upgrading systems with a web server outside the domain | 47 |
| 5.3.19 | Upgrading systems with older data models | 47 |
| 5.3.20 | Upgrading systems with customized data models | 48 |
| 5.3.21 | Upgrading systems with Project Designer customizations | 48 |
| 5.3.22 | Upgrading renewal jobs | 48 |
| 5.3.23 | Upgrading card issuance jobs | 48 |
| 5.3.24 | Known issues with upgrading | 49 |
| 5.4 | Running the installation program | 49 |
| 5.4.1 | NT Event Log messages | 54 |
| 5.5 | Running GenMaster | 55 |
| 5.5.1 | Using GenMaster | 55 |
| 5.6 | Setting the HSM PIN | 61 |
| 5.7 | Required updates | 62 |

| | | |
|-----------|---|-----------|
| 6 | Securing the MyID Application..... | 63 |
| 6.1 | Device security settings | 63 |
| 6.2 | Access to the MyID web application | 63 |
| 6.3 | Secure access to diagnostic files..... | 63 |
| 6.4 | MyID and SQL Server permissions..... | 64 |
| 6.5 | MyID and COM+ permissions | 65 |
| 6.6 | MyID startup | 66 |
| 6.6.1 | Using the Startup utility | 66 |
| 6.6.2 | Using Startup with an HSM-based master key | 66 |
| 6.6.3 | Startup utility procedure | 67 |
| 6.7 | eKeyServer Service | 67 |
| 6.8 | Protecting the registry | 69 |
| 7 | Testing the Installation | 70 |
| 7.1 | Configure and test the directory connection..... | 70 |
| 7.2 | Configure and test the Certificate Authority connection | 70 |
| 7.3 | Configuring client PCs | 70 |
| 7.4 | Installing MyID Desktop | 70 |
| 7.5 | Configuring MyID Desktop | 72 |
| 7.5.1 | Communication between MyID Desktop and the MyID server | 72 |
| 7.5.2 | Server location | 72 |
| 7.5.3 | One-way SSL/TLS | 73 |
| 7.5.4 | Two-way SSL/TLS | 73 |
| 7.5.5 | Logging..... | 76 |
| 7.5.6 | Troubleshooting connection problems | 76 |
| 7.6 | Launching MyID Desktop..... | 76 |
| 7.6.1 | Launching MyID Desktop with a specific server..... | 76 |
| 7.6.2 | Launching MyID Desktop with a specific workflow..... | 77 |
| 7.6.3 | Launching MyID Desktop for credential activation | 77 |
| 7.6.4 | Launching MyID Desktop for credential unlocking | 77 |
| 7.6.5 | Launching MyID Desktop with a logon code | 78 |
| 7.6.6 | Launching MyID Desktop with automatic Windows Logon | 78 |
| 7.6.7 | Launching MyID Desktop from a hyperlink | 78 |
| 7.7 | MyID Desktop version number..... | 79 |
| 8 | After Installing MyID..... | 80 |
| 8.1 | Integrating with other products..... | 80 |
| 8.2 | Internationalization and localization | 80 |
| 8.2.1 | Specifying the language for MyID Desktop | 80 |
| 8.3 | Email notification..... | 81 |
| 8.4 | Using a separate audit database | 81 |
| 8.4.1 | Create a separate database for audit records..... | 81 |
| 8.5 | Archiving the audit trail | 83 |
| 8.5.1 | Create a separate database for archiving audit records | 83 |
| 8.5.2 | Create an SQL Timed Task on SQL Server 2012..... | 85 |
| 8.6 | Archiving the System Events | 88 |
| 8.7 | Creating database maintenance plans | 88 |
| 8.8 | Scheduled certificate revocation operations | 89 |
| 8.9 | Application recycling | 89 |
| 8.9.1 | Settings for COM+ components..... | 89 |
| 8.10 | HSM concurrency | 90 |
| 8.10.1 | Concurrent sessions | 90 |
| 8.10.2 | Retries | 91 |
| 8.11 | IIS server caching | 91 |
| 9 | Setting Up Email | 92 |
| 9.1 | Signing email messages | 93 |
| 10 | Uninstalling MyID | 94 |
| 10.1 | Completely removing MyID..... | 94 |

| | | |
|-----------|---|------------|
| 11 | Business Continuity Planning..... | 95 |
| 11.1 | Phase 0: Pre-disaster | 95 |
| 11.2 | Recovery..... | 95 |
| 11.3 | High-level recovery plan for re-building a three-server architecture..... | 95 |
| 11.3.1 | Phase 1: Prepare new servers..... | 95 |
| 11.3.2 | Phase 2: Restore backed-up data | 96 |
| 11.3.3 | Phase 3: Test new system..... | 96 |
| 11.4 | Two-server and one-server architectures | 96 |
| 11.5 | System integration | 96 |
| 12 | Failover Strategy | 98 |
| 12.1 | Typical MyID architectures..... | 98 |
| 12.2 | Co-hosted web and application servers..... | 99 |
| 12.2.1 | Duplicate infrastructures | 99 |
| 12.3 | Split web and application servers | 100 |
| 12.4 | Additional considerations | 100 |
| 12.4.1 | User images..... | 100 |
| 12.4.2 | Clustering..... | 101 |
| 12.4.3 | Hardware | 101 |
| 12.5 | Failover and redundancy considerations | 102 |
| 13 | Advanced Deployment..... | 105 |
| 13.1 | Windows services | 105 |
| 13.2 | Communication, security and trust..... | 105 |
| 13.2.1 | Client to web server | 105 |
| 13.2.2 | Web server to MyID server | 106 |
| 13.2.3 | Application server to database server..... | 107 |
| 13.2.4 | Application server to LDAP directory server | 108 |
| 13.3 | Application pools..... | 109 |
| 13.4 | Running multiple servers | 109 |
| 13.4.1 | Multiple web servers | 109 |
| 13.4.2 | Multiple application servers..... | 110 |
| 13.4.3 | Multiple tiers with a web server in a DMZ | 111 |
| 13.4.4 | SQL Server clustering..... | 112 |
| 13.4.5 | Restricting available workflows | 113 |
| 13.5 | Performance and sizing | 113 |
| 13.5.1 | Performance | 113 |
| 13.5.2 | Sizing..... | 114 |
| 13.6 | Other considerations..... | 115 |
| 13.6.1 | Operating across multiple time zones | 115 |
| 13.6.2 | Running multi-lingual environments..... | 116 |
| 14 | Workflow IDs..... | 117 |

1 Introduction

This document describes how to install and configure MyID®.

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 Change history

| Version | Description |
|------------|---|
| IMP1736-01 | First version provided with MyID 10.0. |
| IMP1736-02 | Updates to wording and formatting. |
| IMP1736-03 | Updates to support MyID 10.1. |
| IMP1736-04 | Updates to support MyID 10.2. |
| IMP1736-05 | Updates to support MyID 10.3. |
| IMP1736-06 | Updates to support MyID 10.3 update 1 |
| IMP1736-07 | Updates to support MyID 10.4. |
| IMP1736-08 | Updates to support MyID 10.5. |
| IMP1736-09 | Updates to support MyID 10.6. |
| IMP1736-10 | Updates to support MyID 10.6 Update 1. |
| IMP1736-11 | Updates to support MyID 10.7. |
| IMP1736-12 | Updates to support MyID 10.7 Update 1. |
| IMP1736-13 | Updates to support MyID 10.8. |
| IMP1736-14 | Updates to support MyID 10.8 Update 1. |
| IMP1736-15 | Updates to support MyID 10.8 Update 2. |
| IMP1736-16 | Updated with clarifications regarding the update process. |

1.2 System Interrogation Utility

The System Interrogation Utility, provided in the Support Tools folder on the MyID product CD, allows you to check that your system is correctly configured to install MyID; and once MyID is installed, it confirms that your system is configured correctly. Use the tool in conjunction with this [Installation and Configuration Guide](#).

See the [System Interrogation Utility](#) guide provided with the utility for details.

2 Hardware and Software Requirements

Warning: 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.

2.1 MyID server

2.1.1 Hardware requirements

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.

See also section [13.5, Performance and sizing](#).

- 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.

2.1.2 Operating systems

MyID supports the following server operating system:

- Windows Server 2012 R2
- Windows Server 2016

2.1.3 Database

MyID has been tested with the following SQL Server versions:

- SQL Server 2016 SP1 – CU3 for 2016 SP1 (13.0.4435.0 – May 2017)
- SQL Server 2014 SP2 – CU4 for 2014 SP2 (12.0.5540.0 – February 2017)
- SQL Server 2012 SP3 – CU7 for 2012 SP3 (11.0.6579.0 – January 2017)

Note: Intercede recommend using the database versions listed above. If you are going to use alternative service pack or cumulative update versions, make sure that you carry out additional testing within your environment. For production deployment, SQL Server Enterprise or Standard editions must be used.

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 Microsoft Azure as the database. See the [Microsoft Azure Integration Guide](#) for details.

2.2 Client workstation

2.2.1 Hardware requirements

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 card, you need smart card reader and drivers (see section [2.11, Supported card readers and card types](#))

2.2.2 Operating systems

- Microsoft Windows 7 SP1 (32-bit or 64-bit)
MyID has been tested with the Professional edition. Other variants are expected to work dependent on third party device support.
- Windows 8.1
- Windows 10
 - ♦ Windows 10 November Update (32-bit and 64-bit) – Version 1511
 - ♦ Windows 10 Anniversary Update (32-bit and 64-bit) – Version 1607
 - ♦ Windows 10 Creators Update (32-bit and 64-bit) – Version 1703
 - ♦ Windows 10 Fall Creators Update (32-bit and 64-bit) – Version 1709

Note: Throughout the MyID documentation, where "Windows 10" is listed as a supported operating system, this includes the versions listed above.

Some third party software and devices used with MyID are not supported on certain platforms. See the relevant integration guide for details.

Some product features may not be supported on both 32-bit and 64-bit architectures.

2.2.3 Internet Explorer

MyID Desktop uses Internet Explorer to display workflows within the application.

Note: Microsoft Edge is not supported.

The following combinations of operating system and browser have been tested:

| Operating System | Internet Explorer version | Notes |
|------------------------|---------------------------|---|
| Windows 7 SP1 (32-bit) | Internet Explorer 11 | |
| Windows 7 SP1 (64-bit) | Internet Explorer 11 | MyID runs in Internet Explorer Compatibility View. Enhanced Protected Mode of Internet Explorer 11 is supported. |

| Operating System | Internet Explorer version | Notes |
|------------------|---------------------------|---|
| Windows 8.1 | Internet Explorer 11 | MyID runs in Internet Explorer Compatibility View. Enhanced Protected Mode of Internet Explorer 11 is supported. |
| Windows 10 | Internet Explorer 11 | MyID runs in Internet Explorer Compatibility View. Enhanced Protected Mode of Internet Explorer 11 is supported. |

32-bit and 64-bit versions of Internet Explorer

MyID Desktop automatically uses the 32-bit version of Internet Explorer.

MyID Desktop does not currently support the 64-bit version of Internet Explorer. If you require the use of a 64-bit version, contact Intercede to discuss the requirement further.

2.3 Virtual environments and remote connections

If you are using virtual environments (for example, VMware or Microsoft Azure):

- 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) 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.
- Virtual environments are not supported for client installations; clients must be installed on a supported native Windows platform.
- Currently, MyID Desktop, Self-Service App, and Self-Service Kiosk are not supported over remote desktop connections.

2.4 Mobile devices

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

See the [Mobile Identity Management Installation and Configuration Guide](#) for details of the operating system versions and secure key stores supported.

2.5 Network

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).

2.6 Card printers

For more information on printers, including driver, firmware, and operating system support, see the [Printer Integration Guide](#).

MyID has been tested with the following printers:

- Fargo HDP 5000.
Support for other Fargo printers may be available on request.
- DataCard CD800, SP35, SP55 and SP75.
- Magicard Rio Pro/Rio Tango 2e.
- DIGID XID590ie.
- Zebra ZXP-7, ZXP-8.

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.

2.7 Image capture

MyID supports webcams for capturing user photographs, scanners for capturing documents, and pads for capturing signatures.

2.7.1 Webcams

On Windows 7, MyID supports any DirectX-compatible webcam supported by Video for Windows. MyID has been tested with Microsoft, Logitech and Creative webcams.

On Windows 8.1 and Windows 10, there is currently more limited support for webcams due to the shortage of fully-compatible drivers. MyID has been tested with a Microsoft LifeCam HD-3000. You must ensure that the webcam you intend to use with MyID is supported on Windows 8.1 or Windows 10 and appropriate drivers are available.

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 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 such as Windows 8.1.

2.7.2 Scanning support in MyID 10.7 and later

Use of EZTWAIN for scanning has been replaced with a simpler integration method. TWAIN scanning is no longer supported, and the standard WIA2 method is used instead.

You do not need to set the **Scanner driver support** configuration option.

2.7.3 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
Tested on Windows 7 (32-bit and 64-bit).
- Canon CanoScan LiDE 220 – LiDE 220 Scanner Driver Ver. 20.4.0.16
Tested on Windows 7 (64-bit) and Windows 8.1 (64-bit).
- Epson Perfection V500 Photo – EPSON Scan 3.770

2.7.4 Signature capture

MyID supports the following signature capture devices:

- Interlink Electronics ePad
- Interlink Electronics ePad II
- Interlink Electronics ePad-ink

MyID has been tested using Interlink Electronics Universal Installer v10.5.

Signature capture is supported on Windows 7 using 32-bit browsers only.

Currently, signature capture on Windows 8.1 or Windows 10 is not supported due to the lack of available drivers.

Use of signature capture devices with MyID requires additional customization. Contact customer support for more information, quoting reference SUP-105.

2.8 Directories

V3 compliant LDAP directory providers are supported by MyID and must be fully operational before installing MyID.

MyID has been tested against the following directory:

- Microsoft Active Directory

2.9 Certificate authorities

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

- Microsoft Windows Server Certificate Services
- Symantec
- Entrust
- 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.

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.

2.9.1 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:

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

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

2.10 Other security products

2.10.1 HSM (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:

- nCipher nShield Connect
- nCipher nShield Solo
- SafeNet LUNA SA

2.11 Supported card readers and card types

2.11.1 Card readers

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

2.11.2 Supported smart cards and tokens

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

2.11.3 Virtual Smart Cards

MyID supports the following types of Virtual Smart Card (VSC):

- Microsoft virtual smart cards
- Intel virtual smart cards

See the [*Microsoft Virtual Smart Card Integration Guide*](#) and [*Intel Virtual Smart Card Integration Guide*](#) for details.

3 Getting Started

MyID provides a comprehensive management solution to the problems associated with the issuance and maintenance of credentials to smart cards and tokens as well as hardware devices such as tablets, computers, smart phones and other mobile devices. It can help you to retain full control over the content and lifecycle of these devices and credentials, while permitting day to day operation by non-expert staff.

This document explains the design processes and configuration steps that you need to undertake to deploy MyID in your organization in the most efficient manner.

3.1 Basic concepts

To work effectively with MyID, it is important to understand some of the basic concepts that are fundamental to the product. These are primarily concerned with personnel account management, device content control and issuance models.

3.1.1 Personnel account management

A User Account is created for each MyID user in the MyID database. These accounts hold information about the individuals, which includes their rights and privileges within MyID and the devices and credentials that are known to be issued to them.

In any IT system, there are often many sources of information relating to individuals – directories, HR systems, accounting packages etc. MyID can integrate with systems such as these to collect and share such information, and also record data that is specific to MyID (such as roles and issued credentials).

User information must be kept current and MyID acts as a ‘cache’ for data that has been read from other systems. This means that it can be configured to verify that the user details are still correct before the data is used.

MyID can also be used as the primary owner of this information – data can be entered about a person directly to the user interface, and also provide business processes to ensure that information is in the correct and approved state prior to credentials being issued.

3.1.2 Role separation

A fundamental concept in the design of a secure credential issuance system is that of ‘Role Separation’. This describes the practice of ensuring that no individual is permitted both to enroll users and issue credentials, thus avoiding a single point of failure in the deployment.

To support this, MyID lets you define multiple named ‘Roles’, each of which is granted access to a chosen subset of the MyID management options. Some default roles are provided as standard, but you may prefer to design your own roles to suit your particular organization and expected issuance models.

3.1.3 Groups and Directory Organizational Units

MyID lets you organize personnel into ‘Groups’. These form a strict hierarchy, with each person belonging exclusively to a single group. This structure should normally be used to represent the reporting structure within your organization, since it forms the basis for defining the security ‘scope’ of each person.

If you are integrating with a directory, groups are usually associated with a particular Organizational Unit. This is especially important if you have a Certification Authority using data from the same directory (for example, to support Windows smart card logon). MyID is able to record such relationships and provides synchronization, import, and export options to help maintain the integrity of the overall solution.

3.1.4 Scope and multiple roles

A common problem with strict role-based authorization systems is that they struggle to accommodate the real-world situations where most people have multiple roles within their job description. Typically this means that you have to define role content for every possible combination of actual roles. MyID avoids this problem by permitting the allocation of multiple roles to each individual. In this manner, a person may be both a Manager and a Help Desk Operator without needing to define a 'Manager and Help Desk Operator' composite role.

The MyID roles mechanism can combine the allocation of a role to a person with the concept of 'Scope'. This determines which user accounts the person is allowed to manage within the menu options associated with the role. For example, individuals can be managers for people in their own groups and help desk operators for everyone in the organization.

Under these circumstances, a person connecting to MyID will see the combined set of menu options that are available for each of the assigned roles. However, when they execute each option they will only see those user account that they are allowed to carry out the selected operation on, according to their roles and associated scope.

Also, Administrative Groups can be used to allow an operator to manage user accounts located in MyID groups anywhere within the group hierarchy, including groups that are not directly connected to the operator's home group. See the [Administration Guide](#) for details.

3.1.5 Extended attributes

MyID can be customized by adding attributes to record further information for objects held in the MyID database – for example, you may want to record postal addresses for each person or an asset tag number for a stored device. These attributes can then be used in management and personalization processes. The definition and implementation of custom attributes generally requires advice and assistance from the Professional Services team.

3.1.6 Credential personalization

Smart cards and tokens can be personalized electronically with a wide range of credentials, applications and data. These can be applied to either the contact or contactless portions of suitable cards and tokens. In addition, cards can be physically printed using a mixture of static and dynamic data, such as logos, photographs, names, dates and serial numbers.

Many mobile and other computing devices incorporate secure elements such as UICC SIM cards, secure microSD cards and Trusted Platform Modules that can behave in a similar way to smart cards. There are a growing number of software based alternative solutions that may also offer secure storage of credentials.

With such a range of possibilities, it is important to define and control a finite number of valid combinations, so that you can be certain that all issued devices and credentials will behave correctly in the application environment for which they were created.

To manage this, MyID lets you create named credential profiles. A profile defines:

- what may be issued – the technology type such as a smart card, a printed identity badge, a virtual smart card or mobile identity
- the policy to be used – what are the PIN requirements, how shall the device be personalized, is an authentication code or fingerprint match required before issuance can take place
- how the request process is controlled – is pre-enrollment required, should an administrator approve issuance of this profile to a user
- which certificates are to be issued by the integrated PKI

This logical definition can also be associated with one or more visual ID badge layouts, giving you the ability to include rapid visual identification of logically different card types should you wish.

Finally, each credential profile has an associated list of permitted recipient roles and issuers. This means that you can define card content for different levels of privilege and be certain that they can only be issued to and by people who have been assigned the appropriate roles within MyID.

3.1.7 Issuance models

MyID supports a wide range of issuance models. You should be able to find an appropriate combination to suit your particular business model, whether this is primarily face-to-face, self-service or centralized bulk issuance. MyID lets you implement multiple issuance models, since we recognize that the method used for initial deployment is likely to be different to that needed for 'steady state' post-issuance management.

The important thing to consider is how the different stages of card and credential lifecycle are to be managed. The primary phases are:

- **Enrollment**
How will you get user details into MyID? This might be individual keyed entry, import from a directory, or import through a web service.
- **Request**
Will a card be requested at enrollment time or as a separate operation? Can users request their own credentials or should this be done by their manager or an administrator?
- **Request authorization**
Do you want to have an additional person to authorize requests for cards?
- **Collection**
Are the credentials to be collected by the users or their managers? Will you use a bureau or desktop printing? Are credentials to be collected in person or distributed by mail?
- **Unblocking**
When the credentials are protected by a PIN, it is common for the PIN to be forgotten or become locked after a number of authentication attempts with the wrong value. Do you want users to be able to unblock the PIN on their own or should this be done by a manager or via a telephone help desk?
- **Canceling and suspension**
Will the credentials be canceled centrally or remotely? Is any smart card recycling expected? What 'Reasons for Replacement' are required and what should the corresponding action be?
- **Activation**
Are the credentials enabled immediately once created, or are they issued in a locked state, requiring an activation process either by the credential owner or with the help of an operator? How do you want to deal with this activation – do you want to use one-time authorization codes or pre-registered security questions to prove the identity of the owner?

3.2 Quick start system check

Once you have installed MyID, following the instructions in this document, you should have completed the following steps:

1. Installation of MyID application server, web server and database.
2. Initialization of the system and creation of a startup user password using GenMaster.
3. Configuration of a client PC.
4. Installation of MyID Desktop client.

Note: Ensure you follow the instructions for configuring your client's Internet Explorer. Log on to MyID with the startup user.

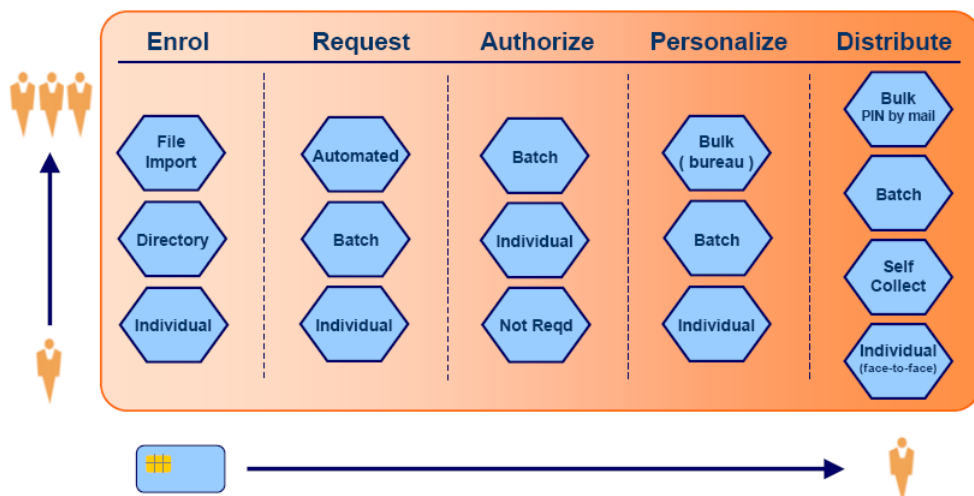
To test basic operation, you should try the following sequence:

1. Add a user – check the connection to LDAP to import a user, if you are using an LDAP directory.
2. Check CA configuration and (if present) enable at least one certificate policy for issuance.
3. Create a Credential Profile with MyID logon and a certificate (if a CA is present).
4. Issue a card to the user you created.
5. Check the certificate is on the card.
6. Verify logon to MyID with the newly issued card.
7. Cancel the card.
8. Check the certificate has been revoked.

3.3 Suggested configuration sequence

Before you start to install your production environment, it is essential that you design your implementation carefully. In many cases, this is best done through an iterative process, using a pilot or test installation to refine the model.

The first thing to consider is what issuance model(s) you want to implement, since this will directly affect the menu options and management roles that you will need. The simplest approach to this is to use the diagram below to decide which mechanism(s) you want to use for each stage in the card and credential's lifecycle.



This should enable you to decide whether you want to use one-pass face-to-face card issuance, a separate request-authorize-collect design, whether you are printing cards centrally or collecting remotely etc. It is important that this design stage is considered carefully, so that you have a consistent, efficient deployment model that meets your business objectives.

3.3.1 Roles

Use the issuance model requirements to define the roles that you will need to operate the system. Try to keep the roles 'atomic' in nature; that is, define discrete job functions rather than try to create a role for each combination of tasks that individuals may perform in your organization.

As an example, you might define a CardHolder role to contain those operations available to every cardholder (for example, Collect My Card). If you then define a 'Personnel' role, you should not repeat Collect My Card within that role, since you will expect every Personnel operator to also be a CardHolder. If you construct roles in this manner, it becomes much easier to change individual roles in one place.

3.3.2 Groups

Next, you should establish the organizational group structure that you will use to control the lines of authority within your MyID deployment. This may be by job function, geographically, based on LDAP Organizational Units etc. It is important that this structure matches the 'Scope' of the roles that you have defined; usually this will reflect the reporting structure of your organization.

Many organizations will choose to use their LDAP Organizational Unit structure as the basis for their MyID group structure. In this case, we advise that before adding users to MyID, you should use the Edit Groups option to import the LDAP structure and thus create the MyID groups automatically. You may subsequently add to and modify your MyID groups if you wish.

Warning: If you are integrating with authentication servers or disk encryption solutions, you should ensure that the connections to these external components are configured BEFORE creating MyID Groups or Users. This is because MyID group information must be 'pushed' to the external system as it is created.

3.3.3 Certificate templates

If you intend to use PKI certificates, you should now verify the connection to your certification authority (CA) and decide which certificate templates you will need to be issued through MyID. This will need someone with reasonable PKI knowledge and a good understanding of the applications and functions for which certificates are to be used. See your CA integration guide for details.

For each template (sometimes referred to as a 'policy') in each CA, you must decide whether it will be made available for MyID issuance, what friendly name and description you want it to have, plus settings such as key length, duration, hardware/software issuance, etc.

When choosing friendly names for templates, you should consider that the person who will be using these names is the individual responsible for defining credential profiles. Their perspective is likely to be from a 'Business Services' viewpoint, so where appropriate, you should name templates to indicate the service(s) they are to be used for, rather than a description of their implementation and origin. As an example, you might rename 'Client signing 1024-RSA-365 on CA1' as 'Email Signature'.

3.3.4 Card layouts

If you are using smart cards that need to be printed to display details of your organization or the card holder, you should create a card layout using the Card Layout Editor. It is usually easiest to create composite images for the backgrounds using tools such as Photoshop or Paintshop Pro, and then store these as GIF or JPEG files. Typical card printers are capable of around 600dpi printing, so your images should be at least 2000x1275 pixels to take advantage of this.

Barcodes and magnetic stripe information are also configured through the Card Layout Editor. For barcodes, you should pick a 3 of 9 barcode font for fixed or system text items. For further information on a suitable font, contact customer support, quoting reference SUP-106.

The font must be installed on the client PC to operate and may need a script change to MyID if it is not a font that is supported by default; contact professional services if you are unsure about this.

For magnetic stripe information, choose one of the magstripe1-3 fonts. You may position the magstripe text outside the displayed area of the card; it will be ignored by the 'Fit to Content' operation in the editor.

3.3.5 GlobalPlatform keys

If you are writing applets to Java cards, or you wish to change the GlobalPlatform keys for cards at issuance, you should define the Factory and Customer keys at this point.

See the [Administration Guide](#) and the [System Security Checklist](#) for details.

3.3.6 Applets

If you need to add applets to Java smart cards, you will need to prepare and install the applets. Contact Intercede for further details of this process.

3.3.7 Licensing

MyID has a licensing mechanism that you must activate soon after installation. Without activation, MyID is restricted to a maximum of 25 user accounts for a maximum of 30 days. To request or install a license, from the Configuration category in MyID, select the **Licensing** workflow. The licensing process involves an email contact to customer support, so you should plan ahead to avoid delays in your implementation.

4 Preparation and Setup

4.1 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 MyID [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.

Contact your system installer for details if you require any assistance in configuring this feature.

4.1.1 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 25 user accounts and credentials.

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.

4.1.2 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.

4.2 Preparation

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.

4.2.1 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.

4.2.2 Prerequisites

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

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

Note: MyID is developed and tested using .NET framework 4.6. If you need to use a later version of the .NET framework, contact customer support quoting reference SUP-283.

The Microsoft .NET framework version 4.6 *must* be installed on web server, application server, and database server before you install MyID. The database server must also have .NET framework version 3.5 installed.

You can install support for .NET framework version 4.6 on Windows Server 2016 by setting the appropriate server roles. For more details, see section [4.6, Setting up server roles](#).

Note: For Windows Server 2012 R2, you must upgrade your system from .NET 4.5 to .NET 4.6. See the Microsoft website for details. See also Microsoft KB2919355 for details of a required update.

- Databases

Supported databases are listed in section [2.1.3, Database](#).

- Default Web Site

On the MyID web server, you must have a web site called Default Web Site within IIS (Internet Information Services).

Note: If you have problems when submitting large amounts of data to an ASP page, and receive an error regarding buffer limits, you must increase the limits in IIS. See section [4.3, Timeouts, limits and other settings](#) for details.

4.2.3 User accounts

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

- Installation

We recommend that your installation is carried out using a domain user that is part of the local Administrators 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.
- ♦ Must have 'dbcreator' and 'public' Server Role privileges for their logon to SQL Server.

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

Note: You are also recommended to ensure that the installation user is permitted to impersonate a client after authentication. On rare occasions, Windows service packs have caused installation problems that this membership will overcome.

On both the application server and the web server, use the Windows Local Security Policy Editor to add the **Impersonate a client after authentication** option from the User Rights Assignment section of the Local Policies to the installation user.

- MyID COM+ account

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.
- ♦ 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.

After creating the account, on the MyID application server:

- a) Run the **Local Security Policy** application.
- b) Under **Local Policies**, select **User Rights Assignment**.
- c) Double-click **Log on as a service**.
- d) 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.

- IIS user account

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.
- ♦ 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.
- ♦ Set the password for the account so that it does not expire.
- ♦ Ensure the account is active (not disabled), unlocked, and does not expire.

- Web service user account

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.
- ♦ 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.
- ♦ Set the password for the account so that it does not expire.
- ♦ Ensure the account is active (not disabled), unlocked, and does not expire.

4.2.4 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.

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.

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.

4.2.5 Launch and activation permissions

You must grant additional permissions to the account used to run MyID.

Note: Follow the following instructions for a deployment with the web server and application server on the same machine. For a split deployment, see section [4.2.6, Web server on a separate machine](#).

On the server holding the MyID components (the application server) the MyID COM+ user account must be given **Local Launch** and **Activation** permissions in the **COM Security** section.

For example:

1. Open the Windows **Component Services** tool.
2. Expand the **Component Services** tree until you can see **My Computer**.
Right-click **My Computer** and select **Properties** from the menu.

3. 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 MyID COM+ account.
 - d) Ensure that the **Allow** options for **Local Launch** and **Local 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
```

4.2.6 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**.
Right-click **My Computer** and select **Properties** from the menu.
6. 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
```

4.3 Timeouts, limits and other settings

4.3.1 Windows 32KB ASP process limit

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 32KB 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.

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.

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).

Increase the following field to 00:04:00:

- ♦ **Script Time-out**

This will reduce the likelihood of the timeout being reached prior to completion.

3. Click **Apply**.
4. Restart IIS.

4.3.2 Component transaction timeout

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.

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**.

4.3.3 MSDTC security configuration

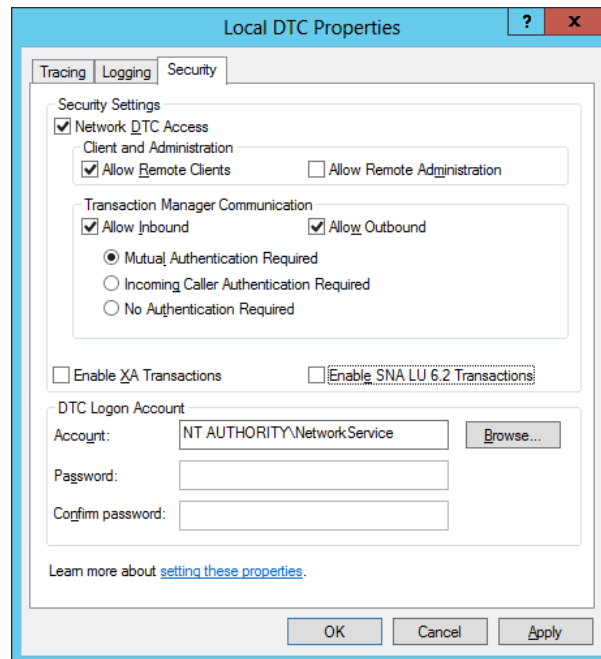
If your system is split across more than one server you must set up your MSDTC security on the web server, application server and the database server to allow access. If you experience an error similar to the following, you may have to check either your MSDTC or Windows Firewall configuration:

Unable to perform the requested operation

Set up your MSDTC settings on the application and database tiers.

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. See [5.4, Running the installation program](#) for details.

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.

4.3.4 Windows Firewall settings

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

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**.

4.3.5 Setting up email

You can set up your system to send email messages from within MyID. See section [9, Setting Up Email](#).

4.3.6 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 SYSWOW64\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.

4.3.7 Post-installation IIS server caching

After you have installed MyID, you must set up your IIS server caching. See section [8.11, IIS server caching](#) for details.

4.3.8 ADO and MSADC requirements on the application server

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 Temporary folders for remote connection

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

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.

4.5 Database setup

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. If the application server is not the same PC as the database server, install the following SQL Server tool packages on the MyID application server:

- ◆ Client Tools Connectivity.

You must also make sure that the above SQL Server tools are installed on the PC on which you run the database tier of the installation program. For simplicity, you can run the database tier of the installation program from the MyID application server.

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.

4.5.1 Additional database configuration considerations

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 account you specify has the correct permissions to create a database on your SQL Server.

If you are installing MyID into an already-created database, you do not need user permissions to create a database; however, you *do* need permissions to alter the schema.

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.

When you are installing MyID (or a patch for MyID), it is helpful to have the SQL Server Browser service running (found in **Administrative Tools > Services**); this helps the installation program to find the SQL Server if you are installing from a separate tier. You can disable the SQL Server Browser service after you have completed the installation.

See section [6.4, MyID and SQL Server permissions](#) for more information on the required database permissions for the MyID COM+ user.

See your Microsoft SQL Server documentation for further details.

4.6 Setting up server roles

4.6.1 Server roles for Windows Server 2012 R2

You must configure the server roles using Server Manager.

1. Set up the MyID application server using Server Manager.

Make sure the roles include the following:

- ♦ Application Server\ .NET Framework 4.5
You do not need the WCF Support option.
- ♦ Application Server\COM+ Network Access
- ♦ Application Server\Distributed Transactions
- ♦ File and Storage Services\Storage Services

Set up the following features:

- ♦ .NET Framework 4.5 Features\ .NET Framework 4.5
- ♦ .NET Framework 4.5 Features\WCF Services\TCP Port Sharing
- ♦ User Interfaces and Infrastructure\Graphical Management Tools and Infrastructure
- ♦ Windows PowerShell\Windows PowerShell 4.0
- ♦ WoW64 Support

2. Set up the MyID web server using Server Manager.

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 4.5
- ♦ Web Server (IIS)\Web Server\Application Development\ASP
- ♦ Web Server (IIS)\Web Server\Application Development\ASP.NET 4.5
- ♦ 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
- ♦ Web Server (IIS)\Management Tools\Management Service

Set up the following features:

- ♦ .NET Framework 4.5 Features\ .NET Framework 4.5

- ♦ .NET Framework 4.5 Features\ASP.NET 4.5
 - ♦ .NET Framework 4.5 Features\WCF Services\TCP Port Sharing
 - ♦ User Interfaces and Infrastructure\Graphical Management Tools and Infrastructure
 - ♦ Windows PowerShell\Windows PowerShell 4.0
 - ♦ Windows Process Activation Service\Process Model
 - ♦ Windows Process Activation Service\Configuration APIs
 - ♦ WoW64 Support
3. Set up the MyID database server using Server Manager.
- Make sure the roles include the following:
- ♦ File and Storage Services\Storage Services
- Set up the following features:
- ♦ .NET Framework 3.5 Features\ .NET Framework 3.5 (includes .NET 2.0 and 3.0)
 - ♦ .NET Framework 4.5 Features\ .NET Framework 4.5
 - ♦ .NET Framework 4.5 Features\WCF Services\TCP Port Sharing
 - ♦ User Interfaces and Infrastructure\Graphical Management Tools and Infrastructure
 - ♦ Windows PowerShell\Windows PowerShell 4.0
 - ♦ Windows PowerShell\Windows PowerShell 2.0 Engine

4.6.2 Server roles for Windows Server 2016

You must configure the server roles using Server Manager.

1. Set up the MyID application server using Server Manager.
- Make sure the roles include the following:
- ♦ File and Storage Services\Storage Services
- Set up the following features:
- ♦ .NET Framework 4.6 Features\ .NET Framework 4.6
 - ♦ .NET Framework 4.6 Features\WCF Services\TCP Port Sharing
 - ♦ Windows PowerShell\Windows PowerShell 5.1
 - ♦ WoW64 Support
2. Set up the MyID web server using Server Manager.
- 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 4.6
- ◆ Web Server (IIS)\Web Server\Application Development\ASP
- ◆ Web Server (IIS)\Web Server\Application Development\ASP.NET 4.6
- ◆ 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
- ◆ Web Server (IIS)\Management Tools\Management Service

Set up the following features:

- ◆ .NET Framework 4.6 Features\.NET Framework 4.6
 - ◆ .NET Framework 4.6 Features\ASP.NET 4.6
 - ◆ .NET Framework 4.6 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
3. Set up the MyID database server using Server Manager.
- Make sure the roles include the following:
- ◆ File and Storage Services\Storage Services
- Set up the following features:
- ◆ .NET Framework 3.5 Features\.NET Framework 3.5 (includes .NET 2.0 and 3.0)
 - ◆ .NET Framework 4.6 Features\.NET Framework 4.6
 - ◆ .NET Framework 4.6 Features\WCF Services\TCP Port Sharing
 - ◆ Windows PowerShell\Windows PowerShell 5.1
 - ◆ Windows PowerShell\Windows PowerShell 2.0 Engine

4.7 Client software

4.7.1 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.

4.7.2 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%**

4.8 Configuring Internet Explorer

4.8.1 Adding the MyID website to the Trusted sites or Local intranet group

To add the MyID website to the **Trusted sites** or **Local intranet** security group in Internet Explorer.

1. Open the **Internet Options** dialog:
 - ♦ Select **Internet Options** from the **Tools** menu in Internet Explorer, or:
 - ♦ 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 in Internet Explorer. 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.

4.8.2 Disabling the pop-up blocker

MyID requires the ability to display pop-up windows.

To disable the pop-up blocker for the MyID web site:

1. Open the **Internet Options** dialog:
 - ♦ Select **Internet Options** from the **Tools** menu in Internet Explorer, or:
 - ♦ 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**.

4.8.3 Exceptions

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.
- Automated Testing – requires the **Initialize and script ActiveX controls not marked as safe for scripting** option in Internet Options.
- Aware PreFace – the MyID website must be placed in the **Trusted sites** zone, and 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**.

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.

4.8.4 Performance improvements for client PCs without internet access

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. Disable the following option in Internet Explorer:

Internet Options > Advanced tab > Security section > Check for publisher's certificate revocation

Note: This setting affects the security of all .NET components on the client PC that are accessed by Internet Explorer. Do not set this option if your PC has internet access.

2. Restart Internet Explorer.

5 Installing MyID

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 CD, 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.

Note: This section contains instructions for installing MyID.

5.1 Overview

Important: If you already have MyID 10.8 or MyID 10.8 Update 1 installed, do not run the `setup.exe` program in the root of this release. Instead, follow the instructions in the `\Server Core Platform Updates\` folder to update your system to MyID 10.8 Update 2. See section [5.3.7, Installing the latest updates](#) for details.

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 from the CD.
 - ♦ Install and configure the MyID database.
 - ♦ Install MyID middleware components.
 - ♦ Install and configure the MyID web server.
 - ♦ Install exported COM+ Components on web server.
 - ♦ Install optional PKI and Authentication Service connectors.
3. 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.

4. Install MyID software updates.

Between major versions of MyID, Intercede also supplies customers with updates that provide improvements and new functionality; for example, MyID 10.8 Update 2. These updates are not provided as full installation programs for MyID, but as a series of smaller patches and updated modules which you must install on your system to ensure your installation is fully up to date.

See section [5.3.7, Installing the latest updates](#) for details.

5. 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.
6. Configure and test the Certificate Authority connection.
7. Configure any Authentication Server connections.
8. Define and test MyID Security Policies.
 - ♦ Define User Roles.
 - ♦ Define Certificate Policy filters.
 - ♦ Construct Credential Profiles.
 - ♦ Add a user and test card issuance.
9. Install and test a Client Machine.

5.2 Split deployment

To implement a split deployment, where the MyID application, web, and database tiers are installed on different physical machines, you must follow a strict implementation procedure. This ensures the various tiers 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 server tiers.

Note: Make sure you have DTC set up to allow the tiers to communicate with each other. See section [4.3, Timeouts, limits and other settings](#) for details.

1. Create the MyID database.
 - a) Run the MyID installer 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 tier and application tier at the same time.
 - b) Select the **Database Tier** option in the Select Tiers dialog.

Note: SQL Client Components must be installed on the MyID application server.

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 Installer on the MyID Server and check only the **Application Tier** option in the Select Tiers 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 tiers.

3. Run GenMaster to generate a master key for the database and a startup user.

This application runs automatically during the MyID server installation and is used to generate your Master Keys in the registry or in your HSM. See section [5.5.1, Using GenMaster](#) for details.

4. Create the web server.

Run the MyID installer on the web server and select the **Web User Interface Tier** in the Select Tiers dialog. (You do not need to select the **MyID Process Driver** **Web Service** tier – the web services are installed automatically with the web user interface tier.)

If you want to use the Lifecycle API, select the **Lifecycle API Web Services** option also.

5. Transfer COM proxies to allow communication between the web server and the application server.

The COM proxies also allow communication between the web services and the application server.

You must export the COM Proxies from the application server to the web server. To do this, you need the .msi files in the following folder on the application server:

`C:\Program Files (x86)\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 (x86)\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.

6. Open MyID Desktop.

7. Log on to MyID with the startup user.

5.3 Upgrading

Important: If you already have MyID 10.8 or MyID 10.8 Update 1 installed, do not run the setup.exe program in the root of this release. Instead, follow the instructions provided in the readme in the \Server Core Platform Updates\ folder to update your system to MyID 10.8 Update 2. See section [5.3.7, Installing the latest updates](#) for details.

5.3.1 Before you upgrade

Note: Before you upgrade your MyID system to the current version of MyID, contact Intercede customer support 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.

Before you upgrade to this version of MyID, check section [2, Hardware and Software Requirements](#) to make sure that your system supports the latest version of MyID.

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.

5.3.2 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) 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.

5.3.3 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.

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.

5.3.4 Upgrading from MyID 10.0 or earlier

Note: If you are upgrading from MyID 10.1 or later, you do not have to uninstall MyID before installing the new version. See section [5.3.5, Upgrading from MyID 10.1 – 10.6](#).

Note: If you have customized JavaScript hooks in your installation, you must contact customer support before you upgrade.

When you are upgrading an existing MyID installation to the current version, you must carry out the following procedure:

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.

On 32-bit servers, this is:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Intercede\
```

On 64-bit servers, this is:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Intercede\
```

4. Back up the MyID database and program folder.

5. Uninstall any MyID patches or modules.

You must uninstall the patches and modules in the reverse order in which they were applied. See the **Installation History** tab of the **System Status** report within MyID for a list of the updates that have been applied to your system.

If you are asked to reboot at any point, do so.

6. Uninstall MyID.

To uninstall MyID:

- a) In the Control Panel, uninstall the following items:

- MyID Client Components x86
- MyID Server

- b) Reboot your machine.

- c) If the MyID program folder still exists, make a backup, then remove it.

The easiest way to do this is to rename the folder.

Warning: Do not delete the Intercede values in the registry. If you do, the KeyServer cannot start after the upgrade. If this happens, you must reinstall MyID with a new database and restore it from the backup database.

7. On each client, uninstall the MyID Client Components or the previous version of the MyID Desktop software.

If the client has any supplemental installers (for example, the Cross Match components for MyID) you must uninstall these too.

8. 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.

9. Run the pre-install script that addresses issues with updating older databases to the current version of MyID.

Contact customer support quoting reference SUP-285 for details.

10. Install MyID.

Make sure you are installing to an empty folder.

11. If you experience any problems with MyID failing to start, check that the registry is still correct. If it does not match the backup you took before uninstalling, you must restore the registry from the backup.

12. Copy the contents of the backup `\Web\upimages\` folder to the `\Web\upimages\` folder of the new installation.

MyID now stores uploaded user images in the database. For details of migrating your images to the database, contact customer support, quoting reference SUP-153.

Note: Images uploaded from the **Card Layout Editor** continue to be stored in the `upimages` folder.

13. If you have any customized files, such as language dictionaries, custom JavaScript files, and so on, copy them from the backup folder into the corresponding location in the new installation.

Contact customer support if you want to discuss possible integration issues with customized files.

14. On a split deployment, uninstall the COM proxies and reinstall the new versions from the application server.

See section 5.2, *Split deployment* for details.

15. If you are using an nCipher HSM, on each MyID application server, rename the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\wow6432Node\Intercede\Edefice\MasterCard\nShield
```

to:

```
HKEY_LOCAL_MACHINE\SOFTWARE\wow6432Node\Intercede\Edefice\MasterCard\nCipher
```

16. For PIV systems, make sure you set up the server signing certificate registry entries again.

See the *Configure server signing certificates* section in the *PIV Integration Guide*.

17. On each client:

- a) Install the MyID Desktop application.
- b) Clear the Internet Explorer cache. Make sure you deselect the **Preserve favorites website data** option, if it is available.

18. 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.

19. Install the latest updates for your system.

See section 5.3.7, *Installing the latest updates* for details.

5.3.5 Upgrading from MyID 10.1 – 10.6

Note: If you have customized JavaScript hooks in your installation, you must contact customer support before you upgrade.

When you are upgrading an existing MyID installation to the current version, you must carry out the following procedure:

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.
5. Uninstall any MyID patches.

You must uninstall the patches (VTEN-10.x.xxxx.x) in the reverse order in which they were applied. See the **Installation History** tab of the **System Status** report within MyID for a list of the updates that have been applied to your system.

If you are asked to reboot at any point, do so.

6. Uninstall any MyID modules, as required.

Follow the instructions in the module readme or installation guide, which will advise whether you must remove the module before installing the new version. For example, you must uninstall MyID Web Service Architecture (MWS) modules, but you can install a new version of the Credential Web Service (CWS) on top of an existing version, as long as the new version has a later version number.

7. On each client, uninstall the previous version of the MyID Desktop software.
If the client has any supplemental installers (for example, the Cross Match components for MyID) you must uninstall these too.
8. 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.
9. Run the pre-install script that addresses issues with updating older databases to the current version of MyID.
Contact customer support quoting reference SUP-285 for details.
10. Install MyID.
11. If you experience any problems with MyID failing to start, check that the registry is still correct. If it does not match the backup you took before uninstalling, you must restore the registry from the backup.
12. On a split deployment, uninstall the COM proxies and reinstall the new versions from the application server.
See section [5.2, Split deployment](#) for details.
13. If you are using an nCipher HSM, on each MyID application server, rename the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\wow6432Node\Intercede\Edefice\MasterCard\nShield
```


to:

```
HKEY_LOCAL_MACHINE\SOFTWARE\wow6432Node\Intercede\Edefice\MasterCard\nCipher
```
14. For PIV or CIV systems, make sure you set up the server signing certificate registry entries again.
See the *Configure server signing certificates* section in the [PIV Integration Guide](#) or [CIV Integration Guide](#).
15. On each client:
 - a) Install the MyID Desktop application.
 - b) Clear the Internet Explorer cache. Make sure you deselect the **Preserve favorites website data** option, if it is available.
16. 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.
17. Install the latest updates for your system.
See section [5.3.7, Installing the latest updates](#) for details.

5.3.6 Upgrading from MyID 10.7

Important: Due to an issue in the upgrade process from MyID 10.7 or MyID 10.8, you must carry out an additional step between installing the new version of MyID and continuing with the GenMaster process.

Note: If you have customized JavaScript hooks in your installation, you must contact customer support before you upgrade.

When you are upgrading an existing MyID installation to the current version, you must carry out the following procedure:

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.
5. Uninstall any MyID patches.

You must uninstall the patches (VTEN-10.x.xxxx.x) in the reverse order in which they were applied. See the **Installation History** tab of the **System Status** report within MyID for a list of the updates that have been applied to your system.

If you are asked to reboot at any point, do so.

6. Uninstall any MyID modules, as required.

Follow the instructions in the module readme or installation guide, which will advise whether you must remove the module before installing the new version. For example, you must uninstall MyID Web Service Architecture (MWS) modules, but you can install a new version of the Credential Web Service (CWS) on top of an existing version, as long as the new version has a later version number.

7. On each client, uninstall the previous version of the MyID Desktop software.

If the client has any supplemental installers (for example, the Cross Match components for MyID) you must uninstall these too.

8. 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.

9. Install MyID.

Important: After the installer has completed, it starts the GenMaster utility. *Before* you proceed with the GenMaster process, you *must*:

- a) Right-click the KeyServer icon in the Windows task bar.

Ignore any errors that appear on the Card Manager Startup screen. Cancel the message.

- b) From the KeyServer pop-up menu, select **Stop**.

- c) Restore your registry from the backup you took before starting the upgrade process.

- d) Right-click the KeyServer icon in the Windows task bar and select **Start**.

- e) Continue with the GenMaster configuration.

If you do not do this, GenMaster will display an error similar to the following:

```
Error in eKeySrvEncrypt
```

10. On a split deployment, uninstall the COM proxies and reinstall the new versions from the application server.
See section 5.2, *Split deployment* for details.
11. For PIV or CIV systems, make sure you set up the server signing certificate registry entries again.
See the *Configure server signing certificates* section in the *PIV Integration Guide* or *CIV Integration Guide*.
12. On each client:
 - a) Install the latest version of the MyID Desktop application.
 - b) Clear the Internet Explorer cache. Make sure you deselect the **Preserve favorites website data** option, if it is available.
13. 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.
14. Install the latest updates for your system.
See section 5.3.7, *Installing the latest updates* for details.

5.3.7 Installing the latest updates

Between major versions of MyID, Intercede supplies customers with updates that provide improvements and new functionality; for example, MyID 10.8 Update 2. These updates are not provided as full installation programs for MyID, but as a series of smaller patches and updated modules.

See the instructions provided with these patches and modules for details of how to install your update. In particular, check the `\Server Core Platform Updates\` folder in the release for essential software updates – you must install these on your system to ensure your installation is fully up to date.

5.3.8 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 sections 5.3.19, *Upgrading systems with older data models* and 5.3.20, *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.

5.3.9 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.

5.3.10 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.

5.3.11 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 to MyID 10.6 or later, 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 section [9, Setting Up Email](#) for details.

5.3.12 Upgrading the storage of PINs for HSMs

From version 10.7, MyID stores the PINs for SafeNet HSMs encrypted in the registry for the MyID COM+ user. If you are upgrading an existing SafeNet HSM system and want to migrate the PIN, or if you are using a Thales nShield HSM and want to store the PIN, you can use the SetHSMPIN utility to do this.

See section [5.6, Setting the HSM PIN](#) for details.

5.3.13 Modifying an existing installation

If you want to use the installation program to modify your installation of MyID after the original installation is completed, contact customer support for advice.

5.3.14 Upgrading systems with Virtual Smart Cards

If your system is using server-generated Virtual Smart Cards, note that the server-generated VSC feature is no longer available on new installations of MyID. 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. You can continue to issue new server-generated VSCs; however, note that some additional software and configuration is required. See the [Server-Generated Virtual Smart Card Integration Guide](#) that was provided with your previous release.

If your system is using locally-generated Virtual Smart Cards, you can still carry on using the previously installed MyID Windows Integration Service. However, if you want ensure the latest functionality is included in the MyID Windows Integration Service, make sure you are using the latest version of the MyID Windows Integration Service software. See the [Microsoft Virtual Smart Card Integration Guide](#).

5.3.15 Upgrading SQL Server configuration

From MyID 10.7, you must install the SQL Server Full Text Search option on your database server.

5.3.16 Upgrading the web service user account

MyID 10.7 introduces the web service user account. If you are upgrading an existing system, you must create this user before you run the installation program.

See section [4.2.3, User accounts](#) for details.

5.3.17 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 [5.5, Running 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.

5.3.18 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.

5.3.19 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.

5.3.20 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.

5.3.21 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.

5.3.22 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 on the MyID CD in the `Support Tools\Upgrade\` folder.

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_RegenerateCertRenewalJobs.sql
```

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

5.3.23 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 on the MyID CD in the `Support Tools\Upgrade\` folder.

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.

5.3.24 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.

- **IKB-220 – Errors during upgrade when the SCEP module has previously been installed**

When upgrading MyID, you may see the following error when previous MyID patches have provided the component `XMLeXchange.dll` – in most cases this is when the SCEP module for MyID has been installed:

```
Error 1905. Module C:\Program Files
(x86) Intercede\MyID\Components\Core\XMLeXchange.dll failed to
unregister. HRESULT -2147220472. Contact your support personnel.
```

You can close the error message and the installation will continue successfully.

5.4 Running the installation program

Note: If you experience problems with the installer, customer support may ask you to run the installation program with options to create a full log. For more information, contact customer support, quoting reference SUP-137.

To install MyID:

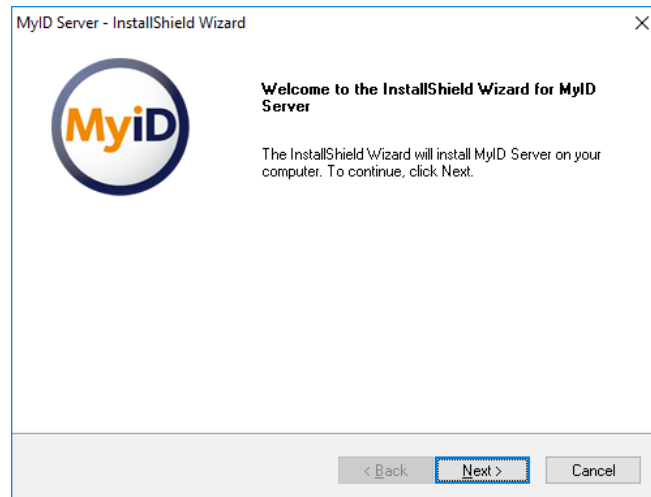
1. Log on to the MyID server.

You must have the correct privileges to install the software. Log on to the server as a user with local administrative privileges who can run the installation program for the MyID installation using **Run as administrator**.

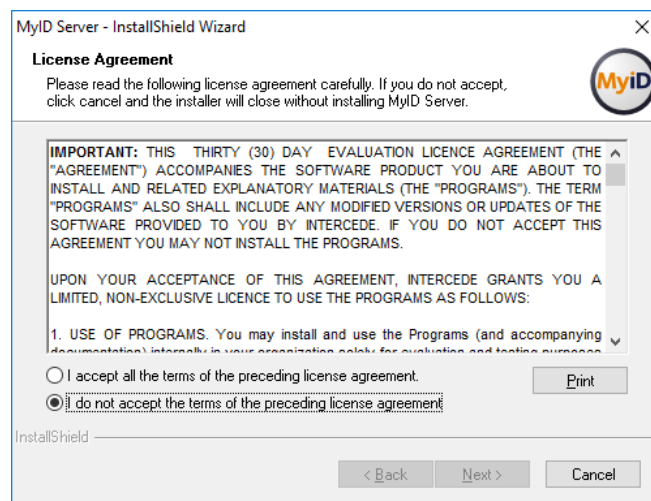
2. Close all application windows.

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.

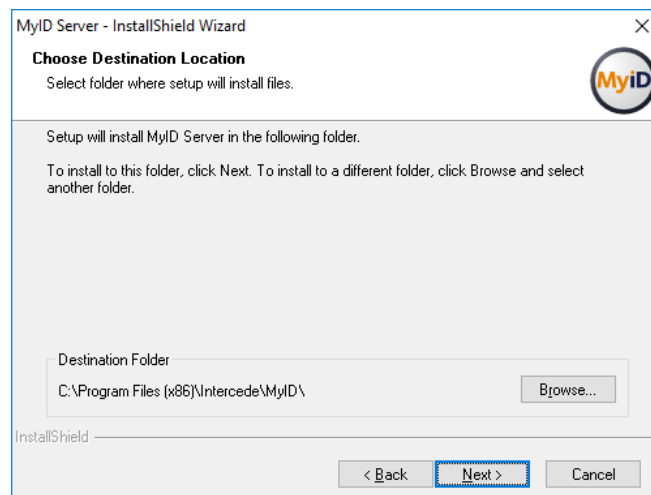
3. Insert the MyID product CD, right-click the installer program and select **Run as administrator**.



4. Click **Next**.

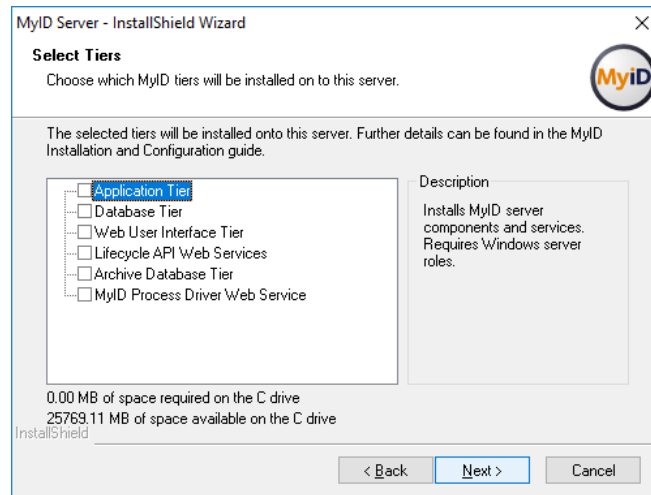


5. Read the license agreement, accept the terms, then click **Next**.
6. Select the destination folder.



By default, MyID installs to C:\Program Files (x86)\Intercede\MyID.

7. Select the tiers you want to install.



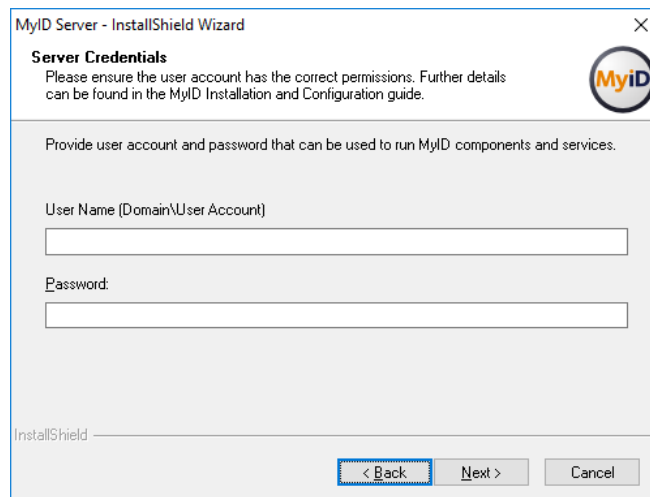
Choose from the following:

- ♦ **Application Tier** – this tier contains the MyID application components.
 - ♦ **Database Tier** – this tier contains the MyID database.
 - ♦ **Web User Interface Tier** – this tier contains the MyID web server, including the web services that are used to communicate with the self-service apps and the Desktop client.
 - ♦ **Lifecycle API Web Services** – this tier contains the MyID web services to support the lifecycle API. See the [Lifecycle API](#) document for details.
 - ♦ **Archive Database Tier** – this tier contains a database that can contain an archive of some parts of the MyID database. See sections [8.4, Using a separate audit database](#) and [8.5, Archiving the audit trail](#) for details.
- Note:** You are recommended to create the archive database *after* running the main installation, rather than at the same time.
- ♦ **MyID Process Driver Web Service** – this tier contains the web services that are used to communicate with the self-service apps and the Desktop client. These services are automatically installed when you select the **Web User Interface Tier** – you need select this option only if you are installing the web services on a different server to the MyID web site.

For information on configuring the web services, see the [Web Service Architecture Installation and Configuration](#) document.

You can install multiple tiers on the same machine, or on different physical machines. See section [5.2, Split deployment](#) for details.

8. Type the **User Name** and **Password** for the MyID COM+ user.



MyID Server - InstallShield Wizard

Server Credentials
Please ensure the user account has the correct permissions. Further details can be found in the MyID Installation and Configuration guide.

Provide user account and password that can be used to run MyID components and services.

User Name (Domain\User Account)

Password:

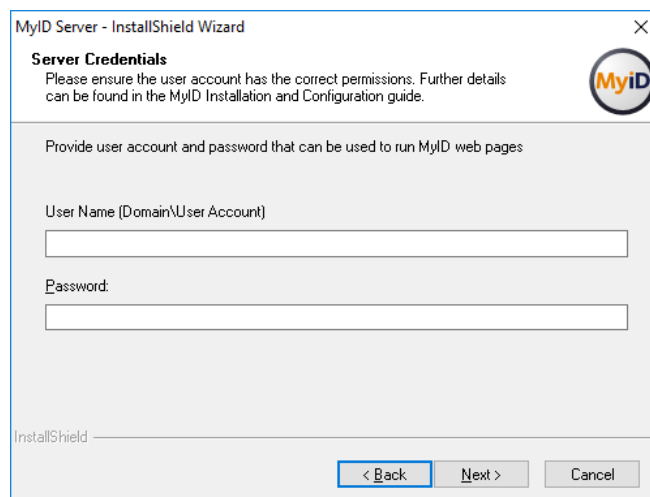
InstallShield

< Back Next > Cancel

This account is used to run the MyID components and Windows services.

See section [4.2.3, User accounts](#) for details.

9. Type the **User Name** and **Password** for the MyID IIS user.



MyID Server - InstallShield Wizard

Server Credentials
Please ensure the user account has the correct permissions. Further details can be found in the MyID Installation and Configuration guide.

Provide user account and password that can be used to run MyID web pages

User Name (Domain\User Account)

Password:

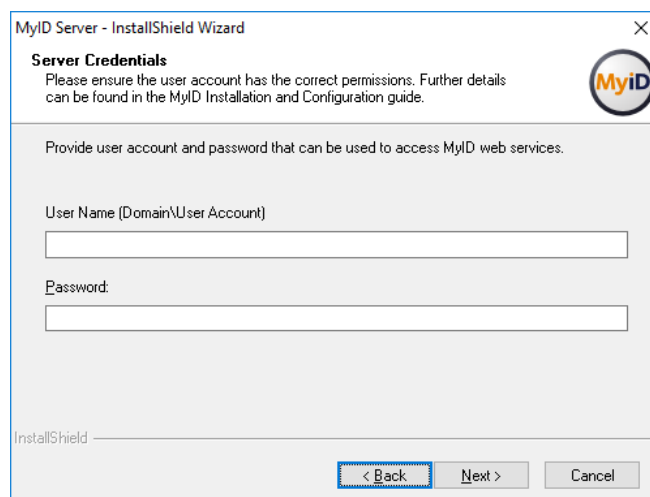
InstallShield

< Back Next > Cancel

This account is used to run the MyID website.

See section [4.2.3, User accounts](#) for details.

10. Type the User Name and Password for the MyID web services user.



MyID Server - InstallShield Wizard

Server Credentials
Please ensure the user account has the correct permissions. Further details can be found in the MyID Installation and Configuration guide.

Provide user account and password that can be used to access MyID web services.

User Name (Domain\User Account)

Password:

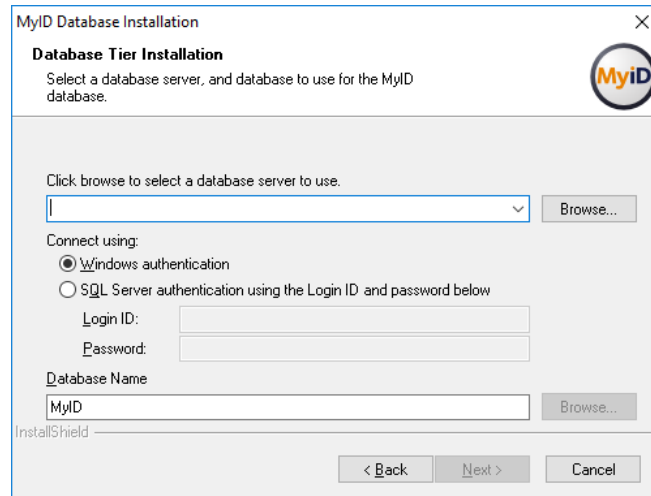
InstallShield

< Back Next > Cancel

This account is used to run the MyID web services.

See section 4.2.3, [User accounts](#) for details.

11. Select the database server.



The screenshot shows the 'MyID Database Installation' window, specifically the 'Database Tier Installation' tab. It prompts the user to 'Select a database server, and database to use for the MyID database.' There is a dropdown menu for selecting a database server, with a 'Browse...' button next to it. Below this, there are two radio buttons for 'Connect using:'. The first is 'Windows authentication', which is selected. The second is 'SQL Server authentication using the Login ID and password below', which has fields for 'Login ID:' and 'Password:'. There is also a 'Database Name' field with 'MyID' entered and a 'Browse...' button. At the bottom, there are '< Back', 'Next >', and 'Cancel' buttons.

12. 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 Server authentication** – you must specify the **Login ID** and **Password** for the user you want to use to authenticate to the SQL Server database.

Note: SQL Server authentication is available only for Microsoft Azure databases. See the [Microsoft Azure Integration Guide](#) for details.

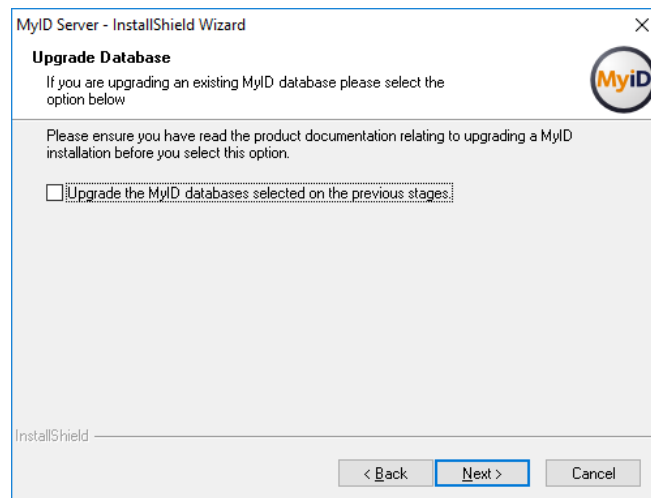
13. Type the name for the MyID database you want to create on the database server.

The default is `MyID`.

Alternatively, you can click **Browse** to select an existing database.

Click **Next**.

14. Specify whether you need to upgrade the database.

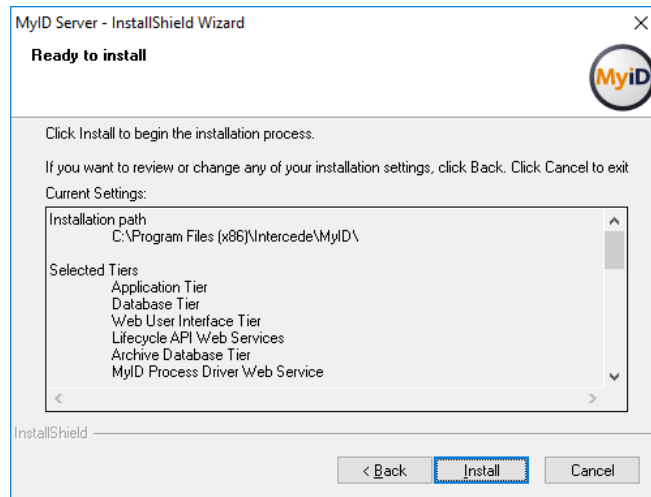


The screenshot shows the 'MyID Server - InstallShield Wizard' window, specifically the 'Upgrade Database' tab. It prompts the user to 'If you are upgrading an existing MyID database please select the option below'. There is a checkbox labeled 'Upgrade the MyID databases selected on the previous stages'. Below this, there is a note: 'Please ensure you have read the product documentation relating to upgrading a MyID installation before you select this option.' At the bottom, there are '< Back', 'Next >', and 'Cancel' buttons.

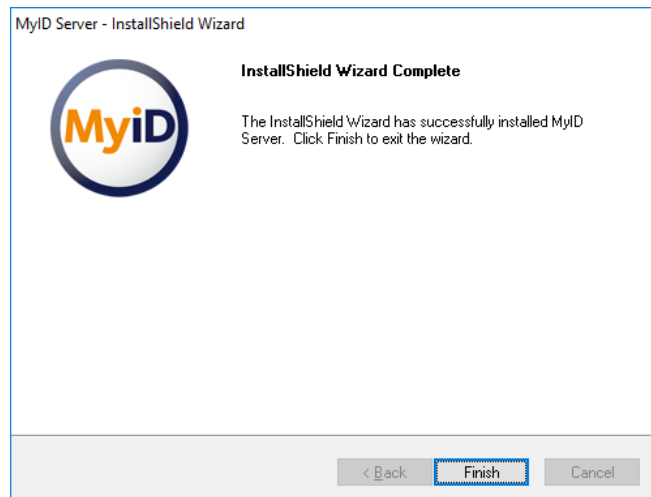
If you are upgrading an existing installation from before version 10.0, select the **Upgrade the MyID databases selected on the previous stages** option.

Click **Next**.

15. Click **Install** to start the installation process.



A series of progress messages will be displayed as the files are copied and the application is installed.



The **GenMaster Welcome** dialog (see section [5.5, Running GenMaster](#)) is displayed automatically. GenMaster allows you to secure your MyID installation with a Master key, and set up a startup user that you can use to access the system for the first time.

16. Install the latest updates for your system.

See section [5.3.7, Installing the latest updates](#) for details.

5.4.1 NT Event Log 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`. These messages are normal and expected.

5.5 Running GenMaster

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.

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.

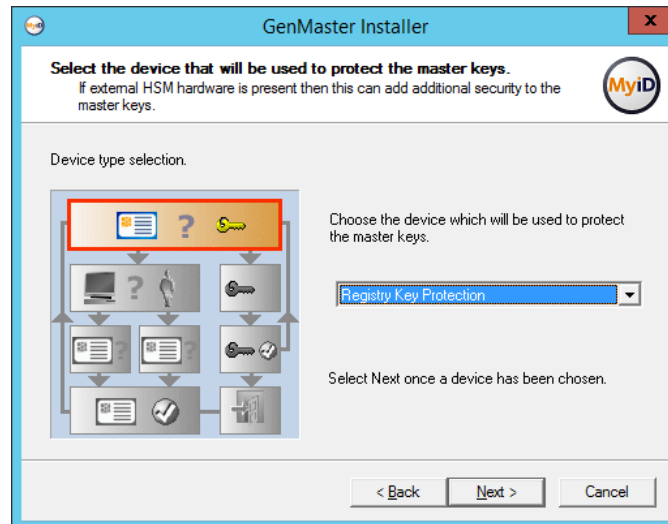
5.5.1 Using GenMaster

The GenMaster program is started automatically by the installation process. You can also start the program from the **Start** menu; use the **Run as administrator** option.

1. Run GenMaster.



2. Click **Next**.
3. 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 Thales nShield HSM.
- ♦ **LUNA SA HSM key protection** – the key is generated and stored in the SafeNet Network HSM.

Note: Thales nShield (nCipher) 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.

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\SYSTEM64` directory.

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

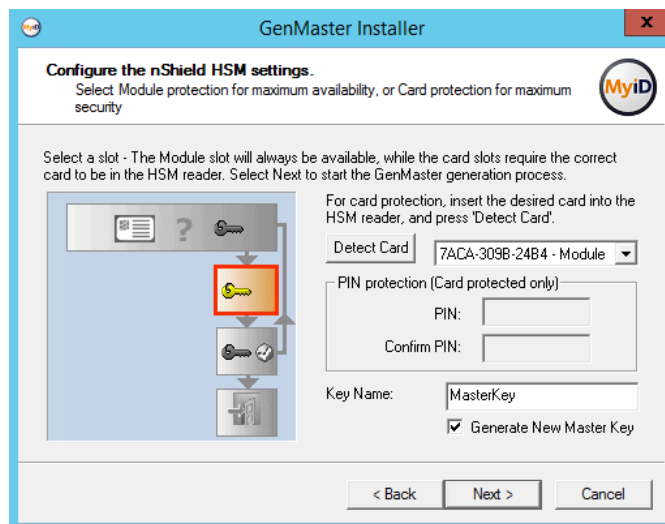
- a) Select **Registry Key Protection** from the drop-down list.
- b) Click **Next**.
- c) Create a backup of the registry key, or skip the backup step.



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.

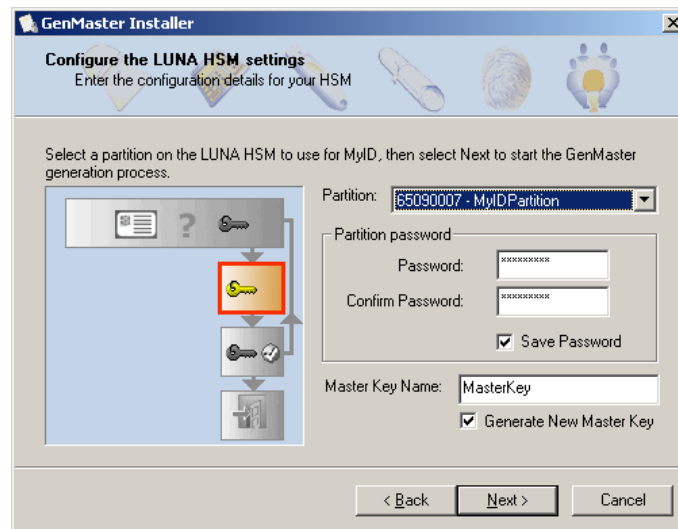
Note: There must not already be a key of this name installed on the HSM.

- e) Click **Next** to generate the keys – this may take a few seconds.

For more information, see the [Thales 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 **Masterkey 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\wow6432Node\Intercede\Edefice\
MasterCard
```

The password is saved encrypted to the registry; see section 5.6, [Setting the HSM PIN](#).

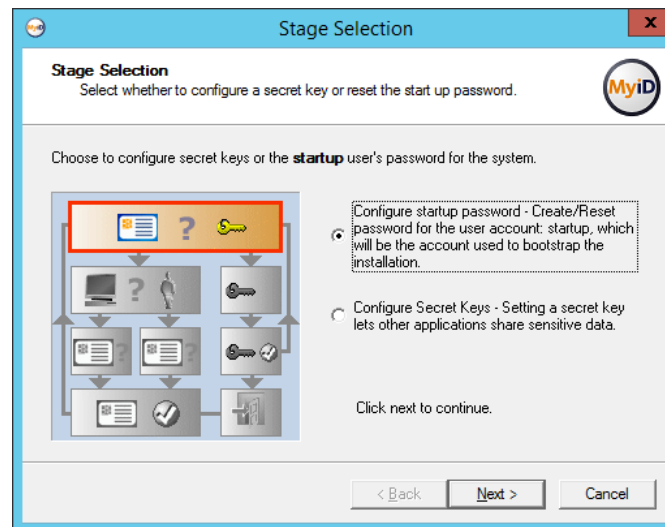
- g) Click **Next** to generate the keys – this may take a few seconds.

For more information, see the [SafeNet Network HSM Integration Guide](#).

4. You can now select one of the following options:

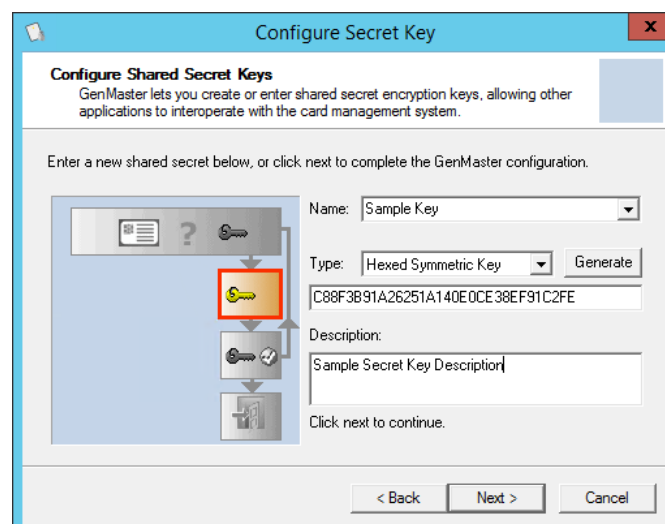
- ♦ **Configure Secret Keys** – this option allows you to set up secret keys that allow other applications to share sensitive data.
- ♦ **Configure startup password** – this option allows you to set the password for the startup user account.

Note: You *must* set up a password for this account when you first install MyID or you will be unable to access the system.

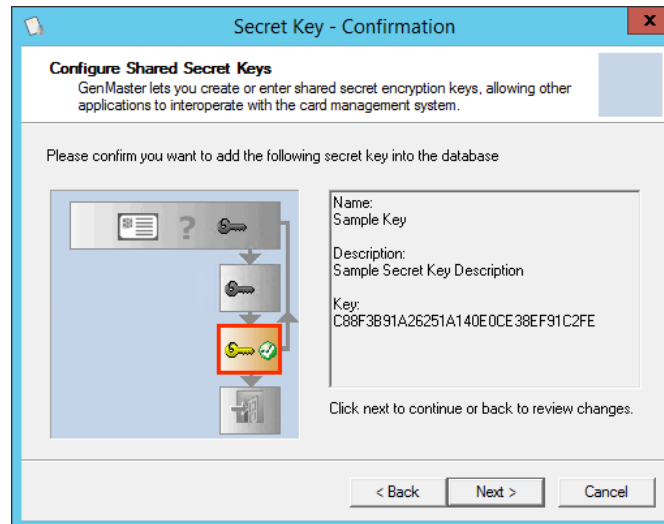


To configure secret keys:

- 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.

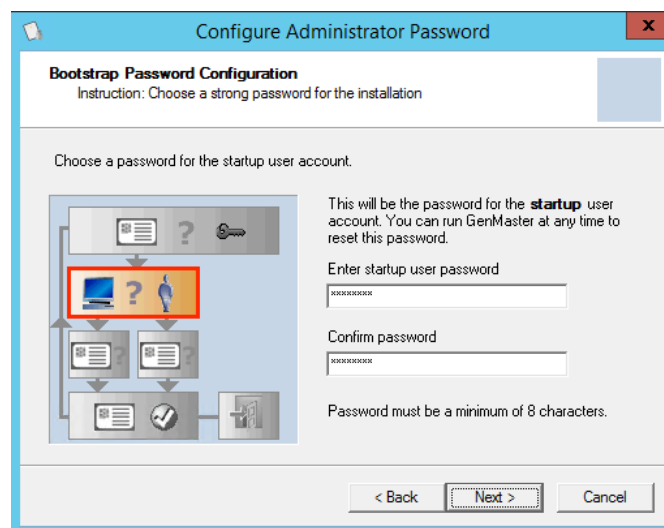


f) Click **Next** to confirm the details of the shared secret key.

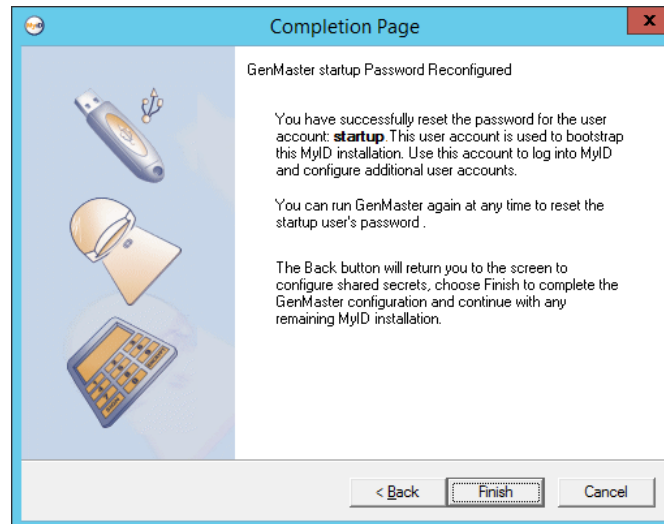
To set the startup user password:

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, contact Intercede customer support, quoting reference SUP-132.

- 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.

5. Click **Finish**.

GenMaster returns control to the main MyID installation program, which completes its setup.

5.6 Setting the HSM PIN

When you save the PIN for a SafeNet 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 Thales HSMs are *not* stored in the registry by GenMaster.

In previous versions of MyID, the PIN for SafeNet 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 a Thales HSM.
- Move and encrypt the PIN for an upgraded system.

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 (x86)\Intercede\MyID\Utilities\
```

3. 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
```

5.7 Required updates

When you are provided with the installation media for MyID, your Intercede representative may provide you with a set of updates that provide additional security and functionality to MyID to provide you with the best possible up-to-date user experience.

Make sure that you install all of the updates provided, in the order specified, before you use MyID for operational purposes.

6 Securing the MyID Application

Important: For your production environment, you *must* ensure that your MyID system is secure. The latest [System Security Checklist](#) document provided with MyID provides important information about risks and recommendations for a wide variety of security considerations, and you are strongly advised to complete the checklist for your system.

The following sections include additional information about securing your system – whether you choose to implement them depends on the security requirements of your organization. Note, however, that by default MyID requires some security options that you must explicitly disable if you do not want to use them; see section [6.1, Device security settings](#) for more information.

Note: You should carry out the additional lockdown procedures after you have installed MyID. You may experience problems if you attempt to install MyID on a system that has already been locked down.

6.1 Device security settings

When you install MyID, the settings on the **Device Security** page of the **Security Settings** workflow are configured to require you to use customer GlobalPlatform keys and random Security Officer PINs (SOPINs). The system is also configured to display warnings if your system is not securely configured; for example:

MyID is not configured to issue this card.

See the [Administration Guide](#) for details of these settings.

6.2 Access to the MyID web application

The installation program sets up the MyID website to use anonymous authentication using the IIS user you specified when installing MyID. You can configure IIS to provide further security if required.

6.3 Secure access to diagnostic files

There are various diagnostic files that exist within MyID to help Intercede determine where issues might lie in the system. These files may sometimes return information that is considered private.

These files are located in the `diagnostics` subfolder within each language folder on the MyID web server. This subfolder is not accessible anonymously.

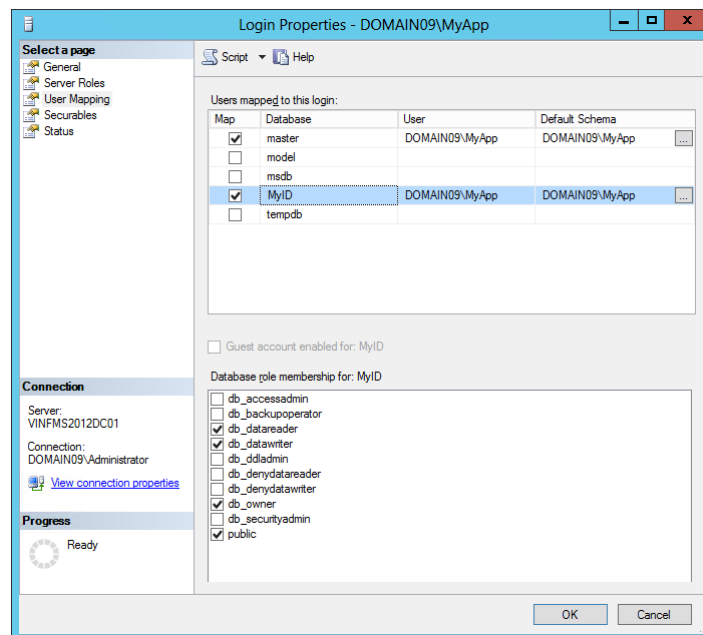
By default, this subfolder is locked to prevent *any* access. If you need to access the diagnostic features, including Automated Testing, contact customer support, quoting reference SUP-101.

6.4 MyID and SQL Server permissions

Warning: If running MyID with a named user, make sure the MyID COM+ account is added with 'English' as the default language, or date formats will cause failures.

The account used for database access (the MyID COM+ account) is assigned the permissions needed to create and use the MyID databases when MyID is installed. If you want to reduce the level of these permissions following installation, you must ensure that the account being used keeps the following levels of access as a minimum.

- The account *must* have the following roles on the MyID databases:
 - ♦ public
 - ♦ db_datareader
 - ♦ db_datawriter



Set these permissions in SQL Server Manager. Under the database instance, select **Security > Logins**, then right-click the MyID COM user.

- Ensure that the **Default Schema** is set to `dbo` or another appropriate setting; a default schema of `sys` will cause connection problems.
- The stored procedures executed by the system also need to allow execute permission to the MyID COM user. This includes all 'User' type stored procedures in the MyID database. You can assign permissions to stored procedures individually, or grant `db_owner` access to the MyID COM user in **Security > Logins**.
- Authentication

You specify whether to use SQL Server authentication or Windows authentication when installing MyID. See [5.4, Running the installation program](#) for details.

- ♦ For Windows Authentication to operate, the MyID application server must belong either to the same domain as the database server or to a trusted domain.

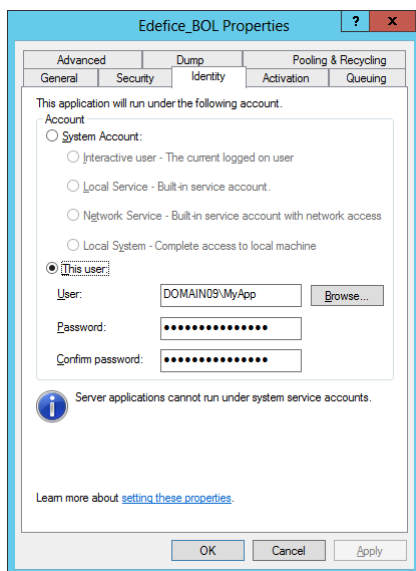
6.5 MyID and COM+ permissions

These permissions are set automatically during the installation process.

If you want to review or change these permission settings, they can be found in the **Properties** of the specified COM+ DLL. In **Component Services > My Computer > COM+ Applications**, right click the component then select **Properties**.

MyID installs some or all of the following COM objects, depending on the options you selected during installation:

| | |
|-----------------|---------------------|
| APDUCardServer | EAudit |
| eCS | Edefice_BOL |
| Edefice_CS | Edefice_DAL |
| eEventLog | eExternalDataSource |
| Entrust_Admin | ePKIConfig |
| ImportProcessor | |



6.6 MyID startup

If you are using an HSM that requires password entry, you can use the Card Manager Startup utility on the application server to enter your HSM credentials and control the operation of the MyID eKeyServer service that secures the MyID application.

Note: You must set the Startup utility to run when the MyID application server starts up.

6.6.1 Using the Startup utility

To start the utility:

1. Open the Windows Start menu.
2. In the MyID group, select **Startup**.
3. Locate the **Startup** icon in the Windows **Start** menu, right-click and select **Run as Administrator**.

The Startup utility now starts. The logged-on user must have permission to access the MyID database and stop or start the eKeyServer service.

You can also set the Startup utility to run as administrator when the system starts up. See your Windows documentation for details. For example, in Windows 2016, create a shortcut to the utility in:

`C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp`

Right-click the shortcut, select **Properties**, then on the **Compatibility** tab select **Run this program as an administrator**.

6.6.2 Using Startup with an HSM-based master key

When you log on to Windows on the server, the MyID **Startup** utility should run automatically. If it does not, select **Startup** from the **MyID** folder of the **Start** menu.

1. The **Startup** box is displayed.



If the eKeyServer service is already running, a warning message is displayed and only the **Cancel** button is active.

2. Depending on the type of user created on the HSM, you must do one of the following:
 - If the user was created with **No Authentication**, type the username.
 - If the user was created with **PIN Authentication**, type the username, then a space, then the PIN.
 - If the user was created with **Smartcard Authentication**:
 - i Type the username.
 - ii Insert the smartcard into the HSM card reader.
 - iii Enter the PIN on the PIN-Pad on the HSM card reader when the green light flashes.

Note: You cannot use the Cache keys option for an HSM-based master key. If you want to set up unattended startup, you must configure this when you first run GenMaster, if your HSM supports it.

3. The Startup utility then starts the eKeyServer service, which takes a few seconds. The message “Key Server is now active” is displayed when the service has successfully started.
4. Click **Close**.
5. The system tray shows the status of the eKeyServer service. A grey icon indicates that the service is not running. Right-click the icon to display the pop-up menu:
 - ♦ **Start** to start the eKeyServer service.
 - ♦ **Stop** to stop the eKeyServer service.
 - ♦ **Restart** to stop the eKeyServer service and then restart.
 - ♦ **Exit** to exit the Startup application, leaving the eKeyServer service running.

6.6.3 Startup utility procedure

The Card Manager Startup utility requires the appropriate permissions to carry out its processes. The utility carries out the following steps – you must make sure that your users are configured with the correct permissions for each step.

1. The utility reads the registry.
For the `Mastercard` key in the registry, and any subkey beneath it:
 - ♦ The MyID COM+ user needs read access.
 - ♦ Any user that logs onto the application server to use the utility needs read access.
 - ♦ In the rare occasions where the `Mastercard` part of the registry needs to be changed by MyID, full control to the `Mastercard` key and its subkeys is required for the MyID COM+ user account, and the logged on user. Situations that require this part of the registry to be updated include:
 - Running GenMaster for the first time.
 - Using the cache keys feature where master cards have previously been used.

The `Mastercard` is located in the following part of the registry on the application server:

```
HKEY_LOCAL_MACHINE\SOFTWARE\wow6432Node\Intercede\Edefice\MasterCard
```

2. Launches the Edefice_DAL component and pull back configuration information from the database.

This is launched by the utility using the logged-on user account's permissions.

3. Attempts to start the eKeyServer service.
Again, this uses the permissions of the logged-on user account.

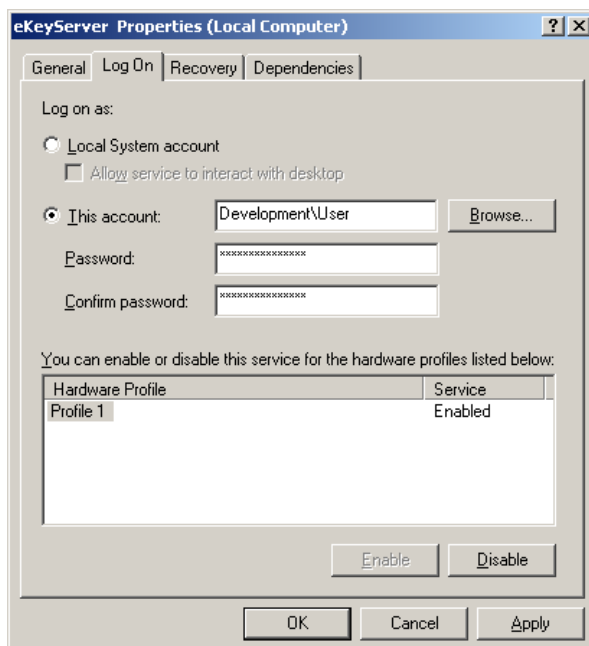
6.7 eKeyServer Service

The eKeyServer service is automatically configured to run using the MyID COM+ account, specified during the installation of MyID server.

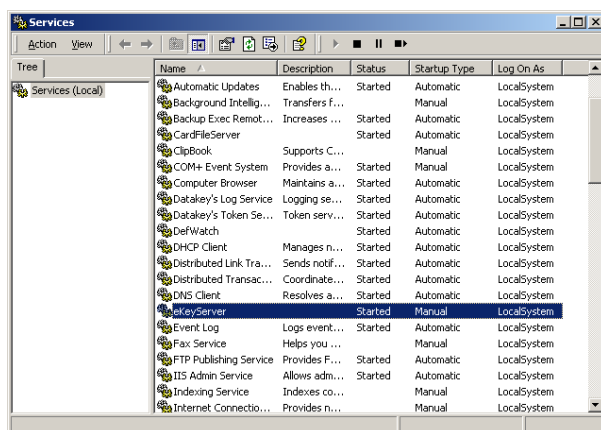
If you need to change this account for any reason, you must ensure that the new account has `Read` rights to the `.udl` files in the `SYSWOW64` folder that are used to access the database server. No additional permissions need to be assigned to this account.

The format of the user name must be `DOMAIN\UserName` rather than the form returned by the **Browse** feature on the property page (`UserName@DOMAIN`).

If the account selected does not already have **Log On As A Service** rights on the MyID server, the Service Control Manager MMC snap-in automatically assigns those rights and displays a confirmation message.



To verify the status of the eKeyServer service, open the **Service Control Manager**, (by selecting **Administrative Tools** then **Services**) from the control panel.



6.8 Protecting the registry

Warning: If eKeyServer is running in 'cached key' mode, the entries in the registry *must* be protected.

You can protect the registry using `regedt32.exe` to set permissions on the `HKEY_LOCAL_MACHINE\SOFTWARE\wow6432Node\Intercede\Edefice\MasterCard` branch of the registry on the application server. Read permission is needed for normal use, write permission is required when creating master keys that stored in the registry.

Make sure the following users have read access to this branch of the registry:

- The MyID COM user.
- Any user who logs on to the application server to use the Startup utility.

Make sure the following users have full control over this branch of the registry and its subkeys when running GenMaster for the first time:

- The MyID COM user.
- The logged-on user.

7 Testing the Installation

7.1 Configure and test the directory connection

- 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 [Administration Guide](#) for full details.

7.2 Configure and test the Certificate Authority connection

This varies between different PKI vendors. See the corresponding integration guide provided with MyID for details.

7.3 Configuring client PCs

The MyID Desktop application uses Internet Explorer to display workflows within the application. See section 4.8, [Configuring Internet Explorer](#) for information about configuring Internet Explorer on your client PCs.

7.4 Installing MyID Desktop

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 on the MyID CD in the `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: You must have .NET Framework 4.6 installed on each client PC on which you want to install MyID Desktop. MyID is developed and tested using .NET framework 4.6; 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**.
4. Select the desired shortcuts to be installed.
By default, a desktop shortcut is created.
5. Click **Next**.
6. In the **Server** 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 sections [7.5.3, One-way SSL/TLS](#) and [7.5.4, 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** 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 [7.6.1, Launching MyID Desktop with a specific server](#) 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.

7.5 Configuring MyID Desktop

7.5.1 Communication between MyID Desktop and the MyID server

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.

7.5.2 Server location

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 [7.6.1, 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. See sections [7.5.3, One-way SSL/TLS](#) and [7.5.4, Two-way SSL/TLS](#) for details.

- Server address – the address of the server. For example:

```
myserver.example.com
```


For example:

`https://myserver.example.com`

7.5.3 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.

7.5.4 Two-way SSL/TLS

MyID Desktop supports two-way SSL/TLS.

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 web site 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 (x86)\Intercede\MyID`
- `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 web sites and web services:

- MyIDDataSource
- MyIDProcessDriver
- MyID
- MyIDEnroll
- MyIDWebService
- upimages
- CertificateCheck

The script will also turn off SSL for the `images` folder in `MyIDDDataSource`, and `GetImage.aspx` and `WindowsAuth.aspx` in `MyIDProcessDriver`.

When disabled, the script turns off SSL/TLS for the MyID web sites and web services.

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 Internet Explorer. If you select the wrong certificate, you must restart MyID Desktop and try again.

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\SendTrustedIssuerList
```

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=f27cc86a95570505dd5cfffcbd670e65091f14620
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.

7.5.5 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.

Contact customer support quoting reference SUP-236.

7.5.6 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.

7.6 Launching MyID Desktop

7.6.1 Launching MyID Desktop with a specific server

When you install MyID, you can specify multiple servers in the list of allowed server addresses; see sections [7.4, Installing MyID Desktop](#) and [7.5.2, Server location](#). This 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
```

7.6.2 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 [14, Workflow IDs](#) for a list of workflow IDs.

Note: The user must have access to the specified workflow.

7.6.3 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"
```

7.6.4 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"
```

7.6.5 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.

For example:

```
MyIDDesktop.exe /opid:216 /lc
```

7.6.6 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.

For example:

```
MyIDDesktop.exe /lw /opid:216
```

See the [Administration Guide](#) for details of setting up your system to allow Integrated Windows Logon.

7.6.7 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 [14, 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.

7.7 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.

8 After Installing MyID

8.1 Integrating with other products

Check the integration guides for any products you are using with MyID and carry out any configuration that is required after MyID has been installed.

8.2 Internationalization and localization

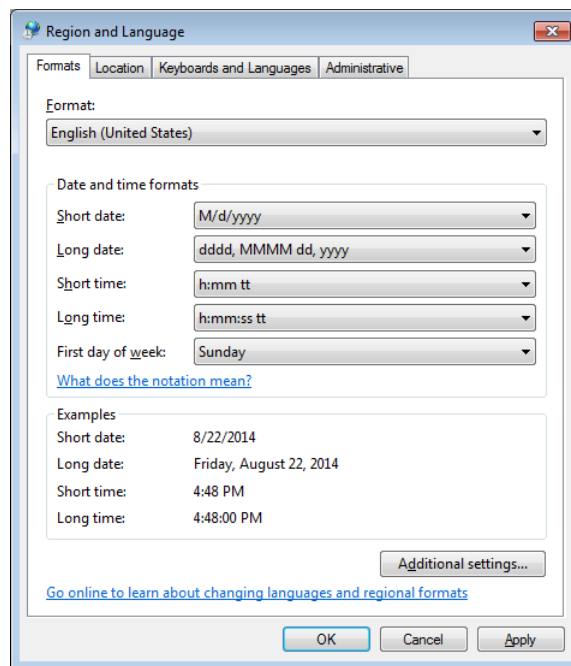
MyID can operate in multiple languages from the same installation, and can be translated into new languages. For more information on translating MyID, contact customer support, quoting reference SUP-138.

8.2.1 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, select **Region and Language**, 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 Internet Explorer – 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.

8.3 Email notification

MyID has a series of standard email templates that are used to notify individuals who are approaching a specified renewal point for their cards, certificates or other distributed component.

These users can automatically be notified of an impending deadline and be given instructions to carry out some action within a specified time frame. Further messages can be generated if the action is not completed in the time specified.

The installation of MyID automatically sets up processes to:

- Schedule the execution of these notification tasks to operate on a daily basis
- Cause emails to be sent immediately to selected users, selecting the message content based on the specified countdown method.

See section [9, Setting Up Email](#) for details of setting up email messages.

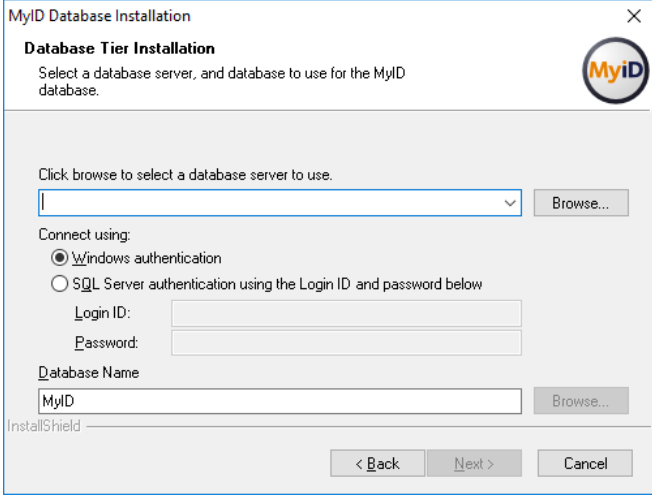
See the [Administration Guide](#) for details of configuring email notifications within MyID.

8.4 Using a separate audit database

If you want to store the audit information in a separate database from the main MyID database, you can set up MyID to use a dedicated audit database.

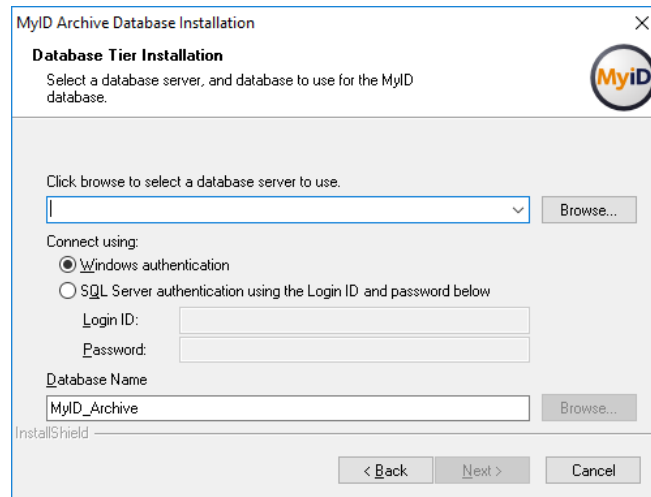
8.4.1 Create a separate database for audit records

1. Run the MyID installation program.
2. Select **Modify**, then click **Next**.
3. Select the **Archive Database Tier** option.
Note: Do not deselect any of the existing options.
4. Click **Next**.
5. Type the **User Name** and **Password** for the MyID COM user, then click **Next**.
6. Type the **User Name** and **Password** for the MyID web user, then click **Next**.
7. If required, type the **User Name** and **Password** for the MyID web service user, then click **Next**.

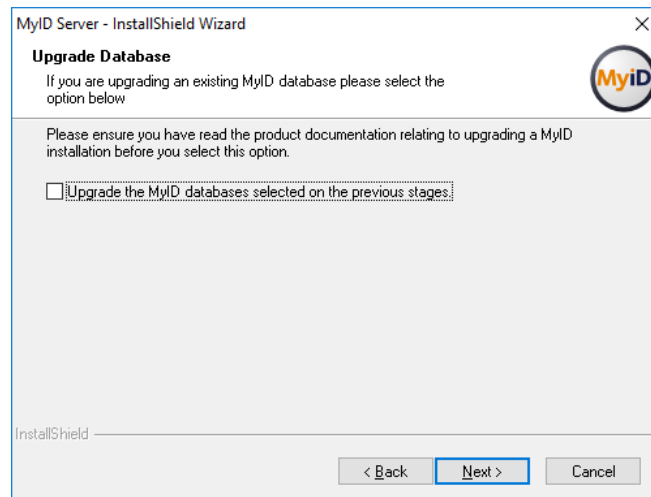


The screenshot shows the 'MyID Database Installation' window with the 'Database Tier Installation' tab selected. The instructions state: 'Select a database server, and database to use for the MyID database.' Below this, there is a section for selecting a database server with a dropdown menu and a 'Browse...' button. The 'Connect using:' section has two options: 'Windows authentication' (selected) and 'SQL Server authentication using the Login ID and password below'. The SQL authentication section includes fields for 'Login ID:', 'Password:', and 'Database Name' (with a 'Browse...' button). At the bottom, there are 'Back', 'Next >', and 'Cancel' buttons. The 'MyID' logo is visible in the top right corner.

8. Select the **Database Server** from the drop-down list.
9. Click **Browse** and select the main MyID database from the list.
10. Click **Next**.



11. Select the archive **Database Server** from the drop-down list.
12. Type the **Database Name** for the new audit database.
13. Click **Next**.



Do not select the upgrade option. Click **Next**.

Note: When the installation has completed, if you have any patches installed on your system, you must run all of the patch installation programs to select the Archive Database tier to ensure that the structure and operation data of the archive database matches the main database.

14. Update the audit .udl file to point to the correct database:
 - a) Open a Windows command prompt as an Administrator.
 - b) Navigate to the Windows `SYSWOW64` folder.
 - c) Type the name of the audit .udl file; for example, `MyiDAudit.udl`, then press Enter.
This opens the Data Link Properties dialog, which allows you to change the data link file.
 - d) Set the properties to point to the server and database you created to store the audit information.

8.5 Archiving the audit trail

Every operation within MyID generates audit information. Over time, this information can build up and ultimately reduce performance due to the size of the data. As a solution to this, you can create an *archive* database.

- Old audit data (which is likely to be rarely viewed) is transferred into this database using an SQL scheduled task.

Note: MyID does not automatically archive records; you must set up the scheduled SQL task. See section [8.5.2 Create an SQL Timed Task on SQL Server 2012](#) for details.

- The quantity of the *live* (recent) audit data, which is the data that is viewed most often, is kept small. This improves search performance.

Warning: The instructions in this section allow you to archive the audit trail. You must check Microsoft documentation for full operating instructions for Microsoft SQL Server.

You can still view archived audit information within MyID. The default MyID installation stores both current and archived audit information (separately) within the main MyID database. You can also store current and archived audit information in separate databases, which could be on separate servers.

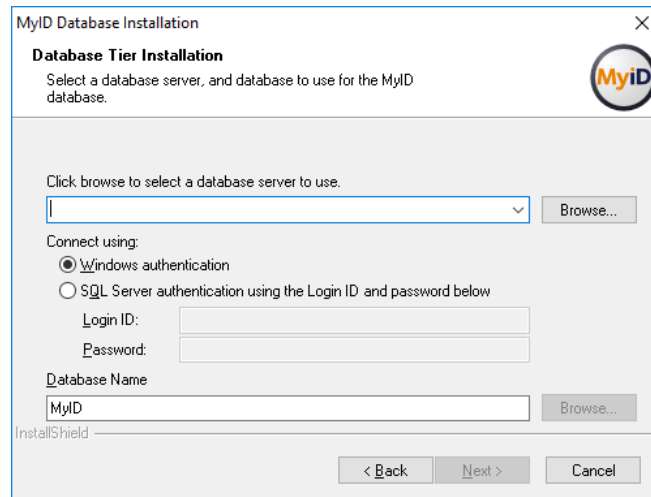
8.5.1 Create a separate database for archiving audit records

You can select the **Archive Database Tier** option when installing MyID to create an archive database. Alternatively, you can modify an existing installation to add an archive database.

Note: This procedure is very similar to creating a separate audit database. The difference is that the audit database is used for *current* audit records and uses the `MyIDAudit.udl` file to point to the database, and the archive database is used for *old* audit records, and uses the `MyIDArchive.udl` file to point to the database.

1. Run the MyID installation program.
2. Select **Modify**, then click **Next**.
3. Select the **Archive Database Tier** option.

Note: Do not deselect any of the existing options.
4. Click **Next**.
5. Type the **User Name** and **Password** for the MyID COM user, then click **Next**.
6. Type the **User Name** and **Password** for the MyID web user, then click **Next**.
7. If required, type the **User Name** and **Password** for the MyID web service user, then click **Next**.



MyiD Database Installation

Database Tier Installation
Select a database server, and database to use for the MyiD database.

Click browse to select a database server to use.

[Drop-down list] [Browse...]

Connect using:

☒ Windows authentication

☐ SQL Server authentication using the Login ID and password below

Login ID: [Text Box]

Password: [Text Box]

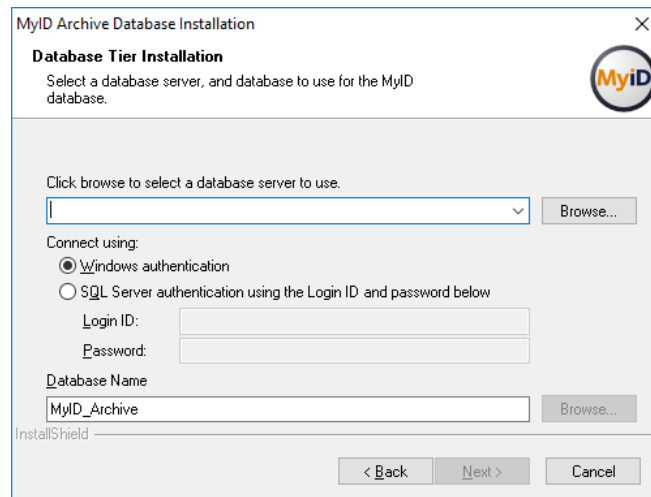
Database Name

MyiD [Browse...]

InstallShield

< Back Next > Cancel

8. Select the **Database Server** from the drop-down list.
9. Click **Browse** and select the main MyiD database from the list.
10. Click **Next**.



MyiD Archive Database Installation

Database Tier Installation
Select a database server, and database to use for the MyiD database.

Click browse to select a database server to use.

[Drop-down list] [Browse...]

Connect using:

☒ Windows authentication

☐ SQL Server authentication using the Login ID and password below

Login ID: [Text Box]

Password: [Text Box]

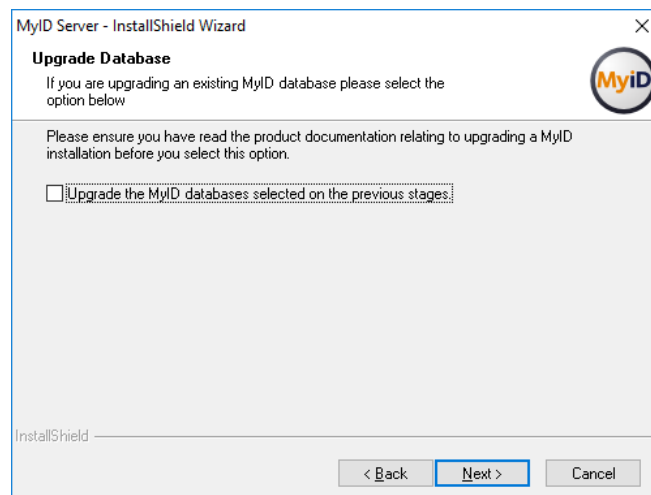
Database Name

MyiD_Archive [Browse...]

InstallShield

< Back Next > Cancel

11. Select the archive **Database Server** from the drop-down list.
12. Type the **Database Name** for the new archive database.
13. Click **Next**.



MyiD Server - InstallShield Wizard

Upgrade Database
If you are upgrading an existing MyiD database please select the option below

Please ensure you have read the product documentation relating to upgrading a MyiD installation before you select this option.

☐ Upgrade the MyiD databases selected on the previous stages.

InstallShield

< Back Next > Cancel

14. Do not select the upgrade option. Click **Next**.

Note: When the installation has completed, if you have any patches installed on your system, you must run all of the patch installation programs to select the Archive Database tier to ensure that the structure and operation data of the archive database matches the main database.

15. Update the archive .udl file to point to the correct database:

- a) Open a Windows command prompt as an Administrator.
- b) Navigate to the Windows SYSWOW64 folder.
- c) Type the name of the archive .udl file; for example, MyIDArchive.udl, then press Enter.

This opens the Data Link Properties dialog, which allows you to change the data link file.

- d) Set the properties to point to the server and database you created to store the audit information.

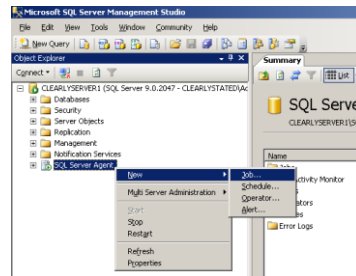
8.5.2 Create an SQL Timed Task on SQL Server 2012

This procedure is performed on the SQL server that stores the live audit information.

1. Select the **SQL Server Agent** in the Microsoft SQL Server Management Studio.

Note: You will not be able to access the folders described in the following steps unless the service is running. You may have to start it by right-clicking it and selecting **Start** from the menu.

2. Right-click the **SQL Server Agent** and select **New**, then **Job** from the menus displayed.



3. The **New Job** box is displayed, with the **General** page highlighted.

- a) Give the job an appropriate **Name** to help you identify it later.
- b) Set **Owner** to an account with administrative privileges.

Note: If the archived data is to be stored on a separate server, the account must have sufficient privileges for both the current server *and* the server that will be used to store the archive.

4. On the **Steps** page, click **New** to create a new step for the job.

The **New Job Step** box is displayed.

- a) Enter a **Step name**.
- b) Select the **Database** that contains the data to be archived; this is your main MyID database.

5. In the **Command:** area, type:

```
sp_ArchiveAudit '<archivedatabase>', <daysOld>
```

where

- ♦ **<archivedatabase>** is the name of the database that will store the archived data.

- If a single database is being used to store both live and archive information, then the value of `<archivedatabase>` will be the same as the name selected from the list in **Database**. The archived data will be moved into a separate table.
- If the archive database name begins with numbers, you must enclose the database name in square brackets. For example:

```
sp_ArchiveAudit '[20100101_CMSArchive]', 90
```

- If the archive database exists on a different server, you must configure this as a named "linked server" within SQL Enterprise manager.

The `<archivedatabase>` would then be specified as:

```
<LinkedServerName>.<ArchiveDatabaseName>
```

where:

`<LinkedServerName>` is the name of the linked server.

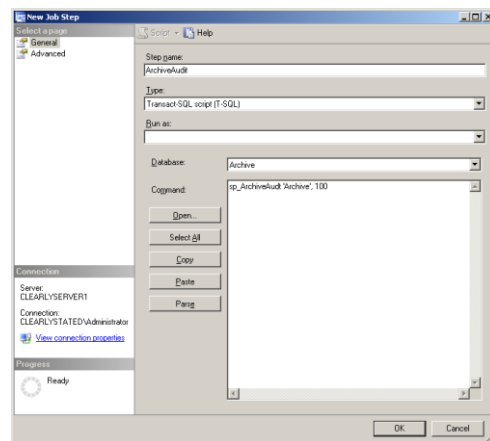
`<ArchiveDatabaseName>` is the name of the archive database on that server.

- ◆ `<daysOld>` is the age of data, in days, that will be archived.

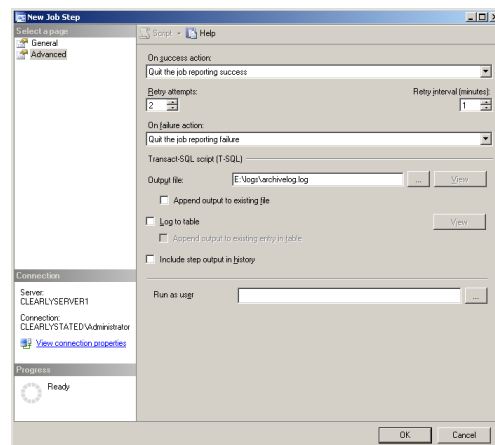
For example:

```
sp_ArchiveAudit 'ArchiveDB', 90
```

When this task runs, all audit data that is more than 90 days old is moved from the database chosen in **Database** to the `ArchiveDB` database.



6. On the **Advanced** page, specify a log file.



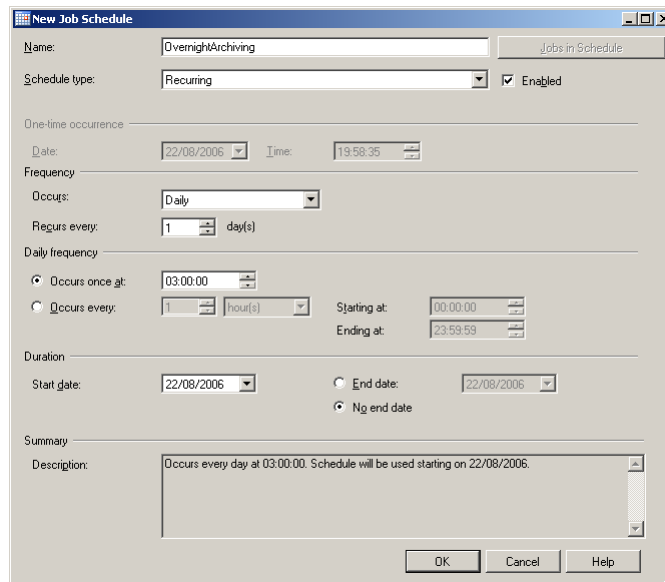
The audit archiving procedure produces a log file that reports statistics concerning the archiving procedure, including the number of records archived and error information. Intercede recommends that you record this information in a log file as a record of the archiving procedure.

- a) Enter a name for the log file in the **Output file** box.
Make sure that the path specified is a valid directory on the SQL server.
- b) If you want to keep earlier information, select **Append output to existing file**.
If you do not select **Append output to existing file**, the log file will be replaced every time the archive procedure runs and you will lose earlier information unless you have taken other steps to retain it.
- c) Select the **Include step output in history** option.
- d) Click **OK**.

7. Create a schedule.

- a) Click **Schedules**.
- b) Click **New**.

Although it is possible for users to access MyID while archiving is taking place, it is better to select an off-peak time (for example, overnight) so database performance is not affected.



- c) Give the schedule an appropriate **Name**.
 - d) Select **Recurring** in **Schedule type**.
 - e) Make sure the **Enabled** box is selected.
 - f) Set a schedule to meet your requirements. The example shows a daily schedule, at 3:00 a.m.
 - g) Click **OK** on the **New Job Schedule** dialog box to accept the schedule.
 - h) A summary of the schedule is displayed. Click **OK**.
8. Click **Notifications**.
- a) Select **Write to the Windows Application event log** and **When the job completes** from the associated drop-down list.

You may optionally specify that operators be emailed or paged according to your own administrative policies. This would allow you to further track the status of the archiving.

- b) Click **OK**.

The timed archiving task is now configured. Check the logs to make sure that the audit archive procedure is running successfully.

8.6 Archiving the System Events

You can set up MyID to archive the contents of the system events table in the MyID database periodically in a similar way to archiving the `Audit` table; see section 8.5, [Archiving the audit trail](#).

You can use the `LogEventsArchive` table, and a stored procedure, `sp_ArchiveLogEvents`.

Set up a SQL Timed Task on your MyID database to run the `sp_ArchiveLogEvents` procedure periodically. The syntax is as follows:

```
sp_ArchiveLogEvents '<archivedatabase>', <daysOld>
```

where:

- `<archivedatabase>` is the name of the database that will store the archived data.
 - ♦ If a single database is being used to store both live and archive information, then the value of `<archivedatabase>` will be the same as main MyID database. The data will be moved into a separate table.
 - ♦ If the archive database name begins with numbers, you must enclose the database name in square brackets. For example:

```
sp_ArchiveLogEvents '[20100101_CMSArchive]', 90
```

- ♦ If the archive database exists on a different server, you must configure this as a named "linked server" within SQL Enterprise manager.

The `<archivedatabase>` would then be specified as:

```
<LinkedServerName>.<ArchiveDatabaseName>
```

where:

- `<LinkedServerName>` is the name of the linked server.
- `<ArchiveDatabaseName>` is the name of the archive database on that server.
- `<daysOld>` is the age of data, in days, that will be archived.

For example:

```
sp_ArchiveLogEvents 'ArchiveDB', 90
```

8.7 Creating database maintenance plans

A maintenance plan should form part of your database authority recovery procedures.

Enterprise Manager provides a method to create maintenance procedures to manage the size of the transaction log and database files. It is important that these procedures are adopted following installation.

The maintenance plan is activated as a wizard within Enterprise Manager. You can either:

- Select **Taskpad** from the **View** menu and choose **Create a Maintenance Plan** from the list of wizards provided.
- Right-click the database, select **All Tasks** and then **Maintenance Plan** from the menu displayed.

For a full explanation of maintenance plan procedures, consult the appropriate Microsoft SQL documentation available as part of the SQL installation or online from <http://msdn.microsoft.com>.

8.8 Scheduled certificate revocation operations

MyID provides the ability to execute scheduled certificate request and revocation operations. This is typically used to perform regular maintenance tasks, such as automatically revoking certificates that have been suspended for a pre-configured length of time.

The detection and flagging of certificates to be revoked is typically performed by a stored procedure (for example, `sp_CertStatusRevokeProcess`). The submission of these requests to the Certificate Authority relies on processes carried out automatically by the Certificate Services, which are setup during installation.

Note: To configure MyID to revoke suspended certificates after a given time period, you have to edit the **Suspend to revoke period** option in the **Certificates** tab of the **Operation Settings** workflow. Update the value to the number of days a suspended certificate exists before revocation. By default, this option has a value of zero, which will be ignored by the automatic processor.

8.9 Application recycling

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.

8.9.1 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.

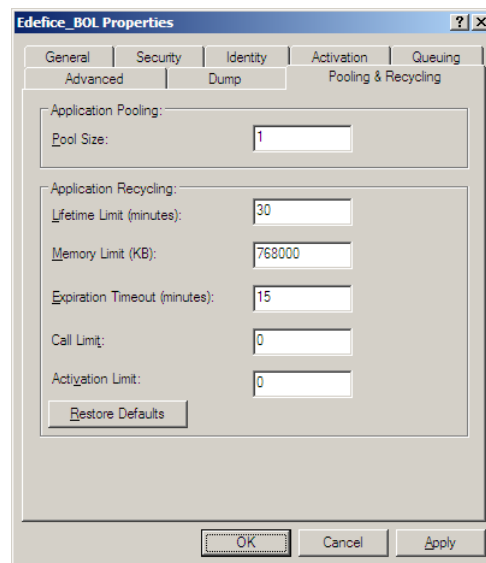
The Edefice_BOL component is installed with a default lifetime of 120 minutes; the other MyID components are installed with a lifetime of 0. All MyID components are installed with a memory limit of 0.

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
 - ♦ ePKIConfig
 - ♦ Entrust_Admin
 - ♦ ImportProcessor
- 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.

8.10 HSM concurrency

You can control the multithreading behavior of KeyServer using registry settings on the MyID application server.

8.10.1 Concurrent sessions

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Intercede\Edefice\MasterCard\KeyProviderMaxConcurrentSessions

This option controls the number of HSM sessions that will be created by KeyServer; 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.

8.10.2 Retries

`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Intercede\Edefice\MasterCard\KeyProviderMaxRetries`

This option defines the maximum number of times a failed operation will be retried by `KeyServer`, 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.

8.11 IIS server caching

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 web site (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.

9

Setting Up Email

MyID allows you to configure SMTP servers to send email messages.

You can create more than one SMTP server – MyID will send email notifications through each configured external system.

Note: Previous versions of MyID used Database Mail. For more information on upgrading existing systems, see [5.3.11, Upgrading email support](#).

To set up an SMTP server:

1. From the **Configuration** category, select **Operation Settings**.
2. On the **Notifications** tab, set the **Send Email Notifications** option to **Yes**.
Note: You may have to restart the MyID Notifications Service to pick up this change.
3. Click **Save changes**.
4. From the **Configuration** category, select **External Systems**.
5. Click **New**.
6. From the **Listener Type** drop-down list, select **SMTPServer**.

7. Set the following options:
 - ♦ **Name** – Type a name for the external system.
 - ♦ **Description** – Type a description for the external system.
 - ♦ **Enabled** – Make sure this option is set to **Yes**
 - ♦ **SMTP Server** – Type the IP address or name of the SMTP server. For example:
smtp.example.com
 - ♦ **SMTP Port** – Type the port number of the SMTP server. For example, 25.
 - ♦ **SMTP Authentication** – Select one of the following options:
 - **Anonymous** – The SMTP server does not require any authentication.

- **Use application account** – Authenticate to the SMTP server using the MyID named COM user.
- **User/password authentication** – Type the SMTP Username and enter and confirm the SMTP Password to be used to authenticate to the SMTP server.
- ♦ **Use TLS for SMTP** – Select this option if you want MyID to connect to the SMTP server using a secure (TLS/SSL) connection.
- ♦ **MyID Mail From address** – Type the email address that will appear in the From field on email messages sent by MyID.
- ♦ **MyID Mail Reply-To address** – Type the email address that will be used when a user replies to an email message sent by MyID.
- ♦ **Sign outgoing emails** – Select this option to sign the content of the email messages that MyID sends. See section 9.1, *Signing email messages* for details.
- ♦ **Email address (for test connection)** – Type an email address that will be used when you click the **Test connection** button.

Note: The email address for the test connection is not stored when you save the external system.

8. Click **Test connection**.

MyID sends a test email message to the specified email address. Check that the email message has been received.

Note: You cannot send a test email message if the **Send Email Notifications** option is set to **No**. Also, if you are using signing, and have multiple application servers, this test will confirm that the signing certificate is set up only on the application server to which you are currently connected.

9. Click **Save**.

9.1 Signing email messages

MyID can sign the content of the email messages it sends. You must make sure that you have set up the following:

- Set up the certificate template on the certificate authority to include the **Secure Email** attribute in the **Application Policies** extension.

Note: If you do not set this attribute on the certificate template, the email messages will be sent, but will be unsigned.

- Configure the MyID application server that is processing the email with a valid signing certificate.

To configure the application server's signing certificate:

- ♦ Import or create an email signing certificate where the Subject matches the From address of the SMTP configuration.
- ♦ Export the email signing certificate to a `.cer` file on the application server.
- ♦ Set the following registry value to the full path of the `.cer` file on the application server:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Intercede\Edefice\Server
\Mail\SigningCertificate
```

- Set the **Sign outgoing emails** option for the SMTP server in the **External Systems** workflow.
- Set the **Signed** option for the appropriate email template in the **Email Templates** workflow.

10 Uninstalling MyID

A Domain Administrator can uninstall MyID without any issues. However, a Local Administrator will experience problems when uninstalling MyID through the Windows Control Panel. Instead, you must uninstall MyID by running the MyID installation program using **Run as administrator** and selecting the **Remove** option.

10.1 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 application and web servers, delete the MyID program folder.
For example, `C:\Program Files (x86)\Intercede\MyID`.
3. On the application server, delete the MyID `.udl` files from the Windows `SYSWOW64` folder.
These files start with the name you provided for the MyID database; for example, `MyID.udl`, `MyIDAudit.udl` and `MyIDArchive.udl`.
4. On the application server, delete the MyID section of the registry.

You must delete the following section:

- ◆ `HKEY_LOCAL_MACHINE\SOFTWARE\wow6432Node\Intercede`

11 Business Continuity Planning

MyID is designed to be a critical part of enterprise security architecture and needs to be fully integrated into a disaster recovery plan. The critical part of any disaster recovery system is advanced preparation.

In practice each system deployment is different, with its own characteristics. While this document can provide a high-level outline plan, we recommended that you contact Professional Services at Intercede to design a full disaster recovery capability.

11.1 Phase 0: Pre-disaster

Ensure you have backed up the live data.

- Backup the MyID databases on the existing live server.
- Backup the MyID data in the `upimages` folder on the live web server, if necessary.
- Backup the MyID windows registry information on the live application server.
- Ensure any security credentials are backed up. For example: authentication or signing credentials to access a PKI system, or HSM data.
- Store copies of the MyID application software, plus any local customization and patches, in a secure location, off-site.

11.2 Recovery

Disasters can happen on many levels, from losing just one disk on one server through to an entire server infrastructure being lost. This section describes rebuilding a full three-tier MyID installation. You can use portions of this information if the disaster is confined to a specific server.

Warning: Before attempting any system recovery, we recommend that you contact Intercede's support team to validate your recovery plan.

11.3 High-level recovery plan for re-building a three-server architecture

Note: This section assumes a standard three-server architecture without advanced configuration such as a DMZ.

11.3.1 Phase 1: Prepare new servers

1. Install Windows Server on three new servers: web, application and database.
 - ♦ SQL Server should be installed on the database server.
 - ♦ All three servers should be members of the same Windows domain.
 - ♦ Ensure that the time on the new database server is synchronized with the time on the previous database server.
2. Restore any third party systems that MyID requires access to, for example a directory or certification authority (CA).
3. Restore any credentials needed to access the third party systems: for example PKI keys, HSMs.
4. Install the MyID web, application and database components on the appropriate servers. Follow the installation documentation on the CD but incorporate any site-specific deviations that you made for the original installation.

5. Install any local customizations and patches.

11.3.2 Phase 2: Restore backed-up data

1. Restore data from the `upimages` folder on the live web server to the web server.
If you are using an external server as an image store, you may not need to carry out this step.
2. Restore the MyID registry files from the live application server to the new application server. This will overwrite the existing registry settings, with the appropriate key information relating to the backed up database.
3. On the database server, replace the newly installed MyID databases with the backed up database from the live system.
4. Replay any transaction log data from the live system to the new database to ensure data is restored up until the point of failure.
5. Check the **Configuration** tab on the **System Status** report and update any configuration options that refer to specific server names or IP addresses.
6. Reboot the three new servers to ensure they are using the new registry and databases.

11.3.3 Phase 3: Test new system

1. Test basic MyID operations. For example, can Operators logon with their smart cards.
2. Test end-to-end card production.
3. Assuming everything is functioning correctly, backup the new MyID database.

11.4 Two-server and one-server architectures

The procedure for two-server and one-server architectures is essentially the same as for a three-server architecture. Apply the appropriate steps to the relevant co-located server.

11.5 System integration

MyID is designed to interact with third party systems, such as directories and certification authorities. Depending on the scope of the disaster, these systems may need to be restored as well.

This introduces a complexity in the recovery timing that needs to be carefully planned to ensure the security integrity of the overall system. Care needs to be taken to ensure that the recovered system has end-to-end data integrity.

For example consider a three-component system, containing a directory, a CA and MyID. To issue a PKI credential, the user must be known to all three components.

In a disaster where data recovery is required, it is important to ensure that MyID, the directory and the CA are all restored to exactly the same point in time. If not:

- The directory may contain users not in MyID, if the database was recovered from a later period than MyID.
- The CA may have records of certificates issued that are not known to MyID and so cannot be revoked by MyID. This would happen if the CA was recovered from a later period than MyID.

- MyID may have knowledge of credentials issued that are not known to the CA, if the CA was recovered to a period of time before MyID. This is a critical security issue as in principle a live certificate has been issued by MyID that cannot be revoked, as the CA has no knowledge of it.

12 Failover Strategy

MyID has been designed to support failover and redundant component architectures to ensure the availability of the MyID solution. This section describes the architecture options available.

12.1 Typical MyID architectures

MyID consists of three major system components: a web server, an application server and a database server.

These can be hosted on:

- A single machine
- Two machines (separating the database from the other two components)
- Three separate machines

Typically a two-machine architecture is used, with the web server and application server co-hosted on a single machine, as shown in Figure 1.

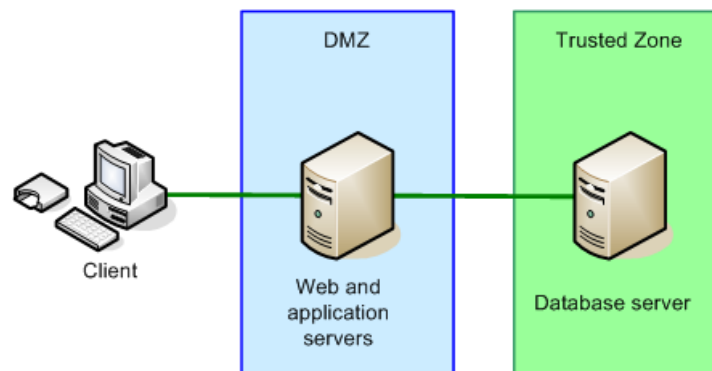


Figure 1 The database server hosted separately to the web and application servers.

For high security environments, a three-machine architecture may be used, as shown in Figure 2.

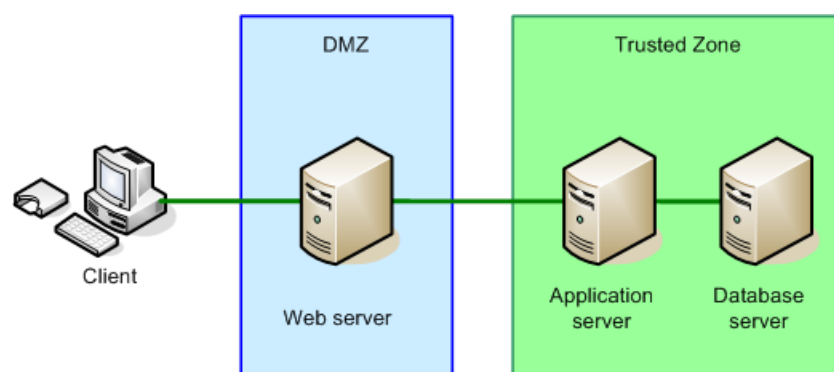


Figure 2 The application server hosted on a separate machine, in the trusted zone.

12.2 Co-hosted web and application servers

12.2.1 Duplicate infrastructures

One option is to have a duplicate MyID infrastructure, with a failover TCP/IP router providing access.

- If the web server fails, the router will automatically switch traffic to the backup website.
- If the database server fails, a manual switch of the failover router would be required. There are many commercially available products for monitoring systems that can do this automatically.
- The backup database contains a duplicate of the main database, provided using the Microsoft SQL Server Transaction Log Shipping system, for example.

Other systems that can provide database duplication are:

- ♦ Database failover clustering
- ♦ Database backup / restore procedures
- ♦ Disk / file system mirroring
- ♦ Third party utilities

Note: You cannot have two live databases running at the same time.

During a failover, any current operations will fail and the user will need to re-authenticate before continuing. Other than that the operation should be seamless.

An example of this configuration is shown Figure 3, with the web server and application server co-hosted on a single machine.

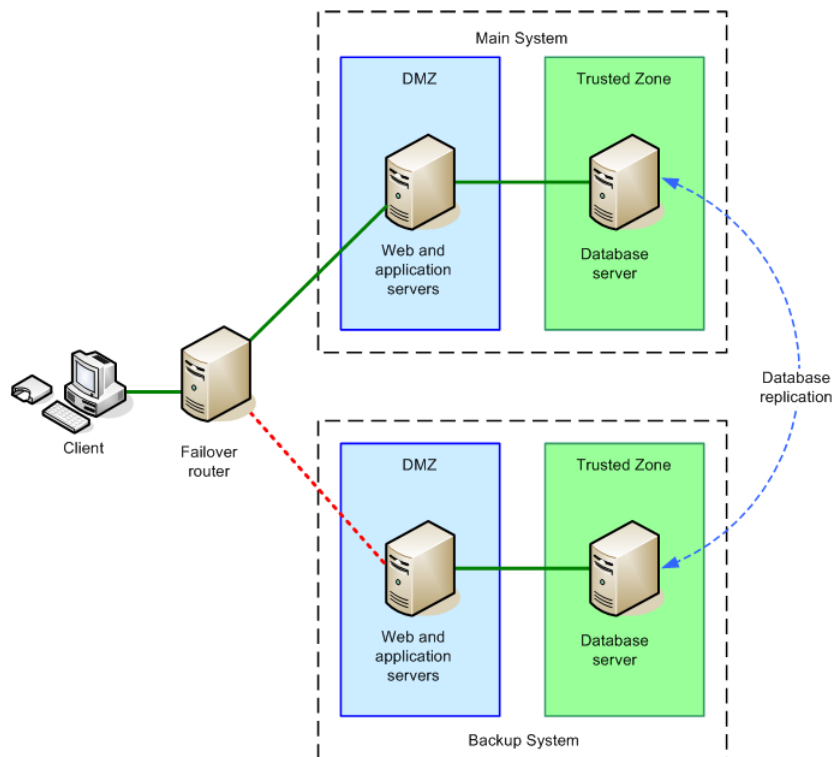


Figure 3 Duplicate MyID infrastructure: web and application servers on the same machine.

This solution provides resilience against both component and network failure. It is common to locate the main system and backup system on different networks, hosted on different sites, to protect against total infrastructure failure at on site, such as a major power failure.

12.3 Split web and application servers

For additional security, the application and web servers may be hosted on separate machines, on different network segments.

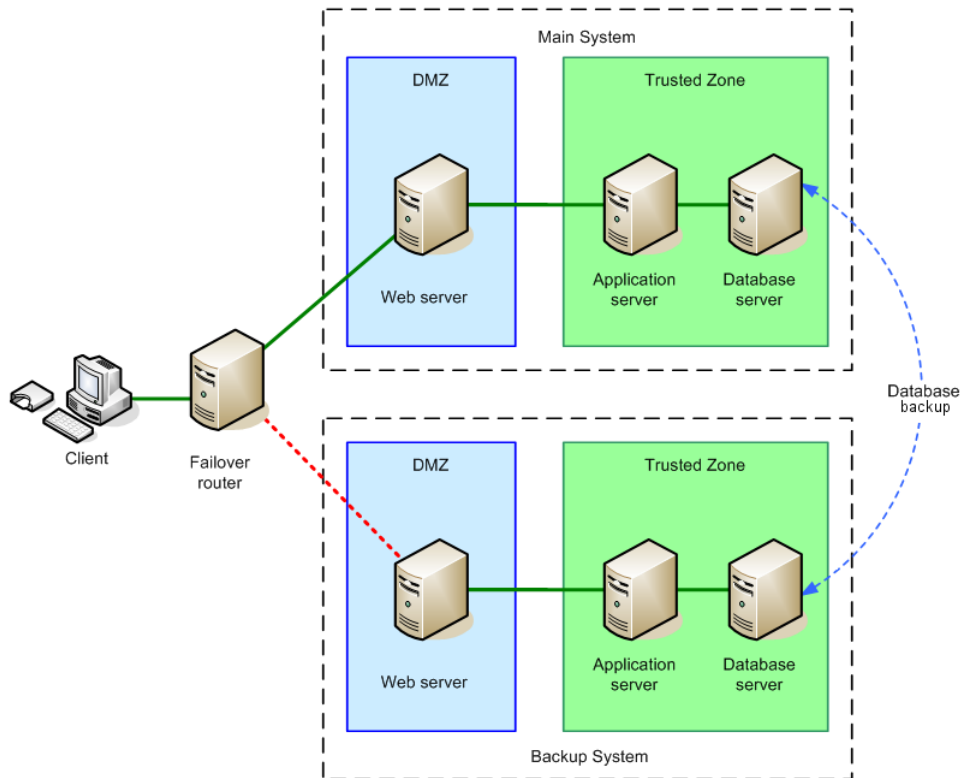


Figure 4 Use of database failover in a three-machine deployment.

If the database server fails, a manual switch of the failover router would be required. As previously stated, there are many commercially available products for monitoring systems that can do this automatically. Contact customer support for more information.

Note: You cannot mix servers from the main system with the backup system – if the web server from the main system fails, and the application server from the backup system fails, there is no load balancing configuration that will allow the backup web server to work with the main application server.

12.4 Additional considerations

12.4.1 User images

User images are stored on the MyID database server, and are handled by database replication.

Images uploaded from the Card Layout Editor are stored on the web server.

On older systems, user images may also be stored on the web server; in environments where the images are uploaded by the user and duplicate web servers are used, extra configuration will be required to ensure the virtual file store used by the images is available to both servers. A typical option to use is Microsoft's file store synchronization.

Note: You may store your images on a separate server, in which case you must ensure that the image store is available on a duplicate server.

12.4.2 Clustering

The architectures presented in this document so far can be used to build a resilient infrastructure when a failover capability is required to ensure system availability.

In some environments, once redundancy has been built into the system, the backup systems are used to provide load-sharing. This can be achieved using clustering technology.

A cluster architecture will also provide even greater system availability than the failover solutions described above.

The example in Figure 5 shows how MyID can be used with a database cluster.

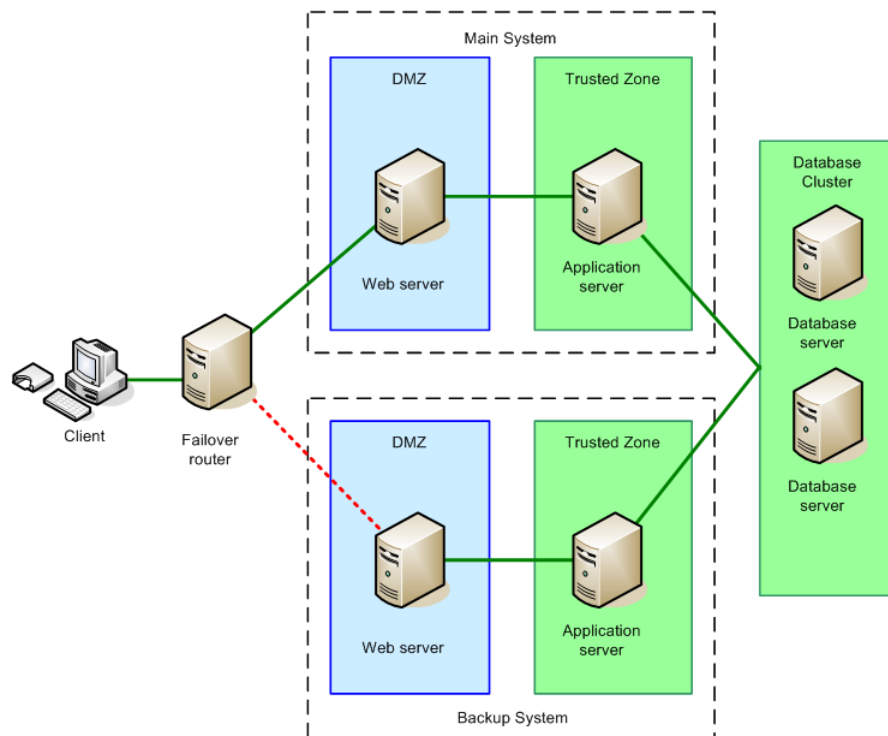


Figure 5 MyID configured to use a database cluster.

As well as database clusters, web server clusters or farms can be used, provided that support for session affinity is enabled, as MyID uses ASP Session State. You must make sure that your servers support session affinity both for the MyID web servers and the MyID web services servers.

You can also consider using load-balancing across a farm of application servers.

12.4.3 Hardware

All of the servers in the system should have redundant components. Specifically we recommend dual power supplies, a RAID disk array and dual network cards.

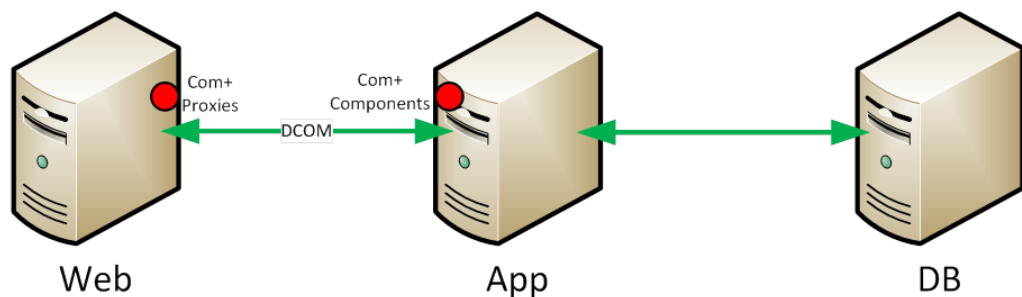
Clustering Microsoft Windows servers usually requires dedicated cluster hardware with high-speed connections between the servers. While this is more expensive than 'standard' servers, it provides the highest levels of redundancy and load-balancing.

12.5 Failover and redundancy considerations

The text referring to support for 'web server clusters' means that you can add additional servers for failover/backup purposes for the web layer, but the important thing to understand is that there is an architectural limitation of the COM+ components that are at the core of MyID that means that there must be a fixed mapping between web servers and the application server that they are paired with.

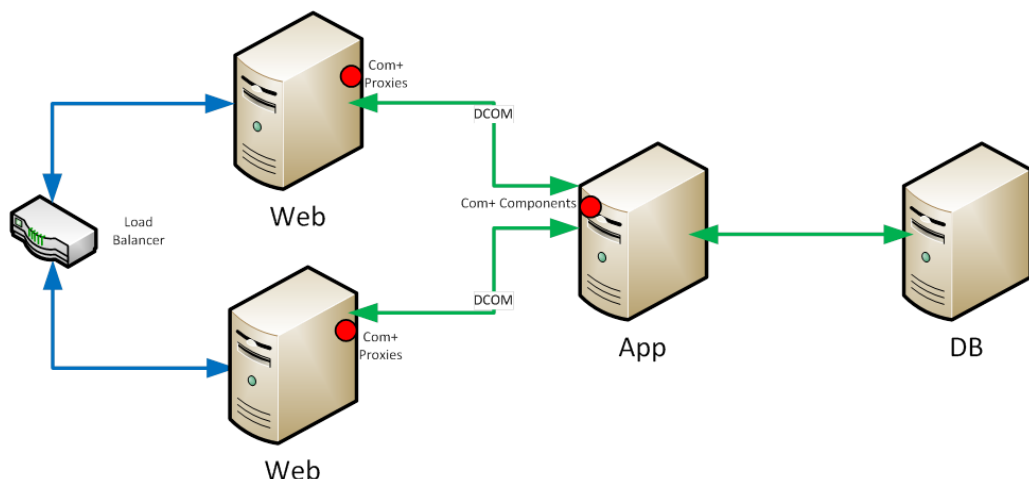
For example, in this diagram on a linear 3-tier model, the COM+ proxies that run on the web server are:

- created from the original COM+ components on the application server,
- then exported to the web server and installed there,
- then used by the MyID web site to drive the primary components on the application server.



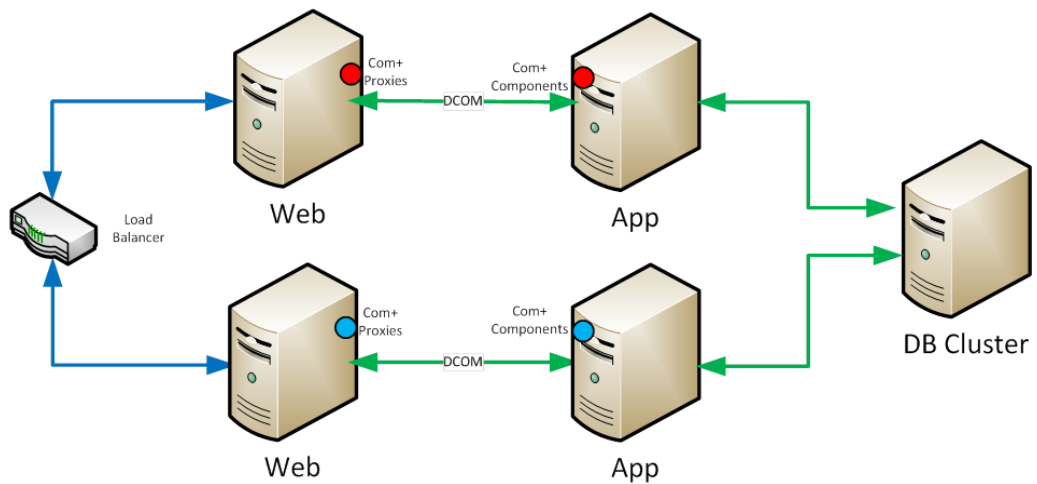
The proxies that run on the web server must be derived from the instance of the components on the individual application server that they are paired with.

This means that you can add additional web servers (for example, a cluster or farm) that share the same proxies and are therefore paired with a specific application server. For example:



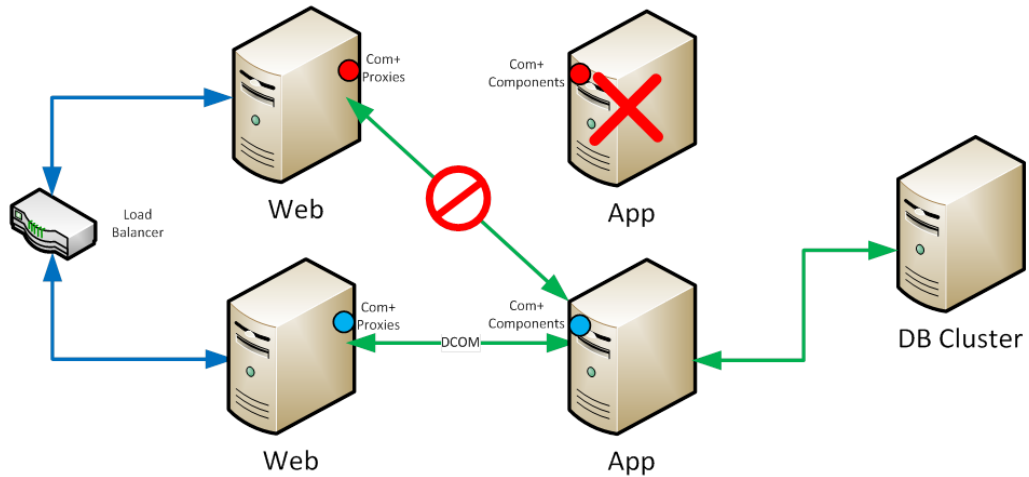
This is OK because each web server (with the COM+ proxies that run it) is still paired with a specific application server. However, this model creates redundancy/failover in the web layer only, meaning that there is still a single point of failure at the application server level.

Therefore, customers seeking a fully redundant system are advised to duplicate the application/web channel, as well as using a SQL Cluster for hosting the MyID database:



In this model each web server is individually paired with each application server (represented by the different colored circle for the COM+ components).

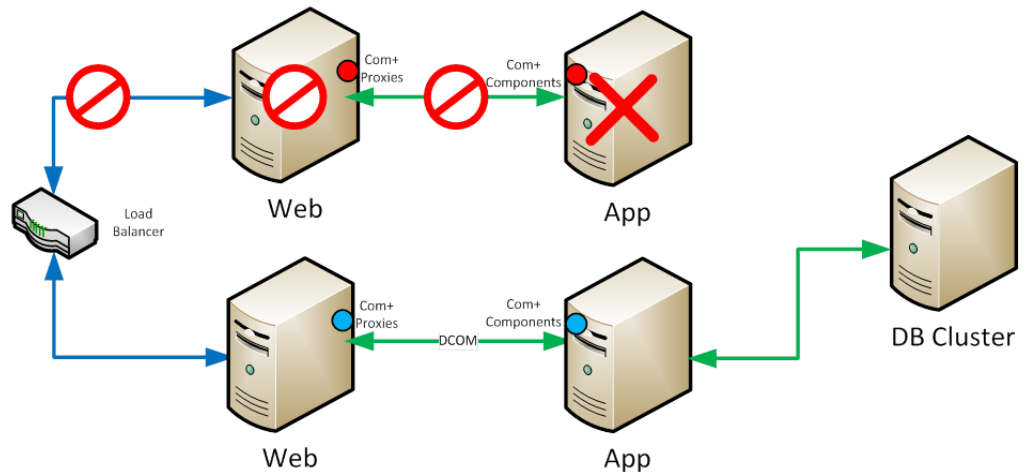
There cannot be any failover from a web server in one channel to the application server in another without manual reconfiguration. For example:



This is because the proxies on the web server in the top channel are not paired with the application server on the second channel. That is, the communications from top channel web server to the second channel application server will not work.

It is for this reason that each web to application channel must be treated as a single unit in failover decisions.

That is, if any part of the top channel fails, the load balancer/failover router can switch all MyID traffic to the second channel:



This requires that the load balancer/failover router be capable of monitoring the health of each channel as a whole and not just the web server that sits at the front of it.

This depends on the capabilities of the load balancer/failover router in use. For example, potentially it could base its failover decisions on a combination ping/heartbeat to both the web and application server in each channel.

13 Advanced Deployment

13.1 Windows services

The following is a list of the Windows services installed on the application server by MyID:

| Name | Display Name | Startup | Description |
|----------------------|------------------------------|---------------------------|--|
| eBureauSrv | eBureauSrv Services Server | Automatic | eBureauSrv Services Polling Agent. Note: Only present on systems that have been configured for bureau integration. |
| eCertificateSrv | eCertificate Services Server | Automatic (Delayed Start) | eCertificate Services Polling Agent. |
| eJobServer | eJobServer | Automatic | Asynchronous processing of CMS jobs. |
| eKeySrv | eKeyServer | Manual | Encryption Service – must be set to manual start. |
| eMessageSrv | eMessageServer | Manual | Messaging service. |
| NotificationsService | MyID Notifications Service | Automatic | MyID Notifications service |

All MyID services run using the MyID COM user.

13.2 Communication, security and trust

The following descriptions explain the communication channels that are needed when deploying each tier on a separate machine.

Note: Each Windows server used with MyID must be in the same, or a trusted, Windows domain. MyID relies on Windows domain level security.

If you need to work in a non-domain environment, or require additional levels of security between server tiers, contact customer support quoting reference SUP-74 to discuss your requirements.

13.2.1 Client to web server

MyID client to web server communication is performed via HTTP or HTTPS (recommended).

HTTPS can be used in either server-authentication only mode, or to authenticate both client and server. This is achieved through standard Windows IIS configuration. For production environments, as a minimum, you must set up one-way SSL/TLS to ensure encryption of traffic between the client and the webserver.

MyID web-based clients require some ActiveX components in order to allow communication between the browser and other devices such as smart card readers, biometric devices, card printers, cameras, or scanners.

These components may be installed locally from CD, or downloaded as an Authenticode-signed cabinet from the MyID server, or pushed out as an MSI file using group policy.

13.2.2 Web server to MyID server

The web server comprises ASP, HTML, JS, XSL, XML and image files, as well as ASP.NET and WCF web services. These communicate with the MyID middleware components using COM+ object instantiation.

- Where the middleware is co-located on the web server, this communication is directly through the COM+ framework.
- If the middleware is located on a separate MyID server, this communication is performed through the DCOM architecture.

DCOM uses RPC running over a TCP protocol which, by default, assigns communications ports on demand in the range 1024 to 65535. It is possible to restrict the ports used – this is important if you intended placing a firewall between the website and the MyID server. You will also need to enable port 135 to support the ‘end point mapper’. The Windows authentication and Active Directory protocols must also be opened. For further details see the document entitled “How to Configure Firewalls for Domains and Trusts” on the Microsoft website.

Note: DCOM will operate through a firewall *provided that it does not perform network address translation*. For further details see the document entitled “Using Distributed COM with Firewalls” on the Microsoft website.

Before installing MyID, verify that the necessary bidirectional RPC communication is available by using the Microsoft **DTC Ping** tool (available from the Microsoft website – Knowledge Base article 306843).

In addition to the above, it is recommended that additional intrusion detection software is implemented on the web server to prevent security breaches through unauthorized changes to the website.

DCOM port ranges

To force the RPC system to use a specific range for its dynamic ports:

1. From the Windows **Administrative Tools**, select **Component Services**.
2. Browse to **Console Root > Component Services > Computers**.
3. Right-click **My Computer** and select **Properties**.
4. Select the **Default Protocols** tab, ensure **Connection-oriented TCP/IP** is selected in the list and click the **Properties** button.
5. Set a port range.

You should ensure the base port is above 1024. You need a range of at least 100 ports; for example, 5000–5099.

6. Add the range, then click **OK**.

The port limit is not active until you reboot; however, you should set up the firewall before you reboot the machine.

Firewall configuration

You must open ports for the following:

- The ports to/from the Domain Controller to allow the web user to be authenticated.
- The DCOM port range you have set up (for example, 5000-5099).
- The RPC port (135). There is a predefined rule for port 135 called **COM+ Network Access** that you can enable.

- The HTTP or HTTPS ports (for example, 80 or 443). You need to open these ports from the application server to the web server, but not from the web server to the application server. General communications between the web server and the application server are carried out purely by DCOM – however, if you are using specific services on the web server that the application server needs to access (for example, for notifications, bureau, PACS, or web-hosted uploaded images) you must open the HTTP or HTTPS port.
- The ports for any external systems with which MyID needs to communicate.

See the documentation for the firewall you are using to open the necessary range of ports.

For example, to set up the default Windows firewall to use ports 5000-5099:

1. From the Windows **Administrative Tools**, select **Windows Firewall with Advanced Security**.
2. Select **Inbound Rules** and add a new rule using the **Actions** on the right.
3. In the wizard that appears, select **Port** for the rule type and click **Next**.
4. Select **TCP**.
5. Provide a list of the ports you specified in **Component Services**.
You can specify a range; for example:
`5000-5099`
6. Click **Next**.
7. Select **Allow the Connection** then click **Next**.
8. Make sure all three **Apply** rules are selected then click **Next**.
9. Type a name for the rule.
10. Finish the wizard.
11. Ensure the firewall is switched on, then reboot the machine

Note: You must carry out this procedure on both the web server and the application server.

13.2.3 Application server to database server

The MyID application server comprises middleware components that implement business object logic, interact with the various additional services (CA, authentication etc.) and abstracts the storage and retrieval of persistent data. This demands a connection to the database.

Database connectivity is achieved using data link (UDL) files that communicate through DTC/RPC. As it is possible to split the main, audit and archive databases across three separate data sources, three data link files are created. These may all point to the same database or different databases. The data link files are created in the `SYSWOW64` directory of the `Windows` directory with the following names:

- `<websitename>.udl`
- `<websitename>audit.udl`
- `<websitename>archive.udl`

The MyID COM+ account must be given at least read rights to the `.udl` files subsequently used to access the database server.

MS DTC must be configured to allow network DTC access on both the database server and the MyID server. See section [4.3, Timeouts, limits and other settings](#) for details.

It is also recommended that the SQL Server network utility on the database server and the SQL client network utility on the MyID server are configured to use TCP/IP only (*not* Named Pipes). You are recommended to disable Named Pipes on the application and database servers in **SQL Native Client 11.0 Configuration (32bit)** and **SQL Server Network Configuration** in the SQL Server Configuration Manager – if you have a firewall configured between the application server and database server, this step is essential.

It is recommended that the Microsoft **DTC Tester** tool is used to confirm connectivity. This is available from the Microsoft Knowledge Base website, article 293799.

DCOM port ranges

You must set up a range of approximately 100 ports to use between the application server and the database server.

Firewall configuration

You must open ports for the following:

- The DCOM port range you have set up. You must open the firewall for these ports in both directions.
- The SQL Server port (by default, 1433). Set up the firewall to allow communication from the SQL Server port to ANY, and from ANY to the SQL Server port.

See the documentation for the firewall you are using to open the necessary range of ports.

Encrypting the connection to SQL Server

The MyID application server communicates with the database server using the data link (UDL) files described above – typically this is configured to use Microsoft OLE DB Provider for SQL Server which in turn results in the database communications using MS DTC/RPC. By default these calls are made unencrypted.

For deployments where the MyID application server and database server reside in a dedicated secure server environment, this unencrypted transmission of data from server to server is not typically seen as a risk. That is, the physical and firewall separation of the server environment is enough to satisfy any security concerns.

However, for deployments where an extra level of security is required for communicating with the SQL Server database server, configuring SQL Server to use SSL/TLS will ensure that all data transmitted from MyID to the database is encrypted.

This is a SQL Server configuration rather than a MyID configuration. Instructions are provided by Microsoft in Technet article ms189067.

The following points should be noted if you want to set this configuration:

- SSL/TLS is a server-wide setting in SQL Server so enabling this configuration will affect every hosted database.
- There will potentially be a minor performance impact due to the SSL/TLS handshaking and encryption/decryption overheads.

13.2.4 Application server to LDAP directory server

MyID can import user account information from an LDAP directory ('slave' mode). It can also be configured to export user account information to an LDAP directory ('master' mode). The LDAP connection and attribute mappings are maintained in the MyID database.

MyID communicates with directory services using the LDAP protocol. By default, this will operate through port 389. If you are running in a Windows environment with both Active Directory and another directory service present, you will need to change this assignment to exchange data with the other directory. Secure LDAP may be employed where necessary.

By default, MyID authenticates to the LDAP server using the MyID COM+ account – the account under which the `edefice_BOL` component is running. Appropriate access rights must therefore be granted to the MyID account, depending on the operational mode of the installation.

Further details of LDAP configuration are covered in the [Administration Guide](#).

13.3 Application pools

MyID uses the following application pools:

- **MyIDPoolClassic** – uses a **Managed Pipeline** of **Classic**. Used for the MyID websites (including each language variant – **MyID\en** and **MyID\us** for example).
- **MyIDWebService** – uses a **Managed Pipeline** of **Integrated**. Used for the MyID web services (MyIDDataSource, MyIDProcessDriver, MyIDEnroll).

The application pools are created by the MyID product installation program.

13.4 Running multiple servers

A MyID system comprises a web server, an application server, and a database server. You may want to increase the number of servers of each type to provide more processing power, to distribute traffic, or to provide failover capability.

Note: Each web server must be paired with a single application server. You cannot load-balance the web server to application server traffic. However, you can have multiple web servers connected to the same application server – you can balance the client load across multiple web servers.

13.4.1 Multiple web servers

You can install multiple MyID web servers (and web services servers) that you can use in conjunction with a load balancer to distribute the network traffic across several servers.

Run the MyID application installation program on each web server and set up the COM proxies. See section [5.2, Split deployment](#) for details of installing the web server on a separate tier.

Once you have installed the web servers, configure your load balancer to distribute the traffic amongst the servers and set up session affinity. See your load balancer documentation for details.

13.4.2 Multiple application servers

You can install multiple MyID application servers to work in conjunction with your multiple MyID web servers.

You can use your load balancer to distribute traffic to the different web servers, and then you can configure each web server to communicate with a different MyID application server. All the application servers are connected to the same MyID database.

When you install the COM proxies on the web servers, you can decide which application server to use; this allows you to distribute the load. For example, you might have four web servers and two application servers – web servers A and B have the proxies for application server Alpha, which web servers C and D have the proxies for application server Beta installed.

To set up multiple application servers:

1. Establish an operational MyID system using a single application server.
2. On the primary application server, export the registry key that contains the master key.

The master key is located in the following part of the registry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Intercede\Edefice\Mastercard
```

You must make sure that all of the application servers use the same master key.

If you are using an HSM, you must install the HSM client software before you can import the key onto the additional application server. You must follow the instructions in your HSM integration guide; however, you do not need to create a partition or run GenMaster, as these have already been carried out on the primary application server.

If you require additional information on using multiple application servers with HSMs, contact customer support, quoting reference SUP-90.

3. If you are using a Microsoft Windows CA, issue a new Enrollment Agent certificate along with its private key. You must also export the KRA certificate on the app server and import it to each application server.
4. On each additional application server:
 - a) Import the master key registry settings.
 - b) Run the MyID product installation program to install the application tier.
 - c) If you are using a Microsoft Windows CA, each additional application server requires an Enrollment Agent certificate.

Normally this will be a different enrollment agent certificate for each application server, but if required you can export a copy of the enrollment agent certificate and private key from the original application server and configure on each additional application server.

If you manually import the same enrollment agent certificate onto additional application servers, you must write the certificate to a certificate store called `edefice`, using the `certutil` utility:

```
certutil -addstore -f -user edefice my.cer
```

where `my.cer` is the name of the file to which you exported the certificate.

Note: If your system uses a different certificate store for EA certificates, change `edefice` to the name of the appropriate store.

Note: The private key must also be present on the machine; for example, imported as a `pfx` file.

d) Disable the following service:

- `eBureauService` (only installed on systems that have been configured for bureau integration)

This service must be running on the primary application server only. If you do not disable the service on the additional application servers, you may experience problems.

e) If you have multiple MyID certificate services, make sure you set the `RecordSize` parameter in the registry for each to a value of 1.

The default registry location for this parameter is:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\eCertificateSrv\Parameters
```

Note: If you have multiple instances of the MyID certificate services running on the same application server, the registry key will be different from `eCertificateSrv` for the additional instances.

f) Export the COM proxies from the application server to the appropriate web server.

This allows you to distribute the traffic amongst your application servers.

g) On systems that use signing certificates (for example, PIV or CIV implementations):

i Check the registry key on the primary application server:

```
HKEY_LOCAL_MACHINE\SOFTWARE\wow6432Node\Intercede\Edefice\PIV
```

ii For each of the signing certificates (for example, `CHUIDSigningCertificate` or `SecurityObjectSigningCertificate`) check the location of the certificate, then copy the file from that location on the primary application server to the same location on the additional application server.

iii Update the registry on the additional application server for each signing certificate to match the primary application server.

h) Confirm that the MyID `.udl` files in the Windows `SYSWOW64` folder point to the correct database server.

These files start with the name you provided for the MyID database; for example, `MyID.udl`, `MyIDAudit.udl` and `MyIDArchive.udl`.

Note: To edit the `.udl` files, you must open a Windows command prompt, navigate to the `SYSWOW64` folder, then type the name of the `.udl` file and press Enter.

i) Restart the MyID application server.

▪ **IKB-206 – Multiple email notifications**

If you have multiple certificate servers configured in your MyID system, users may receive duplicate email notifications for certificate renewals. This is due to conflicting settings between the certificate services.

You are recommended to use an alternative configuration that prevents this situation by allowing the database server to control sending email notifications instead of the certificate services.

For more information, contact customer support, quoting reference SUP-253.

13.4.3 Multiple tiers with a web server in a DMZ

You may want to configure your system to have a web server in a separate domain. This web server can serve as a bridge between the outside world and the protected network that hosts the MyID application server and database.

To configure this, you must set up local users on your application and web servers, and configure the firewall to allow communication between the servers.

1. On both the application server and web server in the separate domain, create the following user accounts, and add them to the Distributed COM Users group:
 - ♦ LocalApp – this is the local account for running the MyID COM+ components.
 - ♦ LocalWeb – this is the local account for running the MyID web site.
 - ♦ LocalMWS – this is the local account for running the MyID web services.

Note: These are suggested names for the local accounts. You can use your own names, as long as you use them consistently across both servers.

2. On the application server, in **Component Services**, under **My Computer > COM+ Applications**, add the appropriate LocalApp, LocalWeb, and LocalMWS users to the MyID roles for each MyID component – these roles are:
 - ♦ App_Role
 - ♦ Web_Role

Add the appropriate local users to each role that contains the existing domain users. That is, if the role has the MyID COM+ domain user, add the local app user; if the role has the MyID web domain user, add the local web user; if the role has the MyID web service domain user, add the local MWS user.

3. On the web server, install the MyID **Web User Interface Tier** using the main MyID installation program.

When you install the web server and web service components, specify the local users you created above. Specify the local machine name with the user name; for example:

`MYSERVER01\LocalApp`

4. Set up the Windows firewall between the web and application servers to allow the following:
 - ♦ 135/TCP – RPC Endpoint Manager.
 - ♦ 5000-5099/TCP – DCOM.
 - ♦ 49152-65535/TCP – RPC for LSA, SAM, Netlogon.
5. On the application server, export the proxy MSI files for each of the MyID components.
 - a) From the Windows Component Services window, right-click the COM+ application you want to export and select Export from the pop-up menu.
 - b) In the COM+ Application Export Wizard, click **Next**, then set the following:
 - i Click **Browse** to set the path to which you want to export the MSI.
 - ii Select **Application proxy**.
 - c) Click **Next**.
 - d) Click **Finish**.
6. Copy the proxy MSI files to the web server in the separate domain and install them.

13.4.4 SQL Server clustering

Where high availability is critical, you are advised to set up SQL Server failover clustering for your MyID database server.

See your Microsoft documentation for details.

13.4.5 Restricting available workflows

You can configure the web services to prevent clients from being able to view particular workflows. This is a global setting that affects all clients, unlike configuring the roles within MyID.

You may want to do this, for example, if you have multiple web servers operating in environments with different levels of security.

For more information, contact customer support, quoting reference SUP-256.

13.5 Performance and sizing

MyID is an application that can be deployed in many different configurations dependent upon business requirements.

These deployment models include high data storage solutions (for example, where a 1 million user population is to be managed) and high usage solutions (for example, where 300,000 cardholders are self-collecting certificates concurrently).

Due to the many different ways the system can be deployed and the different systems it can be integrated with to meet a particular project's requirements, it is not possible to have a 'one size fits all' recommended deployment strategy and resultant sizing model; a 1 million user project issuing cards via a 3rd party bureau may well place less load on the web server than a 10,000 user self-service solution for example.

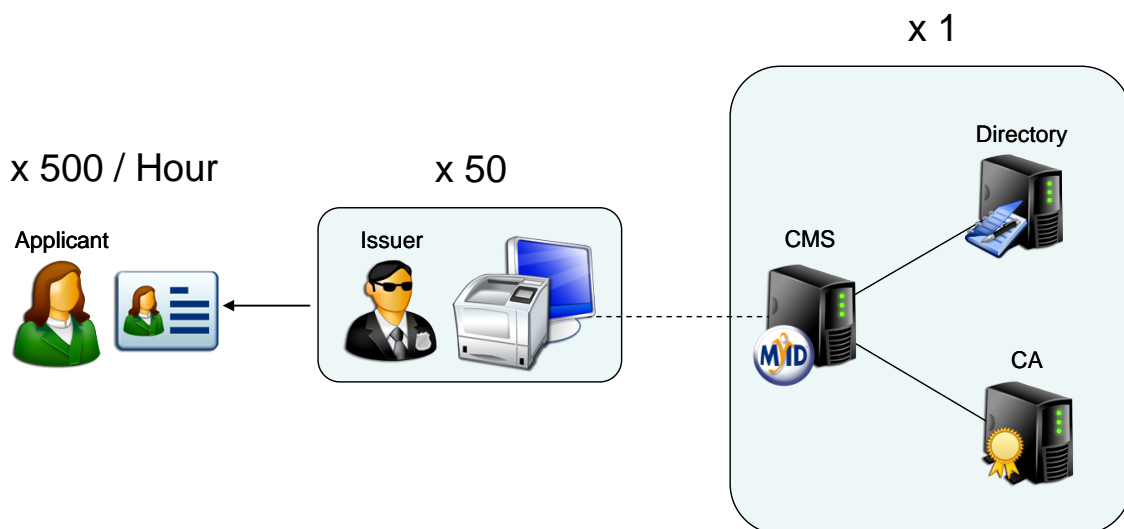
The purpose of this section is to give information on how MyID should be expected to perform under known circumstances. It is designed to act as a start point to allow partners to calculate the required number and specification of servers for a particular project.

13.5.1 Performance

Every individual action performed by an operator within MyID creates a 'session' with the server. This session is not a permanent link in that it does not hold onto resources, but a way of associating packets of data received with a particular operation (for example, issue card).

The more operations that need to occur simultaneously, the more memory and processing power is required to perform them.

The following information is based on data retrieved from a large real-world MyID installation and can be used to estimate how many concurrent operations can be managed by a single server.



In the example above a simple single tier MyID architecture (web server, application server and database all installed on the same machine) was used. MyID was connected to an Active Directory and a CA.

The use case was as follows:

- Log on to MyID with certificate on card.
- Access the issue card workflow.
- Browse to a user in the directory.
- Select a user and choose a credential profile.
- Insert a new card to issue.
- User enters PIN.
- MyID writes two certificates to the card.
- Log off.

It was found a single machine could cope with 50 operators (each connecting from a different client PC) each logging on and issuing cards concurrently. This placed a 75% processor load on the machine and was seen to give negligible performance loss over a single operator usage.

During this time each operator was issuing 10 cards per hour leading to a total of 500 cards per hour (50 operators at 10 cards per hour each) or 1,000 certificates per hour.

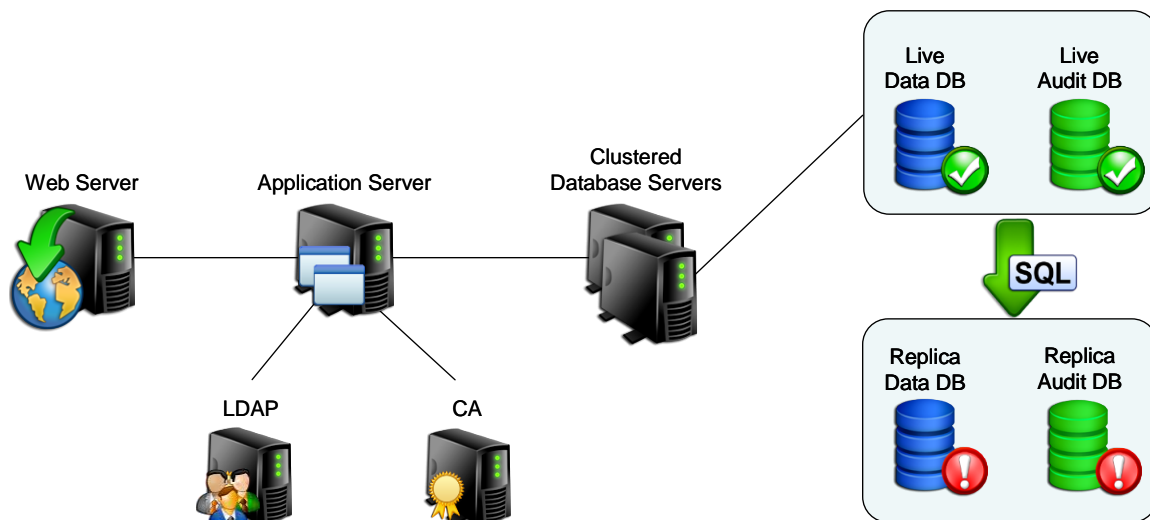
13.5.2 Sizing

Due to the capability of storing information on the form of customized attributes (that is, fields of information held against a group / device or person) and the dynamic content of those attributes it is difficult to predict the exact storage requirements of MyID.

In addition, the ability to define exactly how much information is audited and the fact that different credentials may be used per project (an archived key and certificate will require more storage than a single system wide applet for example) means the best place to calculate the exact storage requirements is from the deployed architecture itself.

In reality, an estimated sizing can be carried out in advance with this estimate being checked during a POC / pilot phase of a project (please contact Professional Services for assistance if required).

The following information is based on data retrieved from an actual installation of MyID and can be used to estimate how much data storage is typically required per user record.



In the example above Microsoft SQL Server Clustering was used to provide failover only, no load balancing was used. In addition the audit database was split out from the main operational database.

The data storage requirements can be broken down into discrete components:

- Basic configuration data and so on is approximately 2MB, as this remains static regardless of the number of users stored, this can be ignored for storage calculations.
- User records
 - ♦ A typical user record with 2 fingerprints and a facial biometric averages 56KB.

Note: If you are capturing extensive user biometric data such as 10 slap/roll prints, facial biometrics and EFT data, you require a significant amount of disk space to store this information on the database server.

For example, a fully-enrolled person with 10 slap/roll prints, EFT and facial biometrics may require over 2MB of data.
 - ♦ From MyID 10.0, image data relating to user records is stored in the MyID database. This offers greater security, performance and backup options over storing images as files on the server. However, this also increases the size of the database. This is a configurable feature, so the range of data stored can cover photographs, uploaded images and scanned documents, but can be extended to add other uploaded document types such as PDFs or Word documents.

The image stored in the database will be approximately the same size as stored on the file server.
- Each card record averages 2KB
- Each certificate record averages 13KB (CA dependent)
- Each audit record averages 2KB (variable dependent upon configuration)

Since audit information can be archived at configurable intervals, these figures are separated.

For a static deployment of 100,000 users with 100,000 cards and 200,000 certificates a storage requirements calculation would be as follows:

Note: For the purposes of this example, it is assumed that each user has 1 photograph (of 250KB) and 1 scanned document (of 250KB).

- User data = 100,000 users x 56KB = 5.34 GB
- User images and scanned documents = 100,000 users x 500KB = 48 GB

Note: The above estimate excludes any data stored outside of the database (for example, bureau export files). They also exclude the storage requirement of the database infrastructure itself (for example, transaction logs and indices).

13.6 Other considerations

13.6.1 Operating across multiple time zones

MyID can be deployed in environments where the servers and clients span time zones. The MyID database server time is treated as the definitive time source, so it is important that this is synchronized with the domain controller time, which should ideally be synchronized with a trusted time source.

Dates and times are stored in the database using UTC.

Clients connecting to MyID will operate in their own locales, but all date and time information transmitted back to the servers is first converted to UTC. Individual records (card expiry dates and so on) are converted back to local time on retrieval, but it should be noted that the audit records are always reported using the database local server time, so that consistent comparisons can be made between the data seen by the users and central administrators. Events in the **System Events** workflow are always displayed in UTC.

13.6.2 Running multi-lingual environments

MyID can operate multiple websites, each with its own translated version of the software. The MyID entry page will automatically detect the locale of the connecting browser and route the connection to the appropriate site. For details of how to configure multi-lingual sites contact customer support quoting reference SUP-138.

14 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 |
| 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 |

| ID | Name |
|-------|--------------------------------|
| 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 |
| 140 | Edit PIV Applicant |
| 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 |
| 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 |

| ID | Name |
|-------|--------------------------------------|
| 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 |
| 104 | Person Import |
| 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 |
| 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 |

| ID | Name |
|-------|----------------------------------|
| 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 |
| 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 |