intercede

MyiD CMS

MyID Enterprise
Version 12.10

Password Change Tool

Copyright

© 2001-2024 Intercede Limited. All rights reserved.

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

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

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

Licenses and Trademarks

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

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

Apache log4net

Copyright 2004-2021 The Apache Software Foundation

This product includes software developed at

The Apache Software Foundation (https://www.apache.org/).

Conventions used in this document

- Lists:

    - Numbered lists are used to show the steps involved in completing a task when the order is important.

    - Bulleted lists are used when the order is unimportant or to show alternatives.

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

    For example:

    - Record a valid email address in **'From' email address**.

    - Select **Save** from the **File** menu.

- *Italic* is used for emphasis:

    For example:

    - Copy the file *before* starting the installation.

    - Do *not* remove the files before you have backed them up.

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

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

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

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

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

    For example:

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

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

    For example:

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

Contents

1 Introduction

This document contains information on the MyID Password Change Tool (PCT).

The Password Change Tool (PCT) is a support tool for automating the changing of passwords used by MyID. You are recommended to use it if MyID is already installed and you are required to change passwords regularly by your security policy, or if a security breach has occurred.

For each user specified, it will:

- Change the password of all affected MyID Windows services.
- Change the password of all affected MyID COM+ Applications in Component Services.
- Change the password of all affected MyID IIS app pools.
- Change the password of all affected MyID IIS sites using anonymous authentication.
- Change the password of Active Directory service users (optional).
- Change the password for SQL secure authentication (optional).
- Display a color-coded summary.
- Generate a log file.

Note: The PCT is not responsible for validating that the new passwords supplied are secure.

1.1 Installing the utility

The utility is provided in the `Support Tools\Password Change Tool\` folder in the MyID release. See the readme provided with the release for details of installing the utility.

2 Usage

To start PCT, hold the Shift key and right-click the `PasswordChangeTool.exe` file and select **Run as different user**. Enter domain administrator credentials to start the tool. If you do not intend to change Active Directory passwords, you can select **Run as administrator** and enter local administrator credentials instead.

If you are changing the MyID COM+ user, you must run the PCT as a user who has the ability to set permissions for SQL Server users on the MyID database.

Note: Tool-tips are available on the form.

By default, the PCT log file is saved in the same directory as the executable; however, you can update the `Log.config` file in the tool folder to give it a different file path.

To change the log file path, edit the value of the `file` parameter:

```
<file value="PasswordChangeTool.log" />
```

The recommended and fastest method of updating all MyID passwords using the PCT is as follows:

On the MyID application server:

1. Start PCT.

2. Carry out section *2.1*, *Working with Active Directory accounts* to simulate and perform setting the AD password and MyID password for the MyID COM+ user.

3. Carry out section *2.1*, *Working with Active Directory accounts* to simulate and perform setting the AD password and MyID password for the IIS user.

4. Carry out section *2.1*, *Working with Active Directory accounts* to simulate and perform setting the AD password and MyID password for the Web Services user.

5. If you are using SQL authentication, carry out section *2.2*, *Working with SQL accounts* to simulate and perform setting the SQL password for the SQL secure authentication user.

6. Exit PCT.

Important: If you are changing the password for the Web Services user, you must make the change on the application server *before* you make the change on the web server or web services server.

If your system has multiple web servers, or if the web services are installed on a separate server to the website, you must update all web servers and web services servers.

On the MyID web server or web services server:

1. Start PCT.

2. Carry out section *2.1*, *Working with Active Directory accounts* to simulate and perform setting the MyID password for the IIS user.

3. Carry out section *2.1*, *Working with Active Directory accounts* to simulate and perform setting the MyID password for the Web Services user.
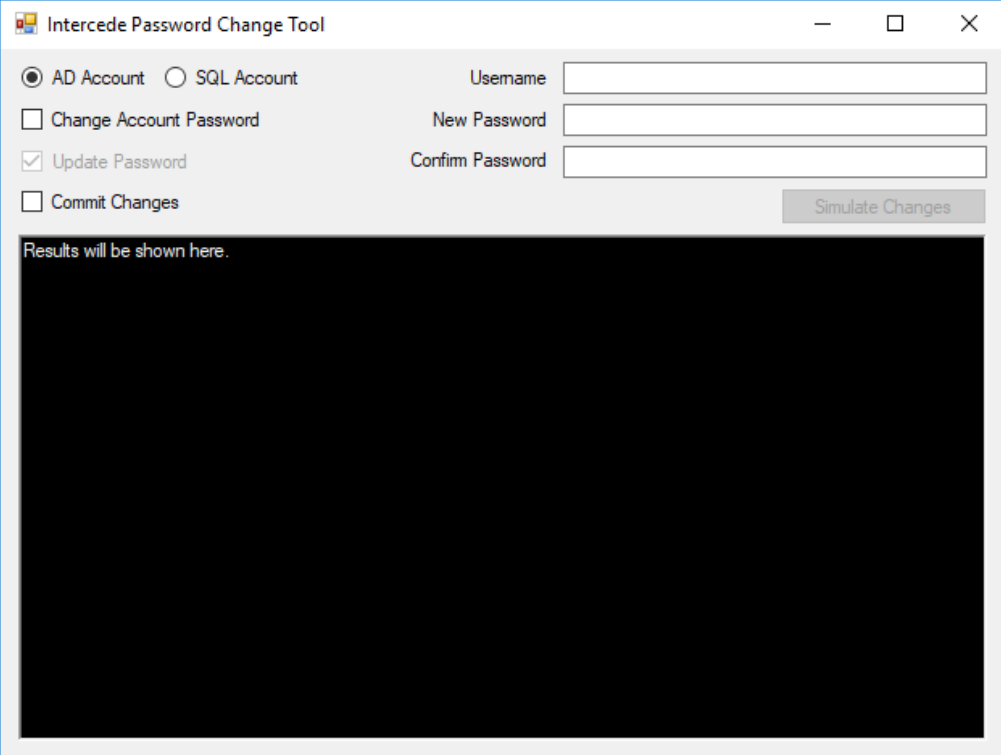
4. Exit PCT.

This password change process changes the following:

	MyID COM+ User	IIS User	Web Service User	SQL secure authentication user
Active Directory on Domain Controller	MyID COM+ User	IIS User	Web Service User	n/a

Windows services on Application Server	`AMAGPACSConnector`
	`eCertificate Services Server`
	`eJobServer`
	`eKeyServer`
	`eMessageServer`
	`MyID Expiring Items: App`
	`MyID Notifications Service`
	`MyID SNMP Agent`
		n/a	n/a	n/a

Windows services on Web Services Server	n/a	`MyID Expiring Items:Web`	`MyID Expiring Items:Mws`	n/a

COM objects on Application Server	`APDUCardServer`
	`EAudit`
	`Edefice_BOL`
	`Edefice_CS`
	`Edefice_DAL`
	`Entrust_Admin`
	`ExpiringItems`
	`ImportProcessor`
	`MyID SNMP Agent`
	`MyIDSCEPHandler`
	`eCS`
	`eEventLog`
	`eExternalDataSource`
	`ePKIConfig`
		n/a	n/a	n/a

	MyID COM+ User	**IIS User**	**Web Service User**	**SQL secure authentication user**

IIS application pools on Web Server	n/a	`MyIDPoolClassic`	`CredentialWebServicePool`
			
			`DeviceManagementAPIPool`
			
			`MyIDiOSOTAPool`
			
			`MyIDWebService`
			
			`SCEPPool`
				n/a

IIS sites on Web Server	n/a	`MyID`
		`MyIDDataSource`
		`MyIDProcessDriver`
		`MyID/en`
		`MyID/us`
		`upimages`
			`MyIDSCEP`	n/a

SQL secure authentication	n/a	n/a	n/a	`Dal4Net`
				`web.oauth2`
				`web.oauth2.ext`
				`InternalWS`
				`ExternalWS`

2.1 Working with Active Directory accounts

1. Ensure **AD Account** is selected.

2. If you want to change the password on the Active Directory at the same time, select the **Change Account Password** option.

   Note: The user under which you are running the PCT must have the appropriate permissions for this to be successful.

   If you have already changed the password on the Active Directory, and just want to update the MyID components and services to use the new password, make sure that **Change Account Password** is *not* selected.

3. Type the **Username** and the **New Password** for the user, then type the password again in the **Confirm Password** field.

   For usernames, you can enter either the fully-qualified user name of the user in either the format `domain\user`, or `user@domain` – if you enter username on its own without specifying the domain, the domain of the currently logged on user is used.

4. Ensure the **Commit Changes** option is not selected.

5. Click **Simulate Changes**.

   The PCT checks the user details with the Active Directory service. The PCT abandons the change at this point if either the **Username** cannot be found or the specified **Password** is incorrect. In any of these cases, the PCT makes no changes to your system.

6. Verify that no errors (shown in red) are displayed. All the actions that would have been performed are shown in green.

   Note: Confirm that all of the proposed password changes are acceptable before continuing.

7. Select the **Commit Changes** option.

   This changes the **Simulate Changes** button to **Commit Changes**.

   Note: Log out of MyID on all clients before proceeding.

8. Click **Commit Changes**.

   The PCT makes all the changes to your system.

   Any Windows services are automatically restarted as part of the update and all affected IIS application pools will be recycled.

   Note: If you have configured an IIS client certificate, the Password Change Tool does not update the stored password; you must set this manually. See the *Configuring IIS client certificates* section in the ***Securing Websites and Web Services*** guide for details.

9. Verify that there are no errors shown.

10. If you have changed the password for MyID COM+ account, restart the MyID COM+ running processes:

    a. On the MyID application server, open the **Component Services** tool.

    b. Expand **Component Services > Computers > My Computer > Running Processes**.

    c. For each MyID component in the list, right-click and select **Shut down**.

       The MyID components will restart when needed.

       You can determine which components belong to MyID by viewing the **COM+ Applications** folder – the MyID components run under the MyID COM+ user account.

2.2 Working with SQL accounts

This option applies only if you selected the SQL authentication option when installing MyID. You must run the PCT on the MyID application server to update the SQL authentication account password.

Note: You must first change the SQL account password on the SQL Server. The PCT cannot change the password on the SQL Server – it just updates MyID to use the new password.

1. Make sure there are no active connections to the SQL Server using the account for which you are updating the password. Use the `KILL` statement to terminate any user sessions.

2. Log on as the MyID COM+ user and use **Run as administrator** to launch the Password Change Tool.

   The user must have permissions to change the MyID `Dal4Net.dll.config` file, and the `appsettings.json` file for the following web services:

   • web.oauth2

   • web.oauth2.ext

- InternalWS (for mobile authentication)
- ExternalWS (for mobile authentication)

3. Ensure SQL Account is selected.

4. Type the **Username** and the **New Password** for the SQL account you are using, then type the password again in the **Confirm Password** field.

5. Ensure the **Commit Changes** option is not selected.

6. Click **Simulate Changes**.

   The PCT checks the user details exist in the following configuration file:

   `C:\Program Files\Intercede\MyID\Components\Dal4Net\Dal4Net.dll.config`

   The PCT abandons the change at this point if the configuration file cannot be found, the system is configured to use Windows Authentication and not SQL Authentication, the **Username** cannot be found, or the specified **Password** is incorrect. In any of these cases, the PCT makes no changes to your system.

7. Verify that no errors (shown in red) are displayed. All the actions that would have been performed are shown in green.

   Note: Confirm that all of the proposed password changes are acceptable before continuing.

8. Select the **Commit Changes** option.

   This changes the **Simulate Changes** button to **Commit Changes**.

   Note: Log out of MyID on all clients before proceeding.

9. Click **Commit Changes**.

   The PCT makes all the changes to your system.

10. Verify that there are no errors shown.

Important: In previous versions of MyID, to change the password used for the web.oauth2 or web.oauth2 web services, you edited the `appsettings.Production.json` override file for each of the web services. The Password Change Tool does not change this override file, but updates the main `appsettings.json` file for the web services. You must check that you do not have a `ConnectionStrings` section in the `appsettings.Production.json` file; delete this section so that it does not override the password provided in the `appsettings.json` file. Alternatively, if you want to continue using the override file, you can use the Password Change Tool to update the `appsettings.json` file, then copy the updated `PasswordDPAPI` parameter value into the `appsettings.Production.json` file

3 Command-line arguments

You can run PCT from the `Password Change Tool` subfolder in various ways to suit your system, depending on command-line arguments supplied from an administrative command prompt or Windows shortcut.

Examples of the syntax are:

- Interactively in a GUI window (default):

  `PasswordChangeTool.exe`

- Interactively in a GUI window, with defaults:

  `PasswordChangeTool.exe /g /a=UpdateAdPassword /u="<Username>" /p="<NewPassword>"`

- Non-interactively in a console window:

  `PasswordChangeTool.exe /a=UpdateAdPassword /u="<Username>" /p="<NewPassword>"`

- Show help in a console window:

  `PasswordChangeTool.exe /?`

The following table contains a list of the command-line arguments supported by PCT:

Argument	Purpose
`/?`	Show the command line arguments help.
`/g`	Show the GUI. Any other commands become the default values in the GUI, but the tool will not execute the specified action; instead, you must click **Simulate Changes** or **Commit Changes**.
`/c`	**Commit Changes** (if not specified, the tool will simulate changes only).
`/a=Action(s)`	Mandatory. Specify the action to perform. Valid actions are: `ChangeAdAccountPassword` – change the user password in Active Directory and update MyID to use the new password. `UpdateAdPassword` – update MyID to use the new password. `UpdateSqlPassword` – update MyID to use the new SQL account password. **Note:** If you specify `ChangeAdAccountPassword`, you do not need to select `UpdateAdPassword` – the PCT updates the password in MyID automatically,

Argument	Purpose

`/u="Username"`	Mandatory.
	
	Specify the **Username**.
	
	You can use one of the following formats:
	
	`user`
	
	`domain\user`
	
	`user@domain`
	
	If no domain is specified, the tool uses the domain of the currently logged-on user.

`/p="Password"`	Mandatory. Specify in plain text the new password of the account being changed. You are recommended to surround long and complex passwords with quote characters to avoid the Windows error from a long command line: `"The system cannot find the file specified."` This means that the password cannot contain quote characters.
`/ss="Password"`	Required if you are changing the SQL Authentication password. Specify in plain text the password for the MyID Web Service User.
`/sa="Password"`	Required if you are changing the SQL Authentication password. Specify in plain text the password for the MyID Authentication User.

4 Troubleshooting

If you see a popup window asking for a smart card or virtual smart card, this is caused by entering user details that are invalid for the directory – Windows is attempting to find an alternative means of authentication. Cancel the popup window, enter the correct details for the user, and try again.

If the PCT returns an exception, unusual results, or fails to run:

- Ensure the operating system is supported.

- Ensure the PCT version is compatible with your MyID installation.

- Ensure the PCT is started with the correct credentials.

- Contact customer support, quoting reference SUP-261.

4.1 Known issues

- **IKB-262 – Restarting Windows services**

  After you have used the Password Change Tool, you may need to restart some Windows services for the changes to take effect. The services affected are:

  - MyID Notifications Service

  - MyID SNMP Agent

  These services run under the MyID COM+ account on the application server.