API Gateway

Version 7.6.2

14 July 2020

Validation Authority Interoperability Guide

This documentation describes the following Axway software:

Axway API Gateway 7.6.2

Contents

Preface

This guide describes how to configure API Gateway and Axway Validation Authority to work together.

Who should read this guide

The intended audience for this guide is system integrators who are responsible for integrating API Gateway with other applications.

Others who might find parts of this guide useful include network or systems administrators and other technical or business users.

How to use this guide

This guide should be used in conjunction with the other guides in the API Gateway documentation set. Before configuring API Gateway to work with Axway Validation Authority you should understand exactly what message filters are, and how they are chained together to create a message policy. These concepts are documented in detail in the *API Gateway Policy Developer Guide*.

You should also consult the documentation set for Axway Validation Authority.

Before you begin integrating API Gateway with Axway Validation Authority, review this guide thoroughly. The following is a brief description of the contents of each section:

API Gateway and Axway Validation Authority on page 7 – Provides an overview of integrating API Gateway with Axway Validation Authority.

Configure API Gateway on page 8 – Describes how to configure the **OSCP Client** filter in Policy Studio.

Direct trust model on page 9 – Describes how to configure API Gateway and Axway Validation Authority for the direct trust model.

VA delegated trust model on page 12 – Describes how to configure API Gateway and Axway Validation Authority for the VA delegated trust model.

Related documentation

The AMPLIFY API Management solution enables you to create, publish, promote, and manage Application Programming Interfaces (APIs) in a secure and scalable environment. For more information, see the *AMPLIFY API Management Getting Started Guide*.

The following reference documents are also available on the Axway Documentation portal at https://docs.axway.com:

- *Supported Platforms*

  Lists the different operating systems, databases, browsers, and thick client platforms supported by each Axway product.

- *Interoperability Matrix*

  Provides product version and interoperability information for Axway products.

Support services

The Axway Global Support team provides worldwide 24 x 7 support for customers with active support agreements.

Email support@axway.com or visit Axway Support at https://support.axway.com.

See "Get help with API Gateway" in the *API Gateway Administrator Guide* for the information that you should be prepared to provide when you contact Axway Support.

Training services

Axway offers training across the globe, including on-site instructor-led classes and self-paced online learning. For details, go to: http://www.axway.com/support-services/training

Accessibility

Axway strives to create accessible products and documentation for users.

This documentation provides the following accessibility features:

Screen reader support

- Alternative text is provided for images whenever necessary.
- The PDF documents are tagged to provide a logical reading order.

Support for high contrast and accessible use of colors

- The documentation can be used in high-contrast mode.
- There is sufficient contrast between the text and the background color.
- The graphics have the right level of contrast and take into account the way color-blind people perceive colors.

API Gateway and Axway Validation Authority 1

This guide describes the interoperability between API Gateway and Axway Validation Authority. For specific information about the installation and general use of either API Gateway or Axway Validation Authority, refer to their respective documentation.

Why use the products together

Axway Validation Authority server (VA server) ensures the integrity and validity of online transactions by delivering real-time validation of digital certificates issued by any Certification Authority (CA). To validate a digital certificate, a client application can query the VA server using the Online Certificate Status Protocol (OCSP) as an alternative to retrieving Certificate Revocation Lists (CRLs).

In API Gateway, you can use the **OCSP Client** filter to retrieve certificate revocation status from an OSCP responder, such as Axway Validation Authority. When using Axway Validation Authority as an OCSP responder, the following use cases are supported:

- *Direct trust model* on page 9
- *VA delegated trust model* on page 12

Prerequisites

The prerequisites for API Gateway and Axway Validation Authority interoperability are as follows.

API Gateway

You must install Axway API Gateway version 7.6.2 or higher, and have a valid API Gateway license file from Axway.

Axway Validation Authority

You must install Axway Validation Authority version 4.11.2 or higher and have a valid Validation Authority license file from Axway.

Configure API Gateway 2

This section describes how to configure API Gateway to work together with Axway Validation Authority. This involves configuring an **OCSP Client** filter to retrieve certificate revocation status from Axway Validation Authority.

Configure an OCSP client filter

The **OSCP Client** filter is available in the **Certificate** category in Policy Studio.

The input to the filter is a message attribute containing the certificate to verify.

The return value of the filter is `True` if the certificate has a status of GOOD, and `False` if the certificate has a status of REVOKED, or UNKNOWN, or an exception occurs.

The filter also outputs the following message attributes:

- `ocsp.response.certificate.status`
- `ocsp.response.signing.certificate`

For more information on the **OCSP Client** filter, including the input and output message attributes, and how to configure the settings on the filter dialog, see the *API Gateway Policy Developer Filter Reference*.

Direct trust model 3

When using the direct trust model with Axway Validation Authority, the signing certificate is the VA server certificate, which is self-signed.

In this model, OCSP responses are signed with the OCSP signing certificate of the VA server. The signing certificate is not included in the OCSP response.

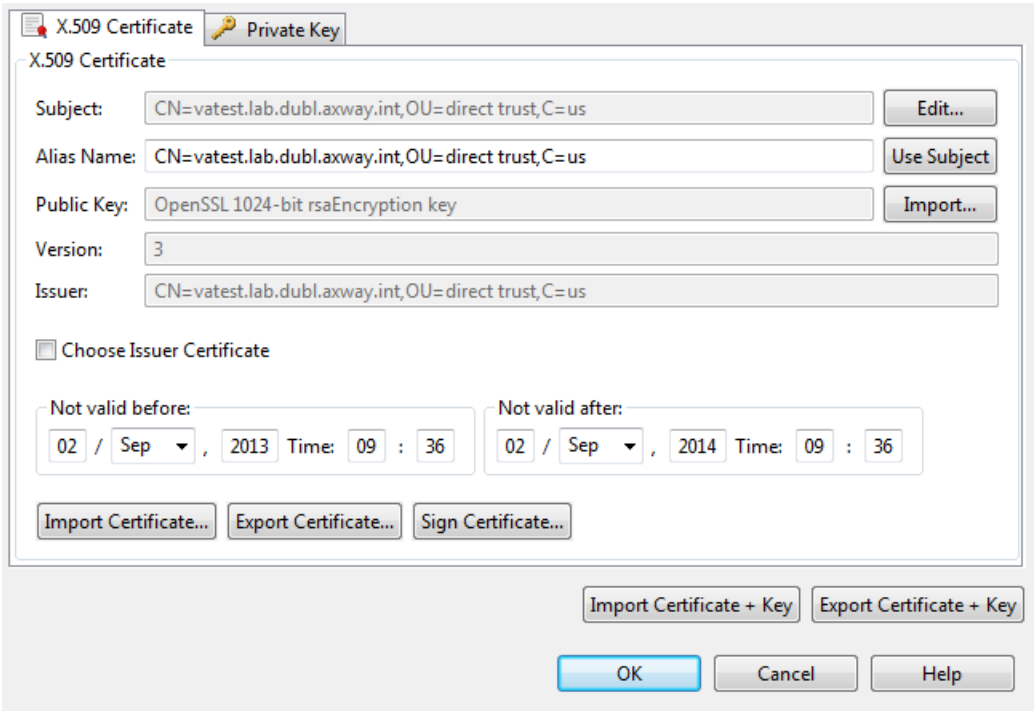
Configure direct trust

To configure the direct trust model, perform the following steps:

1. *Import the certificate* on page 9
2. *Configure an OCSP client filter* on page 10

Import the certificate

Using Policy Studio, import the certificate into the API Gateway certificate store.



For more information on importing certificates, see the *API Gateway Policy Developer Guide*.

Configure an OCSP client filter

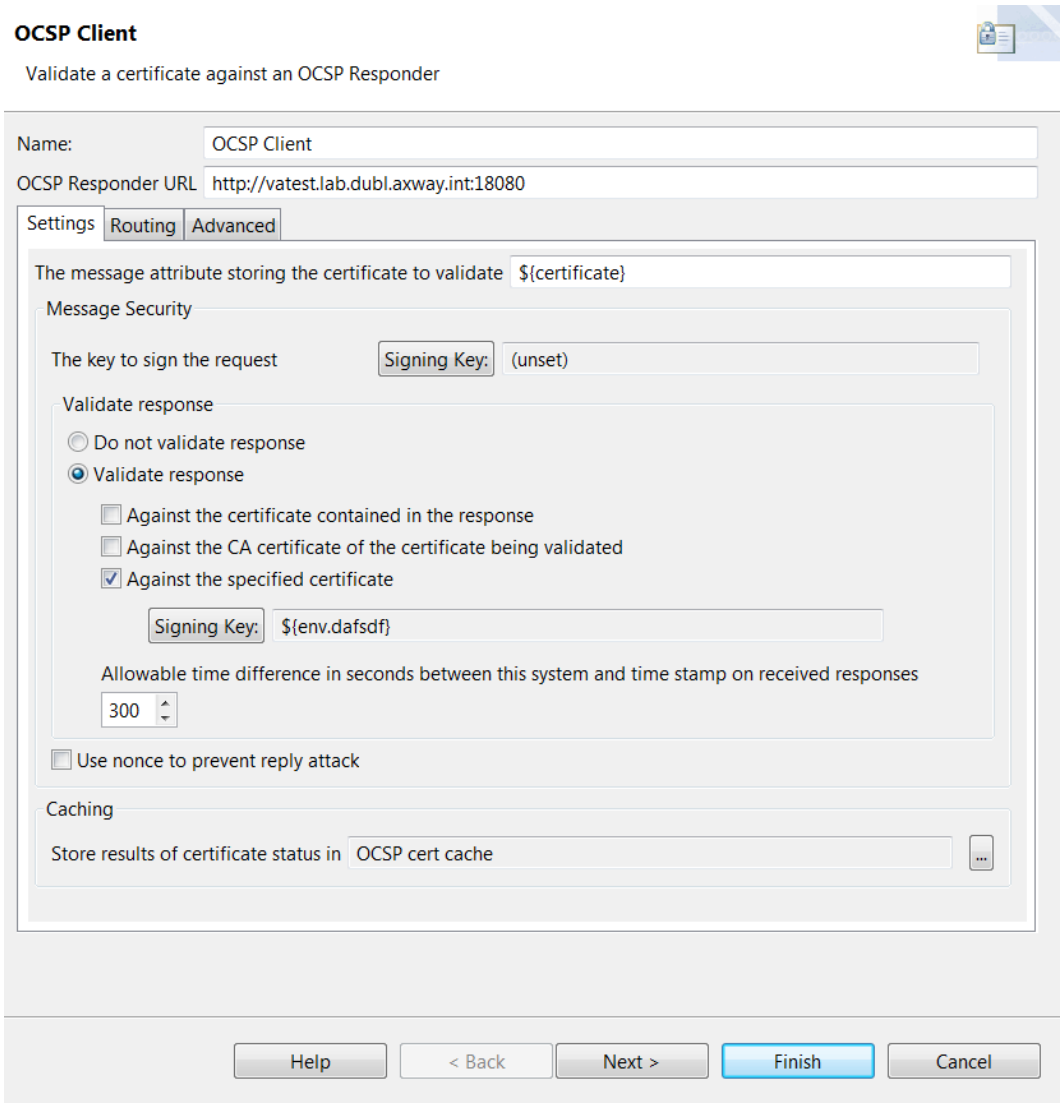
In Policy Studio, configure an **OCSP Client** filter with the following settings:

General settings

- Enter the address of the Validation Authority system configured for direct trust in the **OCSP Responder URL** field. This example uses an HTTP connection.

Settings tab

- Enter the name of the message attribute that contains the certificate to validate. In this example the target certificate is extracted from a message attribute called `certificate`.
- Select the **Validate response** option and select the **Against the specified certificate** check box. Click **Signing Key** to choose the VA server OCSP signing certificate from the certificate store or to specify a certificate to bind to at runtime.



You can use the default values for the other settings. For more information on the settings, see the *API Gateway Policy Developer Filter Reference*.

VA delegated trust model 4

When using the VA delegated trust model with Axway Validation Authority, the signing certificate is the OCSP signing certificate of the delegated VA root.

In this model, the signing certificate is included in the OCSP response. API Gateway might not have this certificate. If not, it must have the issuer (CA) certificate of the signing certificate.

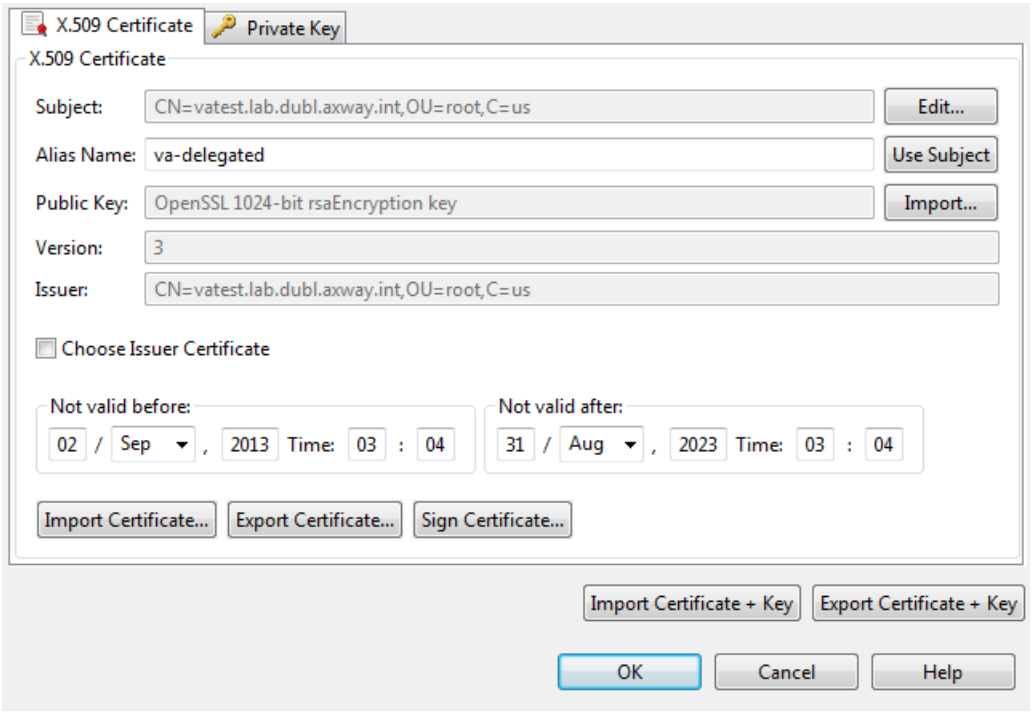
Configure VA delegated trust

To configure the VA delegated trust model, perform the following steps:

1. *Import the signing certificate* on page 12
2. *Configure a policy with two OCSP client filters* on page 13

Import the signing certificate

Using Policy Studio, import the signing certificate into the API Gateway certificate store.

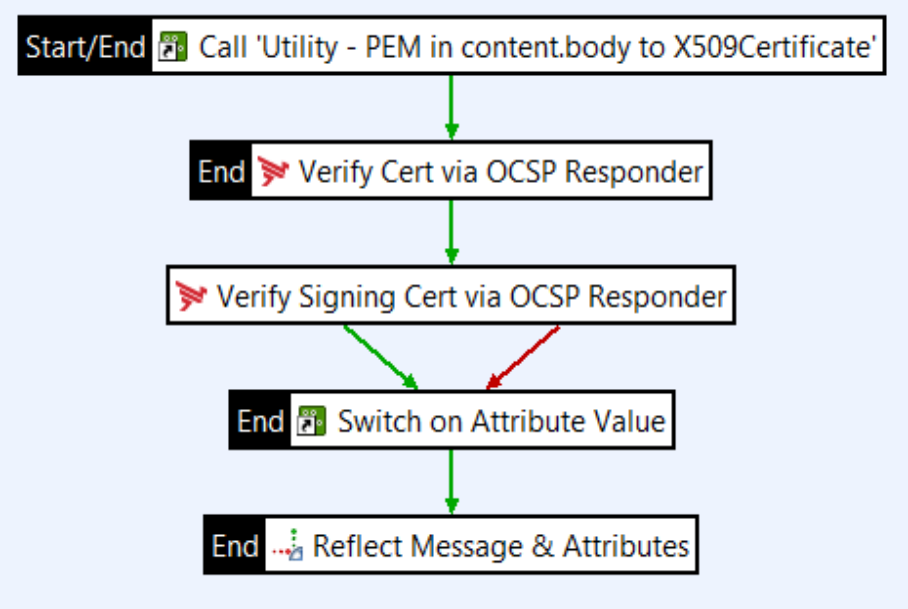


For more information on importing certificates, see the *API Gateway Policy Developer Guide*.

Configure a policy with two OCSP client filters

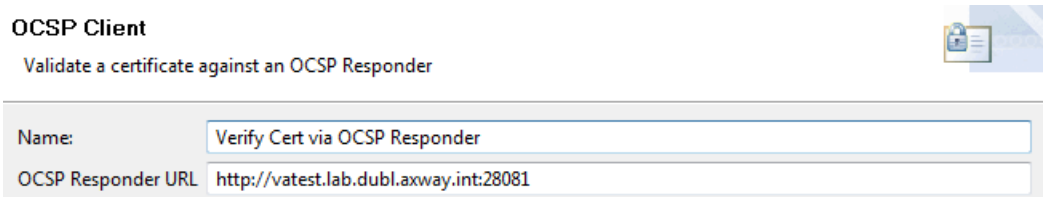
This use case requires two chained OCSP client filters:

- One filter to verify the target certificate
- One filter to verify the response signing certificate

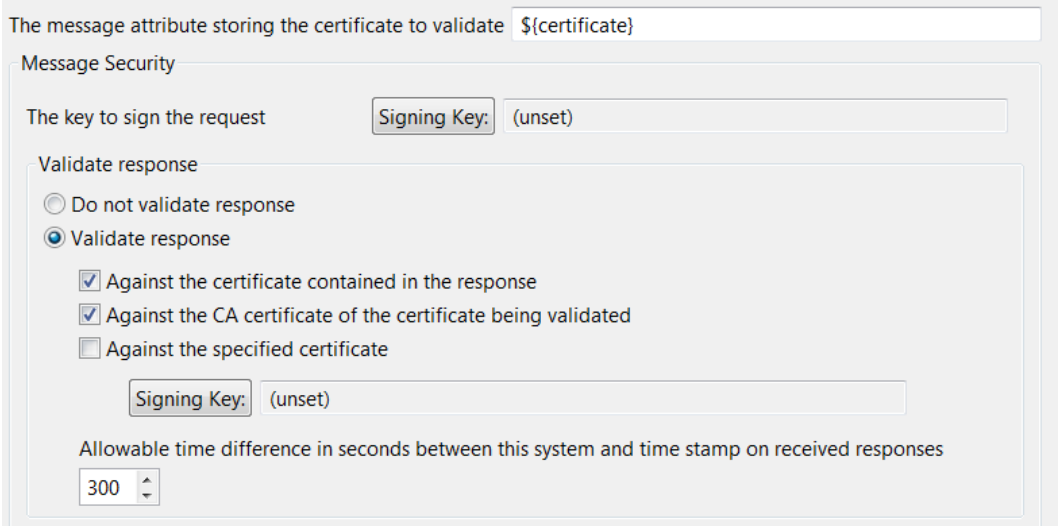


Verify target certificate

In this OCSP client filter, set the **OCSP Responder URL** to point to the VA server configured for VA delegated trust. This server can validate the target certificate (it has the target certificate issuer/CA details).



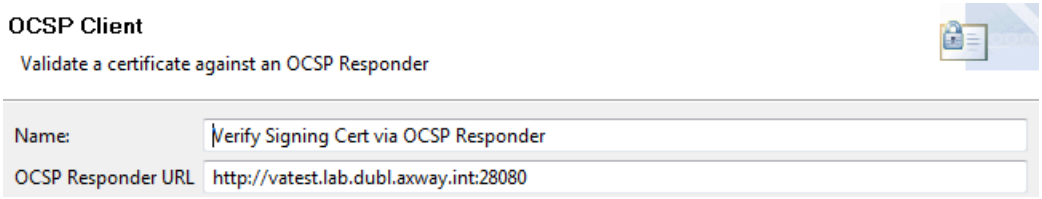
Extract the certificate from the `certificate` message attribute. Select the **Validate response** option and select the **Against the certificate contained in the response** and the **Against the CA certificate of the certificate being validated** check boxes.



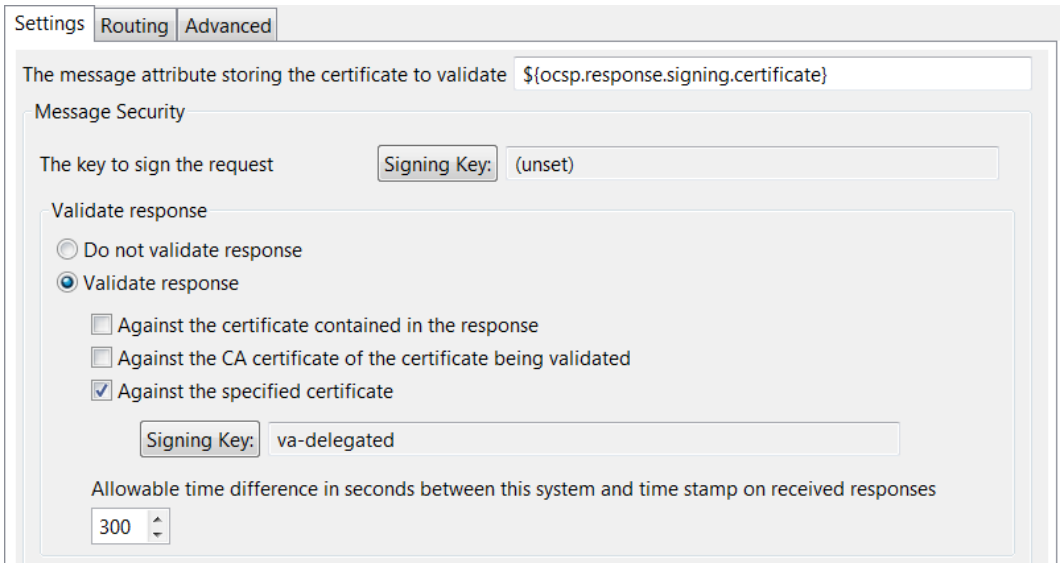
Verify signing certificate

Validation Authority returns the OCSP responder URL to use in the signing certificate's AIA extension. The API Gateway OCSP client does not support extraction of this information.

This example directly uses and trusts the root VA server:



Extract the signing certificate from the `ocsp.response.signing.certificate` message attribute. Select the **Validate response** option and select the **Against the specified certificate** check box. Click **Signing Key** to select the root VA certificate.



For more information on the OCSP client filter settings, see the *API Gateway Policy Developer Filter Reference*.