Integration of Amazon Web Services with DoubleClue using SAML

1. Introduction

This guide is intended for users of Amazon Web Services (AWS) who would like their employees to log into Amazon Web Services via DoubleClue Multi-Factor Authentication (MFA) using SAML 2.0. For more information on this product, please visit https://aws.amazon.com/

Requirements:

- AWS root user account
- DoubleClue Enterprise Management (DCEM) installation

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 AWS

1. Sign into the AWS root user console on https://aws.amazon.com/.
2. Go to “Services” > “IAM” (under “Security, Identity & Compliance”).
3. From the menu on the left, select “Identity Providers”.
4. Click “Create Provider”.
5. For “Provider Type”, choose “SAML”.
6. Type in a Provider Name of your choice, e.g. “DoubleClue”.
7. For “Metadata Document”, upload the IdP Metadata file you downloaded during SAML setup (see chapter 12.1.4 of “DCEM_Manual_EN.pdf”).
8. Click “Next Step”.
9. Click “Create”.
10. Click on your newly created provider from the list and copy the “Provider ARN” for future use.
11. From the menu on the left, select “Roles”.
12. Click “Create Role”.
13. For “Select type of trusted entity”, select “SAML 2.0 federation”.
14. For “SAML provider”, choose the provider you just created.
15. Select “Allow programmatic and AWS Management Console access”.

16. Click “Next: Permissions”.
17. Click “Next: Review”.
18. Type in a role name of your choice, e.g. “dcuser”.
19. Click “Create role”.
20. Click on your newly created role from the list and copy the “Role ARN” for future use.

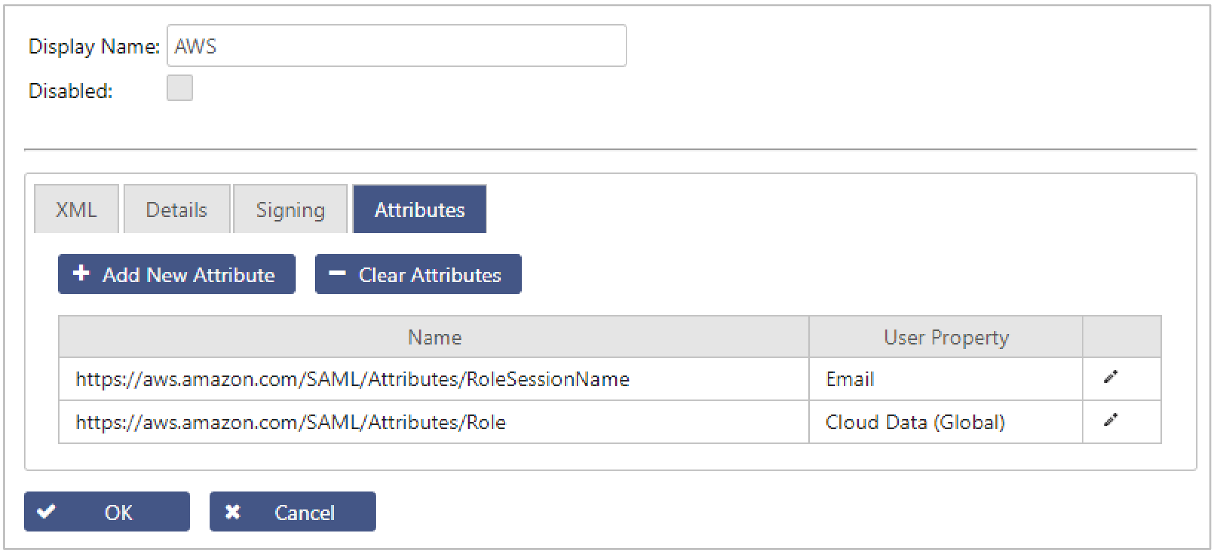
4. Setting AWS as a Service Provider for DCEM

Option 1: Using the pre-set configuration

1. In DCEM, go to main menu item “SAML”, sub menu “SP Metadata”.
2. Click “Add”.
3. From the dropdown, choose “AWS” and click “Continue”.
4. Click “OK”.

Option 2: Using a custom configuration

1. Download the XML-File at https://signin.aws.amazon.com/static/saml-metadata.xml.
2. In DCEM, go to main menu item “SAML”, sub menu “SP Metadata”.
3. Click “Add”.
4. From the dropdown, choose “Custom” and click “Continue”.
5. Upload the downloaded file using the “Upload” button.
6. Go to the “Attributes” tab.
7. Click the pencil icon in the row containing “RoleSessionName” and change the User Property to “Email”. Click the tick icon to save the change.
8. Repeat for “Role”, but choose “Cloud Data (Global)” as the User Property.
9. Click “OK”.



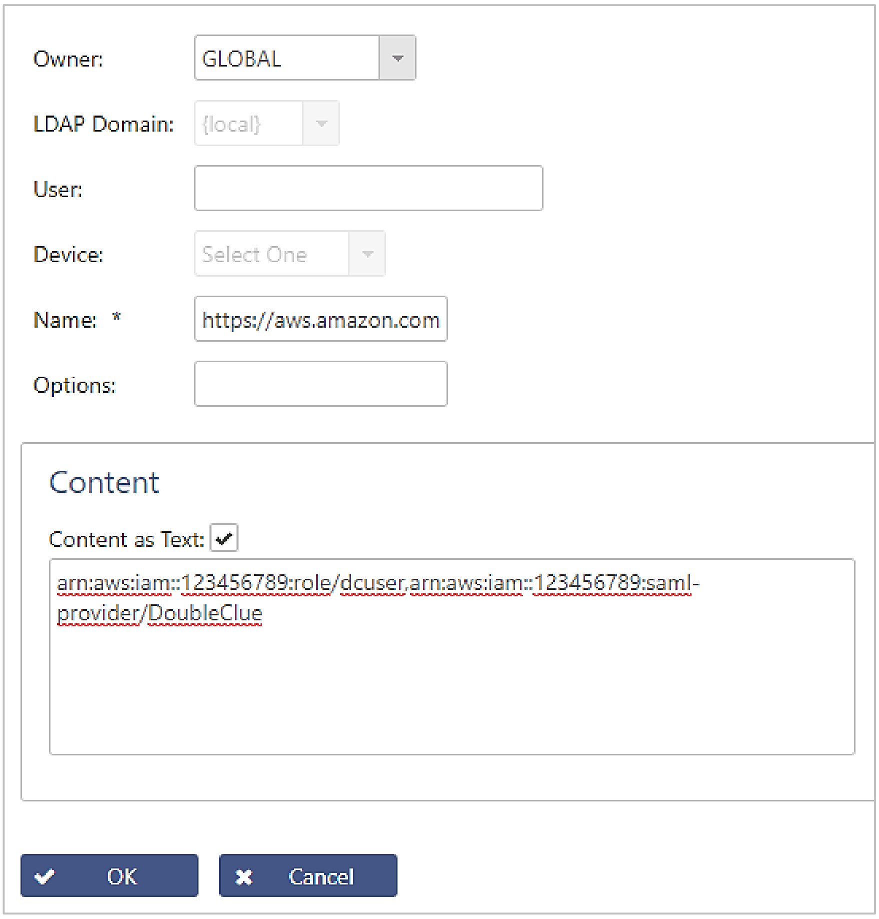
Display Name:	AWS
Disabled:	□

Name	User Property	
https://aws.amazon.com/SAML/Attributes/RoleSessionName	Email	✎
https://aws.amazon.com/SAML/Attributes/Role	Cloud Data (Global)	✎

After either option:

1. Go to main menu item “Identity-Management”, sub menu “Cloud-Data”.
2. Click “Add”.
3. For “Owner”, select “GLOBAL”.
4. For “Name”, type in “https://aws.amazon.com/SAML/Attributes/Role”.
5. Check “Content as Text”, if it is not already checked.
6. Paste in the ARN values you copied in chapter 3 in the following format:

<role_arn_from_3(2nd value)>,<provider_arn_from_3(1st value)>



Owner: GLOBAL

LDAP Domain: {local}

User:

Device: Select One

Name: * https://aws.amazon.com

Options:

Content

Content as Text: ☑

arn:aws:iam::123456789:role/dcuser,arn:aws:iam::123456789:saml-provider/DoubleClue

7. Click “OK”.

AWS is now registered as a Service Provider for DCEM.