

Integration of Salesforce with DoubleClue using SAML



1. Introduction

This guide is intended for users of Salesforce CRM who would like their employees to log in to Salesforce via DoubleClue Multi-Factor Authentication (MFA) using SAML 2.0. For more information on these products, please visit <https://www.salesforce.com/>.

Requirements:

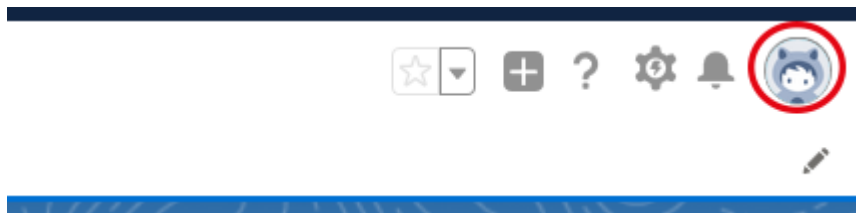
- Salesforce Version Spring 19 or newer
- Salesforce-Account
- DoubleClue Enterprise Management-Systems (DCEM) with registered users matching employee-emails

2. Preparing DCEM to be an Identity Provider

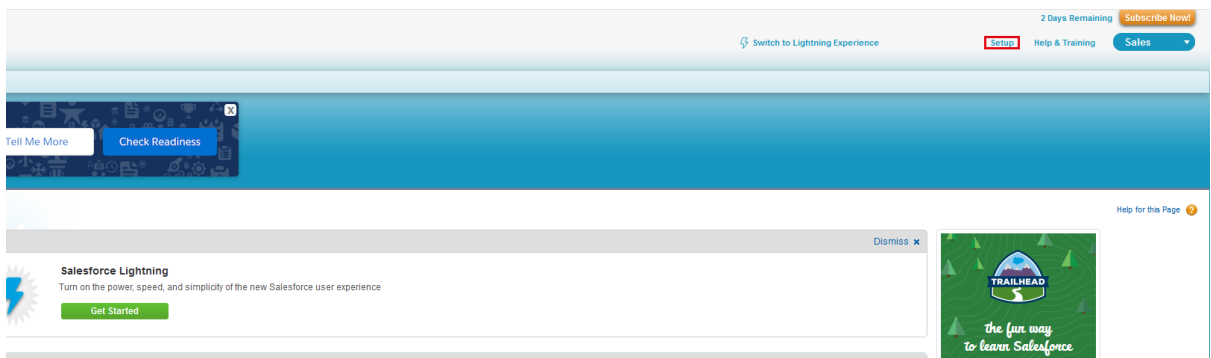
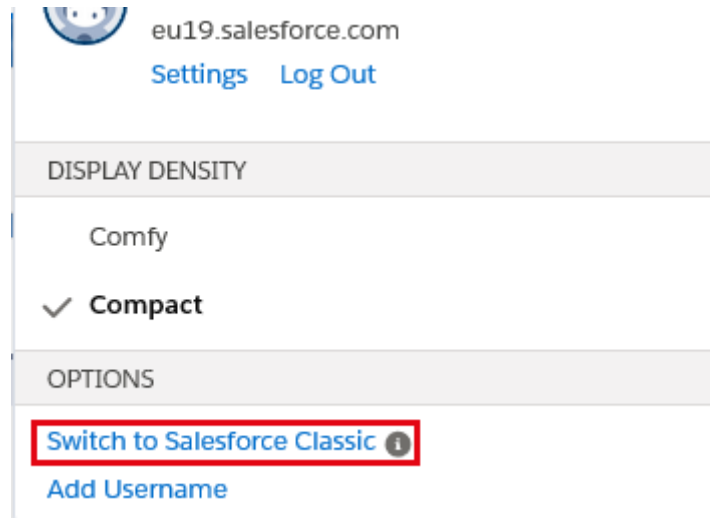
In order to prepare DCEM to be an Identity Provider, please see chapter 12 of "DCEM_Manual_EN.pdf".

3. Setting up Salesforce CRM

1. Log into your Salesforce Organization Center at <https://login.salesforce.com>.
2. Click on the user icon in the upper right corner.



3. In the following dialogue choose under options „Switch to Salesforce Classic.“ You will then be forwarded to the classic Salesforce view.

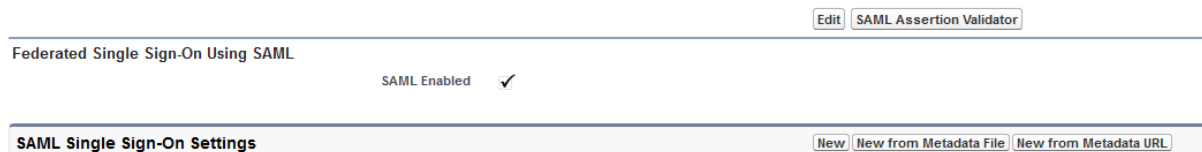


4. Go on „Setup“ on the right side of the upper menu bar. Then use the Quick Search to search for „Single Sign-On Settings“.
5. Make sure that “SAML Enabled” is checked.

Single Sign-On Settings

Configure single sign-on in order to authenticate users in salesforce.com from external environments. Your organization has the following options available for single sign-on:

- Federated authentication, a single sign-on method that uses SAML assertions sent to a Salesforce endpoint.



6. Click on “New from Metadata File” and choose the IdP-Metadata-XML-file, which you downloaded during the SAML-Setup (see chapter 12 of “DCEM_Manual_EN.pdf”).
7. Click on „Create“.

- Enter the SAML login URL into the „Identity Provider Login URL” and „ Custom Logout URL” fields. The other fields will be filled automatically after uploading the file. Click on “Save”

SAML Single Sign-On Settings

Save Save & New Cancel

Name

SAML Version 2.0

Issuer

Identity Provider Certificate Keine Datei ausgewählt.

Request Signing Certificate

Request Signature Method

Assertion Decryption Certificate

SAML Identity Type Assertion contains the User's Salesforce username
 Assertion contains the Federation ID from the User object
 Assertion contains the User ID from the User object

SAML Identity Location Identity is in the NameIdentifier element of the Subject statement
 Identity is in an Attribute element

Identity Provider Login URL

Custom Logout URL

Custom Error URL

Single Logout Enabled [i](#)

Just-in-time User Provisioning

User Provisioning Enabled [i](#)

Save Save & New Cancel

DCEM is now registered as an identity provider for Salesforce.

4. Setting up Salesforce as a Service-Provider for DCEM

- Upload the XML-file from your Salesforce Organization Center. Navigate to the SAML Single Sign-On Settings as described under 3.

SAML Single Sign-On Settings

[Back to Single Sign-On Settings](#)

		Edit	Delete	Clone	Download Metadata	SAML Assertion Validator
Name	DCEM					
SAML Version	2.0					
Issuer	https://dev.hws-gruppe					
Identity Provider Certificate	CN=HWS001S0210 Expiration: 10 Sep 2118 08:14:24 GMT					
Request Signing Certificate	SelfSignedCert_28Mar2019_112743					
Request Signature Method	RSA-SHA256					
Assertion Decryption Certificate	Assertion not encrypted					
SAML Identity Type	Username					
SAML Identity Location	Subject					
Identity Provider Login URL	http://hws001s0202:8888/dcem/saml					
Custom Logout URL	http://hws001s0202:8888/dcem/saml					
Custom Error URL						
Single Logout Enabled	<input type="checkbox"/>					

Just-in-time User Provisioning

User Provisioning Enabled

Endpoints
View SAML endpoints for your organization, communities, or custom domains.

Your Organization

Login URL	https://login.salesforce.com?so=00D11000000UFR3
OAuth 2.0 Token Endpoint	https://login.salesforce.com/services/oauth2/token?so=00D11000000UFR3

[Edit](#) [Delete](#) [Clone](#) [Download Metadata](#) [SAML Assertion Validator](#)

2. Click on the name of the file entry (most likely DCEM).
3. Click on „Download Metadata“.
4. Log into DCEM and select the SAML item in the menu on the left side of the screen.
5. Choose „SP Metadata“ and click on „Add“.
6. Choose „Custom“ in the dropdown menu of the following dialogue and click on „Continue“.
7. Upload the downloaded xml-file with the „Upload“-button.
8. Enter a unique and informative „Display Name“ like Salesforce.
9. Go to the Tab „Details“.
10. Choose „email“ in the „Expected Name ID Format“ dropdown menu.
11. Click on „OK“.

Salesforce is now registered as an ID provider for DoubleClue.