# DoubleClue KeePass Plugin

## Content

**Version 2.7.1**

# 1. Introduction

The DoubleClue KeePass Plugin stores and retrieves '.kdbx-files' in/from DoubleClue CloudSafe, a high security cloud protecting data with multi-factor authentication (MFA).  Push Approval, a user friendly and high secure MFA method, is available via the DoubleClue App, which can be downloaded from App Store or Google PlayStore. Alongside it, DoubleClue supports 7 further authentication methods like QR-Code Scans, FIDO or SMS.

By storing KeePass files in CloudSafe, DoubleClue users can manage them through the DoubleClue App or by logging into DoubleClue UserPortal. In UserPortal, they can further share the files with other DoubleClue users and manage them together.

The DoubleClue KeePass Plugin can be downloaded at https://doubleclue.com/files/DoubleClueKeePassPlugin.zip.

It is available in English and German.

Users can create a free DoubleClue account at https://doubleclue.online.

There is also an enterprise version of DoubleClue available for companies, who want to install DoubleClue on premises or use it as a service in the cloud. For more information about it, please contact sales@doubleclue.com.

Features:

- Access to KeePass files is protected by Multi-Factor Authentication (MFA)
- The encrypted KeePass files are additionally encrypted and stored in DoubleClue CloudSafe
- KeePass files are never stored on any devices
- Users can manage their KeePass files by using the plugin, DoubleClue PasswordSafe in UserPortal or the DoubleClue App

Requirements:

- Installation of *KeePass Password Safe 2.4.1* and higher
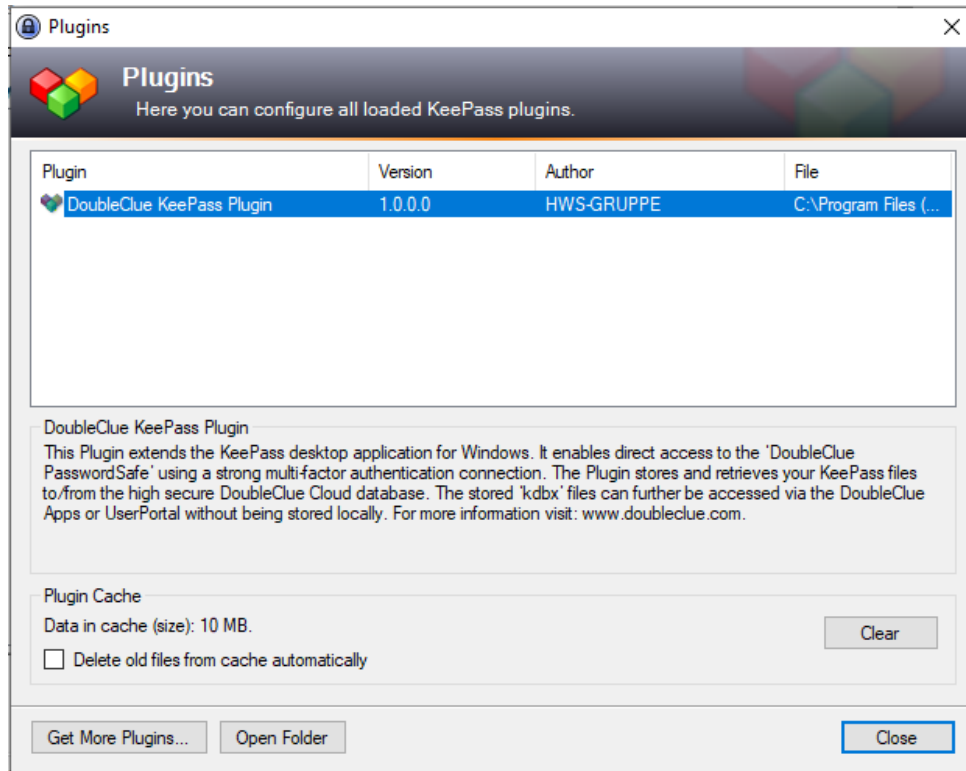- Active user account at a DoubleClue Enterprise Management (DCEM) system

# 2. Setting up the DoubleClue KeePass Plugin

## 2.1 Installation

1. Download the most recent KeePass version from https://keepass.info and install *KeePass Password Safe* according to the instructions.
2. Download the DoubleClue KeePass-Plugin at https://doubleclue.com/files/DoubleClueKeePassPlugin.zip.
3. Extract the downloaded file.
4. Navigate to the *KeePass Password Safe* directory and copy the extracted "DoubleClueKeePassPlugin.plgx" file into the "**Plugins**" folder.

5. Restart the KeePass application.

If you want to check whether the plugin is active, open KeePass, go to "Tools" > "Plugins" and see if the "**DoubleClue KeePass Plugin**" is displayed in the window.



## 2.2 Connection

By default, the plugin connects with DoubleClue CloudSafe at https://doubleclue.online.  All private users who have created their account at https://doubleclue.online can use this default connection.

Enterprise users need to configure their plugin, so that it connects successfully with their company's DoubleClue. For more information about this see chapter 3. Configuration for Enterprise Users.

# 3. Configuration for Enterprise Users

The following instructions are for DCEM admins who want to configure the DoubleClue KeePass Plugin to connect with a DoubleClue Enterprise Management (DCEM) running on premises or on a tenant. For the configuration, you need two meta files from your DCEM: the "**SdkConfig.dcem**" and "**AuthConnector.dcem**" file.

⚠ To create and download these files, you need to log into DCEM as an administrator. If you do not have administrator access, contact your company's DCEM administrator.

## 3.1 Creating the "SdkConfig.dcem" file

If you are using DCEM in the Cloud, please send an e-mail at support@doubleclue.com and contact the DoubleClue team to get this file.

If you installed DCEM on your premises, continue as follows:

1. In DCEM, go to the main menu item "Identity & Access", submenu "App Versions", and click on "Generate SDK Configuration".
2. In most cases, the URL is entered automatically in the opening window. If not, enter it according to the following pattern:
   **wss://*Host Name of the Server*:*Port*/dcem/ws/appConnection**
   The address has to be accessible from the internet. In case you use a load balancer, through which you access DCEM, you need to enter the load balancer's address here.
3. Under "Choose Certificate Source" we advise to select "Get certificate from URLs" in the drop down menu and then click on "Retrieve Certificates"
4. Click on "Download SDK Configuration" to get the file "**SdkConfig.dcem**".

## 3.2 Creating the "AuthConnector.dcem" file

If your DCEM runs on a tenant, ensure that you download the AuthConnector.dcem from the tenant's DCEM, not from the master DCEM.

1. In DCEM, go to main menu item "Identity & Access", submenu "Auth Connector", and click on "Add".
2. Enter a unique name, e.g. "DoubleClue KeePass Plugin", and click on "OK".
3. Now click on the button "Download" to download the file "**AuthConnector.dcem**".

## 3.3 Get a Preconfigured KeePass Plugin

We can provide you with a preconfigured version of the KeePass Plugin. You can then forward this plugin to your users, and they will be automatically redirected to your DCEM or tenant whenever they use the plugin. If you want to use this option, please send the "SdkConfig.dcem" and the "AuthConnector.dcem" at support@doubleclue.com.

It is also possible to implement the configuration for several DCEMs into one plugin. Users can connect to the different DCEMs or tenants, by adding a realm name separated by a dollgar sign ($) to their username e.g. Jane.Smith$realmname.

If you want to create the plgx file yourself, please contact us at support@doubleclue.com.

## 3.4 Set up the Configuration Files Manually on the User Workstation

If you don't want to send your users a pre-configured version of the DoubleClue KeePass Plugin, you can also configure the plugin manually by storing the meta files on the user workstation. The location in which the files are stored differs according to whether all users of this workstation shall connect to the same DCEM or tenant or to different ones.

### 3.4.1   Set up the Configuration for all Users of the Workstation

1. Navigate to the KeePass installation directory and create a folder called "DoubleClueAuthConnector".
2. Copy the files "AuthConnector.dcem" and "SdkConfig.dcem" into the new folder "DoubleClueAuthConnector".
3. Restart KeePass.

The DoubleClue KeePass Plugin will now connect to your DCEM.

### 3.4.2   Set up the Configuration for one Specific User of the Workstation

1. Navigate to the user directory, e.g. C:\users\username
2. Create a new "DoubleClueAuthConnector" folder.
3. Copy the files "AuthConnector.dcem" and "SdkConfig.dcem"" into the new folder "DoubleClueAuthConnector".
4. Restart KeePass.

The DoubleClue KeePass Plugin will now connect to your DCEM.

⚠ The plugin will always check for the configuration files in the user folder first. Should configuration files be stored in both places, the plugin will connect to the DCEM specified in the user folder.

### 3.4.3 Connect to multiple DCEMs

It is possible to connect to different DCEMs using the same workstation or user by following these steps:

1. Create several subfolders in the "DoubleClueAuthConnector" folder and give each a unique name.
2. Copy the configuration files of the different DCEMs into different subfolders.
3. Choose a DCEM by using the name of the respective folder added as an suffix to your username, separated from your username by a dollar sign ($). Example: Username$foldername.

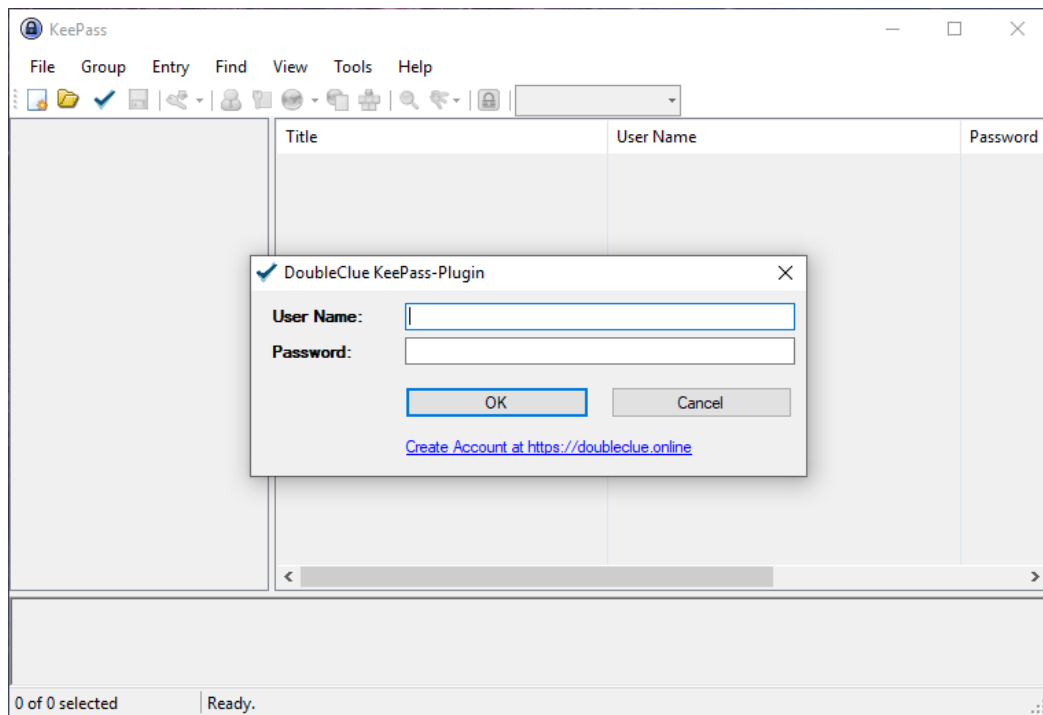By using different suffixes, you can switch to different DCEM connections.

# 4. Using the DoubleClue KeePass Plugin
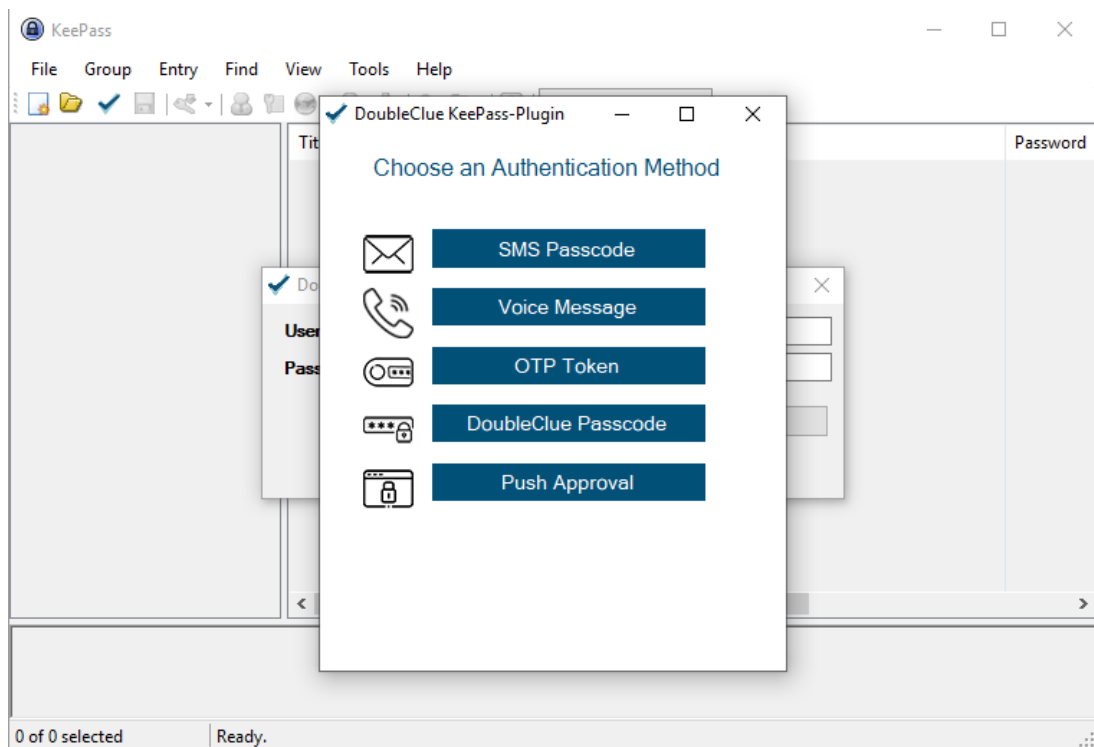
## 4.1 Opening the KeePass file with DoubleClue

1. Open KeePass.
2. In the menu on the upper-left side, click on "File" > "Open" > "Open from DoubleClue".
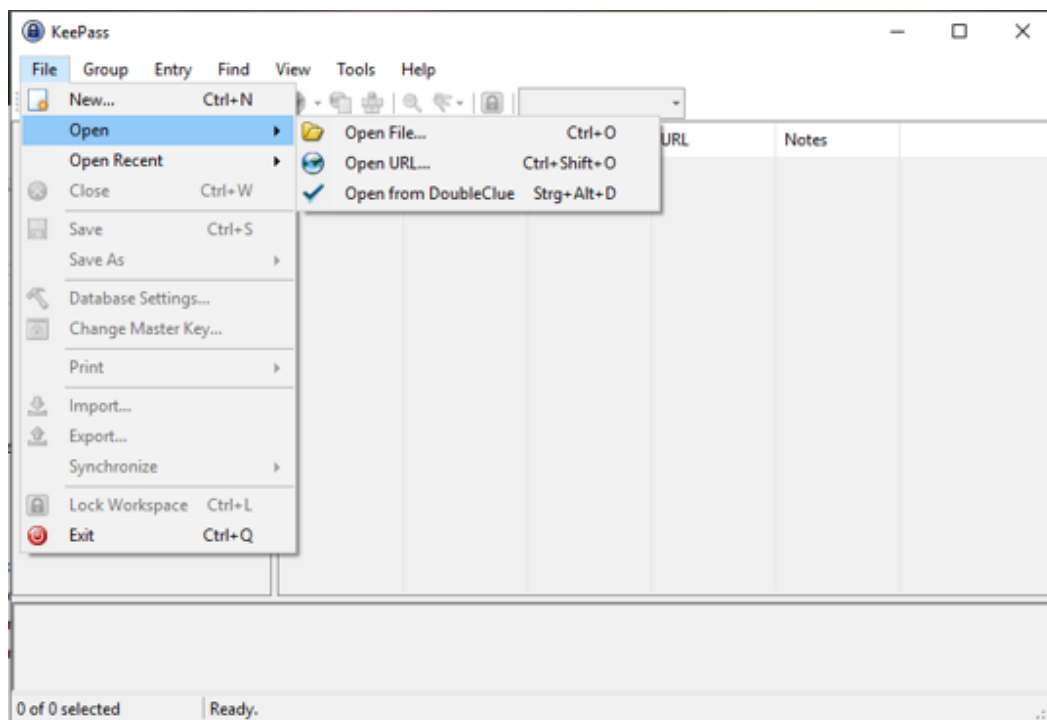
3. A login window will appear. Enter your DoubleClue credentials:



4. Choose the authentication method you wish to use to connect to DoubleClue. The available authentication methods can be defined in DCEM under 'Identity & Access' > 'Policies' > 'Applications'.

## 4.2  Saving the KeePass file in DoubleClue

In the menu on the upper-left side, click on "File" > "Save as" > "Save to DoubleClue" in order to save your KeePass file in the DoubleClue cluster.

If you would like to save only a copy of the file in DoubleClue, click on "Save copy to DoubleClue".

Log into DoubleClue as described in chapter 3.1 step 3 and for.