



Benutzerhandbuch

DoubleClue Enterprise Management (DCEM)

Version: 2.1.1

Inhaltsverzeichnis

1.	Einleitung	7
2.	Installation und Inbetriebnahme	8
2.1	Voraussetzungen	8
2.1.1	Hardware-Voraussetzungen	8
2.1.2	Datenbank-Voraussetzungen.....	8
2.2	Informationen zur Installation	8
2.3	Installation	9
2.3.1	Installation auf Windows	9
2.3.2	Installation auf Linux.....	10
2.3.3	Installation mit einem Headless-Betriebssystem	10
2.3.4	Installation erneut ausführen	10
2.4	Datenbank-Konfiguration	11
2.4.1	Integrierte Datenbank / "Embedded Database"	11
2.4.2	Externe Datenbank	12
2.4.2.3	<i>Konfiguration einer Postgre-Datenbank als externe DCEM-Datenbank</i>	15
2.5	DCEM unter Linux als Daemon installieren	15
2.6	Datenbank-Migration.....	16
2.6.1	Migration mit Windows	16
2.6.2	Migration mit Linux.....	16
2.6.3	Ablauf der Migration.....	17
2.7	Anmeldung bei DCEM	17
2.7.1	Login mit Benutzername und Passwort.....	17
2.7.2	Login mit DoubleClue Multi-Faktor-Authentifizierung	18
2.8	Anmeldung bei DCEM	18
2.8.1	Datei "configuration.xml"	18
2.8.2	Ordner "DCEM_HOME"	19
3	DCEM-Systemhauptmenü.....	19
3.1	Clusterkonfiguration	19
3.1.1	Allgemeine Einstellungen.....	20
3.1.2	Verbindungsdienste	21
3.2	Clusterknoten.....	24
3.2.1	Installation eines weiteren Knotens	24
3.2.2	Clusterknoten hinzufügen.....	25
3.2.2.1	<i>Knotennamen festlegen</i>	25
3.2.2.2	<i>Knotentyp festlegen</i>	25

3.2.2.3	KeyStore anlegen	27
3.2.2.4	Bestätigung	27
3.3	KeyStores	28
3.3.1	Neuen KeyStore hinzufügen	28
3.4	Mögliche Verbindungen zum Endnutzer	28
3.4.2	SSL/TLS vom Endnutzer terminiert beim Load Balancer und ungesichert zu DCEM	29
3.4.3	SSL/TLS vom Endnutzer terminiert beim Load Balancer und gesichert zu DCEM	30
3.4.4	SSL/TLS vom Endnutzer terminiert bei DCEM mit Load Balancer (Passthrough)	31
3.4.5	SDK-Konfigurationsdatei	32
3.5	Neuen KeyStore hochladen	32
3.6	Cluster-Netzwerk-Kommunikation	32
3.6.1	Ein Netzwerk	32
3.6.2	Mehrere Netzwerke mit Multicast	32
3.6.3	Mehrere Netzwerke ohne Multicast.....	32
4	Administration	33
4.1	Benutzer.....	33
4.1.1	Benutzer hinzufügen	33
4.1.2	Benutzer Anmeldename	34
4.1.3	Benutzerpasswort	34
4.1.4	Hinzufügen eines Aktivierungscodes	34
4.1.5	Telefon- und Mobilnummer.....	35
4.1.6	Benutzerpasswort wiederherstellen.....	35
4.1.7	Gesperrte Benutzer	35
4.2	Rollen	35
4.3	SuperAdmin-Zugriff wiederherstellen	36
4.4	Zugriffsrechte	37
4.5	Gruppen	38
4.6	Integration von Active Directory / Microsoft Azure AD / LDAP	38
4.6.1	Hinzufügen einer standardmäßigen Active Directory-Konfiguration	38
4.6.2	Hinzufügen einer Azure AD-Konfiguration.....	39
4.6.3	Hinzufügen einer LDAP-Konfiguration	39
4.6.4	Import von Benutzern aus Gruppen aus einer Domäne.....	40
4.7	Vorlagen	41
4.7.1	Aufbau einer Vorlage	41
4.8	Textquellen	43
4.9	Änderungshistorie.....	44

4.10	Lizenzen.....	44
4.11	Einstellungen.....	44
5.	Mandantenfähigkeit (Multi-Tenant)	44
5.1	Konzept	45
5.2	Mandanten als Subdomains	45
5.3	Management mehrerer Mandanten	45
5.4	Anmeldeszenarien bei mehreren Mandanten.....	46
5.4.1	Anmeldung via Subdomain bei mehreren Mandanten	46
5.4.2	App- und RADIUS-Anmeldung bei mehreren Mandanten.....	46
5.4.3	Alternativ: Anmeldung mit mandantenspezifischen Benutzernamen	47
5.5	Lizenzen für Mandanten	47
6.	Verbindungsszenarien	47
6.1	Überblick	47
6.1.1	Direkte Verbindung mit eigener App.....	47
6.1.2	Dispatcher-Verbindung	48
6.1.3	Reverse-Proxy-Verbindung	50
6.2	Konfiguration	51
6.2.1	Konfiguration des DoubleClue-Dispatchers	51
6.2.2	Konfiguration von DCEM für Reverse-Proxy.....	52
6.3	Die DoubleClue-App.....	53
7.	Authentifizierungsmethoden und Policies.....	53
7.1	Authentifizierungsmethoden.....	53
7.1.1	Push Approval	54
7.1.2	QR-Code Approval.....	54
7.1.3	FIDO U2F Token	55
7.1.4	OTP Token	55
7.1.5	DoubleClue Passcode.....	56
7.1.6	Passwort.....	56
7.1.7	SMS / Voice Message	56
7.2	Policies und Anwendungen.....	57
7.2.1	Policies hinzufügen und konfigurieren	57
7.2.2	Anwendungstypen	58
7.2.3	Zuweisung von Policies	58
7.2.4	Auswahl einer Authentifizierungsmethode	59
8.	Identity-Management.....	60
8.1	Aktivierungs-codes	60

8.2	Smart Devices	60
8.2.1	Gesperrtes Smart Device	60
8.2.2	Smart Device löschen.....	61
8.3	FIDO-Authentifikatoren	61
8.4	CloudSafe	61
8.4.1	CloudSafe License und Verteilung des Speicherplatzes an die Benutzer	61
8.4.2	Dateiinformation.....	62
8.4.3	Dateien mit individuellem Passwort	63
8.5	Push Approval	63
8.5.1	Eigenschaften einer Push Approval	63
8.5.2	Einstellungen für Push Approvals	66
8.5.3	Senden von Push Approvals über REST-Web Services.....	67
8.5.4	Status von Push Approvals.....	68
8.5.5	Lebenszyklus einer Push Approval.....	71
8.6	Konfiguration für Push-Benachrichtigungen	71
8.7	Versionen	72
8.8	Reporting	72
8.9	Auth-Connector	72
8.10	Einstellungen.....	72
9.	RADIUS	73
9.1	Ohne RADIUS-Challenge	73
9.2	Mit RADIUS-Challenge	74
9.3	NAS-Clients.....	74
9.4	Einstellungen.....	75
9.5	Offline-Login mit RADIUS	75
10.	REST-Web Services.....	75
10.1	Vorhandene "LibRestDcClient" für JAVA verwenden	76
10.2	Neue "LibRestDcClient" für andere Programmiersprachen erstellen	76
10.3	Demo einer einfachen REST-Web Services-Anwendung	77
11.	SAML	77
11.1	Einrichten von DCEM als Identity-Provider.....	77
11.1.1	DCEM-SAML Trust-Zertifikate	77
11.1.2	Einstellungen für SAML	79
11.1.3	Download der Identity-Provider-Metadaten-Datei	79
11.1.4	Hinzufügen eines Service-Providers.....	79
11.2	Individuelle Anpassung der SAML-Webseiten	83

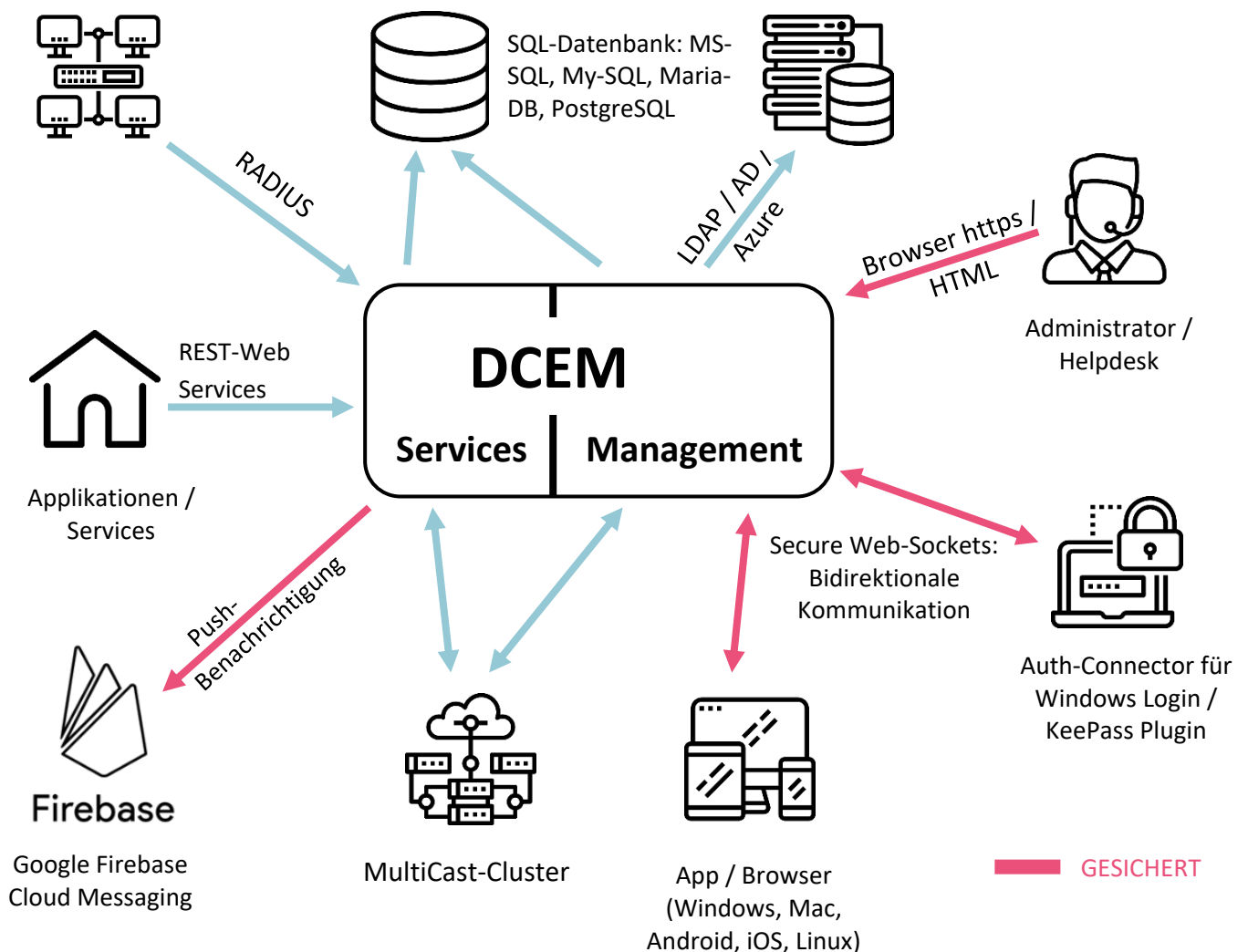
12.	OpenID	83
12.1	Vorbereitung von DCEM als OpenID Authentication Server	84
12.1.1	Eingabe des Clusternamens	84
12.1.2	DCEM OpenID Certificate	84
12.1.3	Einstellung der OpenID Preferences	85
12.1.4	Hinzufügen eines OpenID Clients	86
12.2	Anpassung der OpenID Web Pages	87
13.	Datenbank-Archiv	88
14.	UserPortal	88
14.1	Konfiguration	88
14.1.1	Allgemeine Einstellungen	89
14.1.2	Konfiguration der sichtbaren Elemente	89
14.1.2.1	<i>Sichtbare Views</i>	89
14.1.2.2	<i>Sichtbare Views, die Multi-Faktor-Authentifizierung erfordern</i>	89
14.1.2.3	<i>Sichtbare Aktionen</i>	89
14.1.2.4	<i>Sichtbare Aktionen, die Multi-Faktor-Authentifizierung erfordern</i>	90
14.1.3	Captcha Konfiguration mit Google reCAPTCHA v2	90
15.	Lizenzierungssystem	90
15.1	Beantragung eines neuen Lizenzschlüssels	91
15.2	Hinzufügen eines Lizenzschlüssels	92
15.3	Lizenzen einsehen	92
15.4	Funktionen des Lizenzierungstyps	93
15.4.1	Aktivierung	93
15.4.2	Login	94
16.	Logging	94
16.1	Konfigurierung	95
16.2	Datei-Output	95
16.3	SysLog-Output	95
16.4	Aktivierung des SysLogs	96
17.	PortalDemo	96

1. Einleitung

DoubleClue Enterprise Management (DCEM) ist die zentrale Komponente der DoubleClue-Plattform. Es kann auf mehreren Clusterknoten installiert und so bei Bedarf zu einem ausfallsicheren Cluster ausgebaut werden.

Ein Vorteil des Clusters ist, dass es sowohl Anlaufstelle für die zentralen Dienste als auch für das Management der Infrastruktur (Benutzer, Geräte, Knoten, Einstellungen usw.) ist. Es gibt ein umfassendes Berechtigungssystem, bei dem den Benutzern Rollen und Zugriffsrechte zugewiesen werden können. Außerdem können über DCEM Verbindungen zu diversen Drittanbieter-Services über bekannte Sicherheitsstandards und -schnittstellen wie SAML, RADIUS oder OpenID hergestellt werden.

Dieses Szenario stellt möglichen Komponenten des DCEM dar und mit welchem Bereich sie kommunizieren:



2. Installation und Inbetriebnahme

2.1 Voraussetzungen

2.1.1 Hardware-Voraussetzungen

- RAM: Minimum 4 GB (abhängig von der Benutzeranzahl)
- Festplatte: Minimum 20 GB
- Betriebssystem: Lauffähig auf Windows und Linux 64 Bit
- DNS-Eintrag im internen Firmennetzwerk sowie extern
- Netzwerk-Ports: 443, (optional) 8000, 8001 und 8002

Sie können die Ports für die verschiedenen Dienste und Verbindungen in DCEM unter „System“ -> „Clusterkonfiguration“ einstellen.



8001 ist der Standard-Port für die DoubleClue Apps. Dieser Port muss vom Internet aus erreichbar sein. Bitte aktivieren Sie den Port in Ihrer Firewall.

Die Software ist lauffähig ab Windows 7 (64-Bit) und Windows Server 2008 (64-Bit) und wurde auf Windows Server 2016 (64-Bit) getestet.

Ebenfalls lauffähig ist sie auf Linux-Distributionen mit 64 Bit und wurde auf Linux Ubuntu Server 18.04 getestet.

Auf Anfrage können weitere Versionen gezielt getestet werden.

2.1.2 Datenbank-Voraussetzungen

DCEM wird mit einer integrierten Datenbank („Embedded Database“) ausgeliefert. Die „Embedded Database“ hat die gleichen Features wie die externen Datenbanken, unterstützt jedoch nur einen DCEM-Knoten.

Neben der internen Datenbank werden derzeit diese externen Datenbanktypen unterstützt:

- MYSQL Getestete Version: MYSQL Vers.5.7
- MARIADB Getestete Version: MYSQL Vers.15.1 Distrib 10.1.23 - MariaDB
- MSSQL Getestete Version: Microsoft SQL Server 2008
- PostgreSQL Getestete Version: PostgreSQL 11

Weitere Datenbanktypen können auf Anfrage eingebunden und getestet werden.

2.2 Informationen zur Installation

Zur Installation benötigen Sie Administrator- bzw. Root-Rechte.

Sie erhalten zwei Installationspakete, eines für Windows (Paketname: „**DCEM-2.1.0.exe**“) und eines für Linux (Paketname: „**DCEM-2.1.0-Linux.tar.gz**“). Entpacken bzw. speichern Sie die entsprechende Datei am Speicherort Ihrer Wahl.

Der Verzeichnisname der Installation ist **“DCEM”**.

DCEM läuft als Dienst auf Windows und als Daemon auf Linux.


Bevor DCEM gestartet werden kann, muss das DCEM Setup ausgeführt werden, um die Datenbank und weitere Einstellungen zu konfigurieren.

2.3 Installation

Das Setup konfiguriert die Datenbankverbindung und initialisiert die Datenbanktabellen für DCEM. Des Weiteren wird das Passwort für den DCEM-Administrator **“SuperAdmin”** festgelegt.

Die im Setup getroffenen Einstellungen werden in der Datei **“DCEM_HOME/configuration.xml”** gespeichert.

Das Setup muss nur einmal ausgeführt werden. Es ist ausschließlich in englischer Sprache verfügbar.

 Port 8443 darf zum Zeitpunkt des Setups nicht von einer anderen Applikation belegt sein!

2.3.1 Installation auf Windows

Starten Sie das Setup, indem Sie die Datei **“DCEM-2.1.0.exe”** ausführen:

1. **“Installation on the first DCEM cluster node”:**
Wählen Sie diese Option, wenn Sie DCEM zum ersten Mal installieren.
2. **“Update current DCEM cluster node”:**
Wählen Sie diese Option, wenn es eine neue Version von DCEM gibt und Sie die alte updaten möchten.
3. **“Installation on a further node”:**
Wählen Sie diese Option, wenn Sie DCEM ein weiteres Mal installieren möchten. Ein Upload der Konfigurations-Datei des ersten DCEM-Knotens ist nötig ist während der Installation nötig. Folgen Sie dazu den Anweisungen des Setup-Assistenten.

Folgen Sie dann den nächsten Setup-Schritten.

Nachdem die notwendigen Dateien ins Verzeichnis kopiert worden sind, wird eine Command View angezeigt. DCEM wird nun versuchen, Ihren Standardbrowser zu öffnen und Sie direkt zum Datenbank Setup weiterzuleiten. Sollte sich Ihr Browser nicht selbständig öffnen, kopieren Sie die URL des Setups aus der Command View und öffnen Sie sie in Ihrem Browser.

Das Setup verwendet eine gesicherte HTTPS-Verbindung mit einem **“Self-Signed”**-Zertifikat. Deshalb wird beim Verbinden im Browser eine Sicherheitswarnung angezeigt. Bestätigen Sie diese Warnung.

Fahren Sie nun mit Kapitel [2.4 Datenbank-Konfiguration](#) fort.

2.3.2 Installation auf Linux

Gehen Sie, nachdem Sie **“DCEM-2.1.0-Linux.tar.gz”** entpackt haben, zum Verzeichnis **“DCEM/sh”** und starten Sie das Setup, indem Sie die Datei **“runSetup.sh”** ausführen. Die Setup-Konfigurationsmaske wird sich nun automatisch in Ihrem Standardbrowser öffnen, wenn Sie einen Linux-Desktop verwenden. Sollte sich das Setup nicht automatisch öffnen, kopieren Sie die Setup-URL aus Ihrer Konsole und öffnen Sie sie in Ihrem Browser.

Das Setup verwendet eine gesicherte HTTPS-Verbindung mit einem **“Self-Signed”**-Zertifikat. Deshalb wird beim Verbinden im Browser eine Sicherheitswarnung angezeigt. Bestätigen Sie diese Warnung.

Es kann passieren, dass wenn Sie DCEM oder das DCEM Setup auf Linux ausführen, der Prozess plötzlich ins Stocken gerät oder gar komplett stehen bleibt. Das liegt oft daran, dass dem Randomgenerator nicht genug Entropien für die Verschlüsselung zur Verfügung stehen und sie aus diesem Grund blockiert wird.

In diesem Fall empfehlen wir Ihnen Haveged zu installieren, um zusätzliche Entropien zu erstellen. Installieren Sie Haveged indem Sie die folgenden Befehle in die Kommandozeile eingeben:

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

Dieses Problem tritt vor allem bei neueren Linux-Maschinen auf.

Fahren Sie nun mit Kapitel [2.4 Datenbank-Konfiguration](#) fort.

2.3.3 Installation mit einem Headless-Betriebssystem

Geben Sie bei einem Headless-Betriebssystem folgende URL ein:

https:// --Hostname/IP des Servers-- :8443/setup

Das Setup verwendet eine gesicherte HTTPS-Verbindung mit einem **“Self-Signed”**-Zertifikat. Deshalb wird beim Verbinden im Browser eine Sicherheitswarnung angezeigt. Bestätigen Sie diese Warnung.

Fahren Sie nun mit Kapitel [2.4 Datenbank-Konfiguration](#) fort.

2.3.4 Installation erneut ausführen

Sollte es notwendig sein, das Setup erneut auszuführen, öffnen Sie bei einem Windows-Betriebssystem den Ordner **“DCEM/bat”**. Beenden Sie den Dienst mit **“stopDcemService.bat”**. Führen Sie dann die Datei **“runSetup.bat”** aus.

Gehen Sie bei einem Linux-Betriebssystem zum Verzeichnis **“DCEM/sh”** und beenden Sie den Daemon zunächst mit **“stopDcemDaemon.sh”**. Führen Sie anschließend die Datei **“runSetup.sh”** aus.

Das Setup kann nicht gestartet werden, solange DCEM noch läuft.

2.4 Datenbank-Konfiguration

DCEM benötigt eine SQL-Datenbank, um betrieben zu werden.

Sie können sich zwischen einer vorinstallierten "Embedded Database" oder der vorherigen Installation einer externen SQL-Datenbank entscheiden.

2.4.1 Integrierte Datenbank / "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_1_6

Administrator Name: * root

Administrator Password: *****

Save

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

Die deaktivierten Eingabefelder sind für die integrierte Datenbank nicht notwendig.

⚠ Die Integrierte Datenbank unterstützt keine multiplen DCEM-Knoten und keine Mandantenfähigkeit!

2.4.1.1 Backup der Integrierten Datenbank

⚠ Bitte beachten Sie, dass diese Konfiguration erst vorgenommen werden kann, wenn das **Setup beendet und DCEM gestartet** wurde.

Um das automatische Backup der Integrierten Datenbank zu aktivieren, gehen Sie zum Hauptmenüpunkt "System", Untermenü "Einstellungen" und scrollen Sie bis zu "Embedded Database" ganz unten.

Embedded Database

Embedded Database-Backup ausführen ☒ If you use the Em


Pfad Embedded Database-Backup

Other

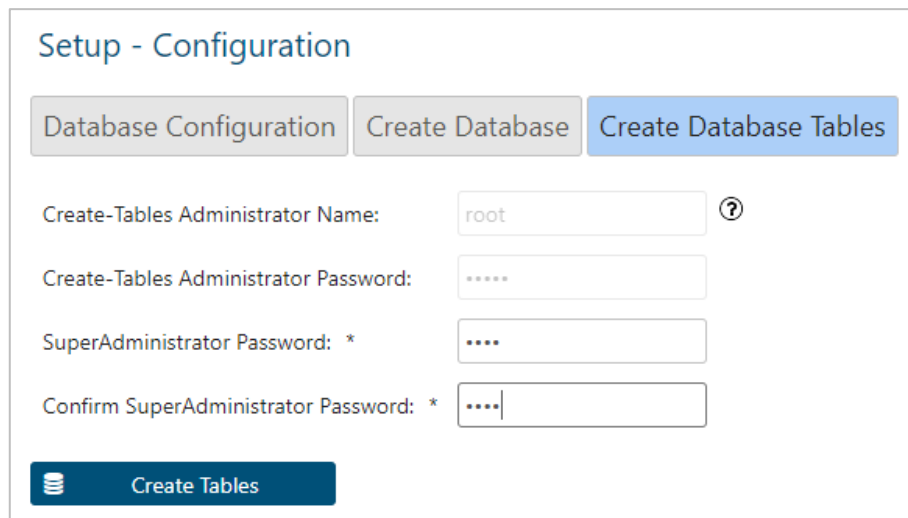
Nächtliche Ausführungszeit **02:00** The time of

Setzen Sie einen Haken in die Box “Embedded Database-Backup ausführen”, um ein Backup der Integrierten Datenbank zu jeder “Nächtlichen Ausführungszeit” vorzunehmen. Sie können eine “Nächtliche Ausführungszeit” unter dem Punkt “Other” eingeben.

Geben Sie einen Pfad für das Backup der Integrierten Datenbank neben “Pfad Embedded Database-Backup” ein.

 Während des Backup-Prozesses ist das Schreiben in die Datenbank blockiert!

2.4.1.2 Datenbanktabelle anlegen



Setup - Configuration


Database Configuration | **Create Database** | Create Database Tables

Create-Tables Administrator Name: ?

Create-Tables Administrator Password:

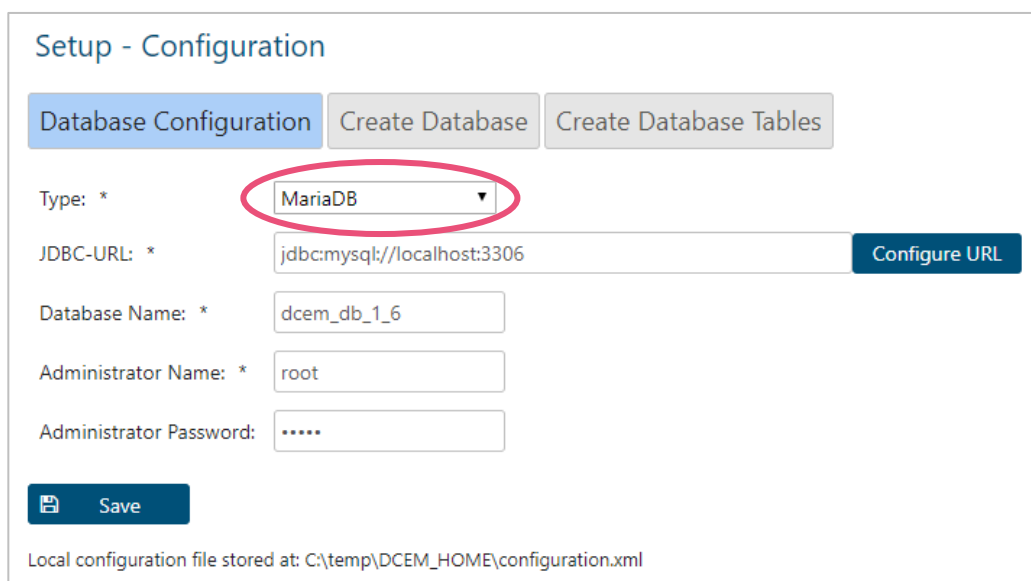
SuperAdministrator Password: *

Confirm SuperAdministrator Password: *

 **Create Tables**

Super-Administrator Password: Legen Sie das Passwort für den Super-Administrator von DCEM fest. Der Benutzername des Super-Administrators ist dabei immer “SuperAdmin”.

2.4.2 Externe Datenbank



Setup - Configuration

Database Configuration | Create Database | Create Database Tables


Type: * MariaDB ▼

JDBC-URL: * **Configure URL**

Database Name: *

Administrator Name: *

Administrator Password:

 **Save**

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

Type:

Wählen Sie die Art der externen Datenbank aus, die Sie verwenden möchten. Derzeit unterstützt DCEM die folgenden externen Datenbanken:

- MYSQL Getestete Version: MYSQL Vers.5.7
- MARIADB Getestete Version: MYSQL Vers.15.1 Distrib 10.1.23 - MariaDB
- MSSQL Getestete Version: Microsoft SQL Server 2008
- PostgreSQL Getestete Version: PostgreSQL 11

URL:

Die eingetragene URL muss ein JDBC-Format haben. Ist Ihnen die URL bekannt, können Sie diese direkt eingeben. Ist Ihnen die URL nicht bekannt, können Sie diese über den Button "Configure URL" erstellen.

Administrator Name / Administrator Password:

Diese Angaben werden benötigt, damit sich DCEM gegenüber der Datenbank authentifizieren kann. Das Passwort wird dabei immer in verschlüsselter Form gespeichert.

Save:

Beim Speichern wird überprüft, ob eine Verbindung zur Datenbank hergestellt werden kann. Es werden entsprechende Meldungen angezeigt (Verbindung erfolgreich, Verbindung fehlgeschlagen, Passwort falsch usw.)

2.4.2.1 *Datenbank oder Schema erstellen*

The screenshot shows a web-based configuration interface titled "Setup - Configuration". It has three tabs: "Database Configuration", "Create Database" (which is active and highlighted in blue), and "Create Database Tables". Under the "Create Database" tab, there are two input fields: "Database-Administrator Name:" with the value "root" and a help icon, and "Database-Administrator Password:" with masked characters "*****". Below these fields are two buttons: a blue "Create Database" button and a grey "Back" button with a left-pointing arrow.

Existiert noch keine Datenbank mit diesem Namen, wird sie nun angelegt. Wurde die Datenbank im Voraus mit einem Datenbank-Tool erstellt, wird dieser Schritt nicht benötigt.

Database Administrator Name:

Der Datenbank-Administrator muss die Rechte haben, eine Datenbank erstellen zu dürfen. Um die Verbindung zur Datenbank herzustellen, müssen Benutzername und Passwort des Datenbank-Administrators eingegeben werden. Diese Daten werden nur einmalig zur Authentifizierung benötigt und nicht gespeichert.

2.4.2.2 Datenbanktabelle anlegen

The screenshot shows a web-based configuration interface titled "Setup - Configuration". It has three tabs: "Database Configuration", "Create Database", and "Create Database Tables" (which is active). Below the tabs are four input fields with labels and asterisks indicating required fields:

- "Create-Tables Administrator Name: *" with the value "root" and a help icon.
- "Create-Tables Administrator Password:" with masked dots.
- "SuperAdministrator Password: *" with masked dots.
- "Confirm SuperAdministrator Password: *" with masked dots.

At the bottom left, there is a blue button with a database icon and the text "Create Tables".

Mit "Create Database Tables" werden die Datenbanktabellen erstellt.

Create-Tables Administrator Name:

Der Create-Tables Administrator muss die Rechte haben, Datenbanktabellen erstellen zu dürfen.


Super-Administrator Password:

Legen Sie das Passwort für den Super-Administrator von DCEM fest. Der Benutzername des Super-Administrators ist dabei immer "SuperAdmin".


Create Tables:

Durch Klicken des Buttons "Create Tables" wird im Verzeichnis "**DCEM/DCEM_HOME**" die Datei "**configuration.xml**" erstellt. Jedes Mal, wenn die Aktion "Create Tables" ausgeführt wird, wird eine neue Version der Datei erzeugt. Die alte Version wird innerhalb desselben Ordners unter dem Namen "**configuration.xml.Datum-Uhrzeit**" gespeichert.

Werden beim Erstellen der Datenbank keine Fehler angezeigt, erhalten Sie eine Meldung, in welcher der Pfad zum Speicherort der Datei "**configuration.xml**" angezeigt wird. Speichern Sie diese Datei an einem sicheren Ort. Sie wird benötigt, um weitere Knoten hinzuzufügen.

 Sie können das Setup nun schließen und die Installation von DCEM beenden.

Das Setup muss beendet und geschlossen sein, bevor DCEM gestartet werden kann.

 Bitte beachten Sie: Wenn Sie ein DCEM auf einem Linux-Betriebssystem verwenden möchten, fahren Sie mit Kapitel [2.5 DCEM als Daemon installieren](#) fort.

Wenn Sie stattdessen ein Windows-Betriebssystem nutzen, gehen Sie weiter zu Kapitel [2.7 Anmeldung bei DCEM](#).

2.4.2.3 Konfiguration einer Postgre-Datenbank als externe DCEM-Datenbank

Getestet mit PostgreSQL 11

1. Legen Sie in PostgreSQL eine neue Datenbank für DoubleClue an.
2. Wählen Sie im DCEM Setup „PostgreSQL“ als Datenbanktyp aus.
3. Fügen Sie zur JDBC-URL einen Slash („/“) und den Namen der PostgreSQL-Datenbank hinzu.
Zum Beispiel: jdbc:postgresql://yourhost:5432/dcem_db)
4. Fügen Sie unter „Database Name“ den Namen des Schemas der Datenbank ein. Dieses wird beim Speichern automatisch angelegt.
5. Geben Sie den Namen des Administrators und das entsprechende Passworts ein. Klicken Sie auf ‚Speichern‘.

The screenshot shows the 'Setup - Configuration' window for DoubleClue Enterprise Management. The 'Database Configuration' tab is active. It contains the following fields and buttons:

- Type:** A dropdown menu set to 'PostgreSQL'.
- JDBC-URL:** A text field containing 'jdbc:postgresql://localhost:5432/dcem_db' and a 'Configure URL' button.
- Database Name:** A text field containing 'dcem_db'.
- Administrator Name:** A text field containing 'postgres'.
- Administrator Password:** An empty text field.
- Buttons:** 'Create Database', 'Create Database Tables', 'Save', and 'Next'.



PostgreSQL ist eine casesensitive Datenbank. Alle Einträge und Suchanfragen müssen casesensitive angelegt werden.

2.5 DCEM unter Linux als Daemon installieren

Nach Beendigung des DoubleClue-Setups müssen Sie DCEM noch als Daemon installieren, indem Sie zum Verzeichnis **“DCEM/sh”** gehen und die Datei **“installDcemDaemon.sh”** ausführen.

Sie können den Daemon immer wieder anhalten oder starten, indem Sie die Datei **“stopDcemDaemon.sh”** oder **“startDcemDaemon.sh”** ausführen.

2.6 Datenbank-Migration

Aufgrund der ständigen Weiterentwicklung unserer DoubleClue-Software veröffentlichen wir regelmäßig neue Versionen. Um eine ältere Version auf die aktuelle upzudaten, ist eine Datenbank-Migration nötig.

2.6.1 Migration mit Windows

Wenn Sie ein Windows-Betriebssystem verwenden, starten Sie einfach den DoubleClue Windows Installer und folgen Sie den Setup-Schritten.

 Bitte beachten Sie, dass Sie vor der Migration ein Backup der Datenbank erstellen sollten.


Wenn Sie die Integrierte Datenbank verwenden, kopieren Sie dafür einfach den Ordner **“DCEM_HOME/EmbeddedDB”** in ein neues, sicheres Verzeichnis. Beziehen Sie sich bei anderen Datenbanktypen bitte auf die Datenbank-Handbücher der jeweiligen Anbieter.

Fahren Sie mit Kapitel [2.6.3 Ablauf der Migration](#) fort.

2.6.2 Migration mit Linux

Bitte beachten Sie, dass DCEM während des Prozesses der Datenbank-Migration nicht laufen darf.

Gehen Sie deshalb bitte zum Ordner **“DCEM/sh”** und klicken Sie auf **“stopDcemDaemon.sh”**, um den Daemon anzuhalten.

 Vor der Migration sollten Sie ein Backup der Datenbank machen. Wenn Sie die Integrierte Datenbank verwenden, kopieren Sie einfach den Ordner **“DCEM_HOME/EmbeddedDB”** in ein neues, sicheres Verzeichnis. Beziehen Sie sich bei anderen Datenbanktypen bitte auf die Datenbank-Handbücher der jeweiligen Anbieter.


Führen Sie nun die Datei **“runSetup.bat”** aus. Wählen Sie einen Datenbank-Typ aus und klicken Sie auf **“Save”**. Der Konfigurations-Dialog wird Ihnen mitteilen, dass eine Migration notwendig ist.


Fahren Sie mit dem nächsten Kapitel fort.

2.6.3 Ablauf der Migration

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

 Folgen Sie den Anweisungen, um den Migrationsprozess zu vervollständigen:


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
as	Identity-Management	2	3



Die Migration war erfolgreich, wenn der Text “No records found” in der Spalte “Module ID” angezeigt wird. Klicken Sie auf “Close DoubleClue Setup”, um die Datenbank-Migration abzuschließen.

2.7 Anmeldung bei DCEM

2.7.1 Login mit Benutzername und Passwort

Die URL zur Anmeldung bei DCEM lautet:

[https:// --Hostname/IP des Servers-- :8443/dcem/mgt/login.xhtml](https://--Hostname/IP des Servers--:8443/dcem/mgt/login.xhtml)

Loggen Sie sich mit dem Benutzernamen “SuperAdmin” und dem im Setup für den Super-Administrator festgelegten Passwort ein.

Nach der Anmeldung können Sie DCEM verwalten.

2.7.2 Login mit DoubleClue Multi-Faktor-Authentifizierung

Aktivieren Sie dieses Feature, wenn Sie möchten, dass sich Administratoren mit DoubleClue MFA in DCEM einloggen.

Die Aktivierung wird empfohlen, wenn Sie DCEM in der Cloud installieren.

2.7.2.1 DoubleClue MFA aktivieren

Wenn Sie sich mit DoubleClue MFA (Multi-Factor-Authentication) bei DCEM anmelden möchten, passen Sie nach Ihrem ersten Login unter „Identity Management“ -> „Policies“ die DCEM Management Policy entsprechend an. Deaktivieren Sie die Anmeldung per Passwort und wählen Sie Multi-Faktor-Authentifizierungsmethoden, die Sie verwenden möchten. Unter „Standard Auth-Methode“ können Sie eine der ausgewählten Authentifizierungs-Methoden als präferierte Standardmethode auswählen.

The screenshot shows a 'Ändern' (Change) dialog box for the 'DCEM-Management' policy. The settings are as follows:

- Name:** DCEM-Management
- Zugriff verweigern:** ☐
- MFA innerhalb Timeout unterdrücken:** ☐
- Browser-Fingerprint merken:** ☐
- Session-Authentifizierung:** ☐
- Timeout (Stunden):** 0
- Network-Bypass:** 172.16.0.0-172.16.255.255
- Auth-Methoden erlauben:**
 - ☒ Password
 - ☐ Hardware Token
 - ☒ QrCode Approval
 - ☐ SMS Passcode
 - ☒ DoubleClue Passcode
 - ☐ FIDO Authentication
 - ☐ Voice Message
 - ☒ Push-Approval
- Standard Auth-Methode:** (Keine)
- MFA beim Entsperren von Windows:** ☐

At the bottom, there are two buttons: 'OK' and 'Abbrechen' (Cancel).

Weitere Informationen über die Verwaltung der Authentifizierungsmethoden finden Sie in Kapitel [Z Authentifizierungsmethoden und Policies](#).

2.8 Anmeldung bei DCEM

2.8.1 Datei "configuration.xml"

In der Datenbank werden vertrauliche Daten in verschlüsselter Form gespeichert. Um diese Daten zu schützen, enthält die Datei einen Datenbank-Schlüssel, der zum Entschlüsseln der Daten benötigt wird.

Geht die Datei **“configuration.xml”** verloren, kann die Datenbank nicht mehr verwendet werden.

2.8.2 Ordner “DCEM_HOME”

In diesem Ordner befinden sich neben der Datei **“configuration.xml”** die folgenden Ordner, die automatisch erstellt und gefüllt werden:

“certs”	für Zertifikate
“jna”	für Logdateien
“logs”	für Logdateien

Es ist erforderlich, dass der DCEM-Account Schreibrechte für den Ordner **“DCEM_HOME”** besitzt, um in die Dateien schreiben und aus ihnen lesen zu können.

3 DCEM-Systemhauptmenü

Im Hauptmenüpunkt „System“ können die Clusterknoten und Mandanten konfiguriert werden. Dieser Hauptmenüpunkt wird nur angezeigt, wenn man sich über den Haupt-Mandanten in DCEM einloggt. Administratoren die lediglich über einen DCEM-Zugang für einen Sub-Mandanten verfügen, können diesen Bereich nicht einsehen.

3.1 Clusterkonfiguration

DCEM besteht aus mehreren miteinander vernetzten eigenständigen Servern (auch “Knoten” genannt).

Zur Lastverteilung wird ein Load Balancer eingesetzt. Fällt ein Server aus, fällt nicht das ganze System aus, sondern die Last wird gleichmäßig auf die übriggebliebenen Server verteilt. Der Load Balancer ist nicht Bestandteil der DCEM-Plattform. Sie benötigen dazu einen Software- oder Hardware-Balancer.

In der Clusterkonfiguration können Sie die allgemeinen Cluster-Einstellungen sowie die Einstellungen für jeden Connection-Service dieses Clusters verwalten.



Bitte beachten Sie: Alle Änderungen an dieser Konfiguration benötigen einen DCEM-Neustart um aktiv zu werden.

3.1.1 Allgemeine Einstellungen



Clusterkonfiguration

Cluster

Cluster-ID:	nphi3TPtGgFrTFDA
Skalierungsfaktor: %20	<input type="range"/>
Cluster-Name: *	<input type="text"/>
Passwort:	5kqmpws4
Host Domain Name *	localhost

3.1.1.1 Cluster ID

Die Cluster ID ist eine zufällig generierte Zahl, die automatisch während der Installation erstellt wird und nicht geändert werden kann.

Die Cluster ID wird in folgenden Situationen benötigt:


- Um DCEM zu lizenzieren
- Um DCEM beim DoubleClue.online-Dispatcher zu registrieren
- DoubleClue Apps senden die Cluster-ID an die Smart Device Web-Socket URL. Load-Balancer können dadurch Anfragen ankommender Verbindungen sofort ablehnen, wenn die Cluster-ID falsch ist.

3.1.1.2 Skalierungsfaktor

Über den Skalierungsfaktor können Sie einstellen, wieviel der Serverkapazität für DCEM reserviert wird. Je höher der Faktor umso mehr Systemressourcen werden für DCEM bereitgestellt. Wenn der Skalierungsfaktor zu hoch gesetzt wird, können andere Programme auf diesem Server beeinflusst werden.

Die maximale Anzahl an erlaubten parallelen Verbindungen ist 20000. Der Skalierungsfaktor wird proportional gesetzt. Wenn der Skalierungsfaktor z.B. auf 20% gesetzt ist, beträgt die maximale Anzahl an Verbindungen 4000.

3.1.1.3 Cluster Name

 Bevor Sie die Connection Services in der Clusterkonfiguration modifizieren können, ist es notwendig, dem Cluster einen Namen zu geben. Füllen Sie deswegen einen aussagekräftigen Namen in dieses Feld ein.

3.1.1.4 *Password*

Dieses Passwort wird von den DCEM-Knoten zur Kommunikation untereinander verwendet.

3.1.1.5 *Host Domain Name*

Der Host Domain Name ist der Host-Name für DCEM ohne den Namen einer potentiellen Mandanten-Sub-Domain. Wenn die DCEM-URL zum Beispiel „https://doubleclueone.online:8444/dcem/mgt“ lautet, sollten Sie „doubleclueone.online“ in dieses Feld eingeben. Die URL für einen Mandanten mit Subdomain lautet dann „https://xxx.doubleclueone.online:8444/dcem/mgt“, wobei xxx der Name der Sub-Domain ist.

Sie können mehrere Host-Namen getrennt mit einem **Semikolon** eingeben, z.B. „doubleclueone.online;localhost“. Groß- und Kleinschreibung wird bei den Namen nicht beachtet. Alle anderen Host-Namen werden mit dem Fehler Code (401) Unauthorized abgelehnt.

3.1.2 Verbindungsdienste

DoubleClue unterstützt diverse Verbindungsdienste. In der Cluster-Konfiguration können Sie diese aktivieren, deaktivieren und die Einstellungen für die verschiedenen Dienste anpassen. Drei der Verbindungsdienste, Management, REST Web-Services und Smart-Device Web-Sockets, werden benötigt, um DCEM auszuführen und sind deswegen standardmäßig aktiviert.

3.1.2.1 *Management Connection*

Die Management Connection ist die Verbindung zwischen Browser und DCEM. Sie muss immer eine mit SSL/TLS gesicherte Verbindung sein. Für diese Verbindung wird beim Setup ein „selbstsigniertes“ Zertifikat erstellt. Ein neues Zertifikat kann bei Bedarf hochgeladen werden (siehe Kapitel [3.5 Neuen KeyStore hochladen](#)).

3.1.2.2 *REST-Web Services Connection*

Die Rest-Web Services Verbindung ist die Verbindung zwischen DCEM und Ihrem Server. Diese Verbindung ist eine HTTP/HTTPS-Verbindung. Sie finden weitere Informationen in Kapitel [10. REST-Web Services](#).

Da dies normalerweise eine interne Verbindung ist, muss sie nicht SSL/TSL verschlüsselt werden. Wenn sie trotzdem gesichert werden soll, müssen Sie einen KeyStore für diese Verbindung erstellen, wie es im Kapitel [3.3.1 KeyStores hinzufügen](#) beschrieben wird, oder Sie können ein Zertifikat, wie beschrieben in Kapitel [3.5 Neuen KeyStore hochladen](#), hochladen.

3.1.2.3 *Smart-Device Web-Sockets*

Die Web Sockets Connection ist die Verbindung zwischen DCEM und der DoubleClue App, die vom Endnutzer verwendet wird. Es werden Apps für Android, iOS und Windows unterstützt.

Die Verbindung zwischen dem Endnutzer (App) zu DCEM oder dem Loadbalancer muss immer SSL/TLS verschlüsselt sein.

Die Verbindung zwischen dem internen Loadbalancer zu DCEM muss in diesem Fall nicht verschlüsselt sein. Wenn sie dennoch verschlüsselt werden soll, müssen Sie einen KeyStore für diese Verbindung erstellen, wie es im Kapitel [3.3.1 KeyStores hinzufügen](#) beschrieben wird, oder Sie können ein Zertifikat, wie beschrieben in Kapitel [3.5 Neuen KeyStore hochladen](#), hochladen.

3.1.2.4 *RADIUS-Authentifizierung und Buchhaltung*

RADIUS ist ein Authentifizierungs-, Autorisierungs- und Buchhaltungsprotokoll zwischen Netzwerkclient und -server. DoubleClue kann konfiguriert werden, um als RADIUS Server zu fungieren. Die Identität des Endnutzers wird mittels Nutzernamen und Passwort sichergestellt. DCEM verstärkt die Features und Sicherheit von RADIUS mit Multi-Faktor-Authentifizierung, die vom Benutzer eine zusätzliche Identitätsbestätigung via App oder einer anderen MFA Methode fordert.

Mehr Informationen darüber, wie man DoubleClue als RADIUS-Server einrichten kann, finden Sie in Kapitel [9 RADIUS](#).

3.1.2.5 *SAML*

SAML (Security Assertion Markup Language) ist ein offener Standard für den Austausch von Authentifizierungsdaten zwischen einem Identity Provider (IdP) und einem Serviceanbieter. Es ist eine XML-basierte Markup Language für Sicherheitsbestätigungen. Die wichtigste Verwendung für SAML ist als Webbrowser Single Sign-on (SSO).

Mehr Informationen darüber, wie Sie DoubleClue als SAML Identity Provider einrichten können finden, Sie in Kapitel [11 SAML](#).

3.1.2.6 *OpenID OAuth*

OpenID ist ein offener Standard und ein Authentifizierungsprotokoll, das auf OAuth 2.0 aufbaut. Es wird für den Austausch von Daten zwischen einem OpenID Authentifizierungsserver und einem OpenID Client verwendet. DoubleClue kann eingerichtet werden, um als OpenID-Authentikator zu agieren.

Mehr Informationen finden Sie in Kapitel [12 OpenID](#).

3.1.2.7 Health Check

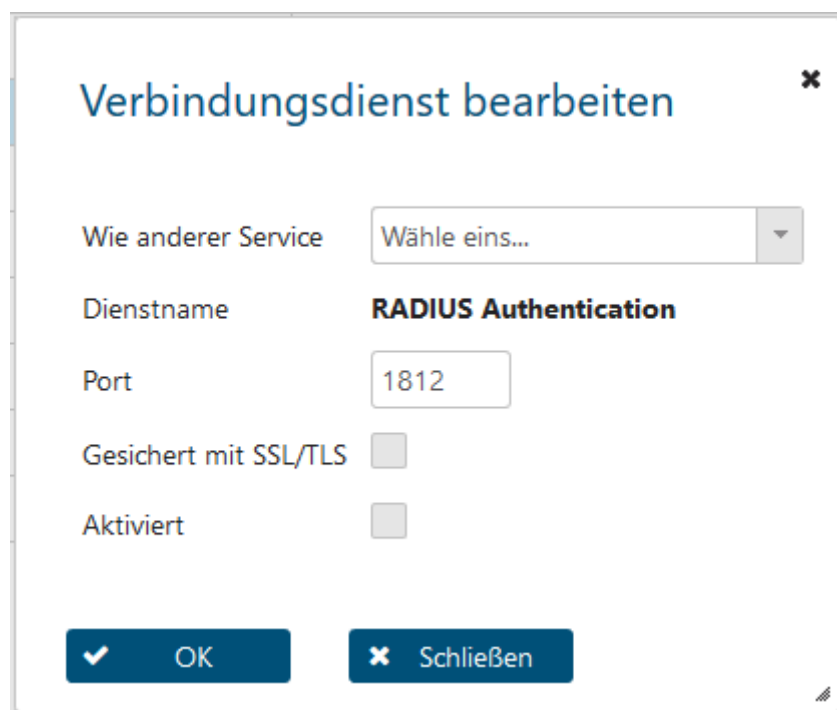
Der Gesundheitscheck ist eine URL über die der Loadbalancer prüfen kann, ob ein Knoten erreichbar ist.

3.1.2.8 UserPortal

Standardmäßig ist UserPortal aktiviert und nutzt die gleichen Einstellungen wie die Management Connection. Weitere Informationen finden Sie in Kapitel [14 UserPortal](#).

3.1.3 Verbindungsdiensteinstellungen

Sie können die Verbindungseinstellungen für die verschiedenen Verbindungsdienste bearbeiten. Denken Sie daran, dass Sie die Veränderungen speichern müssen, bevor Sie das Menü verlassen. Starten Sie anschließend DCEM neu, um die Änderungen zu aktivieren.



The screenshot shows a dialog box titled "Verbindungsdienst bearbeiten" (Edit Connection Service). It contains the following fields and controls:

- Wie anderer Service**: A dropdown menu with the text "Wähle eins..." and a downward arrow.
- Dienstname**: A text field containing "RADIUS Authentication".
- Port**: A text field containing "1812".
- Gesichert mit SSL/TLS**: A checkbox that is currently unchecked.
- Aktiviert**: A checkbox that is currently unchecked.
- At the bottom, there are two buttons: "OK" (with a checkmark icon) and "Schließen" (with a close icon).

3.1.3.1 Wie anderer Service

Wenn Sie möchte, dass ein Verbindungsservice die gleichen Einstellungen verwendet wie ein anderer, können Sie diesen Server einfach als „wie anderer Service“ setzen. Beachten Sie, dass wenn Sie die Einstellungen des Servers der als Vorlage dient ändern, sich auch die Settings des verbundenen Service entsprechend ändern.

3.1.3.2 Port

Geben Sie die Nummer des Ports ein, den Sie für den jeweiligen Service nutzen wollen. Die Standardeinstellungen sind:

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

3.1.3.3 Verschlüsselung mit SSL/TSL

Wählen Sie aus ob Sie möchten, dass der jeweilige Dienst SSL/TSL verschlüsselt wird oder nicht. Für die Management Connection und die Web-Sockets-Connection ist die Aktivierung der Verschlüsselung Pflicht. Für die REST-Web Service Connection wird keine Verschlüsselung benötigt, da es sich um eine interne Verbindung handelt. Darum ist Sie für diesen Dienst standardmäßig deaktiviert. Für alle anderen Verbindungsdienste wird es empfohlen, die Verschlüsselung zu aktivieren.

3.2 Clusterknoten

Der erste Clusterknoten wird beim Setup automatisch eingerichtet, wobei der Knotenname bei Bedarf geändert werden kann (siehe hierzu Kapitel [3.2.2.1 Knotennamen festlegen](#)).

3.2.1 Installation eines weiteren Knotens

Installieren Sie DCEM wie in Kapitel [2.2 Installation](#) beschrieben.

Kopieren Sie die Datei "**DcemInstallation/DCEM_HOME/configuration.xml**" und speichern Sie diese unter demselben Pfad auf dem neuen Knoten.

Wird die originale Datei "**configuration.xml**" verändert, muss sie auf jedem Knoten durch die neue Datei ersetzt werden.

3.2.2 Clusterknoten hinzufügen

Einen Clusterknoten können Sie unter dem Hauptmenüpunkt "System", Untermenü "Clusterknoten" hinzufügen. Legen Sie dazu einen Knotennamen und den Knotentyp fest.

3.2.2.1 Knotennamen festlegen

Um einen Knotennamen festzulegen, gibt es verschiedene Möglichkeiten.

DCEM sucht der Reihe nach an folgenden Orten, ob ein Knotenname gefunden wird. Sobald ein Name gefunden wurde, wird die Suche abgebrochen:

- 1) Inhalt "**configuration.xml**"
- 2) Umgebungsvariable "COMPUTERNAME"
- 3) Umgebungsvariable "HOSTNAME"
- 4) IP-Name des Servers

Knotenname in der **configuration.xml** festlegen:

Auf jedem Knoten muss die originale "**configuration.xml**"-Datei gespeichert werden. Anschließend muss auf jedem einzelnen Knoten in dieser Datei der eindeutige Knotenname des jeweiligen Knotens eingetragen werden.

Fügen Sie dazu die folgende Codezeile in der Datei "**configuration.xml**" innerhalb des Bereichs `<configuration>` und `</configuration>` ein und geben Sie statt **--Knotenname--** den gewünschten Namen an:

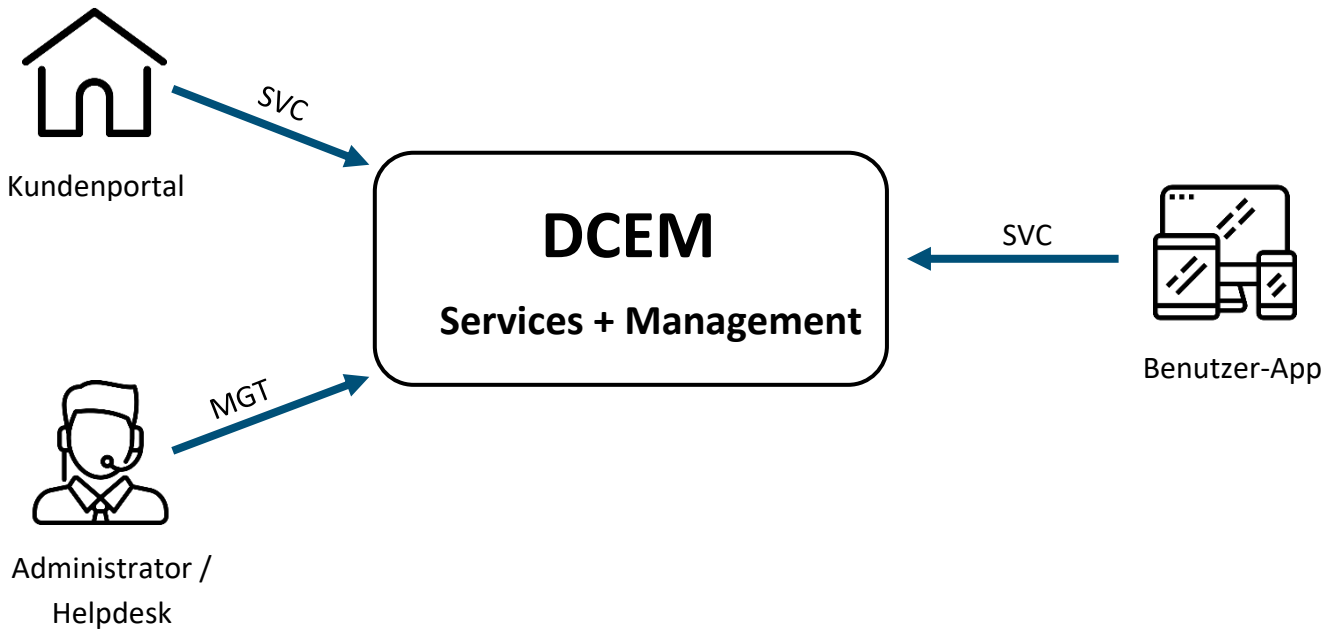
```
<nodeName> --Knotenname-- </nodeName>
```

3.2.2.2 Knotentyp festlegen

Für jeden Knoten muss ein Knotentyp festgelegt werden. Es stehen drei Knotentypen zur Auswahl:

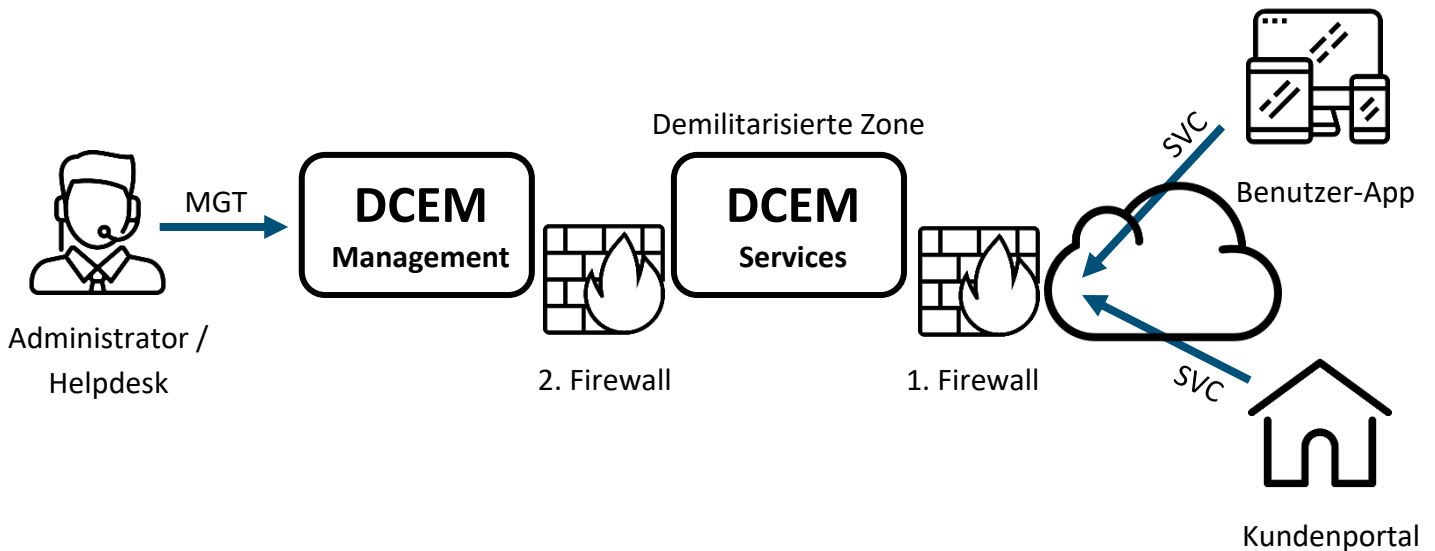
Der MGT_SVC-Knotentyp ermöglicht es, dass das DECM Management und die DCES Services auf dem/den gleichen Knoten laufen.

Ein Server für alle Verbindungen: *MGT_SVC-Knotentyp*



Es ist also möglich, die DCEM Services und das Management auf unterschiedlichen Knoten laufen zu lassen. In diesem Szenario läuft das Management auf spezifischen MGT-Knoten, die nur vom internen Netzwerk aus erreichbar sind und die Services auf SVC-Knoten.

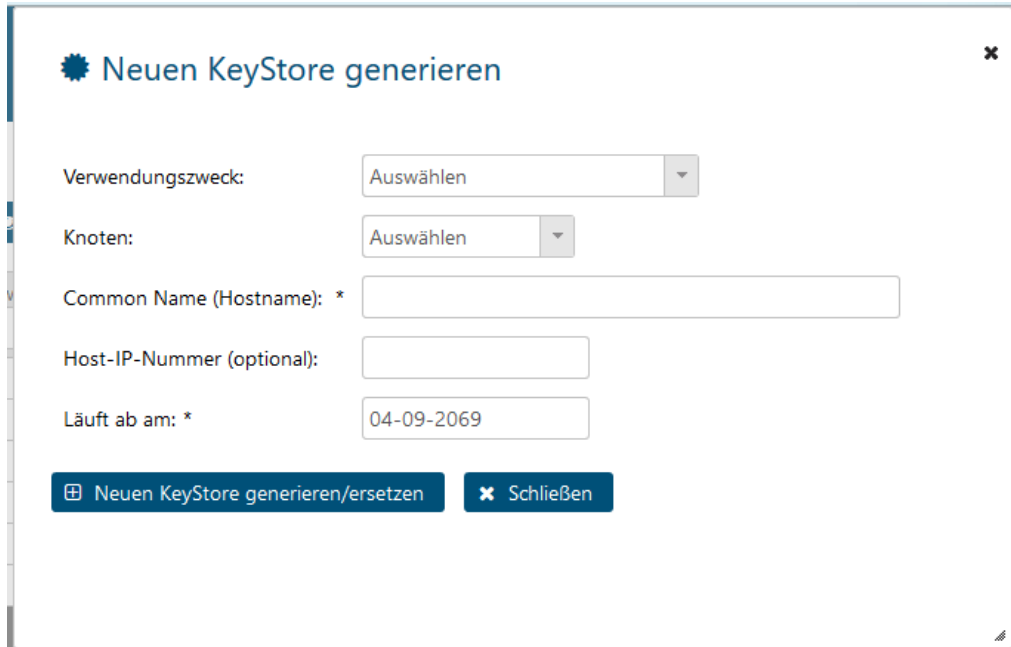
Getrennte Server für Management- und Service-Verbindung: MGT-Knotentyp + SVC-Knotentyp



Sollen die Management- und die Serviceverbindung intern getrennt werden, muss die Serviceverbindung in der sog. "Demilitarisierten Zone" angeordnet sein, damit sie von außen erreichbar ist. Die Management-Verbindung darf dabei nicht von außen erreichbar sein.

3.2.2.3 KeyStore anlegen

Legen Sie wie in Kapitel [3.3.1 Neuen KeyStore hinzufügen](#) beschrieben einen neuen Management_CA KeyStore an und wählen Sie unter „Knoten“ den neu angelegten Knoten aus.




Alternativ können Sie auch einen neuen Knoten hochladen. Laden Sie dafür zunächst einen bereits existierenden Management_CA KeyStore als PKCS#12 herunter und laden Sie ihn anschließend wieder hoch. Ordnen Sie den KeyStore beim Hochladen dem neuen Knoten zu.

Sie werden beim Hochladen nach dem Passwort des KeyStores gefragt. Dies ist dasselbe wie das des heruntergeladenen Knotens. Sie können es sich im KeyStore-Menü anfragen lassen.

3.2.2.4 Bestätigung

Wurde der neue Knoten korrekt installiert und gestartet, wird er nun unter dem Untermenüpunkt „Clusterknoten“ (Hauptmenü: „System“) mit dem Status „Aktiv“ angezeigt.

 Der Dienst wird abgebrochen, wenn kein Knotenname gefunden wurde. Überprüfen Sie, ob der Knotenname wie in Kapitel [3.2.2.1 Knotennamen festlegen](#) beschrieben korrekt vergeben wurde.

3.3 KeyStores

Für jede Verbindung, die mit SSL/TLS gesichert sein soll (siehe hierzu auch Kapitel [3.1 Clusterkonfiguration](#)), wird ein KeyStore benötigt. Im KeyStore werden das Zertifikat, der Private Key und der Public Key gespeichert. Der KeyStore wird benötigt, damit die durch SSL/TLS gesicherte Verbindung aufgebaut werden kann. Eine SSL/TLS-Verbindung benötigt mehr Rechenleistung als eine ungesicherte Verbindung.

Das Zertifikat kann entweder von einem offiziellen Trust Center (CA) vergeben werden, oder es wird ein "Self-Signed"-Zertifikat erstellt.

3.3.1 Neuen KeyStore hinzufügen

KeyStores können im „Keystore“-Menü (Hauptmenü: "System") erstellt. Für jeden KeyStore muss dabei ein „Purpose“ ausgewählt worden. Es stehen verschiedene Purposes für die unterschiedlichen Verbindungsdienste zur Verfügung. Die Angabe einer IP-Adresse ist optional und wird nur benötigt, wenn als Knotenname die IP-Adresse verwendet werden soll.

3.4 Mögliche Verbindungen zum Endnutzer

Bei der Verbindung zum Endnutzer muss unterschieden werden, an welcher Stelle die Verbindung terminiert (unterbrochen) werden soll. Es gibt folgende Möglichkeiten:

3.4.1 SSL/TLS vom Endnutzer terminiert bei DCEM



3.4.1.1 KeyStore-Typ: DeviceWebsockets_CA

Wird die Verbindung vom Endnutzer bei DCEM terminiert, ist diese Verbindung standardmäßig immer mit SSL/TLS gesichert.

3.4.1.2 SDK-Konfigurationsdatei erstellen

Wechseln Sie zum Hauptmenüpunkt "Identity-Management", Untermenü "Versionen", und erstellen Sie die SDK-Konfigurationsdatei. Geben Sie dazu die folgende URL an:

wss:// --Hostname/IP des Servers-- : --Port des Servers-- /dcem/ws/appConnection

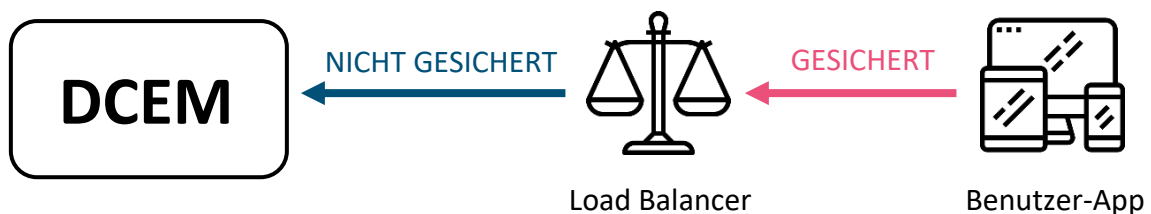
Nach der Installation wird ein Standard-Serverzertifikat für die SSL/TLS DeviceWebsockets-Verbindung (DeviceWebsockets_CA) generiert. Als Common Name (CN) des Zertifikats wird der URL-Hostname des Browsers eingestellt. Unterscheidet sich die Internet-Hostadresse vom Standard-CN des "DeviceWebsocket_CA"-Keystores, müssen Sie einen neuen "DeviceWebsocket_CA"-Keystore generieren und als CN die Internet-Hostadresse einstellen.

Gehen Sie zum Hauptmenüpunkt "System", Untermenü "KeyStores", um einen neuen "DeviceWebsocket_CA"-Keystore zu generieren, und klicken Sie auf "Neuen Keystore generieren".

Wechseln Sie zum Hauptmenüpunkt "Identity-Management", Untermenü "Versionen", und setzen Sie einen Haken neben "DCEM ,CA_Root Certificate' verwenden", wenn Sie den DoubleClue-Dispatcher in Kombination mit unserer DoubleClue-App verwenden möchten. Siehe hierzu Kapitel [6. Verbindungsszenarien](#) für weitere Schritte.

Wenn Sie Ihre eigene App verwenden möchten, laden Sie die SDK-Konfigurationsdatei herunter und integrieren Sie diese in Ihre App (siehe Bedienungsanleitungen zur Bereitstellung der App: [DC_Dev_Guide_Android.pdf](#) / [DC_Dev_Guide_iOS.pdf](#)).

3.4.2 SSL/TLS vom Endnutzer terminiert beim Load Balancer und ungesichert zu DCEM



3.4.2.1 KeyStore-Typ: DeviceWebsockets_CA

In diesem Fall wird die SSL/TLS-Verbindung vom Endnutzer am Load Balancer terminiert. Die Verbindung vom Load Balancer zu DCEM wird nicht mit SSL/TLS gesichert. DCEM benötigt keinen KeyStore für das DeviceWebsockets_CA.

3.4.2.2 SDK-Konfigurationsdatei erstellen

Wechseln Sie zum Hauptmenüpunkt "Identity-Management", Untermenü "Versionen", und erstellen Sie die SDK-Konfigurationsdatei. Geben Sie dazu die folgende URL an:

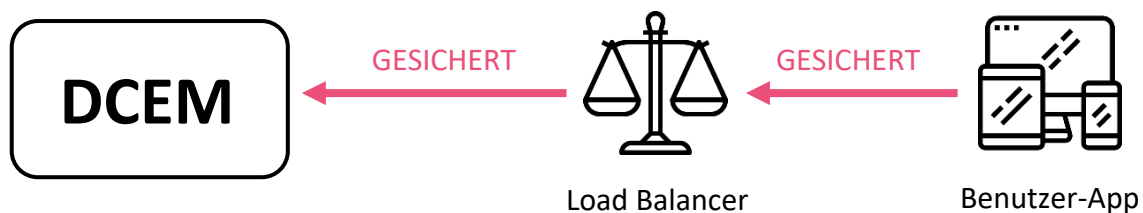
wss:// --Hostname/IP des Load Balancers-- : --Port des Load Balancers-- /dcem/ws/appConnection

Entfernen Sie den Haken neben "DCEM ,CA_Root Certificate' verwenden" und laden Sie den TrustStore mit den Zertifikaten des Load Balancers unter "Externen TrustStore im PEM-Format hochladen" hoch.

Laden Sie die Datei "**SdkConfig.dcem**" herunter, wenn Sie den DoubleClue-Dispatcher in Kombination mit unserer DoubleClue-App verwenden möchten. Siehe hierzu Kapitel [6. Verbindungsszenarien](#) für weitere Schritte.

Wenn Sie Ihre eigene App verwenden möchten, laden Sie die SDK-Konfigurationsdatei herunter und integrieren Sie diese in Ihre App (siehe Bedienungsanleitungen zur Bereitstellung der App: **DC_Dev_Guide_Android.pdf** / **DC_Dev_Guide_iOS.pdf**).

3.4.3 SSL/TLS vom Endnutzer terminiert beim Load Balancer und gesichert zu DCEM



3.4.3.1 KeyStore-Typ: DeviceWebsockets_CA

In diesem Fall wird die SSL/TLS-Verbindung vom Endnutzer am Load Balancer terminiert. Die Verbindung vom Load Balancer zu DCEM wird zusätzlich mit SSL/TLS gesichert. DCEM benötigt einen KeyStore für das DeviceWebsockets_CA, wobei der Hostname immer der des jeweiligen Knotens sein muss.

3.4.3.2 Download als PEM

Laden Sie für das Root_CA den TrustStore im PEM-Format herunter und speichern Sie die Datei auf dem Load Balancer. Dieser Schritt ist notwendig, damit die gesicherte Verbindung zwischen Load Balancer und Server hergestellt werden kann.

3.4.3.3 SDK-Konfigurationsdatei erstellen

Wechseln Sie zum Hauptmenüpunkt "Identity-Management", Untermenü "Versionen", und erstellen Sie die SDK-Konfigurationsdatei. Geben Sie dazu die folgende URL an:

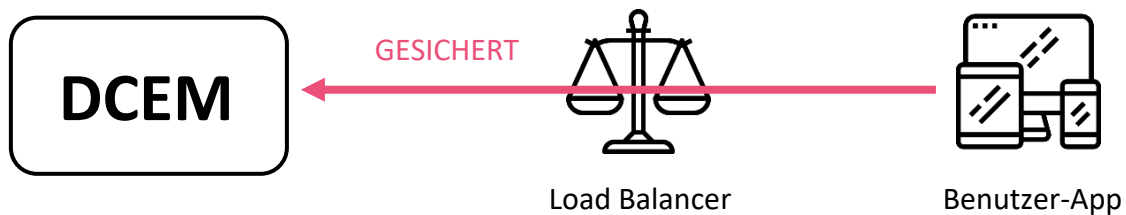
wss:// --Hostname/IP des Load Balancers-- : --Port des Load Balancers-- /dcem/ws/appConnection

Entfernen Sie den Haken neben "DCEM ,CA_Root Certificate' verwenden" und laden Sie den TrustStore mit den Zertifikaten des Load Balancers unter "Externen TrustStore im PEM-Format hochladen" hoch.

Laden Sie die Datei "**SdkConfig.dcem**" herunter, wenn Sie den DoubleClue-Dispatcher in Kombination mit unserer DoubleClue-App verwenden möchten. Siehe hierzu Kapitel [6. Verbindungsszenarien](#) für weitere Schritte.

Wenn Sie Ihre eigene App verwenden möchten, laden Sie die SDK-Konfigurationsdatei herunter und integrieren Sie diese in Ihre App (siehe Bedienungsanleitungen zur Bereitstellung der App: **DC_Dev_Guide_Android.pdf** / **DC_Dev_Guide_iOS.pdf**).

3.4.4 SSL/TLS vom Endnutzer terminiert bei DCEM mit Load Balancer (Passthrough)



3.4.4.1 KeyStore-Typ: DeviceWebsockets_CA

In diesem Fall wird die SSL/TLS-Verbindung vom Endnutzer bei DCEM terminiert und dabei durch einen Load Balancer durchgeschleift. DCEM benötigt einen KeyStore für das DeviceWebsockets_CA, wobei der Hostname immer der des Load Balancers sein muss.

3.4.4.2 SDK-Konfigurationsdatei erstellen

Wechseln Sie zum Hauptmenüpunkt "Identity-Management", Untermenü "Versionen", und erstellen Sie die SDK-Konfigurationsdatei. Geben Sie dazu die folgende URL an:

wss:// --Hostname/IP des Load Balancers-- : --Port des Load Balancers-- /dcem/ws/appConnection

Setzen Sie einen Haken neben "DCEM ,CA_Root Certificate' verwenden", wenn Sie das DoubleClue-Root-Certificate als Identifizierungszertifikat für die DoubleClue-App verwenden möchten. Wenn Sie ein eigenes Zertifikat verwenden wollen, entfernen Sie den Haken und laden Sie Ihr eigenes Zertifikat hoch. Siehe hierzu auch Kapitel [6. Verbindungsszenarien](#) für weitere Schritte.

Wenn Sie Ihre eigene App verwenden möchten, laden Sie die SDK-Konfigurationsdatei herunter und integrieren Sie diese in Ihre App (siehe Bedienungsanleitungen zur Bereitstellung der App: **DC_Dev_Guide_Android.pdf** / **DC_Dev_Guide_iOS.pdf**).

3.4.5 SDK-Konfigurationsdatei

Die SDK-Datei wird vom Server erstellt. Sie beinhaltet die Verbindungskonfigurationen sowie den Public Key des Clusters. Unabhängig davon, ob die Verbindung mit SSL/TLS gesichert ist, wird geprüft, ob die SDK den gültigen Public Key besitzt.

Die SDK-Datei wird aus den folgenden Gründen benötigt:

- Festlegen des Verbindungsziels der App
- Speicherort für den Public Key des Clusters

3.5 Neuen KeyStore hochladen

Möchten Sie statt des hier erstellten DeviceWebsockets_CA einen KeyStore mit Zertifikaten hochladen, können Sie dies über den Button "Neuen KeyStore hochladen" (Hauptmenü: "System", Untermenü: "KeyStores") tun. Dazu werden der KeyStore im PKCS#12-Format und das dazugehörige Passwort benötigt.

3.6 Cluster-Netzwerk-Kommunikation

3.6.1 Ein Netzwerk

Befinden sich alle Knoten im selben Netzwerk, können die Standardeinstellungen für Multicast verwendet werden.

3.6.2 Mehrere Netzwerke mit Multicast

Befinden sich die Router in unterschiedlichen Netzwerken, muss auf ihnen Multicast erlaubt sein, um die Standard-Einstellungen für Multicast verwenden zu können.

Standardmäßig wird Multicast-Group 224.2.2.3 mit Port 54327 verwendet.

3.6.3 Mehrere Netzwerke ohne Multicast

Ist Multicast nicht erlaubt, müssen die Standard-Einstellungen auf TCP/IP umgestellt werden.

Dazu benötigen Sie die im Ordner "**DCEM_HOME**" gespeicherte Datei "**x_HazelcastClusterConfig.xml**". Benennen Sie diese um in "**HazelcastClusterConfig.xml**".

DCEM liest die Cluster-Konfigurationsdatei namens **“DCEM_HOME/HazelcastClusterConfig.xml”**. Solange keine Datei mit diesem Namen vorhanden ist, wird eine Standard-Konfiguration verwendet.

Die Datei **“HazelcastClusterConfig.xml”** muss, wie die Datei **“configuration.xml”**, auf jeden dazugehörigen Server kopiert werden.

Dabei müssen in der Datei **“HazelcastClusterConfig.xml”** folgende Änderungen vorgenommen werden:

- 1) `<multicast enabled = "true">`

Setzen Sie den Wert **“true”** auf **“false”**.

- 2) `<tcp-ip enabled = "false">`

Setzen Sie den Wert **“false”** auf **“true”**.

- 3) `<interface> --IP der Netzwerkkarte-- </interface>`

Tragen Sie die Netzwerkkarten-IP des Servers ein. Diese Einstellung muss auf jedem Server individuell vorgenommen werden.

Sind mehrere Netzwerkkarten auf dem Server vorhanden, kopieren Sie die Zeile für jede Netzwerkkarte und tragen jede IP einmal ein.

- 4) `<member> --Hostname/IP des Servers-- </member>`

Kopieren Sie die Zeile für jeden Server und tragen Sie jeweils den Hostnamen bzw. die IP ein. Es können beliebig viele Server hinzugefügt werden.

Kommt ein neuer Server hinzu, muss dieser in jeder Datei **“HazelcastClusterConfig.xml”** auf jedem Server hinzugefügt werden.

Weitere Details finden Sie in Kapitel 6 des Dokuments **“DcemInstallation/doc/ClusterHazelcast-3.7.4.pdf”**.

4 Administration

4.1 Benutzer

4.1.1 Benutzer hinzufügen

Neue Benutzer können sich selbstständig im UserPortal registrieren oder über die REST-Web Services-Schnittstelle aus einem Active Directory importiert werden. DoubleClue unterstützt das Microsoft Active Directory, Microsoft Azure Active Directory und LDAP und erlaubt es Benutzer direkt aus diesen Directories zu importieren. Außerdem können Administratoren neue Benutzer manuell unter „Administration“ > „Benutzer“ anlegen.

Bitte beachten Sie: Der Anmeldename eines Domain-Benutzers benötigt immer den Namen der Domain als Präfix, gefolgt von einem Backslash (Beispiel: **“BEISPIELDOMAIN\max.muster”**).

4.1.2 Benutzer Anmeldename

Es ist nicht möglich, Benutzer mit einem Anmeldennamen hinzuzufügen, der eines der folgenden Zeichen enthält:

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

4.1.3 Benutzerpasswort

Lokale Benutzer benötigen ein Benutzerpasswort. Bei der Registrierung über UserPortal können Benutzer ihr Passwort selbst festlegen. Werden sie von einem Administrator registriert, kann dieser Ihnen ein Passwort zuweisen, dass die Benutzer später im UserPortal selbstständig ändern können.

Domain-Benutzer verwenden Ihr Domain-Passwort.



Da Domain-Nutzer beim Einloggen mit dem Active Directory synchronisiert werden, ist es nicht möglich, für sie ein spezielles DoubleClue-Passwort anzulegen. Es wird bei jedem Log-in automatisch überschrieben und durch das Domain-Passwort ersetzt.

4.1.4 Hinzufügen eines Aktivierungscodes

Aktivierungscodes werden zur ersten Aktivierung der DoubleClue-App benötigt.

Nachdem ein neuer Benutzer angelegt wurde, muss für diesen ein Aktivierungscode erstellt werden.

Es gibt vier Möglichkeiten, dies zu tun:

1. Gehen Sie zum Hauptmenüpunkt "Identity-Management", Untermenü "Aktivierungscodes" und klicken Sie auf "Hinzufügen". Tragen Sie den Benutzernamen in das entsprechende Feld ein, wählen Sie die Methode aus, mit der Sie den Code versenden wollen, und bestätigen Sie die Angabe.
2. Gehen Sie zum Hauptmenüpunkt "Administration", Untermenü "Benutzer". Markieren Sie den/die Benutzer, dem/denen Sie einen Aktivierungscode zuweisen möchten und klicken Sie auf "Aktivierungscode erstellen".
Dieses Vorgehen kann ebenfalls für Gruppen gewählt werden (Hauptmenüpunkt "Administration", Untermenü "Gruppen").
3. Aktivierungscodes können auch automatisch über die REST-Web Services-Schnittstelle hinzugefügt werden oder während des Imports von Benutzern aus einer Domäne.
4. Benutzer können im DoubleClue UserPortal unter Geräteverwaltung selbst einen Aktivierungscode anfordern.



Bitte beachten Sie: Wenn Sie mehrere Aktivierungscodes auf einmal per E-Mail senden, könnte Ihr E-Mail-Server ab einer bestimmten Anzahl an E-Mails Senderrestriktionen auf den von Ihnen verwendeten E-Mail-Account anwenden. Deshalb ist es eventuell nötig, die Anzahl der E-Mails, die gleichzeitig versendet werden dürfen, zu erhöhen. Verwenden Sie z.B. Microsoft Exchange, können Sie den entsprechenden Parameter, "Message Rate Limit", unter "Receive Connector" verändern.

4.1.5 Telefon- und Mobilnummer


Die Telefonnummer und Mobilnummer eines Nutzers werden nur benötigt, wenn sie SMS und/oder Voice Message als Authentifizierungsmethode verwenden wollen (siehe hierzu Kapitel [7. Authentifizierungsmethoden und Policies](#)).

Wenn beide Nummern hinterlegt sind, wird DCEM für Voice Messages immer auf der Festnetznummer anzurufen. Wenn keine Festnetznummer für den Benutzer angelegt ist, wird es stattdessen auf die Mobilnummer wählen.


Für Domain-Benutzer werden automatisch die Telefon- und Mobilnummer aus dem Active Directory übernommen. Über UserPortal haben Benutzer außerdem die Möglichkeit, eine vertrauliche Telefonnummer anzulegen. Über diese kann DCEM SMS und Voice Messages verschicken, Administratoren können sie jedoch nicht einsehen.

4.1.6 Benutzerpasswort wiederherstellen

Hat ein lokaler Benutzer sein Passwort vergessen, kann ein Administrator, für dessen Rolle unter Zugriffsrechte die Funktion „reset_password“ aktiviert wurde, ihm ein neues Passwort zuweisen. Dies geht im „User“-Menü über den „Passwort zurücksetzen“-Button.

 Das neue Passwort wird dem Benutzer nicht automatisch mitgeteilt! Der Administrator muss es ihm auf einem anderen Weg (E-Mail, Messenger etc.) zukommen lassen.

Der Benutzer kann das zugewiesene Passwort in UserPortal ändern.

 Das Passwort von Domain-Benutzern kann nicht über DCEM zurückgesetzt werden. Dies muss über das entsprechende Active Directory erfolgen.

4.1.7 Gesperrte Benutzer

Wenn ein Benutzer sein Passwort zu oft falsch eingibt, wird sein Account gesperrt. Wie oft ein Benutzer das Passwort falsch eingeben kann, können Sie unter „Administration“ > „Einstellungen“ > „Max. Loginversuche (falsches Passwort)“ einstellen.

Sie können einen gesperrten Benutzer im Administrations-Menü unter „Benutzer“ wieder freischalten.

Wenn ein SuperAdmin seinen Zugriff verloren hat und das freischalten durch einen anderen Administrator nicht möglich ist, können Sie den Zugang über die Backdoor wieder herstellen (siehe Kapitel [4.3 SuperAdmin-Zugriff wiederherstellen](#)).

4.2 Rollen

Über die Rolle werden die Zugriffsrechte eines Users festgelegt. Weitere Informationen finden Sie unter Kapitel [4.4 Zugriffsrechte](#).

DCEM stellt 6 automatisch angelegte Standard-Rollen zur Verfügung. Weitere Rollen können in DCEM unter „Administration“ > „Rollen“ angelegt werden.

4.2.1 Rang

Rollen können einem von 11 verschiedenen Rängen zu geordnet werden. Der höchste Rang ist 10, der niedrigste ist null. Benutzer mit einem niedrigeren Rang können nicht die Benutzerinformationen oder Zugriffsrechte von Benutzer und Rollen mit einem höheren Rang verändern, selbst wenn Sie diese Rechte theoretisch haben.

Beispiel:

Ein Administrator (Rang 8) hat das Recht neue Benutzer anzulegen. Er kann aber nur neue Benutzer mit Rollen die Rang 8 oder einen niedrigeren Rang haben anlegen. Er kann keine Benutzer mit Rolle SuperAdmin (Rang 10) oder anderen Rollen mit Rang 9 oder 10 anlegen.

Rollen mit Rang 0 haben nur Zugriff auf UserPortal und können sich nicht in DCEM einloggen. Benutzer mit Rang 1-10 haben generell Zugriff auf DCEM. Was diese dort sehen können und welche Aktionen sie nutzen können, kann über die Zugriffsrechte eingestellt werden.

4.3 SuperAdmin-Zugriff wiederherstellen

4.3.1 SuperAdmin-Zugriff des Haupt-Mandanten wiederherstellen

Um den SuperAdmin-Zugriff für den *Haupt-Mandanten* wiederherzustellen, halten Sie DCEM an und rufen Sie das DoubleClue Setup auf, wie beschrieben in [2.3.4 Setup erneut ausführen](#). Speichern Sie die Database Configuration. Daraufhin wird der Button zur „Wiederherstellung des SuperAdmin-Zugriffs“ (Recover SuperAdmin Access) angezeigt.

Starten Sie den Wiederherstellungs-Prozess und geben Sie ein neues SuperAdmin-Passwort ein. Loggen Sie sich anschließend mit diesem Passwort und der User ID SuperAdmin in DCEM ein. Sie können nun unter Identity-Management die Policies bearbeiten und die MFA wieder aktivieren.

4.3.2 SuperAdmin-Zugriff eines Sub-Mandanten wiederherstellen

Um den SuperAdmin-Zugang für einen Sub-Mandanten wiederherzustellen, benötigen Sie einen SuperAdmin Zugriff auf das DCEM des Haupt-Mandanten. Rufen Sie im Hauptmenü „System“ den Bereich Mandanten aus. Wählen Sie den Mandanten, dessen SuperAdmin Sie wiederherstellen möchten, und starten Sie anschließend den Vorgang über den entsprechenden Button über der Liste der Mandanten. Geben Sie ein neues SuperAdmin-Passwort ein. Loggen Sie sich anschließend mit diesem Passwort und der User ID SuperAdmin in das Sub-Tenant-DCEM ein. Sie können nun unter Identity-Management die Policies bearbeiten und die MFA wieder aktivieren.

4.3.3 Effekt der Wiederherstellung des SuperAdmin-Zugriffs

Sollten Sie den Zugriff auf Ihren SuperAdmin-Account verlieren, z.B. weil das Passwort vergessen oder das MFA Gerät verloren wurde, können Sie den Zugang über das Backdoor-System wiederherstellen.

Durch diesen Vorgang wird:

- ein neuer Nutzer mit SuperAdmin-Rechten mit dem Namen „SuperAdmin“ eingerichtet, sollte dieser zuvor gelöscht worden sein.
- der Nutzer mit dem Namen SuperAdmin entsperrt, sollte der Account zuvor gesperrt gewesen sein, und erhält die Rolle eines SuperAdmins.
- das SuperAdmin-Passwort zu dem eingegebenen Passwort geändert.
- dem SuperAdmin das Recht gegeben, Zugriffsrechte zu modifizieren.
- die Sicherheits-Policy von DCEM modifiziert und der Login ohne MFA nur mit dem Passwort erlaubt.



Achtung: Es wird empfohlen, die Sicherheits-Policies nach der Wiederherstellung sofort wieder zu ändern und MFA für DCEM zu aktivieren.

4.4 Zugriffsrechte

Die Zugriffsrechte für die verschiedenen Rollen können in DCEM unter Administration > Zugriffsrechte verwaltet werden. Hier können Sie mithilfe von Checkboxes festlegen, welche Rollen auf DCEM selbst, die Hauptmenüpunkte in DCEM, deren Untermenüpunkte und jede dazugehörige Aktion Zugriff haben sollen.

Der Bereich „Modul“ zeigt die einzelnen Hauptmenüpunkte an, für welchen Zugriffsrechte festgelegt werden können.

Der Bereich „Subjekt“ zeigt die zu den jeweiligen Hauptmenüpunkten gehörenden Untermenüpunkte an, für welche Zugriffsrechte festgelegt werden können.

Der Bereich „Aktion“ beinhaltet alle durchführbaren Aktionen, die in den einzelnen Teilbereichen möglich sind. Dazu gehören unter anderem die Aktionen „Add“, „Edit“, „Delete“ und „Save“. Für jede Aktion muss einzeln das Recht vergeben werden, dass diese von einer bestimmten Rolle durchgeführt werden darf.

Sie können einer Rolle für einen Punkt des Haupt- oder Untermenüs generell das Recht geben, alle Aktionen durchzuführen. In diesem Fall benötigt die Rolle für den gewünschten Menüpunkt das Recht für die Aktion „Manage“.

Soll ein Administrator nur Leserechte haben, legen Sie für dessen Rolle für den gewünschten Menüpunkt die Aktion „View“ fest.

4.5 Gruppen

Benutzer können in verschiedene Gruppen eingeteilt werden. Über die Gruppen kann man den Benutzer anschließend verschiedene Policies zuweisen (siehe Kapitel [7.3 Policies](#)). Ein Benutzer kann Mitglied mehrerer Gruppen sein.

4.6 Integration von Active Directory / Microsoft Azure AD / LDAP

DCEM unterstützt multiple Domänen. Es ist absolut notwendig, dass jeder Domain-Eintrag einen einzigartigen Domain-Namen hat. Neue Benutzer können danach aus verschiedenen Domains importiert werden. DCEM unterstützt drei Domain-Typen:

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

Sie können Ihre Benutzer gegenüber der Domäne mit Benutzername und Passwort authentifizieren. Ist ein Benutzer als "Domain-Benutzer" gekennzeichnet, verifiziert DCEM die Kontoanmeldedaten des Benutzers gegenüber dem Active Directory / Azure AD / LDAP.

Verwendete Domänen müssen zunächst konfiguriert werden.



Bitte beachten Sie: Haben Sie eine Domäne einmal konfiguriert und den entsprechenden Domain-Typ gewählt, kann diese Auswahl nicht mehr verändert werden.

4.6.1 Hinzufügen einer standardmäßigen Active Directory-Konfiguration

Gehen Sie zum Hauptmenüpunkt "Administration", Untermenü "Domain" und klicken Sie auf "Hinzufügen". Wählen Sie dann als Domain-Typ "Active Directory" aus.

Name:

Vergeben Sie einen einzigartigen, aussagekräftigen Namen für die Domäne. Dieser wird als Präfix für alle Benutzernamen der Benutzer aus dieser Domäne verwendet.

URL:

Sie können mehrere URLs eingeben, die mit einem Leerzeichen getrennt werden müssen. Haben Sie mehr als eine URL angegeben, wird DCEM versuchen, sich mit der ersten URL zu verbinden. Sollte dies fehlschlagen, wird DCEM versuchen, sich mit der nächsten konfigurierten URL zu verbinden usw.

Basis-DN:

Geben Sie den Distinguished Name des Active Directory-Servers an. Auf dieser Basis werden die Benutzer für das Active Directory gesucht.

Search Account-DN/UPN:

DCEM benötigt einen "Search Account", um im Active Directory nach Benutzern und Gruppen zu suchen.

Map E-Mail Suffixes to this Domain:

Geben Sie hier die E-Mail-Suffixes der UPNs ein, die sie dieser Domain zuordnen können. Sie können mehrere E-Mail-Suffixes eingeben, indem Sie sie durch ein Semikolon (;) trennen.

Rank:

Wenn ein E-Mail-Suffix mehreren Domains zugeordnet wird, legt der Rang fest mit welcher Domain sich UPNs mit diesem Suffix verbinden.

Timeout in Sek:

Zeit, die benötigt wird, um eine Verbindung von DCEM mit dem Active Directory herzustellen.

4.6.2 Hinzufügen einer Azure AD-Konfiguration

Eine genaue Anleitung zur Integration Ihres Microsoft Azure Active Directory finden Sie unter:

DcemInstallation/doc/Integrating Azure_EN.pdf.

4.6.3 Hinzufügen einer LDAP-Konfiguration

Gehen Sie zum Hauptmenüpunkt "Administration", Untermenü "Domain" und klicken Sie auf "Hinzufügen". Wählen Sie dann als Domain-Typ "Generic LDAP" aus.

Name:

Vergeben Sie einen einzigartigen Namen für die Domäne.

URL:

Sie können mehrere URLs eingeben, die mit einem Leerzeichen getrennt werden müssen. Haben Sie mehr als eine URL angegeben, wird DCEM versuchen, sich mit der ersten URL zu verbinden. Sollte dies fehlschlagen, wird DCEM versuchen, sich mit der nächsten konfigurierten URL zu verbinden.

Basis-DN:

Geben Sie den DN (Distinguished Name) des LDAP-Servers an. Basierend darauf werden die LDAP-Benutzer gesucht.

Search Account-DN/UPN:

DCEM benötigt einen "Search Account", um im LDAP nach Benutzern zu suchen.

Filter + Login-Attribut:

Bei einem Active Directory können beim Filter und dem Login-Attribut die Standardeinstellungen beibehalten werden:

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

Login-Attribut: sAMAccountName

Wenn Sie einen anderen auf LDAP basierenden Verzeichnisdienst verwenden, kann es sein, dass Sie in beiden Fällen "sAMAccountName" z. B. durch den Common Name "cn" ersetzen müssen.

Vornamen-Attribut + Mobiltelefon-Attribut:

Passen Sie die Attribute an Ihr LDAP-Verzeichnis an.

Standard-Einstellungen:


Timeout in Sek:

Zeit, die benötigt wird, um eine Verbindung von DCEM mit LDAP herzustellen.

4.6.4 Import von Benutzern aus Gruppen aus einer Domäne


Im Hauptmenü „Administration“ Untermenü "Import aus Domain" können Administratoren Benutzer und Gruppen aus dem Active Directory /Azure AD / LDAP importieren, indem sie entweder eine Wildcard-Suche für Benutzer und Gruppen durchführen oder Benutzer aus existierenden Gruppen auswählen. E-Mail-Adressen, Anzeigenamen, Mobiltelefonnummern und die LDAP-Distinguished Names (DN) bzw. die Azure AD User Object-ID werden ebenfalls abgerufen.

Der Anmeldename von Benutzern, die aus einer Domäne importiert wurden, besteht aus dem Domain-Namen als Präfix, wobei ein Backslash dieses vom Domain-Anmeldenenamen des Benutzers trennt (wird z.B. der Benutzer "max.muster" aus der LDAP-Domain "BEISPIELDOMAIN" importiert, ist sein Anmeldename "BEISPIELDOMAIN\max.muster").

 Ein Benutzer-Anmeldename ohne Backslash wird von DCEM als lokaler Benutzer angesehen.

Während des Imports von Benutzern haben Administratoren die Möglichkeit, AktivierungsCodes für die zu importierenden wie auch die bereits existierenden Benutzer zu generieren. AktivierungsCodes können automatisch per E-Mail oder SMS an Benutzer gesendet werden, wenn die E-Mail- oder SMS-Dienste entsprechend in den Systemeinstellungen konfiguriert wurden.

Bevor Benutzer aus einer Domäne importiert werden können, muss eine Domain-Verbindung konfiguriert werden (siehe hierzu Kapitel 3.7.1 bis 3.7.3).

 Bitte beachten Sie: DCEM speichert keine Domain-Passwörter von Benutzern.

4.6.4.1 Admin-Einstellung „enableUserDomainSearch“

Unter „Administration“ im Untermenüpunkt „Einstellungen“ können Administratoren auswählen, ob sich Benutzer mit ihrem vollständigen Anmeldenamen inklusive ihres Domain-Namens einloggen müssen, oder nicht.

Befindet sich kein Häkchen in der Box neben „Benutzer-Domain-Suche aktivieren“ (dies ist Standard), müssen alle Benutzer ihren vollständigen Anmeldenamen inklusive der Domäne eingeben.

Ist das Häkchen gesetzt, können Benutzer ihren Anmeldenamen ohne Domain-Namen („max.muster“) eingeben. In diesem Fall sucht DCEM lokal und in allen Domänen nach den Benutzern. Der Benutzer-AnmeldeName wird zurückgewiesen, wenn die Suche in multiplen Einträgen resultiert, was bedeutet, dass der Benutzer seinen Anmeldenamen mit dem Domain-Namen-Präfix („BEISPIELDOMAIN\max.muster“) eingeben muss.


Sollte sich der Benutzer dennoch als lokaler Benutzer anmelden wollen, muss er einen Backslash vor seinen Anmeldenamen setzen („\max.muster“).

Wenn die Benutzersuche nur einen Eintrag ergibt, wird der Benutzer-AnmeldeName „max.muster“ akzeptiert.

4.7 Vorlagen

Um Daten oder Texte in der DoubleClue-App anzeigen zu können, werden Vorlagen benötigt. Mit der Installation von DCEM werden diverse Standard-Vorlagen bereitgestellt. Diese finden Sie im Hauptmenü „Administration“, Untermenü „Vorlagen“.

4.7.1 Aufbau einer Vorlage

Der Inhalt einer Vorlage kann in Textform oder im HTML-Format eingefügt werden. Das Umschalten zwischen GUI und HTML-Format erfolgt im jeweiligen Bearbeitungsfenster über den Button: 

Um eingegebene Daten aus dem Portal anzeigen zu können, müssen die Vorlagen um Platzhalter (sog. Daten-Token) ergänzt werden. Ein Daten-Token wird in eine doppelte geschweifte Klammer gesetzt: **{{Name Data Token}}**. Für die Anzeige werden die Daten-Token durch die Daten aus der REST-Schnittstelle ersetzt.

Wird eine Vorlage zum Senden einer Push Approval an die DoubleClue-App erstellt, muss diese immer einen Button zum Bestätigen bzw. Schließen der Message haben. Dazu müssen Buttons im HTML-Format mit dem Befehl `<button>` eingefügt und mit einer Aktions-ID versehen werden.

Beispiel: `<button id="ID-Name">Buttontext</button>`

4.7.2 Sprache

Für jede Sprache, die verfügbar sein soll, muss eine eigene Vorlage angelegt werden. Eine Sprache kann als Standardsprache definiert werden. Soll eine Vorlage in einer Sprache verwendet werden, in der sie nicht vorhanden ist, wird stattdessen die entsprechende Vorlage in der gewählten Standardsprache verwendet. Sollte die Vorlage auch in der Standardsprache nicht verfügbar sein, wird als Default Englisch verwendet.

4.7.3 Hinzufügen einer Vorlage

Vorlagen, die den gleichen Inhalt haben, aber in unterschiedlichen Sprachen erstellt werden, müssen für alle Sprachen den gleichen Namen haben (Vorlagengruppe). Die Differenzierung der Vorlagen erfolgt über die Sprachauswahl.

- Legen Sie pro Vorlagengruppe eine Standard-Vorlage fest. Diese wird verwendet, wenn für den Benutzer eine Sprache gewählt wurde, für die es keine eigene Vorlage gibt.
- Legen Sie den Inhalt der Vorlage fest:
 - Anzeigetext: Fester Text, der in der Vorlage angezeigt werden soll.
 - KeyToken: Platzhalter, die durch erfasste Werte ersetzt werden. Diese stehen immer in doppelter geschweiffter Klammer `{{ }}`.
 - Aktionsfelder: Button z.B. zum Bestätigen oder Ablehnen der Aktion.

- Beispiel:

Edit

Name: Language: Default: ☐

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

Überweisung

Empfänger: {{recipient}}
 IBAN: {{iban}}
 Betrag: {{amount}}
 Verwendungszweck: {{purpose}}

Bestätigen **Ablehnen**

☒ OK ☐ Cancel

4.7.4 Ändern einer Vorlage

Sobald eine Vorlage an einer Stelle verwendet wird, wird der Wert für “In Verwendung” im Hauptmenü “Administration”, Untermenü “Vorlagen” auf “true” gesetzt. Diese Vorlage kann nicht mehr geändert werden. Es kann jedoch eine neue Version der Vorlage angelegt werden.

4.7.5 Löschen einer Vorlage

Sobald eine Vorlage an irgendeiner Stelle verwendet wurde, kann diese nicht mehr gelöscht werden.

4.8 Textquellen

Unter Textquellen können Sie verschiedene Texte modifizieren, die insbesondere in SAML- und Single Sign-on-Interfaces angezeigt werden. Sie können jeden Text in verschiedenen Sprachen anlegen. Ein eingeloggtter Benutzer sieht die Texte dann grundsätzlich in der Sprache, die er als Benutzersprache ausgewählt hat. Ist ein Text in einer bestimmten Sprache nicht vorhanden oder der Benutzer nicht eingeloggt, wird der Text automatisch in der eingestellten Standardsprache angezeigt.

4.9 Änderungshistorie

In der Änderungshistorie werden alle Aktionen aufgelistet, die von den Administratoren im System durchgeführt wurden.

4.10 Lizenzen

In diesem Submenü können Sie Lizenzschlüssel importieren und finden eine Übersicht über Ihre aktuellen Lizenzen. Mehr Informationen über Lizenzen finden Sie in [Kapitel 15. Lizenzierungssystem](#).

4.11 Einstellungen

In diesem Submenü können Sie die folgenden generellen Einstellungen für DoubleClue vornehmen:

Banner-Stil – Passen Sie das DCEM-Banner Ihrem individuellen Style an, indem Sie die Anpassungen in CSS-Code eingeben (z.B. *font-style: italic; background-color: orange*). Sie müssen sich neu in DCEM einloggen, damit die Änderungen aktiv werden.

Benutzer-Domain-Suche aktivieren – Die Benutzer-Domain-Suche erlaubt es Ihnen, Benutzer nach Ihrem Benutzernamen ohne Präfix zu suchen. Sollte der gleiche Benutzername in mehreren Subdomains/Mandaten zu finden sein, werden diese Optionen aufgelistet.

Speicherdauer-Historien-Archiv – Stellen Sie ein, wie viele Tage das Historien-Archiv die aufgezeichneten Einträge speichert.

5. Mandantenfähigkeit (Multi-Tenant)

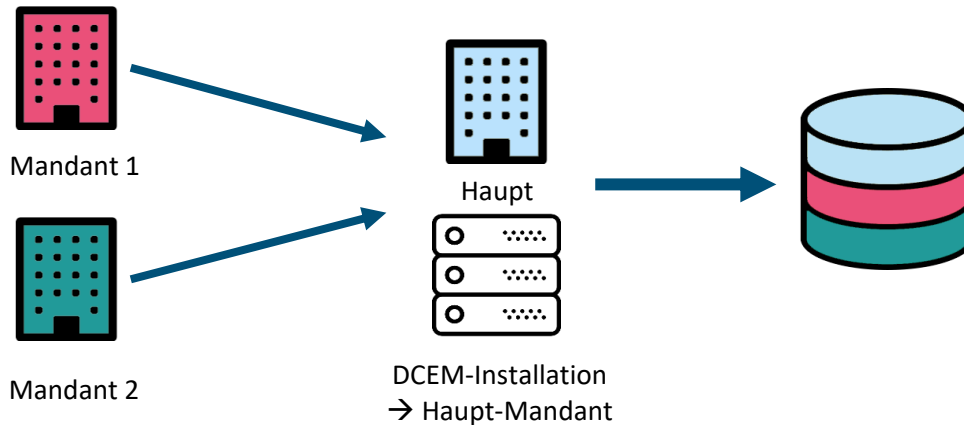
DCEM unterstützt mehrere Mandanten (Tenants) und kann daher als "SaaS" (Software as a Service) ausgeführt werden. Es gibt eine Infrastruktur, das heißt, alle Mandanten teilen sich dieselbe DCEM-Installation, Datenbank, PKI, URL und Clusterknoten.

Nach der Installation wird ein Haupt-Mandant erstellt, welcher als Standard-Mandant fungiert. Von dort aus können zusätzliche Sub-Mandanten erstellt werden.

Die Mandantenfähigkeit wird nur von externen Datenbanken unterstützt. Mit einer Embedded Datenbank kann sie nicht genutzt werden.

5.1 Konzept

Für jeden Sub-Mandanten erstellt DCEM eine neue Datenbank / ein neues Schema, sodass jeder Mandant seine eigene abgeschlossene Datenbank besitzt. So werden die Daten des Master-Mandanten und die der Sub-Mandanten klar voneinander getrennt.



Jeder Mandant hat seine eigene Lizenz und kann seine Benutzer, Geräte, Policies, LDAP-Domains, RADIUS, SAML etc. vollständig selbst verwalten. Die PKI, URLs, Ports, Clusterknoten und Diagnosen jedoch werden zentral im Master-Mandanten verwaltet.

⚠ Bitte beachten Sie die folgenden Einschränkungen:

- Mehrere Mandanten werden nicht unterstützt, wenn die “Embedded Database” verwendet wird.
- Nachdem ein Mandant gelöscht oder deaktiviert wurde, ist die Anmeldung für einen Benutzer dieses Mandanten nicht mehr möglich. Die Datenbank des gelöschten Mandanten bleibt jedoch bestehen. Dies bedeutet, dass veraltete Datenbank-Schemas manuell gelöscht werden müssen.

5.2 Mandanten als Subdomains

Verschiedene Mandanten können über Subdomains erreicht werden. In diesem Fall benötigen Sie ein SSL / TLS Wildcard-Zertifikat für DCEM, um die Subdomains abzusichern. Die Hauptdomain (z.B. doubleclueOne.com) muss in der Clusterkonfiguration konfiguriert werden. Jeder Mandant erhält eine Subdomain, zum Beispiel „tenantName.doubleclueOne.com“.

5.3 Management mehrerer Mandanten

Mandanten können durch den Administrator des Haupt-Mandanten von DCEM verwaltet werden. Gehen Sie zum Hauptmenüpunkt “System”, Untermenü “Mandanten”, um einen Mandanten hinzuzufügen oder zu bearbeiten.

Um einen neuen Mandanten anzulegen, benötigen Sie Administratorzugriff auf die Datenbank. Geben Sie den entsprechenden Benutzernamen und das Passwort an. Legen Sie anschließend einen einzigartigen und aussagekräftigen **Namen**, **Schema-Namen** und **Anzeigenamen** für den neuen Mandanten fest.


Der angegebene **Name** wird zukünftig auch als Suffix für den Anmeldenamen zum App-Login und das Präfix für die Subdomain verwendet und sollte deswegen für Benutzer leicht zu merken und zu schreiben sein.

Der **Name** und **Anzeigename** können bei Bedarf im Nachhinein geändert werden.

Der **Name** und der **Schema-Name** dürfen nur aus alphanumerischen Zeichen bestehen.

Wenn der Mandant neu erstellt wurde, übernimmt er zunächst die Global und DCEM Management Policies des Haupt-Mandanten. Die Policies können anschließend im DCEM des jeweiligen Sub-Mandanten überarbeitet werden.

 Nachdem ein Mandant angelegt wurde, ist er sofort in Betrieb.

 Achten Sie beim Festlegen von Mandanten darauf, dass der Host Domain Name unter Clusterkonfiguration richtig angelegt ist. Wenn Sie mehrere Host Domain Namen verwenden, trennen Sie diese mit einem **Semikolon (;)**.

5.4 Anmeldeszenarien bei mehreren Mandanten

5.4.1 Anmeldung via Subdomain bei mehreren Mandanten

In einem Szenario mit mehreren Mandanten kann man sich bei einem bestimmten Mandanten anmelden, indem man sich über die entsprechende Subdomain einloggt. Der Name der Subdomain entspricht dabei dem Namen des Mandanten. Wird keine Subdomain angegeben, wird automatisch der Master-Mandant verwendet.

Die URLs setzen sich gemäß der Formel: subdomain. + host domain/ + Anwendung zusammen. Die Anmeldung via Subdomain ist für folgende Anwendungen verfügbar:

- DCEM – Beispiel: *mandant.doubleclue.online/dcem/mgt*
- DoubleClue UserPortal – Beispiel: *mandant.doubleclue.online/dcem/userportal*
- Service-initiierte Anmeldung mit SAML
- Provider-initiierte Anmeldung mit SAML

5.4.2 App- und RADIUS-Anmeldung bei mehreren Mandanten

Die DoubleClue App und RADIUS verwenden keine Subdomain. Die Anmeldung in einem Szenario mit mehreren Mandanten funktioniert deswegen wie folgt:

- DoubleClue-App:
Um einen Nutzer bei Anmeldung in der DoubleClue App einem bestimmten Mandanten zuzuordnen, wird der Anmelde-name des Nutzers wie folgt aufgebaut:
"user\$RealmName!mandant1"

“RealmName” ist der Name der „Host Domain“ und “mandant1” ist der Name des Mandanten, getrennt durch ein Ausrufezeichen.

- RADIUS:
Mandanten können ihre eigenen RADIUS-Clients unterstützen und konfigurieren. Die Clients werden durch ihre IP-Nummer voneinander unterschieden. Eine RADIUS NAS-Client IP-Nummer muss für die globale Installation von DCEM eindeutig sein.

5.4.3 Alternativ: Anmeldung mit mandantenspezifischen Benutzernamen

Anstatt eine Sub-Domain zu verwenden, kann man auch mandantenspezifische Benutzernamen nutzen, um sich bei verschiedenen DoubleClue-Anwendungen anzumelden.

“mandant1” ist der eindeutige Name des Mandanten, getrennt durch ein Ausrufezeichen.

- Benutzeranmeldename für DCEM: “superAdmin!*mandant1*”
- Anmeldename des REST-Services-Administrators: “administrator!*mandant1*”
- Anmeldename für UserPortal-Nutzer: “user!*mandant1*”
- Service-initiierte Anmeldung mit SAML: “-- URL -- ?*mandant=mandant1*”
Ist SAML service-initiiert, muss die URL den Namen des Mandanten enthalten.
- Provider-initiierte Anmeldung mit SAML: “userLoginId!*mandant1*”

5.5 Lizenzen für Mandanten

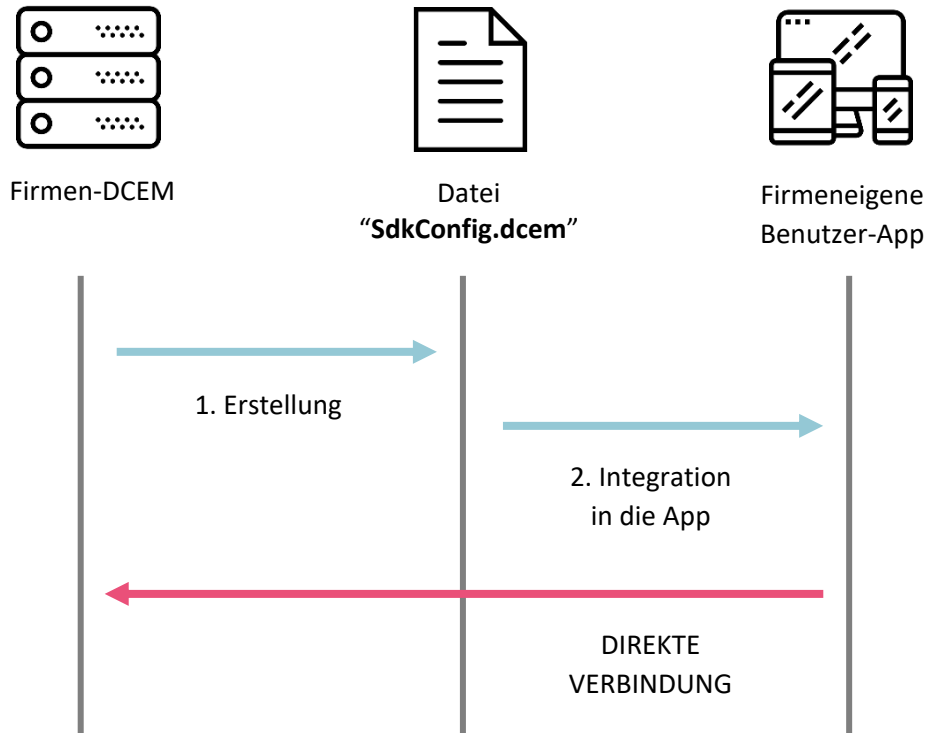
Jeder Mandant benötigt seinen eigenen Lizenzschlüssel. Nachdem ein Mandant erstellt wurde, wird ihm eine Testlizenz für 100 Benutzer über einen Zeitraum von drei Monaten zugewiesen. Bitte kontaktieren Sie sales@doubleclue.com, um eine volle Lizenz für einen Mandanten zu erhalten.

6. Verbindungsszenarien

6.1 Überblick

6.1.1 Direkte Verbindung mit eigener App

Die App verbindet sich direkt mit Ihrer Firmeninstallation von DCEM. Sie müssen die App erstellen und in Cloud-Stores wie den Google Playstore oder den App Store hochladen.



Die sichere Artefakt-Datei **"SdkConfig.dcem"**, die von DCEM generiert wird, muss ins App-Ressourcenverzeichnis kopiert werden. Siehe hierzu die Bedienungsanleitungen zur Bereitstellung der App: [DC_Dev_Guide_Android.pdf](#) / [DC_Dev_Guide_iOS.pdf](#).

Vorteile:

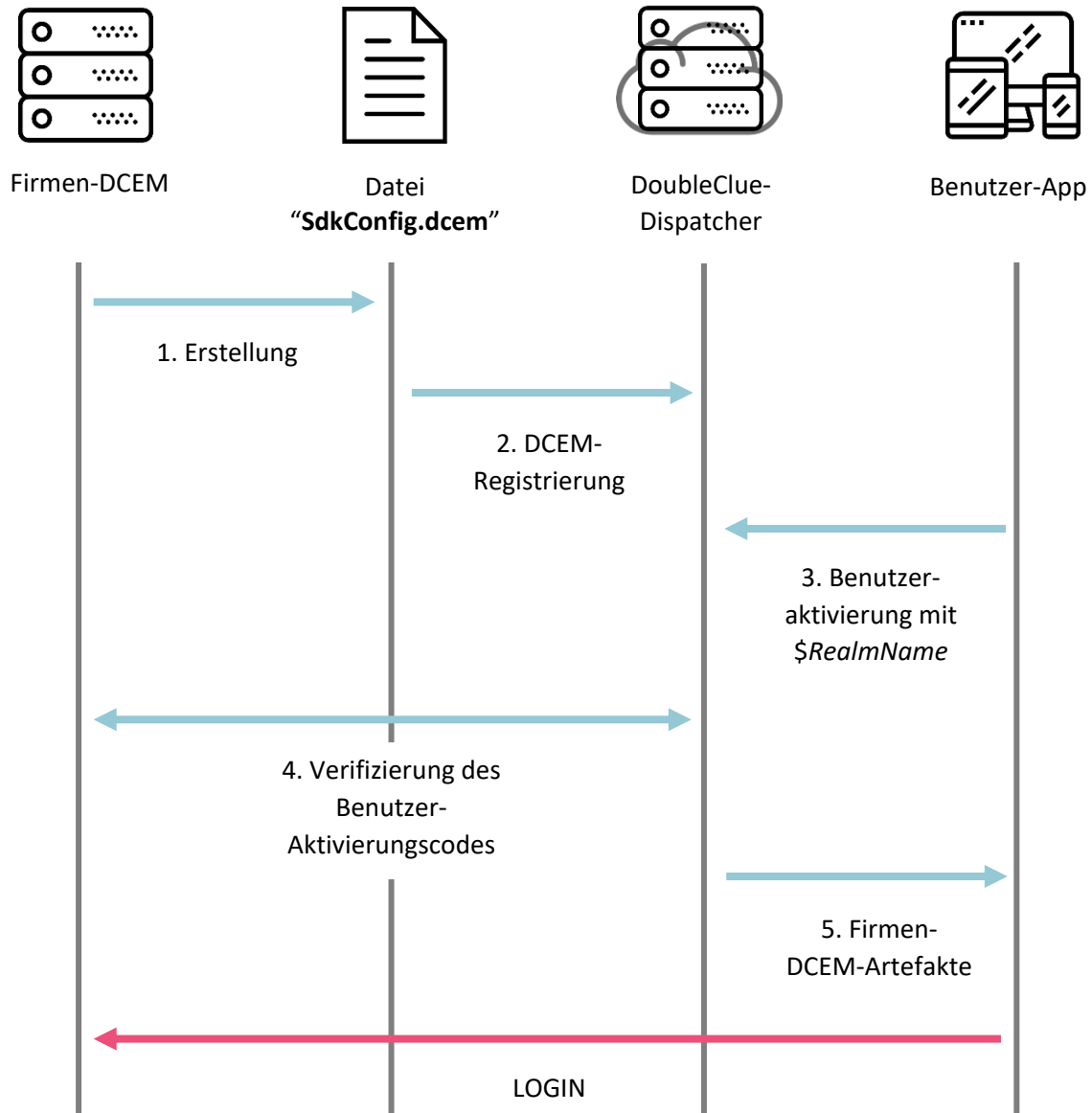
- Es werden keine Cloud-Server oder Server Dritter benötigt. Die Client-App verbindet sich direkt mit der Firmeninstallation von DCEM.
- Die App kann vollständig auf Ihre Bedürfnisse zugeschnitten werden.

Nachteile:

- Es ist nötig, eine eigene App bereitzustellen.
- Die bereitgestellte App kann sich nur mit einer einzigen DCEM-Cluster-Installation verbinden.
- Der DCEM-Web-Sockets-Port muss vom Internet aus erreichbar sein. Dieser Port muss in der Firmen-Firewall geöffnet werden.
- DCEM benötigt eine öffentlich zugängliche URL.

6.1.2 Dispatcher-Verbindung

Die DoubleClue-App kann für alle DCEM-Installationen weltweit verwendet werden, ohne eine eigene App bereitstellen zu müssen. Für diesen Verbindungstyp müssen Sie Ihre DCEM-Installation beim cloud-basierten DoubleClue-Dispatcher registrieren (siehe hierzu Kapitel [6.2.1 Konfiguration des DoubleClue-Dispatchers](#)).



Vorteile:

- Die DoubleClue-App kann für alle DCEM-Installationen weltweit genutzt werden.
- Benutzer können die App direkt von den öffentlichen Cloud-Stores herunterladen.
- Sie müssen keine eigene App bereitstellen.

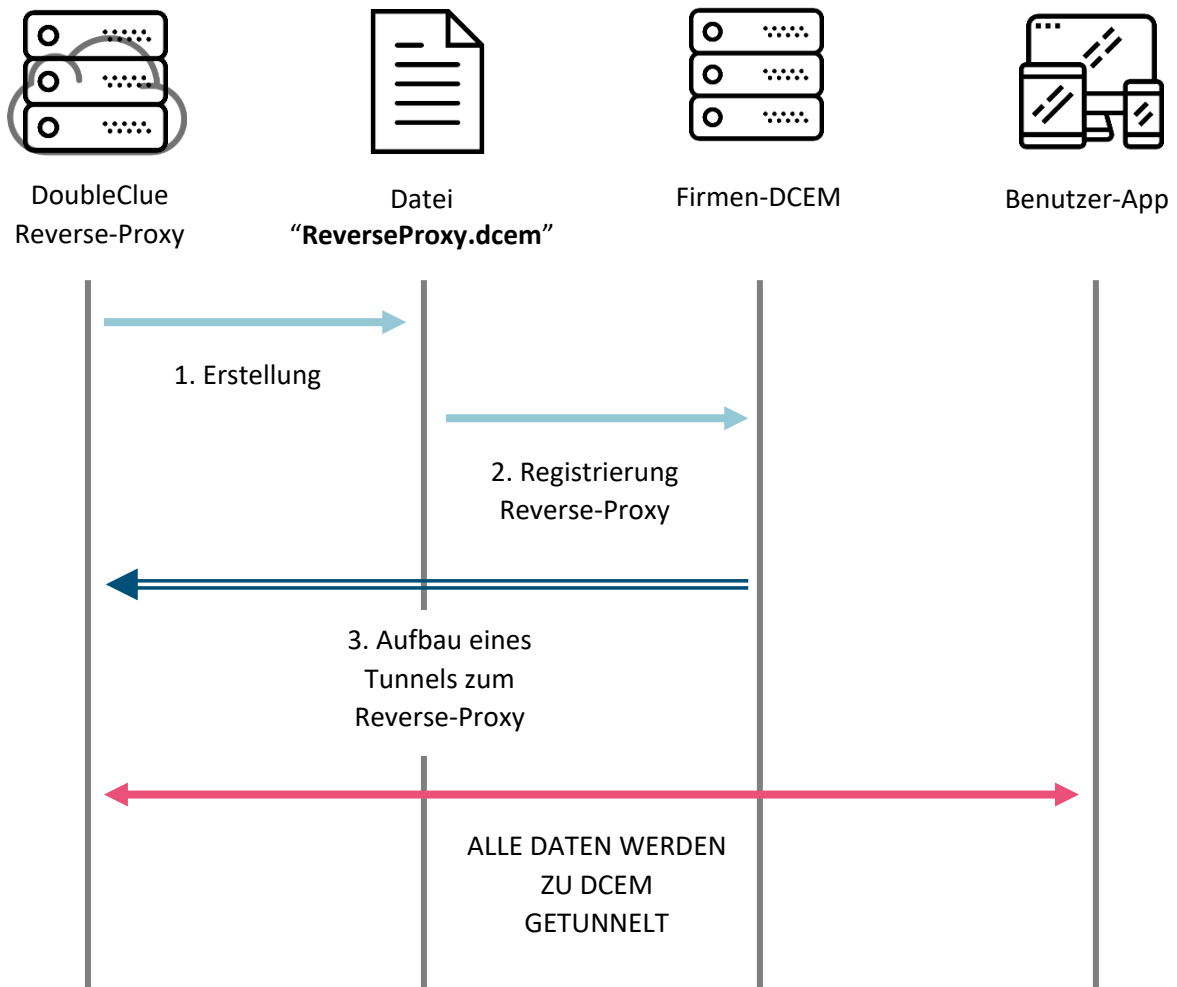
Nachteile:

- Der DCEM-Web-Sockets-Port muss vom Internet aus erreichbar sein. Dieser Port muss in der Firmen-Firewall geöffnet werden.
- DCEM benötigt eine öffentlich zugängliche URL.
- Bei der Geräteaktivierung ist man abhängig vom DoubleClue-Dispatcher-Server.

6.1.3 Reverse-Proxy-Verbindung

⚠ Die Reverse-Proxy-Verbindung sollte NICHT für eine produktive Umgebung verwendet werden!

Die DoubleClue-App kann für alle DCEM-Installationen weltweit verwendet werden, ohne eine eigene App bereitstellen zu müssen. Für diesen Verbindungstyp müssen Sie Ihre DCEM-Installation beim cloud-basierten DoubleClue-Dispatcher registrieren (siehe hierzu Kapitel [6.2.2 Konfiguration von DCEM für Reverse-Proxy](#)).



Vorteile:

- Die DoubleClue-App kann für alle DCEM-Installationen weltweit genutzt werden.
- Benutzer können die App direkt von den öffentlichen Cloud-Stores herunterladen.
- Sie müssen keine eigene App bereitstellen.
- Es ist nicht nötig, die Firmen-Firewall zu öffnen.
- Sie müssen keine öffentlich zugängliche URL haben.

Nachteile:

- Alle Daten werden zwischen dem DoubleClue Reverse-Proxy und DCEM getunnelt.
- Versagt die Tunnelverbindung, schlagen auch alle Client-Verbindungen fehl.

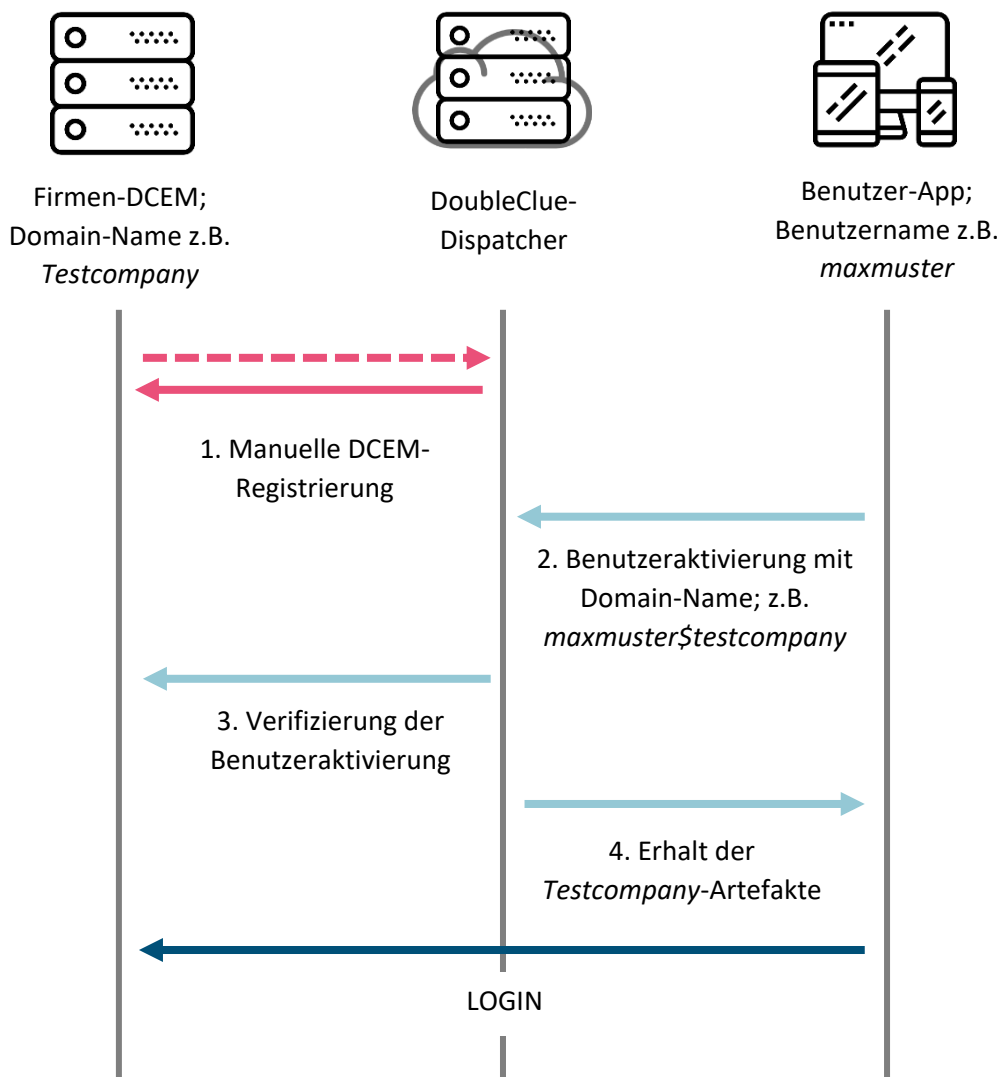
6.2 Konfiguration

6.2.1 Konfiguration des DoubleClue-Dispatchers

Der DoubleClue-Dispatcher ist ein DCEM-Cluster in der Cloud, die von der *HWS Informationssysteme GmbH* verwaltet wird. Bei der Geräteregistrierung verifiziert der Dispatcher Benutzer-Anmeldename und Aktivierungscode mit der Domäne "Dcem-Installation". Ist der Aktivierungscode gültig, sendet der Dispatcher die DCEM-SDK-Konfigurationsdatei zu dem Gerät. Bei erneuter Anmeldung verbindet sich das Gerät dann direkt mit dem firmeneigenen DCEM und baut keine Verbindung in die Cloud mehr auf.

Bitte beachten Sie: Der Dispatcher speichert keine Benutzerdaten wie Aktivierungscodes, Passwörter etc.

6.2.1.1 Datenfluss beim DoubleClue-Dispatcher



6.2.1.2 Registrierung beim DoubleClue-Dispatcher

Wählen Sie einen Domainnamen aus, der benötigt wird, um Ihr DCEM-Cluster gegenüber dem DoubleClue-Dispatcher zu identifizieren. Wir schlagen vor, Ihren Firmennamen als Domain-Namen zu verwenden. Der Domain-Name muss für den Dispatcher einzigartig sein.


Senden Sie den gewählten Namen zusammen mit der Datei **“SdkConfig.dcem”** an support@doubleclue.com, um Ihr DCEM-Cluster beim DoubleClue-Dispatcher zu registrieren.

6.2.2 Konfiguration von DCEM für Reverse-Proxy

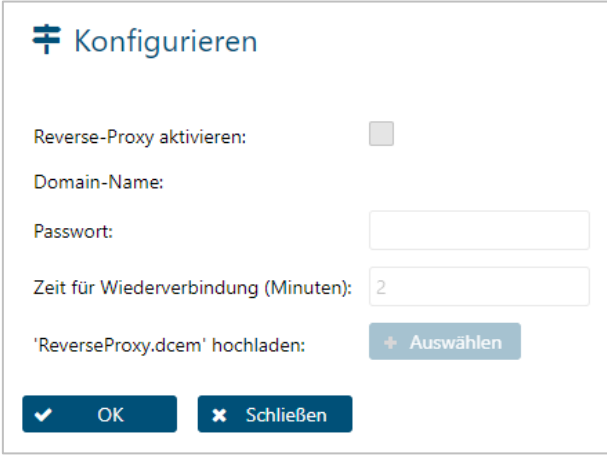
6.2.2.1 Registrierung beim DoubleClue-Dispatcher

Wählen Sie einen Domain-Namen aus, der benötigt wird, um Ihr DCEM-Cluster gegenüber dem DoubleClue-Dispatcher zu identifizieren. Wir schlagen vor, Ihren Firmennamen als Domain-Namen zu verwenden. Der Domain-Name muss für den Dispatcher einzigartig sein.

Senden Sie den gewählten Namen an support@doubleclue.com, um Ihr DCEM-Cluster beim DoubleClue-Dispatcher zu registrieren. Nach der Registrierung werden Sie die Metadaten-Datei **“ReverseProxy.dcem”** und ein geheimes Passwort von Ihrem DCEM-Support-Team erhalten.

 Die Anzahl der gleichzeitigen Sitzungen mit dem DoubleClue-Dispatcher ist standardmäßig auf 10 Sitzungen beschränkt. Wenn Sie mehr simultane Sitzungen benötigen, kontaktieren Sie bitte support@doubleclue.com.

6.2.2.2 Konfigurationsprozess



Gehen Sie zum Hauptmenüpunkt **“Identity-Management”**, Untermenü **“Reverse-Proxy”** und klicken Sie auf den Button **“Konfigurieren”**.

Reverse-Proxy aktivieren:

In diese Box kann ein Häkchen gesetzt werden, wenn Sie Reverse-Proxy aktivieren wollen. Lassen Sie es anderenfalls leer.

Domain-Name:

Dies ist der einzigartige Domain-Name, den Sie gewählt haben, um Ihr DCEM-Cluster gegenüber dem DoubleClue-Dispatcher zu identifizieren.

Passwort:

Tragen Sie das Passwort ein, welches Ihnen vom DoubleClue-Team zugeschickt wurde.

Erneut verbinden in (Minuten):

Hier können Sie das Zeitintervall eintragen, in welchem Ihre DCEM-Installation versucht, sich wieder mit dem DoubleClue Reverse-Proxy zu verbinden, wenn ein Verbindungsversuch fehlschlägt.

„ReverseProxy.dcem“ hochladen:

Laden Sie hier die Datei **“ReverseProxy.dcem”** hoch, welche Ihnen vom DoubleClue-Team zugeschickt wurde.

6.3 Die DoubleClue-App

DoubleClue-Apps für Android und iOS sind im Google Playstore und App Store zu finden. Die DoubleClue-Desktop-App kann von www.doubleclue.com heruntergeladen werden.

Alle DoubleClue-Apps sind fähig, sich mit jedweder DCEM-Clusterfarm eines Unternehmens zu verbinden, wenn dieses DCEM-Cluster vorher beim zentralen DoubleClue-Dispatcher registriert wurde.

Sie müssen nicht Ihre eigene App bereitstellen, um mit Ihrer installierten DCEM-Software zu arbeiten. Benutzer, die schon bei DCEM registriert sind, können einfach die DoubleClue-Apps von den entsprechenden Stores herunterladen und sie direkt mit Ihrem DoubleClue-Account verbinden. Natürlich ist es für Sie immer noch möglich, Ihre eigene App zu erstellen und zu verwenden, wenn es gewünscht ist.

7. Authentifizierungsmethoden und Policies

DoubleClue unterstützt eine Reihe von Authentifizierungsmethoden, Applikationen und Policies, die festlegen, welcher Applikation welche Authentifizierungsmethode zugeordnet wird.

7.1 Authentifizierungsmethoden

DoubleClue unterstützt folgende Authentifizierungsmethoden:

- Push Approval
- QR-Code Approval
- FIDO U2F Token
- OTP Token
- DoubleClue Passcode
- Passwort
- SMS Passcode
- Voice Message

Diese Authentifizierungsmethoden können im Hauptmenü "Identity-Management", Untermenü "Policies" konfiguriert werden.

7.1.1 Push Approval


Dies ist die sicherste Authentifizierungsmethode, welche auf einem PKI Private Key 2048 Bit-Zertifikat basiert. Bei der Authentifizierung erhält der Benutzer eine Push-Benachrichtigung auf sein Mobiltelefon. Nachdem er die DoubleClue-App gestartet und sich angemeldet hat, was optional biometrisch erfolgt, kann er die Push Approval mit seiner App bestätigen oder ablehnen.

Voraussetzungen:

- Der Benutzer muss die DoubleClue-App herunterladen und installieren.
- Die DoubleClue-App muss aktiviert werden.

7.1.2 QR-Code Approval

Diese Authentifizierungsmethode basiert auf einem 32 Bytes AES zufälligen Verschlüsselungs-Schlüssel. Der Benutzer kann sich per Scan eines QR-Codes mit seinem Smart Device authentifizieren.

 Diese Methode steht für RADIUS oder das Microsoft ADFS-Plugin nicht zur Verfügung.

Voraussetzungen:

- Der Benutzer muss die DoubleClue-App herunterladen und installieren.
- Die DoubleClue-App muss aktiviert werden.

7.1.2.1 Ablauf einer Authentifizierung mit QR-Code

Der QR-Code-Login funktioniert wie folgt:

1. Der Endnutzer ruft die Anmeldeseite des UserPortals auf.
2. Das Portal führt über die REST-Web Services-Schnittstelle die Methode "*requestLoginQrCode()*" aus, um von DCEM einen QR-Code zu erhalten.
3. Der Inhalt des QR-Codes wird von DCEM an den Webserver des UserPortals geschickt.
4. Der neu generierte QR-Code wird im UserPortal angezeigt.
5. Der Endnutzer meldet sich in der App an.

6. Der Endnutzer scannt mit der App den QR-Code aus dem UserPortal.
7. Die App sendet den Inhalt des QR-Codes zu DCEM.
8. Ab Schritt 4 führt das Portal über die REST-Web Services-Schnittstelle parallel zu den anderen Schritten die Methode *"queryLoginQrCode()"* aus. Diese Methode fragt in periodischen Zeitabständen bei DCEM an, ob der Inhalt des QR-Codes schon vorliegt.
9. DCEM antwortet mit "OK", wenn der korrekte Inhalt des QR-Codes übermittelt wurde. In diesem Fall werden der Benutzername und der Geräte name an das Portal übermittelt und der Endnutzer in das UserPortal eingeloggt.

Wird ein Fehler zurückgemeldet, wird Schritt 8 wiederholt, bis die Antwort "OK" ist oder die Gültigkeit des Passcodes abgelaufen ist und deshalb vom Portal ein Timeout erfolgt.

7.1.3 FIDO U2F Token

FIDO ist ein offener Standard für Multi-Faktor-Authentifizierung. FIDO Security Keys sind physische Tokens, die sich über die Bluetooth- oder USB-Schnittstelle mit einem Gerät verbinden können. Weitere Informationen finden Sie unter <https://fidoalliance.org/>.

7.1.4 OTP Token

Bei dieser Authentifizierungsmethode identifiziert der Benutzer sich mit einem Passcode, der von einem Hardware Token generiert wird.



Bitte beachten Sie: Momentan unterstützt DCEM den Token-Typ **"TIME_6_SHA1_60"**. Dies ist ein zeitbasiertes OTP mit sechs Ziffern, das einen SHA1-Algorithmus und ein Zeitfenster von 60 Sekunden verwendet.

Wenn RADIUS verwendet wird, muss der Benutzer den Passcode eingeben, gefolgt von einem Schrägstrich und dem Passwort (Beispiel: **"123456/passwort"**).

Voraussetzungen:

- Der DCEM-Server muss mit einer NTP (Network Time Protocol)-Domain zeitsynchronisiert werden.
- Es ist notwendig, Hardware Token zu kaufen. Bitte kontaktieren Sie den DoubleClue-Vertrieb unter sales@doubleclue.com.
- Von Ihrem DoubleClue-Vertriebskontakt erhalten Sie ebenfalls die sichere Hardware-Token-Datei sowie einen Entschlüsselungsschlüssel.

Importieren Sie die OTP Token-Datei und geben Sie den Entschlüsselungsschlüssel unter Hauptmenüpunkt "OTP-Tokens", Untermenü "OTP-Token".

Tokens können über DCEM den einzelnen Benutzern zugewiesen werden oder die Benutzer können sie über das UserPortal selbst hinzufügen.

Unter dem Hauptmenüpunkt "OTP-Tokens", Untermenü "Einstellungen", können Sie ein "Zeitverzögerungsfenster" konfigurieren. Dies ist die Anzahl an 60-Sekunden-Zeitfenstern, die DCEM zurückgeht, um das OTP zu verifizieren.

7.1.5 DoubleClue Passcode

Die Anmeldung mit einem DoubleClue Passcode kann im Offlinemodus durchgeführt werden.

Diese Variante wird benötigt, wenn der Benutzer auf dem Gerät mit der App keine Internetverbindung hat und er sich gegenüber dem Server authentifizieren will. Der Benutzer muss dazu nicht in der App eingeloggt sein.

Für diese Authentifizierungsmethode wird die DoubleClue-App verwendet. Ein Benutzer muss im App-Menü auf "Offline Login" klicken, um einen Passcode zu generieren.

Voraussetzungen:

- Der Benutzer muss die DoubleClue-App herunterladen und installieren.
- Die DoubleClue-App muss aktiviert werden.

7.1.5.1 Gültigkeitsdauer des Passcodes

Die zur Verfügung stehende Antwortzeit kann in den Einstellungen des Identity-Managements unter "Login QR-Code Antwortzeit" festgelegt werden. Die Rechnerzeit von DCEM und der App des Endnutzers müssen synchron laufen, sonst kann es passieren, dass die Zeit abgelaufen ist, bevor der Endnutzer tätig werden konnte.

7.1.6 Passwort

Ein Benutzer identifiziert sich mit seinem Anmeldenamen und Passwort. Ist der Benutzer ein Domain-Benutzer, wird das Passwort direkt von der Domäne validiert und das Passwort des Benutzers wird nicht in der DCEM-Datenbank gespeichert.

7.1.7 SMS / Voice Message

Bei dieser Authentifizierungsmethode erstellt DCEM einen zufälligen Passcode, der per SMS an das Mobiltelefon des Benutzers gesendet wird, oder es werden die Festnetznummer oder Handynummer des Benutzers angerufen. Der Passcode ist für einen bestimmten Zeitraum in Minuten gültig, welcher im Hauptmenü "Identity-Management", Untermenü "Einstellungen" ("Passcode gültig bis") eingestellt werden kann.

Voraussetzungen:

- Sie müssen SMS-Credits von www.messagebird.com kaufen.
- Konfigurieren Sie den "Zugriffsschlüssel SMS-Provider" im Hauptmenü "System", Untermenü "Einstellungen".
- Um SMS versenden zu können, muss für den Benutzer ein Mobiltelefon konfiguriert sein.
- Um Voice Messages zu erhalten, müssen entweder eine Festnetznummer oder eine Handynummer für den Benutzer angelegt sein.



Bitte beachten Sie, dass SMS und Voice Message nicht in verschlüsselter Form über die Leitungen versendet werden.

7.2 Policies und Anwendungen

Im Hauptmenüpunkt "Identity-Management", Untermenü "Policies", bietet DCEM die Möglichkeit, Benutzergruppen verschiedene Policies zuzuweisen. Über die Policies können Sie festlegen, welche Authentifizierungsmethoden den verschiedenen Benutzern zur Verfügung stehen.

7.2.1 Policies hinzufügen und konfigurieren

Über die Policies können Sie die Zugriffsrechte bestimmter Benutzergruppen für verschiedene DoubleClue Anwendungstypen und die damit verbundenen Anwendungen einstellen.

In den Policies haben Sie die folgenden Einstellungsmöglichkeiten:

Zugriff verweigern:

Wenn Sie in dieser Box einen Haken setzen, wird allen entsprechenden Benutzern der Zugriff komplett verweigert.

Sie können zwischen den folgenden drei Optionen wählen (die Auswahl einer Option schließt die anderen beiden aus):

MFA innerhalb Timeout unterdrücken:

Innerhalb eines voreingestellten Zeitraums kann sich ein Benutzer mit Anmeldename / Passwort anmelden, nachdem er sich einmal per MFA authentifiziert hat.

Browser-Fingerprint merken:

Diese Einstellung wird verwendet, um jedwede MFA zu umgehen, wenn der Benutzer denselben Browser wie während seiner letzten erfolgreichen Anmeldung verwendet. Produziert der Browser den gleichen Fingerabdruck, reicht es für den Benutzer aus, für die Authentifizierung innerhalb eines bestimmten Zeitraums nur seinen Anmeldnamen und sein Passwort zu verwenden.



Dieses Feature steht nur für SAML-, OpenID-OAuth-, DCEM, UserPortal und REST-Web Services-Applikationen zur Verfügung, wenn sie über einen Browser aufgerufen werden.

Session-Authentifizierung:

Nachdem sich ein Benutzer erfolgreich per MFA angemeldet hat, gibt DCEM einen Session-Cookie zurück. Dieser 32 Byte zufällige Schlüssel ist innerhalb eines voreingestellten Zeitraums gültig. Ein Benutzer kann sich so unter Verwendung des Session-Cookies mittels eines sog. „Silent Logins“ anmelden.


Weitere Einstellungen:

Timeout (Stunden):

Hier können Sie die Zeitdauer in Stunden einstellen, während derer jedwede MFA umgangen wird, wenn eine der obigen drei Optionen ausgewählt wurde.

Network-Bypass:

Diese Einstellung wird verwendet, um jedwede MFA zu umgehen, wenn die Quell-IP-Adresse des Benutzers innerhalb einer der eingegebenen IP-Bereiche liegt.

 Dieses Feature steht nur für SAML-, OpenID-OAuth-, DCEM, UserPortal und REST-Web Services-Applikationen zur Verfügung, wenn sie über einen Browser aufgerufen werden.

Auth-Methoden erlauben:

Wählen Sie die Authentifizierungsmethode(n), welche eine bestimmte Benutzergruppe verwenden darf.

7.2.2 Anwendungstypen

DoubleClue unterstützt die folgenden Anwendungstypen:

- Auth-Connector (z.B. DoubleClue Windows Login)
- DCEM
- OpenID-OAuth
- REST-Web Services
- RADIUS
- SAML
- UserPortal

Für jeden Anwendungstypen können mehrere Anwendungen konfiguriert werden.

7.2.3 Zuweisung von Policies

Policies können Anwendungstypen (z.B. Auth-Connector, RADIUS, DCEM, SAML, Web-Services), Anwendungen (z.B. Cisco Meraki, Citrix ShareFile, Dropbox etc.) und Benutzergruppen zugewiesen werden.

Unter den zugewiesenen Policies wählt DCEM die Policy, die zur Anwendung kommt, wie folgt aus:

- a) Wird eine Policy einer Benutzergruppe für einen gewissen Dienst zugewiesen, so gilt sie für jedes Mitglied der Gruppe.

- b) Ist ein Benutzer ein Mitglied in mehreren Gruppen, denen verschiedene Policies zugewiesen wurden, wird die Policy derjenigen Gruppe verwendet, welche die höchste Priorität hat. Die Gruppenpriorität kann der entsprechenden Gruppe direkt mit der Zuordnung zu einer Policy zugewiesen werden.
- c) Ist einer Anwendung für eine bestimmte Benutzergruppe keine Policy zugewiesen, so greifen die Richtlinien des entsprechenden Anwendungstypen.
- d) Wurden einer Benutzergruppe weder für die Anwendung noch für den Anwendungstypen eine Policy zugewiesen, dann gilt die „Global-Policy“.

7.2.4 Auswahl einer Authentifizierungsmethode

Wenn die zugewiesene Policy eines Benutzers nur eine Authentifizierungsmethode beinhaltet, verwendet DCEM diese Authentifizierungsmethode.

Lässt eine Policy mehrere Authentifizierungsmethoden zu, werden die folgenden Auswahlmethoden angewendet:

Standard Auth-Methode:

Sie können in den Policies eine Standard Auth-Methode anlegen. Diese wird daraufhin allen zugewiesenen Benutzern als erste angezeigt. Sie können jedoch manuell während der Anmeldung eine andere Methode auswählen, wenn diese in der Policy für sie erlaubt ist. Es kann sein, dass einige Anwendungstypen oder Anwendungen die Auswahl einer Standard Auth-Methode nicht übernehmen. Die Auswahl der Methode muss dann per Vorauswahl oder hinterher erfolgen.

Vorauswahl:

Die verschiedenen Anwendungstypen erfordern möglicherweise eine Vorauswahl der verfügbaren Authentifizierungsmethoden vor der eigentlichen Benutzerauthentifizierung. Dies bietet dem Benutzer die Möglichkeit, vor der Authentifizierung seine bevorzugte Authentifizierungsmethode auszuwählen.

Die Vorauswahl kann mittels Anwendungs-GUI, z.B. einer Dropdown-Auswahlbox, getroffen werden. Falls dies nicht möglich ist, z.B. im Falle von RADIUS, kann ein Benutzer die Authentifizierungsmethode mittels eines Präfixes, das getrennt durch ein Hash-Zeichen “#” zum Benutzer-Anmeldenamen hinzugefügt wird, auswählen. Das Präfix ist eine Abkürzung der Authentifizierungsmethode.

Verfügbare Präfixe sind:

- pwd = Passwort
- sms = SMS Passcode
- voice = Voice Message
- otp = OTP Token
- motp = DoubleClue Passcode
- push = Push Approval
- fido = FIDO U2F Token

Beispiel: Möchte ein Benutzer ein Hardware Token verwenden, muss er “**otp#max.muster**” eingeben.

Auswahl hinterher:


Hat sich ein Benutzer erfolgreich per Passwort authentifiziert, ohne zuvor eine Authentifizierungsmethode ausgewählt zu haben, wird eine Liste möglicher Authentifizierungsmethoden zurückgegeben, welche DCEM in der zugewiesenen Policy gefunden hat.

 Dieser Auswahltyp steht für RADIUS-Schnittstellen nicht zur Verfügung.

8. Identity-Management

8.1 Aktivierungscodes

Unter Aktivierungscodes können Sie Benutzern via E-Mail oder SMS einen Aktivierungscode für ihre DoubleClue App zukommen lassen. Außerdem werden in diesem Untermenü sämtliche versandten Aktivierungscodes protokolliert und können nachträglich überarbeitet werden.

 Bitte beachten Sie, dass Sie zunächst unter „System“ > „Einstellungen“ E-Mail und SMS konfigurieren müssen, um die Aktivierungscodes zu versenden.

Die Möglichkeit, einen Aktivierungscode an eine ganze Gruppe zu verschicken, finden Sie unter „Administration“ > „Gruppe“.

8.2 Smart Devices

Hier finden Sie eine Liste der Smart Devices, die per App mit dieser DCEM-Installation verbunden wurden. Ein Benutzer kann mehrere Smart Devices mit seinem Account verbinden.

Wenn Sie in das DCEM eines Sub-Mandanten eingeloggt sind, sehen Sie nur die zu diesem Sub-Mandanten gehörenden Smart Devices.

8.2.1 Gesperrtes Smart Device

Es gibt drei Möglichkeiten ein Smart Device zu sperren. Ein Administrator kann ein Smart Device in DCEM unter „Identity Management“ – „Smart Devices“ sperren, ein Benutzer kann sein eigenes Smart Device in UserPortal unter Gerätemanager sperren und ein Smart Device wird automatisch gesperrt, wenn auf diesem Gerät beim Versuch sich über App einzuloggen das Passwort zu oft falsch eingegeben wurde. Wie viele Versuche ein Benutzer hat, um sich erfolgreich anzumelden, können Sie unter „Identity-Management“ > „Einstellungen“ einstellen.

Besitzt ein Benutzer gleichzeitig mehrere aktivierte Smart Devices, gilt für jedes Gerät dasselbe Passwort. Gibt er auf einem Gerät das Passwort mehrmals falsch ein, wird nur dieses Smart Device gesperrt. Über die anderen aktivierten Smart Devices kann er sich weiterhin einloggen.

Ein gesperrtes Smart Device kann vom Benutzer über UserPortal oder von einem Administrator über DCEM entsperrt werden.

8.2.2 Smart Device löschen

Gelöschte Smart Device werden als gelöscht markiert. Sie sind weiterhin in der Datenbank zu finden. Ausnahme: Siehe Kapitel [8.8 Einstellungen](#).

8.3 FIDO-Authentifikatoren

Unter diesem Menüpunkt werden die mit dieser DoubleClue-Infrastruktur verbundenen FIDO-Authentifikatoren angezeigt. Wer über eine Subdomain bei DCEM angemeldet ist, sieht nur die FIDO-Authentifikatoren, die für diesen Mandanten registriert wurden.

Administratoren können in diesem Menü Authentifikatoren für Benutzer hinzufügen und löschen.

8.4 CloudSafe

CloudSafe ist ein Cloud-Speicher, in dem Daten und Dokumente mit DoubleClue MFA gespeichert werden können. CloudSafe ist über UserPortal erreichbar.

In DCEM können Administratoren den verfügbaren Speicherplatz für jeden Benutzer einstellen und finden eine Übersicht über die in CloudSafe gespeicherten Dateien.

8.4.1 CloudSafe License und Verteilung des Speicherplatzes an die Benutzer

Unter den „Einstellungen“ im „Identify Management“-Untermenü ist es möglich, ein Standardlimit für den CloudSafe-Speicher für die einzelnen Benutzer festzulegen. Dieses Standardlimit legt fest, wieviel Speicherplatz einem einzelnen Benutzer zur Verfügung steht. Es ist auch möglich einzustellen, ob PasswordSafe standardmäßig aktiviert oder deaktiviert werden soll.

Im „CloudSafe“-Eintrag im „Identity Management“-Menü können Administratoren außerdem den verfügbaren Speicher für jeden einzelnen Benutzer individuell einstellen.



Sollte der allgemeine Speicherplatz der Lizenz komplett ausgenutzt sein, können die Benutzer keine weiteren Dokumente hochladen, selbst wenn von dem ihnen zugeteilten Maximum-Speicherplatz noch etwas übrig ist.

Wenn Sie Änderungen an Ihrer CloudSafe-Lizenz möchten, kontaktieren Sie sales@doubleclue.com.



Hat ein Benutzer bereits Dateien in seinen CloudSafe hochgeladen, kann nicht nachträglich ein Limit für diesen Benutzer gesetzt werden, das kleiner als die Größe der hochgeladenen Dateien

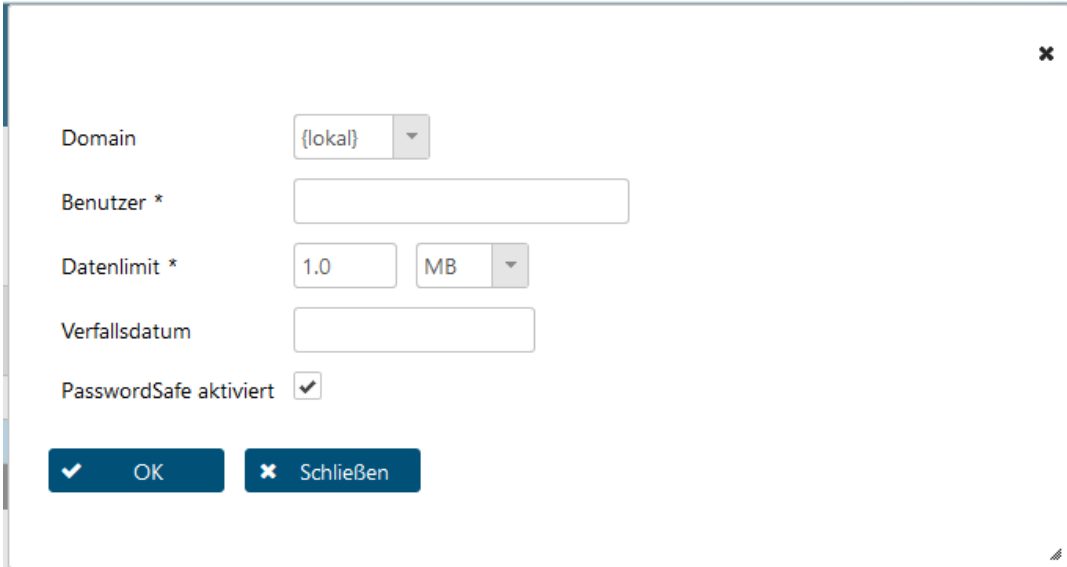
ist. Es wird daher empfohlen, Speicherplatzlimits einzurichten, bevor die Benutzer Zugriff auf CloudSafe erhalten.

8.4.1.1 Festlegung eines Standardlimits für jeden Benutzer

Im Bereich „Identity Management“ kann unter „Einstellungen“ ein Standardlimit für den CloudSafe-Speicherplatz eingestellt werden. Dieses Standardlimit legt fest, wie viel Speicherplatz in CloudSafe ein User maximal verwenden kann. Hier kann auch eingestellt werden, ob PasswordSafe standardmäßig aktiviert oder deaktiviert sein soll.

8.4.1.2 Individuelle Speicherplatzlimit für Benutzer festlegen

Im „Identity Management“-Untermenü unter CloudSafe kann ein Administrator einzelnen Benutzern mehr oder weniger Speicherplatz zuweisen. Dafür wird einfach der entsprechende Benutzer aus der Liste ausgewählt und seine Einstellungen entsprechend bearbeitet.

The image shows a dialog box for configuring user settings. It has a title bar with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Domain:** A dropdown menu currently showing "{lokal}" with a downward arrow.
- Benutzer *:** A text input field.
- Datenlimit *:** A text input field containing "1.0", followed by a unit dropdown menu showing "MB".
- Verfallsdatum:** A text input field.
- PasswordSafe aktiviert:** A checkbox that is currently checked.
- Buttons:** At the bottom, there are two buttons: "OK" with a checkmark icon and "Schließen" with an X icon.

In diesem Fenster können Administratoren auch einstellen, ob Sie PasswordSafe für einen bestimmten Benutzer aktivieren oder deaktivieren möchten und ob die individuellen Einstellungen für einen Benutzer ein Verfallsdatum haben, an dem sie automatisch zurückgesetzt werden. Individuelle Einstellungen für einen Benutzer überschreiben die Standardeinstellungen.

Benutzer erscheinen automatisch in der Liste, sobald sie eine Datei hochgeladen haben. Möchte man die Einstellungen für einen Benutzer bearbeiten, der noch keine Datei hochgeladen hat, kann der Benutzer über den „Hinzufügen“-Button manuell hinzugefügt werden.

8.4.2 Dateiinformation

Administratoren können in DCEM eine Übersicht über die Dateien im Cloud Safe aufrufen. Sie können die Dateien jedoch nicht öffnen, löschen oder verändern. Im Normalfall hat nur der Benutzer, der die

Datei hochgeladen hat, Zugriff auf die Datei. Der Benutzer kann die Dateien in seinem CloudSafe jedoch mit anderen Benutzern teilen und ihnen auch das Recht geben, die Dateien zu verändern.

Ein Administrator kann die Dateiliste eines Benutzers einsehen, indem er den Benutzer in der CloudSafe-Liste auswählt und auf „Zeige Dateien“ klickt.

8.4.3 Dateien mit individuellem Passwort

Benutzer haben die Möglichkeit, einzelne Dateien in ihrem CloudSafe mit einem individuellen Passwort zu schützen. Wenn der Benutzer die Datei öffnen möchte, muss er, nachdem er sich über DoubleClue identifiziert hat, zusätzlich dieses Passwort eingeben.



Achtung: Der Schutz einzelner Dateien mit einem zusätzlichen Passwort (PWD) wird nur für höchst vertrauliche Dateien empfohlen. Das zusätzliche Datei-Passwort kann nicht zurückgesetzt werden. Wenn der Besitzer es verliert, kann der Zugriff auf die Datei nicht wiederhergestellt werden. Möchte der Benutzer diese Datei mit anderen Benutzern teilen, muss er ihnen das Passwort mitteilen, damit sie die Datei öffnen können.

8.5 Push Approval

Push Approval ist eine Authentifizierungsmethode, die von allen Anwendungen die DoubleClue unterstützt an die DoubleClue-App geschickt werden kann. Die Rückmeldung kann bei Bedarf digital signiert werden.

8.5.1 Eigenschaften einer Push Approval

Bei den meisten Anwendungen sind die Eigenschaften der Push Approvals festgelegt. Für REST-Anwendungen können Sie die Eigenschaften wie folgt festlegen:

8.5.1.1 *Vorlagenname*

Diverse Standard-Vorlagen sind bei der Installation enthalten. Ist keine passende Vorlage vorhanden, können Sie wie in Kapitel [4.7 Vorlagen](#) beschrieben die gewünschte Vorlage neu erstellen.

Die Sprache der Vorlage wird abhängig vom Benutzer oder Gerät gewählt, für den die Push Approval bestimmt ist.

8.5.1.2 *Anmeldename des Benutzers*

Jede Push Approval muss einem festen Empfänger zugeordnet werden. Dafür wird der Anmeldename des Benutzers übergeben.

8.5.1.3 *Gerätename*

Soll die Push Approval nur an ein bestimmtes Gerät des Benutzers geschickt werden, muss zusätzlich der Gerätename übergeben werden.

Wird kein Gerätename übergeben, wird die Push Approval wie folgt verschickt:

Mehrere Geräte aktiv: (aktiv = eingeloggt in der App)

Sind mehrere Geräte eines Benutzers gleichzeitig aktiv, wird die Push Approval an das Gerät geschickt, welches als Letztes aktiviert wurde.

Ein Gerät aktiv:

Ist nur ein Gerät eines Benutzers aktiv, wird die Push Approval an dieses Gerät geschickt.

Kein Gerät aktiv:

Ist kein Gerät eines Benutzers aktiv, wird eine Push-Benachrichtigung an alle seine Geräte geschickt, wenn in den Einstellungen zum "Identity-Management" Push-Benachrichtigungen erlaubt sind (siehe hierzu auch Kapitel [8.4 Push-Benachrichtigung](#)).

8.5.1.4 *Erforderlichkeit einer Antwort*

Ist für eine Push Approval keine Antwort erforderlich, gibt es keine Garantie, dass der Empfänger die Nachricht erhalten hat. Um dies zu verhindern, kann festgelegt werden, dass eine Antwort erforderlich ist. Ist eine Antwort erforderlich, müssen auch Angaben zur Antwortzeit (in Sekunden) und Signatur gemacht werden.

8.5.1.5 *Antwortzeit (in Sekunden)*

Die Antwortzeit gibt an, wie lange der Benutzer Zeit hat, auf die Push Approval zu reagieren. Ist sie abgelaufen, gibt es einen Timeout-Fehler (siehe Kapitel [8.5.4 Status von Push Approval](#)).

Wenn keine Antwort erforderlich ist, muss keine Antwortzeit eingetragen werden.

Es gibt folgende Möglichkeiten, eine Antwortzeit festzulegen:

- Antwortzeit für die zu sendende Push Approval:

Beim Senden der Push Approval kann eine Antwortzeit festgelegt werden, die nur für diese Message gültig ist.

Voreingestellt ist hier der Wert "0". In diesem Fall wird die "Antwortzeit für Meldungen" aus dem Untermenü "Einstellungen" im Hauptmenü "Identity-Management" übernommen.

- Generelle Antwortzeit festlegen:

Hauptmenü "Identity-Management", Untermenü "Einstellungen":

Diese Einstellung ist für alle Push Approvals gültig. Die Antwortzeit aus den Einstellungen wird immer dann verwendet, wenn die Antwortzeit für die direkt zu sendende Message auf "0" gesetzt ist.

8.5.1.6 *Erforderlichkeit einer Signatur*

Die Antwort der gesendeten Push Approval kann bei Bedarf mit dem Benutzerzertifikat des Gerätes signiert werden. Dieses wird bei der Aktivierung des Gerätes auf DCEM automatisch erstellt.

Es wird mehr Rechenleistung benötigt, wenn die Push Approval signiert werden soll.

8.5.1.7 *Aktions-IDs für Buttons*

Eine Vorlage für eine Push Approval muss immer mindestens einen Button zur Reaktion auf die Message haben. Durch die Aktions-ID kann zugeordnet werden, welche Aktion (d. h. welchen Button) der Benutzer gedrückt hat. Der ID-Name muss eindeutig sein.

Eine Aktions-ID im HTML-Format können Sie wie folgt in Ihrer Vorlage definieren:

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

`<button > </button>` = HTML-Format für einen Button

`id="ID-Name"` = Aktions-ID

`Buttonname` = Anzeigetext für den Button

8.5.1.8 *DataMap*

Eine Vorlage kann Token enthalten. Der Inhalt dieser Token wird als "DataMap" bezeichnet. Das Token wird durch den Dateninhalt der dazugehörigen DataMap ersetzt und in dieser Form an den Benutzer geschickt. Eine DataMap besteht immer aus Key-Value-Paaren:

Key = Der Key entspricht dem Token in der Vorlage.

Value = Der Value des Keys wird durch den Inhalt der Token ersetzt.

8.5.1.9 InputMap

Vorlagen können Eingabefelder enthalten. Eine InputMap ist der Inhalt dieser Felder. Sie besteht immer aus Key-Value-Paaren:

Key = Der Key entspricht der ID des Eingabefeldes.

Value = Der Value des Keys ist der Inhalt, den der Benutzer eingegeben hat.

Ein Eingabefeld wird im HTML-Format wie folgt eingefügt:

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

<input>	=	Eingabefeld
type = "text"	=	Typ "Textfeld"
id="ID-Name"	=	ID des Eingabefelds
value=""	=	Eingabewert des Benutzers

8.5.1.10 Status

Siehe Kapitel [8.5.4 Status von Push Approval](#).

8.5.2 Einstellungen für Push Approvals

Folgende Einstellungen müssen im Menü "Identity-Management", Untermenü "Einstellungen" getroffen werden:

8.5.2.1 Antwortzeit für Push Approvals

Siehe Kapitel [8.5.1.5 Antwortzeit \(in Sekunden\)](#).

8.5.2.2 Policy zur Push Approval-Speicherung

Auswahl, ob der Inhalt der MapData oder der InputData in der Datenbank gespeichert werden soll. Die gespeicherten Daten können unter dem Hauptmenüpunkt "Identity-Management", Untermenü "Meldungen" mit dem Button "Details der Meldung anzeigen" eingesehen werden.

Dabei steht zur Wahl:

1) Weder MapData noch InputData sollen gespeichert werden:

Getroffene Einstellung: **"none"**
 Anzeige in "Details der Meldung anzeigen": keine Anzeige

2) Die gesendeten MapData sollen gespeichert werden:

Getroffene Einstellung: **"to_device"**
 Anzeige in "Details der Meldung anzeigen": **"Send Data:"**

3) Die empfangenen InputData sollen gespeichert werden:

Getroffene Einstellung: **"from_device"**
 Anzeige in "Details der Meldung anzeigen": **"Received Data:"**

4) Sowohl MapData als auch InputData sollen gespeichert werden:

Getroffene Einstellung: **"both"**
 Anzeige in "Details der Meldung anzeigen": **"Send Data:"**
"Received Data:"

8.5.2.3 *Timeout für Push Approval-Abruf*

Dauer, wie lange eine Push Approval vom Portal abgerufen werden kann, nachdem sie den finalen Status erhalten hat. Ist diese Zeit abgelaufen, kann die Message nicht mehr abgeholt werden.

8.5.3 Senden von Push Approvals über REST-Web Services

Ausführliche Informationen zur REST-Web Services-Schnittstelle finden Sie in folgendem HTML-Dokument:

<DcemDistribution/artifacts/yajsw/doc/REST-WebServices/index.html>

Diese Push Approvals sind asynchron. Das bedeutet, dass die Message noch nicht erledigt ist, sobald eine Rückmeldung dazu erfolgt ist. Erst wenn der Status der Message final ist, ist sie erledigt.

Wenden Sie folgende Methoden an, um Push Approvals über REST-Web Services verschicken zu können:

8.5.3.1 *"addMessage()"*

Um eine Push Approval vom Portal zum Server zu senden, muss die Methode "addMessage()" aufgerufen werden. Als Rückmeldung gibt der Server dem Portal die dazugehörige Message-ID.

8.5.3.2 *"getMessageResponse()"*

Das Portal muss in bestimmten Zeitabständen anfragen, ob ihm Antworten vorliegen. Die Zeitabstände sollten nicht unter einer Sekunde liegen (unsere Empfehlung: 2,0 Sekunden). Benutzen Sie dazu die Methode "getMessageResponse()". Die Abfrage wird solange wiederholt, bis ein finaler Status gemeldet wird (siehe hierzu Kapitel [8.5.4.3 Schaubild zum Status einer Transaction Message](#)). Die Antwort erhält die gleiche ID wie die Anfrage und kann dadurch korrekt zugeordnet werden.

8.5.3.3 *"cancelUserMessage()"*

Die Push Approval kann mit dieser Methode abgebrochen werden, solange sie den Status "queued" besitzt.

8.5.4 Status von Push Approvals

Siehe hierzu auch Kapitel [8.5.4.3 Schaubild zum Status einer Transaction Message](#).

8.5.4.1 *Status von offenen Push Approvals*

Push Approvals können folgenden nicht-finalen Status haben:

Queued:

Die Push Approval wurde vom Portal an den Server geschickt. Sie wurde noch nicht an den Endnutzer weitergeleitet, da sie noch intern in der Warteschleife ist.

Sending:

Die Push Approval wird im Moment vom Server zum Endnutzer geschickt.

Waiting:

Die Push Approval wurde erfolgreich an den Endnutzer geschickt. Es ist allerdings noch keine Antwort zurückgekommen.

8.5.4.2 *Finaler Status von Push Approvals*

Push Approvals können folgenden finalen Status haben:

Ok:

Die Push Approval wurde vom Endnutzer bestätigt. Dabei ist es nicht wesentlich, welche Aktion er ausgeführt hat.

Rec_Error:

Der Endnutzer hat die Push Approval bekommen, kann aber aus technischen Gründen nicht auf sie antworten. Dieser Fehler wird direkt aus der App-SDK-Library gemeldet.

Send_Error:

Beim Senden der Push Approval an den Endnutzer ist ein Fehler aufgetreten. Sie konnte nicht gesendet werden.

Disconnected:

Die Verbindung vom Server zum Endnutzer wurde unterbrochen. Der Vorgang muss wiederholt werden.

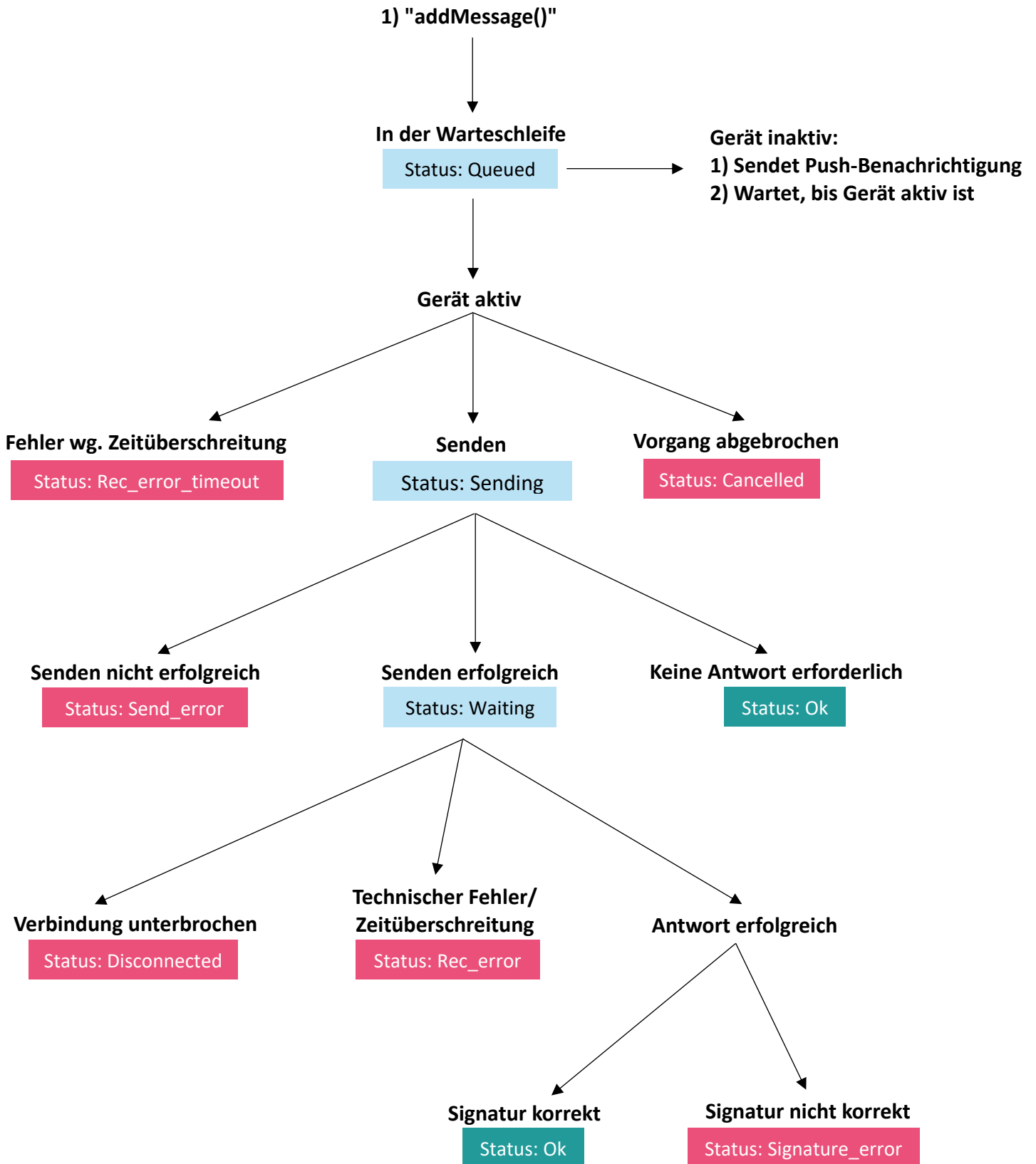
Cancelled:

Der Vorgang wurde von der REST-Web Services-Schnittstelle abgebrochen.

Signature_Error:

Die Antwort vom Endnutzer zum Server wurde erfolgreich erhalten, die Signatur ist allerdings fehlerhaft.

8.5.4.3 Schaubild zum Status einer Push Approval



8.5.5 Lebenszyklus einer Push Approval

8.5.5.1 Offene Push Approvals

Eine Push Approval kann über die REST-Web Services-Schnittstelle oder die Management-GUI erstellt werden. Neue Meldungen sind immer als offen gekennzeichnet und befinden sich im Hauptmenü "Identity-Management", Untermenü "Offene Meldungen".

8.5.5.2 Geschlossene Push Approvals

Offene Push Approvals werden unter folgenden Voraussetzungen geschlossen:

- 1) Eine Push Approval, auf die keine Antwort erwartet wird, wird nach dem Senden geschlossen.
- 2) Eine Push Approval, auf die eine Antwort erwartet wird, wird geschlossen, wenn die Antwort darauf vom Portal abgeholt wurde oder ihre Abholzeit abgelaufen ist ("Timeout für Push Approval-Abruf").

Geschlossene Push Approvals befinden sich im Hauptmenü "Identity-Management", Untermenü "Push Approvals".

8.6 Konfiguration für Push-Benachrichtigungen

Damit Ihre Benutzer Push-Benachrichtigungen erhalten, wenn eine neue Push Approval für Sie eingetroffen ist, nehmen Sie im Hauptmenüpunkt "Identity-Management", Untermenü "Einstellungen", Bereich „Konfiguration für Push-Benachrichtigungen“ die folgenden Einstellungen vor:

Aktiviere Push-Benachrichtigungen:

Diese Checkbox muss aktiviert sein, wenn Sie Push-Benachrichtigungen zur App verschicken möchten.

Wenn Sie die DoubleClue-App in Kombination mit dem DoubleClue-Dispatcher verwenden, müssen Sie keine Firebase-Cloud Messaging-URL konfigurieren. Push-Benachrichtigungen werden automatisch eingesetzt.

Falls Sie Ihre eigene App verwenden möchten, gehen Sie wie folgt vor:

Firebase-Cloud Messaging-URL:

Die FCM-URL lautet standardmäßig: **<https://fcm.googleapis.com/fcm/send>**

Um eine FCM-URL zu erhalten, müssen Sie bei Google registriert sein.

Firebase-Cloud Messaging-Schlüssel:

Den FCM-Key finden Sie in Ihrem Google-Projekt.



Bitte beachten Sie: Wird ein Firebase-Cloud Messaging-Schlüssel verwendet, müssen Sie Ihre eigene App erstellen. Lassen Sie dieses Feld leer, wenn Sie die DoubleClue-App in Kombination mit dem DoubleClue-Dispatcher nutzen möchten.

Ausführliche Informationen zur Firebase finden Sie hier:

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

8.7 Versionen

Jede App hat eine Versionsnummer.

Die App-Version und den App-Namen erhalten Sie von Ihrer App-Entwicklungsabteilung.

Um die jeweilige Version der App verwenden zu können, fügen Sie diese unter dem Hauptmenüpunkt "Identity-Management", Untermenü "Versionen" hinzu.

Um die Version zu aktivieren, muss sie von mindestens einem Benutzer genutzt werden.

Soll die Version nur bis zu einem bestimmten Zeitpunkt genutzt werden, kann ein Ablaufdatum festgelegt werden. Es erfolgt bei jedem Start der App eine Warnung, dass die Version zum Ablaufdatum abläuft. Ist das Ablaufdatum überschritten, ist ein Einloggen in die App mit dieser Version nicht mehr möglich.

8.8 Reporting

Im Hauptmenü "Identity-Management", Untermenü "Reporting" sind alle Vorgänge bzw. Aktionen protokolliert, die von Benutzern durchgeführt wurden.

8.9 Auth-Connector

Der Authentifizierungs-Connector wird für Remotezugriffe und Logins benötigt.

Um einen neuen Auth-Connector hinzuzufügen, gehen Sie zum Hauptmenüpunkt "Identity-Management", Untermenü "Auth-Connector". Dem Auth-Connector muss ein einzigartiger Name gegeben werden, da Sie gleichzeitig mehrere Auth-Connectors haben können.

Für den "DoubleClue Windows Login" müssen Sie die sichere "**AuthConnectorConfig.dcem**"-Datei herunterladen, indem Sie auf den Button "Herunterladen" klicken. Bitte beziehen Sie sich für weitere Schritte auf das Handbuch "**DoubleClue_Windows_Login_EN.pdf**".

8.10 Einstellungen

Hier können diverse Einstellungen zur Benutzer-App vorgenommen werden.

Login-Fehlversuchs-Zähler:

Anzahl der fehlerhaften Login-Versuche, bevor der Account gesperrt wird.

Antwortzeit QR-Code-Login:

Dauer, wie lange der Benutzer Zeit hat, den QR-Code einzuscannen (in Sekunden).

Verbindung aufrecht erhalten:

Dauer, nach welcher die App bei Inaktivität automatisch ausgeloggt wird (in Sekunden).

Aktivierungsverzögerung nach Fehlversuch:

Dauer, wann die Aktivierung nach dem Sperren wieder freigeschaltet wird (in Minuten).

Wartende Push Approval überschreiben:

Ist diese Funktion aktiviert, werden alle Push Approvals, die sich in der Warteschleife befinden und als „queued“ markiert sind, beim Erhalt einer neuen Push Approval aus der Warteschleife entfernt. So ist immer nur die neuste Push Approval verfügbar.

Speicherdauer Report-/Meldungs-Archiv:

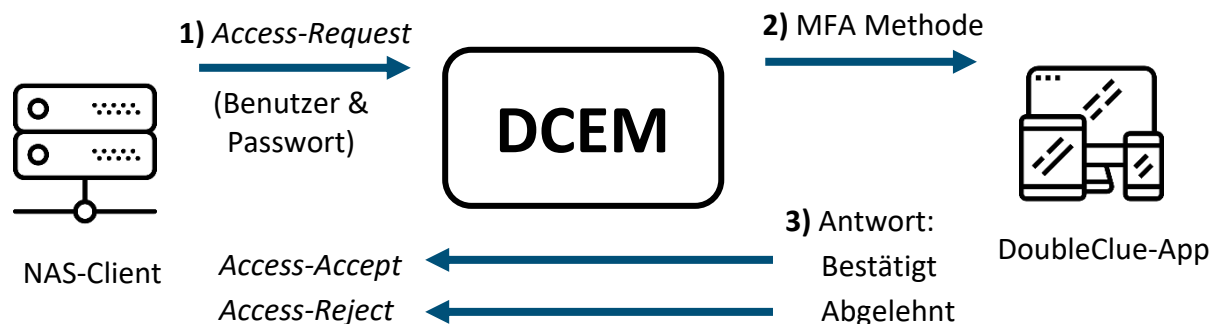
Bitte gehen Sie zu Kapitel [12. Datenbank-Archiv](#).

9. RADIUS

RADIUS ist ein Authentifizierungsprotokoll zwischen einem Netzwerk-Client und einem Server. DCEM übernimmt in diesem Fall die Rolle des RADIUS-Servers. Die Authentifizierung des Endnutzers erfolgt über den Benutzernamen und das Passwort. DCEM erweitert die Funktionalität von RADIUS um eine Multi-Faktor-Authentifizierung, die eine zusätzliche Bestätigung durch Push Approval, Passcode, OTP Token, SMS oder Voice Message erfordert (die anderen Authentifizierungsmethoden werden derzeit nicht von RADIUS unterstützt).

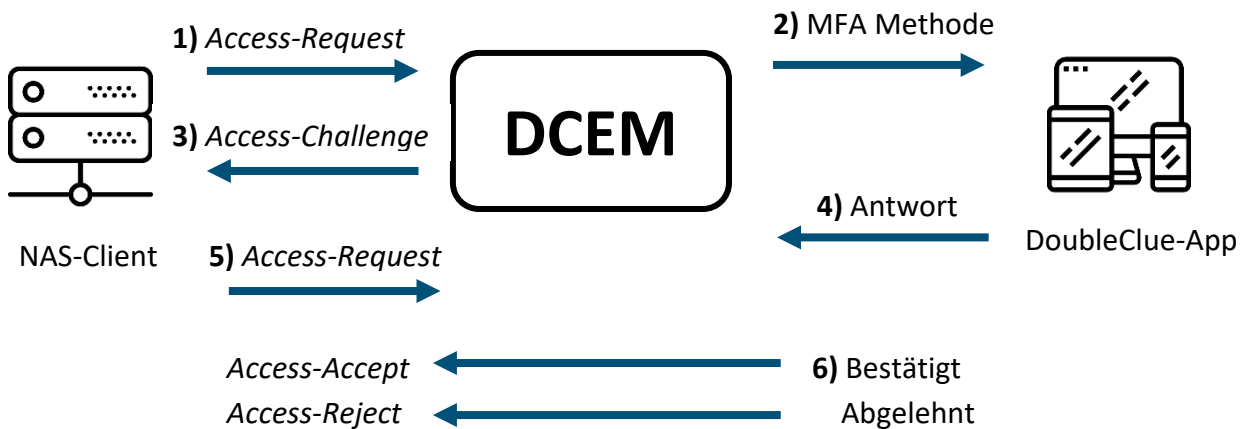
Es gibt zwei Varianten von RADIUS-Verbindungen:

9.1 Ohne RADIUS-Challenge



Bei dieser Variante bekommt der NAS-Client erst eine Antwort, nachdem der Benutzer die Anfrage “1) Access-Request” bestätigt hat. Sie müssen für den NAS-Client eine maximale Antwortzeit einstellen, die größer ist als die Zeit, die der Benutzer zum Bestätigen der Meldung “2) MFA Methode” hat.

9.2 Mit RADIUS-Challenge



Bei dieser Alternative erhält der NAS-Client als Antwort auf die Request-Anfrage sofort eine “3) Access-Challenge” von DCEM. Hierfür muss keine Antwortzeit festgelegt werden. Die Challenge-Meldung ist eine Textnachricht. Diese wird dem Endnutzer angezeigt (“Bitte schalten Sie Ihre App ein und bestätigen Sie die Meldung mit dem Code ... Schließen Sie anschließend diese Meldung.”). Den Text der Challenge-Meldung finden Sie in den Textquellen “radius.ClientChallenge” (Hauptmenü “Administration”, Untermenü “Textquellen”). Es gibt zwei Login-Vorlagen für die Benutzerbestätigung, die Vorlage “radius.Login” sowie “radius.LoginChallenge”. Der Inhalt dieser Meldungen kann bei Bedarf angepasst werden.

Erst wenn der Benutzer die Challenge-Meldung schließt, schickt der NAS-Client eine neue Request-Anfrage an DCEM. Diese wird mit “Access-Accept” oder “Access-Reject” beantwortet.

Ein Vorteil von “Access-Challenge” ist, dass dem Benutzer ein Passcode angezeigt wird, den er mit dem Code in der App vergleichen kann. Durch die Code-Prüfung ist eine höhere Sicherheit gewährleistet.

9.3 NAS-Clients

DCEM unterstützt mehrere NAS-Clients. Dazu muss jeder NAS-Client hinzugefügt und konfiguriert werden.

Name

Name des NAS-Clients - dieser muss eindeutig sein und ist frei wählbar.

IP-Nummer

IP-Adresse des NAS-Clients.

Shared Secret

Shared Secret des NAS-Clients - dieses muss auf DCEM eingegeben werden, um eine Verbindung zwischen den beiden herstellen zu können.

Challenge verwenden

Es muss gewählt werden, ob RADIUS-Challenge verwendet werden soll (siehe oben).

Benutzerpasswort ignorieren

Wenn der NAS-Client das Passwort selbst verifiziert und es nicht an DoubleClue übergibt, muss „Benutzerpasswort ignorieren“ eingeschaltet werden.

9.4 Einstellungen

Daten verfolgen

Wenn „Daten verfolgen“ eingeschaltet ist, werden alle Kommunikationsdaten zwischen dem NAS-Client und DCEM im Logfile protokolliert. Diese Einstellung sollte im Produktivbetrieb nicht eingeschaltet sein, es sei denn Sie werden vom DoubleClue-Support dazu aufgefordert.

9.5 Offline-Login mit RADIUS

Damit ein Offline-Login bei einer RADIUS-Verbindung möglich ist, muss der Offline-Login in den RADIUS-Einstellungen erlaubt werden.

Wird der Offline-Login in Verbindung mit RADIUS verwendet, muss der Endnutzer im Feld „Passwort“ den Passcode und das Passwort in folgendem Format eingeben:

#Passcode#Passwort z. B.: #123456#1234

10. REST-Web Services

DCEM bietet eine REST-Web Services-Schnittstelle, welche nur für den SVC-Knoten verwendet werden kann.

Die Authentifizierung der REST-Web Services-Schnittstelle erfolgt über das HTTP-Basic-Access-Authentication-Verfahren.

Damit Sie eine Verbindung herstellen können, hinterlegen Sie folgende URL in Ihrer REST-Web Services-Schnittstelle:

http:// --Hostname/IP des Servers-- : Port /dcem/restApi/dc

Um diese Schnittstelle nutzen zu können, benötigen Sie einen DCEM-Administrator, der das Recht hat, die Aktion „restWebServices“ durchzuführen. Standardmäßig wird nach der Installation der

Administrator **“RestServicesOperator”** angeboten. Dieser hat die benötigten Berechtigungen. Der Administrator ist zur Benutzung gesperrt. Um ihn zu aktivieren, müssen Sie im Hauptmenü **“Administration”**, Untermenü **“Benutzer”** folgende Änderungen vornehmen:

- Legen Sie ein Passwort für den Administrator fest.
- Entsperren Sie den Administrator.

Im Hauptmenü **“System”**, Untermenü **“Cluster-Konfiguration”** können Sie bei Bedarf den Port und die Sicherheitseinstellungen ändern.

Über die REST-Web Services-Verbindung können Sie folgende Methoden ausführen:

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

10.1 Vorhandene **“LibRestDcClient”** für JAVA verwenden

Der Lieferumfang der DCEM-Software beinhaltet die Datei **“LibRestDcClient-x.x.x.jar”** (x.x.x ist die Versionsnummer). Sie finden diese .jar-Datei im Verzeichnis **“bin”**. Wenn Ihr Kundenportal in JAVA programmiert ist, können Sie diese Datei verwenden. Die Bibliothek wurde mit einem Java 1.8-Compiler kompiliert.

Fügen Sie die vorhandene JAR-Datei in Ihr Kundenportal ein.

10.2 Neue **“LibRestDcClient”** für andere Programmiersprachen erstellen

Ist Ihr Kundenportal in einer anderen Sprache als JAVA programmiert, müssen Sie zuerst die **“LibRestDcClient”**-Datei für Ihr Kundenportal erstellen.

Für Java steht Ihnen eine fertige Bibliothek zur Verfügung, die Sie verwenden können. Diese finden Sie unter dem Namen **“LibRestDcClient”**.

Mit *Swagger* (www.swagger.io) können Sie Ihre Bibliothek in anderen Programmiersprachen erstellen. Hierzu benötigen Sie die **“DoubleClue.yaml”** Datei, welche im Lieferumfang der DCEM-Software im Verzeichnis **“DcemDistribution\artifacts\yajsw\REST-WebServices”** enthalten ist.

Ausführliche Informationen zur REST-Web Services-Schnittstelle finden Sie in folgendem HTML-Dokument:

DcemDistribution/artifacts/yajsw/doc/REST-WebServices/index.html

10.3 Demo einer einfachen REST-Web Services-Anwendung

Im Verzeichnis **“DcemInstallation/REST-WebServices/JavaSimpleDemo”** finden Sie ein Beispiel einer einfachen JAVA-Anwendung, welche die **“LibRestDcClient”**-Bibliothek initialisiert, eine Push Approval an einen Benutzer sendet und auf die Antwort wartet. Dies wird Ihnen helfen, die DCEM Rest-API kennenzulernen.

11. SAML

SAML, Security Assertion Markup Language, ist ein offener Standard für den Austausch von Authentifizierungsinformationen zwischen einem Identity-Provider und einem Service-Provider. SAML ist eine XML-basierte Markup-Sprache. Die wichtigste Verwendung von SAML ist der Webbrowser-Single Sign-On (SSO).

11.1 Einrichten von DCEM als Identity-Provider

11.1.1 DCEM-SAML Trust-Zertifikate

DoubleClue ist ein SAML-Identity-Provider und benötigt zwei verschiedene vertrauenswürdige Zertifikate:

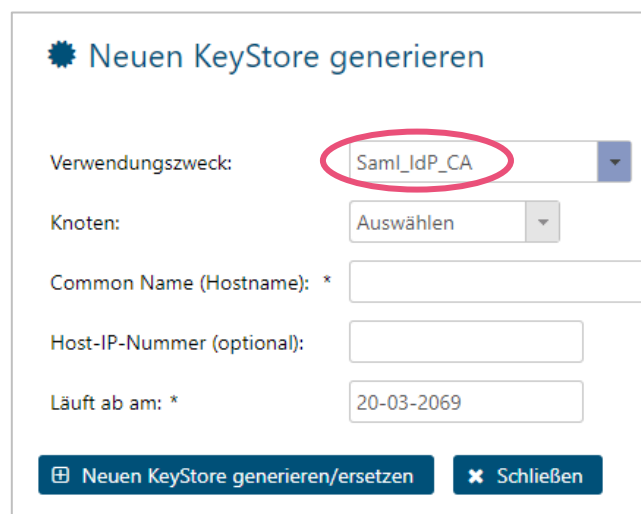
- SAML-Identity-Provider-Zertifikat
- SAML-Verbindungs-Zertifikat

Konfigurieren Sie SAML unter System > Clusterkonfiguration wie in Kapitel [3.1.2 Verbindungsdienste](#) beschrieben.

11.1.1.1 SAML-Identity-Provider-Zertifikat

Das SAML-Identity-Provider-Zertifikat wird benötigt, um die Metadaten, die DoubleClue an den SAML-Service-Provider zurückgibt, zu signieren. Beim Setup von DCEM wird der KeyStore für dieses Zertifikat automatisch erstellt und vom DCEM-Root-Zertifikat signiert.

Wenn Sie ein neues Zertifikat erstellen oder installieren möchten, gehen Sie zum Hauptmenüpunkt "System", Untermenü "KeyStores" und generieren oder laden Sie einen neuen KeyStore hoch, indem Sie die entsprechenden Buttons anklicken und den Verwendungszweck "**Saml_IdP_CA**" auswählen. Weitere Informationen finden Sie in Kapitel [3.3 KeyStores](#).



Neuen KeyStore generieren

Verwendungszweck: **Saml_IdP_CA**

Knoten: Auswählen

Common Name (Hostname): *

Host-IP-Nummer (optional):

Läuft ab am: * 20-03-2069

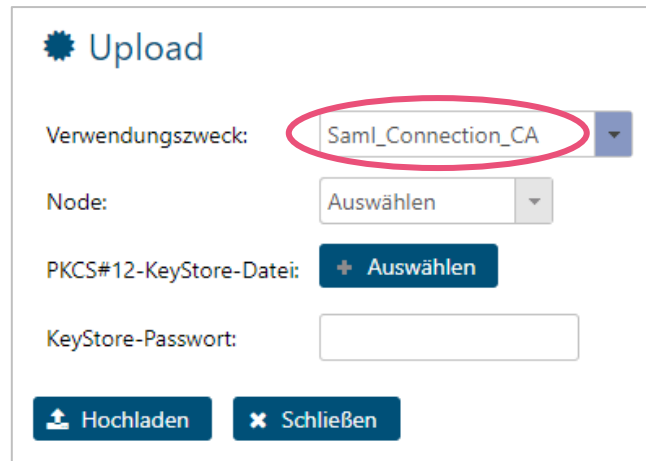
Neuen KeyStore generieren/ersetzen **Schließen**

11.1.1.2 SAML HTTPS (SSL/TLS)-Verbindung

Da DoubleClue ein SAML Identity-Provider ist, muss der Zugriff darauf über das Internet vom Browser eines Benutzers aus erfolgen. Die Verbindung muss sicher sein und HTTPS (SSL/TLS) verwenden. Wird SSL/TLS bei DoubleClue beendet, müssen Sie ein offiziell signiertes Zertifikat von einer weltweit anerkannten Zertifizierungsstelle beziehen und hochladen.

Für Testzwecke können Sie auch ein neues KeyStore-Zertifikat in DCEM generieren. Zu diesem Zweck wird beim DCEM-Setup ein Test-KeyStore erstellt.

Um ein offiziell signiertes Zertifikat einer Zertifizierungsstelle hochzuladen, gehen Sie zum Hauptmenüpunkt "System", Untermenü "KeyStores", klicken Sie auf den Button "Upload" und wählen Sie "**Saml_Connection_CA**" als Verwendungszweck aus. Laden Sie die PKCS#12-Datei hoch.



11.1.2 Einstellungen für SAML

Um SAML-Einstellungen vorzunehmen, gehen Sie zum Hauptmenüpunkt “SAML”, Untermenü “Einstellungen”:

SSO-Domain:

Dies sollte eine extern zugängliche Basis-URL der SAML-SSO-Seiten sein. Für gewöhnlich ist dies die URL der DCEM-Seiten, aber ohne “/dcem/mgt/index.xhtml” und mit dem Port, der für SAML verwendet wird.

IdP-Entitäts-ID:

Geben Sie hier einen Namen ein. Für gewöhnlich wird derselbe Text verwendet, den Sie bei der SSO-Domäne eingegeben haben, um Einzigartigkeit zu gewährleisten, aber Sie können auch jeden anderen Namen auswählen.

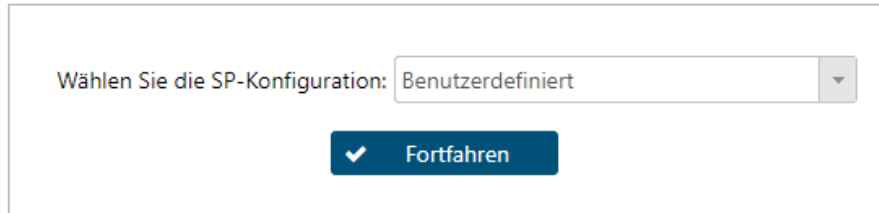
11.1.3 Download der Identity-Provider-Metadaten-Datei

Um die Identity-Provider-Metadaten-Datei herunterzuladen, gehen Sie zum Hauptmenüpunkt “SAML”, Untermenü “SP-Metadaten” und klicken Sie auf den Button “IdP-Metadaten herunterladen”. Klicken Sie auf “Metadaten herunterladen” und speichern Sie die Datei an einem Ort, an dem Sie diese für weitere Verwendung wiederfinden können. Wenn Sie dies möchten, können Sie zudem das X.509-Signierzertifikat (im PEM-Format) herunterladen, indem Sie „Zertifikat herunterladen“ anklicken.

11.1.4 Hinzufügen eines Service-Providers

DoubleClue unterstützt mehrere Service-Provider. Um einen Service-Provider hinzuzufügen, gehen Sie zum Hauptmenüpunkt “SAML”, Untermenü “SP-Metadaten” und klicken Sie auf den Button “Hinzufügen”. Sie können dann einen unserer vorkonfigurierten SP-Metadaten aus dem Dropdown-

Menü auswählen, oder Sie erstellen eine benutzerdefinierte SP-Konfiguration, indem Sie “Benutzerdefiniert” auswählen.

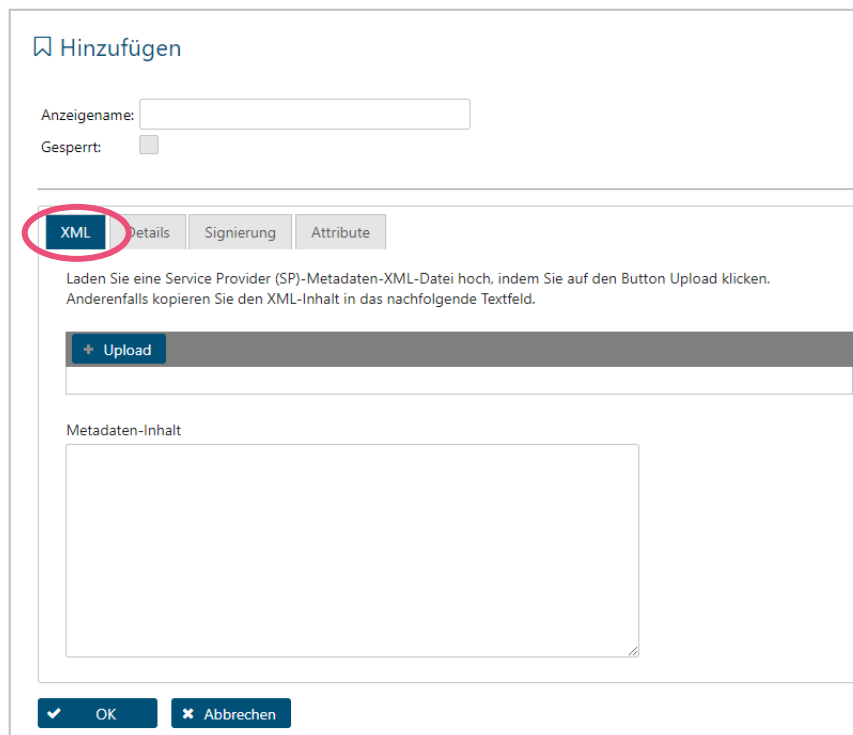


Wählen Sie die SP-Konfiguration: Benutzerdefiniert

Fortfahren

Wenn Sie sich dazu entschließen, einen benutzerdefinierten SP zu erstellen, gibt es zwei Möglichkeiten, dies zu tun:

1. Wenn Sie eine Service-Provider-XML-Metadaten-Datei haben, gehen Sie zum “XML”-Tab. Klicken Sie auf “Hochladen”, um die entsprechende Datei hochzuladen, oder kopieren Sie den XML-Inhalt in das Textfeld “Metadaten Inhalt”. Klicken Sie zum Speichern auf “OK”.



Hinzufügen

Anzeigenname:

Gesperrt: ☐

XML Details Signierung Attribute

Laden Sie eine Service Provider (SP)-Metadaten-XML-Datei hoch, indem Sie auf den Button Upload klicken. Anderenfalls kopieren Sie den XML-Inhalt in das nachfolgende Textfeld.

+ Upload

Metadaten-Inhalt

OK Abbrechen

2. Wenn Sie keine Service-Provider-Metadaten-Datei haben, gehen Sie zum “Details”-Tab.

Geben Sie die einzigartige Entitäts-ID des Service Providers sowie den Standort des ACS (= Assertion Consumer Service) ein. Ändern Sie das NameID-Format in jenes, das mit dem übereinstimmt, welches Ihr Service Provider für die Benutzeridentifikation verwendet. Wenn Ihr SP Single-Logout-Anfragen unterstützt, können Sie eine Single-Logout-Service-URL eingeben. Des Weiteren können Sie festlegen, ob Logout-Anfragen per HTTP POST oder REDIRECT gesendet werden.

Optional können Sie auch ein X.509-Zertifikat (im PEM-Format) unter dem “Signierung”-Tab hinzufügen, wenn Ihr Service Provider SAML-Anfragen mit einem selbstsignierten Zertifikat signiert (dies ist für gewöhnlich der Fall).

Andere Felder:

- **Anzeigename:** Ein benutzerfreundlicher Anzeigename für den Service-Provider. Er wird während des Logins angezeigt, sodass Benutzer wissen, wo sie sich einloggen. Sie können diesen später verändern, wenn gewünscht. Bitte beachten Sie, dass das Textfeld nicht leer bleiben darf!
- **Gesperrt:** Setzen Sie in dieser Box einen Haken, wenn Sie einen Service Provider nicht weiter unterstützen möchten, ohne seinen Datenbankeintrag jedoch vollständig zu löschen.

Signierungs-Tab

Einige Service Provider signieren ihre SAML-Anfragen absichtlich nicht. Dies ist nicht ideal, wird aber dennoch von DCEM unterstützt. Wenn sich Ihr SP so verhält, können Sie den Haken bei “Anfragen werden signiert” entfernen, damit DCEM weiß, dass es vom SP keine Signaturen erwarten darf, und so während SSO-Logins nicht zu einer Fehlerseite weiterleitet. Falls Ihr SP SAML-Anfragen signiert (was normalerweise der Fall ist), **entfernen Sie den Haken nicht**.


Signiert Ihr SP Anfragen mit einem selbst-signierten Zertifikat (was ebenfalls für gewöhnlich der Fall ist), können Sie dieses Zertifikat in das entsprechende Textfeld kopieren. Das Zertifikat muss in einem base64-kodierten PEM-Format ohne Kopf- oder Fußzeilen vorliegen.

Attribute-Tab

Wenn Ihr SP Attribute benötigt (zusätzliche Daten über Benutzer, die in SAML-Elementen mitenthalten sind), können Sie diese im "Attribute"-Tab manipulieren. Falls manche Attribute bereits in einer hochgeladenen SP-Metadaten-XML-Datei als notwendig gekennzeichnet wurden, werden diese automatisch hinzugefügt. Sie müssen jedoch immer noch bearbeiten, welchen Benutzereigenschaften diese Attribute zugeordnet werden sollen, wenn SAML-Login-Anfragen gesendet werden. Standardmäßig wird allen neuen Attributen nichts ("None") zugeordnet.

Klicken Sie auf das Bleistift-Symbol am Ende einer Reihe, um ein Attribut zu bearbeiten. Bearbeiten Sie den Namen und/oder die Benutzereigenschaft wie es Ihnen beliebt und klicken Sie dann auf das Häkchen-Symbol, das anstatt des Bleistift-Symbols erscheint. Attribute können einer der folgenden Benutzereigenschaften zugeordnet werden:

- None: Das Attribut ist immer noch in Antworten mitenthalten, besitzt aber nie einen Wert.
- Display Name: Das Attribut enthält den Anzeigenamen des DoubleClue-Benutzers.
- Login ID: Das Attribut enthält den Anmeldenamen des DoubleClue-Benutzers.
- Email: Das Attribut enthält die E-Mail des DoubleClue-Benutzers, falls eine konfiguriert wurde.
- Cloud Safe (User): Das Attribut enthält benutzerdefinierten Cloud Safe-Text (falls welcher gefunden wird), dessen Name mit dem Attributnamen übereinstimmt und der an den entsprechenden Nutzer gebunden ist. Dies bedeutet, dass der Inhalt für jeden einzelnen Benutzer unterschiedlich sein kann.
- Cloud Safe (Global): Das Attribut enthält benutzerdefinierten Cloud Safe-Text (falls welcher gefunden wird), dessen Name mit dem Attributnamen übereinstimmt und als dessen Besitzer "Global" eingestellt ist. Dies bedeutet, dass der Inhalt für alle Benutzer gleich ist.





 Hinzufügen

Anzeigename:

Gesperrt: ☐

XML Details Signierung **Attribute**

+ Neues Attribut hinzufügen **- Attribute löschen**

Name	Benutzereigenschaft	
name	Display Name	
uid	Login ID	
mail	Email	
country	Cloud Data (User)	

✓ OK **✗ Abbrechen**

11.2 Individuelle Anpassung der SAML-Webseiten

Die SAML-Webseiten für Benutzer können individuell nach Ihren Wünschen angepasst werden.

Um die Webseiten zu ändern, benötigen Sie gute Kenntnisse des **Java Server Faces** (JSF)-Frameworks und der **PrimeFaces**-Komponenten (<https://www.primefaces.org/>).

Die Seiten können unter “**DCEM-Installation-Directory/WebContent/saml**” gefunden werden.

⚠ Wenn Sie die Seiten ändern, müssen Sie vorsichtig sein, wenn Sie ein Update von DCEM vornehmen, da dies die Seiten überschreiben und auf den Auslieferungszustand zurücksetzen wird!

Die Seiten gelten für alle Sprachen. Die Texte dafür werden aus den DCEM-Textquellen geholt.

Beispiel: `value="#{dbMsg['sso.error.expired']}"` mit 'sso.error.expired' als Textquellen-Schlüssel.

12. OpenID

OpenID ist ein offener Standard und Authentifizierungsprotokoll, das auf OAuth 2.0 aufbaut. Es dient dem Austausch von Daten zur Identitätsüberprüfung zwischen einem OpenID Server und einem OpenID Authentication Server.

12.1 Vorbereitung von DCEM als OpenID Authentication Server

12.1.1 Eingabe des Clusternamens

Konfigurieren und aktivieren Sie die OpenID-OAuth-Verbindung unter System > Clusterkonfiguration, wie in Kapitel [3.1.2 Verbindungsdienste](#) beschrieben.

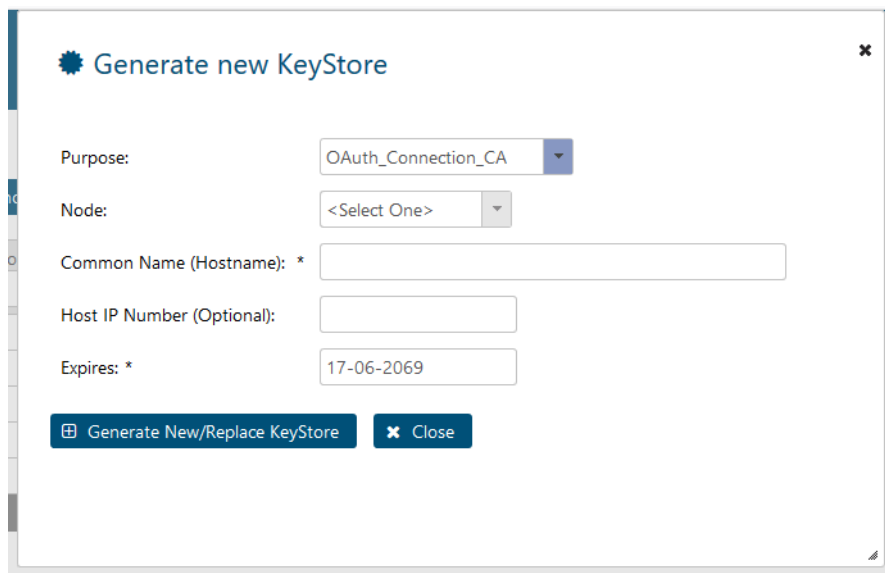
12.1.2 DCEM OpenID Certificate

Um Ihre OpenID SSO Seite mit SSL zu sichern, brauchen Sie ein Connection Certificate.

12.1.2.1 OpenID Connection Certificate

Wenn Sie ein neues Zertifikat generieren oder installieren möchten, gehen Sie zum Hauptmenüabschnitt „System“, Untermenü „Keystores“ und generieren Sie einen neuen KeyStore oder laden Sie ihn hoch, indem Sie auf den entsprechenden Button klicken und dann als Purpose **“OAuth_Connection_CA”** auswählen.

Wählen Sie einen Knoten (Node) und geben Sie den “Hostnamen” ein, um einen neuen KeyStore zu generieren oder wählen Sie die entsprechende Datei, um einen hochzuladen. Bestätigen Sie Ihre Eingaben.



The screenshot shows a dialog box titled "Generate new KeyStore" with a close button (X) in the top right corner. The dialog contains the following fields and buttons:

- Purpose:** A dropdown menu with "OAuth_Connection_CA" selected.
- Node:** A dropdown menu with "<Select One>" selected.
- Common Name (Hostname): *** A text input field.
- Host IP Number (Optional):** A text input field.
- Expires: *** A text input field containing "17-06-2069".
- At the bottom, there are two buttons: "Generate New/Replace KeyStore" (with a plus icon) and "Close" (with an X icon).

12.1.2.2 OpenID HTTPS (SSL/TLS) Connection

Damit DoubleClue als OpenID Authentication Server fungieren kann, muss es über das Internet per Webbrowser erreichbar sein. Es muss sich dabei um eine sicherer Verbindung mit HTTPS(SSL/TLS)-Verschlüsselung handeln. Wenn SSL/TLS via DoubleClue deaktiviert ist, ist es notwendig ein Zertifikat

zu erwerben und hochzuladen, dass von einer der weltweit anerkannten Zertifizierungsstelle ausgegeben wurde.

Zu Testzwecken können Sie auch ein neues KeyStore-Zertifikat in DCEM erstellen. Während des DCEM Setups wird ein Test-KeyStore für diesen Zweck erstellt.


Um einen offiziell signiertes CA hochzuladen, gehen Sie im Hauptmenü auf „System“, Untermenü „KeyStores“, klicken Sie auf „Upload“ und wählen Sie als Purpose **“OAuth_Connection_CA”**. Laden Sie dann die PKCS#12-Datei hoch.

12.1.3 Einstellung der OpenID Preferences

Um die OpenID Preferences einzustellen, gehen Sie zum Hauptmenüabschnitt “OpenID - OAuth”, Untermenü “Preferences”:

- **Issuer:**
Dies sollte die extern zugängliche Basis-URL der OAuth SSO-Seite sein. Normalerweise ist es die URL der DCEM-Seite, aber ohne **“/dcem/mgt/index.xhtml”** und mit dem Port, der für OAuth verwendet wird.
- **Token Configuration:**
Diese Einstellungen erlauben es Ihnen die Laufzeit der Authorisation Codes, Access Tokens, Refresh Tokens und ID Tokens zu konfigurieren, indem Sie die Laufzeit in Sekunden angeben.
- **SSO Service:**
In diesem Bereich können Sie angeben, ob die User Ihr Passwort eingeben müssen, um auf die SSO-Login-Seite zu gelangen oder nicht, ob der login via QR Code möglich ist und, wenn er es ist, ob er als erste Seite angezeigt wird.

Preferences

 Save

-

Authorisation Server Metadata

Issuer

Should contain an accessible base URL of the OAuth SSO page.

-

Token Configuration

Authorisation Code Lifetime

120

Seconds. Also defines session lifetimes for SSO logins.

Access Token Lifetime

3600

Seconds

Refresh Token Lifetime

36000

Seconds

Id Token Lifetime

10000

Seconds

-

SSO Service

Password Required

☒

If unchecked, users do not need to enter their password on the SSO login page, but they still need to log into a client app to acknowledge the request.

Qr Code Enabled

☒

If unchecked, the option to log in via QR Code will be removed from the SSO login page.

Start Sso With Qr Code

☐

If checked, the first SSO screen will be the QR Code page.

Wenn Sie Ihre OpenID-Konfiguration einsehen wollen, können Sie sich die JSON-Datei unter „<issuer>/dcem/oauth/.well-known/openid-configuration“ anzeigen lassen.

12.1.4 Hinzufügen eines OpenID Clients

DoubleClue unterstützt mehrere OpenID Clients. Um einen OpenID Client hinzuzufügen, gehen Sie ins Hauptmenü “OpenID-OAuth”, Untermenü “Client Metadata” und klicken Sie auf “Add”.

Allgemeine Einstellungen:

- **Display Name:** Ein freundlicher Name für den OpenID Client. Er wird während des Logins angezeigt, so dass die Benutzer wissen, wo sie sich einloggen. Sie können diesen Namen jederzeit ändern. Bitte beachten Sie, dass sich bei der Angabe eines Display Namens um eine Pflichtangabe handelt.
- **Disabled:** Wählen Sie diese Box, wenn Sie einen Service Provider nicht länger unterstützen möchten, seinen Datenbankeintrag jedoch nicht löschen wollen.

Client ID und Client Secret

Wenn Sie bereits Zugriff auf einen Open ID Client in Form einer Webseite, die OpenID unterstützt, und Client Anmeldedaten besitzen, geben Sie diese in die entsprechenden Felder ein. Wenn nicht, können Sie die Client ID und das Client Secret hier festlegen und auf dem Server entsprechend einstellen. Sie können die Anmeldedaten frei wählen, aus Sicherheitsgründen würden wir jedoch empfehlen, diese über den „Generieren“-Button automatisch generieren zu lassen.

Sie können in diesem Fenster ebenfalls die URI-Umleitungen Ihres Clients als eine durch Kommas getrennte Liste anlegen. Während das im allgemeinen eine optionale Einstellung ist, kann es sein, dass manche OpenID Clients diese verlangen.

Sobald Sie die benötigten Informationen eingegeben haben, klicken Sie auf "OK", um die Änderungen zu speichern.


The screenshot shows a modal dialog titled "Add". At the top left is a blue button with a white bookmark icon and the text "Add". To its right is a close icon. Below the title bar, there is a "Display Name:" label followed by a text input field. Underneath is a "Disabled:" label followed by a checkbox. A horizontal line separates this from the "Details" section, which has a blue header button labeled "Details". Inside the "Details" section, there are three rows: "Client ID" with a text field and a blue "Generate" button; "Client Secret" with a text field and a blue "Generate" button; and "Redirect URIs" with a text field. At the bottom of the dialog are two buttons: a blue "OK" button with a white checkmark icon and a grey "Cancel" button with a white 'x' icon.

12.2 Anpassung der OpenID Web Pages

OpenID Webpages können individuell Ihren Bedürfnissen angepasst werden.

Um Ihre Webpage zu ändern, benötigen Sie vertiefte Kenntnisse über das Java Server Faces (JSF) Framework und PrimeFace-Komponenten (<https://www.primefaces.org/>).

Die Seite kann unter "**DCEM-Installation-Directory/WebContent/oauth**" gefunden werden.

 Wenn Sie die Seiten ändern, müssen Sie vorsichtig sein, wenn Sie ein Update von DCEM vornehmen, da dies die Seiten überschreiben und auf den Auslieferungszustand zurücksetzen wird!

Die Seiten gelten für alle Sprachen. Die Texte dafür werden aus den DCEM-Textquellen geholt.

Beispiel: `value="#{dbMsg['sso.error.expired']}"` mit 'sso.error.expired' als Textquellen-Schlüssel.

13. Datenbank-Archiv

Die folgenden Datenbank-Tabellen mit Einträgen, die älter als eine konfigurierbare Einstellung in Tagen sind, können regelmäßig in ZIP-Dateien archiviert werden:

- Administration: Änderungshistorie
- Identity-Management: Push Approvals
- Identity-Management: Reporting
- RADIUS: Reporting

Der Archivierungsprozess wird an jedem ersten Tag des Monats ausgeführt. Alle Einträge, die älter als eine bestimmte voreingestellte Zeitdauer sind, werden dann automatisch in ZIP-Dateien im Ordner **“DCEM_HOME/archive”** Ihrer DCEM-Installation archiviert und aus der Datenbank gelöscht. Bitte beachten Sie, dass die Dateien in einer Cluster-Umgebung mit mehreren Knoten nur auf dem Hauptknoten, welches der älteste betriebene Knoten ist, gespeichert werden.

Sie können die Zeitdauer (in Tagen), nach der Einträge automatisch archiviert werden, folgendermaßen einstellen:

- Historien-Archiv: Administration > Einstellungen > Speicherdauer Historien-Archiv
- Report-Archiv: Identity-Management > Einstellungen > Speicherdauer Report-Archiv
- Meldungs-Archiv: Identity-Management > Einstellungen > Speicherdauer Meldungs-Archiv
- RADIUS Report-Archiv: RADIUS > Einstellungen > Speicherdauer Report-Archiv

Wenn Sie die Zeitdauer auf “0” setzen, wird die automatische Archivierung deaktiviert.

14. UserPortal

Das UserPortal ist ein Selfservice-Portal für DoubleClue-Nutzer. Es kann über die URL **https://www.hostname/dcem/userportal** bzw. bei einem Szenario mit mehreren Mandanten **https://www.mandantennamenname/hostname/dcem/userportal** erreicht werden.

UserPortal bietet Benutzern die Option sich zu registrieren, ihre mit DoubleClue verbundenen Smart Devices, FIDO Token und OTP Token selbst zu verwalten und auf den Cloud Safe und den Password Safe zuzugreifen. Welche dieser Optionen den Benutzern zur Verfügung stehen, können Sie in der UserPortal Konfiguration einstellen.

14.1 Konfiguration

Das UserPortal muss für jeden Mandanten einzeln konfiguriert werden. Die verschiedenen Mandanten übernehmen nicht die Einstellungen des Haupt-Mandanten, wenn keine individuelle Konfiguration für diese angelegt wurde.

14.1.1 Allgemeine Einstellungen

- Titel:
Wenn Sie ‚UserPortal‘ einen anderen Titel geben möchten, können Sie ihn hier eingeben.
- Captcha aktivieren:
Stellen Sie ein, ob Sie die Registrierung in UserPortal mit einem Captcha sichern wollen. Damit das Captcha funktioniert, müssen Sie es zunächst konfigurieren. Erfahren Sie mehr dazu in Kapitel [14.1.3 Captcha Konfiguration](#).
- Registrierung als lokaler Benutzer / Domänenbenutzer erlauben
Stellen Sie ein, welche Art von Benutzern sich über UserPortal registrieren können.
- Benachrichtigungstyp
Stellen Sie ein, welche Art von Nachrichtentypen Sie zum Versenden von Aktivierungscodes zulassen wollen.

14.1.2 Konfiguration der sichtbaren Elemente

14.1.2.1 Sichtbare Views

Unter Visible Views können Sie einstellen, welche Bereiche UserPortals die Benutzer einsehen können. Alle Views die hier verborgen werden, können von den Benutzern unter keinen Umständen eingesehen werden. Entsprechend können die Nutzer auch keine Funktionen ausführen, die sich in einer ausgeblendeten View befinden.

14.1.2.2 Sichtbare Views, die Multi-Faktor-Authentifizierung erfordern

Hier können Sie auswählen, welche der sichtbaren Views die Benutzer nur einsehen können, wenn sie sich mittels Multi-Factor-Authentication angemeldet haben. Beachten Sie bitte, dass nur Views die unter „Visible Views“ auf sichtbar gestellt wurden hiervon betroffen sind. Views, die auf „unsichtbar“ gestellt wurden, sind mit und ohne MFA verborgen.

14.1.2.3 Sichtbare Aktionen


Wählen Sie die Aktionen aus, die den Benutzern in UserPortal zur Verfügung stehen sollen. Damit die Benutzer Zugriff auf eine Aktion haben, muss die View, in der sich die Aktion befindet, sichtbar sein.

14.1.2.4 Sichtbare Aktionen, die Multi-Faktor-Authentifizierung erfordern

Hier können Sie auswählen, welche Aktionen die Benutzer nur ausführen können, wenn diese sich mit Multi-Factor-Authentication angemeldet haben. Wie zuvor muss die entsprechende Aktion sowohl unter Visible Actions als sichtbar ausgewählt werden und sich auf einer sichtbaren View befinden, ansonsten kann diese von den Benutzern nicht eingesehen werden – unabhängig wie sich angemeldet haben.

14.1.3 Captcha Konfiguration mit Google reCAPTCHA v2

Gehen Sie auf <https://www.google.com/recaptcha/>. Loggen Sie sich mit Ihrem Google-Account in die ‚Administrator Konsole‘ ein und registrieren Sie Ihre DoubleClue-Domäne für reCAPTCHA v2. Sie erhalten nun zwei reCAPTCHA-Keys, den Websiteschlüssel (Public Key) und den geheimen Websiteschlüssel (Private Key).

 Lassen Sie die Seite mit den Schlüsseln geöffnet, oder kopieren Sie sie an einen sicheren Ort. Sie werden sie im nächsten Schritt brauchen!

Bei der Verwaltung mehrerer Mandanten ist es ausreichend, die Hauptdomain bei Captcha zu registrieren. Die einzelnen Subdomains müssen nicht extra registriert werden.

Loggen Sie sich jetzt in DCEM ein. Gehen Sie im Hauptmenü zum Bereich „System“ und hier zu den „Einstellungen“. Tragen Sie im Abschnitt „Google Captcha“ die beiden Schlüssel in die entsprechenden Felder ein. Speichern Sie die Einstellungen und starten Sie anschließend DCEM neu. Die Änderungen werden nach dem Neustart aktiv.

15. Lizenzierungssystem

Das DoubleClue-Lizenzierungssystem implementiert Bedingungen für die Softwarenutzung.


Momentan bieten wir eine Kategorie von Lizenzierungen an, die mit dem Identity-Management-Modul in Zusammenhang stehen. Gehen Sie zum Hauptmenüpunkt „Administration“, Untermenü „Lizenz-Verwaltung“. Es gelten die folgenden Lizenzbedingungen:

Verfallsdatum:

Dauer der Softwarenutzung.

Maximale Benutzeranzahl:

Anzahl der aktivierten Benutzer.

 Aktivierte Benutzer sind alle unterscheidbaren Benutzer, die sich bereits mittels irgendeiner Authentifizierungsmethode authentifiziert und mindestens einmal innerhalb eines Jahres eingeloggt haben.

Max. Authentifizierungen nur mittels Passwort; Max. Authentifizierungen mittels SMS; Max. Authentifizierungen mittels Voice Message; Max. Authentifizierungen mittels Hardware Token; Max. Authentifizierungen mittels DC App Passcode; Max. Authentifizierungen mittels Push Approval:

Maximale Anzahl an Benutzern, die mittels der entsprechenden Authentifizierungsmethoden authentifiziert werden können.

Test:

Dieses Merkmal wird in einer nicht-produktiven Installation eingestellt.

Bei einem Login im DCEM-Management oder in der DoubleClue-App wird immer eine Warnmeldung angezeigt.

Nach einer neuen DCEM-Installation werden die Lizenzbedingungen wie folgt eingestellt:

- Verfallsdatum: Datum der Installation plus drei Monate
- Maximale Benutzeranzahl: 100
- Max. Authentifizierungen mittels Passwort; jeweils 100
Max. Authentifizierungen mittels SMS;
Max. Authentifizierungen mittels Voice Message;
Max. Authentifizierungen mittels OTP Token;
Max. Authentifizierungen mittels DC App Passcode;
Max. Authentifizierungen mittels Push Approval;
Max. Authentifizierungen mittels FIDO Authenticator;
- Prüfung: True



Die Limitierung bezieht sich auf die Benutzer**aktivierung** und/oder -**authentifizierung**. Dies bedeutet, dass im System zwar eine unbegrenzte Anzahl an Benutzern **hinzugefügt** werden kann, diese aber nur begrenzt **aktiviert** werden können. Die Anzahl der Geräte pro aktiviertem Benutzer ist hingegen unbegrenzt.

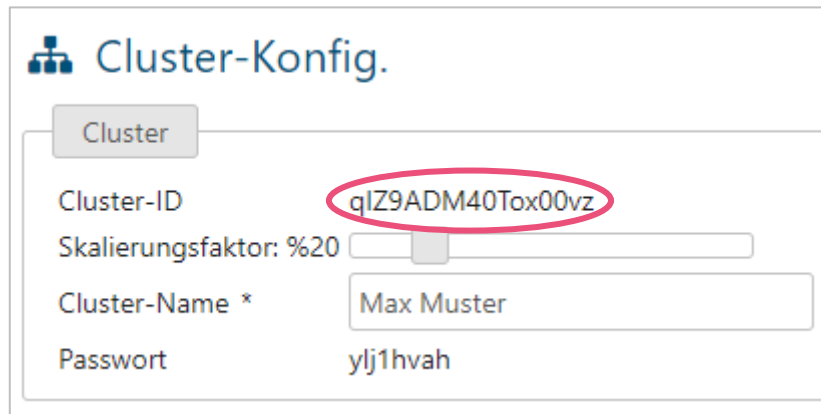
15.1 Beantragung eines neuen Lizenzschlüssels

Nach einer Testphase können Sie eine neue Lizenz beantragen.

Dazu werden folgende Informationen benötigt:

- Firmenname
- Ansprechpartner
- E-Mail-Adresse
- Firmenanschrift
- DCEM-Cluster-ID

Ihre DCEM-Cluster-ID finden Sie unter dem Hauptmenüpunkt "System", Untermenü "Cluster-Konfiguration".



Cluster-Konfig.

Cluster

Cluster-ID: qIZ9ADM40Tox00vz

Skalierungsfaktor: %20

Cluster-Name *: Max Muster

Passwort: ylj1hvah

Senden Sie diese Informationen an sales@doubleclue.com.

Nach Absprache mit dem Vertrieb erhalten Sie einen neuen Lizenzschlüssel per Email.

15.2 Hinzufügen eines Lizenzschlüssels

Gehen Sie zum Hauptmenüpunkt "Administration", Untermenü "Lizenz Verwaltung" und klicken Sie auf "Lizenzschlüssel importieren".

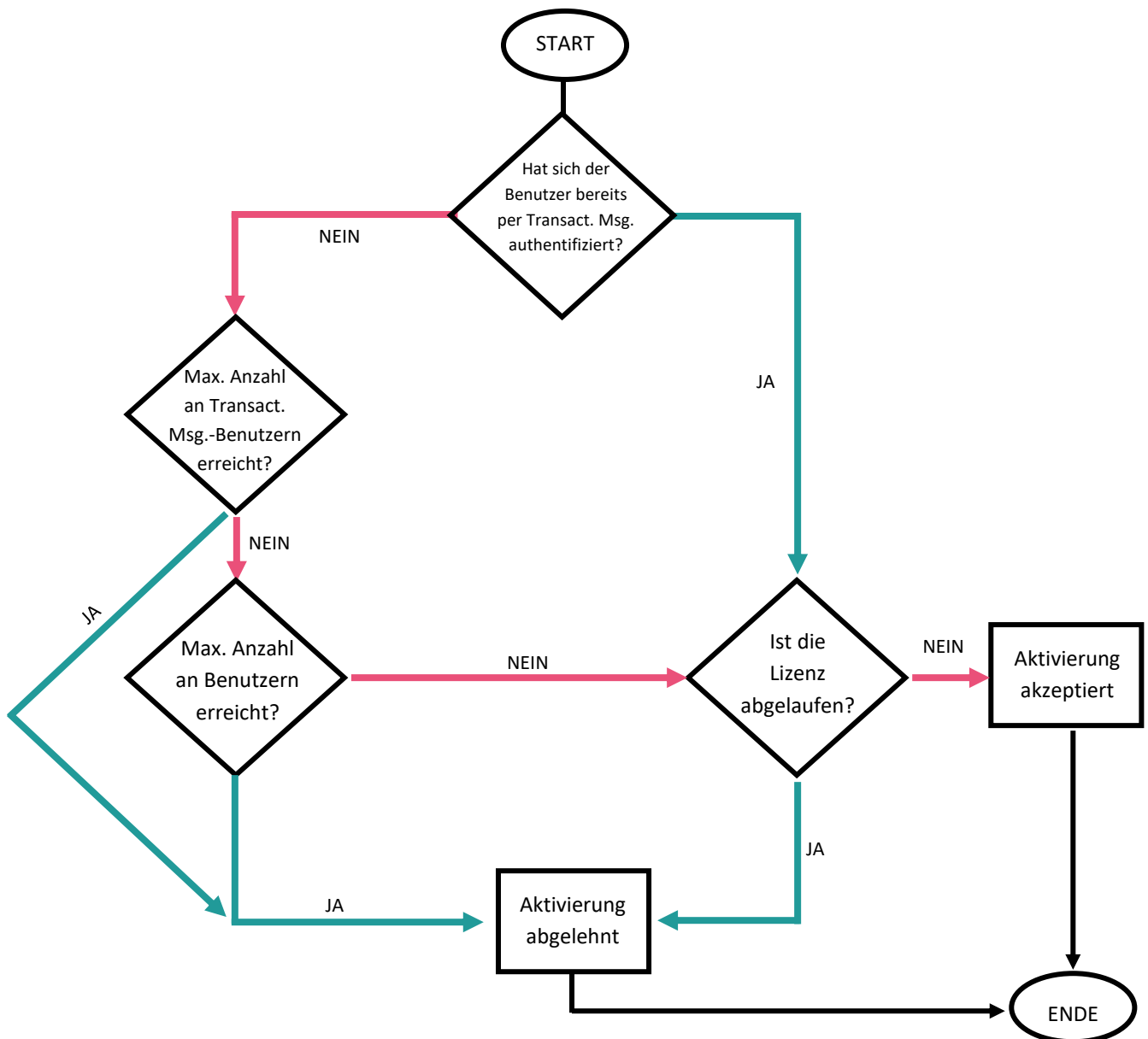
Fügen Sie den Lizenzschlüssel, den Sie zuvor erhalten haben, im Eingabefeld ein und klicken Sie auf "OK". Überprüfen Sie die angezeigten Lizenzbedingungen.

15.3 Lizenzen einsehen

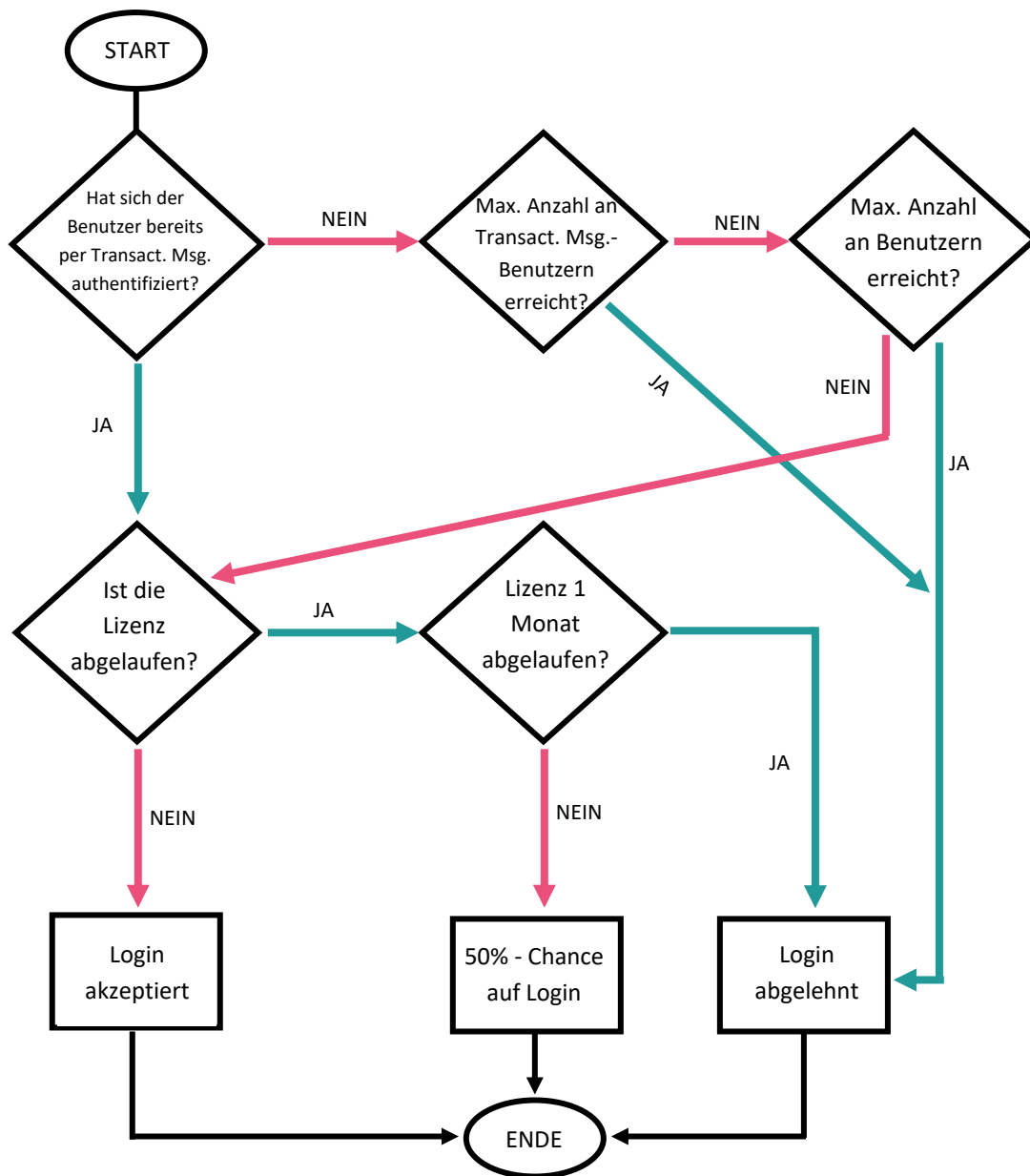
Installierte Lizenzen können ebenfalls unter dem Hauptmenüpunkt "Administration", Untermenü "Lizenzen" eingesehen werden.

15.4 Funktionen des Lizenzierungstyps

15.4.1 Aktivierung



15.4.2 Login



16. Logging

DCEM hat ein ausgefeiltes Log-System. Das System speichert alle Vorkommnisse, die für eine weitere Analyse notwendig sein könnten.

Zu diesem Zweck integriert DCEM das Log-Framework von Apache Log4j Version 2.

Es existieren die folgenden Log-Level:

Error:

Der Administrator muss reagieren, wenn ein Fehler-Level geschrieben wird.

Warning:

Der Administrator muss dies überprüfen.

Debug:

Der Administrator sollte dies auf produktiven Servern nicht aktivieren, sofern er nicht durch das DoubleClue-Support-Team dazu angewiesen wurde.

Trace:

Der Administrator sollte dies auf produktiven Servern nicht aktivieren, sofern er nicht durch das DoubleClue-Support-Team dazu angewiesen wurde.

16.1 Konfigurierung

Die Protokollierungs-Konfiguration wird bei der Inbetriebnahme von DCEM von **"DCEM_HOME/log4j2.xml"** gelesen.

Die Log-Level können in den DCEM-GUI-Systemeinstellungen geändert werden.

Beziehen Sie sich bitte für weitere Details über diese Konfiguration auf <https://logging.apache.org/log4j/2.x/manual/>

16.2 Datei-Output

Die Protokollierung gibt die Daten in fünf Rollover-Dateien aus.

Der aktuelle Dateiname ist **"dcem.log"** und die neuesten Dateien werden entsprechend **"dcem_1.log"** bis **"dcem_4.log"** benannt. Dies ist standardmäßig immer aktiviert.

Diese Output-Dateien werden in das Verzeichnis **"DCEM_HOME/logs"** geschrieben. Die Log-Dateien aller Knoten können auch in die DCEM-GUI heruntergeladen werden, indem Sie zum Hauptmenüpunkt "System", Untermenü "Diag. & Statistiken" gehen und den Button "Log-Files herunterladen" anklicken.

16.3 SysLog-Output

Die Protokollierung kann die Daten unter Verwendung von TCP oder UDP an einen SysLog Daemon ausgeben. Für diesen Zweck benötigen Sie einen SysLog Daemon. Dieser Ausgabetyp ist standardmäßig deaktiviert. Sie müssen ihn manuell konfigurieren.

16.4 Aktivierung des SysLogs

1. Öffnen Sie die Datei "**DCEM_HOME/log4j2.xml**" mit einem Texteditor.
2. Suchen Sie den folgenden 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. Löschen Sie die XML Startkommentar- "**<!--**" sowie die Endkommentar-Sequenz "**-->**".
4. Konfigurieren Sie den korrekten Host und Port.
5. Löschen Sie die XML Startkommentar- und Endkommentar-Sequenzen für:

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

6. Starten Sie DCEM neu.

17. PortalDemo

DoubleClue PortalDemo ist eine Testsoftware, die über REST-API mit DCEM kommuniziert und mit der Sie die Funktionen des Produktes DoubleClue testen können, ohne dass die Software zuvor in Ihrem Portal implementiert wurde.

Für die Installation und Bedienung des PortalDemos lesen Sie bitte die separate Beschreibung **DcemInstallation/doc/DC_Manual_PortalDemo.pdf**.

Mit dem PortalDemo können Sie sämtliche Authentifizierungsmethoden testen.

Nach dem Login-Vorgang können Sie die Transaktion "Money Transfer" testen, bei der in der Endnutzer-App eine Push Approval bestätigt werden muss.