Configuring SAML assertions for the authentication response

PDF (iam-ug.pdf#id_roles_providers_create_saml_assertions) | RSS (aws-iam-release-notes.rss)

After you have verified a user's identity in your organization, the external identity provider (IdP) sends an authentication response to the AWS SAML endpoint at `https://region-code.signin.aws.amazon.com/saml`. For a list of potential *region-code* replacements, see the **Region** column in AWS Sign-In endpoints (https://docs.aws.amazon.com/general/latest/gr/signin-service.html). This response is a POST request that includes a SAML token that adheres to the HTTP POST Binding for SAML 2.0 (http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf) standard and that contains the following elements, or *claims*. You configure these claims in your SAML-compatible IdP. Refer to the documentation for your IdP for instructions on how to enter these claims.

When the IdP sends the response containing the claims to AWS, many of the incoming claims map to AWS context keys. These context keys can be checked in IAM policies using the `Condition` element. A listing of the available mappings follows in the section Mapping SAML attributes to AWS trust policy context keys (#saml-attribute-mapping).

`Subject` and `NameID`

The following excerpt shows an example. Substitute your own values for the marked ones. There must be exactly one `SubjectConfirmation` element with a `SubjectConfirmationData` element that includes both the `NotOnOrAfter` attribute and a `Recipient` attribute. These attributes include a value that must match the AWS endpoint `https://region-code.signin.aws.amazon.com/saml`. For a list of possible *region-code* values, see the **Region** column in AWS Sign-In endpoints (https://docs.aws.amazon.com/general/latest/gr/signin-service.html). For the AWS value, you can also use `https://signin.aws.amazon.com/static/saml`, as shown in the following example. For information about the name identifier formats supported for single sign-on interactions, see Oracle Sun OpenSSO Enterprise Administration Reference (https://docs.oracle.com/cd/E19316-01/820-3886/ggwbz/index.html).

```
<Subject>
  <NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent">_cbb88bf52c2510eabe00c1642d4643f41430fe25e3</Nam
eID>
  <SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    <SubjectConfirmationData NotOnOrAfter="2013-11-
05T02:06:42.876Z" Recipient="https://signin.aws.amazon.com/saml"/>
  </SubjectConfirmation>
</Subject>
```

AudienceRestriction and Audience

For security reasons, AWS should be included as an audience in the SAML assertion your IdP sends to AWS. For the value of the `Audience` element, specify either `https://region-code.signin.aws.amazon.com/saml` or `urn:amazon:webservices`. For a list of possible *region-code* values, see the **Region** column in AWS Sign-In endpoints (https://docs.aws.amazon.com/general/latest/gr/signin-service.html). For `Audience`, you can also use the value: `https://signin.aws.amazon.com/static/saml`. The following sample XML snippets from SAML assertions show how this key can be specified by the IdP. Include whichever sample applies to your use case.

```
<Conditions>
  <AudienceRestriction>
    <Audience>https://signin.aws.amazon.com/saml</Audience>
  </AudienceRestriction>
</Conditions>
```

```
<Conditions>
  <AudienceRestriction>
    <Audience>urn:amazon:webservices</Audience>
  </AudienceRestriction>
</Conditions>
```

> **Important**

The SAML `AudienceRestriction` value in the SAML assertion from the IdP does *not* map to the `saml:aud` context key that you can test in an IAM policy. Instead, the `saml:aud` context key comes from the SAML *recipient* attribute because it is the SAML equivalent to the OIDC audience field, for example, by `accounts.google.com:aud`.

SAML PrincipalTagAttribute

(Optional) You can use an `Attribute` element with the `Name` attribute set to `https://aws.amazon.com/SAML/Attributes/PrincipalTag:` *`{TagKey}`* . This element allows you to pass attributes as session tags in the SAML assertion. For more information about session tags, see Passing session tags in AWS STS (./id_session-tags.html) .

To pass attributes as session tags, include the `AttributeValue` element that specifies the value of the tag. For example, to pass the tag key-value pairs `Project = Marketing` and `CostCenter = 12345`, use the following attribute. Include a separate `Attribute` element for each tag.

```
<Attribute
Name="https://aws.amazon.com/SAML/Attributes/PrincipalTag:Project">
  <AttributeValue>Marketing</AttributeValue>
</Attribute>
<Attribute
Name="https://aws.amazon.com/SAML/Attributes/PrincipalTag:CostCente
r">
  <AttributeValue>12345</AttributeValue>
</Attribute>
```

To set the tags above as transitive, include another `Attribute` element with the `Name` attribute set to `https://aws.amazon.com/SAML/Attributes/TransitiveTagKeys` . This is an optional multivalued attribute that sets your session tags as transitive. Transitive tags persist when you use the SAML session to assume another role in AWS. This is known as role chaining (./id_roles_terms-and-concepts.html#iam-term-role-chaining) . For example, to set both the `Principal` and `CostCenter` tags as transitive, use the following attribute to specify the keys.

```
<Attribute
Name="https://aws.amazon.com/SAML/Attributes/TransitiveTagKeys">
  <AttributeValue>Project</AttributeValue>
```

```
  <AttributeValue>CostCenter</AttributeValue>
</Attribute>
```

SAML RoleAttribute

You can use an `Attribute` element with the `Name` attribute set to `https://aws.amazon.com/SAML/Attributes/Role`. This element contains one or more `AttributeValue` elements that list the IAM identity provider and role to which the user is mapped by your IdP. The IAM role and IAM identity provider are specified as a comma-delimited pair of ARNs in the same format as the `RoleArn` and `PrincipalArn` parameters that are passed to AssumeRoleWithSAML (https://docs.aws.amazon.com/STS/latest/APIReference/API_AssumeRoleWithSAML.html). This element must contain at least one role-provider pair (`AttributeValue` element), and can contain multiple pairs. If the element contains multiple pairs, then the user is asked to choose which role to assume when they use WebSSO to sign into the AWS Management Console.

> **⚠ Important**
>
> The value of the `Name` attribute in the `Attribute` tag is case-sensitive. It must be set to `https://aws.amazon.com/SAML/Attributes/Role` exactly.

```
<Attribute Name="https://aws.amazon.com/SAML/Attributes/Role">
  <AttributeValue>arn:aws:iam::account-number:role/role-
name1,arn:aws:iam::account-number:saml-provider/provider-
name</AttributeValue>
  <AttributeValue>arn:aws:iam::account-number:role/role-
name2,arn:aws:iam::account-number:saml-provider/provider-
name</AttributeValue>
  <AttributeValue>arn:aws:iam::account-number:role/role-
name3,arn:aws:iam::account-number:saml-provider/provider-
name</AttributeValue>
</Attribute>
```

SAML RoleSessionNameAttribute

You can use an `Attribute` element with the `Name` attribute set to `https://aws.amazon.com/SAML/Attributes/RoleSessionName`. This element contains one `AttributeValue` element that provides an identifier for the temporary credentials that are issued when the role is assumed. You can use this to associate the temporary credentials with the user who is using your application. This element is used to display user information in the AWS Management Console. The value in the `AttributeValue` element must be between 2 and 64 characters long, can contain only alphanumeric characters, underscores, and the following characters: **. , + = @ -** (hyphen). It cannot contain spaces. The value is typically a user ID (`johndoe`) or an email address (`johndoe@example.com`). It should not be a value that includes a space, like a user's display name (`John Doe`).

> **⚠ Important**
>
> The value of the `Name` attribute in the `Attribute` tag is case-sensitive. It must be set to `https://aws.amazon.com/SAML/Attributes/RoleSessionName` exactly.

```
<Attribute
Name="https://aws.amazon.com/SAML/Attributes/RoleSessionName">
  <AttributeValue>user-id-name</AttributeValue>
</Attribute>
```

SAML SessionDurationAttribute

(Optional) You can use an `Attribute` element with the `Name` attribute set to `https://aws.amazon.com/SAML/Attributes/SessionDuration"`. This element contains one `AttributeValue` element that specifies how long the user can access the AWS Management Console before having to request new temporary credentials. The value is an integer representing the number of seconds for the session. The value can range from 900 seconds (15 minutes) to 43200 seconds (12 hours). If this attribute is not present, then the credential last for one hour (the default value of the `DurationSeconds` parameter of the `AssumeRoleWithSAML` API).

To use this attribute, you must configure the SAML provider to provide single sign-on access to the AWS Management Console through the console sign-in web endpoint at `https://` *`region-code`* `.signin.aws.amazon.com/saml`. For a list of possible *`region-code`* values, see the **Region** column in AWS Sign-In endpoints (https://docs.aws.amazon.com/general/latest/gr/signin-service.html). You can optionally use the following URL: `https://signin.aws.amazon.com/static/saml`. Note that this attribute extends sessions

only to the AWS Management Console. It cannot extend the lifetime of other credentials. However, if it is present in an `AssumeRoleWithSAML` API call, it can be used to *shorten* the duration of the session. The default lifetime of the credentials returned by the call is 60 minutes.

Note, too, that if a `SessionNotOnOrAfter` attribute is also defined, then the ***lesser*** value of the two attributes, `SessionDuration` or `SessionNotOnOrAfter`, establishes the maximum duration of the console session.

When you enable console sessions with an extended duration the risk of compromise of the credentials rises. To help you mitigate this risk, you can immediately disable the active console sessions for any role by choosing **Revoke Sessions** on the **Role Summary** page in the IAM console. For more information, see Revoking IAM role temporary security credentials (./id_roles_use_revoke-sessions.html) .

> ⚠ **Important**
>
> The value of the `Name` attribute in the `Attribute` tag is case-sensitive. It must be set to `https://aws.amazon.com/SAML/Attributes/SessionDuration` exactly.

```
<Attribute
Name="https://aws.amazon.com/SAML/Attributes/SessionDuration">
  <AttributeValue>1800</AttributeValue>
</Attribute>
```

SAML SourceIdentityAttribute

(Optional) You can use an `Attribute` element with the `Name` attribute set to `https://aws.amazon.com/SAML/Attributes/SourceIdentity`. This element contains one `AttributeValue` element that provides an identifier for the person or application that is using an IAM role. The value for source identity persists when you use the SAML session to assume another role in AWS known as role chaining (./id_roles_terms-and-concepts.html#iam-term-role-chaining) . The value for source identity is present in the request for every action taken during the role session. The value that is set cannot be changed during the role session. Administrators can then use AWS CloudTrail logs to monitor and audit the source identity information to determine who performed actions with shared roles.

The value in the `AttributeValue` element must be between 2 and 64 characters long, can contain only alphanumeric characters, underscores, and the following characters: **. , + = @ -** (hyphen). It cannot contain spaces. The value is typically an attribute that is associated with the

user such as a user id (`johndoe`) or an email address (`johndoe@example.com`). It should not be a value that includes a space, like a user's display name (`John Doe`). For more information about using source identity, see Monitor and control actions taken with assumed roles (./id_credentials_temp_control-access_monitor.html) .

> **Important**
>
> If your SAML assertion is configured to use the SourceIdentity attribute, then your role trust policy must also include the `sts:SetSourceIdentity` action, otherwise the assume role operation will fail. For more information about using source identity, see Monitor and control actions taken with assumed roles (./id_credentials_temp_control-access_monitor.html) .

To pass a source identity attribute, include the `AttributeValue` element that specifies the value of the source identity. For example, to pass the source identity `DiegoRamirez` use the following attribute.

```
<Attribute
Name="https://aws.amazon.com/SAML/Attributes/SourceIdentity">
  <AttributeValue>DiegoRamirez</AttributeValue>
```

Mapping SAML attributes to AWS trust policy context keys

The tables in this section list commonly used SAML attributes and how they map to trust policy condition context keys in AWS. You can use these keys to control access to a role. To do that, compare the keys to the values that are included in the assertions that accompany a SAML access request.

> **Important**
>
> These keys are available only in IAM trust policies (policies that determine who can assume a role) and are not applicable to permissions policies.

In the eduPerson and eduOrg attributes table, values are typed either as strings or as lists of strings. For string values, you can test these values in IAM trust policies using `StringEquals` or `StringLike` conditions. For values that contain a list of strings, you can use the `ForAnyValue`

and `ForAllValues` policy set operators (./reference_policies_multi-value-conditions.html) to test the values in trust policies.

> **Note**
>
> You should include only one claim per AWS context key. If you include more than one, only one claim will be mapped.

eduPerson and eduOrg attributes

eduPerson or eduOrg attribute (Name key)	Maps to this AWS context key (FriendlyName key)	Type
urn:oid:1.3.6.1.4.1.5923.1.1.1.1	eduPersonAffiliation	List of strings
urn:oid:1.3.6.1.4.1.5923.1.1.1.2	eduPersonNickname	List of strings
urn:oid:1.3.6.1.4.1.5923.1.1.1.3	eduPersonOrgDN	String
urn:oid:1.3.6.1.4.1.5923.1.1.1.4	eduPersonOrgUnitDN	List of strings
urn:oid:1.3.6.1.4.1.5923.1.1.1.5	eduPersonPrimaryAffiliation	String
urn:oid:1.3.6.1.4.1.5923.1.1.1.6	eduPersonPrincipalName	String
urn:oid:1.3.6.1.4.1.5923.1.1.1.7	eduPersonEntitlement	List of strings
urn:oid:1.3.6.1.4.1.5923.1.1.1.8	eduPersonPrimaryOrgUnitDN	String
urn:oid:1.3.6.1.4.1.5923.1.1.1.9	eduPersonScopedAffiliation	List of strings
urn:oid:1.3.6.1.4.1.5923.1.1.1.10	eduPersonTargetedID	List of strings
urn:oid:1.3.6.1.4.1.5923.1.1.1.11	eduPersonAssurance	List of strings

eduPerson and eduOrg attributes

eduPerson or eduOrg attribute (Name key)	Maps to this AWS context key (FriendlyName key)	Type
urn:oid:1.3.6.1.4.1.5923.1.2.1.2	eduOrgHomePageURI	List of strings
urn:oid:1.3.6.1.4.1.5923.1.2.1.3	eduOrgIdentityAuthNPolicyURI	List of strings
urn:oid:1.3.6.1.4.1.5923.1.2.1.4	eduOrgLegalName	List of strings
urn:oid:1.3.6.1.4.1.5923.1.2.1.5	eduOrgSuperiorURI	List of strings
urn:oid:1.3.6.1.4.1.5923.1.2.1.6	eduOrgWhitePagesURI	List of strings
urn:oid:2.5.4.3	cn	List of strings

Active Directory attributes

AD attribute	Maps to this AWS context key	Type
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	name	String
http://schemas.xmlsoap.org/claims/CommonName	commonName	String

Active Directory attributes

AD attribute	Maps to this AWS context key	Type
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	givenName	String
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	surname	String
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	mail	String
http://schemas.microsoft.com/ws/2008/06/identity/claims/primarygroupsid	uid	String

X.500 attributes

X.500 attribute	Maps to this AWS context key	Type
2.5.4.3	commonName	String
2.5.4.4	surname	String
2.4.5.42	givenName	String
2.5.4.45	x500UniqueIdentifier	String
0.9.2342.19200300100.1.1	uid	String
0.9.2342.19200300100.1.3	mail	String

X.500 attributes

X.500 attribute	Maps to this AWS context key	Type
`0.9.2342.19200300.100.1.45`	`organizationStatus`	String