



MyID

Version 10.8 Update 2

Microsoft Virtual Smart Card Integration 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 product CD.
- A `fixed width` font is used where the identification of spaces is important, including filenames, example SQL queries and any entries made directly into configuration files or the database.
- **Notes** are used to provide further information, including any prerequisites or configuration additional to the standard specifications.
For example:
Note: This issue only occurs if updating from a previous version.
- Warnings are used to indicate where failure to follow a particular instruction may result in either loss of data or the need to manually configure elements of the system.
For example:

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

Contents

1	Introduction.....	6
1.1	Glossary.....	6
1.2	Change history.....	6
2	What is a Microsoft VSC?	7
3	Deploying Microsoft VSCs.....	8
3.1	Requirements, restrictions, and limitations	8
3.2	Trusted Platform Module configuration	8
3.2.1	Preparing the TPM for use.....	8
3.2.2	Managing the TPM anti-hammering mechanism	9
3.2.3	TPM Capacity	10
3.3	Server to client communications	10
3.3.1	Client configuration and applications	11
4	Issuance and Management Processes for VSCs	13
4.1	Requesting a VSC	13
4.1.1	Policy control in MyID	13
4.1.2	Targeting a device to receive the VSC	13
4.1.3	Adding devices to MyID	13
4.1.4	Creating a VSC request for one person.....	14
4.1.5	Creating a batch of VSC requests	15
4.1.6	Requesting a VSC from an external system	15
4.2	Self-service collection of a VSC.....	15
4.2.1	Notifying the user.....	15
4.2.2	Authenticating the user	16
4.2.3	User controls.....	17
4.2.4	Checking the device identity	17
4.2.5	Creating the VSC.....	17
4.2.6	Personalizing the VSC.....	17
4.3	Notifying other systems of VSC issuance	18
4.4	Lifecycle management of a VSC.....	18
4.4.1	Logical access control	18
4.4.2	PIN management.....	18
4.4.3	Changing the VSC PIN from MyID.....	19
4.4.4	Resetting the VSC PIN from MyID.....	19
4.4.5	Remotely unlocking the VSC PIN from MyID.....	19
4.5	Updating a VSC	20
4.5.1	Changes to the certificate policies present on the VSC are required	20
4.5.2	Changes to the user information within a certificate present on the VSC are required	21
4.5.3	Certificates on the VSC are due to expire.....	21
4.6	Replacing the VSC when the device is lost/forgotten	21
4.6.1	Permanently replacing the VSC on a new device	21
4.6.2	Temporarily replacing the VSC on a new device	22
4.6.3	Re-enabling the original VSC.....	22
4.7	VSC as a backup to a physical smart card	22
4.8	Identifying a VSC by its device	23
4.9	Working with VSC certificates.....	23
4.10	Revoking the VSC	24
4.11	Removing the VSC from a device.....	24
4.12	Managing VSC access	24
4.12.1	Requesting VSC locks	24
4.12.2	Updating and canceling VSC locks.....	25
4.12.3	Setting up timezones	27
4.13	Unlocking VSC temporary access	28
5	Configuring MyID for VSC issuance.....	29
5.1	Windows services	29

5.2	Configuring MyID	29
5.3	Assigning new workflows	30
5.4	Setting up a credential profile	30
5.5	Setting up parent/child credential profiles	31
5.6	Setting the COM+ transaction timeout.....	32
5.7	VSC verification retry timeout	32
6	Troubleshooting	34
6.1	Checking the status of the TPM	34
6.2	Checking MyID Audit and System Event records	34
6.3	Reduced functionality	34
6.4	Diagnosing problems occurring during issuance	34
6.5	General troubleshooting	36
7	Known Issues.....	38

1 Introduction

This document describes the integration of MyID® with Microsoft virtual smart cards (VSCs) on trusted platform modules (TPMs) and provides guidance on deploying and managing VSCs on devices running Windows desktop operating systems.

The following operating systems are supported:

- Windows 7
- Windows 8.1 Pro
- Windows 10

1.1 Glossary

- **VSC** – Microsoft virtual smart card. A container that can hold credentials such as certificates and cryptographic keys. Stored on a *TPM*.
- **TPM** – trusted platform module. A hardware device that may be installed in a variety of computing devices. Located on a *device*.
- **Device** – a computing device (for example, desktop PC or tablet) that contains a TPM. A device contains a *TPM* which contains *VSCs*.

1.2 Change history

Version	Description
IMP1833-01	First version.
IMP1833-02	Version released with MyID 10.6.
IMP1833-03	Minor updates and corrections.
IMP1833-04	Released with 10.7.
IMP1833-05	Released with 10.7 Update 1.
IMP1833-06	Released with 10.8.
IMP1833-07	Released with 10.8 Update 1.
IMP1833-08	Released with 10.8 Update 2.

2 What is a Microsoft VSC?

A Microsoft VSC is a security feature of Windows operating systems, which uses the hardware TPM chip found in many modern computers. The TPM provides cryptographic key generation and protection that is built into the device, and, when used in conjunction with a PIN, it offers similar levels of security to a physical smart card. TPMs also feature an additional level of protection – the TPM Anti Hammering block – where repeated attempts to authenticate with an incorrect PIN will cause the device to delay further attempts to authenticate and ultimately prevent use of the VSC.

Once deployed, a Microsoft VSC can:

- Provide two factor authentication to Windows, VPN or intranet applications.
- Provide a secure container for Email signing and encryption certificates.

MyID will:

- Trigger creation of a VSC on a Windows device with a supported operating system.
 - ♦ A VSC container can be created on the device, which is then presented as a smart card.
 - ♦ Access to the VSC is restricted by creating an Administrator key for management control and setting a user PIN for authentication.
 - ♦ The TPMs key generation capabilities are used to generate cryptographic keys for use in certificate requests.
 - ♦ Certificates are written to the VSC, including injecting private keys from certificates generated on the server environment.
- Update the VSC on the device.
 - ♦ Add or remove certificates from the device as part of a credential profile change.
 - ♦ Re-issue all certificates on the VSC as part of a data re-provisioning process.
 - ♦ Recover server generated certificates to the VSC (for example, encryption certificates where the private keys are created within a hardware security module).
 - ♦ Renew certificates issued to the VSC.
- Enable the user to unlock and change the PIN on a VSC.
 - ♦ When the user PIN becomes locked or is forgotten, provide an unlock capability that is accessible only once additional authentication to MyID has taken place.
 - ♦ Facilitate a challenge/response PIN unlock mechanism in conjunction with Windows built in capabilities when the device is not able to communicate with MyID directly.
- Manage revocation of the credentials on the VSC.
 - ♦ MyID will revoke the certificates assigned to the VSC, on the certificate authority that issued them.
 - ♦ Enable an Administrator to erase the VSC when they are logged onto the device.

Some of these capabilities may vary depending on the Windows operating system in use.

3 Deploying Microsoft VSCs

There are a number of factors to be considered when preparing to deploy Microsoft VSCs in your organization, including preparation of the device to receive a VSC, the network communications to be used between your MyID server and the client device, and the business processes for issuance and lifecycle management.

3.1 Requirements, restrictions, and limitations

You can find system requirements, restrictions, and limitations when using Microsoft VSCs in the Microsoft TechNet article *Use Virtual Smart Cards*.

You can connect a maximum of ten smart cards (including both physical smart cards and VSCs) simultaneously to a PC.

3.2 Trusted Platform Module configuration

Use of VSCs requires the device to have a hardware Trusted Platform Module that complies with TPM specification 1.2 or 2.0 and has been initialized, configured and is ready for use.

Differences may exist between vendor implementations of the TPM specification – you are recommended to check the devices to be used when planning a large deployment of VSCs. Refer also to the device vendor's own instructions for managing TPMs.

3.2.1 Preparing the TPM for use

While a TPM is found in many modern devices, it may not be provided in an enabled state that is ready for use. Further information on initializing and preparing a TPM for use with VSCs can be found in the Microsoft TechNet article *Windows Trusted Platform Module Management Step-by-Step Guide*:

[https://technet.microsoft.com/en-us/library/cc749022\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc749022(v=ws.10).aspx)

For issuance of a VSC to occur, MyID will require that the TPM is Ready – specifically reporting:

- **IsReady:** `True`
- **IsEnabled:** `True`
- **IsOwned:** `True`

This information can be retrieved by running the MyID TPM Interrogator Utility, which is available with the MyID release. See the associated documentation for more information on how to use the utility.

The utility provided can also return some further information that is useful for troubleshooting problems issuing VSCs – see section 6, *Troubleshooting*.

Note: Re-imaging a device, including re-installation of the operating system, may affect the TPM status, resulting in it requiring initialization again.

Some software solutions may also affect the status of the TPM; for example, Microsoft BitLocker Administration and Monitoring functionality will escrow the OwnerAuth password for the TPM, causing the TPM to report **IsReady** as `False`.

Reduced functionality

Under some circumstances, the TPM may display a message similar to:

The TPM is ready for use, with reduced functionality.

This may occur when the TPM password is no longer known to the client PC. You must make sure that the password is stored somewhere else; for example Active Directory or BitLocker.

In this case, the status (as displayed by the TPMInterrogator utility – see section 6.1, [Checking the status of the TPM](#)) shows IsReady to be false; however, it is possible that the TPM is actually available for use, and is in the "reduced functionality" state – run `tpm.msc` to confirm.

You can configure MyID to issue VSCs when the TPM status is "reduced functionality".

To allow MyID to issue VSCs to TPMs with this status:

1. From the **Configuration** category, select **Operation Settings**.
2. Select the **Devices** tab.
3. Set the following option:
 - ♦ **Allow virtual smart card creation with TPM reduced functionality** – set to Yes.
4. Click **Save changes**.

Note: This setting is global. Any TPM that has a status of "ready" or is in a state of "reduced functionality" will be available to hold a VSC. Also, some TPMs may report different status information; these TPMs will still be unable to be issued VSCs.

If you experience any problems issuing VSCs to TPMs with reduced functionality, contact customer support quoting reference SUP-269.

3.2.2 Managing the TPM anti-hammering mechanism

The TPM anti-hammering mechanism provides extra security by limiting the number of PIN attempts that can be made when repeated failures occur. However some TPMs do not reset this count following successful authentication. This can lead to the TPM block being activated in situations when a dictionary attack is not taking place – for example one or two incorrect PIN entries only.

Additional tools can be used to reset this following successful authentication to Windows, typically using a PowerShell script that sends a command to the TPM.

Windows 8.1 introduced further configuration settings for managing when TPM lockout occurs – see the Microsoft TechNet article *Trusted Platform Module Services Group Policy Settings* at <https://technet.microsoft.com/en-us/library/jj679889.aspx>

TPM 2.0 has well-defined dictionary attack logic behavior. This is in contrast to TPM 1.2, for which the dictionary attack logic was set by the manufacturer, and the logic varied widely throughout the industry.

Key changes in TPM 2.0 with Windows 8.1 or later:

- Default of 32 failed attempts before anti hammering is hit.
- Every two hours the system is running, the amount of failed attempts is reduced by one. So after 64 hours the TPM will remember no previous failed attempts.
- If the lockout is hit, this will last for two hours, then the user will have one attempt before lockout is hit again.
- The lockout can still be reset manually by sending a reset lockout command to the TPM.

The following will be configurable through the group policy:

- Attempts before anti hammering is hit for all users and specific users.

For more information, see the *How the TPM mitigates dictionary attacks* section in the Microsoft TechNet article *TPM Fundamentals* at:

https://technet.microsoft.com/en-us/library/ff2bb100-f5c8-4270-a069-603c18df132f#BKMK_HowTPMmitigates

Note: If the password used for the anti-hammering mechanism is missing (because it is being stored elsewhere by some other software – for example, Active Directory or BitLocker) then the TPM may report that it is in "reduced functionality" mode; see the *Reduced functionality* section above.

3.2.3 TPM Capacity

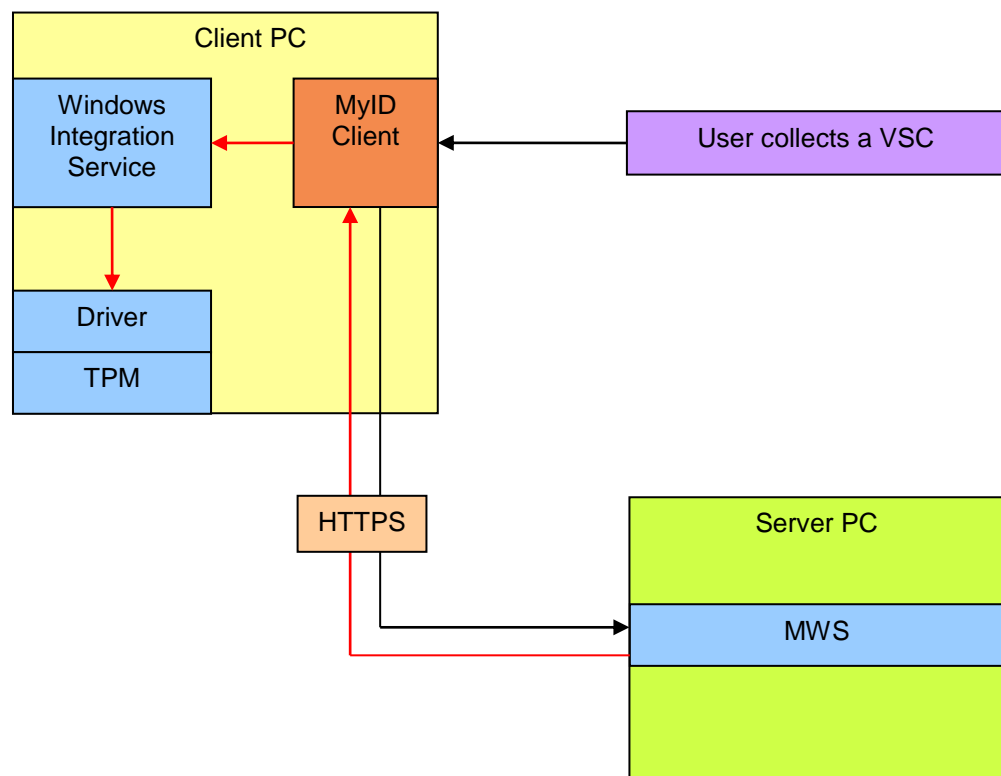
The number of VSCs that may be associated with a TPM may be different depending on the TPM in use. For example, errors may be generated by the TPM if you attempt to create more than ten VSCs on a single device. If you plan to share devices between multiple people, you are recommended to test that the maximum number of VSCs required can be supported by the TPM within your devices.

3.3 Server to client communications

The MyID server communicates with the client device to trigger Windows APIs for creating, personalizing, or erasing a VSC. This network communication takes place over SSL Encrypted connections (HTTPS).

VSC issuance uses a local Windows service running on the client device. The service checks the status of the TPM using a local WMI transaction.

The output of this transaction is stored as part of the MyID audit record to assist with troubleshooting VSC issuance failures. If use of WMI is disabled locally, the status check will show as a failure regardless of the actual state of the TPM.



3.3.1 Client configuration and applications

You can collect VSCs using the Self-Service App, which provides a simple self-service collection process for VSCs.

MyID client software is provided as .msi files; therefore you can deploy them through automated processes.

The MyID release contains the latest versions of the MyID clients and the MyID Windows Integration Service. For Windows 7, you need the MyID Middleware and TPM Software to enable support for VSCs – contact customer support quoting reference SUP-120 to acquire the software.

This table describes the software required for each operating system:

Operating System	Client Software Required	Limitations
Windows 7	MyID Middleware and TPM Software MyID Windows Integration Service Self Service App	TPM Unblock is not supported Remote Erase is not supported Card PIN has a maximum of 14 characters
Windows 8.1	MyID Windows Integration Service Self Service App	TPM Unblock is not supported Remote Erase is not supported
Windows 10	MyID Windows Integration Service Self Service App	TPM Unblock is not supported Remote Erase is not supported

Installing the MyID Windows Integration Service

The Windows service must be installed by and run under a local user account with administrative permissions on the device. Server communications are received by the client, and the signature is checked to verify the source is trusted before any access to sensitive APIs is granted.

When running the Windows service installer, you must specify a user with the correct permissions. This user must either be the Local System account, or a user with matching privileges.

You must have the following installed on your client:

- Microsoft .Net Framework 4.5.
- Microsoft Visual C++ 2010 Redistributable Package.
- For Windows 7 VSCs only, the MyID Middleware and TPM Software.
For example, TPM-5.4.885.
- The MyID Windows Integration Service.
For example, WSVC-1.3.1000.2. Make sure you have the latest version of this software package.

Note: Make sure you install the MyID Middleware and TPM Software using a user with local administrator access. The installation program may appear to continue correctly under a non-privileged account; however it is likely that the resultant installation will be incomplete and non-functional.

To install the software:

1. Install Microsoft .Net Framework 4.5.
2. Microsoft Visual C++ 2010 Redistributable Package
This *must* be installed before installing the TPM software package.
3. If you require Windows 7 VSCs, as a local administrator, run the MyID Middleware and TPM Software installer.
4. Run the MyID Windows Integration Service installer as local administrator, specifying your Local System User Account when prompted.

Note: If the installer fails to start the service, you may have provided the details for a user who does not have the correct permissions.

- **IKB-65 – Cannot install Windows Integration Service on 32-bit clients**

The MyID Windows Integration Service is currently supported on 64-bit client operating systems only.

If you need to use this method of collecting VSCs on 32-bit clients, contact customer support, quoting reference SUP-208.

4 Issuance and Management Processes for VSCs

MyID is a highly configurable credential management system, allowing you to adapt issuance and lifecycle management processes to your organization's needs. The information in this section describes the options available for issuing and managing Microsoft VSCs.

4.1 Requesting a VSC

MyID issues VSCs using a request/collect model, allowing role separation between each stage and more flexibility over the issuance process. The request creates a job, which defines the target user and (optionally) the device to receive the VSC and the credential profile to be used.

4.1.1 Policy control in MyID

Credential issuance in MyID is governed by a credential profile – this defines the lifetime and certificate policies to be provided, the PIN policy to be used, and technology types available to receive the certificates.

It can also determine the business process to be used for requesting and approving the request for credentials, and provides configuration of access control rules to the credential profile, using MyID roles.

MyID roles determine access to MyID workflows, and importantly which user accounts in MyID can receive a credential profile, and issue a credential profile.

This enables your organization's security policy to be enforced by MyID – ensuring that high security credentials can be received only by users entitled to them, and that they can be issued only by those with permissions to receive them and following appropriate approval procedures.

Critical to this is defining the roles available to a user account in MyID. These can be set manually by a MyID administrator, from an external system using the Lifecycle API, or by synchronizing Active Directory security groups to MyID. Synchronization offers the most streamlined approach, allowing access to credentials to be determined by central security policy, instead of requiring individual decisions to be made by MyID Administrators.

For more information about configuring credential profiles, see the [Administration Guide](#).

4.1.2 Targeting a device to receive the VSC

MyID allows a VSC request to be targeted at a named device. MyID uses full computer name of the device – for example `mylaptop.mydomain.com`. At collection of the VSC, the full computer name is read from the device used for collection, and compared to the pre-registered value. If the values do not match, issuance does not continue.

This feature is optional, and works best when your organization uses fixed and predictable device name values. Environments where devices will be collecting VSCs outside of your organization's IT infrastructure (therefore the full computer name may differ from the pre-registered value) are not recommended to use this feature.

4.1.3 Adding devices to MyID

You can import device records from your Active Directory at the point of requesting a VSC. MyID returns a list of PCs in the specified branch of your directory that have a full computer name and are running Windows 7 or later.

Note: The options available in this workflow depend on whether you have permission to import devices from your directory. See section 5.2, [Configuring MyID](#) for details.

Alternatively, you can add a device manually by specifying its full computer name. See the [Administration Guide](#) for details of adding and editing devices.

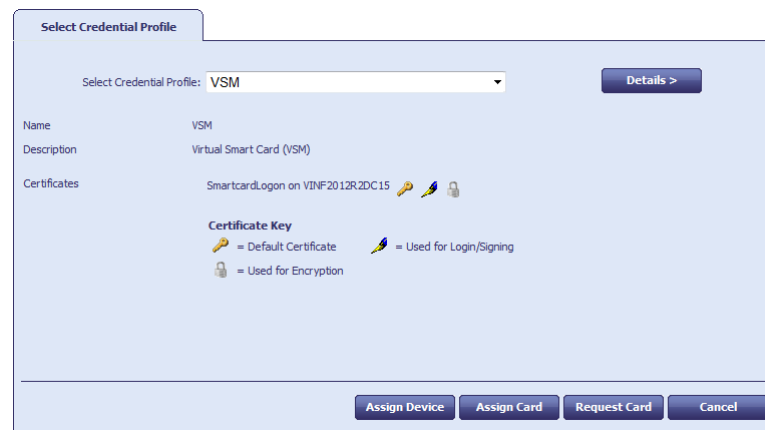
The device information can be added separately, or at the same time as making a request for credentials using the APIs available in MyID. For details, see the [Credential Web Service](#) document.

4.1.4 Creating a VSC request for one person

The Request Card workflow in MyID allows an Administrator to select a user account to receive a VSC. The user account may be retrieved from Active Directory, or from the records that already exist in MyID database. The Administrator is then instructed to choose which credential profile to issue – the choices are restricted based on the MyID roles held by the Administrator and the target user account. If required, a fixed expiry date may also be selected at this point, instead of accepting the default lifespan determined by the credential profile. Optionally, a device can be selected as the target of the VSC.

To request a VSC:

1. From the **Cards** category, select **Request Card**.
2. Use the **Find Person** stage to search for the person to whom you want to issue a card.
3. Select the person.
4. Select the credential profile you want to use from the drop-down list.



5. Do one of the following:
 - To request the card without specifying the device, click **Request Card**.
 - Click **Assign Device** to pre-allocate a specific device to which the VSC will be issued.

You can then search for the device.

If MyID is configured to allow it, you can search the LDAP directory to select a device you have not already added to the MyID database. The new device will be assigned to the VSC card request and added to the list of devices in the database.

Note: Do not select the LDAP entry for a device you have already added to the MyID database. The devices in the database are listed above the devices in the directory in the search results screen.

Note: Ignore **Assign Card** – the option is not applicable when issuing a VSC.

6. Click **Finish**.

4.1.5 Creating a batch of VSC requests

You can use the **Batch Request Card** workflow to request VSCs for multiple people in one operation. User accounts can be retrieved from MyID's database, or a connected directory using common search criteria such as MyID Group, organizational unit, or role. Customized search criteria can be added to enable more specific searches.

During the operation, all requests can optionally be targeted at a single device – for example a shared terminal or tablet in an office, or factory shop floor.

Once the request is completed, a job is created for each user selected which can be collected independently.

4.1.6 Requesting a VSC from an external system

You can also use the Credential Web Service API to request a VSC for a person. This API allows other business systems to generate requests for credentials. The inputs required include the target user account, the credential profile, and (optionally) expiry date of the certificates. You can also provide the target device within this request. Once the request has been generated, it will follow the issuance process defined by the credential profile.

For more information, see the [Credential Web Service](#) document.

4.2 Self-service collection of a VSC

As the VSC is to be created on the user's own device, it is most common for the user to collect the VSC themselves. The business process to be followed depends on a number of factors, including resources available to the end user and permitted technologies prior to receiving credentials that support two-factor authentication. The following options can be combined to provide a solution for the customer.

Note: Earlier releases of MyID allowed an administrator to collect a VSC on behalf of a user. From MyID 10.8, this capability is no longer available with MyID Desktop, and you must use the Self-Service App instead.

4.2.1 Notifying the user

- Direct notification to the end user through email.

When a request for a VSC is ready for issuance, MyID can send an email to the user to prompt them to collect their virtual smartcard. The email template can be customized to contain appropriate information for the organization and contain a hyperlink to launch the collection process.

- Windows desktop notification to the end user.

The Self-Service Application can be configured to run during the Windows logon process, or as a scheduled task. It may also be launched by a hyperlink or desktop shortcut when needed. When it is launched it will check for jobs to be processed for the current user (identified using a configurable parameter, or by picking up Windows logon credentials). When a job is retrieved, it will display a Windows desktop notification informing the user that there is a VSC to collect. Selecting this will then launch the Self-Service App to start the collection process.

For further information, see the [Self-Service App Installation and Configuration](#) document.

4.2.2 Authenticating the user

To confirm that the user who is starting the collection process is the intended owner of the credentials, an authentication stage is required before creating and personalizing the VSC.

- Integrated Windows Authentication

If user accounts have been imported to MyID from Active Directory, the simplest approach is to use the current user's Windows logon credentials to authenticate to MyID. This enables the user to start the VSC collection process without entering any additional information for authentication. MyID relies on the Kerberos credentials provided to it for authentication.

This option is available only where the user account has logged on to Windows with credentials that are trusted by the domain hosting the MyID server, and the domain and SAMAccountName of the user are stored within MyID.

- Pre-registered security phrases

MyID can enable registration of one or more security phrases for the user. These take the form of a question and response that provide information known only to the user. For example, requesting a personal set of information such as mother's maiden name, or first school attended. To ensure this information is kept private, the user can register these questions within MyID themselves, or they can be provided by an external system (for example an HR database) using the MyID Lifecycle API. All responses to security questions are stored securely within MyID to prevent them from being retrieved for malicious purposes. At collection of the VSCs, the user is presented with the security questions and prompted to provide the responses to the questions. Once verified, the collection process continues.

- Externally-generated passwords

You can also use the Lifecycle API to create new security questions and answers for users – this is useful if you do not want to store personal information such as mother's maiden name, and so on. The question and answer are under the control of the source system, not MyID.

Use the following node in the import XML:

```
/Authentication/SecurityPhrase
```

For example:

```
<SecurityPhrase>
  <Prompt>Security Password</Prompt>
  <Answer>ABC+123*xyz</Answer>
</SecurityPhrase>
```

Note: You can encrypt the answer with a transport key.

At collection of the VSCs, the user is prompted to provide the password. Once verified, the collection process continues.

For more information, see the [Lifecycle API](#) document.

- MyID-generated logon code

When a VSC request is created in MyID, a logon code can be generated by MyID and included in the notification to the customer. At collection of the VSCs, the user is prompted to provide the logon code. Once verified, the collection process continues and, once completed, the logon code cannot be reused.

For more information, see the [Administration Guide](#).

4.2.3 User controls

During collection of the VSC, the user, under normal circumstances, can navigate away from the collection process. The process can also be cancelled or closed using Windows controls. The Self-Service App can be configured to hide these controls to prevent the collection process from being incorrectly cancelled or closed.

For more information, see the [Self-Service App Installation and Configuration](#) document.

4.2.4 Checking the device identity

If the full computer name of the device has been registered as part of the request process, MyID will compare this to the value reported by the device before creating the VSC. If the value detected does not match the pre-registered value, issuance of the VSC will not continue.

4.2.5 Creating the VSC

Once authentication has completed, MyID will create the VSC on the device. This involves checking the TPM status, and if the TPM is found to be ready for issuance then creation will commence. At completion of this stage, a VSC will be available for personalization by MyID.

4.2.6 Personalizing the VSC

During this process, the VSC is available as a smart card to MyID and personalized in accordance with the credential profile.

- Changing the Administrator PIN of the VSC.
 - ♦ During the issuance process MyID will set an Administrator PIN on the VSC. This is a randomized value generated by MyID which ensures that malicious attempts to change content within the VSC is prevented.
- Setting the user PIN.
 - ♦ The PIN policy to be used is defined the credential profile in MyID. For example, the minimum and maximum PIN length can be set, and the range of permitted, or required characters. The PIN policy information is displayed to the user, with the display dynamically adjusted to show if the PIN entered meets the required policy. If your organization's PIN policy is enforced via group policy, ensure that the MyID PIN policy is configured to match it.
- Issuing certificates to the VSC.
 - ♦ To issue certificates to the VSC, MyID will instruct the TPM to generate cryptographic keys for each certificate to be issued. A certificate request will then be created and transferred to the certificate authority for issuance. Once issued, MyID will write the certificate to the device. The private keys for this certificate remain protected by the TPM.
 - ♦ MyID can also recover existing certificates for the user, and write them to the VSC. The private keys are injected to the VSC and protected by the TPM.

4.3 Notifying other systems of VSC issuance

In many situations, MyID is used as part of a wider identity management infrastructure involving a number of different systems. To enable interoperability between systems, at completion of issuance of a VSC, MyID can generate a notification message to another system (which has been configured to receive updates). This notification can be sent to an external web service or other listener, and may contain information about the VSC such as its serial number and logon name of the user account that owns it. The external system may then trigger other operations specifically for the VSC by using its serial number as an identifier.

This feature requires you to configure notifications in MyID – for more information see the [Administration Guide](#).

4.4 Lifecycle management of a VSC

Once VSCs have been deployed, consideration needs to be given to the management of the VSCs. MyID offers a range of features to assist with this.

4.4.1 Logical access control

The certificates within the VSC can be disabled, enabled or revoked. Systems that use certificates for access control or signing should check the revocation status to ensure that use of the certificate is still permitted.

MyID can change the status of the certificate in the following situations:

- The user account is disabled or enabled in MyID (including actions occurring following synchronization to a directory)
- The VSC is disabled or enabled in MyID (this can also be triggered by using the **Active credential profiles per person** configuration option in MyID).
- The VSC is cancelled in MyID.
- A request for a replacement VSC is created in MyID, causing cancellation of the original VSC.

All of these scenarios can be triggered by MyID Desktop or an external system using the Lifecycle API.

4.4.2 PIN management

It is common for users to forget, or mistype, PINs resulting in the VSC becoming unusable. The TPM anti-hammering mechanism will protect the device from dictionary attacks, by limiting the number of attempts at PIN entry when repeated attempts are made.

There are differences between how PINs are handled, and also behavior of the TPM Anti-hammering mechanism between versions of Windows operating systems, and also different manufacturers TPMs, so any organization deploying VSCs should check the devices being used and ensure that support processes are defined for each combination.

MyID's PIN locking functionality will not work as with standard smart cards. For example, this means that you cannot use lock at issuance feature.

Capability	Windows 7	Windows 8.1	Windows 10
Lock VSC PIN from Windows	Yes	Yes ¹	Yes ¹
Changing the VSC PIN from MyID	Yes	Yes	Yes
Reset VSC PIN from MyID	Yes	Yes	Yes
Remote Unlock PIN from MyID	No	Yes	Yes
Unblock TPM from MyID	No	No	No

4.4.3 Changing the VSC PIN from MyID

On a Windows device, the simplest approach to managing PIN changes is to allow the user to access the Windows built-in capability. You can access this feature using the ctrl-alt-del key combination in Windows. The original PIN must be entered and accepted before allowing the new PIN to be set.

Alternatively, MyID provides a **Reset Card PIN** workflow that you can use if the Windows feature is restricted within your environment. This will require authentication to MyID first, which can be achieved using the VSC, a separate smart card, pre-registered security questions, or Integrated Windows Logon.

4.4.4 Resetting the VSC PIN from MyID

If the user is able to log on to Windows with alternative credentials, then MyID can provide a self-service unlocking capability. Using a physical smart card, Integrated Windows Logon, an authentication code issued by MyID or a pre-registered security question, the MyID Desktop user interface can be used to unlock the VSC user PIN and set a new PIN.

This feature operates in the same way for VSCs as for physical smart cards. For further details of the **Reset PIN** workflow, see the [Administration Guide](#).

4.4.5 Remotely unlocking the VSC PIN from MyID

Where the user is not able to access Windows, a challenge response mechanism can be used to unlock the PIN of the VSC. The procedure requires the end user to be able to communicate with a helpdesk operator, who will use MyID to generate an unlock code.

The helpdesk operator will use MyID Desktop to access the **Unlock Credential** workflow. Once the user's identity is confirmed MyID will request the challenge code generated by the device holding the VSC.

The user will access the "Integrated Unblock" feature of Windows logon page, which will generate a challenge code. The user provides the challenge code to the helpdesk operator. To use this feature, the Windows group policy setting "Allow Integrated Unblock screen to be displayed at the time of logon" must be enabled.

MyID will generate a response code which is displayed in the MyID user interface. This can be entered to the user's device, which once validated on the device will allow a new PIN to be set by the user.

On Windows 7 clients, you must enable integrated unblock. See the *Smart Card Group Policy and Registry Settings* article on Microsoft TechNet – [https://technet.microsoft.com/en-us/library/ff404287\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/ff404287(v=ws.10).aspx) – for full details.

You must set the following in the **Computer Configuration\Administrative Templates\Windows Components\Smart Card** group policy:

¹ PIN lock will occur after five incorrect attempts.

- **Allow Integrated Unblock screen to be displayed at the time of login** – set to **Enabled**.
- **Display string when smart card is blocked** – set to a message you want to appear when the VSC is locked. For example, `LOCKED`.

To unlock a VSC remotely, using MyID, use the **Unlock Credential** workflow. For information on using this workflow, see the [Administration Guide](#).

4.5 Updating a VSC

Changes may be required to the certificates on the VSC following issuance, or even to the information within the certificates. The following scenarios may be encountered.

4.5.1 Changes to the certificate policies present on the VSC are required

Occasionally changes to security policy in an organization may require certificates to be added or removed from the VSC. Within MyID this would be regarded as a change to the credential profile issued to the VSC. There are a number of ways of managing updates to the VSC to reflect this change in policy:

- **Configuring the change to credential profile.**
A new credential profile can be created, or alternatively the existing credential profile is revised. This creates a new version of the credential profile.
- **Requesting updates.**
 - ♦ **Self-service request for updates.**
The user can access MyID using Desktop, which can provide access the **Request Card Update** workflow (if made available to the MyID roles that the user holds). They will be able to create a request to receive either a new credential profile or an update to the latest version of their current credential profile. Access to credential profiles is controlled by role – so the user must be permitted to request and receive the required profile.
 - ♦ **Update requests generated by an external system.**
An external system may generate update requests for the VSC, using the serial number and required credential profile as an identifier.
 - ♦ **Administrator request for update.**
Administrators may also generate a request for updating the VSC using MyID Desktop. During the process they will find the user account and select the VSC to be updated, and select the new or updated credential profile to be used.
- **Notifying the user that an update is available for self-service collection.**
Once a request for an update has been generated, there are two methods for notifying the user. Starting the MyID Self-Service App will trigger a check for jobs for the user. This can be launched in a number of ways, as described during the collection process. When an update job is available a Windows Notification is displayed, which will then start the collection process.

It is also possible for an email to be generated when the update job is created (this requires additional configuration) which can then provide instructions to the user, and a hyperlink to launch the Self-Service App.

As an alternative option, you can use MyID Desktop to collect updates to a VSC.

Note: In all cases, the original VSC must be present and user PIN entry is required before the updates are collected.

4.5.2 Changes to the user information within a certificate present on the VSC are required

User information may change over time – typically name or email address changes, or changes to organizational unit membership resulting in updates required to the distinguished name of the user. Where this occurs, the certificates on the VSC will need to be replaced with newer certificates containing the correct data.

This requires reissuance of the VSC, using the following process.

- Self Service reprovision.

Using MyID Desktop, the user can log on to MyID with their VSC, and start the **Reprovision My Card** workflow. This will then erase the content of the VSC, and reissue certificates based on the latest user data in MyID, and latest version of the credential profile. This can include changes to the available certificate policies as described in the update case. It is recommended that MyID is synchronized with Active Directory, which will ensure the latest available user information is part of the certificates. MyID will also recover any encryption certificates belonging to the user account, to the VSC as part of this process.

For devices running Windows 7, the original VSC should be revoked, and erased on the device and then reissued.

4.5.3 Certificates on the VSC are due to expire

As certificates approach expiry they will need to be replaced to enable the user to continue to authenticate, sign email, or encrypt data. MyID can provide an automated renewal process.

As certificate expiry approaches, MyID can generate a certificate renewal job. This occurs independently of the credential profile expiry so certificate lifetimes may be shorter depending on your security policy. An email notification can be generated instructing the user to collect the certificate renewal.

Alternatively, the Self-Service App can detect certificate renewal jobs for the VSC when it is started.

The collection process requires the user to enter the PIN for the VSC, and once authenticated the new certificate is issued. The previous certificate is removed, to prevent multiple windows authentication certificates from being displayed on the windows logon screen.

4.6 Replacing the VSC when the device is lost/forgotten

When the device that hosts the VSC is no longer available (for example, it is being replaced, has been lost, broken or even forgotten temporarily) a new VSC may be required. The following options are available when this situation occurs.

4.6.1 Permanently replacing the VSC on a new device

MyID provides a **Request Replacement Card** workflow that allows a current set of credentials to be replaced with a new set. It allows an administrator to locate the user, select the credentials to be replaced, and create a replacement request. It also triggers revocation or suspension of the original credentials. The actions that occur can be customized to suit specific business requirements. The revocation status of the certificates will be published to other system only when the certificate authority publishes its certificate revocation list.

The replacement request is then available for collection using the methods described previously. At collection, new certificates are issued, previously issued encryption certificates can be recovered. The expiry date of the original credentials continues to be enforced.

As an alternative to this process, the original VSC may be cancelled and a new issuance request created.

The **Request Replacement Card** workflow can also be used to replace your own VSC – the user will need to have an alternative authentication method to MyID such as a physical smart card, integrated windows authentication or a pre-registered security question.

Note: Do not attempt to collect a replacement VSC on the same device that already holds a VSC for the same user – this is likely to cause an error during collection. To replace certificates on an existing VSC, see section [4.5, Updating a VSC](#).

4.6.2 Temporarily replacing the VSC on a new device

Where the device hosting the original VSC is temporarily unavailable, MyID can issue a new VSC with a shortened lifespan on a different device. Using **Request Replacement Card**, selecting the Forgotten option will trigger suspension of the original credentials and generate a new request. A temporary version of the credential profile may be created with a shortened lifespan, which is automatically selected when the request is generated.

4.6.3 Re-enabling the original VSC

Once the temporary VSC is no longer required, the original VSC can be enabled. MyID can be configured to disable all other credentials, or a specific group of credentials when the main credential is enabled.

If required, the temporary VSC can be cancelled and removed from the device independently of the original.

4.7 VSC as a backup to a physical smart card

Many organizations have two-factor authentication using physical smart cards as a primary requirement in their security policy. Often production of a replacement takes too long, resulting in the user being unable to access resources required. VSCs are a convenient replacement in these circumstances.

A VSC can be rapidly requested and deployed, assuming the appropriate software has already been deployed to the user's device. Where VSCs are planned to be used as a backup to a physical smartcard, it is advisable to deploy them ready for use before they are required.

- Allow self-service collection, but set a complex server generated PIN.
- At issuance all required certificates are created, but will not be accessible without knowledge of the PIN.
- Use PIN unlock procedures to allow the user to change the PIN number when required.

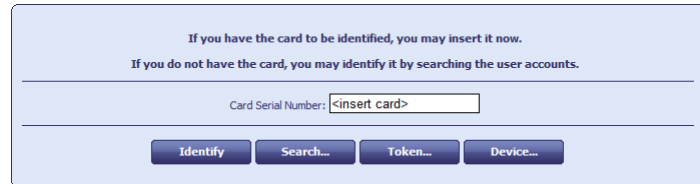
Alternatively, the backup VSC can be disabled at the point of issuance, suspending the certificates on them. They can be easily enabled using MyID, but certificate status changes may take longer to propagate through all systems to enable them to be used.

4.8 Identifying a VSC by its device

You can use the **Identify Card** workflow to display details of the VSCs stored on a device.

To identify a VSC:

1. From the **Cards** category, select **Identify Card**.

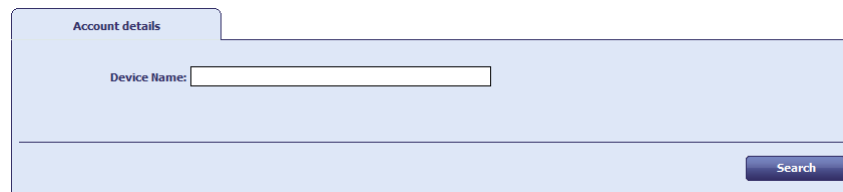


If you have the card to be identified, you may insert it now.
If you do not have the card, you may identify it by searching the user accounts.

Card Serial Number:

Identify **Search...** **Token...** **Device...**

2. Click **Device**.



Account details

Device Name:

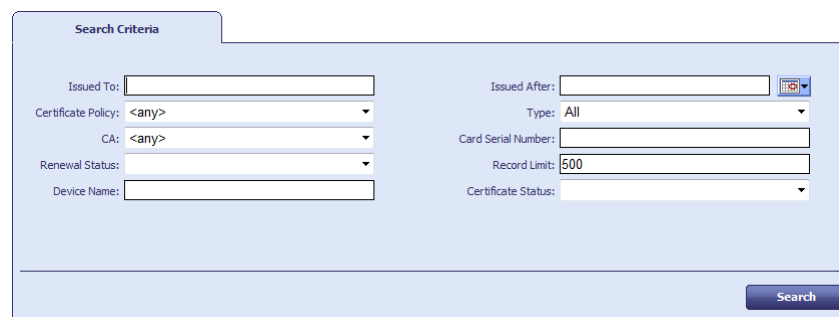
Search

3. Type all or part of the **Device Name**, then click **Search**.
MyID displays all of the VSCs issued to the devices that match your search.
4. Select a VSC to view its details.
5. Click **Back** to view a different VSC, or **Finish** to close the workflow.


4.9 Working with VSC certificates

You can specify a device when searching for certificates in the following workflows:

- **Issued Certificates**
- **Revoked Certificates**
- **Certificate Requests**



Search Criteria

Issued To: Issued After: 

Certificate Policy: Type:

CA: Card Serial Number:

Renewal Status: Record Limit:

Device Name: Certificate Status:

Search

Type all or part of the **Device Name** then click **Search** to return a list of the certificates that were issued to the matching devices.

4.10 Revoking the VSC

When the credentials provided by a VSC are no longer required, they can be revoked. This will cancel the VSC in MyID and trigger revocation of all certificates associated with it.

This can occur when:

- A user account is removed in MyID.
- A user account is disabled in MyID with permanent revocation provided as the reason.
- The VSC is cancelled.

All of these actions can be triggered by an administrator using MyID Desktop, or by an external system sending a request to the Lifecycle API.

Note: Revocation of the VSC does not automatically cause changes to the content of the VSC on the device.

4.11 Removing the VSC from a device

Once the VSC is no longer required, it can be removed from the device. When this process is triggered from MyID, the certificates associated with the VSC are also revoked on the certificate authority, and the VSC is unassigned from the user.

You can use the **Erase Card** workflow in MyID Desktop to erase a VSC that is present on the PC on which Desktop is running.

Note: You can use the **Cancel Credential** workflow to revoke a VSC even if it is not present; however, this revokes the VSC and its certificates without removing the VSC from the PC itself. To remove the VSC from the PC, you must use **Erase Card**.

You can also use the **Credential Group** and **Cancel Previously Issued Device** options on the credential profile to cancel any previously-issued VSCs from the same credential group automatically when you issue a new VSC.

When you collect a new VSC using the Self-Service App, if you have the **Erase Unused VSCs** permission for your role (as configured in the **Edit Roles** workflow), the Self-Service App will delete any previously-cancelled VSCs; for example, VSCs cancelled using **Cancel Credential** or the **Credential Group** settings.

See the [Administration Guide](#) for details of using the **Erase Card** and **Cancel Credential** workflows, and the **Credential Group** options.

4.12 Managing VSC access

You can use the **Manage VSC Access** workflow to schedule a VSC to be locked; for example, if a user is going on leave.

Lock jobs are processed on the user's PC by the Self-Service App Automation Mode. See the [Self-Service App Installation and Configuration](#) guide for details.

4.12.1 Requesting VSC locks

To request a lock:

1. From the **Cards** category, select **Manage VSC Access**.
2. Use the Find Person screen to locate the user.
3. If the user has more than one VSC, select the device you want to use.

Lock Jobs for this Device

Device Details

Device Owner Logon Name: 100005
Expiry Date: Fri Dec 2 16:26:55 UTC 2016
DNS: GBWKS0601-764
Credential Profile:
Associated Credential Profile: New Profile

There are currently no lock jobs pending for the selected device.

Request PIN Lock

Further Details

Select an item from below to see further job information.

	Requested Date	Requested By	Status	Job Process Date
<input type="radio"/>	Tue Dec 8 15:40:36 UTC 2015	startup	Cancelled	Thu Dec 17 14:00:00 UTC 2015
<input type="radio"/>	Tue Dec 8 15:17:57 UTC 2015	startup	Cancelled	Tue Jan 12 07:00:00 UTC 2016
<input type="radio"/>	Tue Dec 8 13:13:38 UTC 2015	startup	Cancelled	Thu Dec 31 08:00:00 UTC 2015

Finish

The screen lists the history of lock requests.

A **Status** of **Awaiting Issue** means that the job is active; a **Status** of **Cancelled** means that the job is not active.

You can have only one lock job active at once. If you already have a lock job, you can update or cancel it; see section [4.12.2, Updating and canceling VSC locks](#).

- To request a lock, click **Request PIN Lock**.
- Specify when you want the lock to be processed.

Select one of the following:

- ♦ **Next Self Service App Run** – the lock is processed the next time the Self-Service App runs.
- ♦ **Specific Date and Time** – select the **Timezone**, **Date**, and **Time** you want the lock to be processed. The next time the Self-Service App runs *after* this time, the VSC will be locked.

You can configure the list of timezones. See section [4.12.3, Setting up timezones](#) for details.

- Type a reason for the lock request.
- Click **Request PIN Lock**.

4.12.2 Updating and canceling VSC locks

To update or cancel a lock:

- From the **Cards** category, select **Manage VSC Access**.
- Use the Find Person screen to locate the user.
- If the user has more than one VSC, select the device you want to use.

Lock Jobs for this Device

Device Details
Device Owner Logon Name: 100005
Expiry Date: Fri Dec 2 16:26:55 UTC 2016
DNS: GBWKS0601-764
Credential Profile:
Associated Credential Profile: New Profile

There is currently a pending lock job for the selected device.
Expected PIN Lock: Thu Dec 17 14:00:00 UTC 2015

Cancel PIN Lock

Update PIN Lock

Further Details
Select an item from below to see further job information.

	Requested Date	Requested By	Status	Job Process Date
<input type="radio"/>	Tue Dec 8 15:40:36 UTC 2015	startup	Awaiting Issue	Thu Dec 17 14:00:00 UTC 2015
<input type="radio"/>	Tue Dec 8 15:17:57 UTC 2015	startup	Cancelled	Tue Jan 12 07:00:00 UTC 2016
<input type="radio"/>	Tue Dec 8 13:13:38 UTC 2015	startup	Cancelled	Thu Dec 31 08:00:00 UTC 2015

Finish

If you have a current lock job, you can cancel or update it; if you do not have a current lock job, you can request a new one; see section [4.12.1, Requesting VSC locks](#).

4. Select one of the following:
 - ♦ **Cancel PIN Lock** – the lock request is canceled.
 - ♦ **Update PIN Lock** – you can select a different date and time for the lock job to be processed.
5. Click **Finish**.

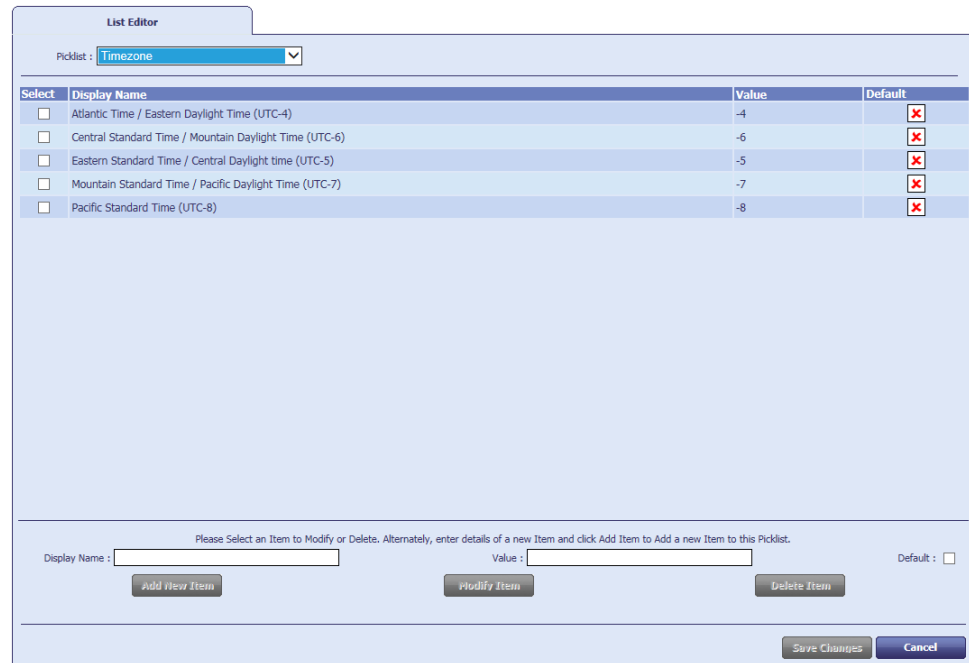
Note: The **Job Management** workflow does not list the jobs created by this workflow. You must use the **Manage VSC Access** workflow for all actions related to these jobs.

4.12.3 Setting up timezones

You can use the MyID **List Editor** workflow to set up the timezones that you use in the **Manage VSC Access** workflow.

To edit the list of timezones:

1. From the **Configuration** category, select **List Editor**.
2. From the **Picklist** drop-down list, select **Timezone**.



Select	Display Name	Value	Default
<input type="checkbox"/>	Atlantic Time / Eastern Daylight Time (UTC-4)	-4	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Central Standard Time / Mountain Daylight Time (UTC-6)	-6	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Eastern Standard Time / Central Daylight time (UTC-5)	-5	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Mountain Standard Time / Pacific Daylight Time (UTC-7)	-7	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Pacific Standard Time (UTC-8)	-8	<input checked="" type="checkbox"/>

Please Select an Item to Modify or Delete. Alternately, enter details of a new Item and click Add Item to Add a new Item to this Picklist.

Display Name : Value : Default : ☐

The **Display Name** is listed in the **Manage VSC Access** workflow. The **Value** is the time difference in hours between the timezone and UTC.

3. To add a new timezone, type a **Display Name** and **Value**, then click **Add New Item**.

To edit a timezone, select the entry, update the **Display Name** and **Value**, then click **Modify Item**.

To delete a timezone, select the entry, then click **Delete Item**.

Note: You cannot use the same **Value** for multiple items. If you want to use different names for the same timezone (for example, Mountain Standard Time and Pacific Daylight Time), as a workaround you can add .0 to the value; for example, -7 and -7.0 are treated as different items, but refer to the same number of hours for the offset from UTC.

4. Click **Save Changes**.

4.13 Unlocking VSC temporary access

You can use the **Unlock VSC Temporary Access** workflow to unlock a VSC; you can specify the length of time that you want the VSC to remain unlocked. This allows you to grant temporary access to the VSC; for example, as an emergency credential to allow access to a laptop when the user's physical smart card is lost or damaged.

To allow you to provide emergency access in this way, you are recommended to issue a VSC and lock it after you have issued the user with their primary smart card.

The procedure is started by the end user, who calls the helpdesk when Windows reports that the VSC is locked.

To unlock a VSC for temporary access:

1. From the **Cards** category, select **Unlock VSC Temporary Access**.
2. Use the Find Person screen to locate the user.
3. If the user has more than one VSC, select the device you want to unlock.

4. From the **How long should the VSC be unlocked for?** drop-down list, select the length of time for which you want to unlock the VSC.

You can select **Unrestricted access**, which means the VSC will be unlocked permanently, or a time from eight hours to one week.

5. Type a reason for unlocking the VSC.
6. Type the **Challenge Code** provided by the user.
7. Click **Generate**.

MyID displays a **Response Code**. Read this code out to the user, who can use it to unlock their VSC.

8. Click **Finish**.
9. You are prompted to check that the VSC has unlocked correctly; if it has not (for example, if the user has provided the wrong challenge code or mistyped the response code), you can click **No** to attempt the unlocking again.

Note: The **Job Management** workflow does not list the jobs created by this workflow. You must use the **Manage VSC Access** workflow for all actions related to these jobs.

5 Configuring MyID for VSC issuance

5.1 Windows services

To collect a VSC, the client PC must have the following Windows services available or running:

Windows	Service Name	Start Type	Must be running?
Windows 7	Smart Card	Automatic	Y
	Certificate Propagation	Automatic	Y
Windows 8.1/10	Smart Card	Automatic	N – triggered start
	Certificate Propagation	Automatic	N – triggered start
	Device Install Service	Manual	N – triggered start

For Windows 7 PCs, the services must be running before you attempt to collect a VSC. For Windows 8.1 and Windows 10, the services must be available, but will be started automatically when required.

5.2 Configuring MyID

To enable device and VSC support within MyID:

1. From the **Configuration** category, select the **Operation Settings** workflow.
2. Click the **Devices** tab.

Set the following options:

- ♦ **Allow device management from the MyID user interface**

Default: No.

Set to **Yes** to allow devices to be used within MyID. Device-specific features (such as a **Device** option on search screens that allows you to specify the device you are searching for) are displayed.

Set to **No** to hide the device features within MyID.

- ♦ **Legacy virtual smart card fallback**

For Windows 7, to support creating VSCs using the TPM-5.1.x client, set this option to **Yes**.

- ♦ **Microsoft virtual smart cards supported within MyID**

Default: No.

Set to **Yes** to allow VSCs to be used within MyID.

Set to **No** to hide the VSC features within MyID.

Note: If you set this option to **No**, you must:

- Use the **Job Management** workflow to remove any existing jobs for VSCs.
- Use the **Credential Profiles** workflow to modify your credential profiles to remove the **Microsoft Virtual Smart Card** option.

3. To enable devices to be retrieved from Active Directory, click the **LDAP** tab.

Note: You must have configured a connection to Active Directory using the **Directory Management** workflow.

Set the following options:

- ♦ **Allow LDAP Search for devices during card requests**

Default: **No**.

Set to **Yes** to allow an operator to add a device from the LDAP directory into the MyID database when requesting credentials.

Set the **No** to prevent an operator from adding a device when requesting credentials. The operator may still be able to add a device using the **Add Devices** workflow.

- ♦ **Allow LDAP Search for Devices during Add Devices**

Default: **No**.

Set to **Yes** to allow an operator to add a device from the LDAP directory into the MyID database using the **Add Device** workflow.

Set to **No** to prevent an operator from adding a device using the **Add Device** workflow. The operator may still be able to add a device when requesting a VSC.

4. Click **Save changes**.

5.3 Assigning new workflows

To work with devices in MyID, the following workflows need to be added to appropriate roles.

- **Add Devices** – allows you to add a device to the MyID database. You can either import the device from your LDAP directory or add the device directly.
- **Edit Devices** – allows you to set devices as active or inactive. You cannot request a VSC for an inactive device.

These workflows are not assigned to any roles by default. Use the **Edit Roles** workflow to assign these workflows to the roles of the users you want to be able to use them.

5.4 Setting up a credential profile

Before you can issue a VSC, you must set up an appropriate credential profile within MyID.

Note: You cannot use the **Validate cancellation** option on VSC credential profiles.

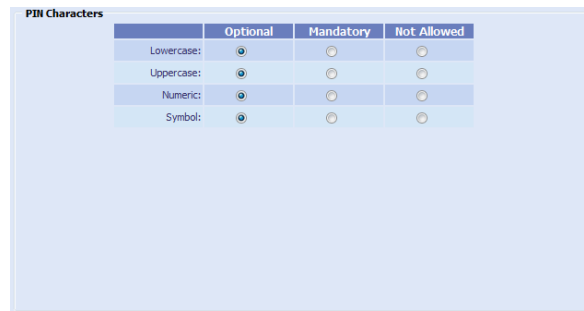
Do not specify a data model for a Microsoft VSC; VSCs do not contain the required data structures.

See the *Managing Credential Profiles* section of the [Administration Guide](#) for general instructions. Specific information for VSCs is given below:

1. In **Card Encoding**, select **Microsoft virtual smart card**.

If you select other options in **Card Encoding** you may experience issues when collecting credentials; you are recommended to set up a credential profile that contains only **Microsoft virtual smart card** in the **Card Encoding** section.

2. In **PIN Characters**, select the options for the PIN used for VSCs.



	Optional	Mandatory	Not Allowed
Lowercase:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Uppercase:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Numeric:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Symbol:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

You can determine whether uppercase letters, lowercase letters, numbers or symbols may be included (**Optional**), must be included (**Mandatory**) or cannot be included (**Not Allowed**).

3. In **Device Profiles**, set the **Card Format** to **None**.

VSCs do not support container for biometrics and so on.

4. Click **Next**.

5. Select the certificates you want to use.

Do not specify any containers for the certificates.

Note: If you want to use a certificate for Integrated Windows Logon, make sure it has 2048-bit keys.

6. Click **Next**.

7. Select the roles you want to be able to issue the VSCs and the roles for which you want to request them. Click **Next**.

8. Card layouts are not relevant for VSCs. Select card layouts only if you are going to be use the same credential profile for VSCs and for printed cards. Click **Next**.

9. Add your comments in the box provided, then click **Next** to create the credential profile.

5.5 Setting up parent/child credential profiles

You can set a credential profile to be a *parent* credential profile; this is then available to be selected as the parent for one or more *child* credential profiles. Child credential profiles can be used only for VSCs.

If you issue a user a VSC using a child credential profile, they can use the VSC until they are issued a credential using the parent credential profile; at this point, MyID creates a job that will lock the child VSC.

This is used, for example, in the situation where your users are issued VSCs only until they are issued more permanent smart card credentials.

Note: You cannot delete a credential profile if it has been marked as the parent of another credential profile.

To enable this feature, set the **Allow parent and child credential profiles** option (on the **Issuance Processes** tab of the **Operation Settings** workflow) to **Yes**.

To set up parent and child credential profiles:

1. From the **Configuration** category, select **Credential Profiles**.
2. Create a new credential profile, or edit an existing credential profile.
3. In the **Issuance Settings** section, set the following:
 - ♦ To set the credential profile as a parent, select the **Is Parent Profile** option.

- ♦ To set the credential profile as a child, from the **Parent Credential Profile** drop-down list, select the parent profile you want to use.

Note: For child credential profiles, you must have **Microsoft Virtual Smart Card** selected as one of the card encoding options.

4. Click **Next** and complete the workflow.

5.6 Setting the COM+ transaction timeout

As some VSC operations may take a significant amount of time to complete, you may want to increase the COM+ transaction timeout on the MyID application server; this prevents errors such as the root transaction error from occurring.

To increase the transaction timeout:

1. From the Windows **Start** menu, click **Programs > Administrative Tools > 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.
6. For example, set the transaction timeout to 900.
7. Click **OK**.
8. Expand **My Computer** and select **COM+ Applications**.
9. Right-click **Edefice_BOL** and select **Properties** from the pop-up menu.
10. Click the **Advanced** tab.
11. Set the **Enable idle shutdown** value to 15.
12. Click **OK**.

5.7 VSC verification retry timeout

For Windows 7 VSCs, during the VSC creation processes, the TPM Software on the client machine prepares device installation, key generation on the TPM and other system configuration necessary for installing a new virtual reader device. This process can often take a few minutes to complete.

It is sometimes the case that a newly created VSC has been successfully created, but the client machine has taken some time to initialize the device fully, possibly due to the machine being under high load. MyID must therefore verify that the device has become ready before further issuance of the device can take place. This is achieved by querying the client for the existence of the new device.

By default MyID waits for up to a minute for the VSC device to become ready. After this point, MyID will assume installation has failed, attempt to remove the device, and subsequently fail the VSC collection.

If this timeout is not long enough (see the error in section [6, Troubleshooting](#)), you can change the timeout:

1. In MyID, from the **Configuration** category, select **Operation Settings**.
2. Click the **Devices** tab.
3. Set the following options:
 - ♦ **MyID virtual smart card detection retry interval**
Default: 10.

The interval, in seconds, at which MyID checks if the operation to create the VSC has completed. To prevent an overly-long period before detecting the completion of VSC generation, the interval is restricted to a maximum of 20 seconds.
 - ♦ **MyID virtual smart card detection retry attempts**
Default: 6.

The number of checks for the completion of VSC generation. The total time allowed for the VSC generation completion (retry interval * retry attempts) is restricted to a maximum of 480 seconds.
4. Click **Save changes**.

6 Troubleshooting

6.1 Checking the status of the TPM

The TPMInterrogator utility is provided with the MyID software; this utility interrogates the TPM and provides information about its current status.

Instructions are provided in the documentation supplied with the utility. This will report the status of the flags that determine the status of the TPM.

The most important flags to be checked are:

- IsReady: True
Note: Not supported in Windows 7.
- IsEnabled: True
- IsOwned: True

If any of these flags return false, it indicates the TPM will not be able to receive VSC. (But see also the information on "reduced functionality" in section [3.2.1, Preparing the TPM for use](#).)

Additional flags are also reported by this utility, but interpretation of these flags is more complex. If you continue to receive errors when issuing VSCs, and these flags are set correctly, include the information provided by the utility in support requests to Intercede.

6.2 Checking MyID Audit and System Event records

During issuance of a VSC, MyID will record information about the process within the Audit trail. This will include details of the TPM status checks made, and the status of actions taken during the issuance process.

Information about a specific issuance process can be found by searching the audit using the device's full computer name as search criteria, in the 'Extended Details' search field.

6.3 Reduced functionality

If you have enabled the **Allow virtual smart card creation with TPM reduced functionality** configuration option, MyID will attempt to issue VSCs to TPMs with a status of "reduced functionality". See section [3.2.1, Preparing the TPM for use](#) for details.

If you experience any problems issuing or managing VSCs on TPMs with this status, or if TPMs are reporting different statuses in the MyID Audit trail, contact customer support quoting reference SUP-269.

6.4 Diagnosing problems occurring during issuance

- **MyID has not been configured to issue VSCs**

If MyID has not been configured to issue VSCs, you may see an error.

In MyID Desktop, the error is:

```
The system is not configured to issue Microsoft Virtual Smart Cards.
This job cannot be collected.
```

In the Self-Service App, the error is:

```
Virtual Smart Card issuance is not allowed. Issuance cannot
continue.
```

▪ Root Transaction Error

If you see an error similar to the following

```
<ErrorCode>-2147164158</ErrorCode>
```

```
<Message>The root transaction wanted to commit, but transaction
aborted (Exception from HRESULT: 0x8004E002)</Message>
```

This error may be caused by a timeout issue. As a workaround, you can increase the COM timeouts. See section [5.6, *Setting the COM+ transaction timeout*](#) for details.

▪ Error caused by witnessing

If you see an error similar to the following:

```
You do not have permissions to witness this operation
```

when cancelling a VSC, this is caused by having the **Validate cancelation** option set in the credential profile. Currently, you cannot use a credential profile for VSCs if it has the **Validate cancelation** option set. See section [5.4, *Setting up a credential profile*](#), for details of setting up a credential profile for VSCs.

▪ Error caused by incorrect Active Directory schema or insufficient privileges

If a client group policy is set to backup the TPM to Active Directory but the Active Directory schema is incorrect or the client does not have permissions to manipulate its own record, you may see the following error.

```
<Error> <number>-2147467259</number> <description>TPM not ready
0x00044000 ----- Exception raised in function:
Tpm::Check::Exists In file .\Check.cpp at line 64 </description>
</Error><TPM>0</TPM>
```

To give the client permission to manipulate its own Active Directory record:

- a) In the Active Directory Users & Computers console, select the appropriate domain and find the Windows 8.1 client under the **Computers** node.
- b) Open the properties dialog for the client machine and click the **Security** tab.
- c) Under **Group or user names**, select SELF.
- d) Under **Permissions for SELF**, select **Full control**.

To correct the Active Directory schema, see the *Schema Extensions for Windows Server 2008 R2 to support AD DS backup of TPM information from Windows 8 clients* article on Microsoft TechNet.

• The client does not have the MyID Middleware and TPM Software installed

If you do not have the MyID Middleware and TPM Software installed on the client, you may see an error similar to the following:

```
No service provider found
```

For a Windows 7 client, this may be caused by the following reasons:

- ♦ The MyID Middleware and TPM Software is not installed. Check that the prerequisite patch specified in the MyID Windows Integration Service readme file is installed.
- ♦ The Microsoft KB2533623 update has not been installed. Download and install the update if it is not installed.

▪ Windows 7 VSC collection errors

A number of different errors may occur due to incorrect set up of the MyID system during VSC collection or deletion. The table below documents typical MyID application server errors and tips for resolving them.

Error	Typical cause	Resolution tips
Provider call failed: CreateCard(); TPM_VSCR_CREATE_FAILED	The card creation process failed, most likely due to incorrectly configured TPM ownership on the client.	Ensure that the TPM is active and owned by a user on the current operating system.

If the issue cannot be resolved, or further error and trace information is required, contact Intercede customer support for assistance.

▪ Removing Windows 7 VSCs left behind by aborted issuance

If you click the **Abort** button on the Confirm Details screen when collecting a VSC, or the issuance fails for some other reason, the VSC is created on your device but is not known to MyID. This means you cannot use MyID to manage or delete the VSC. For more information, contact customer support, quoting reference SUP-192.

▪ Removing Windows 8.1 VSCs left behind by aborted issuance

If you click the **Abort** button on the Confirm Details screen when collecting a VSC, or the issuance fails for some other reason, the VSC is created on your device but is not known to MyID. This means you cannot use MyID to manage or delete the VSC. You must remove the VSC drivers to remove the partially-issued VSC. For more information, contact customer support, quoting reference SUP-192.

▪ MyID Desktop stopped at "Request waiting to be processed" stage after locally generating a VSC

MyID may stop responding at the "Request waiting to be processed" stage after generating a Microsoft VSC locally for a variety of reasons:

- ♦ The server may have failed to read the serial number from the VSC even though the client has generated the VSC. This has been observed to occur due to the client returning before the card has been fully configured. MyID will attempt to retry this operation. For more information contact customer support, quoting reference SUP-205.
- ♦ The eJobServer service may not be running. Check that the service is running correctly on the MyID application server.
- ♦ Make sure that MyID is not configured for random SOPINs when the SOPIN type is set to Factory – on the **Device Security** tab of the **Security Settings** workflow, check the **Security Office PIN Type** and **Require Random Security Office PIN** options.

6.5 General troubleshooting

• A VSC is not shown on the Windows logon screen or the MyID select card screen

If you are cannot see your issued VSC when you try to log into Windows or into MyID, there is likely to be a driver issue.

As a workaround, try restarting your PC or disabling and re-enabling the Virtual Smartcard reader.

- **TPM fails to recover on waking up device from sleep mode**

On some devices, the TPM module does not recover after the device has been woken up from sleep state. This issue has been observed particularly on devices using STM 1.2 TPM. When the TPM is in this state, an unexpected error may be reported for any operation requiring TPM access; for example, creating, deleting, or authenticating with a VSC.

If an unexpected error is reported during a VSC operation, check the state of the TPM by running `tpm.msc` (with elevated privilege) to verify that the TPM is available. Restart the device if the TPM is not available.

- **Authenticating with the Windows Integration Service**

If you see an error similar to the following:

```
Failed to authenticate with service
```

this means that the Windows Integration Service could not authenticate the application that is attempting to communicate with the service. The Windows Integration Service must be able to authenticate the application's digital signature before accepting a request. For more information, contact customer support quoting reference SUP-260.

- **VSC issuance fails with TPM error code 54**

This error may occur if the TPM module supports Legacy FIPS and not WIN8 FIPS. Dell Latitude Exx40 laptops with STM TPM modules are known to be configured with such TPM modules, and this issue has also been seen with ATMEL TPM modules. This configuration setting is built into the TPM module in the TPM system manufacturing process and cannot be changed.

Generation of a Microsoft VSC supports only TPMs that are configured for WIN8 FIPS; you cannot use devices in which the TPM module is configured for Legacy FIPS.

- **Intermittent error when recovering a certificate to a Microsoft Virtual Smart Card**

You may see an intermittent error when recovering an archived certificate to a Microsoft Virtual Smart Card on Windows 10. This is due to an issue within the Microsoft operating system that prevents some certificates from being imported to the TPM.

The issue was reported to Microsoft, and has been resolved in Windows 10 Anniversary update. The required minimum Windows 10 version is Build14352.

7 Known Issues

▪ IKB-47 – Removing Windows VSCs left behind by aborted issuance

If you click the **Abort** button on the Confirm Details screen when collecting a VSC, or the issuance fails for some other reason, the VSC is created on your device but is not known to MyID. This means you cannot use MyID to manage or delete the VSC.

To correct this for Windows 8.1 and 10:

- ♦ Open **Device Manager**.
- ♦ Find the correct reader for your card in Smart Card Readers.
You can find this by the reader reference when viewing this in **Erase Card**.
- ♦ Right-click, then from the pop-up menu click **Uninstall**.
- ♦ Confirm the uninstallation of drivers and so on.

To correct this for Windows 7:

- ♦ Open a Windows command prompt as an administrator.
- ♦ Run the `tpmcfg.exe` utility provided with the MyID Middleware and TPM Software package.
This lists the readers and VSCs on the machine, including serial numbers.
- ♦ Match the serial number or Reader ID to select the entry to remove.
- ♦ Type `Y` to delete a reader/VSC.
- ♦ Type the number of the Reader Index.
This deletes the reader/VSC.
- ♦ Type `N` to create and change PIN.
- ♦ If you need to delete more than one reader/VSC, repeat as necessary.