Offline Breach Database Guide

Fully offline breach database add-on

Product Version: 4.2.1030.0

Publication date: February 2023

Call us on: +44 1344 568 900 (UK/EMEA)
+1 408 706 2866 (US)

Email us: sales@authlogics.com

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organisations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organisation, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user.

Authlogics may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written licence agreement from Authlogics, the furnishing of this document does not give you any licence to these patents, trademarks, copyrights, or other intellectual property.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

The information contained in this document represents the current view of Authlogics on the issues discussed as of the date of publication. Because Authlogics must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Authlogics, and Authlogics cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. AUTHLOGICS MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS Document.

Copyright © 2023 Authlogics. All rights reserved.

Table of Contents

Introduction 3
Prerequisites 3
Database Performace 3
Deployment 4
Overview 4
Installing Authlogics Offline Password Breach Database 4
Uninstalling Authlogics Offline Password Breach Database 6

Introduction

Authlogics has 3 versions of its Password Breach Database:

(1) Offline Password Breach Database (Min)
- Included with Authlogics Authentication Server containing the top 1 million breached passwords.
- Infrequently updated.

(2) Offline Password Breach Database (Full)
- Separate download containing over 2 billion breached passwords.
- Infrequently updated.

(3) Cloud Password Breach Database
- An Internet hosted database containing over 5 billion breached credentials.
- Regularly updated.

The Authlogics Authentication Server includes an Offline Password Breach Database of the top 1 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 Authlogics Cloud Password Breach Database will also be checked.

A full Offline Password Breach Database containing over 2 billion breached passwords is available as a separate addon download from https://authlogics.com/downloads/. When the full database is installed it may be acceptable to disable Cloud Password Breach Database lookups.

Note

The Authlogics Cloud Password Breach Database is regularly updated whereas the Offline Password Breach Database is not. Unless a fully offline solution is required Authlogics still recommends leaving Cloud Password Breach Database lookups enabled to ensure that the most recent entries are being checked.

Prerequisites

The Offline Password Breach Database can only be installed onto a server that is already running the Authlogics Authentication Server 4.0.1740.0 or higher. If the Authentication Server is not installed then the Offline Password Breach Database installer will not complete the setup.

The Offline Password Breach Database requires approximately 6Gb of disk space.

Database Performace

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 Authlogics Authentication Server.

Deployment

The following deployment overview walks through the installation process for deploying Authlogics.

When the Authlogics Offline Password Breach Database is installed the Authlogics Authentication Server will automatically us it instead of the built in Offline Password Breach Database containing only 1 million entries. If the Offline Password Breach Database is uninstlled then the Authlogics Authentication Server will automatically revert to the build in Offline Password Breach Database containing only 1 million entries, if installed.

Overview

To fully deploy the Authlogics Offline Password Breach Database:

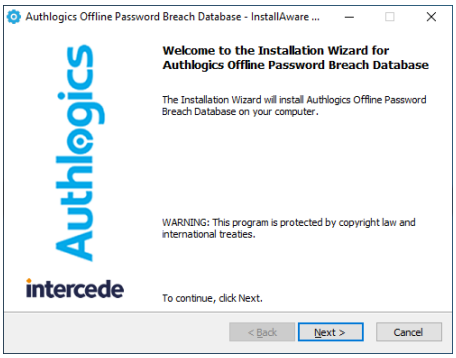
(1) Install the Authentication Server on a Windows Server.
(2) Install Authlogics Offline Password Breach Database.

Installing Authlogics Offline Password Breach Database

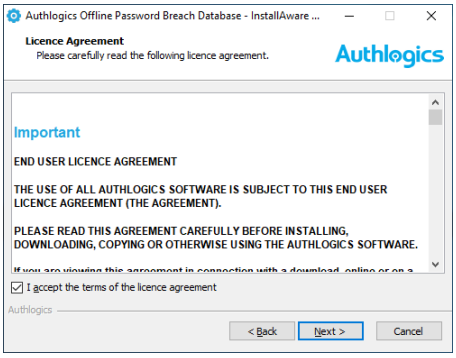
The Authlogics Offline Password Breach Database is an add-on to the Authlogics Authentication Server which must be set up first.

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

(1) To start the Authlogics Offline Password Breach Database installation, run the *Authlogics Offline Password Breach Database xxxxx.exe* installer.

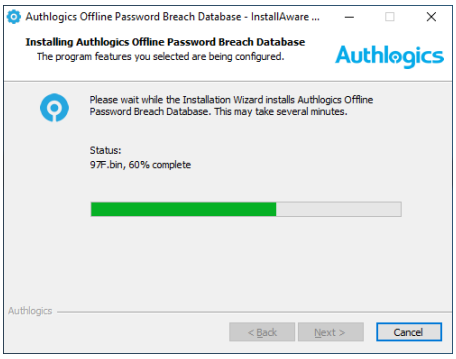


(2) Click *Next* to continue.



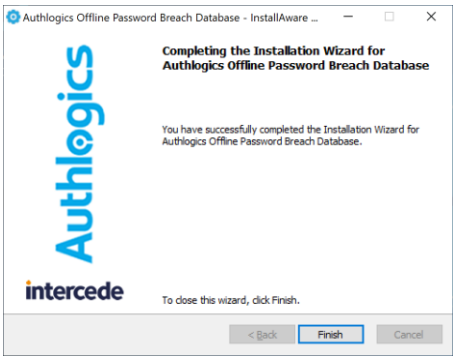
(3) Click *Next* to continue.

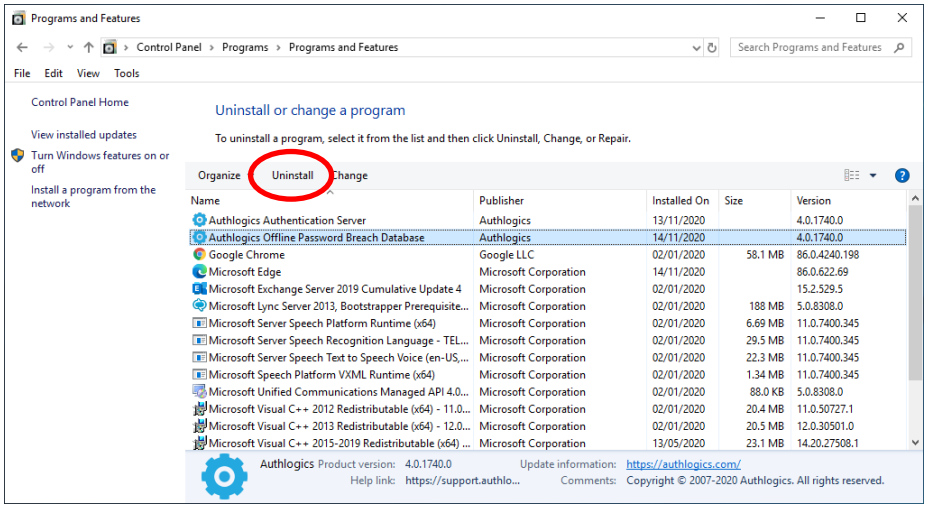
(4) Click *Next* to continue.



The installation is being performed.

(5) Click *Finish* to complete the installation process.



Uninstalling Authlogics Offline Password Breach Database

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