

# Integration von Salesforce mit DoubleClue via SAML

# 1. Einführung



Diese Dokumentation ist für Nutzer von gedacht, die möchten, dass sich ihre Mitarbeiter per DoubleClue Multi-Faktor-Authentifizierung (MFA) unter der Verwendung von SAML 2.0 in Salesforce CRM anmelden können. Für weitere Informationen zu diesem Produkt besuchen Sie bitte <u>https://www.salesforce.com/</u>.

Anforderungen:

- Salesforce Version Spring 19 oder neuer
- Salesforce-Account
- Installation des DoubleClue Enterprise Management-Systems (DCEM) mit registrierten Benutzern, welche den Mitarbeiter-E-Mails entsprechen.

### 2. Vorbereitung von DCEM als Identitäts-Provider

Um DCEM als Identitäts-Provider vorzubereiten, schlagen Sie bitte in Kapitel 12 des DCEM-Handbuchs ("DCEM\_Manual\_DE.pdf") nach.

## 3. Einrichtung von Salesforce CRM

- 1. Loggen Sie sich in Ihr Salesforce Organization Center unter <u>https://login.salesforce.com</u> ein.
- 2. Klicken Sie auf das Benutzericon in der oberen, rechten Ecke.



3. In dem sich daraufhin öffnenden Dialog wählen Sie unter Options "Zu Salesforce Classic wechseln". Sie werden daraufhin zur klassischen Ansicht von Salesforce weitergeleitet.

Integration von Salesforce mit DoubleClue

eu19.salesforce.com Einstellungen Abmelden		
ANZEIGEDICHTE		
 Komfortabel		
✓ Kompakt		
OPTIONEN		
Zu Salesforce Classic wechseln 🚯		
Benutzernamen hinzufügen		



- 4. Klicken Sie in der oberen Menüleiste auf "Setup" und suchen Sie anschließend in der Quick Search nach "Single Sign-On Einstellungen / Settings".
- 5. Achten Sie darauf, dass in den Sign-On Einstellungen bei "SAML-fähig" der Haken gesetzt ist.

		Bearbeiten	SAML-Behauptungsvalidierer
Verbundenes Single Sign On über SAML			
	SAML-fähig 🖌		
SAML Single Sign On-Einstellungen		Neu Neu au	is Metadatendatei)(Neu aus Metadaten-URL)

- Klicken Sie auf "Neu aus Metadatendatei" und wählen Sie die IdP-Metadaten-XML-Datei aus, welche Sie während des SAML-Setups heruntergeladen haben (siehe Kapitel 12.1.4 des DCEM-Handbuchs, "DCEM\_Manual\_DE.pdf").
- 7. Klicken Sie auf "Erstellen".
- 8. Tragen Sie jetzt unter "Anmelde-URL des Identitätsanbieters" und "Benutzerdefinierte Abmelde-URL" die Login-URL von SAML ein. Die anderen Felder werden nach hochladen der Datei automatisch ausgefüllt. Klicken Sie anschließend auf "Speichern".

#### SAML Single Sign On-Einstellungen

	Speichern Speichern & Neu Abbrechen
Name	DCEM
SAML-Version	2.0
Aussteller	https://dev.hws-gruppe
Zertifikat von einem Identitätsanbieter	Durchsuchen Keine Datei ausgewählt.
Signaturzertifikat anfordern	SelfSignedCert_28Mar2019_112743 V
Anforderungssignaturmodell	RSA-SHA256 V
Behauptungsentschlüsselungszertifikat	Behauptung nicht verschlüsselt
SAML-Identitätstyp	Behauptung enthält den Salesforce-Benutzernamen des Benutzers Die Behauptung enthält die Verbund-ID des Benutzerobjekts. Die Behauptung enthält die Benutzer-ID aus dem Benutzerobjekt.
SAML-Identitäts-Standort	Die Identität ist das Namenskennzeichner-Element der Betreffanweisung. Die Identität befindet sich in einem Attributelement.
Anmelde-URL des Identitätsanbieters	http://hws001s0202:8888/dcem/saml
Benutzerdefinierter Abmelde-URL	http://hws001s0202:8888/dcem/saml
Benutzerdefinierter Fehler-URL	
Single Logout aktiviert	
Just-in-Time-Benutzerbereitstellung	
Benutzerbereitstellung aktiviert	
	Speichern Speichern & Neu Abbrechen

DCEM ist nun als Identitäts-Provider für SalesForce egistriert.

#### 4. Einrichtung von Salesforce als Service-Provider für DCEM

- 1. Laden Sie die XML-Datei in Ihrem unter Salesforce Organization Center herunter. Gehen Sie dafür zunächst wie unter 3. beschrieben zu den SAML Single Sign On-Einstellungen
- 2. Klicken Sie auf den Namen des entsprechenden Dateieintrags (vermutlich DCEM).
- 3. Klicken Sie auf Metadateien herunterladen.
- SAML Single Sign On-Einstellungen Zurück zu den Single Sign On-Einstellungen

	Bearbeiten Löschen Duplizieren Metadaten herunterladen SAML-Behauptungsvalidierer			
Name	DCEM			
SAML-Version	2.0			
Aussteller	https://dev.hws-gruppe			
Zertifikat von einem Identitätsanbieter	CN=HWS001S0210 Ablauf: 10 Sep 2118 08:14:24 GMT			
Signaturzertifikat anfordern	SelfSignedCert 28Mar2019 112743			
Anforderungssignaturmodell	RSA-SHA256			
Behauptungsentschlüsselungszertifikat	Behauptung nicht verschlüsselt			
SAML-Identitätstyp	Benutzername			
SAML-Identitäts-Standort	Thema			
Anmelde-URL des Identitätsanbieters	http://hws001s0202:8888/dcem/sami			
Benutzerdefinierter Abmelde-URL	http://hws001s0202:8888/dcem/saml			
Benutzerdefinierter Fehler-URL				
Single Logout aktiviert				
Just-in-Time-Benutzerbereitstellung				
Benutzerbereitstellung aktiviert				
Endpunkte				
Zeigen Sie SAML-Endpunkte für Ihre Organisation, Communities oder benutzerdefinierten Domänen an.				
Ihre Organisation				
Anmelde-URL	https://login.salesforce.com?so=00D1i000000UFR3			
OAuth 2.0 Token-Endpunkt	https://login.salesforce.com/services/oauth2/token?so=00D1i000000UFR3			
	Bearbeiten Löschen Duplizieren Metadaten herunterladen SAML-Behauptungsvalidierer			

- 4. Loggen Sie sich in bei DCEM ein und wählen Sie im Menü "SAML" aus.
- 5. Wählen Sie "SP Metadata" und klicken Sie auf "Hinzufügen".
- 6. Wählen Sie im dem Dropdown-Menü "Benutzerdefiniert" aus und klicken Sie dann auf "Fortfahren".
- 7. Laden Sie die heruntergeladene Datei mittels des "Upload"-Buttons hoch.
- 8. Geben Sie bei "Anzeigename" einen einzigartigen, benutzerfreundlichen Namen wie z.B. "Salesforce" ein.
- 9. Gehen Sie zum Tab "Details".
- 10. Wählen Sie "EMAIL" bei "Erwartetes NameID-Format" aus.
- 11. Klicken Sie auf "OK".

Salesforce ist nun als Service-Provider für DCEM registriert.