CHAPTER 7

Authenticating Requests to Backend Systems

This chapter describes how to configure credentials in outgoing requests. It covers these topics:

Overview

By acting as a network-based access control enforcement point, the ACE XML Gateway helps to ensure that consistent policies are applied across diverse systems and applications. The Gateway also relieves backend systems from having to perform processing-intensive credential verification tasks.

Nevertheless, in some cases backend systems rely upon consumer credentials in incoming requests. For these scenarios, the ACE XML Gateway can generate credentials for inclusion in outgoing messages.

The ACE XML Gateway can generate new credentials or perform credential mediation. In credential mediation an incoming credential is transformed to another type for outgoing delivery (for example, from HTTP Basic Auth to WSS Username tokens or SAML assertions).

In addition to values from incoming credentials, the ACE XML Gateway can generate credentials with values set in the policy, or with data acquired by an LDAP directory lookup performed for authentication.

The Gateway can generate the following types of credentials:

- HTTP Basic Authentication header
- NTLM header
- WSS UsernameToken
- SAML Token

You can configure backend authentication by clicking the **Edit** link next to the Service Authentication settings. The settings appear under the Backend Service heading in the configuration page for the virtual service.

Generating HTTP Header-Based Credentials

For a common class of credentials, the credential is carried in the HTTP header portion of a message. There are two types of HTTP header authentication credentials you can add to outgoing requests:

- HTTP basic authentication header
- NTLM authentication header

HTTP basic auth is a commonly used credential format in which the password is sent in hashed form in the message header. Choose one of the Send Basic Auth header options from the **HTTP Authentication** menu to have the ACE XML Gateway add this header to the outgoing requests.

The ACE XML Gateway also supports generation of NTLM headers. NTLM is an authentication and session security protocol developed by Microsoft and notably used in the IWA (Integrated Windows Authentication) set of technologies.

An NTLM credential is an HTTP header that indicates the username, password, and optionally the target domain of the subject. To have the ACE XML Gateway add NTLM credentials to outgoing requests, choose one of the “Send NTLM auth header” options from the **HTTP Authentication** menu. Optionally, you can have the domain appended to the credential by entering a value in the Domain field that appears when an NTLM option is selected.

Generating WSS UsernameToken Credentials

WSS Username (Web Services Security UsernameToken Profile) is a credential type defined by the OASIS Web Services Security technical committee. The ACE XML Gateway can add WSS Username tokens to outgoing SOAP requests.

The username and password values that the ACE XML Gateway adds to a request can be taken from an incoming credential or specified in the policy. Example 7-1 shows an example of a UsernameToken as generated by the ACE XML Gateway for an outgoing SOAP request.

Example 7-1 WSS Username Token

```
<soap:Envelope>
  <soap:Header>
    <wsse:Security>
      <wsse:UsernameToken>
        <wsse:Username>alice</wsse:Username>
        <wsse:Password
          Type="http://docs.oasis-open.org/wss/2004/01/oasis
           -200401-wss-username-token-profile-1.0#PasswordText">
          mypassword</wsse:Password>
        <wsse:Nonce>4MK0BeHCtAXiwrQF48K0BQ==</wsse:Nonce>
        <wsu:Created>2006-04-25T18:17:30Z</wsu:Created>
      </wsse:UsernameToken>
    </wsse:Security>
  </soap:Header>
  <soap:Body>
    <retrieveQuote>
       ...
    </retrieveQuote>
  </soap:Body>
</soap:Envelope>
```

By default, the password is in clear text. You can configure the ACE XML Gateway to encrypt the password value using a key you specify in the configuration.

To add WSS Username Tokens to outgoing requests:

Step 1 In the **Virtual Services** browser, click on the basic virtual service object or service descriptor for which you want to configure credential generation.

Step 2 Click the **Edit** link next to the **Service Authentication** heading. In a basic virtual service object, you will first need to display the **Backend Service** settings (by clicking the expand control).

Step 3 From the **WSS Username Token** menu, choose **Send this WSS Username Token in the WSS header**.

Step 4 Optionally, choose an item from the **SOAP Role** menu to identify the message recipient that is the intended processor of the SOAP header. The Gateway will add the WSS UsernameToken to a SOAP header in the outgoing message that has this role. If such a header does not already exist in the outgoing message, it is created.

The `role` identifies the intended processor of a SOAP header, particularly if the message may be seen by more than one SOAP node en route to its destination. Use the default value, no role, if roles are not used to identify the header processor in your system.

To choose a SOAP role for the header, choose from these options:

- **custom** to specify a custom, named role you specify.
- **next**, if the WSS header is intended for the next SOAP role that processes the message.
- **ultimateReceiver**, if the WSS header is intended for the final receiver of the message.

Step 5 Choose an item from the **Generate** menu to specify how the service descriptor generates the username and password in the token. These options are available:

- **Using the username and password from the credential** directs the ACE XML Gateway to populate the generated token with username and password values taken from the credentials used to authenticate the request to the ACE XML Gateway.
- **Using the following username and password menu item** specifies a fixed username and password to be used in the WSS Username Token.

Step 6 Optionally, have the ACE XML Gateway encrypt the token by clicking the **Encrypt Username Token** checkbox and configuring these encryption settings:

- **Transport key** is the public key used to encrypt the username token.

  If no key resources have been loaded to the ACE XML Manager, click the **Upload** button and create the key resource from a certificate file that contains the key you want to use.
- **Encryption Algorithm** is the encryption scheme used to encrypt the token. Choose from these standard algorithms: 3DES, AES256, AES-192, AES-128.
- **Transport Cipher** is the cipher used to encrypt transported packets. Choose from RSA-PKCS#1 or RSA-OAEP.

Step 7 Click **Save Changes** to commit your changes to the working policy.

Once the policy is deployed, WSS Username tokens are added to messages sent out from the configured virtual service.

In addition to generating a new WSS UsernameToken, the ACE XML Gateway can pass through tokens received in the incoming message. To configure this option, choose **Pass through WSS Username Token(s) from the inbound message**. In this case, the Gateway adds WSS Username Tokens received in the inbound message to the outbound message.

A token can also be created that is intended for processing only by another ACE XML Gateway (AXG-only). AXG-only tokens are intended for scenarios in which messages are passed from one ACE XML Gateway to another, possibly over an untrusted network (for example, between ACE XML Gateways at different branch offices). The AXG-only role identifies headers that are intended for processing only by another ACE XML Gateway. The source ACE XML Gateway constructs this type of outgoing token if the **Pass through as AXG-only UsernameToken** option is enabled in the token passthrough configuration. The destination ACE XML Gateway can be configured to process the token using the option **Decrypt AXG-only WSS Username Token(s) and pass through**. After decrypting the incoming AXG-only token, the receiving Gateway propagates the token to the outgoing request as specified by the other settings configured for the token.

Note The ACE XML Gateway uses a custom role attribute value to indicate that a WSS UsernameToken is intended for processing only by another ACE XML Gateway. Other than through the use of the **Decrypt AXG-only WSS Username Token(s) and pass through** option, you should not attempt to capture and process headers with this role using other settings of the policy, such as SOAP Header settings.

Generating SAML Assertions

By adding SAML assertions to outgoing requests, the ACE XML Gateway can act as an asserting party for systems that rely on SAML credentials. The SAML assertions generated by the ACE XML Gateway can be in the form of a SAML 1.0, SAML 1.1, or SAML 2.0 credential.

A SAML credential asserts the identity of a particular individual or application as indicated by the Subject NameIdentifier element in the assertion. In generated credentials, the value of the Subject NameIdentifier can be propagated from credentials of the incoming request. The types of values you can use include a username from username/password credentials, subject name of a client SSL certificate, or fixed values. In addition, if the source credential is WSS Username, you can add attributes to the SAML assertion that are derived from attributes of the WSS Username element.

The ACE XML Gateway can add a single SAML assertion to the outgoing request or multiple assertions derived from multiple incoming credentials. (For multiple assertions, the ACE XML Gateway can generate an assertion for each WSS Username token and client SSL certificate that was verified in the incoming request.)

To have the ACE XML Gateway generate multiple SAML assertions, in addition to the configuration steps described here, you must enable multiple assertion verification by the authenticator that receives the request. Note that enabling multiple assertion verification is distinct from simply specifying multiple credential requirements in an authenticator. By enabling multiple credential requirements, the ACE XML Gateway inspects more than one credential of the same type and retains validated credentials for use in generating outgoing assertions.

To add a SAML assertion to outgoing requests:

Step 1 In the **Virtual Services** browser, click on the virtual service or service descriptor for which you want to configure credential generation.

Step 2 In the service settings page, click the **Edit** link next to the **Service Authentication** heading. In a basic virtual service, you will first need to display the **Backend Service** settings by clicking the expand control.

Step 3 You can generate a single token or multiple outgoing SAML tokens, as follows:

- To have the ACE XML Gateway generate a single SAML token, from the **SAML Token** menu of the Service Authentication page, choose **Send one SAML token with an Authentication Statement as specified**.
- To have multiple SAML Tokens generated based on data from WSS Username Token, Client SSL Certificate, or set by an extension, choose **Send multiple SAML tokens with an Authentication Statement as specified**.

The SAML token configuration settings appear.

Step 4 For multiple SAML token generation, choose the data sources for the tokens from the **Credential Sources** section. For example, if you choose WSS Username Token as the source, a SAML token will be created for each WSS Username Token heading in the incoming request, with the username of the incoming token used as the subject NameIdentifier of the outgoing SAML token.

In this mode, you can also specify handling of inbound SAML tokens, with the option to either strip or pass through the headers from the **Inbound SAML Assertions** menu.

Step 5 If the credential is intended for processing by a particular recipient identified by role, from the **SOAP Role** menu choose the role for the token. The ACE XML Gateway will add the token to a WSS header that contain this role in the outgoing message, or add a header with this role if it does not already exist.

The `role` is an optional attribute of the `Security` tag that should be used to identify the one among possibly multiple recipients of the message who should consume the token. Select from:

- **no role**, the default value, indicates that the token is not intended for a particular role.
- **custom** to specify a custom, named role you specify.
- **next** to indicate that the WSS header is intended for the next process that receives the message and is capable of consuming the token.
- **ultimateReceiver** to indicate that the WSS header is intended for the ultimate receiver of the message.

Step 6 Choose the version of the SAML assertion to be generated, 1.0, 1.1, or 2.0. Note that the version you select affects what options are available on the page.

Step 7 The **Subject NameIdentifier** identifies the entity for whom the token is making an identity assertion. You can configure the **Subject NameIdentifier** in the generated token in several ways, depending on whether you are generating multiple tokens or a single token:

- If generating multiple tokens, optionally select the **Set Subject Name Identifier to User DN, if available** option if you want the DN used to perform an LDAP lookup of the client for authentication purposes to be used as the subject nameIdentifier value of the generated tokens.
- If generating a single token, choose from these options in the **Subject NameIdentifer** menu:
  - **SAML Token Subject NameIdentifier** uses the subject of a SAML assertion in the incoming request for the subject in the outgoing request assertion.
  - **HTTPS Certificate Subject DN** uses the DN of the subject of a certificate used to authenticate the request.
  - **HTTP Basic Auth Username** takes the username from the HTTP Basic Auth credential used to authenticate the request.
  - **XPath Username** takes the username value from an XPath Password credential used to authenticate the incoming request.
  - **WSS UsernameToken** uses the username of a WSS Username/Password credential used to authenticate the request.
  - **fixed value** allows you to provide a specific, fixed value for the NameIdentifier element. When you choose this item, a text field appears in which you can type the identifier to use.

Step 8 Optionally, add a time-based condition to the SAML Token to constrain the validity of the assertion based on its timestamp.

Configure the following constraints:

- **NotBefore** causes a `NotBefore` attribute to be added to the assertion with the configured time. This indicates the earliest time the assertion is to be considered valid.
- **NotOnOrAfter** causes a `NotOnOrAfter` attribute to be added to the message, indicating the expiration time of the assertion.

  In either case, the ACE XML Gateway computes the value of the attribute based on the time the assertion is generated, for example:

  ```
  <Conditions NotBefore="2006-03-24T21:54:08Z" NotOnOrAfter="2006-03-25T05:54:13Z">
  ```

Step 9 Optionally, add one or more audience conditions to the SAML Token by clicking the **Audience** checkbox and entering the URI of the intended audience (or relying party) of the assertion.

Step 10 Specify a confirmation method value for the assertion by selecting one of these options from the **Confirmation Method** menu:

- **Sender Vouches** tells the relying party that the SAML assertion is vouched for by the ACE XML Gateway itself, and that the message itself does not necessarily provide any means of authenticating the subject of the assertions or the assertions themselves. This implies that a trust relationship exists between the ACE XML Gateway and the backend service for the assertion to be relied upon by the service.
- **Holder-of-key** specifies that the subject is covered by an XML Signature that the ACE XML Gateway can verify using the SSL/TLS certificate of the authenticator that accepted the original incoming request.

  If you choose the **Holder-of-Key** confirmation method, you must also choose a confirmation key.

  For the **Sender Vouches** confirmation method, choosing a confirmation key is optional.

Step 11 Choose a key resource from the **Confirmation Key** menu to specify the key to appear in the `KeyInfo` element of the subject confirmation.

Step 12 Optionally, have the token signed with the confirmation key by enabling the **Sign the SAML token with the Confirmation Key** option. The signature can be used by the recipient to verify the source and integrity of the token. For the signature, you can further choose from these options:

a. Include the certificate used to sign the token by choosing the **Include X.509 certificate with signature**.

b. If the message is to be consumed by an endpoint developed with Microsoft .NET WSE 2.0, click the **Add unqualified "Id" attributes to Assertion elements for .NET WSE 2.0 compatibility** checkbox.

   This directs the ACE XML Gateway to add to signed elements the `Id` attributes required by Microsoft .NET WSE 2.0.

Step 13 If you chose the option **Send multiple SAML tokens with an Authentication Statement as specified** for generating SAML tokens, an additional configuration option appears, **Include LDAP records, if available, as SAML Attribute**. If this option is enabled, values from LDAP records retrieved as a result of an LDAP directory lookup for the purpose of authenticating the original request are included as SAML Attribute statements in the generated tokens. The values include the dn, the cn and any filtered attributes. That is, if you use * for all attributes in the verification settings for the authenticator, then all attributes on the LDAP record that is found by the authenticating server are propagated to SAML attributes. If you restrict the filter to say, just attribute “member”, then only “member=groupName” will be included with the dn and cn.

Step 14 If you chose to generate SAML Attribute statements from LDAP records, as described in the previous step, or you have chosen to map WSS UsernameToken attributes to SAML Attribute statements, specify the default namespace the Gateway is to use to qualify those attributes by typing the namespace in the URI text field. The field is labelled **Attribute Namespace URI** for SAML 1.0 and 1.1 tokens and **Attribute Format URI** for SAML 2.0. Attributes in the generated token that are not already namespace-qualified will be qualified with this URI.

The Credential Mapping settings in the **System Management >** Gateway **Settings** page includes an option that directs the Gateway to include custom attributes from authenticated WSS UsernameTokens as attributes in the SAML AttributeStatements of the SAML tokens it generates.

The namespace URI you enter here is added to unqualified attributes derived from both LDAP record lookups and WSS UsernameToken attributes.

Step 15 Click **Save Changes** and deploy the policy to have your changes take effect at the ACE XML Gateway.