Quick Installation Guide

for DoubleClue Enterprise Management (DCEM)

on Premises

Version: 2.3.3

Contents

1. Introduction

This guide is intended to quickly set up the DoubleClue Enterprise Management (DCEM) software using an **embedded SQL database** and **Windows or Linux as an operating system**. In this scenario, all components are installed on the same machine.

⚠ Some basic IT knowledge is required to be able to install and deploy "DoubleClue Enterprise Management" (DCEM).

Please be aware that the embedded database does not support multiple tenants. If you want to use DoubleClue with multiple tenants, please follow the more detailed instructions in the DoubleClue Manual.

2. Installation and Launch of DCEM

2.1 Server Requirements

- RAM: Minimum of 4 GB (depending on the number of users)
- Hard Drive: Minimum of 20 GB
- Operating System: Windows 64 Bit or Linux 64 Bit
- DNS entries in the internal company network as well as external
- Default Network Ports
    - 8443   for Management and Setup
    - 443   for Smart-Device Web-Sockets
    - 8001   for REST Web-Services

2.2 Client Requirements

If you intend to use Push Approval, QR-Code Approval or DoubleClue Passcode as authentication methods and therefore need to use DoubleClue App, the following requirements apply:

Android: From Version 5.0 (Android Lollipop)
Windows: From Version 7, 8, 10
iOS: From Version 10.0

⚠ Port 443 is the default port for the Apps. This port must be reachable from the internet. Please enable this port for DCEM in your Firewall.

2.3 Installation

In order to install DCEM, you need administrator / root rights.

You can install DCEM on Windows 64bit or on Linux 64Bit machines.

After the installation is completed, DCEM will run as a service on Windows and as a daemon on Linux.

Before DCEM can be started, the setup needs to be executed in order to configure the database and further settings.

The setup needs to be executed only once. It is exclusively available in English.

2.3.1   Windows Installation

Start the setup by executing the file "**DCEM-X.X.X.exe**" (X.X.X. stands for the version number of the file) with administrator rights.

1. Choose the directory where you want to install DCEM.
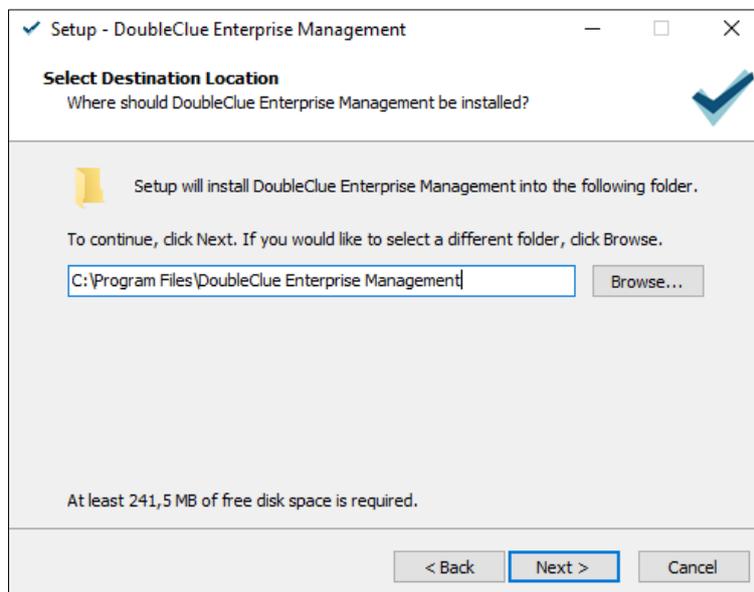
2. Select "Install first DCEM cluster node" and click on "Next".
3. Enter a name for the Start Menu folder or leave as is.
4. Now, the DCEM installation files will be copied to the install directory.
5. The Setup Web will be launched in a command view.
6. If your default browser will not start automatically, then please open your browser and enter the following link: **https://localhost:8443/setup?start=yes**
7. The setup uses a secured HTTPS connection with a "self-signed" certificate. Therefore, a security alert is shown in the browser during the connection process. Confirm this alert and allow the connection as an exception.
8. Configure the Database. See chapter 2.5 Database Configuration.
9. After the database configuration, close the DoubleClue Setup Application.
10. The setup will now automatically install DCEM as a Windows service.

2.3.2   Linux Installation

First, you need to extract the file "**DCEM-Linux-X.X.X.tar.gz**".

1. Open the console and navigate to the parent install directory.
2. Now enter "**tar -xvf DCEM-Linux-X.X.X.tar.gz**" to extract into the current directory.
3. Go to the directory "**DCEM/sh**" and start the setup by executing the file "**runSetup.sh**".
   The setup configuration form will now start automatically in your default browser if you are using a Linux desktop. Otherwise, start the browser and enter the following link:
   https://your-host-name:8443/setup?start=yes
4. The setup uses a secured HTTPS connection with a "self-signed" certificate. Therefore, a security alert is shown in the browser during the connection process. Confirm this alert.
5. Configure the Database configuration as described in chapter 2.4 Database Configuration.
6. After finishing DoubleClue Setup, you need to install and run DCEM as a Daemon by going to the directory "**DCEM/sh**" and executing the file "**installDcemDaemon.sh**".
7. You can always stop or start the Daemon again by executing the file "**stopDcemDaemon.sh**" or "**startDcemDaemon.sh**".

2.4   Database Configuration

DCEM requires an SQL database in order to run.

For testing purposes, you may choose the pre-installed Embedded Database. If you wish to install an external SQL database first, please see the respective manuals and the DCEM Manual. As external databases, DoubleClue supports:

- MS SQL
- MariaDB
- My SQL
- PostgreSQL

2.4.1   Embedded Database

The disabled input fields are not required for the Embedded Database.

1. Select the database type "Embedded-Database" and click on "Save".

⚠ Please note: The Embedded Database does not support multiple DCEM nodes or multi-tenants!

2. DoubleClue Node Name: Per default, the DoubleClue Node Name will be your computer or host name or, if they are not available, your IP address. You can leave the node name as it is or choose a new one.
3. Confirm the message and click on "Next" to continue with the setup.
4. Super-Administrator Password: Specify the password for the super administrator of DCEM. The user name of the super administrator is always "SuperAdmin".
5. DoubleClue Server URL: Enter the URL by which users can access your DCEM from an external location.

6. Click on "Create Tables".
7. Confirm the alert "Database Setup Ready".

You can now close the setup and finish the installation of DCEM.

2.5 Administrator Login to DCEM

The URL for the login to DCEM is:

https://*your-host-name*:8443/dcem/mgt/login.xhtml

Log in with the username "superadmin" and the password specified for the super administrator during setup.

After login you can administrate DCEM.

3. DCEM Configuration

In this chapter, we explain the first steps of a DCEM configuration process to enable you to connect and deploy a **DoubleClue Windows Desktop Application** with DCEM.

DoubleClue supports the following authentication methods:

- Push Approval (with DoubleClue App)
- QR-Code Approval (with DoubleClue App)
- DoubleClue Passcode (with DoubleClue App)
- FIDO U2F and FIDO2 Token
- Password
- SMS Passcode
- Voice Message

▪ OTP Token

3.1 Creating a User

DoubleClue users require a registered user account to use DoubleClue.

1. Go to menu item "Administration", submenu "Users".
2. Click on "Add+". When adding a new user, you can choose between creating a "Local User" or a "Domain User". Fill in the required fields.

   Local users receive an "Initial Password" which you need to inform them about so that they can activate their DoubleClue App.

4. Deploying DoubleClue App

4.1 Register your DCEM with the DoubleClue Dispatcher

In order to use the DoubleClue App, you need to register your DCEM installation at the global DoubleClue Dispatcher https://doubleclue.online, a DCEM Cluster managed by *HWS Informationssysteme GmbH*.

4.1.1 Certificate Common Name and Host Name

To prepare your DCEM to connect it with the DoubleClue Dispatcher, you need to ensure that a proper KeyStore is available for the connection.

After installation, a default server certificate is created for the SSL/TLS device websockets ("**DeviceWebsockets_CA**"). The certificate's Common Name (CN) is set to the URL host name of the browser. If the Internet host address you want to use is different from the default CN of the "**DeviceWebsockets_CA**" keystore, you have to generate a new "**DeviceWebsockets_CA**" keystore and set the CN to the internet host address.

In order to generate a new "**DeviceWebsockets_CA**" keystore, go to main menu item "System", submenu "Keystores" and click on the button "Generate new KeyStore".

4.1.2 Establish Redirection via the DoubleClue Dispatcher

There are two ways to redirect the Doubleclue App to your DCEM on Premises via the DoubleClue Dispatcher: Directly or via Reverse Proxy.

4.1.2.1 Direct Redirection

Requirements: DCEM Server port 443 must be reachable from the internet.

During the app activation, the Dispatcher will verify user ID and Activation Code at the DCEM installation.

If the Activation Code is valid, the Dispatcher will send the DCEM "**SdkConfig.dcem**" metadata file to the device. On login, the app will then connect directly to your DCEM installation.

⚠ Please note: The DoubleClue Online Dispatcher will not store any user data such as activation codes, passwords etc.

The file "**SdkConfig.dcem**" contains secure information about DCEM, which is required to establish a trusted connection to your DCEM installation. Here are the steps to create the SdkConfig.dcem.

1. Go to menu item "Identity-Management", sub menu "Versions" and click on the button "Generate SDK Configuration".
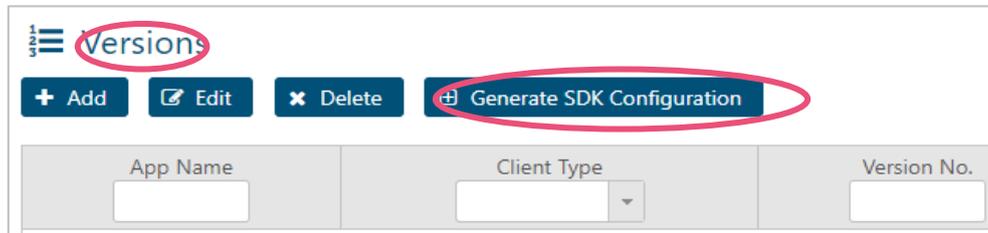
2. Download the SDK Configuration.
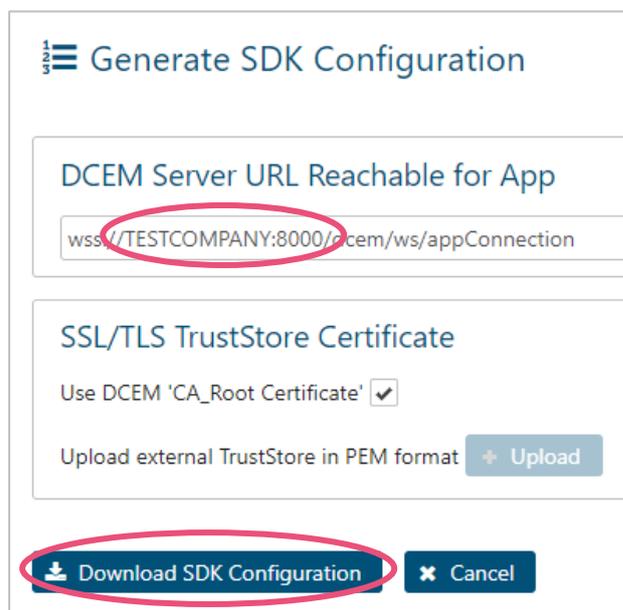
⚠ The host address and port must be reachable from the internet. The host address <u>must</u> also match the <u>Common-Name</u> "CN" of the "**DeviceWebSockets_CA**" keystore certificate. See chapter [4.1.1 Certificate Common-Name and Host Name](#).

3. Choose a short, globally unique name to identify your DCEM installation. This is referred to as the Realm-Name. The Realm-Name will be a suffix for to the username separated by a dollar character. For example:
   user.name$realm where realm is the Realm-Name.

4. Send the downloaded file "**Sdk.Config.dcem**" together with your realm-name to support@doubleclue.com for registration.

4.1.2.2 Redirection via Reverse-Proxy

In this scenario, your DCEM on premises will connect to the global DoubleClue Dispatcher. Hence, the user device won't connect directly to your DECEM and you don't need to open any firewall ports. All data between Apps and your DCEM will pass through the Reverse-Proxy on global DoubleClue Dispatcher.

⚠ Please note: The Reverse-Proxy connection should NOT be used for a productive environment!

4.1.2.2.1 Register DCEM at the DoubleClue Dispatcher

Choose a Realm Name that will identify your DCEM cluster towards the DoubleClue Dispatcher. We suggest using the name of your company as Realm Name. The Realm Name must be unique for the Dispatcher.

Send the chosen name to support@doubleclue.com in order to register your DCEM cluster at the DoubleClue Dispatcher. After registration, you will receive a "**ReverseProxy.dcem**" metadata file and a secret password from your DCEM support team.

4.1.2.2.2 Configuration of DCEM for Reverse-Proxy

Go to main menu item "Identity-Management", submenu "Reverse-Proxy" and click on the button "Configure".
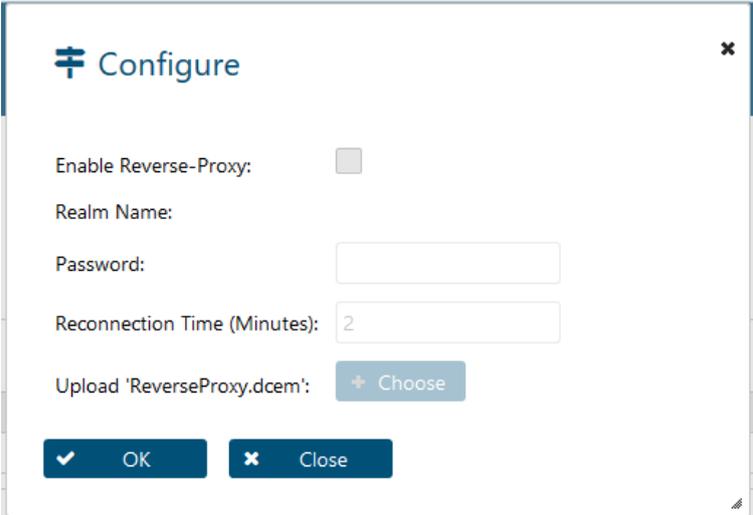
Enable Reverse-Proxy: Check this box to enable the Reverse-Proxy.

Realm Name: This is the unique name that you chose to identify your DCEM cluster towards the DoubleClue Dispatcher. It will be automatically added from the "**ReverseProxy.dcem**" file.

Password: Enter the password which was sent to you by the DoubleClue team.

Reconnect Time (Minutes): Here you can enter the time interval in which your DCEM installation tries to reconnect with DoubleClue Reverse-Proxy if a connection attempt fails.

Upload ReverseProxy.dcem: Upload the file "**ReverseProxy.dcem**"

4.2 Downloading the DoubleClue App

Users can download the DoubleClue App from Google Play Store or the App Store. The Windows Desktop App can be downloaded from www.doubleclue.com.

By default, the DoubleClue App will always connect with the DoubleClue Dispatcher on https://doubleclue.online. Users need to add the realm name connected with a dollar sign '$' to their username in order to connect with a DCEM on premises. When registering the app via E-Mail, the user will receive their full login ID as part of the mail.

4.3 App Activation

When the app is executed on a certain device for the first time, it needs to be activated. For this, the user needs an activation code from DCEM. To create an activation code for a user, follow the following steps:

1. Go to menu item "Identity-Management", submenu "Activation Codes".
2. Click on the button "Add".

3. View the Activation Code by selecting the user and clicking the button "Show Activation Code".

In case you already set the E-Mail configuration, you may send the activation code as a QR-Code to the user.

To send Authentication Codes directly to the user via e-mail or SMS, you must configure the email and SMS settings under "System" > "Preferences". For more information, please see the **DCEM Manual**.

5. Login to DoubleClue UserPortal

UserPortal is a self-service webportal for DoubleClue users. In UserPortal, users can manage their devices and have access to CloudSafe and PasswordSafe. The URL to UserPortal is built in the following pattern: https://your-host-name:8443/dcem/userportal

Login with your username and password. You will be forwarded to a dialog, in which you can select the MFA method you want to use.

Choose "Push Approval" and login through the DoubleClue Clue App.

You will get a confirmation message, when you validate the Push Approval and you will be successful logged into the UserPortal with two-factor authentication.