MyID MFA and PSM

Offline Password Breach Database Guide

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

Document reference: IMP2049-04

July 2025

Copyright

Conventions used in this document

- Lists:
  - Numbered lists are used to show the steps involved in completing a task when the order is important.
  - Bulleted lists are used when the order is unimportant or to show alternatives.
- **Bold** is used for menu items and for labels.

  For example:
  - Record a valid email address in **'From' email address**.
  - Select **Save** from the **File** menu.
- *Italic* is used for emphasis:

  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

Note: MyID MFA and MyID PSM were previously known as Authlogics products. Authlogics is now an Intercede Group company and the products have been rebranded accordingly. The term 'Authlogics' may still appear in certain areas of the product.

Intercede has the following versions of its Password Breach Database:

- Offline Password Breach Database (Min)

  This is the minimum offline database. It is included by default with MyID Authentication Server and contains the top one million breached passwords.

  This is infrequently updated.

- Offline Password Breach Database (Full)

  This is the full offline database. It is a separate download containing over 8 billion breached passwords.

  This is infrequently updated. This is a snapshot of the Cloud Password Breach Database. As it is infrequently updated, it does not contain the most recent entries.

- Cloud Password Breach Database

  An Internet hosted database containing over 8 billion breached credentials.

  This is regularly updated.

The MyID Authentication Server includes an Offline Password Breach Database of the top one million most often breached passwords. This can reduce the reliance on Cloud Password Breach lookups. If a password is not found in the Offline Password Breach Database then, unless disabled by policy, the MyID Cloud Password Breach Database is also checked.

A full Offline Password Breach Database containing the eight billion breached passwords is available as a separate add-on download from the Intercede website:

www.intercede.com/support/downloads/

When you have the full database installed, it may be acceptable to disable Cloud Password Breach Database lookups.

Note: The MyID Cloud Password Breach Database is regularly updated, whereas the Offline Password Breach Database is not. Unless a fully offline solution is required, you are still recommended to leave Cloud Password Breach Database lookups enabled to ensure that the most recent entries are being checked.

1.1 Prerequisites

The Offline Password Breach Database requires a server that is already running the Authentication Server 4.0.1740.0 or higher. If the Authentication Server is not installed, the Offline Password Breach Database installer cannot complete the setup.

The Offline Password Breach Database requires approximately 20GB of disk space.

1.2 Database performance

The Offline Password Breach Database is a custom format designed to be highly efficient at password hash matching. It does not require a database engine such as SQL as the database access logic is built directly into the MyID Authentication Server.

1.3 Change history

Version	Description
IMP2049-01	Reformatted and released with MyID MFA and PSM version 5.0.7.
IMP2049-02	Released with the latest version of the Offline Password Breach Database.
IMP2049-03	Updated installation information.
IMP2049-04	Added information about installing the offline password breach database to a shared location.

2 Deploying the Offline Password Breach Database

The following deployment overview walks through the installation process for deploying the full Offline Password Breach Database.

When you install the full Offline Password Breach Database, the MyID Authentication Server automatically uses it instead of the built-in Offline Password Breach Database that contains only one million entries.

If you uninstall the full Offline Password Breach Database, the MyID Authentication Server automatically reverts to the built-in Offline Password Breach Database containing only one million entries, if installed.

To deploy the Offline Password Breach Database:

1. Install the MyID Authentication Server on a Windows server.

   See the *MyID Authentication Server Installation and Configuration Guide* for details.

2. Install the Offline Password Breach Database.

   See section *2.1*, *Installing the Offline Password Breach Database*.

If you no longer want the Offline Password Breach Database, you can uninstall it. See section *2.2*, *Uninstalling the Offline Password Breach Database*.

2.1 Installing the Offline Password Breach Database

The Offline Password Breach Database is an add-on to the MyID Authentication Server, which you must set up before you install the Offline Password Breach Database.

Note: This section of the installation process requires Local Administrator rights on the server.

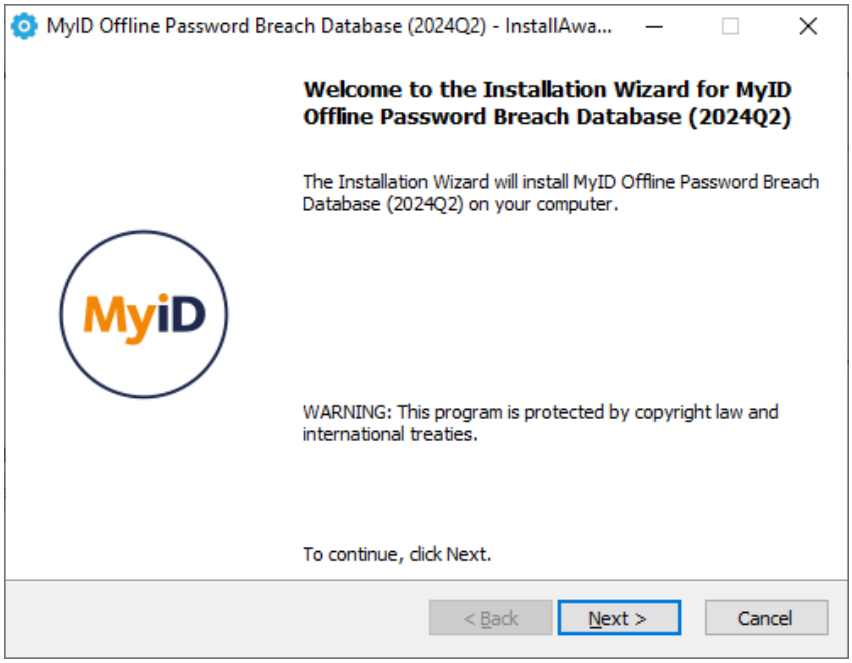
To install the Offline Password Breach Database:

1. Download the following files:
   - `MyIDOfflinePasswordBreachDatabaseXXXXXX.exe` – the MyID Offline Password Breach database installer.
   - `breachdatabaseXXXX.7zip` – the password breach database.
   - `stemsdatabaseXXXX.7zip` – the password stems database.

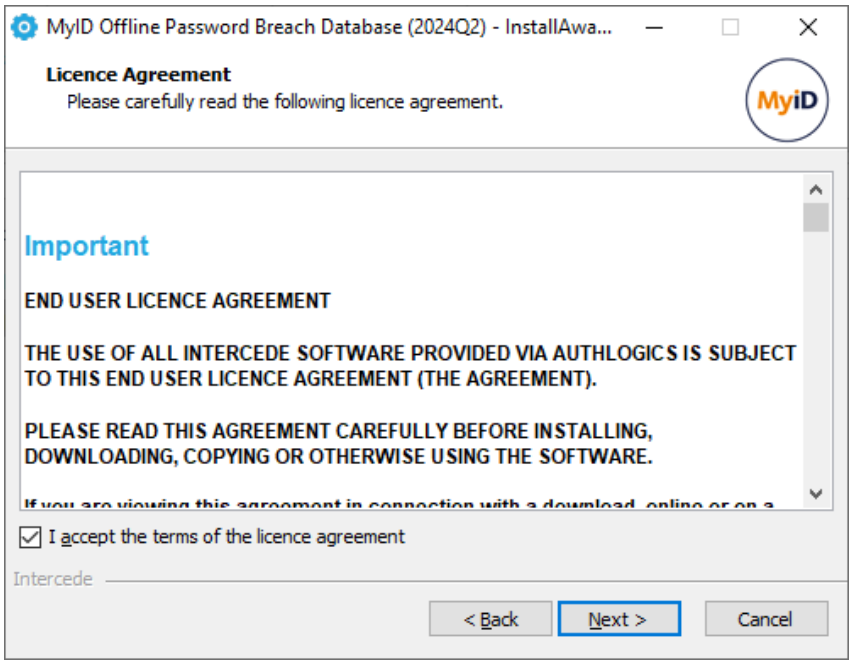
   Links to the password breach database files are available on request.
2. Copy the files to the same folder on a PC on which the MyID Authentication Server is installed and set up.

   Alternatively, you can install the database to a shared location that multiple authentication servers can use; see section *2.1.1*, *Installing the Offline Password Breach Database to a shared location*.
3. Run the installation program:

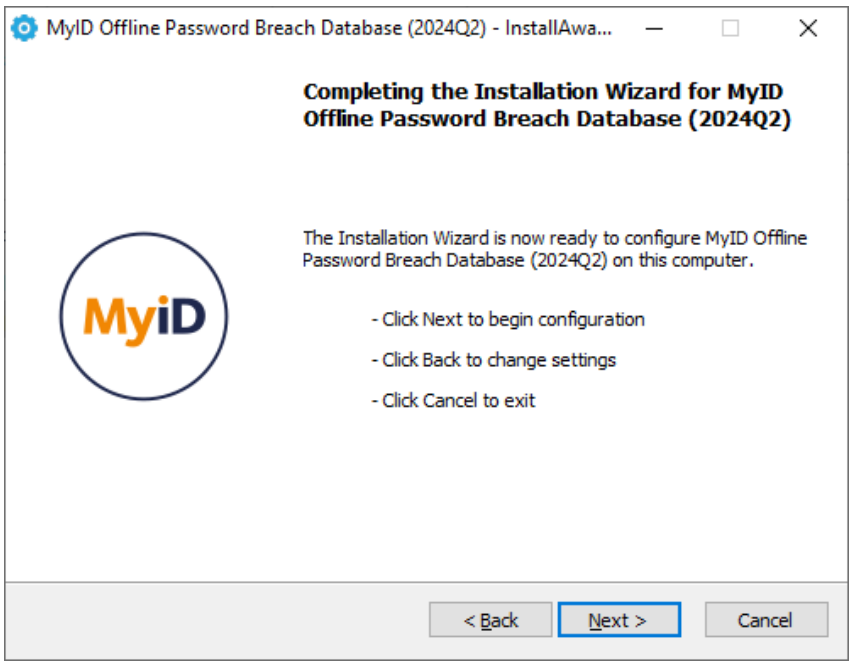
   `MyIDOfflinePasswordBreachDatabaseXXXXXX.exe`



4. Click **Next** to continue.

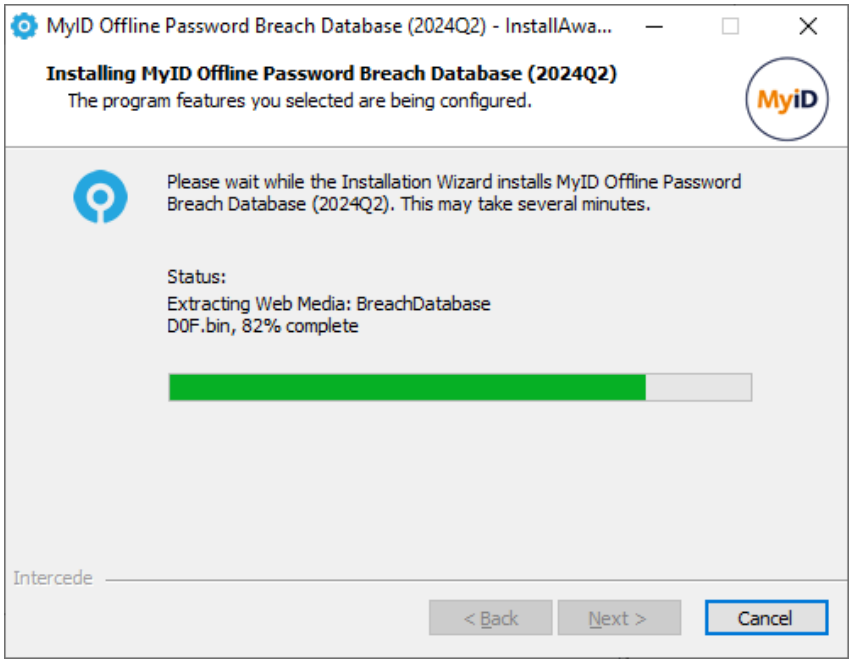


5. Review the license agreement, then click **Next** to continue.

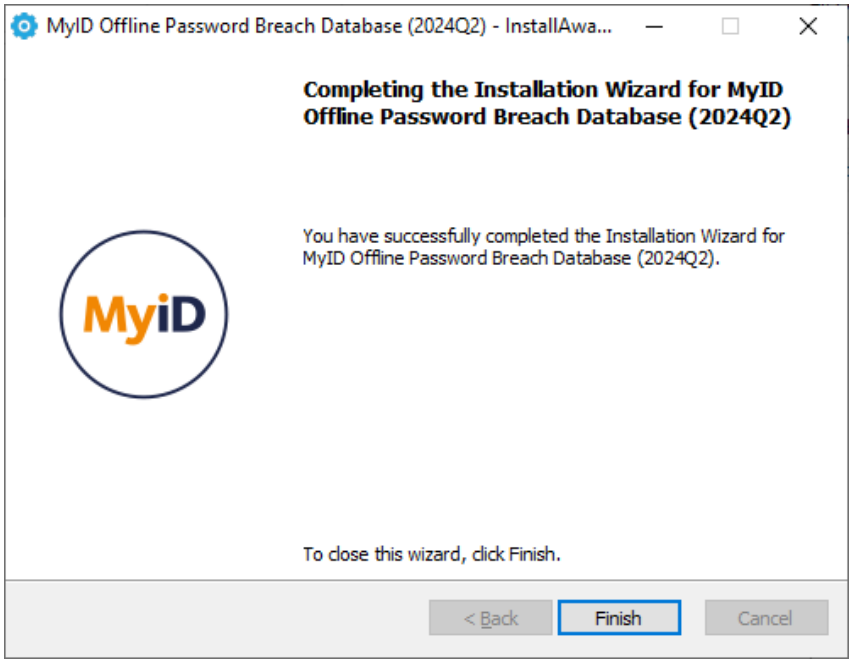


6. Click **Next** to start the installation.

   The installer carries out the installation.



7. Click **Finish** to complete the installation process.



2.1.1 Installing the Offline Password Breach Database to a shared location

If you have multiple authentication servers, you may want to install the Offline Password Breach Database to a shared location rather than duplicating the database on each authentication server.

To install the Offline Password Breach Database to a shared location:

1. Install the Offline Password Breach Database to a single server.

   Follow the instructions in section *2.1*, *Installing the Offline Password Breach Database* above. You can install the database on one of your authentication servers or on a file server.

2. Move the database from its installed location to a location that is accessible from all of your authentication servers.

   By default, the database is installed to the following location:

   `C:\Program Files\Authlogics Authentication Server\Breach Database\`

   Move the entire `Breach Database` folder to the shared location.

   Note: The shared location must be on a server that is on the same domain as the authentication server.

3. If the shared location is not already a network share, create a share for the `Breach Database` folder.

4. On each authentication server, make sure that there is no existing `Breach Database` folder.

   If necessary, delete the folder from its installed location on the authentication server:

   `C:\Program Files\Authlogics Authentication Server\Breach Database\`

5. On each authentication server, run the following command:

   ```
   mklink /d "<local folder>" <network share>
   ```

   where:

   - `<local folder>` – the location where the authentication server looks for the database. By default, this is:

     `C:\Program Files\Authlogics Authentication Server\Breach Database`

     If you have installed the authentication server to a different location, adjust this path accordingly.

   - `<network share>` – the network share where you have moved the shared database.

     Note: You must use a network share; you cannot use a mapped drive.

   For example:

   ```
   mklink /d "C:\Program Files\Authlogics Authentication Server\Breach Database" \\fileServer\BreachDatabase
   ```

   This creates a directory symbolic link so that when the authentication server looks for the database, it is redirected to the shared location.

2.2 Uninstalling the Offline Password Breach Database

If you no longer require the Offline Password Breach Database on a server, you can remove it by performing an uninstallation from **Control Panel > Programs > Programs and Features**: