



Manual

DoubleClue Enterprise Management (DCEM)

Version: 2.8.1

Contents

1.	Introduction	8
2.	Installation & Launch	9
2.1	Requirements.....	9
2.1.1	Hardware Requirements.....	9
2.1.2	Database Requirements.....	9
2.2	Installation Information	10
2.3	Installation Process	10
2.3.1	Installation with Windows	11
2.3.2	Installation with Linux.....	11
2.3.3	Installation with a Headless Operating System	12
2.3.4	Running Installation again.....	12
2.4	Database Configuration	12
2.4.1	Embedded Database	12
2.4.2	External Database	14
2.4.2.3	<i>Configuring a PostgreSQL Database.....</i>	17
2.5	Installing DCEM as a Daemon	18
2.6	Database Migration	18
2.6.1	Migration with Windows	18
2.6.2	Migration with Linux.....	18
2.6.3	Migration Process	19
2.7	Login to DCEM.....	19
2.7.1	Login with User Name and Password	19
2.7.2	Login with DoubleClue Multi-Factor Authentication.....	20
2.8	Log into DCEM.....	20
2.8.1	File “configuration.xml”	20
2.8.2	Folder “DCEM_HOME”	21
3.	DCEM System Main Menu	21
3.1	Cluster Configuration.....	21
3.1.1	General Settings.....	22
3.1.2	Connection Services.....	23
3.1.3	Connection Service Settings.....	24
3.2	Cluster Nodes.....	26
3.2.1	Installing Further Nodes.....	26

3.2.2	Adding a Cluster Node	26
3.3	KeyStores	28
3.3.1	Adding New KeyStores.....	28
3.4	Possible Connections to the End User	28
3.4.1	SSL/TLS from the End User Terminated at DCEM	29
3.4.2	SSL/TLS from the End User Terminated at the Load Balancer and Unsecured to DCEM	30
3.4.3	SSL/TLS from the End User Terminated at the Load Balancer and Secured to DCEM.....	31
3.4.4	SSL/TLS from the End User Terminated at DCEM with the Load Balancer (Passthrough).....	32
3.4.5	SDK Configuration File	32
3.5	Uploading New KeyStore	33
3.6	Cluster Network Communication	33
3.6.1	One Network.....	33
3.6.2	Several Networks with Multicast	33
3.6.3	Several Networks without Multicast	33
3.7	Diagnostics	34
4.	Administration	34
4.1	Home / Dashboard.....	34
4.2	Users	34
4.2.1	Add Users	34
4.2.2	User Login ID	35
4.2.3	User Password.....	35
4.2.4	Adding an Activation Code.....	35
4.2.5	Phone and Mobile Number.....	36
4.2.6	Private E-Mail Address	36
4.2.7	Reset User Password.....	36
4.2.8	Suspended Users.....	36
4.2.9	Disabled Users.....	37
4.2.10	User Picture, Country and Language	37
4.3	Roles.....	38
4.3.1	Rank	38
4.4	Recover SuperAdmin Access.....	38
4.5	Privileges	39
4.6	Groups.....	40
4.7	Integration of Active Directory / Microsoft Azure AD / LDAP	40
4.7.1	Adding a Default Active Directory Configuration.....	40
4.7.2	Adding an Azure AD Configuration	42

4.7.3	Adding a LDAP Configuration	42
4.7.4	Importing Users and Groups from a Domain	43
4.7.5	Activate Windows SSO for Domain Users	44
4.8	Tenant Branding	45
4.8.1	Time Zone	45
4.8.2	Banner Enterprise Management	45
4.8.3	Banner UserPortal	45
4.8.4	Banner SAML and OpenID Login Page	46
4.8.5	Text on Login Page	46
4.8.6	Background & Logo	46
4.9	Templates	46
4.9.1	Structure of a Template	46
4.9.2	Languages	47
4.9.3	Adding a Template	47
4.9.4	Editing a Template	48
4.9.5	Deleting a Template	48
4.10	Text Resources	48
4.11	Reporting	49
4.12	Change History	49
4.13	Licenses	49
4.14	Preferences	49
5.	Multi-Tenant Capability	50
5.1	Concept	50
5.2	Tenants as Sub-Domains	51
5.3	Management of Multiple Tenants	51
5.4	Login Scenarios for Multi-Tenants	51
5.4.1	Login with Subdomain in a Multi-Tenant Scenario	51
5.4.2	App and RADIUS Login with Multi-Tenants	52
5.4.3	Alternative: Login with Tenant-Specific User IDs	52
5.5	Licences for Tenants	52
6.	Connection Scenarios	53
6.1	Overview	53
6.1.1	Direct Connection with In-House App	53
6.1.2	Dispatcher Connection	54
6.1.3	Reverse-Proxy Connection	55
6.2	Configuration	56

6.2.1	Configuration of the DoubleClue Dispatcher	56
6.2.2	Configuration of DCEM for Reverse-Proxy	57
6.3	The DoubleClue App	58
7.	Authentication Methods and Policies	58
7.1	Authentication Methods	58
7.1.1	Push Approval	59
7.1.2	QR Code Approval	59
7.1.3	FIDO U2F Token	60
7.1.4	OTP Token	60
7.1.5	DoubleClue Passcode	61
7.1.6	Password	61
7.1.7	SMS Passcode / Voice Message	61
7.2	Policies and Applications	62
7.2.1	Adding and Configuring Policies	62
7.2.2	Application Types	62
7.2.3	Assigning Policies	63
7.2.4	Selecting an Authentication Method	63
7.3	Stay Logged In (Silent Login)	64
8.	Identity & Access	65
8.1	Activation Codes	65
8.2	Smart Devices	65
8.2.1	Disabled Smart Devices	65
8.2.2	Deleting a Smart Device	65
8.2.3	Device Status	65
8.3	FIDO-Authenticators	66
8.4	CloudSafe	66
8.4.1	CloudSafe License and Distributing Storage Space to Users	66
8.4.2	File Information	67
8.4.3	Files and Folders with Individual Password	68
8.4.4	Change CloudSafe Storage to Network Access Storage	68
8.5	Push Approval	69
8.5.1	Features of a Push Approval	69
8.5.2	Preferences for Push Approvals	72
8.5.3	Sending Push Approvals via REST-Web Services	73
8.5.4	Status of Push Approvals	73
8.5.5	Life Cycle of a Push Approval	76

8.6	Configuration of Push Notifications	76
8.6.1	Download the Google Service Files from Firebase	76
8.6.2	Configure Push Notification in DCEM	78
8.6.3	Receiving a Push Notification	78
8.7	App Versions	79
8.8	AuthConnector	79
8.9	Preferences	80
9.	RADIUS	80
9.1	Without RADIUS Challenge	81
9.2	With RADIUS Challenge	81
9.3	NAS-Clients	82
9.4	Preferences	82
9.5	RADIUS Login with One Time Passcode	83
9.6	RADIUS Attributes	84
9.7	RADIUS Connector	85
10.	OTP Token	85
10.1	Configure OTP Token	85
11.	REST-Web Services	85
11.1	Using the Existing "LibRestDcClient" for JAVA	86
11.2	Creating a New "LibRestDcClient" for other Programming Languages	87
11.3	Demo of a Simple REST-Web Services Application	87
12.	SAML	87
12.1	Preparing DCEM to be an Identity Provider	87
12.1.1	DCEM SAML Trust Certificates	87
12.1.2	Setting Up SAML Preferences	89
12.1.3	Downloading the Id Provider Metadata File	89
12.1.4	Adding a Service Provider	89
12.2	Customizing the SAML Web Pages	94
13.	OpenID	94
13.1	Preparing DCEM to be an OpenID authentication server	95
13.1.1	Enable OpenID/OAuth in the Cluster Configuration	95
13.1.2	DCEM OpenID Certificate	95
13.1.3	Setting Up OpenID Preferences	96
13.1.4	Add an OpenID Client	97
13.1.5	Claims	98
13.2	Customizing the OpenID Web Pages	99

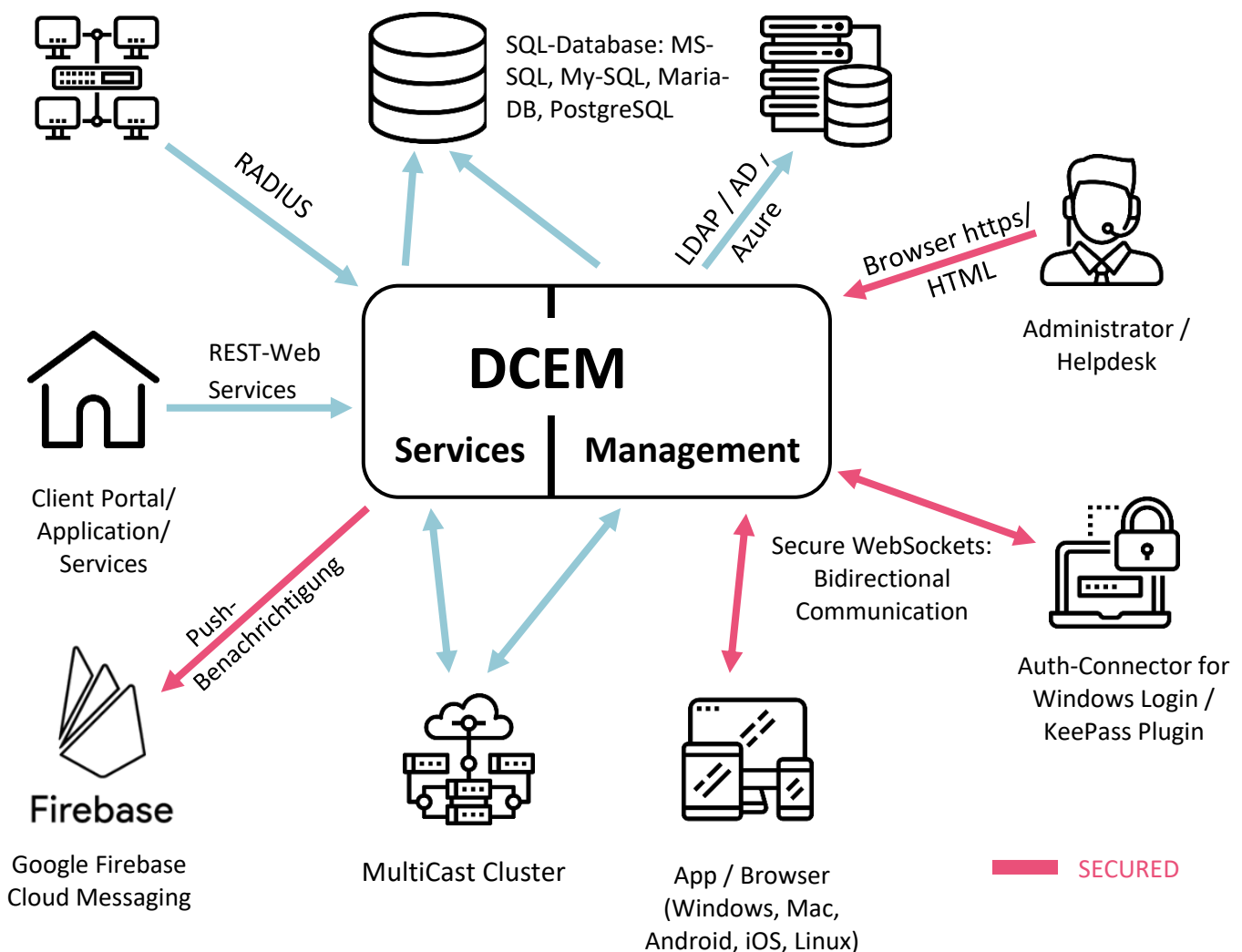
14.	Database Archive	99
15.	UserPortal	100
15.1	Configuration	100
15.1.1	General Settings	100
15.1.2	Configuration of the Visible Elements	100
15.1.2.1	<i>Visible Views</i>	100
15.1.2.2	<i>Views requiring multi-factor authentication</i>	101
15.1.2.3	<i>Visible Actions</i>	101
15.1.2.4	<i>Actions requiring multi-factor authentication</i>	101
15.1.3	Captcha Konfiguration with Google reCAPTCHA v2	101
16.	Licencing System	101
16.1	Applying for a New Licence Key	102
16.2	Adding a Licence Key	103
16.3	Viewing the Licences	103
17.	Logging	103
17.1	Configuration	103
17.2	File Output	103
17.3	SysLog Output	104
17.4	Enabling the SysLog	104
18.	PasswordSafe	104
18.1	DoubleClue PasswordSafe Extension for Browsers	105
18.2	Configuration of Applications	105
18.3	Import and Export Applications	105
18.4	Add Applications	106
18.4.1	Application	106
18.4.2	Actions	107
19.	Additional Services	111
19.1	PortalDemo	111
19.2	Credential Provider for Windows	111
19.3	HealthCheckDetector	111

1. Introduction

DoubleClue Enterprise Management (DCEM) is the central component of the DoubleClue platform. It is an open-source software developed by the HWS-Gruppe in Neustadt an der Aisch, Germany, and published under the [GPL3 license](https://www.gnu.org/licenses/gpl-3.0.html). It can be downloaded at <https://doubleclue.com>. The code is published on [Github](https://github.com/doubleclue).

One advantage of the cluster is that it works as point of contact for both central services and infrastructure management (users, devices, nodes, settings etc.). It possesses a comprehensive authorization system through which roles and access rights can be assigned to the users. In addition, DCEM can connect to various third-party services through known security standards and interfaces such as SAML, RADIUS or OpenID.

The following scenario demonstrates possible components of DCEM and the areas with which they communicate:




2. Installation & Launch

2.1 Requirements

2.1.1 Hardware Requirements

- RAM: Minimum of 4 GB - depending on the number of user logins per hour
If you have more than 200 user logins per hour, we suggest 8 GB.
- Hard drive: Minimum of 20 GB
- Operating system: Runs on Windows and Linux 64-Bit
- Network ports: 443, (optional) 8000, 8001 and 8002

You can set the ports for the various services and connections in DCEM under "System" -> "Cluster Configuration".

 Port 443 is the default port for the Apps. This port on this server has to be reachable from the internet. Please enable this incoming port in your Firewall.

The software runs from Windows 7 and Windows Server 2008 onwards and was tested on Windows Server 2016.

It also runs on Linux distributions with 64-bit and was tested on Linux Ubuntu Server 16.04.2.

Further versions can be specifically tested on request.

2.1.2 Database Requirements

DCEM comes with a built-in Embedded Database. The Embedded Database has the same features as the external databases but it supports only one DCEM node.

External database types:

- MYSQL Tested version: MYSQL vers.5.7
- MARIADB Tested version: MYSQL vers.15.1 Distrib 10.1.23 - MariaDB
- MSSQL Tested version: Microsoft SQL Server 2008
- PostgreSQL Tested version: PostgreSQL 11

These database types are currently supported. Further database types can be integrated and tested on request.

Required Storage Space for Database

Item	Average Storage Required	Comments
Minimum Storage needed for program	20 Mbyte	This is the minimum storage required for installing DoubleClue
User	1.5 KByte	Per registered user
Device	1.5 KByte	Per device record – each device (Smart Phone, FID etc.) requires a device record

History	300 Bytes	Per entry - every change made by an administrator and several of those made by users are recorded in the history record. You can set the “Duration for History Archive” in the Administration preferences to limit the amount of stored entries.
Reporting	500 Bytes	Per record. Every login attempt will create at least one record in the Identity & Access Reporting. You can set the “Duration for Report Archive” in the Identity Management preferences to limit the amount of stored entries.
CloudSafe	350 Bytes + file size	Per uploaded file. In addition to the default storage that is needed per file, the size of the file content is added.
Push Approval	250 Bytes	Per Push Approval. You can set the “Duration for Push Approval Archive” in the Identity Management preferences to limit the amount of stored records.

2.2 Installation Information

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

You will receive two installation packages, one for Windows (package name: “**DCEM-X.X.X.exe**” – X.X.X. stands for the version number of the file) and one for Linux (package name: “**DCEM-Linux-X.X.X.tar.gz**”). Extract the respective file in the storage location of your choice.

The installation directory name is “**DCEM**”.

DCEM runs 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.

2.3 Installation Process

The setup configures the database connection and initializes the database tables for DCEM. It also sets the password for the DCEM administrator “SuperAdmin”.

Settings specified in the setup are saved in the file “**DCEM_HOME/configuration.xml**”.

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

⚠ Port 8443 must not be used by any other application at the time of the setup!

2.3.1 Installation with Windows

Start the setup by executing the file “**DCEM-X.X.X.exe**”.

You can choose how you would like to install DCEM:

1. “Installation on the first DCEM cluster node”:
This option needs to be selected if you install DCEM for the first time.
2. “Update current DCEM cluster node”:
This option needs to be chosen if there is a new version of DCEM and you would like to update the old one.
3. “Installation on a further node”:
It needs to be selected if you would like to have a further installation of DCEM. An upload of the configuration file of the first DCEM node is required.

After the necessary files have been copied to the directory, a command view will be shown. DCEM will now try to open your default browser and automatically start the setup configuration. Should the browser not open automatically, you can find the url to open the setup configuration in the command window. Copy it into a browser and start the setup.

The setup uses a secured HTTPS connection with a “self-signed” certificate. This will trigger a security alert in the browser during the connection process. Confirm this alert.

Then proceed with chapter [2.4 Database Configuration](#).

2.3.2 Installation with Linux

Open the console and navigate to the parent install directory. Enter “**tar -xvf DCEM-Linux-X.X.X.tar.gz**” to extract the file into the chosen directory. Then 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, see next chapter.

The setup uses a secured HTTPS connection with a “self-signed” certificate. This is why a security alert is shown in the browser during the connection process. Confirm this alert.

It can happen that when running DCEM or the DCEM setup on Linux, the process can suddenly stall or even come to a standstill. This is often caused by the random generator being blocked as not enough entropies to generate cryptographic randomness are available. In such a case, we would advice to instal Haveged to create additional entropies. You can install Haveged by entering the following commands into the command-line:

- „sudo apt-get update“
- „apt-get install haveged“

These problems mainly occur on new linux machines.

Then proceed with chapter [2.4 Database Configuration](#).

2.3.3 Installation with a Headless Operating System

If you use a headless operating system, enter the following URL:

https:// --host name/IP of the server-- :8443/setup

The setup uses a secured HTTPS connection with a “self-signed” certificate. This is why a security alert is shown in the browser during the connection process. Confirm this alert.

Then proceed with chapter [2.4 Database Configuration](#).

2.3.4 Running Installation again

Should it be necessary to run the setup again, open the folder “**DCEM/bat**” if you use a Windows operating system. Stop the Service with “**stopDcemService.bat**”. Then execute the file “**runSetup.bat**”

For Linux, go to the directory “**DCEM/sh**” and stop the Daemon with “**stopDcemDaemon.sh**” first, then execute the file “**runSetup.sh**”.

 The setup cannot be started as long as DCEM is running.

2.4 Database Configuration

DCEM requires an SQL database in order to run.

You may choose between a pre-installed Embedded Database or the previous installation of an external SQL database.

2.4.1 Embedded Database

Setup - Configuration

Database Configuration

Create Database

Create Database Tables

Type *

Embedded-Database

JDBC-URL

jdbc:derby:dcem_db;collation=TERRITORY_BASED:PRIMARY

Configure URL

Database Name *

dcem_db_Kerstin

Administrator Name *

root

Administrator Password

••••

DoubleClue Node Name *

001N088


Save

Local configuration file stored at: C:\Users\kerstin.baumann\DCEM_HOME\configuration.xml


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

DoubleClue Node Name:

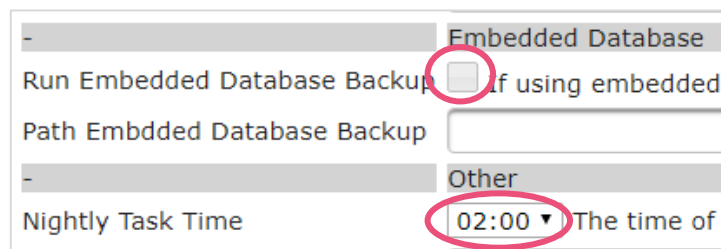
By default, the Node Name will be your computer or host name. If none is available, it will be the IP address. You can change the Node Name to any other name as long as it is globally unique for the DoubleClue cluster.

 The Embedded Database does not support multiple DCEM nodes or multi-tenants!

2.4.1.1 Backup of the Embedded Database

 Please note that this configuration can only be carried out **after the setup has been completed and DCEM is running.**

To enable an automatic backup of the Embedded Database, go to main menu item “System”, sub menu “Preferences” and scroll to “Embedded Database” at the bottom.



-	Embedded Database
Run Embedded Database Backup	<input type="checkbox"/> If using embedded
Path Embedded Database Backup	
-	Other
Nightly Task Time	02:00 ▼ The time of

Tick the check box next to “Run Embedded Database backup” to do a backup of the Embedded Database on every “Nightly Task Time”. You can enter a “Nightly Task Time” under the item “Other”.

Enter a path for the Embedded Data Base backup next to “Path Embedded Database Backup”.

 During the backup process, writing into the database will be blocked!

2.4.1.2 Creating Database Tables

Setup - Configuration

Database Configuration
Create Database
Create Database Tables

Create-Tables Administrator Name: *
sa
?

Create-Tables Administrator Password:

SuperAdmin Password: *

Confirm SuperAdmin Password: *

DoubleClue Server URL *
https://doubleclue.online

Create Tables

Back

Super-Administrator Password:

Specify the password for the super administrator of DCEM. The username of the super administrator is always "SuperAdmin".

DoubleClue Server URL:

The DoubleClue Server URL is the URL for user to connect to your DoubleClue installation from an external location.

2.4.2 External Database

Setup - Configuration

Database Configuration
Create Database
Create Database Tables

Type *
MariaDB

JDBC-URL *
jdbc:mysql://001L0202:3306
Configure URL

Database Name *
dcem_db

Administrator Name *
root

Administrator Password

DoubleClue Node Name *
001L0034

Save

Local configuration file stored at: C:\Users\kerstin.baumann\DCEM_HOME\configuration.xml

Type:

Chose the type of external database you would like to use. At this time, DCEM supports the following data bases:

- MYSQL Tested version: MYSQL vers.5.7
- MARIADB Tested version: MYSQL vers.15.1 Distrib 10.1.23 - MariaDB
- MSSQL Tested version: Microsoft SQL Server 2008
- PostgreSQL Tested version: PostgreSQL 11

URL:

The registered URL has to be in JDBC format. If the URL is known to you, you can enter it directly. If the URL is not known to you, you can create it via the button "Configure URL".

Administrator Name / Administrator Password:

These specifications are needed in order that DCEM can authenticate itself to the database. The password is always saved in encrypted form.

DoubleClue Node Name:

By default, the Node Name will be your computer or host name. If none is available, it will be the IP address. You can change the Node Name to any other name as long as it is globally unique for the DoubleClue cluster.

Save:

It is checked upon saving if a connection to the database can be established. Respective messages are shown (connection successful, connection failed, wrong password etc.).

2.4.2.1 *Creating Database or Schema*

Setup - Configuration

Database Configuration
Create Database
Create Database Tables

Database-Administrator Name:

root

?

Database-Administrator Password:

.....

Create Database

◀ Back

If no database with the given name has existed as yet, it will now be created. If the database was created with a database tool beforehand, this step will not be necessary.

Database Administrator:

The Database Administrator needs to have the rights to create a database. In order to establish the connection to the database, user name and password of the database administrator have to be entered. This data is only needed once for authentication and will not be saved.

2.4.2.2 *Creating Database Tables*

Database tables are created via “Create Database Tables”.

Create-Tables Administrator Name:

The Create-Tables Administrator needs to have the rights to create database tables.

Super-Administrator Password:

Specify the password for the super administrator of DCEM. The username of the super administrator is always “superadmin”.


Create Tables:


By clicking on the button “Create Tables”, the file “**configuration.xml**” in the folder “**DCEM/DCEM_HOME**” is created. Every time the action is performed, a new version of the file is created. The old version is saved within the same folder under the name “**configuration.xml.date-time**”.

If no error messages are shown while the database is created, you will get a message in which the path to the storage location of the file “**configuration.xml**” is shown. Save this file in a secure location. It is needed to add further nodes.

You can now close the setup and finish the installation of DCEM. After closing the setup, DCEM will start. This process will normally take around 30-50 seconds but may occasionally need more time. If you try to open the DCEM link in this time, you will receive an error. If you want to ensure that DCEM has already started or suspect that an error might have happened during the start, check the dcem.log file. You can find it in the DCEM installation folder under DCEM_Home > logs.

Sometimes it is necessary to start the DCEM services manually. Go to your Installation folder under **bat** and execute the **startDcemService.bat**.

 The setup has to be completed and closed before DCEM can be started.

 Please note: For Linux operating systems, go on with chapter [2.5 Installing DCEM as a Daemon](#).

If you use Windows as an operating system, please proceed with chapter [2.7 Login to DCEM](#).

2.4.2.3 Configuring a PostgreSQL Database

Tested with PostgreSQL version 11.

1. Create a new database for DoubleClue in PostgreSQL. For example: dcem_db.
2. In DoubleClue Setup, choose „PostgreSQL“ as database type.
3. Add a slash („/“) to the JDBC-URL. For example: jdbc:postgresql://yourhost:5432/
4. Enter the name of the PostgreSQL schema name in the field ‘Database Name’. The schema will be automatically created to the PostgreSQL database.
5. Enter ‘Administrator Name’ and ‘Password’ and ,Save’ the changes.

Setup - Configuration

Database Configuration

Create Database

Create Database Tables

Type *

PostgreSQL

JDBC-URL *

jdbc:postgresql://hws001S0202:5432

Configure URL

Database Name *

dcem_db

Administrator Name *

postgres

Administrator Password

••••

DoubleClue Node Name *

001L0034

Save

Local configuration file stored at: C:\Users\kerstin.baumann\DCEM_HOME\configuration.xml



PostgreSQL is a case sensitive database. Therefore, all entries and searches have to be case sensitive.

2.5 Installing DCEM as a Daemon

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**”.

You can always stop or start the Daemon again by executing the file “**stopDcemDaemon.sh**” or “**startDcemDaemon.sh**”.

2.6 Database Migration

Due to the constant development of our DoubleClue software, we regularly publish new versions. In order to migrate an older version to the current one, a database migration is required.

2.6.1 Migration with Windows

If you use a Windows operating system, just start the DoubleClue Windows Installer and follow the setup steps.

Please note that before the migration you should do a database backup. If you use the Embedded Database, only copy the folder “**DCEM_HOME/EmbeddedDB**” to a new, safe directory. For other database types, please refer to the database manuals of the vendor.

Proceed with chapter [2.6.3 Migration Process](#).

2.6.2 Migration with Linux

Please note that DCEM must not run during the database migration process. Therefore, please go to the folder “**DCEM/sh**”, then click on “**stopDcemDaemon.sh**” to stop the Daemon.

Before the migration you should do a database backup. If you use the Embedded Database, only copy the folder “**DCEM_HOME/EmbeddedDB**” to a new, safe directory. For other database types, please refer to the database manuals of the vendor.

Now execute the file “**runSetup.sh**”. Choose a Database Type and click on “Save”. The configuration dialogue will tell you that a migration is required.

Proceed with the next chapter.

2.6.3 Migration Process

Setup - Configuration

Database Configuration | Create Database | Create Database Tables | Database Migration

Migration required

Connection successful
Database already exists.
Database exists, please proceed with DB Migration, next step.

Type: *

JDBC-URL: * **Configure URL**

Database Name: *

Administrator Name: *

Administrator Password:

Save

Local configuration file stored at: C:\temp\DCEM_HOME\configuration.xml

! Follow the instructions to complete the migration process:

Setup - Configuration

Database Configuration | Create Database | Create Database Tables | Database Migration

Create-Tables Administrator Name: * ⓘ

Create-Tables Administrator Password:

Module ID	Module Name	Current DB Version	Update to DB Version
system	System	3	4
identity-management	Identity-Management	2	3

Start Migration

The migration has been successful if the text “No records found” is shown in the column “Module ID”. Click on “Close DoubleClue Setup” to conclude the database migration.

2.7 Login to DCEM

2.7.1 Login with User Name and Password

The URL for the login to DCEM is:

https:// --host name/IP of the server-- :8443/dcem/mgt/login.xhtml

Log in with the user name “SuperAdmin” and the password specified for the super administrator during setup.

After the login you are able to administrate DCEM.

2.7.2 Login with DoubleClue Multi-Factor Authentication

This feature can be activated if you would like your operators to log into DCEM with DoubleClue MFA.

An activation is recommended if you install DCEM in the cloud.

2.7.2.1 Activation of DoubleClue MFA

If you want to log into DCEM with DoubleClue MFA (Multi-Factor Authentication), go to "Identity & Access" -> "Policies" after completing your first login and adjust the DCEM Management Policy accordingly. Disable login by password and select the multi-factor authentication methods you want to use. Under "Standard Auth Method", you can select one of the selected authentication methods as the default preferred method.

The screenshot shows the 'Edit' window for a policy named 'DCEM-Management'. The settings are as follows:

- Name:** DCEM-Management
- Deny Access:** ☐
- Refrain MFA within Timeout:** ☐
- Remember Browser Fingerprint:** ☐
- Session Authentication:** ☐
- Timeout (Hours):** 0
- Network Bypass:** 172.16.0.0-172.16.255.255;
- Allow Auth Methods:**
 - ☒ Password
 - ☒ SMS Passcode
 - ☒ Voice Message
 - ☒ Hardware Token
 - ☒ DoubleClue Passcode
 - ☒ Push-Approval
 - ☒ QrCode Approval
 - ☒ FIDO Authentication
- Default Auth Method:** (None)
- Use MFA at Windows Unlock:** ☐

At the bottom, there are 'OK' and 'Cancel' buttons.

For more information about changing the management of authentication methods, see [Chapter 7 Authentication Methods and Policies](#).

2.8 Log into DCEM

2.8.1 File "configuration.xml"

Confidential data is saved in the database in encrypted form. In order to protect this data, the file includes a database key which is needed for decrypting the data.

Should the file "**configuration.xml**" be lost, the database cannot be used anymore.

2.8.2 Folder “DCEM_HOME”

Next to the file “**configuration.xml**”, you will find the following folders here which are automatically created and filled:

“certs”	for certificates
“jna”	for log files
“logs”	for log files

It is necessary that the DCEM account has writing rights for the folder “**DCEM_HOME**” in order to write into the files and read from them.


3. DCEM System Main Menu

In the main menu under ‘System’, you can configure the DCEM connection services, cluster nodes and tenants. This main menu item will only be visible if you log into DCEM on the main tenant. Administrators only holding DCEM access for one of the sub-tenants will not see this item.

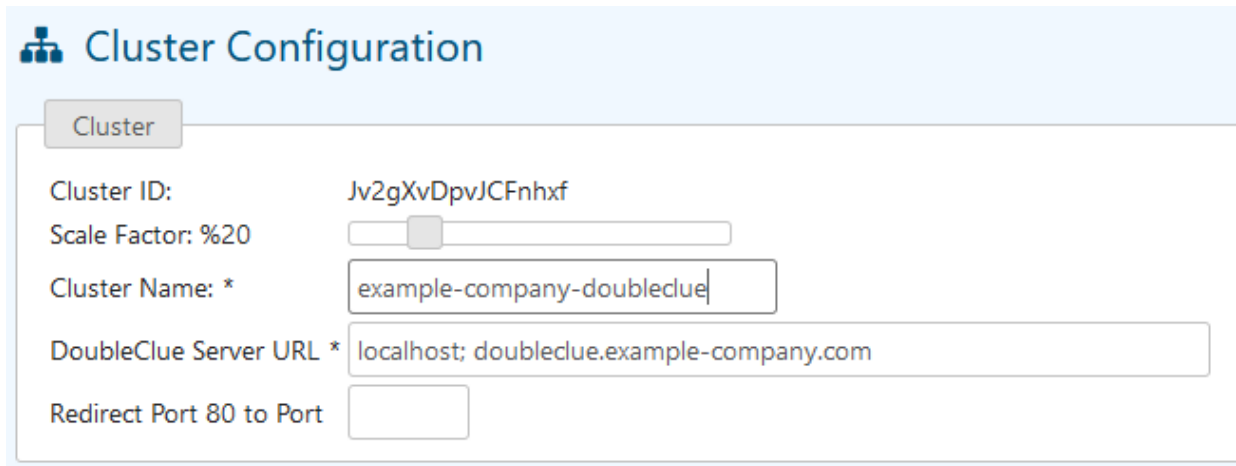
3.1 Cluster Configuration

DCEM runs in a cluster. This cluster consists out of several interconnected independent servers (called “nodes”). For load balancing, a load balancer is used. If a server fails, there will be no whole system breakdown as the load is evenly distributed between the remaining servers. The load balancer is no element of the DCEM platform. You need to install a software or hardware balancer for this task.

In the Cluster Configuration, you can define the general settings and the settings of the Connection Services for this cluster.

 Any changes in this configuration will require a DCEM restart.

3.1.1 General Settings



Cluster Configuration

Cluster

Cluster ID: Jv2gXvDpvJCFnhxf

Scale Factor: %20

Cluster Name: * example-company-doubledclue

DoubleClue Server URL * localhost; doubledclue.example-company.com

Redirect Port 80 to Port

3.1.1.1 Cluster ID

The Cluster ID is a random number that is automatically assigned during the installation process that cannot be changed.

It is used for several purposes as follows:


- a) For licensing DCEM
- b) When registering DCEM at the DoubleClue.online Dispatcher
- c) DoubleClue Apps send the Cluster-ID on the Web-Socket connection URL. This may be used by Load-Balances to immediately refuse in coming connections with a wrong Cluster-ID.

3.1.1.2 Scale Factor

With the “Scale Factor” you can set how much capacity of the server is reserved for DCEM. The higher the factor, the more system resources are available for DCEM. If the scale factor is too high, there could be an impairment of other programs on the server.

The maximum of parallel connections allowed is 20000 connections. The scale factor is set proportionally. If, for example, the scale factor is set to 20%, the maximum amount of connections is 4000.

3.1.1.3 Cluster Name

 Before you can change the Connection Services in the Cluster Config., you need to name the Cluster. Therefore, fill a Cluster Name into the respective field.

3.1.1.4 DoubleClue Server URL

The DoubleClue Cluster URL the Host-Name for DCEM without the tenant sub-domain name. For example if the DCEM URL is <https://doubleclueone.online:8444/dcem/mgt>, then you should enter “doubleclueone.online” in this field. The tenants URLs will be “<https://xxx.doubleclueone.online:8444/dcem/mgt>”, xxx being the sub-domain name.

You can enter multiple host-names separated by a **semi-colon**. For example “doubleclueone.online;localhost”. The name is case insensitive. All other host-names will be rejected with Status code (401) Unauthorized.

3.1.2 Connection Services

DoubleClue supports several Connection Services. In the Cluster Configuration, you can activate, deactivate and adjust the settings for the different Connection Services. Three of them, the Management Connection, the REST-Web Services Connection and the Web Sockets Connection, are necessary for executing DCEM and will be enabled by default.

3.1.2.1 Management Connection

The Management Connection is the connection from the browser to DCEM. It always has to be secured with SSL/TLS. A “self-signed” certificate for this connection is created during the setup. If needed, a new certificate can be uploaded (see [3.5 Uploading New KeyStore](#)).

3.1.2.2 REST-Web Services Connection

The REST-Web Services Connection is the connection between DCEM and your server. This connection is an HTTP/HTTPS connection. You will find further information in chapter [11. REST-Web Services](#).

As this usually is an internal connection, it does not need to be secured with SSL/TLS. If you wish to secure it, you need to create a KeyStore for this connection as described in chapter [3.3.1 Adding KeyStores](#), or you upload a certificate as described in chapter [3.5 Uploading New KeyStore](#).

3.1.2.3 Web Sockets Connection

The Web Sockets Connection is the connection between DCEM and the end user app. Apps are available for Android, iOS and Windows operating systems.

The connection from end user (app) to DCEM or the load balancer always has to be secured with SSL/TLS.

The connection from the internal load balancer to DCEM does not need to be secured in this case. If it should be secured nonetheless, you need to create a KeyStore for this connection as described in

chapter [3.3.1 Adding KeyStores](#), or you have to upload a certificate as described in chapter [3.5 Uploading New KeyStore](#).

3.1.2.4 RADIUS Authentication and Accounting

RADIUS is an authentication, authorization and accounting protocol between a network client and a server. DoubleClue can be set up to act as a RADIUS server. The authentication of the end user is done via user name and password. DCEM enhances the features and security of RADIUS by a Two-Factor Authentication which requires an additional confirmation by the end user via app or other MFA methods.

For more information to set up DoubleClue as a RADIUS server, check chapter [9 RADIUS](#).

3.1.2.5 SAML

SAML (Security Assertion Markup Language) is an open standard for the exchange of authentication data between an Identity Provider and a Service Provider. It is an XML-based markup language for security affirmations. The most important use SAML is as a web browser single sign-on (SSO). DoubleClue can be employed to work as an Identity Provider for SAML.

For more information how to set up DoubleClue as a SAML Identity Provider check chapter [12. SAML](#).

3.1.2.6 OpenID/OAuth

OpenID is an open standard and authentication protocol, which extends upon OAuth 2.0. It is utilized for the exchange of authentication data between an OpenID authentication server and an OpenID Client. DoubleClue can be set up to act as an OpenID authenticator.

For more information check chapter [13. OpenID](#).

3.1.2.7 UserPortal

By default, UserPortal is enabled and uses the settings of the Management Connection. For more information about UserPortal, check chapter [15 UserPortal](#).

3.1.3 Connection Service Settings

You can edit the settings for the different Connection Services. Always remember to save the changes before leaving the menu. You will then have to restart DCEM for the changes to become active.

3.1.3.1 *Same as other Service*

If you want one of your connection services to share the same settings as another one, you can simply set this service as “Same as other Service” under edit. Notice that when you change the settings of the service set as template, all services sharing its setting will change as well.

3.1.3.2 *Port*

Enter the port number you want to use for the different services. The default ports are:

Management:	8443
REST Web-Services:	8001
Smart-Device Web-Sockets:	443
RADIUS Authentication:	1812
RADIUS Accounting:	1813
SAML:	Same as Management
OpenID/OAuth:	Same as Management
Health Check:	Same as Management
UserPortal:	Same as Management

3.1.3.3 *Secure with SSL/TSL*

Choose whether you want the services to be secured with SSL/TSL. It is mandatory to activate this option for the Management Connection and the Web-Sockets-Connection, but it isn't needed for the REST-Web Services Connection which is an internal connection and for which it is by default disabled. It is further advised to activate SSL/TSL for all further enabled connection services.

3.1.3.4 *Enable*

Enable or disable the service.

3.1.3.5 *External Port*

Enable a port specifically for external use in case you want to block the main port from external access via firewall or the like. This field is optional.

3.2 Cluster Nodes

The first cluster node is automatically configured during the setup. If required, the node's name can be changed (see chapter [3.2.2.1 Specifying a Node Name](#)).

3.2.1 Installing Further Nodes

Install DCEM as described in chapter [2.2 Installation](#).

Then copy the file "**DcemInstallation/DCEM_HOME/configuration.xml**" and save it under the same path in the new node.

If the original "**configuration.xml**" is changed, it has to be changed in every node.

3.2.2 Adding a Cluster Node

You can add a cluster node under "System" > "Cluster Nodes". Each cluster node needs a node name.

3.2.2.1 *Specifying a Node Name*

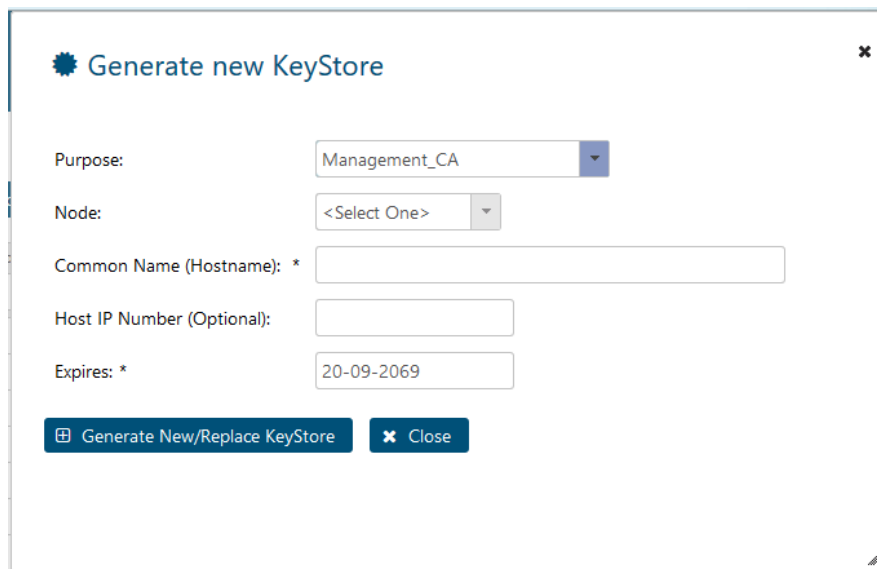
You can change a Node Name by simply selecting the node and clicking on "Change". Then enter the new Node Name in the dialogue. Each Node Name must be unique.

When you want to change the Node Name of the first Node, which was automatically created during set up, you need to ensure that the new name is also changed in the **configuration.xml**-file. If the Node Names for the first node in the configuration.xml and in DCEM are not the same, you will not be able to start DCEM.

You can change the Node Name either directly in the configuration.xml, by altering the entry `<nodeName> --Node Name-- </nodeName>` or by executing the DoubleClue Setup once more and changing it in the Setup Interface.

3.2.2.2 Add KeyStore


Add a new Management_CA KeyStore as described in chapter [3.3.1 Adding KeyStores](#) and select the new Node.



Alternatively, you can upload a new KeyStore. Download an already existing Management_CA KeyStore as PKCS#12 and then reupload it. You need the KeyStores password to upload it. The password is the same as that of the downloaded KeyStore which you can view in the KeyStore menu.

3.2.2.3 Confirmation

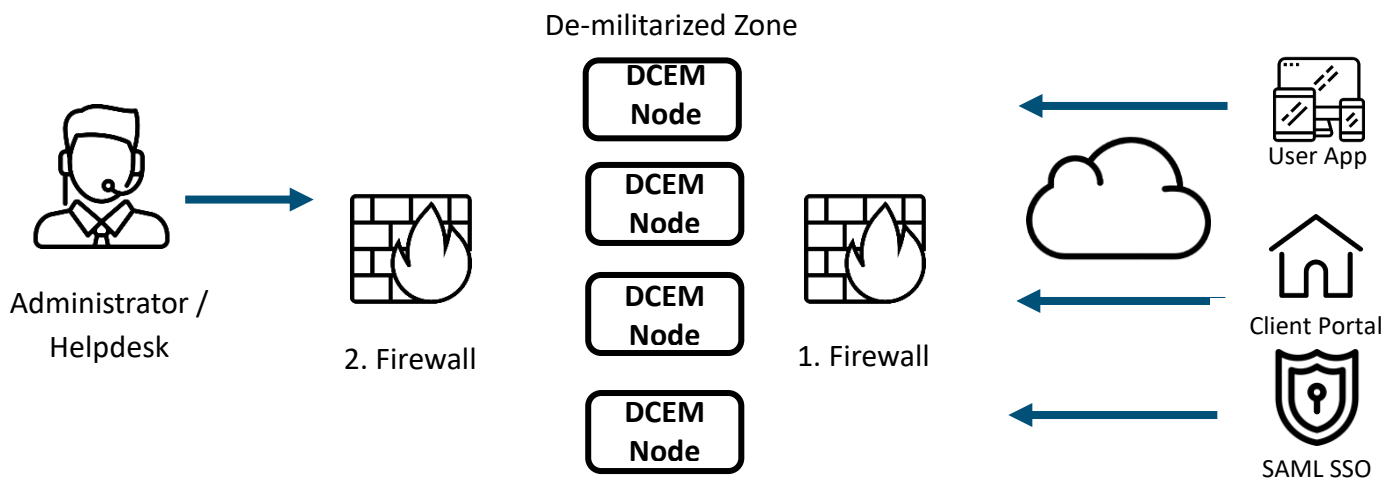
If the new node was installed and started correctly, it is now shown under the sub menu item “Cluster Nodes” and the status “Active”.

 The service is terminated if no node name is found. Check if the node name was specified correctly as described in chapter [3.2.1.1 Specifying the Node Name](#).

3.3 KeyStores

For every connection that shall be secured with SSL/TLS (see chapter [3.1 Cluster Configuration](#)), a KeyStore is needed. The certificate, the private key and the public key are saved in the KeyStore. The KeyStore is necessary in order to establish a connection secured with SSL/TLS. A SSL/TLS connection needs more processing power than an unsecured connection.

The certificate can either be issued by an official Trust Center (CA), or a “self-signed” certificate is created. By mapping the different services to different key stores, you can also assign them to different Cluster Nodes. This way you can, for example allow Management Access to DCEM only from internal connections, while Service connections are allowed from external sources. The service connection in such a scenario needs to be located in the demilitarized zone.



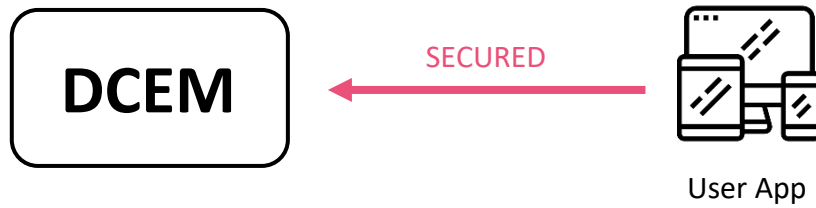
3.3.1 Adding New KeyStores

KeyStores can be created in the "Keystore" menu (main menu: "System"). Each keystore needs a "Purpose". There are different purposes for the different connection services available. The specification of an IP address is optional and is only required if the IP address is to be used as the node name.

3.4 Possible Connections to the End User

Regarding the connection to the end user, it has to be differentiated where the connection should be terminated. There are the following possibilities:

3.4.1 SSL/TLS from the End User Terminated at DCEM



3.4.1.1 Purpose: DeviceWebsockets_CA

If the connection from the end user is terminated at DCEM, it is always secured with SSL/TLS by default.

3.4.1.2 Creating the SDK Configuration File

Switch to main menu item “Identity & Access”, sub menu “Versions” and create the SDK configuration file. Use the following URL for this:

wss:// --host name/IP of the server-- : --port of the server-- /dcem/ws/appConnection

Switch to main menu item “Identity & Access”, sub menu “Versions” and click on “Generate SDK Configuration”. A dialog will open. In the Dropdown Menu under “SSL/TLS TrustStore Certificate” choose “Dcem CA_Root Certificate” if you want to use the DoubleClue Dispatcher together with our DoubleClue App.

Then click on “Save and Download”. See chapter [6. Connection Scenarios](#) for further steps to take.

Generate SDK Configuration

DCEM Server URL Reachable for App

wss://yourhost.com/dcem/ws/appConnection

UserPortal URL

https://yourhost.com/dcem/userportal

SSL/TLS TrustStore Certificate

Choose Certificate Source: DCEM 'CA_Root Certificate'

Issuer	Valid Till
CN=Jv2gXvDpvJCFnhxf	2119-08-09 10:17:23.0

☒ DCEM 'CA_Root Certificate'
☐ Upload external trustStore in PEM format
☐ Get certificates from URL

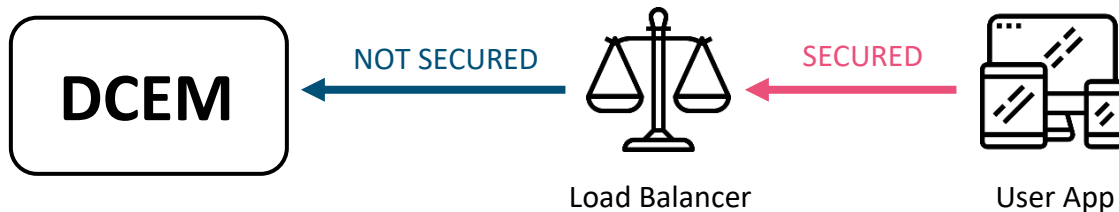
Save and Download

Cancel

If you want to use your own App, please download the SDK configuration file and implement it in your app (see Developer's Guides for the app installation: [DC_Dev_Guide_Android.pdf](#) / [DC_Dev_Guide_iOS.pdf](#)).

⚠ The SDK configuration file can only be created in a Master DCEM, not in a tenant.

3.4.2 SSL/TLS from the End User Terminated at the Load Balancer and Unsecured to DCEM



3.4.2.1 Purpose: DeviceWebsockets_CA

In this case the SSL/TLS connection from the end user is terminated at the load balancer. The connection from the load balancer to DCEM will not be secured with SSL/TLS. DCEM needs no KeyStore for the DeviceWebsockets_CA.

3.4.2.2 Creating the SDK Configuration File

Switch to main menu item “Identity & Access”, sub menu “Versions” and create the SDK configuration file. Use the following URL for this:

wss:// --host name/IP of the load balancer-- : --port of the load balancer-- /dcem/ws/appConnection

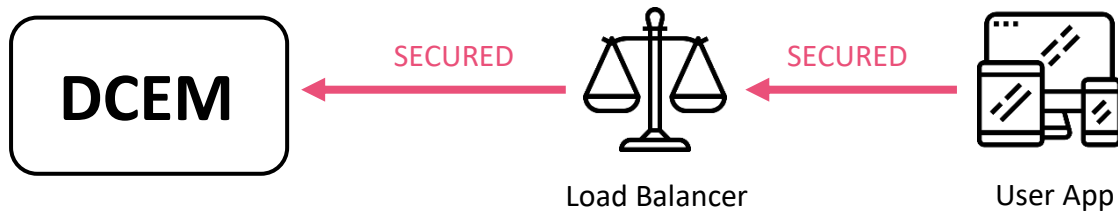
In the Dropdown Menu under SSL/TLS TrustStore Certificate choose “Get certificates from URL” and DCEM will automatically add the certificate from the chosen URL. Alternatively, you can choose “Upload external TrustStore in PEM format” and upload your certificates.

Download the file “**SdkConfig.dcem**” if you want to use the DoubleClue Dispatcher together with our DoubleClue App. See chapter [6. Connection Scenarios](#) for further steps to take.

If you want to use your own App, please download the SDK configuration file and implement it in your app (see Developer's Guides for the app installation: [DC_Dev_Guide_Android.pdf](#) / [DC_Dev_Guide_iOS.pdf](#)).

⚠ The SDK configuration file can only be created in a Master DCEM, not in a tenant.

3.4.3 SSL/TLS from the End User Terminated at the Load Balancer and Secured to DCEM



3.4.3.1 Purpose: DeviceWebsockets_CA

In this case the SSL/TLS connection from the end user is terminated at the load balancer. The connection from the load balancer to DCEM is additionally secured with SSL/TLS. DCEM needs a KeyStore for the DeviceWebsockets_CA. Here, the host name always has to be that of the respective node.

3.4.3.2 Download as PEM

Download the TrustStore for the Root_CA in PEM format under main menu item “System”, sub menu “Keystores” and save the file on the load balancer. This step is necessary in order that the secure connection between load balancer and server can be established.

3.4.3.3 Creating the SDK Configuration File


Switch to main menu item “Identity & Access”, sub menu “Versions” and create the SDK configuration file. Use the following URL for this:

wss:// --host name/IP of the load balancer-- : --port of the load balancer-- /dcem/ws/appConnection

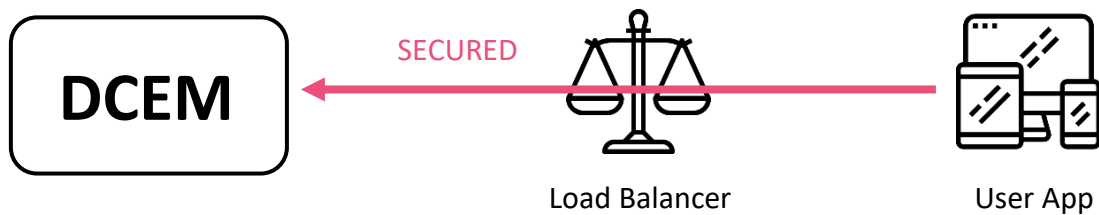
In the Dropdown Menu under SSL/TLS TrustStore Certificate choose “Get certificates from URL” and DCEM will automatically add the certificate from the chosen URL. Alternatively, you can choose “Upload external TrustStore in PEM format” and upload your certificates.

Download the file “SdkConfig.dcem” if you want to use the DoubleClue Dispatcher together with our DoubleClue App. See chapter [6. Connection Scenarios](#) for further steps to take.

If you want to use your own App, please download the SDK configuration file and implement it in your app (see Developer’s Guides for the app installation: **DC_Dev_Guide_Android.pdf** / **DC_Dev_Guide_iOS.pdf**).

 The SDK configuration file can only be created in a Master DCEM, not in a tenant.

3.4.4 SSL/TLS from the End User Terminated at DCEM with the Load Balancer (Passthrough)



3.4.4.1 Purpose: DeviceWebsockets_CA

In this case the SSL/TLS connection from the end user is terminated at DCEM and it is looped through a load balancer in the process. DCEM needs a KeyStore for the DeviceWebsockets_CA. Here, the host name always has to be that of the load balancer.


3.4.4.2 Creating the SDK Configuration File

Switch to main menu item “Identity & Access”, sub menu “Versions” and create the SDK configuration file. Use the following URL for this:

wss:// --host name/IP of the load balancer-- : --port of the load balancer-- /dcm/ws/appConnection

Select “Dcem CA_Root Certificate” in the dropdown menu if you want to use the DoubleClue Root Certificate as identification certificate for the DoubleClue App. If you want to use your own certificate, choose “Get certificate from URL” and DCEM will download the certificate automatically from your URL or “Upload external TrustStore in PEM format” and upload the files. See chapter [6. Connection Scenarios](#) for further steps to take.

If you want to use your own App instead of the DoubleClue App, please download the SDK configuration file and implement it in your app (see Developer’s Guides for the app installation: [DC_Dev_Guide_Android.pdf](#) / [DC_Dev_Guide_iOS.pdf](#)).

 The SDK configuration file can only be created in a Master DCEM, not in a tenant.

3.4.5 SDK Configuration File

The SDK file is created by the server. It includes the connection configurations as well as the public key of the cluster. Whether or not the connection is secured with SSL/TLS, it is checked if the SDK has the valid public key.

The SDK file is necessary for the following reasons:

- Specifying the connection target of the app
- Storage location for the public key of the cluster

3.5 Uploading New KeyStore

If you would like to upload a KeyStore with certificates instead of the DeviceWebsockets_CA created here, you can do this via "Upload New Keystore". You will need the KeyStore in PKCS#12 format and the respective password.

3.6 Cluster Network Communication

3.6.1 One Network

If all nodes are located in the same network, the default settings for Multicast can be used.

3.6.2 Several Networks with Multicast

If all routers are located in different networks, they have to permit Multicast in order to be able to use the default settings for Multicast.

By default, Multicast group 224.2.2.3 with port 54327 is used.

3.6.3 Several Networks without Multicast

If Multicast is not permitted, the default settings have to be set to TCP/IP.

For this you need to save the file "**x_HazelcastClusterConfig.xml**" in the folder "**DCEM_HOME**". Rename it to "**HazelcastClusterConfig.xml**".

DCEM reads the cluster configuration file "**DCEM_HOME/HazelcastClusterConfig.xml**". As long as there is no file with this name, a default configuration is used.

Like the file "**configuration.xml**", the file "**HazelcastClusterConfig.xml**" has to be copied to each associated server.

The following changes have to be made in the file "**HazelcastClusterConfig.xml**":

- 1) **<multicast enabled = "true">**
Set the value "true" to "false".
- 2) **<tcp-ip enabled = "false">**
Set the value "false" to "true".
- 3) **<interface> --IP of the network card-- </interface>**
Enter the network card IP of the server. This setting needs to be done on each server individually.

If there are several network cards on the server, copy the line for each network card and enter each IP once.

4) **<member> --host name/IP of the server-- </member>**

Copy the line for each server and enter the host name / the IP respectively. Any number of servers can be added.

If a new server is added, it has to be added in each file **"HazelcastClusterConfig.xml"** on each server.

3.7 Diagnostics

The diagnostics section gives an overview about the counters and values of your DoubleClue cluster. They are only available for the whole cluster, not for individual tenants. The values for different nodes are listed separately, but only when the respective node is online.

You can also view the System Values and Counters (but not the Static Values) as a graph, by selecting the entries you want to see and click on "Show Charts". If it doesn't work, please check in the System Preferences that monitoring is active. If you have only recently activated it, DCEM will only show you the current data.

You can download the current values as a json-file with the "Download File" button. You can further download the current logs as a .zip by clicking "Download Log Files". DoubleClue keeps log in 4 rotating log files of a size of 50 MB each.

The "Reset" button sets all the counters back to 0. Please be aware that this can't be reversed.

4. Administration

4.1 Home / Dashboard

The Dashboard gives you a general overview of the recent DoubleClue activities.

Should DoubleClue have created any alerts while running, you will find a list of these alerts here. Those alerts are further archived in the Reporting view.

Below you see an overview of the successful and unsuccessful logins per day, week or month. By clicking on one of the bars, you will be redirected to the Reporting view. Below it is a pie chart displaying the used authentication methods for the chosen time frame.

4.2 Users

4.2.1 Add Users

New users can register themselves in UserPortal or be imported from an Active Directory via the REST Web Services interface. DoubleClue supports Microsoft Active Directory, Microsoft Azure Active

Directory and LDAP, allowing users to be imported directly from these directories. In addition, administrators can manually create new users under Administration> Users.

4.2.2 User Login ID

It is not possible to add users with a login ID that contains any of the following characters:

!#\$%&'()*+/-;<=>?[]^`{|}~

Users that have been imported from an Active Directory can also log in with their UPN.

4.2.3 User Password

Local users require a user password. When registering via UserPortal, users can set their own password. If they are registered by an administrator, they can assign you a password that users can later change independently in UserPortal.

Domain users use their domain password.



Since domain users are synchronized with the Active Directory when logging in, it is not possible to create a special DoubleClue password for them. It is automatically overwritten at each log-in and replaced by the domain password.

4.2.4 Adding an Activation Code

Activation codes are required for the first activation of the DoubleClue app. After a new user account has been created, an activation code must be created for this user to activate the app.

There are four ways to do this:

1. Go to the main menu item "Identity & Access", submenu "Activation Codes" and click on "Add". Enter the user name in the corresponding field, choose the method to send the code and confirm the entry.
2. Go to the main menu item "Administration", submenu "User". Select the user(s) to whom you want to assign an activation code and click on "Create Activation Code". This procedure can also be selected for groups (main menu item "Administration", submenu "Groups").
3. Activation codes can also be added automatically through the REST Web Services interface or during the import of users from a domain.
4. Users can request an activation code themselves in the DoubleClue UserPortal under Device Management.

4.2.5 Phone and Mobile Number

The telephone and mobile number of users is only required if they want to use SMS and / or voice message as an authentication method (see chapter [7. Authentication Methods and Policies](#)).

If both numbers are recorded, DCEM will always use the landline for voice messages. If no landline number is registered for the user, it will instead dial to the mobile number.

For domain users, the phone and mobile numbers are automatically imported from the Active Directory. Users also have the option to enter a confidential telephone number via UserPortal. DCEM can use it to send SMS and voice messages, administrators, however, won't be able to see it.


For voice messages and SMS to be sent successfully, a valid country code has to be added to the number. However, if all your users phone and mobile numbers use the same country code, you can configure a 'Default Phone Country Code'. In this case, all phone and mobile numbers who don't have a country code attached to them will automatically use the default country code.

4.2.6 Private E-Mail Address


You can add a private e-mail address to user entries. In this case, when requesting an activation code via email, a mail will be sent at both, the users private and the users regular email address. This feature enables the administrator to send an activation code to users that have no access to their company email address. The private email address can't be imported from an active directory but needs to be added locally in DCEM.

4.2.7 Reset User Password

If a local user has forgotten their password, an administrator can reset the password in the "User" menu by clicking the button "Reset Password". If a user can't see the password, check the "Privileges" if "reset_password" has been activated for this administrator's role.

 The new password is not automatically forwarded to the user! The administrator has to send it to them in another way (e-mail, messenger etc.).

The user can then change the password in UserPortal.

 The password of domain users cannot be resetted via DCEM. This must be done via the corresponding Active Directory.

4.2.8 Suspended Users

If users too often enter an incorrect password, their account will be temporarily suspended. As long as an account is suspended, the user can't log into it or use it to log into other services protected with

DoubleClue. An administrator can check if a user is suspended in DCEM under “Administration” > “Users” and see how long the suspension will last.

The number of times a user can try to enter the password before the account is suspended can be defined at "Administration"> "Preferences"> "Password Max Retry Counter". You can set the duration for how long the user account will be suspended at “Administration” > “Preferences” > “Duration of Account Suspension”.

Alternatively, an administrator can re-enable a suspended user manually in the administration menu under "User" in the same way as they can enable a disabled account. When an administrator re-enables a user, all silent login keys for this user will be revoked. If the users have activated “Stay logged in” for any of their login scenarios, this will thereby be reset.

If a SuperAdmin has lost its access and cannot be unlocked by another administrator or wait till the suspensions is expired, you can restore the access via the backdoor (see chapter [4.4 Recover SuperAdmin Access](#)).

4.2.9 Disabled Users

An administrator can disable a user in DCEM under “Administration” > “User”. The user’s status in the Column “Disabled” will then change to true. Disabled users can’t access DoubleClue or any services that are protected by DoubleClue as long as their account is disabled.

An administrator can reenale a disabled user by selecting the user in the list and clicking the ‘Enable’ button. When an administrator re-enables a user, all silent login keys for this user will be revoked. If the users have activated “Stay logged in” for any of their login scenarios, this will thereby be reset.

If a SuperAdmin has been disabled its access and cannot be unlocked by another administrator, superadmin access needs to be restored via a backdoor (see chapter [4.4 Recover SuperAdmin Access](#)).

4.2.10 User Picture, Country and Language

If a user picture, living country or language is saved among the information in your active directory, this information can be exported to DoubleClue. It will then be displayed in the information about the user. It is also possible to define a language and country in DoubleClue under ‘Administration’ > ‘Users’ by selecting user and clicking on edit.

When a language is defined for a user, they will see interfaces and receive templates in this language if a translation in this language is available. If no translation is available or no language defined, English will be chosen by default. A different default language can be set under ‘Administration’ > ‘User Default Language’. However, English will stay the fall back if resources in the chosen language are not available.

4.3 Roles

The role determines the access rights of a user. Roles can be assigned to Groups or individual users. If a user has several roles, for example by being a member of the several groups, they will get the privileges of all the roles assigned to them. For more information, see chapter [4.5 Privileges](#).

DCEM provides 6 automatically created standard roles. Additional roles can be created in DCEM under "Administration" > "Roles".

4.3.1 Rank

Each role has a rank. There are overall 11 ranks available, the highest being 10, the lowest zero. Lower ranked users cannot change the user information or privileges of higher ranked users and roles, even if they theoretically have these rights.

Example:

An administrator (rank 8) has the right to create new users. However, he can only create new users with roles ranked 8 or lower. He cannot create users with role SuperAdmin (rank 10) or other roles of rank 9 or 10.

Roles with rank 0 only have access to UserPortal and cannot log into DCEM. Rank 1-10 users have in general access to DCEM. What they can see there and what actions they can use can be defined under privileges.

4.4 Recover SuperAdmin Access

4.4.1 Recover SuperAdmin Access for the Master Tenant

To recover SuperAdmin access for the master tenant, open the DoubleClue Setup. You can find information on how to start the DoubleClue Setup once again while DCEM is running in chapter [2.3.4 Running Installation again](#). Save the Database configuration and the "Recover SuperAdmin Access" button will become visible.

Enter a new SuperAdmin password. Log into DCEM with the new password and the User ID "SuperAdmin". You can then reactivate MFA by modifying the policies under Identity & Access.

4.4.2 Recover SuperAdmin for a Sub Tenant

Go to the main menu "System", sub menu "Tenants". Choose the tenant whose SuperAdmin you want to recover and start the process by clicking the "Recover SuperAdmin Access" button above the list of


tenants. Enter a new password. Log into the sub tenant DCEM with the new password and the user ID “SuperAdmin”. You can reactivate MFA by modifying the policies under Identity & Access.

4.4.3 Effects of Recovering SuperAdmin Access

Should you lose access to the SuperAdmin, for example, because you lost your MFA device or the SuperAdmin user has been accidentally deleted or disabled, you can recover this access via the backdoor system.

Using it will:

- create a new user with the SuperAdmin-role, should no user with the name “SuperAdmin” exist.
- enable the user called “SuperAdmin” should it be disabled and set its role to “SuperAdmin”.
- set the SuperAdmin password to the password entered during the recovery process.
- modify the security policy of DCEM to allow access without MFA by only entering the password.
- Give the SuperAdmin the privilege to modify Privileges.

 Attention: We advise to modify the security policies immediately after recovering SuperAdmin access and activate MFA – disabling log in with password only.

4.5 Privileges

Privileges and access rights for the different roles can be administrated in the Privileges submenu under administration. Rights for the main menu items, the respective sub menu items and every associated action are specified by check boxes. If a user has several roles, for example by being a member of the several groups, they will get the privileges of all the roles assigned to them.

The section “Module” shows the separate main menu items for which access rights can be granted.

The section “Subject” shows the sub menu items belonging to the respective main menu items for which access rights can be granted.

The section “Action” includes all feasible actions that are possible in the separate subareas, for example “add”, “edit”, “delete”, or “save”. Each role has to be separately granted the right to perform a certain action.

It is possible to generally grant a role the right to perform all actions for one item of the main or sub menus. In this case the role needs the right for the action “manage”.

If an administrator should have read-only access, specify the action “View” for their role and the respective menu item.

4.6 Groups

Users can be divided into different groups. The groups can then be used to assign different policies and roles to the users (see chapter [7.2 Policies](#)). All members of this group will then receive the respective access rights and/or role. A user can be a member of several groups. In this case they will get the roles of all the groups they are a member of.



Groups can own files in CloudSafe. If a group is deleted, all files owned by this group will be deleted as well. Ensure that important files have been transferred to another owner before deleting a group.

4.7 Integration of Active Directory / Microsoft Azure AD / LDAP

DCEM supports multiple domains. This means that Administrators of DCEM can configure multiple domains as well. It is necessary that every domain entry has its unique domain name. New users can be imported from different domains after that. DCEM supports three domain types:

- Microsoft Active Directory (Active Directory)
- Microsoft Azure Active Directory (Azure AD)
- LDAP

You can authenticate your operators and users towards the domain with username and password. If an operator or user is marked as a “Domain User”, DCEM will verify the user / operator account towards the Active Directory / Azure AD / LDAP.

The domains used need to be configured first.

Please note: Once you have configured a domain and chosen the respective domain type, this choice cannot be changed anymore.

4.7.1 Adding a Default Active Directory Configuration

Go to main menu item “Administration”, sub menu “Domain”, and click on “Add”. Then choose “Active Directory” as the domain type.

Name:

Enter a unique name for the domain.

URL:

You can enter several URLs which need to be separated with a space. If you have specified more than one URL, DCEM will try to connect to the first URL and on connection failure it will try to connect to the next configured URL.

Base DN:

State the Distinguished Name of the Active Directory server. You will need this base to search for Active Directory users.

Search Account DN/UPN:

DCEM needs a search account to look for users and groups in the Active Directory.

Map E-Mail Suffixes to this Domain:

Enter the E-Mail-Suffixes used in the UPNs you wish to connect with this Domain, so that they are matched correctly. You can map more than one suffix to a domain by separating them with a semicolon (;).

Verify Certificate:

Check this box if you want DCEM to check the certificate of the domain.

Connect with AD Connector:

If you want to add your Active Directory on premises to a DCEM in the cloud, you can do this with the help of the Active Directory Connector. The AD Connector is a service you can install on your server. It will then serve as proxy client on your server. You can find further information in the Active Directory Connector documentation: [DC_AD_Connector.pdf](#).

Rank:

If one E-Mail-Suffix has been mapped to several Domains, the UPNs with this suffix will be matched to the domain with the highest rank.



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

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

4.7.2 Adding an Azure AD Configuration

For detailed instructions on how to integrate your Microsoft Azure Active Directory see:
DcemInstallation Location/DoubleClue Enterprise Management/doc/English/Manuals/Integrating Azure_EN.pdf.

4.7.2.1 Login with Microsoft Azure as Identity Provider

It is possible to configure Microsoft Azure as an Identity Provider for DoubleClue. The login will then be handled by Microsoft Azure and MFA policies will be applied as defined in Azure. For a more detailed explanation of how to set up Microsoft Azure as Identity Provider see:
DcemInstallation Location/DoubleClue Enterprise Management/doc/English/Manuals/Integrating Azure_EN.pdf.

4.7.3 Adding a LDAP Configuration

Go to main menu item “Administration”, sub menu “Domain”, and click on “Add”. Then choose “Generic LDAP” as the domain type.

Name:

Enter a unique name for the domain.

URL:

You can enter several URLs which need to be separated with a space. If you have specified more than one URL, DCEM will try to connect to the first URL and on connection failure it will try to connect to the next configured URL.

Base DN:

State the Distinguished Name of the LDAP server. You will need this base to search for LDAP users.

Search Account DN/UPN:

DCEM needs a search account to look for users and groups in LDAP.

Filter + Login Attribute:

In an Active Directory the default settings can be kept for the filter and the login attribute:

Filter: (&(objectCategory=Person)(sAMAccountName=*))

Login Attribute: sAMAccountName

If you use a different directory service based on LDAP, it may be possible that you have to replace “sAMAccountName” e.g. by the common name “cn” or by “uid” in both cases.

First Name Attribute - Mobile Attribute:

Adjust the attributes to your LDAP directory.

Map E-Mail Suffixes to this Domain:

Enter the E-Mail-Suffixes used in the UPNs you wish to connect with this Domain, so that they are matched correctly. You can map more than one suffix to a domain by separating them with a semicolon (;).

Verify Certificate:

Check this box if you want DCEM to check the certificate of the domain.

Connect with AD Connector:

If you want to add your Active Directory on premises to a DCEM in the cloud, you can do this with the help of the Active Directory Connector. The AD Connector is a service you can install on your server. It will then serve as proxy client on your server. You can find further information in the Active Directory Connector documentation: [DC AD Connector.pdf](#).

Default settings for Active Directory:

Add

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

Name:

URL:

Base DN:

Search Account DN/UPN:

Search Account Password:

Filter:

Login Attribute:

First Name Attribute:

Last Name Attribute:

Email Attribute:

Telephone Attribute:

Mobile Attribute:

Enable: ☒

Timeout in Sec:


Time needed for establishing a connection from DCEM to LDAP.

4.7.4 Importing Users and Groups from a Domain

Users will be automatically imported from the Domain to DoubleClue during their first login. It is therefore not necessary to import them manually. However, you can import them manually if you for example want to assign them certain groups or roles before their first login.


Under the sub menu item “Import Domain Users”, Administrators can import users and groups from the Active Directory / Azure AD / LDAP using a wildcard search for users and groups or selecting users from existing groups. Email addresses, display names, mobile phone numbers and their LDAP Distinguished Names (DN) / their Azure AD User Object-ID are also retrieved.

The login ID of users imported from a domain consists of the domain name as a prefix, with a backslash separating it from a user’s domain credentials (e.g. if the user “john.doe” is imported from the LDAP domain “EXAMPLE”, his login ID is “EXAMPLE\john.doe”).

 A user’s login ID without a backslash is usually considered a DCEM local user. This applies to operators’ login IDs as well.

At user import, administrators have the possibility to create Activation Codes for the imported and also for the existing users. Activation Codes can be automatically sent to users by email or by SMS, if email or SMS services have been configured in the system preferences respectively.

Before users or groups can be imported from a domain, a domain connection has to be configured (see chapters 3.7.1 to 3.7.3).

 Please note: DCEM will not save a user’s domain passwords.

4.7.4.1 Admin Preference “enableUserDomainSearch”

Under the sub menu item “Preferences”, Administrators can select if users need to login with their full login ID including their domain name, or not.

If the checkbox next to “Enable User Domain Search” is not ticked (this is default), all users must enter their full login ID inclusive of the domain name.


If the checkbox is ticked, users can enter their login ID or Active Directory UPN without a domain name (“john.smith”). In this case, DCEM will search for users locally and in all domains, according to their ranks. It will always just find the login ID with highest rank. If the user wants to log to a certain domain and not the highest in rank, they need to enter their login ID or UPN with the domain prefix (“EXAMPLE\john.smith”).

Should the user nonetheless want to login only as a local user, they have to put a backslash before their login ID (“\john.smith”).

4.7.5 Activate Windows SSO for Domain Users

It is possible to activate Windows SSO for domain users. This can be simply done by going to ‘Administrations’ -> ‘Preferences’ and checking the ‘Use Windows SSO’ box. By default, this box is not checked.

If this feature is activated and a user has logged into a workstation with a domain account, when opening DoubleClue in a browser, DoubleClue will try to automatically retrieve the credentials from the workstation and log the user in.

 This feature is only available if DoubleClue is installed on a Windows machine and the user is logged in on a windows workstation. The Linux version of DoubleClue does not support this feature. Also some browsers may not support Windows SSO or need a specific configuration.

4.8 Tenant Branding

Tenant Branding allows DoubleClue administrators to customize the appearance of the DCEM, UserPortal, SAML and OpenID login pages and banners. In a scenario with multi-tenants the branding can be defined for every tenant individually.

Please note that you need to save all changes, before they become active. This is also necessary if you want to set the changes back to default.

4.8.1 Time Zone

In this section you can set the local time zone. This time zone will from thereon be used when setting timers that ask you for a date and time, eg. expiration dates for CloudSafe files.

You can first choose a broader time zone and then a more specified location for summer times or local deviations from the regional standard time.

4.8.2 Banner Enterprise Management

In this section you can define the appearance of the banner of your DoubleClue Enterprise Management. If you don't apply any changes, DCEM will use a default design.

You can enter a custom text that will be displayed in the banner at the top of the Enterprise Management. You can further style the text by adding the changes in CSS in the respective field. Just enter the CSS properties you want to use separated by semicolon (;). You can also change the colour of the banner with "background-color: #XXXXXX;". Some of the properties, like vertical-align, have to be defined as "important".

4.8.3 Banner UserPortal

In this section you customize the banner of the UserPortal by adding a text and style it with CSS properties. This works the same way as for the Enterprise Management Banner (see section 4.7.2 above).

4.8.4 Banner SAML and OpenID Login Page

You can define the text for the SAML and OpenID banner under Text Resources (see chapter [4.10 Text Resources](#)). You can add different translations for various languages. The key for the SAML text resource is sso.saml.title, the key for OpenID is sso.oauth.title.

If you want to further style the text, you can do this in the tenant branding in the sections “Banner SAML Login Page” and “Banner OpenID Login Page” by adding CSS code into the respective style fields.

4.8.5 Text on Login Page

Enter a text that will be shown on all the DoubleClue login pages. This is a good place for important messages to the whole company.

As with the banner text, you can style the login page with CSS, including a background for the text area. You can, however, not define the background for the whole page. This is handled in section [4.8.6 Background and Logo](#) below.

4.8.6 Background & Logo

Here you can set the background for the login pages and the logo which will be displayed in the banner. Those will always be the same for all login pages and banners.

The logo is always displayed in the upper left corner. This can't be changed. Please choose a PNG, JPG or JPEG file with a maximum size of 10 KB and a resolution of 209 x 64 px.


You can select either a colour or an image for the background. The size of the image can't exceed 300 KB. The ideal resolution for the background image is 1920 x 1080 px and as with the logo it can be a PNG, JPG or JPEG file.

4.9 Templates

In order to be able to show data or texts in the DoubleClue App, templates are needed. Several default templates are provided with the installation of DCEM. You will find these under the main menu item “Administration”, sub menu item “Templates”.

4.9.1 Structure of a Template

Templates are created via the button “Add” and changed via the button “Edit”.

The content of a template can be written as text or inserted in HTML format. Switching between GUI and HTML format can be done in the respective editing windows via the button: .

In order to be able to show recorded data from the portal, the templates need to be supplemented by placeholders (so-called data tokens). A data token is put in double curly brackets: **{{Name Data Token}}**. For visual display the data tokens are replaced by the data from the REST interface.

If a template for sending a push approval to the DoubleClue App is created, it always has to have a button for confirming or closing the approval. In order to do this, buttons in HTML format need to be inserted via the command `<button>` and given an action ID.

Example: `<button id="ID name">button text</button>`

4.9.2 Languages

A separate template must be created for each language that should be available. One language can be defined as standard. If a language is chosen for which there is no template, the standard template is used.

4.9.3 Adding a Template

If there is no fitting template among the existing templates, a new template needs to be created.

In order to add a template, you need to do the following:

- Give a unique name.
- Choose the language.

Templates that have the same content but are created in different languages must have the same name for all languages (template group). The differentiation of the templates is done via the language selection.

- Specify a standard template for each template group. This standard template is used if a language for which no separate template exists was chosen for the user.
- Specify the content of the template:
 - Display text: Fixed text that should be shown in the template.
 - keyToken: Placeholders that are replaced by recorded values. These are always put in
 - double curly brackets `{{ }}`.
 - Action sections: e.g. button for confirmation or denial of an action

- Example:

Edit

Name: Language: Default: ☒

Data tokens are put in double curly brackets, for example {{keyToken}}.

Money Transfer

Recipient: {{recipient}}
 IBAN: {{iban}}
 Amount: {{amount}}
 Purpose: {{purpose}}

4.9.4 Editing a Template

As soon as a template is used in one place, the value for “In Use” (main menu: “Administration”, sub menu: “Templates”) is set to “true”. This template cannot be changed anymore.

4.9.5 Deleting a Template

As soon as a template has been used in any place, it cannot be deleted anymore.

4.10 Text Resources

Under Text Resources, you can modify various texts, which are displayed in particular in SAML and single sign-on interfaces. You can create any text in different languages. A logged-in user then sees the texts in the language that he has selected as the user language. If a text in a certain language is not available or the user is not logged in, the text will automatically be displayed in the language set as default for this DCEM installation.

4.11 Reporting

Under “Reporting” you can find all processes and actions performed by users. The location, from which the user performs the action, is displayed either by IP address or City. You can define this in the Administration Preferences.

You can also find alerts created by DoubleClue while it is running in this list. They are divided into 4 categories according to their severity: INFO, WARN, ERROR and FATAL.

4.12 Change History

In the change history, all actions are listed that were performed in the system by the administrators. If you set “Audit Enabled” under ‘Identity & Access’ > ‘Preferences’ > ‘CloudSafe & PasswordSafe’ you can also log changes made to CloudSafe and PasswordSafe files by users.

4.13 Licenses

In this submenu you can import license keys and find an overview of your current licenses. For more information about licenses, see chapter [16. Licensing System](#).

4.14 Preferences

In this submenu, you can define the following general settings for DoubleClue:

Enable User Domain Search – Enable users to log into DoubleClue or services secured by DoubleClue using only their username without entering their domain. If the same username is found in multiple subdomains / mandates, these different options will be shown in a drop-down list.

Storage History Archive – Define the number of days the history archive saves the recorded entries.

Inactivity Timer – The time until a user gets automatically logged out of DCEM or UserPortal when not being active

Use Windows SSO – You find detailed information for this setting under [4.7.5 Activate Windows SSO for Domain Users](#).

Location Information – Here you can decide whether you want to display an IP address or a city as location in the reporting

Location API Key – If you want to display the reporting location by city, enter an API key from <https://www.bigdatacloud.com/> into this field.

5. Multi-Tenant Capability

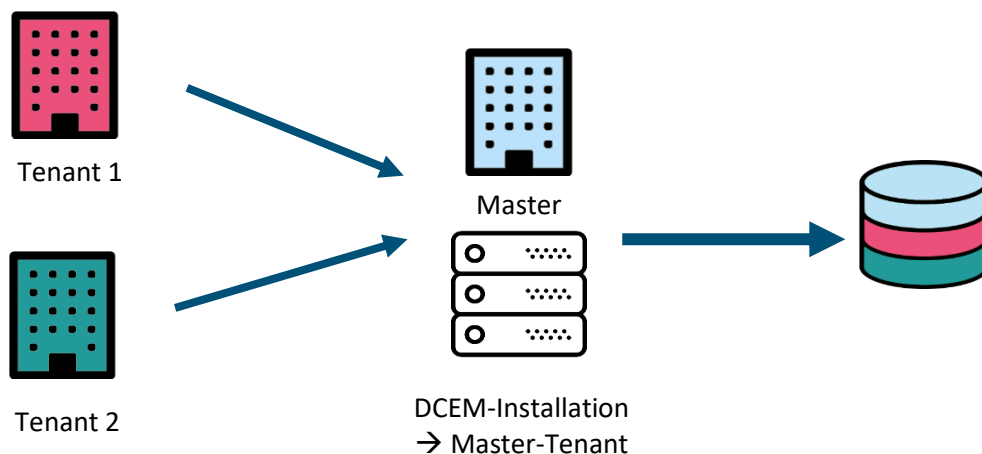
DCEM supports Multi-Tenant and can thus be operated as “SaaS” (Software as a Service). There is one infrastructure, i.e. all tenants share the same DCEM installation, database, PKI, URL and cluster nodes.

After the installation, a master tenant is created which is the default tenant. From there you can create additional sub-tenants.

The multi-tenant Capability is only supported by external databases. It cannot be used with an embedded database.

5.1 Concept

For every subtenant, DCEM creates a new database/schema so that every tenant has its own encapsulated database. Thus, the data of the master tenant and that of the subtenants will be clearly kept apart.



Each tenant has its own licence and can fully administrate its users, devices, policies, LDAP, RADIUS, SAML etc. However, the PKI, URLs, ports, cluster nodes and diagnostics are centrally managed in the master tenant.

⚠ Please note the following restrictions:

- Tenants are not supported when the “Embedded Database” is used.
- After a tenant has been deleted or disabled, a user or operator login is not possible anymore. However, the deleted tenant’s database remains in existence. This means that obsolete database schemes have to be deleted manually.

5.2 Tenants as Sub-Domains

Tenants are accessible using sub-domains. For this purpose, you would need to use SSL/TLS wildcard certificate for DCEM to cover all the subdomains. The master domain name, for example “doubleclueOne.com”, has to be configured in the Cluster Configuration “Host Domain Name”. Every tenant will get a sub-subdomain name for example “tenantName.doubleclueOne.com”.

5.3 Management of Multiple Tenants

Tenants can be managed by the Administrator of the master DCEM installation. To add or edit a tenant, go to main menu item “System”, submenu “Tenants”.

To create a new client, you need administrator access to the database. Enter the appropriate username and password. Then, specify a unique and meaningful **name**, **schema name** and **display name** for the new tenant.

The **name** will also be used as a suffix for the app login name and the subdomain prefix, so it should be easy for users to remember and write.

The **name** and **display** name can be changed later if necessary.

The **name** and the **schema name** may only consist out of alphanumeric characters.

When the client has been created, it adopts the Global and DCEM Management Policies of the main tenant. The policies can then be revised in the DCEM of the respective sub-client.

⚠ After adding a tenant, the tenant is immediately in operation.

⚠ When specifying tenants, ensure that the Host Domain Name is correctly set up under Cluster Configuration. If you use multiple host domain names, separate them with a semicolon (;).

5.4 Login Scenarios for Multi-Tenants

5.4.1 Login with Subdomain in a Multi-Tenant Scenario

In a multi-tenant scenario, you can log into the DCEM of a specific tenant by logging into the appropriate subdomain. The name of the subdomain matches the name of the tenant. If no subdomains have been specified, the master tenant will be used automatically.

The URLs are put together according to the following formula: subdomain. + hostdomain/ + application. The login by subdomain is available for the following applications:

- DCEM – example: *mandant.doubleclue.online/dcem/mgt*
- DoubleClue UserPortal – example: *mandant.doubleclue.online/dcem/userportal*
- Service-initiated login with SAML
- Provider-initiated login with SAML

5.4.2 App and RADIUS Login with Multi-Tenants

The DoubleClue app and RADIUS do not use a subdomain. Therefore, the login procedure in a multi-tenant scenario works as follows:

- DoubleClue App:
To associate a user with a particular tenant when signing in to the DoubleClue app, the user's login name is built as follows:
`"user$RealmName!mandant1"`
- RADIUS:
Tenants can support and configure their own RADIUS clients. The clients are distinguished by their IP number. A RADIUS NAS client IP number must be unique to the DCEM global installation.

5.4.3 Alternative: Login with Tenant-Specific User IDs

Instead of a subdomain a tenant-specific User ID can be used to log into the specific DoubleClue applications.

"tenant1" is the unique name of the tenant, separated by an exclamation mark.

- User ID for DCEM: `"superAdmin!tenant1"`
- User ID for REST service administrators: `"administrator!tenant1"`
- User ID for UserPortal user: `"user!mandant1"`
- Service Initiated Login with SAML: `"-- URL -- ?mandant=mandant1"`
If SAML is service initiated, the URL needs to include the name of the tenant.
- Provider Initiated Login with SAML: `"userLoginId!mandant1"`

5.5 Licences for Tenants

Each tenant requires its own license key. Once a tenant has been created, it is assigned a trial licence for 100 users over a 30-day period. Please contact sales@doubleclue.com to get a full license for a tenant.

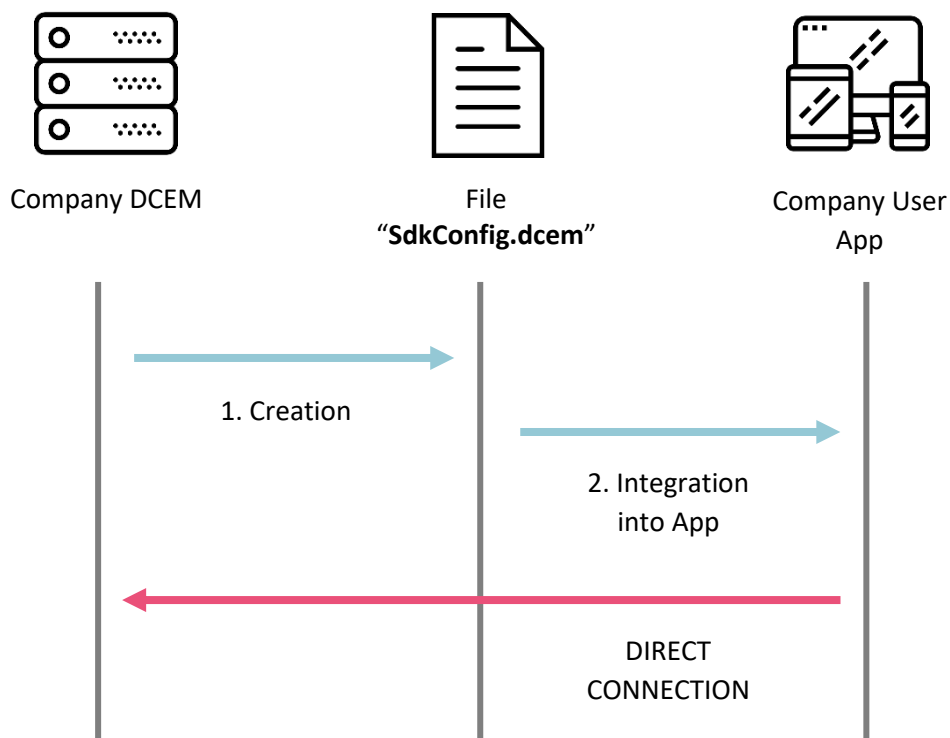
6. Connection Scenarios

6.1 Overview

6.1.1 Direct Connection with In-House App

The App connects directly to a company's DCEM installation. It is customized and you need to create and submit the App to the cloud stores such as Google Playstore or Apple Store.

The secure artifact file **"SdkConfig.dcm"**, which is generated by DCEM, has to be copied to the App resource directory. For more information about App deployment see the DoubleClue App Development Guidelines: [DC_Dev_Guide_Android.pdf](#) / [DC_Dev_Guide_iOS.pdf](#).



Advantages:

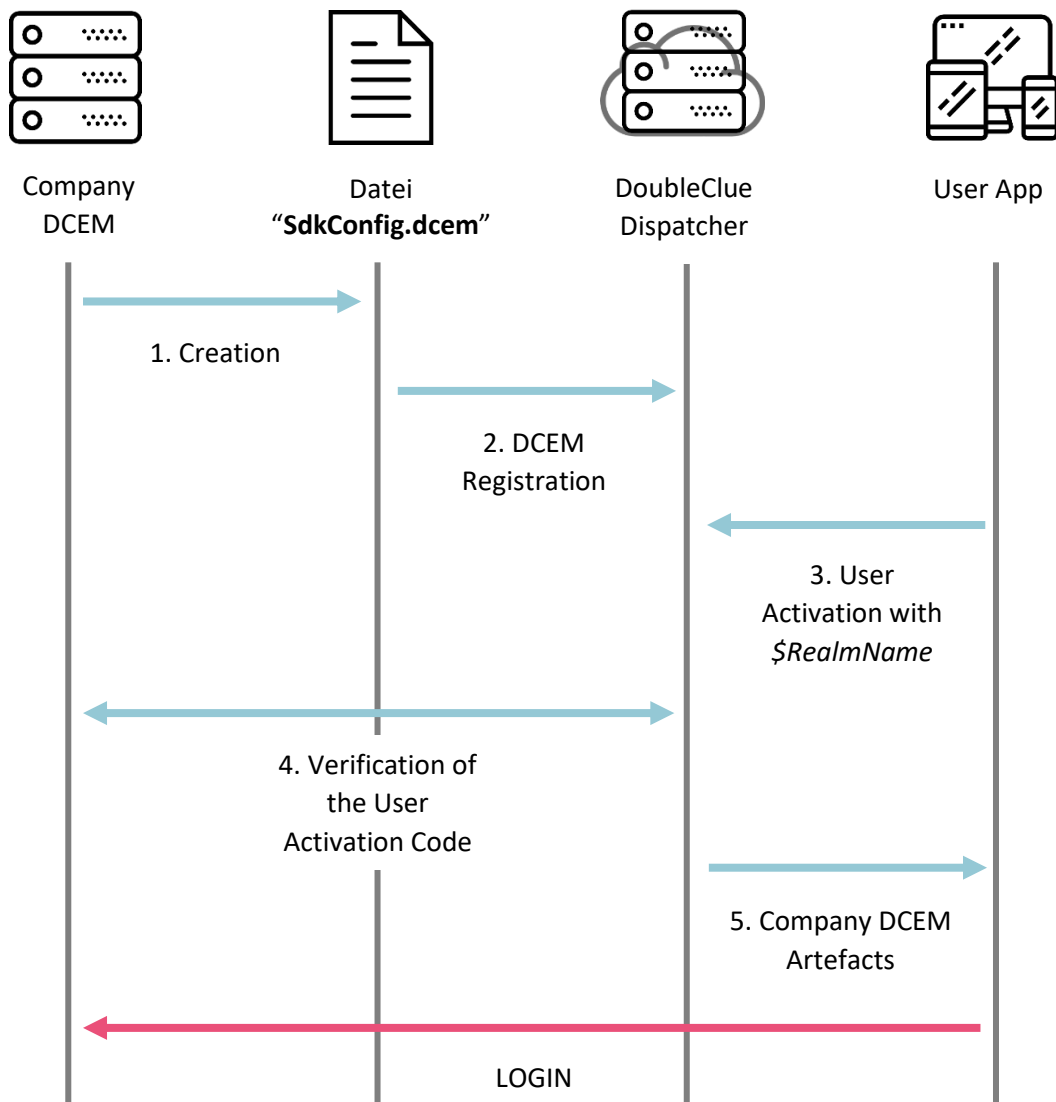
- There is no need for any third party or cloud servers. The Client App connects directly to your DCEM.
- The App can be fully customized to your needs.

Disadvantages:

- An App deployment procedure is required.
- The deployed App can only connect to a single DCEM Cluster installation.
- The DCEM Web-Socket Port has to be reachable from the internet. The company's firewall needs to open this port.
- DCEM needs a public URL.

6.1.2 Dispatcher Connection

The DoubleClue App can be used for all worldwide DCEM installations without the need to deploy your own App. For this type of connection, you have to register your DCEM installation at the cloud-based DoubleClue Dispatcher, see chapter [6.2.1 Configuration of the DoubleClue Dispatcher](#).



Advantages:

- A universal DoubleClue App can be used for all worldwide DCEM installations.
- Users can download the App directly from the public cloud stores.
- There is no need to deploy your own App.

Disadvantages:

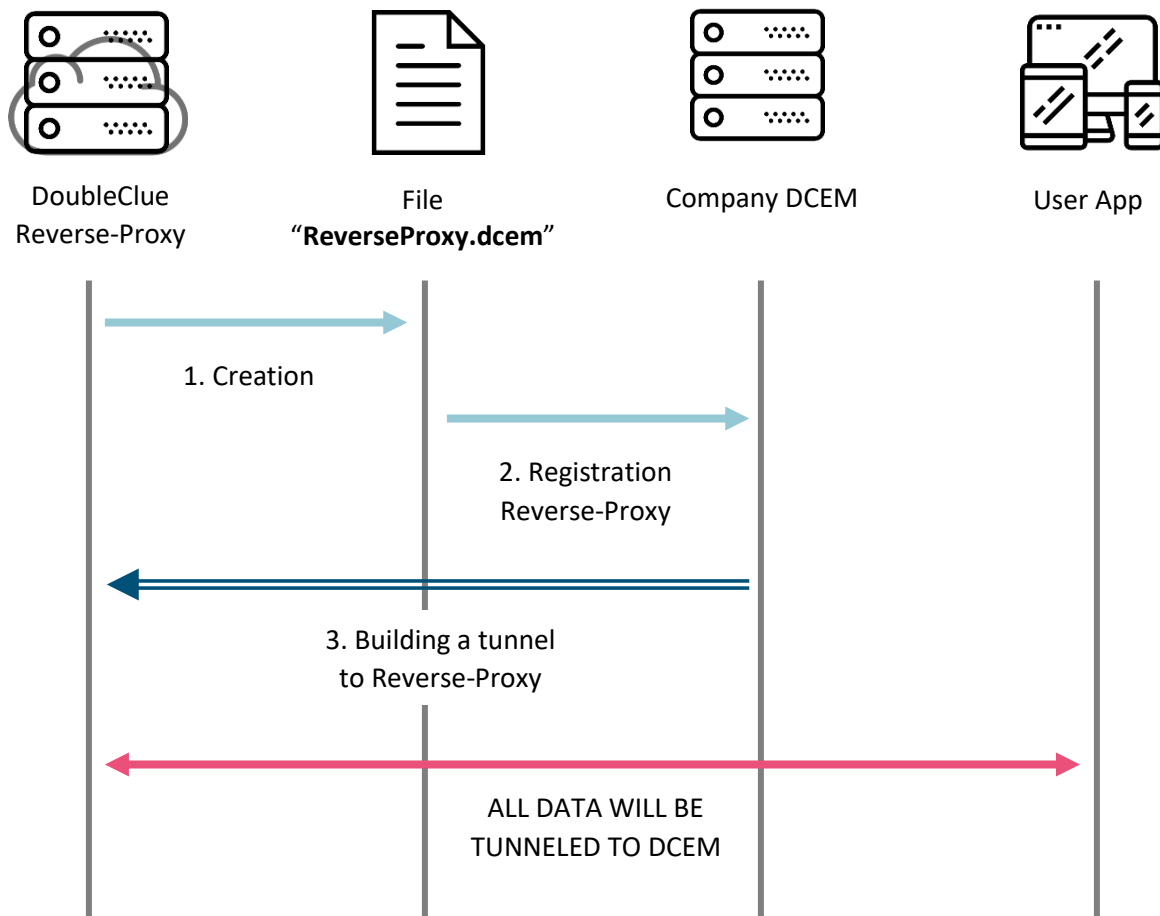
- The DCEM Web-Socket Port has to be reachable from the internet. The company's firewall needs to open this port.

- DCEM needs a public URL.
- At device activation there is a dependency on the DoubleClue Dispatcher Server.

6.1.3 Reverse-Proxy Connection

⚠ The Reverse-Proxy Connection should NOT be used for a productive environment!

The DoubleClue App can be used for all worldwide DCEM installations without the need to deploy your own App. If you intend to use the universal DoubleClue App from the App stores, you have to register your DCEM installation at the cloud-based DoubleClue Dispatcher first. See chapter [6.2.2 Configuration of DCEM for Reverse-Proxy](#).



Advantages:

- The DoubleClue App can be used for all worldwide DCEM installations.
- Users can download the App directly from the public cloud stores.
- There is no need to deploy your own App.
- Moreover, there is no need to open the company's firewall.
- You do not need to have a public URL.

Disadvantages:

- All data is tunneled between DoubleClue Reverse-Proxy and DCEM.
- If the tunnel connection fails, all clients' connections will fail as well.

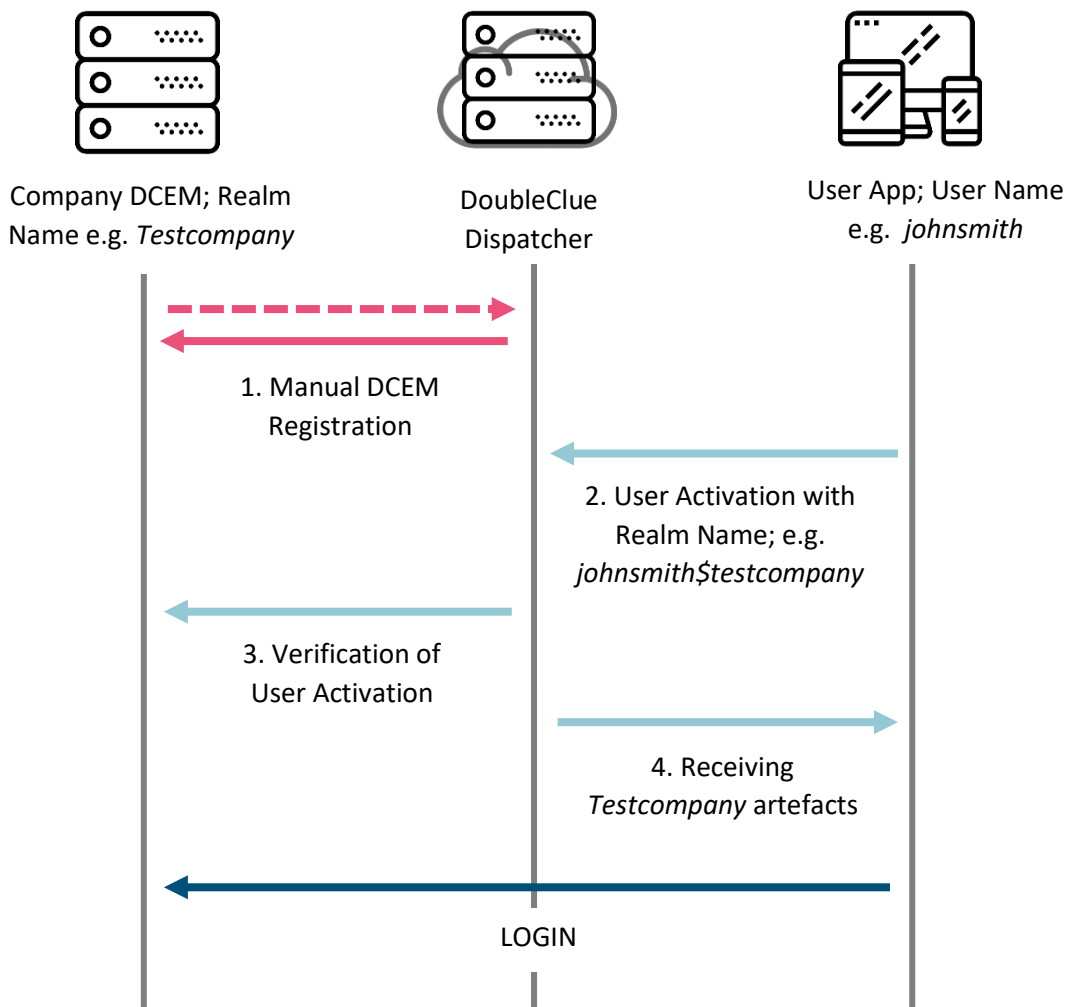
6.2 Configuration

6.2.1 Configuration of the DoubleClue Dispatcher

The DoubleClue Dispatcher is a DCEM Cluster in the cloud managed by *HWS Informationssysteme GmbH*. On device activation, the Dispatcher will verify user ID and Activation Code with the domain "Dcem-Installation". If the Activation Code is valid, the Dispatcher will send the DCEM "**SdkConfig.dem**" metadata file to the device. On login the device will connect directly to your DCEM installation.

⚠ Please note: The Dispatcher will not store any user data such as Activation Codes, passwords etc.

6.2.1.1 DoubleClue Dispatcher Data Flow



6.2.1.2 Registration at the DoubleClue Dispatcher

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


Send the chosen name together with the “**SdkConfig.dcem**” file to support@doubleclue.com in order to register your DCEM cluster at the DoubleClue Dispatcher.

6.2.2 Configuration of DCEM for Reverse-Proxy

6.2.2.1 Registration at the DoubleClue Dispatcher

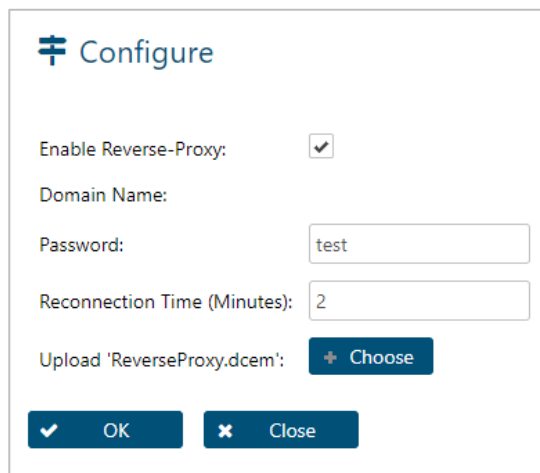
Choose a Realm Name that will be needed to identify your DCEM cluster towards the DoubleClue Dispatcher. We suggest using the name of your company as Realm Name. The Realm Name must be unique for the Dispatcher.

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.

 The amount of concurrent sessions with the DoubleClue Dispatcher is by default restricted to 10 sessions. If you need more concurrent sessions, please contact support@doubleclue.com.

6.2.2.2 Configuration Process

Go to main menu item “Identity & Access”, sub menu “Reverse-Proxy” and click on the button “Configure”.



The screenshot shows a 'Configure' dialog box with the following fields and controls:

- Enable Reverse-Proxy:** A checkbox that is checked.
- Domain Name:** A text input field.
- Password:** A text input field containing the text 'test'.
- Reconnection Time (Minutes):** A text input field containing the value '2'.
- Upload 'ReverseProxy.dcem':** A button labeled 'Choose' with a plus icon.
- Buttons:** At the bottom, there are two buttons: 'OK' (with a checkmark icon) and 'Close' (with an 'x' icon).

Enable ReverseProxy:

This box can be checked if you want to activate Reverse Proxy. Otherwise leave it empty.

Domain Name:

This is the unique domain name that you chose to identify your DCEM cluster towards the DoubleClue Dispatcher.

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**” which was sent to you by the DoubleClue team.

6.3 The DoubleClue App

DoubleClue Apps for Android / iOS can be found in the Google Play Store / App Store. The DoubleClue Desktop App may be downloaded from www.doubleclue.com.

All DoubleClue Apps are able to connect to any company’s DCEM cluster farm if this DCEM cluster has been previously registered at the central DoubleClue Dispatcher.

You do not need to deploy your own App to work with your installed DCEM software. Users who have already been registered at DCEM can just download the DoubleClue Apps from the respective cloud stores and start using DoubleClue security. Of course it will still be possible for you to create and use your own App if required.

7. Authentication Methods and Policies

DoubleClue supports a variety of user authentication methods, applications and policies that define which authentication method will be applied to which application.

7.1 Authentication Methods

DoubleClue supports the following authentication methods:

- Push Approval
- QR Code Approval

- FIDO U2F Token
- OTP Token
- DoubleClue Passcode
- Password
- SMS Passcode
- Voice Message

These authentication methods can be configured under main menu item “Identity & Access”, sub menu “Policies”.

7.1.1 Push Approval

This is the most secure authentication method, which is based on a PKI private key 2048 Bit certificate. At authentication, the user receives a Push Notification on their mobile phone. After starting DoubleClue App and logging into it, which is optionally biometric, they can confirm or reject the push approval with their App.

Pre-Requirements:

- The user has to download and install the DoubleClue App.
- The DoubleClue App needs to be activated.

7.1.2 QR Code Approval

This authentication method is based on a 32 Bytes AES random encryption key. Users can authenticate themselves by scanning a QR code with their user device.

 This method is not available for RADIUS or the Microsoft ADFS Plugin.

Pre-Requirements:

- The user has to download and install the DoubleClue App.
- The DoubleClue App needs to be activated.

7.1.2.1 *Process of a QR Code Authentication*

The QR Code Login works as follows:

1. The end user calls up the login page of the customer portal.
2. The portal executes the method "requestLoginQrCode()" via the REST-Web Services interface in order to get a QR code from DCEM.
3. The content of the QR code is sent from DCEM to the web server of the customer portal.
4. The newly generated QR code is shown in the customer portal.
5. The end user logs in to the app.
6. The end user scans the QR code from the customer portal with the app.

7. The app sends the QR code content to DCEM.
8. From step 4 onwards, the portal executes the method "queryLoginQrCode()" parallel to the other steps via the REST-Web Services interface. This method periodically asks DCEM if the QR code content has already arrived.
9. DCEM responds with "OK" if the correct QR code content was submitted. In this case, user name and device name are sent to the portal and the end user is logged in to the customer portal.


If an error is reported back, step 8 is repeated till the response is "OK" or the validity of the passcode has expired and therefore a timeout has been initiated by the portal.

7.1.3 FIDO U2F Token

FIDO is an open standard for multi-factor authentication. FIDO Security Keys are physical tokens that connect to a device via the Bluetooth or USB interface. For more information, visit <https://fidoalliance.org/>.

7.1.4 OTP Token

When using this authentication method, the users enter a passcode generated by a hardware OTP token.

 Please note: Currently DCEM supports the token type "**TIME_6_SHA1_60**". This is a time-based OTP with 6 digits using an SHA1 algorithm and a time slot of 60 seconds.

When using RADIUS, the user has to enter the passcode followed by a forward slash and then the password (example: "**12345/password**").

Pre-Requirements:

- The DCEM server has to be time synchronized with an NTP (Network Time Protocol) domain.
- It is necessary to purchase Hardware Tokens. Please contact your DoubleClue sales representative under sales@doubleclue.com.
- From your sales representative, you will also receive the hardware token secure file as well as a decryption key.

Import the hardware token secure file and enter the decryption key under main menu item "OTP-Tokens", sub menu "OTP Tokens".

Tokens need to be assigned to single users. You can do this by selecting a token and clicking on the button "Edit", then on "Assign Token to User".

Under main menu "OTP-Tokens", sub menu "Preferences", you can configure a "Delay Window". This is the amount of 60 second-time slots that DCEM will step back to verify the OTP.

7.1.5 DoubleClue Passcode

Logging in with a Passcode can be done in offline mode.

This option is necessary if a user has no internet connection on the device with the app and would like to authenticate themselves towards the server. The user does not need to be logged in to the app for this.

For this authentication method, the DoubleClue App is used. A user needs to click on “Offline Login” in the App menu to generate a passcode.

Pre-Requirements:

- The user has to download and install the DoubleClue App.
- The DoubleClue App needs to be activated.

7.1.5.1 *Validity of the Passcode*

The response time available to the user can be specified in the main menu “Identity & Access”, sub menu “Preferences” under “Login QR-Code Response Time”. The computer time of DCEM and end user app must be synchronous, otherwise it may happen that the time has expired before the end user has been able to act.

7.1.6 Password


A user is authenticated by their login ID and password. If the user is a domain user, the password will be validated directly by the domain and the user’s password will not be saved in the DCEM database.

7.1.7 SMS Passcode / Voice Message

These authentication methods are used additionally to the password authentication method. DCEM will create a random passcode which will be sent to the user’s mobile phone via SMS, or the user’s landline telephone number or mobile number will be called. The passcode is valid for a certain period of time in minutes, which can be configured under main menu item “Identity & Access”, sub menu “Preferences” (“Passcode Valid for”).

Pre-Requirements

- You need to purchase SMS credits from www.messagebird.com
- Configure the SMS Provider Access Key under main menu item “System”, sub menu “Preferences”.
- For sending SMS, a mobile phone must be configured for the user.
- For receiving Voice Messages, either a landline telephone number or a mobile phone number must be configured for the user.

 Please note that SMS and Voice Messages are not sent over the line in encrypted form.

7.2 Policies and Applications

Under main menu item “Identity & Access”, sub menu “Policies”, DCEM offers the possibility to set different policies for applications and user groups to determine which authentication method they are allowed to use during their login process.

7.2.1 Adding and Configuring Policies

The Policies allow you to specify access rights of specific user groups for different types of DoubleClue application types and their associated applications.

You can specify the following options:

Deny Access:

If you tick this checkbox, access will be completely denied to all respective users.

Refrain MFA within Timeout:

Within a pre-set time period, a user can log in with login ID / password after having authenticated themselves via MFA once.

Stay Logged In:

If not activated, you will have to log in each time you want to access the service. If it is Activated, you won't have to log in after a successful login for the time defined under Timeout.

Timeout (Hours):

Here you can set the period of time in hours during which any MFA authentication is bypassed if one of the three options above has been chosen.

Network Bypass:

This setting is used to bypass any MFA authentication if the user source IP Address lies within one of the IP ranges entered.



This feature is only available for SAML and REST-Web Services applications.

Allow Auth-Methods:

Choose the authentication method(s) a certain group of users is allowed to use.

7.2.2 Application Types

DoubleClue supports the following application types:

- AuthConnector (for example DoubleClue Windows Login)
- DCEM
- OpenID/OAuth

- REST-Web Services
- RADIUS
- SAML
- UserPortal

For each interface, several applications may be configured.

7.2.3 Assigning Policies

Policies can be assigned to interfaces (e.g. AuthConnector, RADIUS, DCEM, SAML, Web-Services), applications (e.g. Cisco Meraki, Citrix ShareFile, Dropbox, etc.) and user groups.

DCEM assigns a policy to a user in the following order:

- a) If a policy is assigned to a user group, it applies to every member of that group.
- b) If a user is a member of several groups and different policies are assigned to these groups, the policy of the group that has the highest priority is chosen. Group priority can directly be assigned to the respective group at policy allocation.
- c) If no policy is assigned to a group for a certain application, the policy of the application will be used.
- d) If no policy is assigned to an application, the policy of the respective application type applies.
- e) If neither the user group, nor the respective application or application type have an assigned policy, the “Global-Policy” applies.

7.2.4 Selecting an Authentication Method

If a user’s assigned policy includes only one authentication method, DCEM will use this authentication method.

If a policy allows several authentication methods, the following selection methods apply:

Default Auth Method:

You can specify a Default Auth Method in the policies. This will then be the first to be displayed to all assigned users. However, users can manually select a different method during login if it is allowed in the policies. It may be that some application types or applications do not support the selection of a default auth method. In this case the users need to rely on Pre- or Post-Selection.

Pre-Selection:

In some login scenarios, the user needs to pre-select the authentication method they want to use if no default authentication method is defined or they want to use a different authentication method than the default one.

The Pre-Selection can be made via an application GUI, such as a dropdown choose box. If this is not possible, for example in the case of RADIUS, a user can pre-select the authentication method by adding

a prefix to the password. The prefix is an abbreviation of the authentication method. It is surrounded by two hashes ## at the beginning and at the end.


Available prefixes are:

- pwd = Password
- sms = SMS Passcode
- voice = Voice Message
- otp = OTP Token
- motp = DC App Passcode
- push = Push Approval
- fido = FIDO U2F Token

Example: If a user wants to use a hardware token, they need to enter “##otp##password”.

Post-Selection:

If a user has authenticated themselves successfully by password without selecting an authentication method beforehand, DCEM will return a list of possible authentication methods found in the assigned policy.

 This selection type is not available for RADIUS interfaces.

7.3 Stay Logged In (Silent Login)

DoubleClue supports silent login to access DoubleClue apps and services protected by DoubleClue without having to repeatedly authenticate themselves. To use this option for services accessed through the browser, users have to enable ‘Stay Logged In’.

For the silent login, a 32-Byte key is created during a login with authentication and stored in the data base as well as on the device or browser used for the login. As long as the key exists in both places, the user can log in silently, without redoing the authentication process.


The key is revoked in the following situations:

- After a certain amount of time which can be defined at **Identity & Access Management > Preferences > Time for Silent App Relogin** for apps and in the policies for services
- When a user logs out via the log out button
- When a user is re-enabled by an administrator after having been disabled (e.g. for entering an incorrect password too many times)

8. Identity & Access

8.1 Activation Codes

Under Activation Codes, you can send users an activation code for their DoubleClue app via email or SMS. In addition, all sent activation codes are logged in this submenu and can be revised later.

 Please note that you must first configure the e-mail and SMS settings under **System > Settings** to be able to send the activation codes.

The ability to send an activation code to an entire group can be found under **Administration > Group**.

8.2 Smart Devices

This section shows a list of smart devices that have been connected via the mobile app to this DCEM installation. User can connect multiple smart devices to their account.

If logged into the DCEM of a sub-tenant, you only see the smart devices belonging to this sub-tenant.

8.2.1 Disabled Smart Devices

There are three ways to lock a smart device. An administrator can lock a smart device in DCEM, a user can lock his or her own smart device in UserPortal, and a smart device is automatically locked if the password on that device is incorrectly entered too often when attempting to log in via the app. You can set how many attempts a user has to successfully log in under "Identity & Access" > "Settings".

If a user has several activated smart devices at the same time, the same password applies to each device. If the password is incorrectly entered several times on a device, only this smart device will be blocked. He can still log in via the other activated smart devices.

A locked smart device can be unlocked by the user through UserPortal or by an administrator through DCEM.

8.2.2 Deleting a Smart Device

Deleted devices are marked as "deleted". They can still be found in the database. See chapter [8.8 Preferences](#) for an exception.

8.2.3 Device Status

The device status says whether a user is currently logged into the app on the respective device or not. If the user is currently logged into the app, the device status will be displayed as online. If the user is

not logged into the app or the app is closed, the device will be displayed as offline. Administrators can check the status of a device in DCEM in the list under “Identity & Access” > “Devices”.

8.3 FIDO-Authenticators

This section shows a list of the FIDO authenticators connect with this DoubleClue infrastructure. Anyone logged in to DCEM through a subdomain will only see the FIDO authenticators registered for that tenant.

8.4 CloudSafe


CloudSafe is a cloud storage in which data and documents can be stored with DoubleClue MFA. It is accessible over the DoubleClue UserPortal.

In DCEM, administrators can manage the space available for each user and get an overview of the files stored in CloudSafe.


8.4.1 CloudSafe License and Distributing Storage Space to Users

The storage space in CloudSafe is limited for each DCEM license. The overall amount of available space can be seen under “Administration” in the “Licenses” sub menu. The amount of storage currently used, can be checked in the “Identity & Access” sub menu in the “Reporting” item by clicking on the “Display License Usage” button. As each tenant possesses its own license, the available storage in CloudSafe in a multi-tenant scenario is measured by tenant and not by DCEM installation.

Each license has a certain amount of CloudSafe storage space included that is shared by all users of the respective tenant or DCEM installation. It is further possible to assign a maximum amount of available storage to each user.

 Should the overall storage of the license be filled, users won't be able to upload any more files – no matter if they have exceeded their individual assigned storage space or not.

If you wish to change your CloudSafe license, please contact sales@doubleclue.com.


 Should a user already have uploaded files, the limit cannot be set to a size that is lower than the size of the files already in their CloudSafe. It is therefore advised to set storage limits before giving user access to CloudSafe.

8.4.1.1 Define a Default Limit for All Users

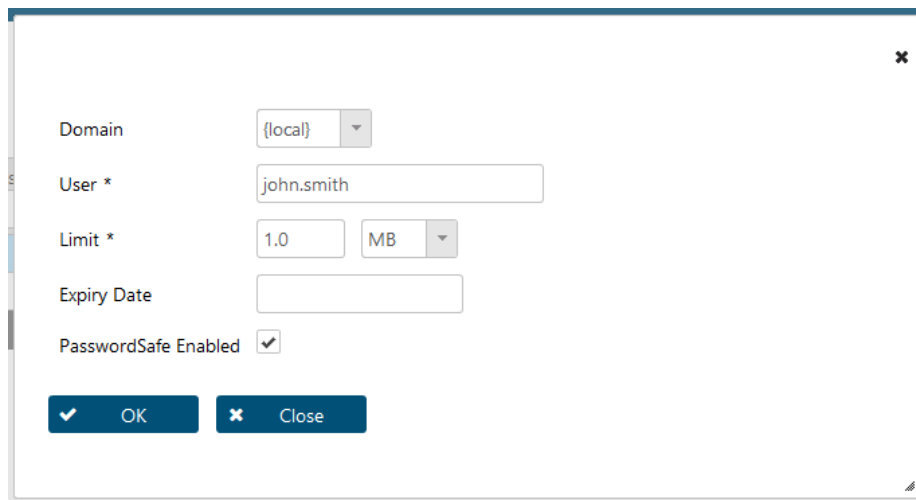
Under ‘Identity & Access’ > ‘Preferences’ it is possible to define a Default Limit of CloudSafe storage for each user. This default limit sets the maximum amount of storage each user has available in CloudSafe.

It is also possible to define in the preferences if PasswordSafe shall by default be activated or deactivate.

8.4.1.2 Define Individual Storage Limit for Users

 The CloudSafe view in DCEM is only available in the Professional Edition. It is therefore not possible to define individual storage limits for users in the Community Edition.

An administrator can assign more or less storage to an individual user in the 'Cloud Safe' item of the 'Identity & Access' sub menu. They can do this by simply selecting a user in the list and then edit their settings.



Administrators can further enable or disable PasswordSafe for this user here and define an Expiry Date after which the settings defined for individual users will automatically be reset. Individual settings for a user will override the default settings.

Users will automatically appear in the list once they have uploaded a file to their CloudSafe. Administrators can further add users manually with the "Add"-button.

8.4.2 File Information

Administrators can see an overview of the files stored in CloudSafe for each users. They can, however, not access, delete or change the files. By default, only the user who uploaded the file has access to it. Users can share CloudSafe files with other users and decide if they want to allow them to change the file.

To see a list of files uploaded by a user, an administrator needs to select a user in the CloudSafe list and then go to "Show Files".

8.4.3 Files and Folders with Individual Password

It is possible for a user to protect single files and folder in CloudSafe with an individual password. When the user wants to access this file or folder, they have to enter the password additionally to identifying themselves when logging into UserPortal.



Beware: Protecting single files and folders with an additional password (PWD) is only recommended for highly confidential data. The individual file or folder password cannot be reset. If the owner loses it, access to the data cannot be restored. If the user wants to share this file or folder with other users, they must share the password with them, so that they can open it.

8.4.4 Change CloudSafe Storage to Network Access Storage

Per default, files stored in CloudSafe will be stored in the database. This can have some disadvantages as big files will need a long time to be processed. It is therefore possible to change the CloudSafe Storage and use a Network Access Storage instead.

To change the CloudSafe Storage, you need to run the setup again as described in chapter [2.3.4 Running Installation again](#). If you run DCEM in a cluster, ensure to terminate all nodes.

On the first page in the setup, click on “Save & Verify DB-Connection”. If a dialogue opens (depending on the used database) confirm it. You will now see several new buttons on the first page, one of them being “Change CloudSafe Storage”.

Setup - Configuration

Database Configuration | Create Database | Create Database Tables

Type * Embedded-Database

JDBC-URL jdbc:derby:dcem_db;collation=TERRITORY_BASED:PRIMARY Configure URL

Database Name * dcem_db

Administrator Name * root

Administrator Password 👁

DoubleClue Node-Name * XXXXXXX

Save & Verify DB-Connection

Close DoubleClue Setup Recover SuperAdmin Access **Change CloudSafe Storage**

In the following dialogue, choose NetworkAccessStorage in the dropdown menu and enter the NAS Path. Then confirm your changes.

Start DCEM anew and the changes will be active.

8.5 Push Approval

Push Approvals are sent to the app via the REST-Web Services interface or the management GUI. They are also used for user authentication for all supported applications. The response can be digitally signed if required.

8.5.1 Features of a Push Approval

For most applications, the properties of the Push Approval are set. For REST applications, however, you can set the properties as follows:

8.5.1.1 *Template Name*

Several default templates are included with the installation. If no suitable template exists, you can create the desired template as described in chapter [4.9 Templates](#).

The chosen language of a template depends on the user or device for whom / which the push approval is meant.

8.5.1.2 *User Login Name*

Each push approval must be allocated to a fixed receiver. For this, the login ID of the user is submitted.

8.5.1.3 *Device Name*

If the push approval should only be sent to a certain user device, the device name has to be submitted additionally.

If no device name is submitted, the push approval will be sent as follows:

Several devices active: (active = logged in to the app)

If several user devices are active at the same time, the push approval is sent to the device which was activated last.

One device active:

If only one user device is active, the push approval will be sent to this device.

No device active:

If no user device is active, a Push Notification will be sent to all devices of a user if Push Notifications are allowed in the settings for "Identity & Access" (see also chapter [8.6 Configuration of Push Notifications](#)).

8.5.1.4 *Response Necessary*

If no response is necessary for a push approval, there will be no guarantee that the receiver has received the push approval. In order to prevent this, it can be specified that a response is necessary. Should a response be required, you also have to set a response time (in seconds) and a signature.

8.5.1.5 *Response Time (in Seconds)*

The response time states how long a user has time to react to a push approval. If it has expired, there will be a timeout error (see chapter [8.3.4 Status of Push Approvals](#)).

If no response is necessary, no response time needs to be set.

There are the following options to specify a response time:

- Response time for the push approval to be sent:

When sending a push approval, a response time can be specified which is only valid for this approval.

The value "0" is preset. In this case the "Push Approval Response Time" is adopted from the main menu "Identity & Access", sub menu "Preferences".

- Specifying a general response time:

Main menu "Identity & Access", sub menu "Preferences":

This setting is valid for all push approvals. The response time specified in the settings is always used when the response time for the actual push approval to be sent is set to "0".

8.5.1.6 *Digital Signature Required*

The response of the sent push approval can be signed with the device certificate if required. This is automatically created when the device is activated on DCEM.

More processing power will be needed if the push approval is signed.

8.5.1.7 *Action IDs for Buttons*

A template for a push approval always has to have at least one button to react to the push approval. With the help of the action ID one can see which action (that is, which button) the user has clicked on. The ID name has to be unique.

An action ID in HTML format can be defined in your template as follows:

```
<button id="ID-Name">Button Name</button>
```

```
<button > </button> = HTML format for a button
```

```
id="ID-Name" = Action ID
```

```
Button Name = Display text for the button
```

8.5.1.8 *DataMap*

A template can include tokens. The content of these tokens is called “DataMap”. The token is replaced by the data content of the associated DataMap and sent to the user in this form. A DataMap always consists of key-value pairs:

Key = The key is equivalent to the token in the template.

Value = The value of the key is replaced by the content of the tokens.

8.5.1.9 *InputMap*

Templates can contain input fields. The content of these fields is the so-called InputMap. It always consists of key-value pairs:

Key = The key is equivalent to the ID of the input field.

Value = The value of the key is the content that the user has entered.

An input field in HTML format is inserted as follows:

```
<input type="text" id="ID-Name" value="">
```

```
<input>= = Input field
```

```
type = "text" = Type “text field”
```

```
id="ID-Name" = ID of the input field
```

```
value="" = Input value of the user
```

8.5.1.10 *Status*

See chapter [8.5.4 Status of Push Approval](#).

8.5.2 Preferences for Push Approvals

The following settings have to be made in the main menu “Identity & Access”, sub menu “Preferences”:

8.5.2.1 *Response Time for Push Approval*

See chapter [8.5.1.5 Response Time \(in Seconds\)](#).

8.5.2.2 *Push Approval Store Policy*

It can be selected if the content of the MapData or the InputData should be saved in the database. The stored data can be read in the main menu “Identity & Access”, sub menu “Push Approvals” via the button “Show Push Approval Details”.

You can choose between:

- 1) Neither MapData nor InputData should be saved:

Setting made:	"none"
Displayed in “Show Push Approval Details”:	no display

- 2) Sent MapData should be saved:

Setting made:	"to_device"
Displayed in “Show Push Approval Details”:	"Send Data:"

- 3) Received InputData should be saved:

Setting made:	"from_device"
Displayed in “Show Push Approval Details”:	"Received Data:"

- 4) Both MapData and InputData should be saved:

Setting made:	"both"
Displayed in “Show Push Approval Details”:	"Send Data:" "Received Data:"

8.5.2.3 *Push Approval Retrieve Timeout Sec*

Duration of how long a push approval can be retrieved from the Portal after having gotten the final status. If this time has been exceeded, the push approval cannot be retrieved anymore.

8.5.3 Sending Push Approvals via REST-Web Services

You will find detailed information about the REST-Web Services interface in the following HTML document:

DCEM/doc/REST-WebServices/index.html

The push approvals are processed asynchronously. This means that the REST method "addMessage()" will return before the push approval is sent to the device. The method "getMessageResponse()" has to be called sequentially till the response has a status set to "final".

Use the following methods to be able to send push approval via the REST-Web Services interface:

8.5.3.1 *"addMessage()"*

In order to send a push approval from the Portal to the server, the method "addMessage()" must be called. The server sends the associated push approval ID to the Portal as response.

8.5.3.2 *"getMessageResponse()"*

The Portal has to request if there are any responses in certain time intervals. The time intervals should not be shorter than one second (our recommendation is 2.0 seconds). Use the method "getMessageResponse()" here. The request is repeated till a final status is reported (see also chapter [8.3.4.3 Flowchart about Push Approval Status](#)). The response gets the same ID as the request and can therefore be attributed correctly.

8.5.3.3 *"cancelUserMessage()"*

The Push Approval can be cancelled with this method as long as it has the status "queued".

8.5.4 Status of Push Approvals

See also chapter [8.3.4.3 Flowchart about Push Approval Status](#).

8.5.4.1 *Status of Open Push Approvals*

Push Approvals can have the following non-final status:

Queued:

The push approval has been sent from the Portal to the server. It has not been forwarded to the end user yet because it is still queued internally.

Sending:

The push approval is being sent from the server to the end user at the moment.

Waiting:

The push approval has been successfully sent to the end user. However, no response has come back yet.

8.5.4.2 *Final Status of Push Approvals*

Push Approval can have the following final status:

Ok:

The push approval has been confirmed by the end user. It is not important which action he selected.

Rec_Error:

The end user has received the push approval but cannot respond to it due to technical reasons. This error is reported directly from the App-SDK-Library.

Send_Error:

While sending the push approval to the end user, an error has occurred. It has not been possible to send the approval.

Disconnected:

The connection from server to end user was interrupted. The process needs to be repeated.

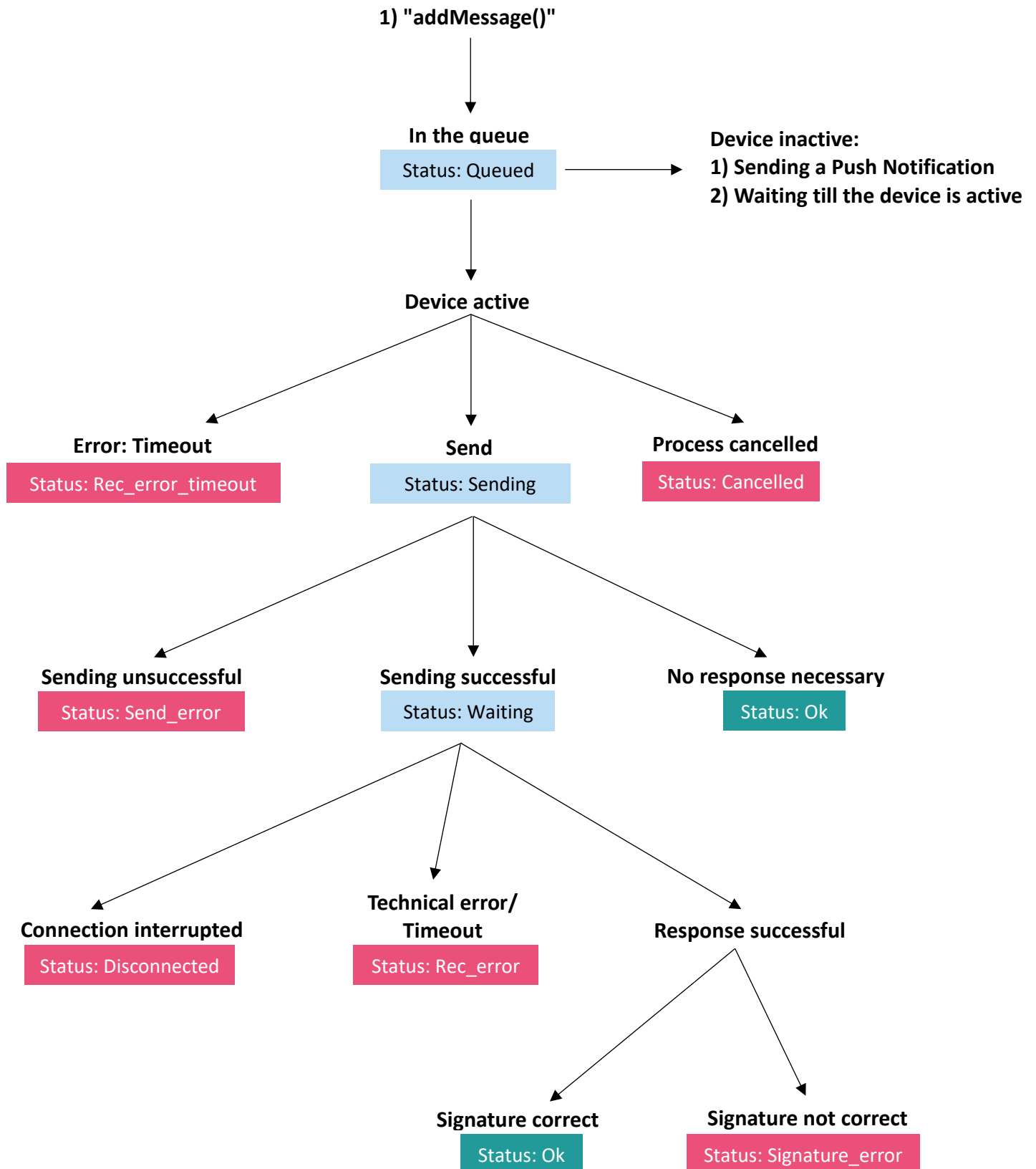
Cancelled:

The process was cancelled by the REST-Web Services interface.

Signature_Error:

The response from end user to server has been received successfully, the signature, however, is incorrect.

8.5.4.3 Flowchart about Push Approval Status



8.5.5 Life Cycle of a Push Approval

8.5.5.1 Pending Push Approvals

A push approval can be created via the REST-Web Services interface or the management GUI. New push approvals are always marked as pending approvals.

You will find pending push approvals in the main menu “Identity & Access”, sub menu “Pending Approvals”.

8.5.5.2 Closed Approvals

Pending push approvals are closed on the following conditions:

- 1) A push approval for which no response is expected is closed after sending.
- 2) A push approval for which a response is expected is closed when the respective response has been retrieved from the Portal or its retrieving time has expired (“Approval Retrieve Timeout Sec”).

You will find closed approvals in the main menu “Identity & Access”, sub menu “Push Approvals”.

8.6 Configuration of Push Notifications

If you use DoubleClue on premises, you need to need to configure Firebase Cloud Messaging in DCEM for your users to receive push notifications.

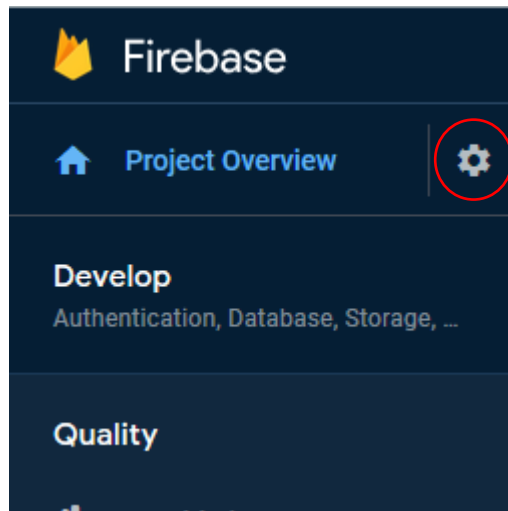
If you use the official DoubleClue app, contact the DoubleClue support team at support@doubleclue.com and we will send you the json-file needed to configure push notifications for the DoubleClue app. In this case, jump right away to chapter [8.6.2 Configure Push Notification in DCEM](#). If you want to use your own DoubleClue app or integrate DoubleClue into your company’s app, you need to create and download your own Google services json-file.

Please be aware that Firebase is a third party service that is not part of DoubleClue. The conditions and configuration of newer Firebase versions may differ from the one described here.

8.6.1 Download the Google Service Files from Firebase

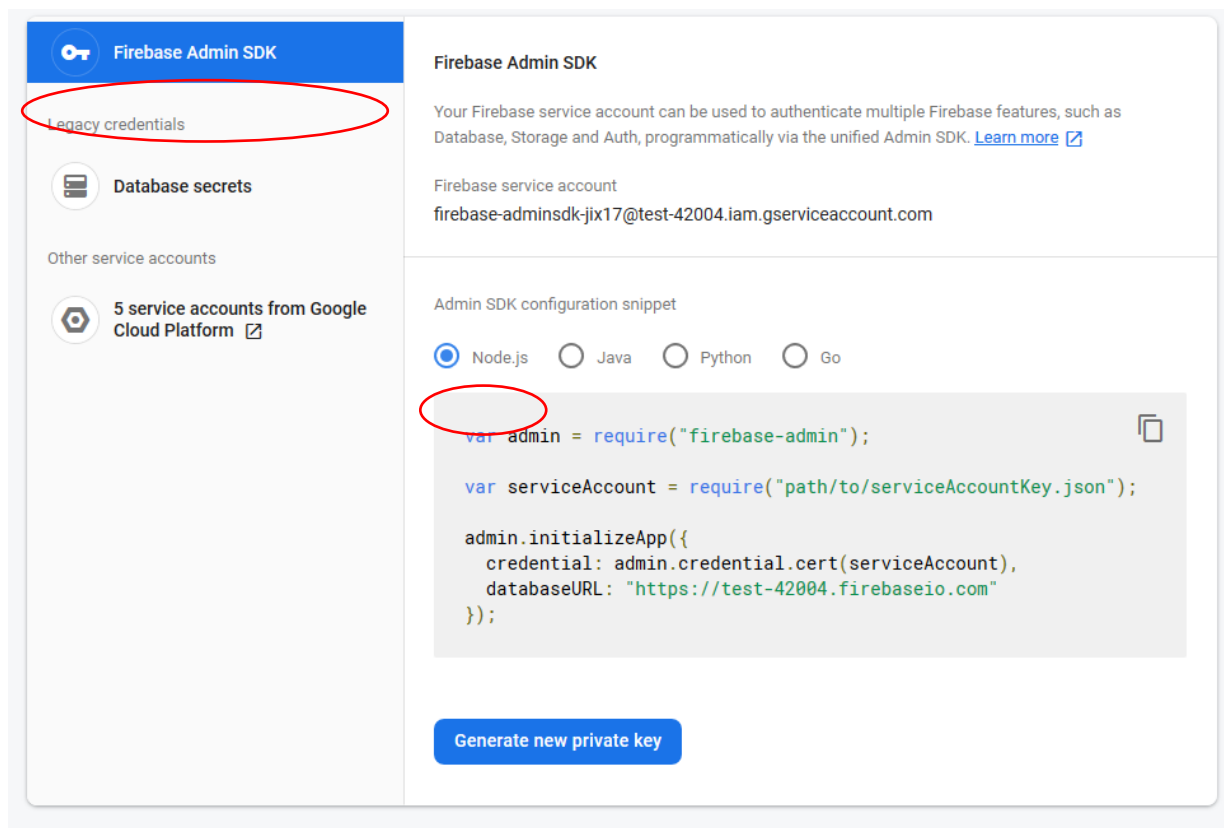
Log into firebase at <https://firebase.google.com/> with your goggle account or create a new account. Then click on “Go to console” in the toolbar.

Add a new project and give it a unique name (i.e. DoubleClue). Then select the new project.



Enter the 'Project Settings' by clicking on the gear icon at the top of the sidebar. Then choose the "Service Account" rider in the "Settings" top menu.

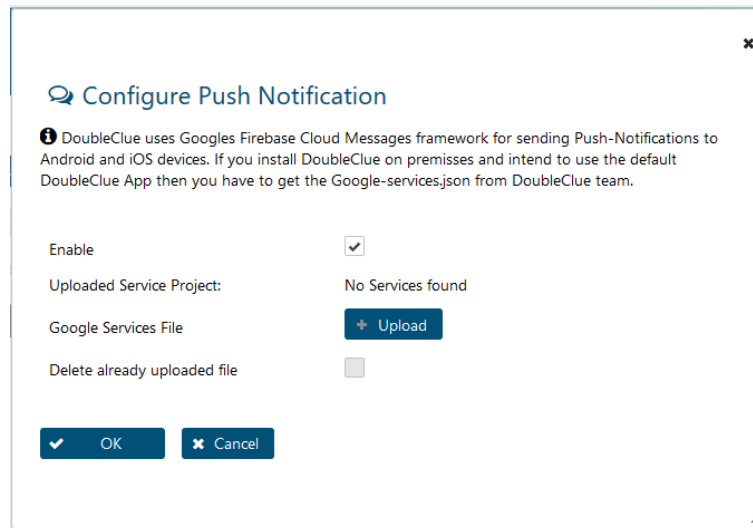
Ensure that you are in the "Firebase Admin SDK" area and Node.js has been selected, before hitting the "Generate new private key"-Button and create and download a json-file to configure your DCEM.



Please be aware that this file can't be restored! In case you need a new file, you have to generate a new private key and replace the file wherever it is used.

8.6.2 Configure Push Notification in DCEM

Log into DCEM and go to the main menu “Identity & Access”, sub-menu “Push Approvals” and click the “Configure Push Notification” button. This will open the configuration window.



Ensure that the “Enable” check box is checked. Then upload the files you downloaded from Firebase or received from DoubleClue under ‘Google Service File’. Confirm your input.

Detailed information about Firebase can be found at:

<https://firebase.google.com/docs/cloud-messaging/android/client>

8.6.3 Receiving a Push Notification

Not every time a user receives a Push Approval they also receive a push notification. There are certain circumstances under which a user may no push notification is sent.

Push Notification Token:

A user will only receive a push notification, when a push notification has been created by the device. This Token will be created when the user logs into the app on a device for the first time. Per default, the user will be automatically logged into the app during the activation process. There are, however, ways how the user can skip this step (e.g. closing the app during the activation process). In this case, the token won’t be created, and the device can’t receive push notifications from DoubleClue until the user has actually completed a log in for the first time. An administrator can view the Push Notification Token of a device by selecting the device in the list under “Identity & Access” > “Devices” and then clicking the “Show Push Notification Token” button.

Several Devices for one Account:

If several smart devices have been added to one account and all are currently offline (see chapter [8.2.3 Device Status](#)) only the device who was last online will receive a push notification.

DoubleClue App is Open and in the Foreground on a Device:

When a user has the DoubleClue app open and in the foreground on one of their devices, they won't receive a push notification. Instead one of the following scenarios will occur:

- User is logged into the Account that receives a Push Approval: The Push Approval will open in the device and the user can confirm it right away.
- User is logged into a different account than the one that receives the Push Approval: The user will receive a notification in the app that another account on the device received a Push Approval. To confirm or reject the Push Approval, the user will need to log out of the account and into the other account.
- The user is currently in the login screen and receives a Push Approval that can allow passwordless confirmation: The user will be automatically logged into the account that received the Push Approval and can approve it.
- The user is currently in the login screen and receives a Push Approval that demands a login with password to be confirmed: The user receives a notification in the app that they received a push approval for the respective account. To confirm or reject it, they need to log into the respective account.

8.7 App Versions

Each DoubleClue app has a version number. This version number must be registered with your DCEM. DCEM will reject requests from apps with version numbers that aren't registered with DCEM. If you use the official DoubleClue app, new versions will per default be automatically registered the moment a user tries to log into their app or register an account on an app with a new version number.

You can deactivate the automatic registration in under "Identity & Access" -> "Preferences" by unchecking "Enable App Auto Registration". In this case, you will need to add new app versions manually under "Identity & Access" -> "App Versions".

If an app version should only be used up to a certain point in time, you can set an expiration date (for example if you want your users to update on a newer version). Once an expiration date has been set, on each start of the app the users will see a warning informing them when the app is about to expire. If the expiration date is exceeded, logging into the app with this version will no longer be possible.

You can also mark a certain app version as a Test App. Select the app version in the list and click on "Edit" to access the settings for this app version. Check the box saying "Test App". If an app is marked as a Test App, DCEM will skip the validation of the device DNA when someone attempts a login or confirms a Push Approval with this app version. As this reduces the security of the DoubleClue mobile app, we advise to use this option only in certain test scenarios in which validating the device DNA interferes with the testing process.

8.8 AuthConnector

The Authentication Connector is required for the "DoubleClue Windows Login".

In order to add a new AuthConnector, go to main menu “Identity & Access”, sub menu “AuthConnector”. The AuthConnector needs to be given a unique name as you can have several AuthConnectors at a time.

For the “DoubleClue Windows Login” you need to download the secure “**AuthConnector.dcem**” file by clicking the button “Download”. For further steps, please refer to the manual “**DoubleClue Credential Provider for Windows.pdf**”.

8.9 Preferences

Here various settings for the end user app can be made.

Login Retry Counter:

Number of faulty login attempts before the account is disabled.

Login QR Code Response Time:

Define the amount of seconds a QR Code is valid. Once it expires a new one is created.

Keep Alive Connection:

Time span after which the connection to the app is automatically disconnected and an inactive user logged out (in seconds).

Delete Waiting Push Approval in Queue:

If set, all queued push approvals which are marked as “queued” will be removed from the queue when a new push approval is received. Therefore, only the newest Push Approval will be available.

Retry Activation Delay:

Duration till the activation is enabled again after having been disabled (in minutes).

Duration for Report / Push Approval Archive:

Please refer to chapter [12. Database Archive](#).

9. RADIUS

RADIUS is an authentication protocol between a network client and a server. In this case, DCEM is the RADIUS server. The authentication of the end user is done via username and password. DCEM enhances the features of RADIUS by a Two-Factor Authentication via Push Approval, Passcode, OTP Token, SMS or Voice Message (other authentication methods are currently not supported by RADIUS) which requires an additional confirmation by the end user app.

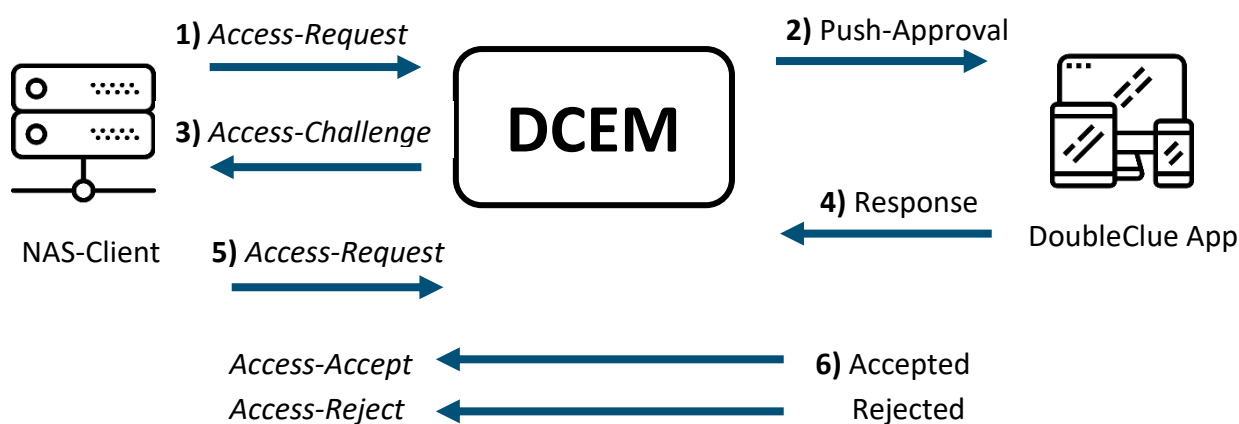
There are two possible RADIUS connections:

9.1 Without RADIUS Challenge



In this option, the NAS-Client does not get a response till the user has confirmed the request “1) Access-Request”. You need to set a maximum response time for the NAS-Client which is longer than the time the user has for the confirmation of the push approval “2) Approval”.

9.2 With RADIUS Challenge



In this alternative, the NAS-Client immediately gets an “3) Access-Challenge” from DCEM as a response to the “1) Access-Request”. It is not necessary to set a response time for this. The challenge message is a text message which is shown to the end user (“Please switch to your mobile app and confirm the message with code ... Then quit this message.”). You will find the text of the challenge message in the Text-Resources “radius.ClientChallenge” (main menu “Administration”, sub menü “Text-Resources”). There are two login templates for user confirmation, the “radius.Login” and the “radius.LoginChallenge” template. The content of these templates can be adapted if required.

The NAS-Client does not send a new access request to DCEM until the user has closed the challenge message. The access request is answered with “Access-Accept” or “Access-Reject”.

An advantage of “Access-Challenge” is that the user is shown a code that they can compare with the code in their app. By verifying the code, a higher level of security can be guaranteed.

9.3 NAS-Clients

DCEM supports several NAS-Clients that have to be configured each.

Name

Name of the NAS-Client which must be unique and can be chosen freely.

IP Number

IP address of the NAS-Client.

Shared Secret

Shared Secret of the NAS-Client that has to be entered in DCEM in order to establish a connection between the two.

Character Encoding

Define the character encoding standard you want to use for each individual NAS Client. DoubleClue supports three different character encoding standards:

1 - ISO 8859-1

2 - ISO 8859-2

3 - UTF-8

Please be aware that some RADIUS versions don't support UTF-8. This may cause problems when some of your users have umlauts or other special characters in their name. In this case, we advise to choose ISO 8859-1 as your character encoding standard.

Use Challenge

You need to choose if RADIUS Challenge should be used (see above).

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.

9.4 Preferences

RADIUS Authentication Port

By default, "1812" is set as "RADIUS Authentication Port". This can be changed if required.

RADIUS Accounting Port

By default, "0" is set as "RADIUS Accounting Port". "0" means that the port is disabled. You can enter a port if the NAS-Client needs this configuration.

Listen Adapter Address

If the connection from NAS-Client to server should only be possible via a certain IP address of the server, it has to be entered here.

Trace Data

If “Trace Data” is enabled, all communication data between NAS-Client and DCEM is recorded in the log file. This setting should not be enabled during live operation.

9.5 RADIUS Login with One Time Passcode

The following DoubleClue Authentication Methods provide the user with a One Time Passcode that needs to be entered alongside the password:

- DoubleClue Passcode
- OTP Token
- SMS
- Voice Mail

In most cases, a GUI solution is available for the user to enter the one time passcode in a separate field. In RADIUS, however, this isn't the case. The RADIUS login GUI is reduced to two entry fields: User ID and password. Therefore, the user needs to enter the one time passcode alongside the password into the password field. This has to follow a pre-defined syntax.

The passcode generated with the OTP Token, DoubleClue Passcode, SMS or Voice Mail is entered first into the password field. It is then followed by a slash / to separate it from the password. The password follows last.

Composition:

passcode/password

Example:

123456/mypassword

If the user wants to use another authentication method than the default method defined by the policy, they need to enter a prefix into the password field as described in chapter [7.2.4 Selecting an Authentication Method](#) in the paragraph ‘Pre-Selection’.

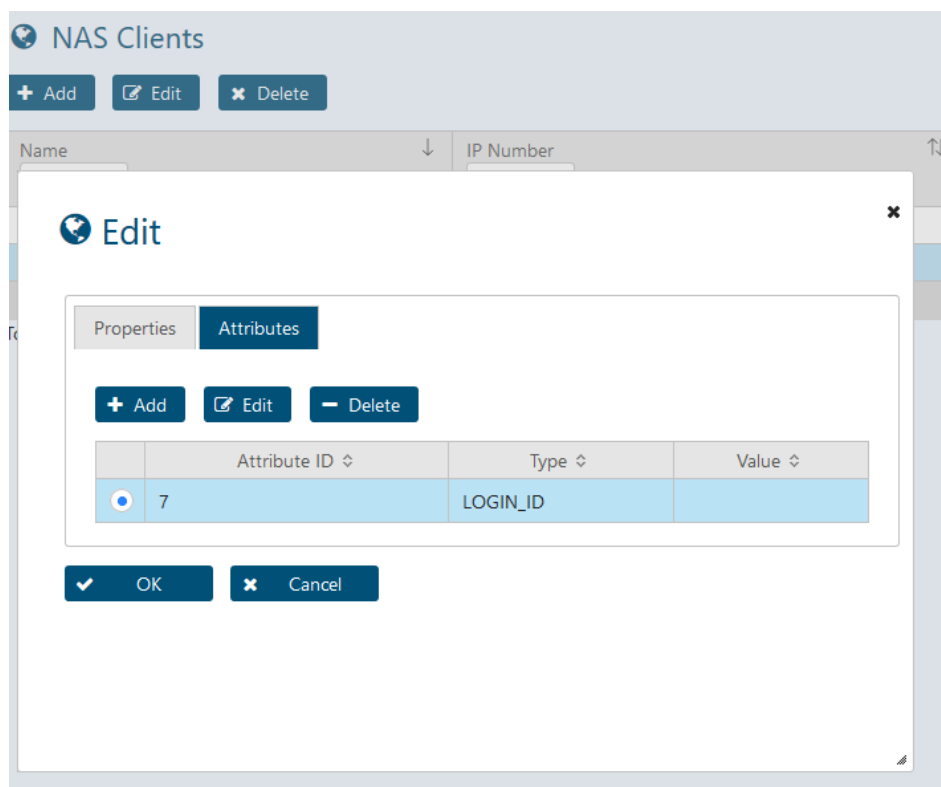
In this case, the prefix to determine the authentication method is entered at the first position into the password field and surrounded by two hashes ## at the beginning and the end. It is then followed by the one time passcode and password as described above.

Example for OTP Token:

##otp##123456/mypassword

9.6 RADIUS Attributes

You can define return attributes that are added to the RADIUS accept packets for each of your RADIUS NAS clients. In DCEM go to **RADIUS > NAS Clients** and choose the client you want to define the s for. Click on 'Edit'. You will see a dialog in which you can change the client settings. Select the 'Attributes' tab. You will now see a list of attributes that have already been defined for this client. In this dialog, you can add, delete or change these attributes.



You can assign the following attributetypes to the different attributes.

- User Login ID
- User Display Name
- User Account Name
- User Email
- User Principal Name
- User Telephone
- User Mobile
- User Locale
- User CloudSafe (contents of a user file)
- User Password
- Groups (with LDAP Filter – Advanced Attribute)
- Domain Attribute (returns any Active Directory Attribute value – Advanced Attribute)
- Policy Name (the policy name applied for this authentication – Advanced Attribute)
- AD ObjectGUID (unique ID for users in the Active directory – Advanced Attribute)

The corresponding information will then be attached to the RADIUS accept packet.

9.7 RADIUS Connector

The DoubleClue RADIUS Connector allows you to forge a connection between a DCEM running in the cloud and a NAS-client on premises. In such a scenario, the RADIUS connector acts as a RADIUS server on premises and forwards the user authentication information to DoubleClue in the cloud through a high security connection. You can find more information in the DoubleClue RADIUS Connector manual.

10. OTP Token

OTP tokens are single button hardware tokens that generate passcodes on demand. They work similar to the DoubleClue Passcode. During the login process, the user will be asked to generate and enter a digit code.



10.1 Configure OTP Token

1. Contact sales@doubleclue.com and order the needed amount of tokens.
2. Apart from the tokens, you will receive two e-mails each containing a txt-file: The token file and the password file. Save the files at a location where you can easily access them.
3. In DCEM, go to OTP Tokens -> Token-Config. and under import upload the token-file. Then copy the password from the password-file into the called Decryption-Key and save the changes. You should now see a list of the imported Tokens.
4. Hand out the tokens to the users. They can activate them themselves in the UserPortal if the necessary views and actions are enabled. Alternative you can assign the tokens to users in DCEM.

11. REST-Web Services

DCEM offers a REST-Web Services interface which can only be used for the SVC node.

The authentication of the REST-Web Services interface is done via the HTTP basic access authentication procedure.

In order to be able to establish a connection, please enter the following URL in your REST-Web Services interface:

http:// --Host name/IP of the server-- : Port /dcem/restApi/dc

To use this interface you need a DCEM operator who has the right to perform the action “restWebServices”. By default, the operator “**RestServicesOperator**” who has the necessary rights is offered after installation. The operator is disabled for use. In order to activate it, you need to make the following changes in the main menu “Administration”, sub menü “Operators”:

- Set a password for the operator.
- Enable the operator.

In the main menu “System”, sub menü “Cluster Configuration”, you can change the port and the safety settings if required.

You can execute the following methods via the REST-Web Services connection:

- addActivationCode
- addMessage
- addUser
- authenticate
- cancelMessage
- cancelUserMessages
- deleteUser
- echo
- getCloudData
- getMessageResponse
- getUser
- modifyUser
- queryLoginOtp
- queryLoginQrCode
- queryCloudData
- queryUsers
- requestLoginQrCode
- setCloudData
- verifyUser

11.1 Using the Existing “LibRestDcClient” for JAVA

The file “**LibRestDcClient-x.x.x.jar**” (x.x.x is the version number) is included in the delivery of the DCEM software. You can find this JAR file in the “**bin**” directory. If your customer portal is programmed with JAVA, you can use this file. The library is compiled with a Java 1.8 compiler.

Implement the existing JAR file in your customer portal.

11.2 Creating a New “LibRestDcClient” for other Programming Languages

If your customer portal is programmed in a different language than JAVA, you need to create the “**LibRestDcClient**” file for your customer portal first.

A complete library that you can use is available for you. You will find it under the name “**LibRestDcClient**”.

With *Swagger* (www.swagger.io) you can create your library in a different programming language. For this you need the “**DoubleClue.yaml**” file, which is included in the delivery of the DCEM software in the folder “**doc/REST-WebServices**”.

You will find more detailed information about the REST-Web Services interface in the following HTML document:

DCEM/doc/REST-WebServices/index.html

11.3 Demo of a Simple REST-Web Services Application

In the directory “**DCEM/doc/REST-WebServices/JavaSimpleDemo**”, you will find an example of a simple Java application which initializes the “**LibRestDcClient**” library, sends a Push Approval to a user and waits for the response. This will help you to start learning about the DCEM Rest-API.

12. SAML

SAML (Security Assertion Markup Language) is an open standard for the exchange of authentication data between an Identity Provider and a Service Provider. SAML is an XML-based markup language for security affirmations. The most important use case of SAML is web browser single sign-on (SSO).

12.1 Preparing DCEM to be an Identity Provider

12.1.1 DCEM SAML Trust Certificates

DoubleClue is a SAML Identity Provider and requires two different Trust Certificates:

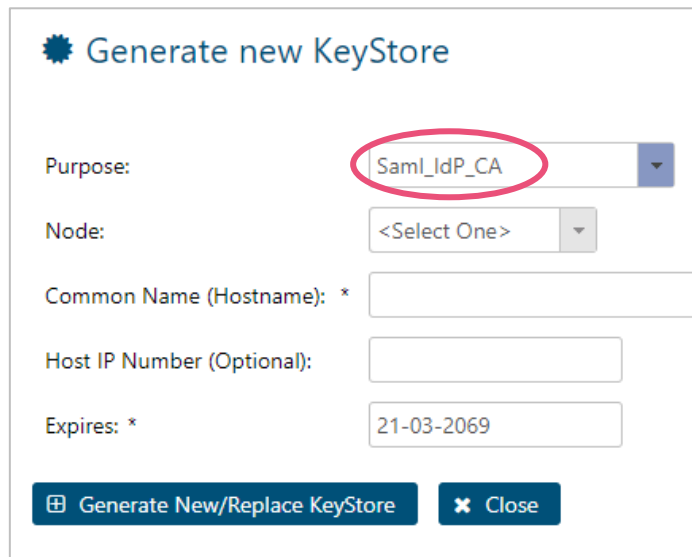
- SAML Identity Provider Certificate
- SAML Connection Certificate

Configure SAML in System > Cluster Configuration as described in chapter [3.1.3 Connection Service Settings](#).

12.1.1.1 SAML Identity Provider Certificate

The SAML Identity Provider Certificate is required to sign the metadata which DoubleClue returns to the SAML Service Provider. At the setup of DCEM, the KeyStore for this certificate is created automatically and is signed by the DCEM Root Certificate.

If you want to generate or install a new certificate, go to main menu item “System”, sub menu “KeyStores” and generate or upload a new KeyStore by clicking on the respective buttons and choosing the Purpose “**SAML_IdP_CA**”. For more information see chapter [3.3 KeyStores](#).



Generate new KeyStore

Purpose: **Saml_IdP_CA**

Node: <Select One>

Common Name (Hostname): *

Host IP Number (Optional):

Expires: * 21-03-2069

Generate New/Replace KeyStore **Close**

12.1.1.2 SAML HTTPS (SSL/TLS) Connection

As DoubleClue is a SAML Identity Provider, it has to be accessed over the internet from a user’s browser. The connection must be a secure connection using HTTPS (SSL/TLS). If SSL/TLS is terminated at DoubleClue, you have to obtain and upload an officially signed certificate from a worldwide known Certificate Authority.

For test purposes, you can also generate a new KeyStore certificate in DCEM. At DCEM setup a test KeyStore is generated for this purpose.

To upload an officially CA signed certificate, go to main menu item “System”, sub menu “KeyStores”, click on the button “Upload” and choose “**Saml_Connection_CA**” as purpose. Upload the PKCS#12 File.

12.1.2 Setting Up SAML Preferences

To set up SAML preferences, go to main menu item “SAML”, sub menu “Preferences”:

SSO Domain:

This should be an externally accessible base URL of the SAML SSO pages. Usually, it is the URL of the DCEM pages, but without “/dcem/mgt/index.xhtml” and with the port used for SAML.

IdP Entity ID:

Type in any name you desire. It is common practice to use the same text you entered for the SSO Domain to ensure uniqueness, but you may use any other name. In SAML, every Identity and Service Provider needs a globally unique Entity ID.






12.1.3 Downloading the Id Provider Metadata File

To download the Id Provider Metadata File, go to main menu item “SAML”, sub menu “Service Providers” and click on the button “Download IdP Metadata”. Click on “Download Metadata” and store the downloaded file in a place where you can find it for future reference. You may also want to download the X.509 signing certificate (in PEM format) by clicking “Download Certificate”.

12.1.4 Adding a Service Provider

DoubleClue supports several Service Providers. To add a Service Provider, go to main menu item “SAML”, sub menu “Service Providers” and click on the button “Add”. You can then choose the metadata of one of the pre-configured Service Providers from the menu, or create a custom one by choosing “Custom”. Once you have made your choice, click “Continue”.

Select SP Configuration:

	Custom
	LogMeIn
	Amazon Web Services
	Microsoft Azure
	DropBox



Continue



Cancel


If you choose to create a custom SP, there are two options on how to do this:

1. If you have an SP (Service Provider) XML Metadata File, go to the “XML” tab. Click on “Upload” to upload the respective file or copy the XML content into the text area “Metadata Content”. Finally, click on “OK” to save.



 Add
Display Name: Disabled: ☐

XML	Details	Signing	Attributes	IdP Settings
-----	---------	---------	------------	--------------

Upload a Service Provider (SP) metadata XML file by clicking the Upload button. Otherwise, copy the XML content into the text area below.

 Upload

Metadata Content

 OK
  Cancel

2. If you have no SP Metadata File, go to the “Details” tab.

Enter the SP’s unique Entity ID as well as its Assertion Consumer Service (ACS) Location. Change the NameID format to the one that matches what your SP uses for user identification.

If your SP supports Single Logout requests, you can enter a Single Logout Service URL, along with a specification whether to send logout requests via an HTTP POST or REDIRECT.

Optionally, you may also add an X.509 certificate (in PEM format) in the “Signing” tab if your SP signs SAML requests with a self-signed certificate (which is usually the case).

 Add ✕

Display Name:
 Disabled: ☐

XML
Details
Signing
Attributes
IdP Settings

Entity ID

Assertion Consumer Service Location

Single Logout Service Location (optional)

☒ HTTP Post
 ☐ HTTP Redirect

Expected NameID Format

Unspecified
▼

✓ OK
✕ Cancel

General properties:

- **Display Name:** A friendly name for the Service Provider. It will be displayed during logins so that users know where they are logging into. You may change it later if required. Please note that this is mandatory!
- **Disabled:** Check this box if you want to stop supporting a Service Provider without actually deleting its entry from the database.

Signing Tab:

A few Service Providers purposefully do not sign their SAML requests. This is not ideal, but is still supported by DCEM. If your SP behaves this way, you may uncheck “Requests are Signed”, so that DCEM knows not to expect signatures from the SP, and thus does not redirect to an error page during SSO logins. If your SP does indeed sign SAML requests (which is usually the case), **do not uncheck this**.

If your SP signs requests with a self-signed certificate (which is also usually the case), you may want to copy its certificate into the text area available. The certificate needs to be in a base64-encoded PEM format, excluding any headers or footers.

 Add

✕

Display Name: Disabled: ☐

XML
Details
Signing
Attributes
IdP Settings


Requests are Signed: ☒

X.509 Certificate for Request Signatures

Attributes Tab:

If your SP requires Attributes (additional data about users included in SAML responses), you can configure them in the “Attributes” tab. Any number of attributes may be added; just make sure their names match with what is expected by the SP. By choosing their Type, DCEM can map their values to user properties, such as the users’ ID, E-Mail or Phone Number. If you want to map info from the users’ Domain, choose Domain Attribute and type in the name of the attribute you want to read. You can also choose ‘Static Text’ and enter a value which will be the same for all users.

User Login ID
 User Display Name
 User Account Name
 User Email
 User Principal Name
 User Telephone
 User Mobile
 User Locale
 User CloudSafe (contents of a user file)
 Static Text
 Groups (with LDAP Filter – Advanced Attribute)
 Domain Attribute (returns any Active Directory Attribute value – Advanced Attribute)
 Policy Name (the policy name applied for this authentication – Advanced Attribute)
 AD ObjectGUID (unique ID for users in the Active directory – Advanced Attribute)

 Add ✕

Display Name:

Disabled: ☐

XML
Details
Signing
Attributes
IdP Settings

+ Add New Attribute
✎ Edit Attribute
- Delete Attribute

Name ↕	Type ↕	Value ↕
No records found.		

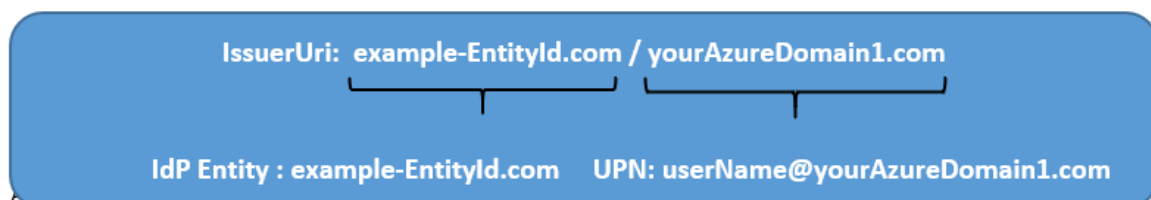
✓ OK
✕ Cancel

IdP Settings:

You can define further parameters concerning the signature and communication of the Identity Provider with the Service Provider in the “IdP Settings” (Identity Provider Settings) tab. The “Response Signature Algorithm” and “Response Digest Algorithm” are normally automatically determined by the Metadata. If you want to adjust them manually, check which algorithms are supported by the Service Provider. At „Response Canonicalization Algorithm“, you can choose how the assertion XML file has to be formatted, before it is signed. This setting rarely needs to be adjusted.

The setting “Add User Domain to IdP Entity ID” needs to be activated when you want to connect several domains of certain Service Providers with one DCEM. Some Service Providers (eg. Microsoft Azure) don’t allow that several of their domains are federated with the same Identity Provider. They demand that each domain needs to be connected to a separate Identity Provider with a unique Entity ID. You can solve this problem by activating “Add User Domain to IdP Entity ID”. DCEM will now send SAML responses with an IdP Entity ID that is composed of the one set in the SAML preferences, suffixed by a forward slash and the domain of the user who successfully logged in. Therefore, from the SP, make sure you configure each domain with an appropriate IdP ID that matches this description.

For example, if you have two domains in your SP, “dom1” and “dom2”, and your DCEM IdP Entity ID is “dceM”, dom1 needs to register with “dceM/dom1” while dom2 would use “dceM/dom2”.



Add

✕

Display Name:

Disabled: ☐

XML
Details
Signing
Attributes
IdP Settings

Response Signature Algorithm
RSA with SHA-256

Response Digest Algorithm
SHA-256

Response Canonicalization Algorithm
Exclusive without Comments

Trace Requests and Responses: ☐

Add User Domain to IdP Entity ID: ☐

✓ OK
✕ Cancel

12.2 Customizing the SAML Web Pages

The user SAML Web Pages can be customized to your needs.

To change the web pages, you require a good knowledge of the **Java Server Faces** (JSF) framework and **PrimeFaces** components (<https://www.primefaces.org/>).

The pages can be found at “**DCEM-Installation-Directory/WebContent/saml**”.

⚠ If you change the pages, you have to be careful when you do a DCEM update, because this will overwrite these pages to default again!

The pages apply to all languages. Texts are retrieved from the DCEM Text-Resources.

Example: `value="#{dbMsg['saml.error.expired']}"` with 'saml.error.expired' as the Text-Resource key.

13. OpenID

OpenID is an open standard and authentication protocol, which extends upon OAuth 2.0. It is utilized for the exchange of authentication data between an OpenID authentication server and an OpenID Resource Server.

13.1 Preparing DCEM to be an OpenID authentication server

13.1.1 Enable OpenID/OAuth in the Cluster Configuration

Ensure that OpenID/OAuth is enabled as a connection service under **System > Cluster Configuration**. If you want to change the configuration, like using a different than the default port, you can define those changes here. For more information on how to configure connection services, see chapter [3.1 Cluster Configuration](#).

13.1.2 DCEM OpenID Certificate

To secure the OpenID SSO pages with SSL, you need to set up a connection certificate.

13.1.2.1 OpenID Connection Certificate

If you want to generate or install a new certificate, go to main menu item “System”, sub menu “KeyStores” and generate or upload a new KeyStore by clicking on the respective buttons and choosing the Purpose “**OAuth_Connection_CA**”. Chose a Node and enter a “Hostname” to generate a new KeyStore or load up the respective file to upload one. Confirm your configuration.

13.1.2.2 OPENID HTTPS (SSL/TLS) Connection

As DoubleClue is an OpenID Authentication Server, it has to be accessed over the internet from a user’s browser. The connection must be a secure connection using HTTPS (SSL/TLS). If SSL/TLS is terminated at DoubleClue, you have to obtain and upload an officially signed certificate from a worldwide known Certificate Authority.

For test purposes, you can also generate a new KeyStore certificate in DCEM. During the DCEM setup a test KeyStore is generated for this purpose.

To upload an officially CA signed certificate, go to main menu item “System”, sub menu “KeyStores”, click on the button “Upload” and choose “**OAuth_Connection_CA**” as purpose. Upload the PKCS#12 File.

13.1.3 Setting Up OpenID Preferences

To set up OpenID preferences, go to main menu item “OpenID - OAuth”, sub menu “Preferences”:

- Issuer:
This should be an externally accessible base URL of the OAuth SSO pages. Usually, it is the URL of the DCEM pages, but without “/dcem/mgt/index.xhtml” and with the port used for OAuth.
- Token Configuration:
These settings allow you to configure the lifetime of Authorisation Codes, Access Tokens, Refresh Tokens and ID Tokens by defining the number of seconds.
- SSO Service:
In this section you can define whether or not users need to enter their password in the SSO login page, whether login via QR Code shall be allowed, and if so, whether it is the first page to be shown.

Preferences

Save

- Authorisation Server Metadata

Issuer

- Token Configuration

Authorisation Code Lifetime

Access Token Lifetime

Refresh Token Lifetime

Id Token Lifetime

- SSO Service

Password Required
 ☒

Enable Redirection to Device Manager
 ☒

If you wish to review the OpenID configuration you can see the JSON file via:
 <issuer>/dcecm/oauth/.well-known/openid-configuration.

13.1.4 Add an OpenID Client

To add an OpenID Client, go to main menu item “OpenID/OAuth”, sub menu “Service Providers” and click on the button “Add”.

Add

Display Name:

Disabled: ☐

Details
 Claims
 IdP Settings

Client ID *

Client Secret *

Redirect URIs

General properties:

- **Display Name:** A user friendly name for the OpenID Client. It will be displayed during logins so that users know where they are logging into. You may change it later if required. Please note that this is mandatory!
- **Disabled:** Check this box if you want to stop supporting a Service Provider without actually deleting its entry from the database.

Client ID and Client Secret

If you already have access to an Open ID Client in form of a website supporting OpenID and already possess Client credentials, enter them in the respective fields.

If not, you can enter a Client ID and Client secret here and set them up on the client. While you could enter them manually, we would advise using the generate button to generate them automatically for security reasons.

You can further define the client's redirect URIs as a comma-separated list. While this is in general an optional setting, it might be required by some OpenID clients.

Once you have entered your configurations click "OK" to save the changes.

13.1.5 Claims

If your resource client requires claims, additional information about users provided in the response, you can configure them in the "Claims" tab. Any number of attributes may be added; just make sure their names match with what is expected by the resource server. By choosing their Type, DCEM can map their values to user properties, such as the users' ID, E-Mail or Phone Number. If you want to map info from the users' Domain, choose Domain Attribute and type in the name of the attribute you want to read. You can also choose Custom Text and enter a value which will be the same for all users.

The following claim types are available for OpenID in DoubleClue.


- User Login ID
- User Display Name
- User Account Name
- User Email
- User Principal Name
- User Telephone
- User Mobile
- User Locale
- User CloudSafe
- User Password
- Static Text
- Authenticator Passcode
- Groups (with LDAP Filter – Advanced Claims)
- Domain Attribute (returns any Active Directory Attribute value – Advanced Claims)
- Policy Name (the policy name applied for this authentication – Advanced Claims)
- AD ObjectGUID (unique ID for users in the Active Directory – Advanced Claims)

13.2 Customizing the OpenID Web Pages

The user OpenID Web Pages can be customized to your needs.

To change the web pages, you require a good knowledge of the **Java Server Faces** (JSF) framework and **PrimeFaces** components (<https://www.primefaces.org/>).

The pages can be found at “**DCEM-Installation-Directory/WebContent/oauth**”.

 If you change the pages, you have to be careful when you do a DCEM update, because this will overwrite these pages to default again!

The pages apply to all languages. Texts are retrieved from the DCEM Text-Resources.

Example: `value="#{dbMsg['sso.error.expired']}"` with 'sso.error.expired' as the Text-Resource key.

14. Database Archive

The following database tables with records older than a configurable setting in days can be regularly archived to ZIP files:

- Administration: Change History
- Identity & Access: Push Approvals
- Identity & Access: Reporting
- RADIUS: Reporting

The archiving process runs on every first day of the month. All entries which are older than a certain pre-configured time period are then automatically archived in ZIP files in the folder “**DCEM_HOME/archive**” of your DCEM Installation and deleted from the database.

Please note that on a multi-node cluster environment the files are stored only on the master node, which is the oldest running node.

You can set the time period (in days), after which records are automatically archived, the following way:

- History Archive: Administration > Preferences > Duration for History Archive
- Report Archive: Administration > Preferences > Duration for Report Archive
- Push Approval Archive: Identity & Access > Preferences > Duration for Push Approval Archive
- RADIUS Report Archive: RADIUS > Preferences > Duration for Report Archive

If you set the time period to “0”, automatic archiving will be turned off.

15. UserPortal

UserPortal is a self-service portal for DoubleClue users. It can be accessed over the URL **<https://www.hostname/dcem/userportal>** or when supporting multi-tenants over **<https://www.tenantname/hostname/dcem/userportal>**.

UserPortal offers users the possibility to register themselves, manage the Smart Devices, FIDO and OTP tokens connected to their account and access their CloudSafe and PasswordSafe. In UserPortal configuration, the administrators determine which of these options are available to the users.

15.1 Configuration

It is necessary to configure UserPortal for each sub-tenant individually. The different sub-tenants will not adopt the settings if the main-tenant if no individual configuration has been defined.

15.1.1 General Settings

- Title:
If you wish to rename ,UserPortal', enter the title in this field.
- Activate Captcha:
Determine if you want to secure the user registration via UserPortal with a captcha. For the captcha to work properly, you will need to configure it. See Chapter [14.1.3 Captcha Configuration with Google reCAPTCHA v2](#) for more information.
- Allow registration for local / domain users
Determine which kind of users can register themselves in UserPortal.
- Message Type
Determine which type of message will be used to send activation codes.

15.1.2 Configuration of the Visible Elements

15.1.2.1 Visible Views

Define which parts of UserPortal the users will be able to see. No views not set to visible will not be visible to users under any circumstances. Users will not be able to use any actions placed on one of them.

15.1.2.2 Views requiring multi-factor authentication

In this section you can choose, which visible views shall only be displayed if the users have identified themselves with multi-factor authentication. Take into consideration that only views which have been chosen as “Visible Views” will be affected by this. Views not set to visible will be invisible with or without MFA.

15.1.2.3 Visible Actions


Choose which actions shall be available in UserPortal. To gain access to the actions, the view in which the action can be found must be visible.

15.1.2.4 Actions requiring multi-factor authentication

Choose which actions require the user to identify themselves with multi-factor authentication to be accessible. Like before, those actions need to set to visible under „Visible Actions“ as well as being part of a visible view. If they aren’t, users will not be able to use them, no matter how they identified themselves.

15.1.3 Captcha Konfiguration with Google reCAPTCHA v2

Visit <https://www.google.com/recaptcha/> and log into the ‘Administration Console’. Register your DoubleClue domain for reCAPTCHA v2. You will receive two reCAPTCHA-Keys, the public key and the private or secret key.

 Leave this page open or copy the keys to a save location. You will need them later.

When using multi-tenants with subdomains, it will suffice to register the main-domain. You do not need to register the different sub-domains.

Log into DCEM and navigate to System main menu, sub menu item Preferences. Go to the ‘Google CAPTCHA’ section and enter the Public Key and the Private Key you received into the respective fields. Save the changes and restart DCEM. The changes will be activated after the restart of DCEM.

16. Licencing System

The DoubleClue Licencing System implements conditions on software usage.

Currently, we offer one category of licences which are connected to the Identity Management module. Go to main menu item “Administration”, sub menu “Licences”. The following licence terms apply:

- Expiry Date: Duration of software usage.

- **Maximum Users:** Maximum number of active users.
Active users are all users that have been added either as local users or through a domain and are enabled. If you have reached the maximum number of active uses, you won't be able to add anymore users.
- **Trial Version:** This attribute indicates a non-productive licence. An alert will always be shown when logging into DCEM and DoubleClue App.
- **Maximum CloudStorage MByte:** The amount of storage available in the CloudSafe in MB

After a new DCEM installation the licence terms are set as follows:

- Expires on: Date of the installation plus 30 days
- Maximum Users: 100
- Maximum CloudSafe Storage: 50
- Trial Version: true
- PasswordSafe: true

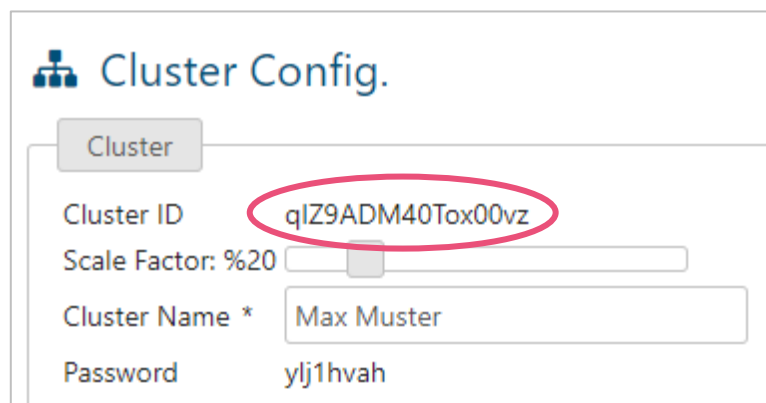
16.1 Applying for a New Licence Key

A new licence can be applied for after a test phase.

We can issue a new licence for you, once we receive the following information:

- Company Name
- Contact Person
- E-Mail Address
- Company Address
- DCEM Cluster ID

You can find your DCEM Cluster ID under the main menu item "System", sub menu "Cluster Configuration".



Cluster Config.

Cluster

Cluster ID: qIZ9ADM40Tox00vz

Scale Factor: %20

Cluster Name *: Max Muster

Password: ylj1hvah

Send this information to sales@doubleclue.com.

After consultation with the Sales Department you will receive a new licence key by email.

16.2 Adding a Licence Key

Go to main menu item “System”, sub menu “Licences” and click on the button “Import Licence Key”.

Paste the licence key that you received beforehand in the input field and click on “OK”. Check the licence terms shown.

16.3 Viewing the Licences

Installed licences can be viewed under the main menu item “System”, sub menu “Licences”, too.

17. Logging

DCEM has a sophisticated logging system. The system saves all events which may be required for further analysis.

For this purpose, DCEM integrates the logging framework from Apache Log4j Version 2.

The following logging levels exist:

- Error: The Administrator has to react when an error level is written.
- Warning: The Administrator has to check this.
- Information
- Debug: The Administrator should not enable this on productive servers unless instructed to by the DoubleClue support team.
- Trace: The Administrator should not enable this on productive servers unless instructed to by the DoubleClue support team.

17.1 Configuration

The logging configuration is read from “**DCEM_HOME/log4j2.xml**” at DCEM startup.

The log levels can be changed in the DCEM GUI system preferences.

For details about this configuration please refer to <https://logging.apache.org/log4j/2.x/manual/>

17.2 File Output

The logging outputs the data in five rollover files.

The current file name is “**dcem.log**” and the most recent files are named “**dcem_1.log**” to “**dcem_4.log**” respectively. This is always enabled by default.

These output files are written in the “**DCEM_HOME/logs**” directory. The log files from all nodes can also be downloaded into the DCEM GUI by going to the main menu item “System”, sub menu “Diagnostics”, and clicking on the button “Download Log-Files”.

17.3 SysLog Output

The logging can output the data to a SysLog Daemon using TCP or UDP. For this purpose, you need a SysLog Daemon. This output type is disabled by default. You will have to configure it manually.

17.4 Enabling the SysLog

1. Open the file “**DCEM_HOME/log4j2.xml**” with a text editor.
2. Look for the following text:

```
<!-- <Syslog name="syslog" format="RFC5424" host="localhost"
port="514" protocol="TCP" appName="DoubleClue" includeMDC="true"
enterpriseNumber="35705" newLine="true" messageId="Audit"
id="App" mdcId="mdc" /> -->
```

3. Remove the XML start comment “<!--” and end comment “-->” sequence.
4. Configure the correct host and port.
5. Remove the XML start and end comments sequences for:

```
<!-- <AppenderRef ref="syslog" /> -->
```

6. Restart DCEM.

18. PasswordSafe

PasswordSafe is a password manager with an integrated single sign-on feature that is available for DoubleClue users in UserPortal. It allows users to securely store their credentials and shorten future logins to one click on the respective tile in UserPortal.

In DCEM, you can pre-define web applications for users and add new applications according to your user’s needs. Users can also add applications by themselves and record the Auto Login Process

themselves in the UserPortal, however prerecording web applications regularly used in your company will save your users a lot of time.

PasswordSafe also implements two-factor authenticators with OTP like Google or Microsoft Authenticator. The OTP codes can either be read in the UserPortal or the Mobile app and then entered manually or automatically entered when using the single sign-on feature in UserPortal and the OTP process has been recorded as part of the Auto Login Process for this application.

You can configure PasswordSafe in DCEM under 'UserPortal' > 'PasswordSafe Config.'. If you can't see this view, check if you have the right access rights under 'Administration' > 'Access Rights'.

18.1 DoubleClue PasswordSafe Extension for Browsers

To enable DoubleClue to access the login masks of web applications in your browser, you need to install the DoubleClue PasswordSafe Add-on. This extension is available for Chrome, Firefox, MS Edge and Safari in the respective add-on and extension sections. If you need a version for another browser, please contact support@doubleclue.com.

18.2 Configuration of Applications

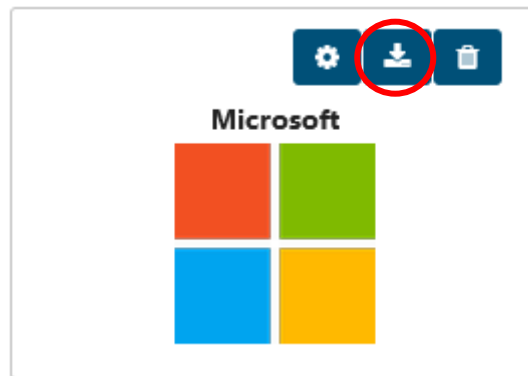
DoubleClue comes with several pre-configured applications. Per default, all these applications will be available to your users in UserPortal without any further actions on your part.

We advise to check the list of applications and remove those applications you don't want to be available for your users in PasswordSafe. However, users will still be able to add this web application and record login process on their own

18.3 Import and Export Applications

Configured applications can be imported and exported via special files that end on the extension .dcMyapp. DoubleClue comes with several preconfigured applications. Their files are available in the myApplications folder in the installation directory.

You can import an application file by simply clicking on the import button and uploading the respective file. You can also export every configured application by clicking on the export button in the respective tile.



If you want to change an already configured application, we advise to use export as a backup. If you have a problem configuring an application, please export the file and send it to doubleclue@support.com. This will provide us with valuable information on analyzing the problem and sending you a functional application file.

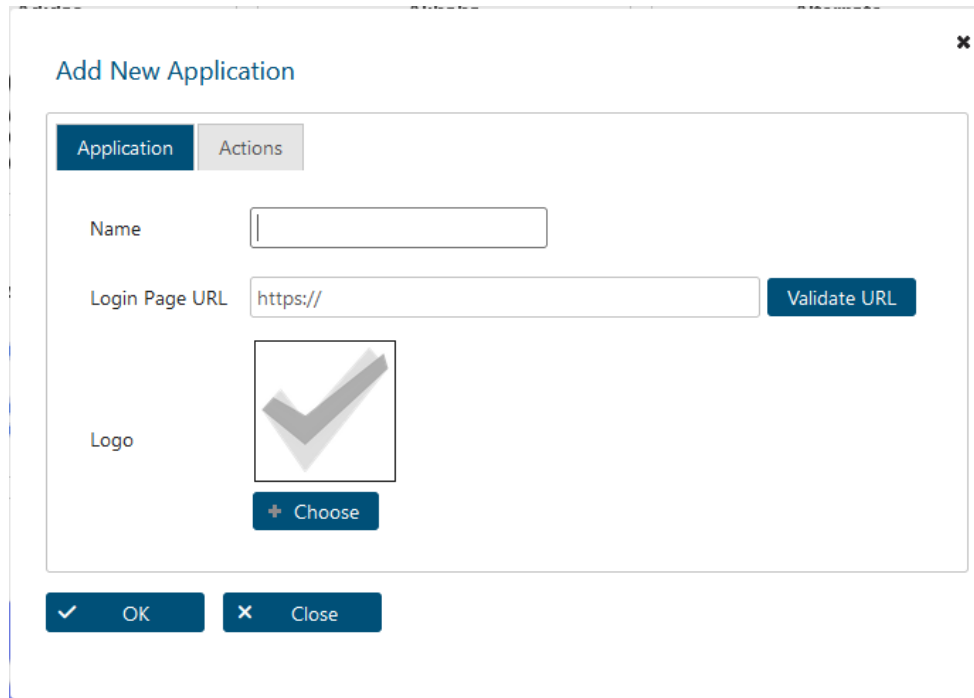
18.4 Add Applications

You can add further applications to be available in UserPortal. Start by simply clicking on the 'Add'-button at the top of the view. This will open a dialogue in which you can configure the new application.

If you have problems configuring certain applications, please contact support@doubleclue.com. We can help you to configure the application and provide you with a file to import applications if the application in question can be accessed freely from the internet.

18.4.1 Application

In the application tab, you can define the general settings of the app. Enter the name of the application. This is the name which the users will see in UserPortal and can be chosen freely. Then enter the login URL of the web application. Please ensure that the entered URL is the direct link to the login page, not the to the main page (eg. https://example_application.com/login instead of https://example_application.com). Click on 'Validate URL'. DCEM will now test if the URL can be reached. It will also add the fav icon of the site as logo of the app. If no favicon is available or you want to use another logo, you can choose a bitmap with the '+ Choose' button.



18.4.2 Actions

In the 'Actions' tab you can define the different elements of the web application's login mask necessary for the auto login process.

18.4.2.1 Recorder Assistant

We advise to use the 'Recorder Assistant' to define the actions for a new application. The 'Recorder Assistant' will automatically open the login url entered under 'Application'. Once you are on the login page, click onto the first element of the login (normally the login id or e-mail field). A DCEM popup will open. In this popup you can see the CSS selector for the field and enter the value. During the login, DoubleClue will then search for a fitting name in the PasswordSafe file. The value for the login id should always be 'Username', even if the application asks for an email address or other ID. After having entered the name, click on 'Add Element'.



If the element is the next step in the login process, insert a display name and confirm to add it to SSO process.

Selector : `#app > div > div:nth-of-type(3) > form > div:nth-of-type(1) > input`

Value :

Add Element **Final Action** **Ignore Field**

Stop Recording

Continue to the second element (normally the password field or the 'Next' button in login scenarios that are split up over several pages) until all necessary elements (fields and buttons) have been added this way. Ensure that the Value for the Password is 'Password'. When you reached the last element, click on 'Final Action' instead of 'Add Element' to return to DCEM.

If you need to click onto another element that is not part of the log in process during the recording, for example to close a pop up or similar, ensure to click on the 'Ignore Field' button, so that this 'Action' is not added to the recorded process.

Some login scenarios do not have all the necessary fields and steps on one site but will direct you through several pages. In such scenarios, each time after which a button is used (except for the last one) a two second delay is automatically added to the process. This shall give the service enough time to open the new page, so that the fields are accessible when the credentials are entered. If you have a quick internet connection and device, you can manually reduce this time, to allow for a quicker login process. However, if the auto login tries to proceed with the next step of the login before the page is loaded, this process will be interrupted. You can find more information on how to manually edit 'Actions' in chapter 18.4.2.2 Add and Edit Actions Manually.

Ensure that you record all the actions necessary for the login process. In some scenarios, certain steps will only become available during the process. For example, when a login is protected with optional MFA, the MFA option will only be displayed after the entering login ID and password if MFA has been activated for this account. To record this part of the process, you will therefore need an account with active MFA.

If you want to cancel the recording process at any point, press the 'Stop Recording' button.

⚠ Some homepages block or limit the access of extensions. On those homepages, the 'Record Assistant' may not work correctly. In this case, you will have to add the actions manually.

⚠ If the Auto Login for an application doesn't work correctly after recording it with the Recorder Assistant, we advise to check all the CSS-Selectors manually. You can find more information about how to manually edit Actions in the next chapter.

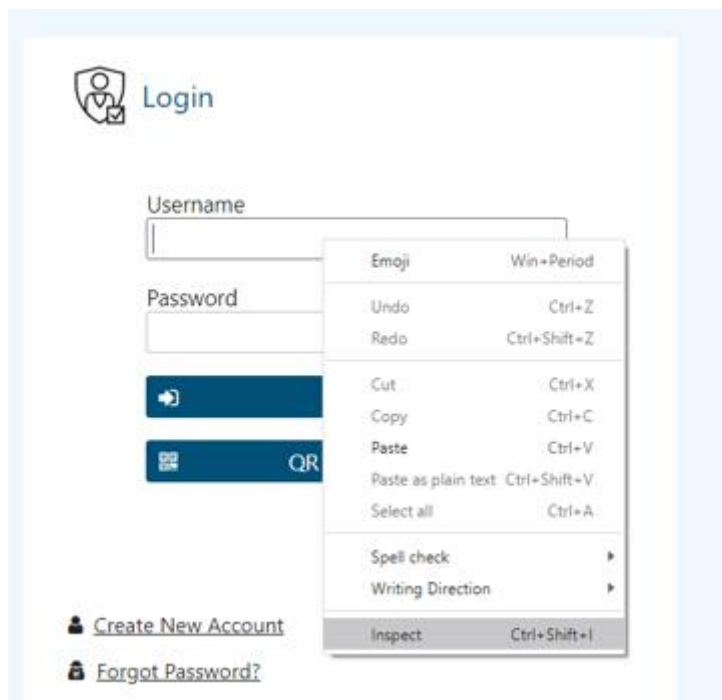
18.4.2.2 Add and Edit Actions Manually

If using the 'Recorder Assistant' is not possible or you want to adjust some of the recorded actions, you can add and edit actions manually. To add an action, just click on the '+ Add' button. The new action will always be added at the bottom of the list, but you can change the order of the actions via drag & drop.

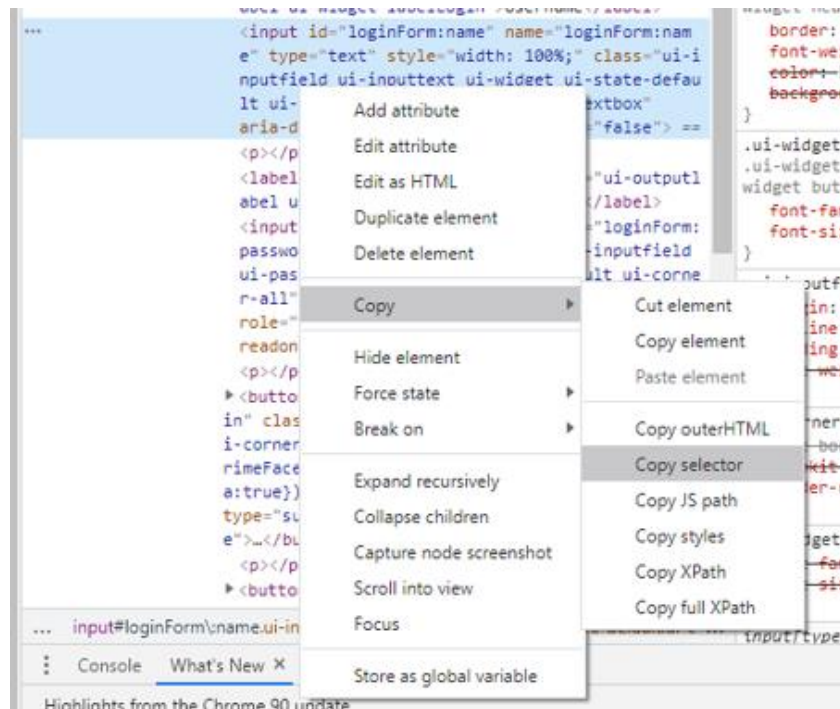
Each action is defined by four parameters: Type, CSS Selector, Value Type and Value. Depending on the Type, not all the parameters need to continue a value. Only a Type must always be selected.

Types: There are three Types of actions available: Button, Input Field and Delay. Button is for buttons used in the login masks, Input Fields is used for all kind of input fields in the login mask and Delay is to give the service time to open new pages and validate credentials in login scenarios that are spread out over several pages.

CSS Selector: This is the CSS Selector by which the element on the site is identified. Only buttons and input fields have a CSS Selector. For Delays this field stays empty. If you want to define CSS Selector to an action manually, open the respective login site and right click into the element whose action you want to add. Then select the option 'Select' in the menu that will open. This will open the developer console. Developer consoles are part of most modern browser. If your browser doesn't support this option, we advise to try Google Chrome or Firefox.



In the developer console you will see the element you have chosen already selected in the code. Right click on the marked area and in the menu go to 'Copy' and then 'Copy Selector'. You can now paste the selector into the field in the action dialogue.



Value Type: Value Types are only defined for input field actions. There are several Value Type options.

- **Static Text:** A Static Text as defined by the administrator is entered into the field each time the action is executed. Static text will be displayed in plain text in the actions overview windows (other options will be displayed in braces). This option should be chosen if the information entered the field should be the same for every login process (e.g. a domain name that is the same for all users).
- **PasswordSafe Entry-Input:** If the value is set to PasswordSafe Entry-Input, then the entered information is retrieved from the data that the user stored in the keepass file. This option should be chosen for services whose accounts are managed independent from DoubleClue or active directory.
- **Authenticator Passcode:** Choose this value type for the into which the OTP Passcode is entered during login processes using 2FA.
- **Attributes (e.g. User Account Name, User Email):** The input entered the field is taken from the user information saved in DoubleClue or an Active Directory. This option should be chosen when the account and/or credentials is connected to the information stored in DoubleClue through active directory or similar.

Value: This is the value that will be entered during the auto login process. For Delays this is always a number indicating the seconds the delay lasts.

For Input Fields, it depends on what was chosen as Value Type. If the Value Type is a Static Text (the text shall be the same for all logins for all users), enter the respective text you want to be entered. If the Value Type is PasswordSafe Entry-Input, the Value should be name of the credential you want to retrieve from the PasswordSafe entry. In most cases this will be Username or Password. Other values can be used as well but need to be added as custom properties by the user in the PasswordSafe entry. If the Value Type is Authenticator Passcode or an Attribute, the value will be set automatically. Buttons don't have a value.

19. Additional Services

19.1 PortalDemo

DoubleClue PortalDemo is a test software with which you can test the functions of the product DoubleClue without having implemented the software in your portal beforehand.

For the installation and usage of PortalDemo, please read **DcemInstallation/doc/DC_Manual_PortalDemo.pdf**.

The PortalDemo enables you to test all authentication methods.

After having logged in, you can test the transaction “Money Transfer” where a message has to be confirmed with the end user app.

19.2 Credential Provider for Windows

DoubleClue Credential Provider for Windows is a software package, which enables DoubleClue to be integrated into Windows’ native Logon UI process. Users are prompted to authenticate themselves with one of DoubleClue’s many multi-factor authentication (MFA) methods in order to be able to log into their Windows machines.

For the installation and use of Credential Provider for Windows, please read **DcemInstallation/Manuals/pdf/English/Manuals/DoubleClue Credential Provider for Windows_EN.pdf**

19.3 HealthCheckDetector

DoubleClue HealthCheckDetector is a standalone service which checks if DCEM is up and running. Thereby, it logs any errors that may arise during the monitoring.

For the installation and use of DoubleClue HealthCheckDetector, please read **DcemInstallation/Manuals/pdf/English/Manuals/DoubleClue HealthCheckDetector.pdf**