

**Installation und VPN- Konfiguration**

**von DoubleClue Enterprise Management (DCEM)**

**auf dem eigenen Server**

**Version: 2.2.1**

Inhaltsverzeichnis

[1. Einführung 4](#_Toc35271442)

[2. Installation und Inbetriebnahme 4](#_Toc35271444)

[2.1 Voraussetzungen 4](#_Toc35271445)

[2.1.1 Hardware-Voraussetzungen 4](#_Toc35271446)

[2.1.2 Datenbank-Voraussetzungen 4](#_Toc35271447)

[2.2 Informationen zur Installation 5](#_Toc35271448)

[2.3 Anforderung der Dateien zur Installation 5](#_Toc35271449)

[2.4 Installation 5](#_Toc35271450)

[2.4.1 Installation auf Windows 5](#_Toc35271451)

[2.4.2 Installation auf Linux 6](#_Toc35271452)

[2.4.3 Installation mit einem Headless-Betriebssystem 7](#_Toc35271453)

[2.5 Datenbank-Konfiguration 7](#_Toc35271454)

[2.5.1 Integrierte Datenbank / “Embedded Database” 7](#_Toc35271455)

[2.5.2 Externe Datenbank 8](#_Toc35271456)

[*2.5.2.3* *Konfiguration einer Postgre-Datenbank als externe DCEM-Datenbank* 11](#_Toc35271457)

[2.6 DCEM unter Linux als Daemon installieren 11](#_Toc35271458)

[2.7 Anmeldung bei DCEM 12](#_Toc35271459)

[2.7.1 Login mit Benutzername und Passwort 12](#_Toc35271460)

[2.7.2 Login mit DoubleClue Multi-Faktor-Authentifizierung 12](#_Toc35271461)

[3. Lizenzierungssystem 13](#_Toc35271463)

[3.1 Beantragung eines Lizenzschlüssels 13](#_Toc35271464)

[3.2 Hinzufügen eines Lizenzschlüssels 13](#_Toc35271465)

[3.3 Lizenzen einsehen 14](#_Toc35271466)

[4. Konfiguration des Client VPN Services via RADIUS am Beispiel von Cisco Miraki 14](#_Toc35271467)

[4.1 Vorbereitung von DCEM als RADIUS-Server 14](#_Toc35271468)

[4.2 Konfiguration von Cisco Meraki 15](#_Toc35271469)

[4.3 Timeout-Konfiguration 15](#_Toc35271470)

[4.4 Timeout-Konfiguration 16](#_Toc35271471)

[4.5 Windows 10 Timeout 16](#_Toc35271472)

[5. Benutzer importieren 17](#_Toc35271473)

[5.1 Integration von Active Directory / Microsoft Azure AD / LDAP 17](#_Toc35271474)

[5.1.1 Hinzufügen einer standardmäßigen Active Directory-Konfiguration 17](#_Toc35271475)

[5.1.2 Hinzufügen einer Azure AD-Konfiguration 18](#_Toc35271476)

[5.1.3 Hinzufügen einer LDAP-Konfiguration 18](#_Toc35271477)

[5.1.4 Import von Benutzern aus Gruppen aus einer Domäne 19](#_Toc35271478)

[6. Verbindung mit dem DoubleClue Dispatcher 20](#_Toc35271479)

[7. E-Mail, Voice Message und SMS-Versand einrichten 22](#_Toc35271480)

[8. Informationen für Benutzer 22](#_Toc35271481)



# Installation und Inbetriebnahme

## 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.

### Datenbank-Voraussetzungen

DCEM wird mit einer integrierten Datenbank (“Embedded Database”) ausgeliefert. Diese ist jedoch nicht Mandantenfähig und bietet weniger Möglichkeiten, Daten über ein Backup abzusichern. Wir empfehlen darum die Verwendung einer externen Datenbank für den produktiven Betrieb.

Derzeit werden 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.

## Informationen zur Installation

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

Sie erhalten das Installationspaket “**DCEM-2.2.1.exe** ”. Wenn Sie DoubleClue auf Linux laufen lassen wollen, kontaktieren Sie bitte [sales@doubleclue.com](mailto:sales@doubleclue.com).

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

## Anforderung der Dateien zur Installation

Erstellen Sie einen DoubleClue-Account unter <https://doubleclue.online/dcem/userportal/login.xhtml>. Wenden Sie sich anschließend an [sales@doubleclue.com](mailto:sales@doubleclue.com) und teilen Sie uns die E-Mail-Adresse mit, auf die der Account registriert wurde und ob Sie DoubleClue einem Windows oder einem Linux-Server installieren möchten. Das DoubleClue-Support-Team wird Ihnen daraufhin in Kürze die benötigte Datei über den CloudSafe zur Verfügung stellen. Sie können die Datei von hier aus herunterladen und auf Ihrem Server installieren.

Bitte beachten Sie, dass der von Ihnen erstellte Account auf <https://doubleclue.online> nicht automatisch in das DCEM auf ihrem Sever importiert wird. Sie müssen sich auf Ihrem Firmen-DCEM neu registrieren.

## 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.

C:\Users\maike.behnsen\Desktop\Grafiken\caution-sign.pngDas 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!

### Installation auf Windows

Starten Sie das Setup, indem Sie die Datei “**DCEM-2.2.1.exe**” ausführen:

1. “Installation on the first DCEM cluster node”:

Wählen Sie diese Option, wenn Sie DCEM zum ersten Mal installieren.

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 Browers 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.

## Datenbank-Konfiguration

DCEM benötigt eine SQL-Datenbank, um betrieben zu werden. Wir empfehlen die Verwendung einer externen Datenbank. Für Testzwecke und Installationen mit geringer Benutzeranzahl steht auch eine “Embedded Database” zur Verfügung. Bei der Verwendung einer Embedded Database können Sie einige der Angaben und Schritte zur Datenbank-Konfiguration überspringen.

Type:

Wählen Sie die Art der Datenbank aus, die Sie verwenden möchte.

JDBC-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.

Database Name:

Geben Sie hier den Namen der Datenbank ein. Wenn Sie die Datenbank neu erstellen, wählen Sie einen aussagekräftigen, einmaligen Namen.

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.)

#### Datenbank oder Schema erstellen (Create Database)

Existiert noch keine Datenbank mit diesem Namen, legen Sie sie unter „Create Database“ an. 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.

#### Datenbanktabelle anlegen

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:Bei der Installation von DCEM wird automatisch ein Benutzer mit Namen SuperAdmin angelegt. Dieser Benutzer hat Zugriff auf sämtliche Bereiche dieser DCEM-Installation und kann sämtliche Änderungen und Einstellungen, die zur Verwaltung von DCEM notwendig sind, vornehmen. Nach der Installation können vom SuperAdmin weitere Benutzer mit Administrationsrechten angelegt werden.

An dieser Stelle können Sie das Passwort für Ihren SuperAdmin festlegen.

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.

C:\Users\maike.behnsen\Desktop\Grafiken\caution-sign.pngWerden 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.

C:\Users\maike.behnsen\Desktop\Grafiken\caution-sign.pngSie können das Setup nun schließen und die Installation von DCEM beenden.

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

### *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‘.

C:\Users\maike.behnsen\Desktop\Grafiken\caution-sign.pngPostgreSQL ist eine casesensitive Datenbank. Entsprechend muss bei allen Einträgen und Suchanfragen auf Groß- und Kleinschreibung geachtet werden.

## Anmeldung bei DCEM

### Login mit Benutzername und Passwort

Die URL zur Anmeldung bei DCEM lautet:

**https:// *--Hostname/IP des Servers--* :8443/dcem/mgt/**

z.B. https://companyServer001:8443/dcem/mgt/

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.

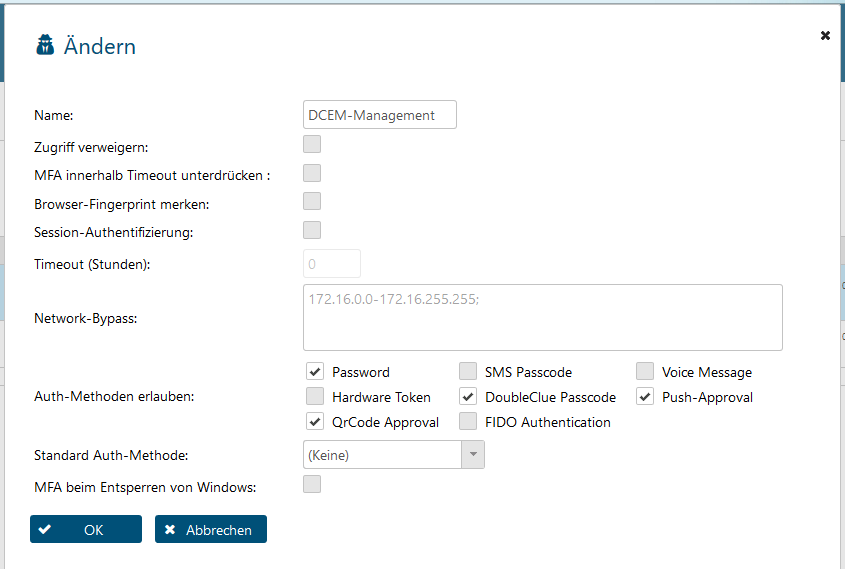
### Login mit DoubleClue Multi-Faktor-Authentifizierung

Es wird empfohlen, dieses Feature zu aktivieren, damit auch Administratoren DoubleClue MFA nutzen, um sich in DCEM einzuloggen.

Achten Sie jedoch darauf, die entsprechende Authentiefizierungsmethode für Ihren SuperAdmin-Account eingerichtet zu haben, bevor Sie die Änderung vornehmen, damit Sie sich nicht selbst aus DCEM aussperren.

#### 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 die Multi-Faktor-Authentifizierungsmethoden, die Sie verwenden möchten. Unter „Standard Auth-Methode“ können Sie eine der ausgewählten Authentifizierungs-Methoden als präferierte Standardmethode auswählen.



Weitere Informationen über die Verwaltung der Authentifizierungsmethoden finden Sie im DoubleClue Benutzerhandbuch, ´Kapitel 7: Authentifizierungsmethoden und Policies`.



# Lizenzierungssystem

Mit der Installation von DCEM wird automatisch eine Testlizenz eingerichtet. Um DoubleClue über den in der Testlizenz vorgesehenen Umfang hinaus nutzen zu können, benötigen Sie einen Lizenzschlüssel.

## Hinzufügen eines Lizenzschlüssels

Um einen neuen Lizenzschlüssel zu beantragen, kontaktieren Sie bitte [sales@doubleclue.com](mailto:sales@doubleclue.com). Bitte lassen Sie uns dabei die folgenden Informationen zukommen, die zur Erstellung eines Lizenzschlüssels benötigt werden:

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

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

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

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.

## Lizenzen einsehen

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

Weitere Informationen zum DoubleClue- Lizenzierungssystem finden Sie im DoubleClue-Benutzerhandbuch ‚Kapitel 16 Lizenzierungssystem‘.

# Konfiguration des Client VPN Services via RADIUS am Beispiel von Cisco Meraki

Es gibt verschiedene VPN-Anbieter. Der Prozess zur Einrichtung von DoubleClue-MFA ist je nach Anbieter unterschiedlich. Bitte schlagen Sie in der Dokumentation Ihres entsprechenden Anbieters nach, wie Sie DoubleClue über in Ihren VPN-Zugriff einbinden können. Bei Fragen und Problemen wenden Sie sich bitte an [support@doubleclue.com](mailto:support@doubleclue.com). Teilen Sie uns bitte direkt mit, welchen VPN-Anbieter Sie verwenden.

## Vorbereitung von DCEM als RADIUS-Server

Sie können DCEM als NAS-Client (Verbindungsclient) für verschiedene RADIUS-Dienste verwenden. Für jeden Dienst muss hierfür unter dem Hauptmenüpunkt „RADIUS“, Untermenü „NAS Clients“ ein neuer Eintrag angelegt 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 oder nicht.

Benutzerpasswort ignorieren

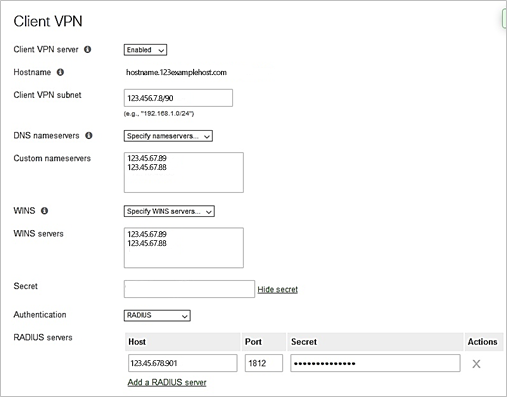
Wenn der NAS-Client das Passwort selbst verifiziert und es nicht an DoubeClue übergibt, muss „Benutzerpasswort ignorieren“ eingeschaltet werden.

1. Gehen Sie in DCEM zum Hauptmenüpunkt „RADIUS“, Submenü „NAS-Clients“, und klicken Sie auf „Hinzufügen“.
2. Die „IP-Nummer“ muss die Quell-IP der CISCO Meraki-Anwendung sein.
3. Setzen Sie in der Checkbox „Challenge verwenden“ keinen Haken.
4. Klicken Sie auf „OK“. Die Konfiguration wird sofort danach wirksam sein.

## Konfiguration von Cisco Meraki

Richten Sie im Cisco Meraki Dashboard im Bereich ‚Security & SDWAN‘ Unterbereich ‚Client VPN‘ DCEM als RADIUS-Server für Cisco Meraki ein.

Hier können Sie eine typische RADIUS-Konfiguration von CISCO Meraki sehen.

**

Bitte überprüfen Sie, dass der Port mit demjenigen, welchen Sie in DCEM konfiguriert haben und den Sie unter dem Hauptmenüpunkt „System“, Untermenü „Cluster-Konfigurationen“, Eintrag „RADIUS Authentication“ einsehen und konfigurieren können, übereinstimmt.

## Timeout-Konfiguration

DoubleClue verwendet mobile Endgeräte für die MFA. Während der Authentifizierungsphase benötigt der Benutzer möglicherweise einige Zeit, um sein Mobilgerät einzuschalten, die DoubleClue-App zu starten und die Meldungen zu bestätigen.

Der Standard-Timeout für CISCO Meraki ist 5 Sekunden für 3 Versuche. Dies bedeutet, dass Benutzer insgesamt nur 15 Sekunden haben, was möglicherweise zu kurz ist. Wir empfehlen, die Timeout-Dauer zu verlängern.

Sie können die Timeout-Dauer in der Konfigurations-GUI von CISCO Meraki nicht ändern. Bitte kontaktieren Sie für Änderungen den Meraki-Support unter <https://meraki.cisco.com/support/>

Wir empfehlen 60 Sekunden x 3 Versuche.

## Windows 10 Timeout

Der Standard-Timeout des Windows 10 VPN Client beträgt 30 Sekunden, was möglicherweise zu kurz für den Benutzer ist, um sein Mobilgerät einzuschalten und die Authentifizierungsmeldung zu bestätigen.

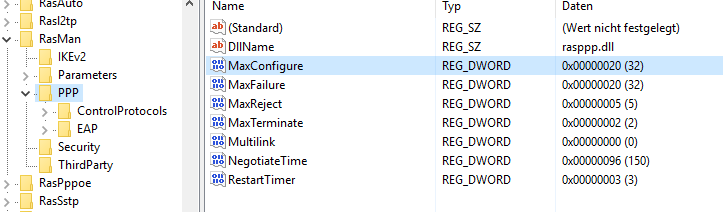
Um die Dauer bis zum Timeout zu verlängern, müssen Sie in der Windows-Registrierung die folgenden Einstellungen ändern.

Wir empfehlen, die Dauer ebenfalls auf 3 Minuten zu erhöhen. Der Windows 10 Client wiederholt mit einer Rate von 3 Sekunden, daher wird die Anzahl der Wiederholungen auf 60 gesetzt:

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\PPP\MaxConfigure = 60 (decimal)*

und

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\PPP\MaxFailure = 60 (decimal)*



# Benutzer importieren

Sie können Ihr Active Directory mit DoubleClue synchronisieren und so Benutzer direkt in DoubleClue importieren. Da DoubleClue die Verwendung mehrerer Domänen unterstützt, müssen Sie hierbei darauf achten, dass jeder Domain-Eintrag einen einzigartigen Namen hat, um Benutzer korrekt zuordnen zu können.

## Integration von Active Directory / Microsoft Azure AD / LDAP

DCEM unterstützt drei Domain-Typen:

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

Ihre Benutzer können sich gegenüber der Domäne mit Ihrem Benutzernamen 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.

C:\Users\maike.behnsen\Desktop\Grafiken\caution-sign.pngBitte beachten Sie: Haben Sie eine Domäne einmal konfiguriert und den entsprechenden Domain-Typ gewählt, kann diese Auswahl nicht mehr verändert werden.

### 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.

### Hinzufügen einer Azure AD-Konfiguration

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

<https://doubleclue.com/ressourcen/#handbuecher>

### 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.

Timeout in Sek:

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

### 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-Anmeldenamen des Benutzers trennt (wird z.B. der Benutzer “max.muster” aus der LDAP-Domain “BEISPIELDOMAIN” importiert, ist sein Anmeldename “BEISPIELDOMAIN\max.muster”).

C:\Users\maike.behnsen\Desktop\Grafiken\caution-sign.pngEin 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.

C:\Users\maike.behnsen\Desktop\Grafiken\caution-sign.png Bitte beachten Sie: DCEM speichert keine Domain-Passwörter von Benutzern.

* + - 1. *Admin-Einstellung „enableUserDomainSearch“*

Unter „Administration“ im Untermenüpunkt “Einstellungen” können Administratoren auswählen, ob sich Benutzer mit ihrem vollständigen Anmeldenamen inklusive ihres Domain-Namens (z.B. BEISPIELDOMAIN\max.muster) 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.

Wir das Häkchen gesetzt, kann sich ein Benutzer nur mit seinem Benutzernamen („max.muster“) oder seiner UPN anmelden. Dies kann jedoch zu Problemen führen, wenn in den verschiedenen Domains Benutzer mit dem gleichen Namen vorhanden sind. Hier wird dann immer nur der Benutzer aus der Domäne mit der höchsten Priorität gefunden.

# Verbindung mit dem DoubleClue Dispatcher

Wenn Sie die offizielle DoubleClue-App benutzen möchten, müssen Sie Ihre DCEM Installation beim cloudbasierten DoubleClue-Dispatcher registrieren.

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.

Um Ihre DCEM-Installation beim DoubleClue Dispatcher zu registrieren, laden Sie zunächst die **SdkConfig.dcem-**file herunter. Wechseln Sie zum Hauptmenüpunkt “Identity-Management”, Untermenü “Versios”, und erstellen Sie die SDK-Konfigurationsdatei.

Das Feld URL sollte automatisch ausgefüllt werden. Die eingetragene URL wird nach dem folgenden Schema aufgebaut:

**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.

Klicken Sie auf „Download SDK Configuration“ und speichern Sie die **SdkConfig.dcem-**file auf Ihrem Rechner.

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](mailto:support@doubleclue.com), um Ihr DCEM-Cluster beim DoubleClue-Dispatcher zu registrieren.

Wenn Sie eine eigene App verwenden möchten, finden Sie weitere Informationen im [DCEM Benutzerhandbuch](https://doubleclue.com/ressourcen/#handbuecher) „Kapitel 6: Verbindungsszenarien“.

# E-Mail, Voice Message und SMS-Versand einrichten

Damit DCEM selbstständig E-Mails und SMS an die Benutzer schicken kann, müssen diese entsprechend konfiguriert werden. Diese Konfiguration können Sie im Bereich Hauptmenü „System“, Untermenü „Einstellungen“ vornehmen. Füllen Sie hier die Bereiche ‚E-Mail SSL/TLS Configuration‘ und ‚SMS Configuration‘ aus.

Die Informationen, die Ihnen zur Konfiguration der E-Mail SSL/TLS-Verbindung benötigt werden, erhalten Sie von dem Host, bei dem Ihr E-Mail-Server verwaltet wird. Bitte prüfen Sie in Ihrem Account nach, ob Ihnen die Informationen dort zur Verfügung gestellt werden. Wenn nicht, fordern Sie sie bei Ihrem Host Service an. Das Feld ‚E-Mail from Person‘ können Sie selbstständig ausfüllen. Hier wird der Name eingetragen, der als Absender der E-Mail erscheint. Wir empfehlen einen aussagekräftigen Namen zu wählen, den Empfänger schnell zuordnen können.

Um SMS und Voice-Mail zu verwenden, müssen Sie außerdem SMS-Credits von [www.messagebird.com](http://www.messagebird.com) erwerben. Bitte beachten Sie, dass es sich bei Messagebird um einen unabhängigen Drittbanbieter handelt.

SMS und Voice Messages werden nicht in verschlüsselter Form über die Leitungen versendet.

# Informationen für Benutzer

Lassen Sie ihren Benutzern die URL für das DobleClue UserPortal zukommen. Diese wird nach dem Muster **https://hostname/dcem/userportal/** gebildet.

Der Benutzername entspricht dem aus der Domain importierten Benutzernamen. DoubleClue unterstützt außerdem UPN, entsprechend ist auch die Anmeldung mit E-Mail-Adresse möglich.

Das Passwort entspricht dem Benutzerpasswort, das in der Domain hinterlegt ist. Es kann vom Benutzer nicht geändert werden. Wir das Domainpasswort geändert, ändert sich automatisch auch das DoubleClue-Passwort.