Integration von Azure Active Directory

1. Einführung

Diese Anleitung richtet sich an Administratoren, die ein Azure Active Directory mit DoubleClue verbinden möchten.

Voraussetzungen:

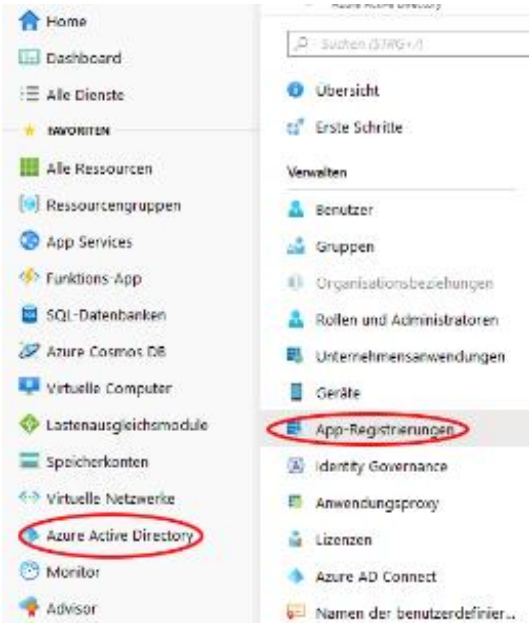
- DoubleClue Installation
- Azure Account

2. Einrichtung einer Azure Applikation

2.1 App Registrierung & Konfiguration

1. Loggen Sie sich unter https://portal.azure.com in Ihr Administratorenkonto ein.

2. Gehen Sie zu “Azure Active Directory” und wählen Sie im sich darauf öffnenden Submenü “App - Registrierungen” aus.

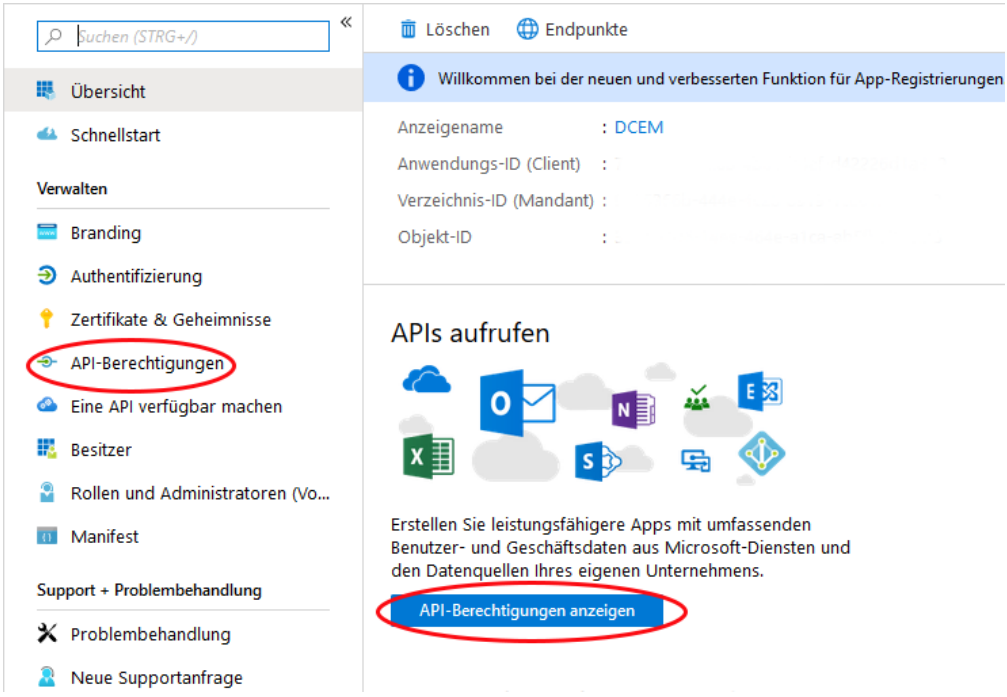


3. Klicken Sie auf “Neue Registrierung”. Wenn Sie bereits eine passende App angelegt haben, können Sie diesen Schritt überspringen. Wählen Sie die entsprechende App aus und gehen Sie direkt zu Schritt 5.

4. Geben Sie Ihrer Applikation einen gut erkennbaren Namen, z.B. “DoubleClue”. Wählen Sie anschließend den Account-Typ aus, den Sie unterstützen möchten. Klicken Sie zum Abschluss auf „Registrieren“.

5. Kopieren Sie die “Anwendungs-ID (Client)” und “Verzeichnis-ID (Mandant)” aus der Übersicht der Applikation. Speichern Sie sie an einem sicheren Ort – Sie werden sie im späteren Verlauf des Prozesses noch benötigen.

6. Klicken Sie auf “API-Berechtigungen anzeigen” oder “API-Berechtigungen” im Untermenü auf der linken Seite.



7. Gehen Sie auf “Berechtigungen hinzufügen”. Wählen Sie in der sich darauf öffnenden Auswahl zunächst „Microsoft Graph“ und anschließend „Anwendungsberechtigungen“ aus. Daraufhin wird sich ein Menü öffnen, in dem Sie die Berechtigungen auswählen können.

8. Öffnen Sie den Bereich “Directory” und setzen Sie einen Haken bei “Directory.Read.All”. Öffnen Sie danach “Users” und setzen Sie einen Haken bei “User.Read.All”. Bestätigen Sie Ihre Auswahl mit dem „Berechtigungen hinzufügen“-Button am unteren Rand der Auswahl.

9. Gehen Sie noch einmal auf „Berechtigungen hinzufügen“ und wählen Sie „Micorosft Graph“, dann „Delegierte Berechtigungen“. Öffnen Sie den Bereich „User“ und aktivieren Sie

„User.Read.All“. Bestätigen Sie die Auswahl mit dem „Berechtigung hinzufügen“-Button am Ende des Menüs.

10. Gehen Sie sicher, dass für alle Berechtigungen Administratorzustimmung gegeben wurde.

11. Gehen Sie zu “Zertifikate & Geheimnisse” im Untermenü auf der linken Seite.

12. Legen Sie einen “Neuen geheimen Clientschlüssel” an und Sie aus, wie lange der gültig sein soll.

13. Kopieren oder notieren Sie den neuen geheimen Clientschlüssel. Achtung, der geheime Clientschlüssel wird nur einmal angezeigt. Geht er verloren, muss ein neuer Schlüssel angelegt werden.

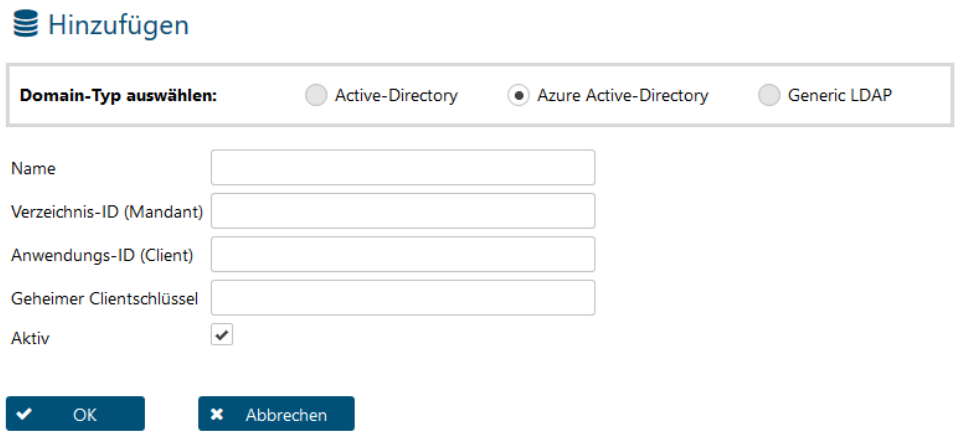
2.2 Verbindung mit DCEM

1. Loggen Sie sich als Administrator in DCEM ein.

2. Gehen Sie im DCEM Hauptmenü zum Bereich “Administration” und daraufhin zum Bereich „Domain“.

3. Fügen Sie eine neue Domain hinzu.

4. Wählen Sie “Azure Active-Directory” als Domain-Typ aus.



5. Wählen Sie einen Namen aus, der ausdrucksstark und leicht zu merken ist, zum Beispiel Ihren Firmennamen. Der Name ist später das Präfix, das Nutzer zu ihrem Login-Namen hinzufügen müssen, um sich bei DoubleClue anzumelden.

6. Tragen Sie die Anwendungs-ID (Client) und die Verzeichnis-ID (Mandant), die Sie in Schritt 2.1.5 kopiert haben, in die entsprechenden Felder ein.

7. Tragen Sie den geheimen Clientschlüssel aus Schritt 2.1.11 in das entsprechende Feld ein.

8. Bestätigen Sie die Eingaben. Sie haben Ihr Azure Active Directory jetzt erfolgreich mit DoubleClue verbunden.