



Schnellinstallations- anleitung

für DoubleClue Enterprise Management (DCEM)
auf dem eigenen Server


Version: 2.8.4

Inhaltsverzeichnis

1. Einführung.....	3
2. Installation und Inbetriebnahme von DCEM	3
2.1 Server-Anforderungen	3
2.2 Client-Anforderungen	3
2.3 Installation	4
2.3.1 Windows Installation	4
2.3.2 Linux Installation	5
2.4 Datenbank-Konfiguration	5
2.4.1 Integrierte Datenbank / “Embedded Database”	6
2.5 Login bei DCEM als Administrator	8
3. DCEM-Konfiguration	8
3.1 Erstellung eines Benutzers.....	8
4. Einrichtung der DoubleClue-App	9
4.1 Registrierung von DCEM beim DoubleClue-Dispatcher.....	9
4.1.1 Common Name des Zertifikats und Hostname.....	9
4.1.2 Umleitung über den DoubleClue Dispatcher einrichten.....	10
4.2 Herunterladen der DoubleClue App	13
4.3 App-Aktivierung	13
5. Anmelden im DoubleClue UserPortal.....	14
6. Deinstallation.....	14
6.1 Windows Deinstallation.....	14
6.2 Linux Deinstallation.....	15

1. Einführung

Diese Anleitung ist dazu gedacht, die “DoubleClue Enterprise Management”-Software (DCEM) schnell mit **einer integrierte SQL-Datenbank** sowie **Windows oder Linux als Betriebssystem** einzurichten. Alle Komponenten werden auf derselben Maschine installiert.

 Es werden IT-Grundkenntnisse benötigt, um “DoubleClue Enterprise Management” (DCEM) installieren und einrichten zu können.

Bitte beachten Sie, dass die integrierte Datenbank nicht mandantenfähig ist. Wenn Sie eine DoubleClue-Installation mit mehreren Mandanten benötigen, folgen Sie bitte der Anleitung im DoubleClue Manual.

2. Installation und Inbetriebnahme von DCEM


2.1 Server-Anforderungen

- RAM: Minimum 4 GB (abhängig von der Benutzeranzahl)
- Festplatte: Minimum 20 GB
- Betriebssystem: Windows 64 Bit oder Linux 64 Bit
- DNS-Einträge im internen Firmennetzwerk sowie extern
- Standardmäßige Netzwerk-Ports:
 - 8443 für das Management
 - 433 für die App-Verbindung
 - 8001 für REST Web-Services

2.2 Client-Anforderungen

Wenn Sie beabsichtigen, Push Approval, QR-Code Approval oder DoubleClue Passcode als Authentifizierungsmethoden zu verwenden und deshalb die DoubleClue-App benötigen, gelten außerdem die folgenden Anforderungen:

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

 Port 443 ist der Standard-Port für die Apps. Dieser Port muss vom Internet aus erreichbar sein. Bitte öffnen Sie diesen Port in Ihrer Firewall.

2.3 Installation

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

Sie können DCEM auf Windows 64bit oder Linux 64bit-Maschinen installieren.

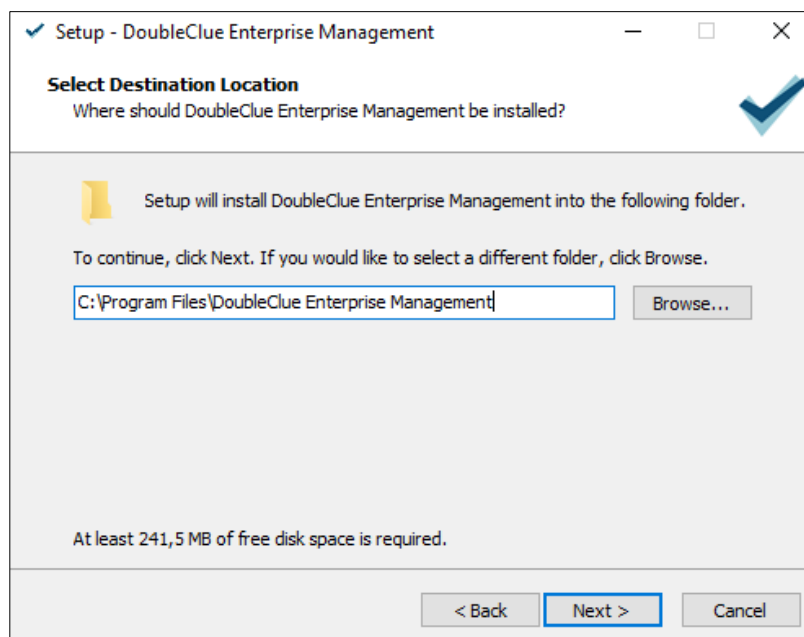
Nach der Installation läuft DCEM als ein Service auf Windows oder als ein Daemon auf Linux. Bevor DCEM gestartet werden kann, muss zunächst das Setup ausgeführt und eine Datenbank sowie weitere Einstellungen konfiguriert werden.

Das Setup muss nur einmal ausgeführt werden. Es ist nur in Englisch verfügbar.

2.3.1 Windows Installation

Starten Sie das Setup, indem Sie die Datei **“DCEM-X.X.X.exe”** (X.X.X steht für die Versionsnummer der Datei) mit Administratorrechten ausführen.

1. Wenn Sie eine Warnung von Windows erhalten, klicken Sie auf ‚Weitere Informationen‘ und wählen Sie dann ‚Trotzdem Ausführen‘.
2. Wählen Sie das Verzeichnis, in welchem Sie DCEM installieren möchten



3. Wählen Sie „Install first DCEM cluster node“ und klicken Sie auf „Next“.
4. Geben Sie einen Namen für den Startmenü-Ordner ein oder lassen Sie den voreingestellten Namen.
5. Nun werden die DCEM-Installations-Dateien in das Installationsverzeichnis kopiert.
6. Das Setup Web wird in einem Command Window gestartet.
7. DoubleClue wird nun versuchen, dass Setup automatisch in Ihrem Standardbrowser zu starten. Wenn sich der Browser nicht automatisch öffnet, starten Sie ihn manuell und geben Sie den folgenden Link ein: <https://localhost:8443/setup?start=yes>

8. Das Setup verwendet eine gesicherte HTTPS-Verbindung mit einem selbstsignierten Zertifikat. Deshalb wird beim Verbinden im Browser eine Sicherheitswarnung angezeigt. Bestätigen Sie diese Warnung und fügen Sie die Verbindung als Ausnahme hinzu.
9. Konfigurieren Sie die Datenbank, wie im Kapitel [2.4 Datenbank-Konfiguration](#) beschrieben.
10. Nachdem die Datenbank konfiguriert wurde, schließen Sie die DoubleClue-Setup-Anwendung.
11. Das Setup wird nun DCEM als einen Windowsservice installieren.

2.3.2 Linux Installation

Extrahieren Sie als erstes die Datei **“DCEM-Linux-X.X.X.tar.gz”**.

1. Öffnen Sie die Konsole und navigieren Sie zum Elterninstallationsverzeichnis.
2. Geben Sie nun **“tar -xvf DCEM-Linux-X.X.X.tar.gz”** ein, um die Datei in das entsprechende Verzeichnis zu entpacken.
3. Gehen Sie 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. Ansonsten öffnen Sie den Browser und geben Sie den folgenden Link ein: <https://your-host-name:8443/setup?start=yes>
4. 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 und fügen Sie die Verbindung als Ausnahme hinzu.
5. Konfigurieren Sie die Datenbank, wie im Kapitel [2.4 Datenbank-Konfiguration](#) beschrieben, fort.
6. Nachdem das DoubleClue Setup abgeschlossen ist, installieren und starten Sie DCEM als Daemon, indem Sie zum Verzeichnis **„DCEM/sh“** gehen und dort die Datei **„installDcemDaemon.sh“** ausführen.
7. Sie können den Daemon jederzeit stoppen oder starten, indem Sie die Datei **„stopDcemDaemon.sh“** oder **„startDcemDaemon.sh“** ausführen.

2.4 Datenbank-Konfiguration

DCEM benötigt für den Betrieb eine SQL-Datenbank.

Für Testzwecke können Sie sich für eine vorinstallierte integrierte Datenbank (“Embedded Database”) entscheiden. Wenn Sie eine externe Datenbank installieren möchten, finden Sie die Anleitung dafür im DCEM Benutzerhandbuch. DoubleClue unterstützt die folgenden externen Datenbanken:

- MS SQL
- MariaDB
- My SQL
- PostgreSQL


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
Administrator Name *
root
Administrator Password
Current Node-Name
HWS001L0187
New Node-Name
HWS001L0187
Save
Local configuration file stored at: D:\DCEM\DoubleClue Enterprise Management\DCEM_HOME\configuration.xml
Next

1. Wählen Sie den Datenbank-Typ “Embedded-Database” aus.

 Bitte beachten Sie: Die integrierte Datenbank unterstützt keine multiplen DCEM-Knoten oder mehrere Mandanten!

2. DoubleClue Node Name: Als Node Name wird standardmäßig Ihr Computer- oder Hostname oder alternativ Ihre IP-Adresse eingetragen. Sie können diesen Namen übernehmen oder einen anderen eintragen.
3. Die restlichen Eingabefelder werden bei der Verwendung einer integrierten Datenbank nicht benötigt und sind aus diesem Grund deaktiviert.
4. Klicken Sie auf „Save“ wenn Sie alle Einstellungen vorgenommen haben.
5. Bestätigen Sie die Warnung und klicken Sie dann auf “Next”, um mit dem Setup fortzufahren.
6. Super-Administrator Password: Legen Sie das Passwort für den Super-Administrator von DCEM fest. Der Benutzername des Super-Administrators ist immer “SuperAdmin”.
7. DoubleClue Server URL: Geben Sie die URL ein, über die Benutzer Ihr DoubleClue von einem externen Zugriffsort aus erreichen können.

Setup - Configuration

Database Configuration
Create Database
Create Database Tables


Create-Tables Administrator Name:
?

Create-Tables Administrator Password:

SuperAdmin Password: *

Confirm SuperAdmin Password: *

DoubleClue Server URL *

 Create Tables

Back

8. Klicken Sie auf "Create Tables".
9. Bestätigen Sie die Meldung, die Ihnen daraufhin angezeigt wird.

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

Setup - Configuration

Database Configuration
Create Database
Create Database Tables

Setup is Ready

Close setup application and afterwards install and run DCEM as a service by running the script **'installDcemServer'**
Wait till DCEM has started and proceed with this URL:

<https://HWS001L0131:8443/dcem/mgt>

 Close DoubleClue Setup

Back

Nachdem das Setup geschlossen ist, wird DCEM gestartet. Dieser Prozess dauert normalerweise 30-50 Sekunden, selten länger. Wenn Sie versuchen, den DCEM-Link in dieser Zeit zu öffnen, erhalten Sie eine Fehlermeldung. Wenn Sie sich versichern möchten, dass DCEM bereits gestartet wurde oder vermuten, dass während des Starts ein Fehler aufgetreten ist, überprüfen Sie die dcem.log-Datei. Sie finden die Datei im DCEM-Installationsverzeichnis unter DCEM_Home > logs.

Manchmal muss man den DCEM Service manuell starten. Gehen Sie dafür in das Installationsverzeichnis unter bat und führen Sie die **startDcemService.bat** aus.

2.5 Login bei DCEM als Administrator

Die URL für die Anmeldung bei DCEM ist:

<https://localhost:8443/dcem/mgt/login.xhtml>

Loggen Sie sich mit dem Benutzernamen "SuperAdmin" und dem Passwort, das Sie während des Setups festgelegt haben, ein.

Nach der Anmeldung können Sie DCEM administrieren.

3. DCEM-Konfiguration

In diesem Kapitel erklären wir Ihnen die ersten Schritte eines DCEM-Konfigurations-Prozesses, der es Ihnen ermöglicht, eine **DoubleClue Windows Desktop-Applikation** mit DCEM zu verbinden und anzuwenden.

DoubleClue unterstützt die folgenden Authentifizierungsmethoden:

- Push Approval (mit DoubleClue-App)
- QR-Code Approval (mit DoubleClue-App)
- DoubleClue Passcode (mit DoubleClue-App)
- FIDO U2F and FIDO2 Token
- Passwort
- SMS Passcode
- Voice Message
- OTP Token

3.1 Erstellung eines Benutzers

DoubleClue-Benutzer benötigen einen registrierten Benutzeraccount, um DoubleClue zu verwenden.

1. Gehen Sie zum Hauptmenüpunkt "Administration", Untermenü "Benutzer".
2. Klicken Sie auf „Hinzufügen +“. Sie können nun auswählen, ob Sie einen „Lokalen Benutzer“ oder einen „Domainbenutzer“ anlegen möchten. Füllen Sie die benötigten Felder aus.

Lokale Benutzer erhalten in diesem Schritt ein “Initialpasswort”, über das Sie sie informieren müssen, damit Sie ihre DoubleClue-App aktivieren oder sich in UserPortal anmelden können.

 **Hinzufügen**

Typ: ☒ Lokaler Benutzer ☐ Domainbenutzer

Anzeigename:

Anmeldename:

Initialpasswort:

E-Mail:

Telefonnummer:

Mobilnummer:

Gesperrt: ☐

Sprache: ▼

Rolle: ▼

☒ OK ☒ Abbrechen

4. Einrichtung der DoubleClue-App

4.1 Registrierung von DCEM beim DoubleClue-Dispatcher

Um die DoubleClue App zu nutzen, müssen Sie Ihre DCEM-Installation beim globalen DoubleClue Dispatcher anmelden, einem DCEM-Cluster, das von der *HWS Informationssysteme GmbH* verwaltet wird. Im folgenden Abschnitt leiten wir Sie durch die zur Registrierung notwendigen Schritte.

4.1.1 Common Name des Zertifikats und Hostname

Um die Verbindung Ihres DCEMs mit dem globalen DoubleClue-Dispatcher vorzubereiten, prüfen Sie zunächst ob ein geeigneter KeyStore angelegt ist.

Bei der Installation wird ein Standardserverzertifikat für SSL/TSL Geräte-Websockets angelegt („**DeviceWebSockets_CA**“). Der Common Name (CN) des Zertifikats wird dabei dem URL-Hostnamen des Browsers gleichgesetzt. Wenn Sie eine Internet-Host-Adresse verwenden möchten, deren Bezeichnung sich vom CN des automatisch angelegten Keystores unterscheidet, generieren Sie einen neuen „**DeviceWebsockets_CA**“-Keystore und geben Sie als Common Name den Namen der Internet-Host-Adresse ein.

Gehen Sie dafür zum Hauptmenübereich „System“, Submenu „KeyStores“ und gehen Sie auf „Neuen KeyStore generieren“.

The screenshot shows the 'KeyStores' management interface. At the top, there is a toolbar with buttons: 'Neuen KeyStore generieren' (circled in red), 'Download als PEM', 'Download als PKCS#12', 'Upload', 'Passwort anzeigen', and 'Löschen'. Below the toolbar is a table of existing KeyStores with columns for 'Knoten' and 'Name'. The table contains 7 entries, with names like 'DCEM-01' and 'DCEM-02'. A modal window titled 'Neuen KeyStore generieren' is open, showing a form with the following fields: 'Verwendungszweck' (dropdown menu, circled in red, showing 'DeviceWebsockets_CA'), 'Knoten' (dropdown menu, showing 'Auswählen'), 'Common Name (Hostname): *' (text input, showing 'TESTCOMPANY'), 'Host-IP-Nummer (optional):' (text input), and 'Läuft ab am: *' (date input, showing '05-12-2069'). At the bottom of the modal are two buttons: 'Neuen KeyStore generieren/ersetzen' and 'Schließen'.

4.1.2 Umleitung über den DoubleClue Dispatcher einrichten

Es gibt zwei Möglichkeiten DoubleClue Apps über den DoubleClue Dispatcher zum DCEM auf dem eigenen Server umzuleiten: direkt oder über Reverse Proxy.

4.1.2.1 Direkte Weiterleitung

Voraussetzung: DCEM Serverport 443 muss vom Internet aus erreichbar sein.

Überprüfen Sie in DCEM unter ‚System‘ > ‚Clusterkonfiguration‘, dass der Verbindungsdienst für die Smart-Device Web-Sockets aktiv ist. Hier können Sie auch den Serverport ändern, wenn Sie einen anderen Port als 443 verwenden möchten. Bitte achten Sie darauf, dass dieser Port ebenfalls über das Internet aus erreichbar sein und gegebenenfalls bei Ihrem Router extra freigegeben werden muss.

Bei der Aktivierung einer App verifiziert der Dispatcher die Benutzer-ID und den Aktivierungscode bei der DCEM-Installation.

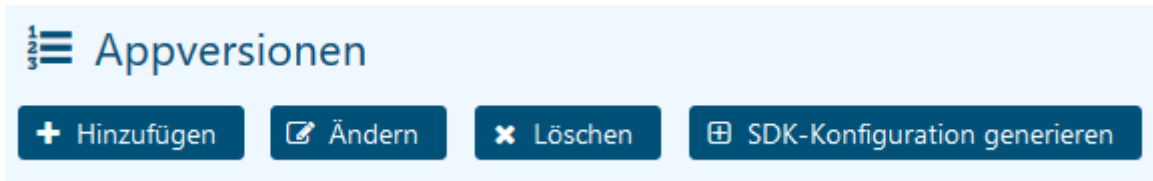
Wenn die Benutzer-ID und der Aktivierungscode gültig sind, schickt der Dispatcher die DCEM „SdkConfig.dcem“-Metadatendatei zum Endnutzergerät. Bei der Anmeldung verbindet sich dann das Gerät direkt mit Ihrer DCEM-Installation.



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

Die Datei „**SdkConfig.dcem**“ enthält Sicherheitsinformationen über DCEM, welche benötigt werden, um eine vertrauenswürdige Verbindung zu Ihrer DCEM-Installation herzustellen. Im Folgenden erklären wir, wie Sie die SdkConfig.dcem erstellen können.

1. Gehen Sie zum Hauptmenüpunkt “Identity & Access”, Untermenü “Appversionen” und klicken Sie auf den Button “SDK-Konfiguration generieren”.



2. Überprüfen Sie die Angaben im Dialogfenster. Die DCEM-Server-URL und der Port müssen vom Internet aus erreichbar sein. Die DCEM-Server-URL muss ebenfalls identisch mit dem Common Name “CN” des “**DeviceWebSockets_CA**”-Keystore-Zertifikats sein. Siehe hierzu Kapitel [4.3 Common Name des Zertifikats und Hostname](#). Wenn Sie die UserPortal-URL ändern möchten, können Sie dies hier tun. Wenn Sie mit der SDK-Konfiguration fertig sind, speichern Sie sie und laden Sie sie herunter.

SDK-Konfiguration generieren

DCEM-Server-URL, welche für die App erreichbar ist

Benutzerportal URL

SSL/TLS-TrustStore-Zertifikat


Quelle:

Vertrauenswürdige Zertifikate		
Ausgestellt von	Ausgestellt für	Gültig bis
Keine Einträge vorhanden.		

3. Wählen Sie einen kurzen, global einzigartigen Namen aus, damit wir Ihre DCEM-Installation gegenüber dem Dispatcher identifizieren können. Dieser Name wird von Ihren Benutzern bei allen zukünftigen Anmeldungen gebraucht werden und wird als “Realm-Name” bezeichnet. Nach der erfolgreichen Registrierung wird er unter dem Hauptmenüpunkt “Identity & Access”, Untermenü “Einstellungen” sichtbar sein.
4. Senden Sie die heruntergeladene Datei “**Sdk.Config.dcem**” zusammen mit Ihrem gewählten Realm-Namen an support@doubleclue.com zur Registrierung.

4.1.2.2 Weiterleitung über Reverse-Proxy

In diesem Szenario verbindet sich Ihr DCEM mit dem globalen DoubleClue Dispatcher. Entsprechend verbinden sich die Geräte der Benutzer nicht direkt mit Ihrem DCEM und Sie müssen keine Firewallports öffnen. Alle Daten, die zwischen der App und DCEM ausgetauscht werden, werden per Reverse-Proxy durch den globalen DoubleClue-Dispatcher weitergeleitet.

 Bitte beachten Sie: Die Reverse-Proxy-Verbindung sollte NICHT in einer produktiven Umgebung verwendet werden!

4.1.2.2.1 Registrierung von DCEM beim DoubleClue-Dispatcher

Wählen Sie einen Realm-Namen, der benötigt wird, um Ihr DCEM-Cluster gegenüber dem DCEM-Dispatcher zu identifizieren. Wir schlagen vor, den Namen Ihrer Firma als Realm-Namen zu verwenden. Der Realm-Name muss für den Dispatcher einzigartig sein.

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

4.1.2.2.2 Konfiguration von DCEM für die Reverse-Proxy-Verbindung

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



Konfigurieren

Reverse-Proxy aktivieren: ☐

Realm-Name:

Passwort:

Zeit für Wiederverbindung (Minuten):

'ReverseProxy.dcem' hochladen:

Reverse-Proxy aktivieren: Setzen Sie den Haken in dieser Box.

Realm-Name: Dies ist der einzigartige Realm-Name, den Sie wählen, um Ihr DCEM-Cluster gegenüber dem DCEM-Dispatcher zu identifizieren.

Passwort: Geben Sie das Passwort ein, welches Ihnen vom DoubleClue-Team zugesendet wurde.

Zeit für Wiederverbindung (Minuten): Hier können Sie das Intervall eintragen, in welchem Ihre DCEM-Installation versucht, eine erneute Verbindung mit dem DoubleClue-Reverse-Proxy herzustellen, falls ein Verbindungsversuch fehlgeschlagen ist.

'ReverseProxy.dcem' hochladen: Laden Sie die Datei "**ReverseProxy.dcem**", die Ihnen vom DoubleClue-Team zugeschickt wurde, hoch.

4.2 Herunterladen der DoubleClue App

Benutzer können die DoubleClue App aus dem [Google Play Store](#) oder dem [App Store](#) herunterladen. Die Windows Desktop App kann von www.doubleclue.com heruntergeladen werden.

Standardmäßig verbindet sich die DoubleClue App immer mit dem DoubleClue-Dispatcher auf <https://doubleclue.online>. Benutzer müssen ihren Realmenamen verbunden mit einem Dollarzeichen '\$' zu ihrem Benutzernamen hinzufügen, um sich mit einem DCEM auf einem Firmenserver zu verbinden. Wenn dem Benutzer der Aktivierungscode per E-Mail zugesendet wird, wird ihm auch gleich seine komplette Login ID in der E-Mail mitgeteilt.

4.3 App-Aktivierung

Ein DoubleClue-Benutzer benötigt einen Aktivierungscode, um sich zum ersten Mal mit der DoubleClue-App auf einem Gerät anzumelden. Im Folgenden erklären wir, wie Sie einen solchen Aktivierungscode generieren können:

1. Gehen Sie zum Hauptmenüpunkt "Identity & Access" zum Untermenü "Aktivierungscodes".
2. Klicken Sie auf den Button "Hinzufügen".

Hinzufügen

Domain: {local}

Benutzer: max.muster

Gültig bis: 01.04.2019 10:09

Info:

Aktivierungscode senden per: EMAIL

✓ OK ✕ Abbrechen

3. Klicken Sie auf den Benutzer und dann auf den Button „Aktivierungscode anzeigen“, um diesen Aktivierungscode anzusehen. Um Aktivierungscodes direkt mittels E-Mail oder SMS an einen Benutzer senden zu können, müssen Sie die E-Mail und SMS-Settings unter „System“ > „Einstellungen“ konfigurieren. Weitere Informationen finden Sie im DCEM Manual.
4. Starten Sie die DoubleClue-App auf Ihrem Smartgerät. Wenn Sie die App zum ersten Mal benutzen, sehen Sie eine kurze Einführung, bis Sie zum ‚Konto hinzufügen‘-Bereich kommen.
5. Fügen Sie Ihr Konto entweder durch Eingabe des alphanumerischen Aktivierungscodes oder Scannen des QR-Codes zur App hinzu.
6. Am Ende des Aktivierungsprozesses werden Sie automatisch in der App angemeldet. Die App ist nun aktiviert.

Wenn Sie während dem Hinzufügen des Kontos oder bei der Anmeldung eine Fehlermeldung erhalten, die sagt, dass diese Version **auf dem Server nicht registriert** ist, loggen Sie sich in DCEM ein und gehen Sie zum Menü „Identity & Access“ > „Einstellungen“. Überprüfen Sie ob bei ‚Automat. App-Versionregistrierung aktivieren‘ ein Haken gesetzt ist. Wenn der Haken nicht gesetzt ist, fügen Sie die aktuelle Version unter „Appversionen“ in die Liste hinzu.

5. Anmelden im DoubleClue UserPortal

UserPortal ist ein Self-Service-Webportal für DoubleClue-Benutzer. In UserPortal können DoubleClue-Benutzer ihre Authentifizierungsgeräte selbst verwalten und erhalten Zugriff auf CloudSafe und PasswordSafe. Die URL zum UserPortal ist wie folgt aufgebaut: <https://dein-host-name:8443/dcem/userportal>

Loggen Sie sich zunächst mit Ihrem Benutzernamen und Passwort ein. Sie werden dann zu einem Fenster weitergeleitet, in der Sie eine Multi-Faktor-Authentifizierungsmethode auswählen können. Wählen Sie „Push Approval“ und melden Sie sich mit Hilfe der DoubleClue-App an.

Sie erhalten eine Bestätigungsmeldung, wenn Sie die Push Approval validiert haben und werden erfolgreich in DoubleClue UserPortal eingeloggt.

6. Deinstallation

6.1 Windows Deinstallation

Sie können DCEM einfach über die Systemeinstellungen deinstallieren.

1. Drücken Sie die Win + X-Taste, um die Windows-Suche zu öffnen
2. Suchen Sie „Programme hinzufügen und entfernen“
3. Wählen Sie in der Liste „DoubleClue Enterprise Management“ aus
4. Klicken Sie auf den Deinstallieren-Button, der Ihnen angezeigt wird, nachdem Sie DCEM ausgewählt haben. DCEM wird jetzt deinstalliert.

6.2 Linux Deinstallation

Auf einem Linux-System können Sie DCEM deinstallieren, indem Sie die `uninstallDcemDaemon.sh` ausführen.

1. Öffnen Sie die Konsole und navigieren Sie zum DCEM-Installationsverzeichnis.
2. Stoppen Sie DCEM indem Sie die Datei „**stopDcemDaemon.sh**“ ausführen.
3. Deinstallieren Sie DCEM anschließend, indem Sie die Datei „**uninstallDcemDaemon.sh**“ ausführen.