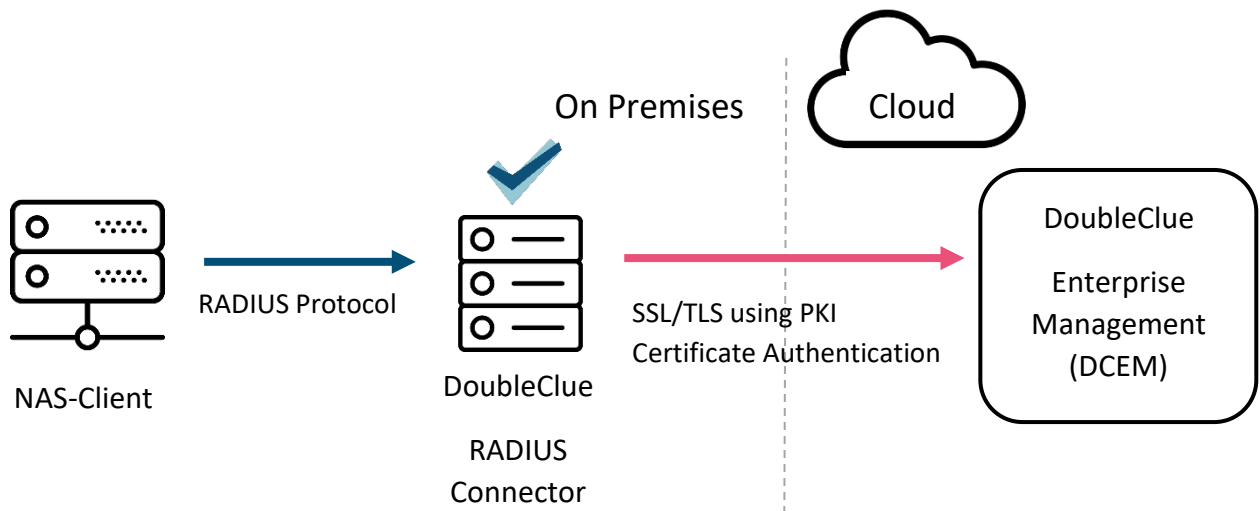# DoubleClue RADIUS Connector
Version 2.3.1

1. Introduction

This documentation is intended for administrators, who use DoubleClue Enterprise Management (DCEM) as a service and want to protect their RADIUS NAS-client running on premises. The RADIUS Connector acts as a RADIUS Server on premises and forwards the user authentication on a high secure connection to DoubleClue in the cloud as depicted in the scenario below.

2. Scenario

3. Installing DoubleClue RADIUS Connector

3.1 Windows Installation

On Windows, the RADIUS Connector will be installed as a Windows Service. To install it, execute **RADIUS-ConnectorX.X.X.exe** with administrator rights.

3.2   Linux Installation

On a Linux server, the RADIUS Connector is installed as a Linux daemon. For the installation, you need to extract the RadiusConnector-Linux-X.X.X.tar.gz with administrator rights.

1.   Open the console and navigate to the parent install directory.
2.   Now enter "**tar -xvf RadiusConnector-Linux-X.X.X.tar.gz**" to extract into the current directory.
3.   Install and run RADIUS Connector as a Daemon by going to the directory "**RadiusConnector/sh**" and executing the file "**installRadiusConnector.sh**".
4.   You can always stop or start the Daemon again by executing the file "**stopRadiusConnector.sh**" or "**startRadiusConenctor.sh**".

3.3   Access to the Configuration Web Interface

The Radius Connector has a web interface for configuration and diagnostics. You can access it any time via browser at **https://yourhostname:9443/radiusconnector/**

When you open the Configuration Web Interface for the first time, you will be asked to set a password to protect the access in the future.

4.   Configuring DoubleClue RADIUS Connector

DoubleClue RADIUS Connector requires two meta files from your DCEM, the **AuthConnector.dcem** and the **SdkConfig.dcem.** Both files must be stored in the following folder:

*InstallationDirectory***\DCEM_HOME\radiusAuthConnector**

4.1   Create AuthConnector.dcem

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

In DCEM navigate to the main menu subject "Identity Management" and here to the submenu "Auth-Connector". Add a new connector and give it a unique name. Choose the new connector in the list below and click on "Download".

⚠   Please be aware that you need to download the AuthConnector.dcem from the tenant's DCEM, not the master 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", submenu "Versions". Here choose "Generate SDK Configuration". According to the individual network scenario, you may have to change the settings. Check the DCEM Manual for more information.

⚠ 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 https://doubleclue.online, please contact support@doubleclue.com.

Once you have added the two files as described, the DoubleClue RADIUS Connector will successfully communicate with your DCEM. You can now configure the RADIUS Connector to connect with your NAS client.

5. Configuration

5.1 RADIUS

RADIUS Port:
The port of the NAS client, by default 1812. If you change this setting, you must to restart DoubleClue RADIUS Connector.

Accounting Port:
The Accounting Port of the NAS client if applicable. By default, this port is set to 0, which means not active. If you change this setting, you must to restart DoubleClue RADIUS Connector.

Shared Secret:
Enter the Shared Secret of the NAS client. If this won't match with the shared secret on your NAS-Client, the user's passwords would always be invalid.

IP Number:
Enter the IP Number of the NAS-Client. DoubleClue RADIUS Connector will only accept request from the NAS-Client with this IP number.

Ignore User Password:
If the Password has already been checked by the NAS client, you can activate 'Ignore User Password' to prevent a second validation by DoubleClue. For some services which do not forward the password to DoubleClue, like Microsoft Remote Desktop Gateway, it is compulsory to activate this option.

Data Tracing:
Enable Data Tracing for support and diagnostic purposes. This option should only be activated on request of the DoubleClue support team. If active, all radius traffic will be inserted in the logfile.

5.2 Web Interface

Web Port:
Enter the Web Port number for DoubleClue RADIUS Connector.

Web Password:
The password to log into the DoubleClue RADIUS Connector Web Interfaces. You can change the password here at any time.

5.3 Proxy

DoubleClue Connector needs to connect to DCEM over the internet. If you are using http-proxy to access the internet, then you have to configure this here.

6. Monitoring

Under Monitoring, you can find a detailed overview off all the events concerning the connection with the RADIUS Connector, including successful and unsuccessful user logins.