DoubleClue White Paper

1. Introduction

The Identity & Access Management (IAM) Software *DoubleClue* makes the administration of identities as well as the management of access rights to various applications, systems and networks possible. A Multi-Factor Authentication (MFA) with seven different authentication methods is the key element of the IAM solution.

2. Access Policies

In DoubleClue Enterprise Management, central access policies can be set. These policies define which users are allowed to access which application/s with which authentication method/s.

2.1 Options

- Assignment of unique policy names
- Refraining of MFA within a specific time frame:
  After using MFA, a user can authenticate themselves by user name/password for a certain period of time.
- Browser Fingerprint:
  Calculation of a unique browser fingerprint for the distinct identification of a used browser/ device. The user can authenticate themselves by user name/password for a certain period of time if the Browser Fingerprint matches. You will find an open source solution to create a Browser Fingerprint as well as detailed information here:
  https://github.com/Valve/fingerprintjs2
- Network Bypass:
  A user who connects with the application from a network that was excepted by the Network Bypass function can also authenticate themselves by user name/password. We support IPv4 and IPv6.
- Choice of authentication methods:
  Authentication methods which a user is allowed to use can be (de-)activated. If required, the user can choose from the pre-configured authentication methods themselves.
- Default authentication method:
  The user uses this default authentication method. In exceptional cases, they can use one of the pre-configured authentication methods by putting a certain prefix before their login ID.

2.2 Assigning Policies

DoubleClue supports four application types: RADIUS, SAML, REST-WebServices and Auth-Remote Gateway.

Access rights can be assigned to application types, applications (e.g. Cisco Meraki, Citrix ShareFile, Dropbox etc.) and user groups within an application or application type.

Policy assignments are hierarchically inherited according to the following schema:

a) If a user is a member of a group and this group has an assigned policy, the policy of this group applies to the user as well.
b) If a user is a member of several groups and these groups have different assigned policies, the policy of the group that has the highest weight is taken for the user.
c) If a user is a member of several groups, but these groups have no assigned policies, or if the user is no group member, the policy assigned to the respective Application is used for them.
d) If an Application has no assigned policy, the policy assigned to the Application Type is chosen for the user.
e) If an Application Type has no assigned policy, the “Global-Policy” is assigned to the user.

2.3 Global Policy

If no policy has been assigned to an application, DCEM will use the “Global-Policy” which cannot be deleted.

3. Authentication Methods

Based on a cluster farm as single point of administration, users are authenticated by DoubleClue for various applications. Users have the option to choose from several authentication methods.

3.1 Password

A user logs in with user name and password only. This classic option is meant for applications in certain trusted networks for which an MFA is not absolutely essential.

3.2 SMS Passcode

In addition to an authentication with password, a random passcode is created that is sent to the user’s mobile phone via SMS. The SMS Passcode is transmitted without any encryption!

3.3 Voice Message

In addition to an authentication with password, a randomly generated passcode is transmitted via call to a user's mobile phone or landline.

3.4 Hardware Token

In addition to an authentication with password, a one-time passcode (OTP) is generated by a hardware token.

3.5 DC App Passcode

Users generate an offline passcode with their DoubleClue App if no internet connection is available.

3.6 Secure QR Code

The one-click authentication method is based on a PKI Private Key 2048 Bit certificate and a random AES-256 encryption algorithm. Users scan a QR code with their DoubleClue App. The QR code key is usually valid for only two minutes.

3.7 DC Secure Message

The most secure authentication method is based on a PKI Private Key 2048 Bit certificate. Users receive a push notification on their smartphone. After they have logged into their DoubleClue App, they can confirm or reject secure messages and transactions.

The secure messages are HTML-formatted and pre-configured as templates with placeholders.

Responses are digitally signed and verified at DoubleClue Enterprise Management.

4. DoubleClue App

4.1 Universal DoubleClue App

The default DoubleClue App is provided for Android, iOS, Windows Desktop, MAC and Linux. It can be directly downloaded from Google Playstore or the App Store. Please contact support@doubleclue.com for other operating systems.

After the installation, the App is activated by means of a user name, password and an activation code. User name and activation code can be automatically inserted via QR Code scan. During the activation process, a Private Public Key is generated. The Private Key does not leave the smart device and is stored on it in encrypted form. It is necessary in order to digitally sign message transactions.

As DoubleClue identifies the unique DNA of smart devices, the activated App only functions on the respective device.

Users can install and activate their DoubleClue App on different platforms.

An App installed and activated on one device also supports usage by several different users.

App requirements:

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

4.2 DoubleClue SDK-Library for Android and iOS

The DoubleClue App consists of a DoubleClue SDK library and the App GUI. With the help of the SDK library, the DoubleClue features can be integrated into one’s own company app, or a customized DoubleClue App can be created.

5. Integration of Applications with DoubleClue

DoubleClue supports all applications via the following interfaces:

- REST-API Services
- RADIUS
- SAML
- Windows Login Credential Provider

6. DoubleClue Enterprise Management (DCEM)

6.1 Feature Overview

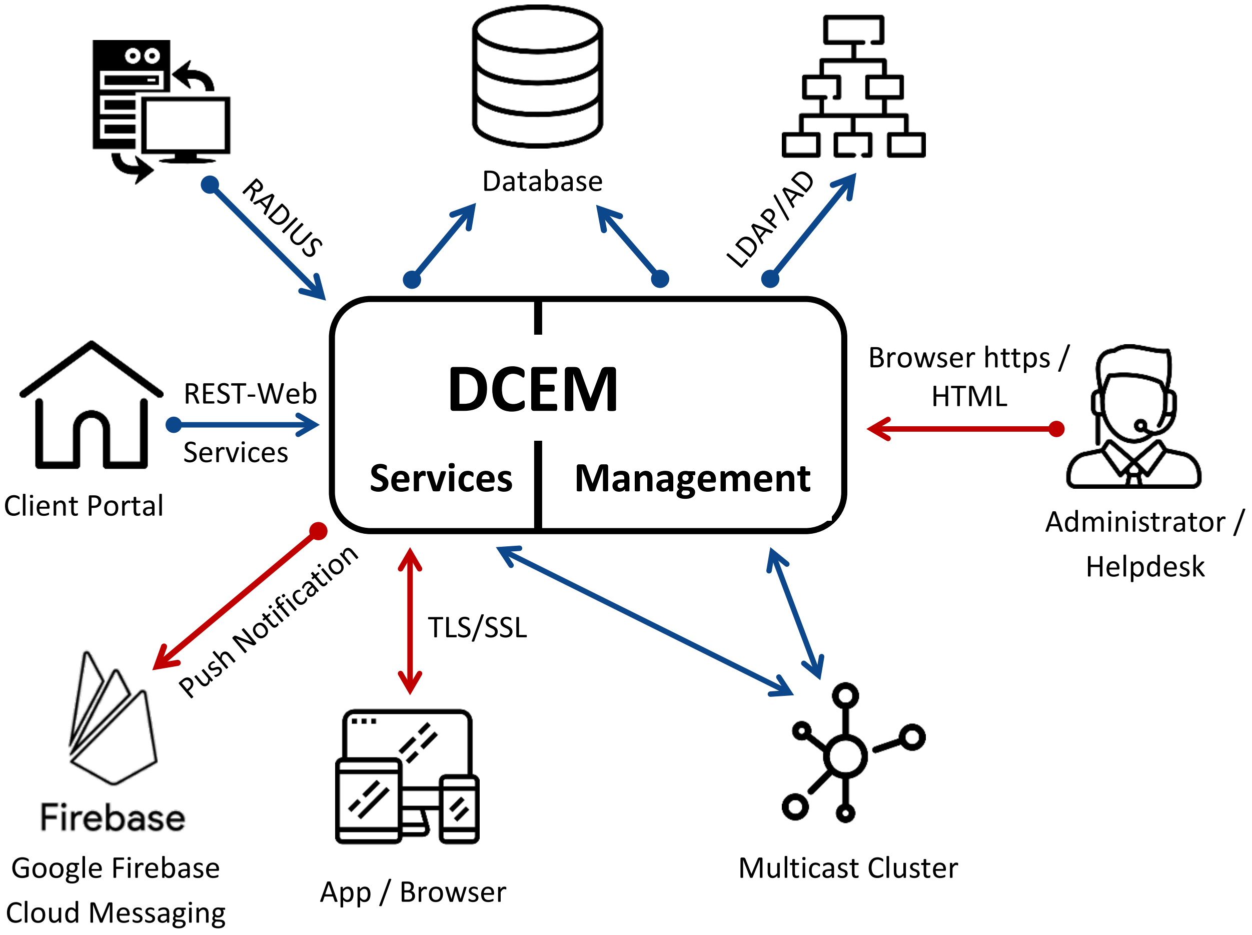
- Single point of administration for users, devices, operators, access policies etc.
- High fail-safety due to load distribution by highly scalable cluster nodes. The necessary load balancer is not part of the DoubleClue solution.
- Finely tuned, role-based access rights for operators
- History about every change
- Integration of and communication with company applications via REST Web-Services, RADIUS or SAML

- Communication with the DoubleClue App via secure Web Sockets
- Usage of an own PKI for communicating with the DoubleClue App. Thus, the App is independent from the operating system's PKI.
- Own built-in Certificate Authority with support for external CAs
- Support of an integrated database ("Embedded Database") as well as the external databases Maria DB, MySQL and MS SQL
- For Windows and Linux
- Full Active Directory integration (domains, users and groups)
- Prepared for multiple domain infrastructure
- Support of cloud data for devices and users

6.2 Structure of DCEM

DCEM is a cluster that consists of several interlinked, independent servers. It is the central component of the DoubleClue platform.

DCEM is divided into the areas "Management" and "Services". The following scenario demonstrates all possible components of DCEM and the areas with which they communicate:

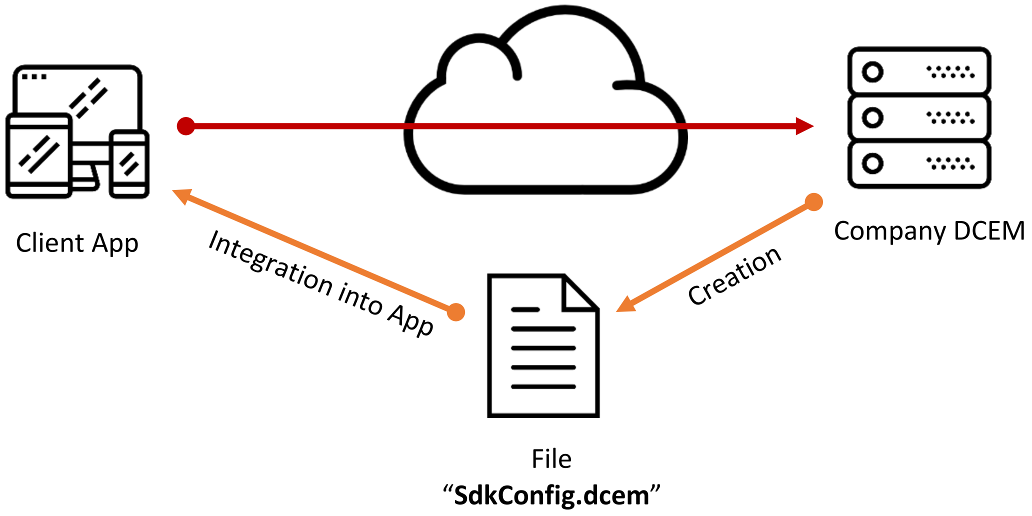


6.3 Connection Scenarios

The DoubleClue App can connect to DCEM directly or via the global DoubleClue Dispatcher.

6.3.1 Direct Connection

The App directly connects to a company's DCEM installation. For this connection type, a customer needs to create their own app, as the DCEM certificates have to be integrated into the customized app.

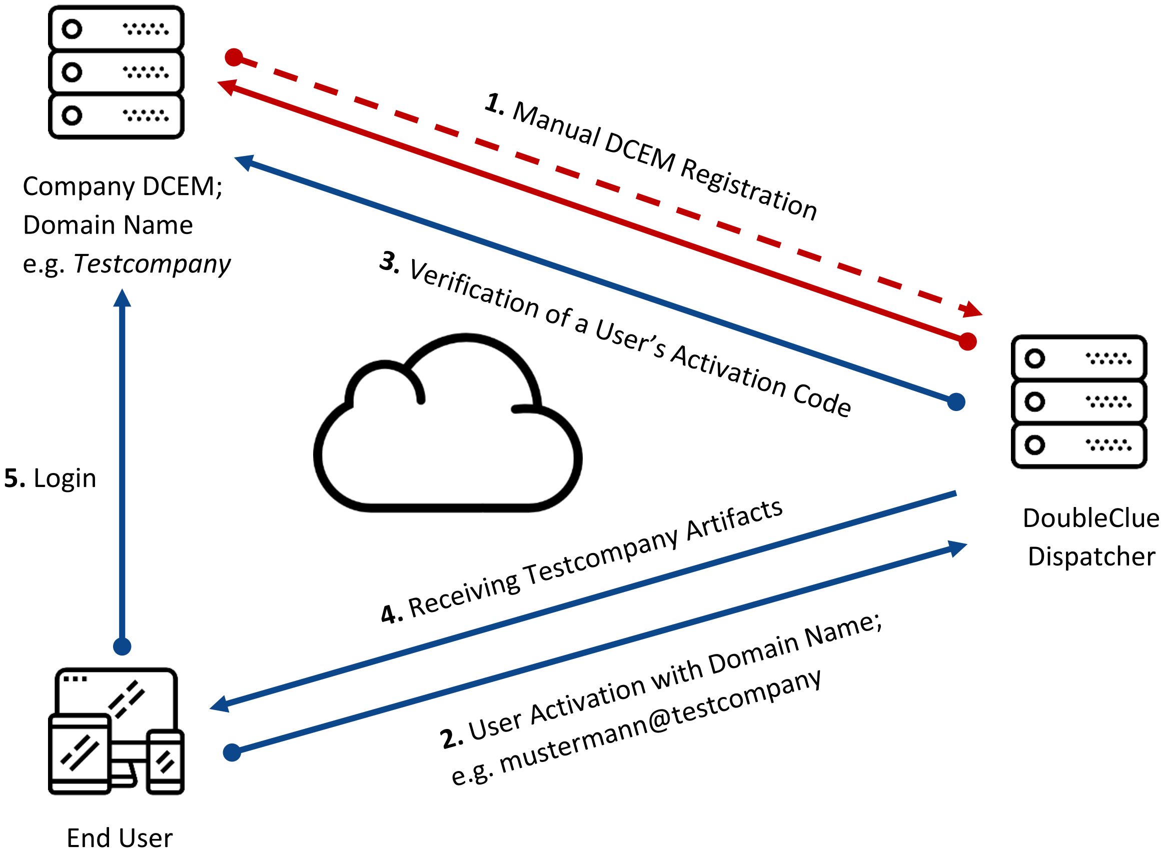


6.3.2 Connection via the DoubleClue Dispatcher

With this connection type, the universal DoubleClue App can be used. The installed DCEM cluster needs to be registered at the global DoubleClue Dispatcher beforehand.

Prerequisites are that the DCEM cluster has a Domain Name System (DNS) and the secure Web Sockets port is open for the internet.

The DoubleClue Dispatcher is a DCEM Cluster in the cloud managed by *HWS Informationssysteme GmbH*. On device activation, the Dispatcher will verify login ID and activation code with the domain "Dcem-Installation". If the Activation Code is valid, the Dispatcher will send the DCEM SDK configuration metadata file to the device. At login the device will connect directly to a company's DCEM installation.


1. Manual DCEM Registration
2. User Activation with Domain Name;
e.g. mustermann@testcompany
3. Verification of a User's Activation Code
4. Receiving Testcompany Artifacts
5. Login
Company DCEM;
Domain Name
e.g. *Testcompany*
DoubleClue
Dispatcher
End User

6.4 Multi-Tenant (Multi-Client Capability)

DoubleClue Enterprise Management (DCEM) supports Multi-Tenant. This feature will be available from Version 1.6.1:

- Use of ONE installation, ONE database, ONE URL access for several companies or rather subcontractors (tenants).
- For each tenant, an isolated database schema is created.
- Each tenant can fully administrate their users, devices, policies, LDAP, RADIUS, SAML etc.
- PKI, URLs, ports, cluster nodes and diagnostics are centrally managed.

DoubleClue can thus be operated in the cloud for several tenants.