Certificate Attributes

Contents

Overview

The Enterprise Gateway can authorize access to a Web Service based on the X.509 attributes of an authenticated client's certificate. For example, a simple **Certificate Attributes** filter might only authorize clients whose certificates have a Distinguished Name (DName) containing the following attribute: *O=oracle*. In other words, only "oracle" users are authorized to access the Web Service.

An X.509 certificate consists of a number of fields. The `Subject` field is the one of most relevance to this tutorial. It gives the DName of the client to which the certificate belongs. A DName is a unique name given to an X.500 directory object. It consists of a number of attribute-value pairs called Relative Distinguished Names (RDNs). Some of the most common RDNs and their explanations are as follows:

- `CN`: CommonName
- `OU`: OrganizationalUnit
- `O`: Organization
- `L`: Locality
- `S`: StateOrProvinceName
- `C`: CountryName

For example, the following is the DName of the *sample.p12* client certificate supplied with the Enterprise Gateway:

```
CN=Sample Cert, OU=R&D, O=Company Ltd., L=Dublin 4, S=Dublin, C=IE
```

Using the **Certificate Attributes** filter, it is possible to authorize clients based on, for example, the "CN", "OU", or "C" in the DName.

Configuration

The **X.509 Attributes** table lists a number of attribute checks that will be run against the client certificate. Each entry tests a number of certificate attributes in such a way that the check will only pass if all of the configured attribute values match those in the client certificate. So, in effect, the attributes listed within a single attribute check are AND-ed together.

For example, imagine the following is configured as an entry in the **X.509 Attributes** table:

```
OU=Eng, O=Company Ltd
```

If the Enterprise Gateway receives a certificate with the following DName, this attribute check will pass because *all* the configured attributes match those in the certificate DName:

```
CN=User1, OU=Eng, O=Company Ltd, L=D4, S=Dublin, C=IE
CN=User2, OU=Eng, O=Company Ltd, L=D2, S=Dublin, C=IE
```

However, if the Enterprise Gateway receives a certificate with the following DName, the attribute check will fail because the attributes in the DName do not match *all* the configured ones (i.e. the "OU" attribute has the wrong value):

```
CN=User1, OU=qa, O=Company Ltd, L=D4, S=Dublin, C=IE
```

The **X.509 Attributes** table can contain several attribute check entries. In such cases, the attribute checks (i.e. the entries in the table) are OR-ed together, so that if any of the checks succeed, the overall **Certificate Attributes** filter succeeds.

So to summarize:

- Attribute values within an attribute check will only succeed if *all* the configured attribute values match those in the DName of the client certificate.
- The filter will succeed if *any* of the attribute checks listed in the **X.509 Attributes** table succeed.

To configure a **Certificate Filter** complete the following fields:

Name:
Enter a name for the filter here.

X.509 Attributes:
To add a new X.509 attribute check, click the **Add button** button. In the **Add X.509 Attributes** dialog, enter a comma-separated list of name-value pairs representing the X.509 attributes and their values, for example, "OU=dev,O=Company".

The new attribute check will appear in the **X.509 Attributes** table. Existing entries can be edited and deleted by clicking the **Edit** and **Remove** buttons respectively.