



DoubleClue Active Directory Connector

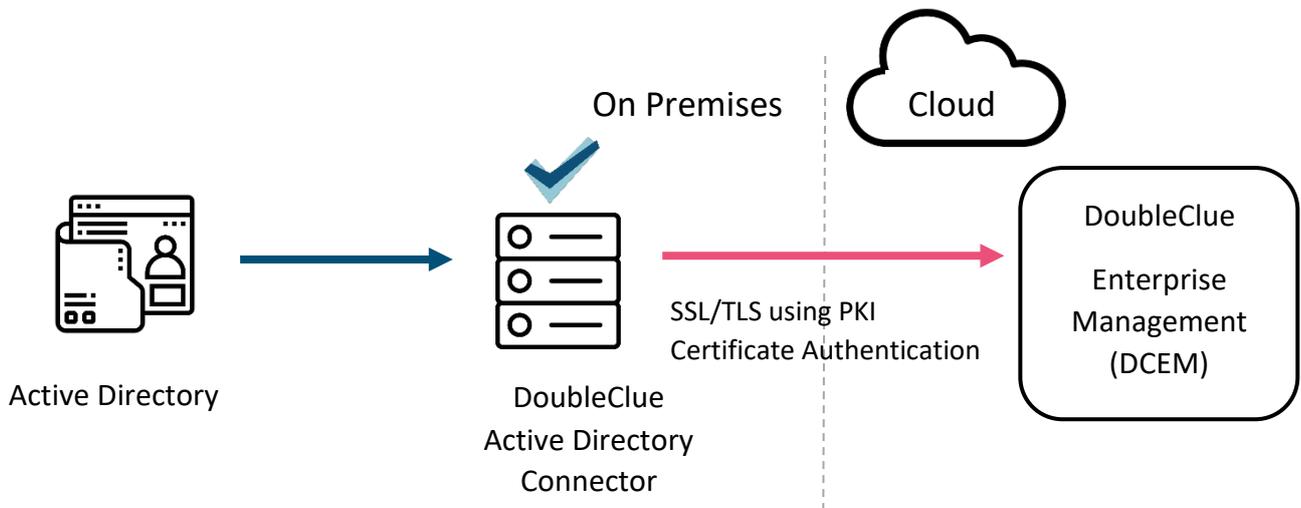
Content

1. Introduction	2
2. Scenario.....	2
3. Installing DoubleClue Auth Connector Proxy.....	2
3.1 Windows Installation	2
3.2 Linux Installation	2
4. Configuring DoubleClue Auth Connector Proxy.....	3
4.1 Create Auth Connector.dcem	3
4.2 Create SdkConfig.dcem.....	3
5. Add Domain to DCEM	4
6. Add an Active Directory Trust Certificate	4
6.1 Add the Trusted Certificate to a Linux Server.....	5

1. Introduction

The DoubleClue Active Directory Connector is a service that connects a DoubleClue Enterprise Management (DCEM) running in the cloud as a service with an Active Directory on premises. In this scenario, a proxy is installed on the server on premises and acts as the proxy client while DCEM acts as the proxy server.

2. Scenario



3. Installing DoubleClue Active Directory Connector

3.1 Windows Installation

On Windows, install Auth Connector Proxy as a Windows service by executing the **ADConnector-X.X.X.exe** (X.X.X. stands for the version number of the file) with administrator rights.

3.2 Linux Installation

On a Linux server, install Auth Connector Proxy as a Linux daemon. You need administrator rights for the installation. Start by extracting the **ADConnector-X.X.X.tar.gz** file.

1. Open the console and navigate to the parent install directory.
2. Now enter **"tar -xvf ADConnector-X.X.X.tar.gz"** to extract into the current directory.
3. Install and run Auth Connector Proxy as a Daemon by going to the directory **"ADConnector/sh"** and executing the file **"installADConnector.sh"**.

4. You can always stop or start the Daemon again by executing the file “**stopADConnector.sh**” or “**startADConnector.sh**”.

4. Configuring DoubleClue Active Directory Connector

DoubleClue Active Directory Connector requires two meta files from your DCEM to connect successfully with it, the **AuthConnector.dcem** and the **SdkConfig.dcem**. Both files must be stored in the following folder:

InstallationDirectory/DCEM_HOME/ADConnector

4.1 Create AuthConnector.dcem

The AuthConnector.dcem file can be downloaded in your tenant’s DCEM. If you do not have the necessary access rights, please contact your DoubleClue administrator.

In DCEM, navigate to “Identity Management” > “Auth Connector”. Add a new connector and give it a unique name, e.g. “Active Directory Connector”. Choose the new connector in the list below and click on “Download”.

 If your DoubleClue is running on a tenant, ensure that you download the file from the tenant’s DCEM.

4.2 Create SdkConfig.dcem

The SdkConfig.dcem file can be downloaded in the Master DCEM of your DoubleClue installation.

Log into your DCEM account and go to “Identity Management” > “Versions”. Click on “Generate SDK Configuration”.

 Please be aware that you need to download the SdkConfig.dcem from the installation’s Master DCEM, not the tenant DCEM. If you don’t have the necessary access, please contact your administrator. If your tenant is hosted at the official DoubleClue dispatcher (<https://doubleclue.online>), please contact support@doubleclue.com.

Once you have added the two files as described, the DoubleClue Active Directory Connector will successfully communicate with your DCEM tenant.

5. Add Domain to DCEM

Log into your DCEM. Then go to “Administration” > “Domain”. Click on “Add” to add your domain to DCEM.

Choose either “Active Directory” or “Generic LDAP”, depending of what kind of Active Directory you want to add.

Enter the information of your active directory into the mask as described in the DCEM Manual Chapter [3.6 Integration of Active Directory / Azure AD / LDAP](#).

Check the box saying “Connect with AD Connector”. In the dropdown menu below, choose the name you gave to the new connector in step 4.1.

 Edit

Select a Domain-Type: Active-Directory Azure Active-Directory Generic LDAP

Name	<input type="text" value="doubleclue"/>
URL	<input type="text" value="ldaps://dc01.doubleclue.local:3269"/>
Base DN	<input type="text" value="DC=doubleclue,DC=local"/>
Search Account DN/UPN	<input type="text" value="john.smith@doubleclue.local"/>
Search Account Password	<input type="password" value="....."/> 
Map E-Mail Suffixes to this Domain	<input type="text" value="doubleclue.local; test.doubleclue.com"/>
Verify Certificate	<input type="checkbox"/>
Connect with AD Connector	<input checked="" type="checkbox"/>
Choose AuthConnector	<input type="text" value="AD Connector"/>
Rank	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/>

✔ OK
✘ Cancel

6. Add an Active Directory Trust Certificate

While Active Directory will always sign its request with a trust certificate, DoubleClue will only verify the certificate if this option has been activated.

If you want to activate the verification of the certificate, log into your tenant’s DCEM. Then go to “Administration” > “Domain”. Select the domain for which you want DCEM to verify the certificate (in case you have several) and click on the “Edit” button.

Check the box saying “Verify Certificate”.

 Edit

Select a Domain-Type: Active-Directory Azure Active-Directory Generic LDAP

Name	<input type="text" value="doubleclue"/>
URL	<input type="text" value="ldaps://dc01.doubleclue.local:3269"/>
Base DN	<input type="text" value="DC=doubleclue,DC=local"/>
Search Account DN/UPN	<input type="text" value="john.smith@doubleclue.local"/>
Search Account Password	<input type="password" value="....."/> 
Map E-Mail Suffixes to this Domain	<input type="text" value="doubleclue.local; test.doubleclue.com"/>
Verify Certificate	<input checked="" type="checkbox"/>
Connect with AD Connector	<input checked="" type="checkbox"/>
Choose AuthConnector	<input type="text" value="AD Connector"/> ▼
Rank	<input type="text" value="1"/> ▼
Enable	<input checked="" type="checkbox"/>

As Windows trusts all certificates in the Windows “Trusted Root Certificate Authorities”, you don’t have to do anything else if your DCEM runs on a Windows server.

6.1 Add the Trusted Certificate to a Linux Server

When you want to activate the “Verify Certificate” option on a Linux server, you need to add the trust certificate into the DCEM Java Virtual Machine (JVM). Do so with the following steps:

1. Export the certificate from the Windows Certification Manager. If you don’t have access to the Windows Certificate Manager of your Active Directory, ask the respective Administrator to forward it to you.
2. Copy the certification file to „*DCEM-Installation/jvm/bin*“
3. Open a terminal session and go to the path „*DCEM-Installation/jvm/bin*“
4. Execute the command: `keytool -keystore ../lib/security/cacerts -importcert -alias activedirectory -file active-directory.cer`
5. The keytool will then ask you for a password. The default password is “changeit”.
6. Repeat this for every DCEM node.