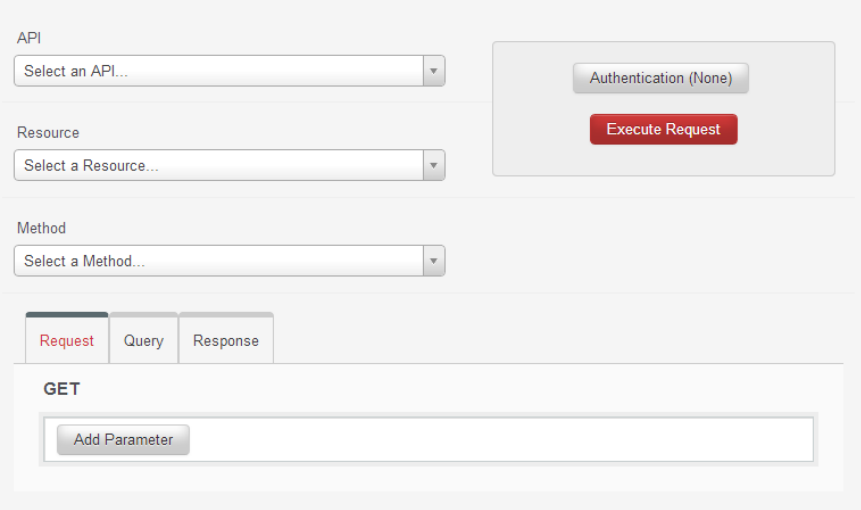
Alaska Airlines Developer Portal

Testing Tool Guide

The API Explorer lets developers interactively discover your APIs. By making choices from among your API's valid resources and methods, and then submitting queries and viewing responses, developers can gain a better understanding of not only how your APIs work, but also the authentication methods required to access them.

1. Log in to the API Portal. The API Portal for your organization is displayed.
2. On the menu bar, click [Resources] to access the Resources page.
3. Click API Explorer on the navigation sidebar. The API Explorer interface displays.



4. Complete the following fields.

Setting	Description
API	Choose the WADL/API to use from the drop-down list.
Resource	Choose the resource for the selected API from the drop-down list.
Method	Choose the method to use for the selected resource. **Note**: This list may or may not contain an entry as this field is optional. If no methods are displayed, the API Explorer defaults to using the GET method.
[Request] tab	This tab is used to set the resource and method input parameters (if available).
[Add Parameter]	This control is under the [Request] tab. It displays the Add Parameter dialog that is used to add additional parameters that are not otherwise specified in the WADL file. Complete the Add Parameter dialog as follows: • Name: Enter the name of the parameter to add. This field is required.

	• Value: Enter the value of the parameter to add. This field is required. • Parameter Type: Choose a parameter type from the following: Query: The input is part of the query parameter. Header: The input is part of the request header. • Click [Add] to validate the input (for existence of value) and add the input to the request.
[Authentication]	Displays the Authentication dialog where you attach an authentication to the selected API. For details on how to authenticate an API, see "Authenticating an API" below. **Note**: The authentication type and requirement are not specified in the WADL file.

5. Click [Execute Request]. The results are displayed in the [Response] tab.

The [Query] tab displays the actual result being sent to the server:

- Raw request that contains the HTTP request method
- Full request URL, including the query parameters
- Request headers
- Request body (if available)

Authenticating an API

In order for the request to execute correctly, an API must be authenticated on the Layer 7 Gateway.

API Key

1. Choose the API Key from the Service Authentication drop-down list.

2. Enter the Name of the API Key to add. This field is required.

3. Enter the Value of the API Key to add. This field is required. The API key must be generated on the Layer 7 API Portal when registering an application (see Developer's Manual).

4. Select whether the API Key Type is part of the Query parameter, or part of the request Header.

5. Click [OK] to validate your input and add it to the request.

HTTP Basic

1. Choose HTTP Basic from the Service Authentication drop-down list.

2. Enter the Username and Password to authenticate.

3. Click [OK] to validate your input and add it to the request.

OAuth 1.0

1. Choose OAuth 1.0 from the Service Authentication drop-down list.

2. Complete the following fields:

Setting	Description
Client Key	Enter the client key assigned by the service provider. If using the Layer 7 OAuth Toolkit, enter the API key, which is generated on the portal when registering an application.
Client Secret	Enter the client secret assigned by the service provider. If using the Layer 7 OAuth Toolkit, enter the API secret, which is generated on the portal when registering an application.
Request URL	Enter the URL/endpoint to request an unauthorized request token. This URL is required. This URL should be a fully qualified hostname matching the OAuth server (Layer 7 Gateway) SSL certificate.
Authorization URL	Enter the URL/endpoint to authorize a request token. This URL is optional. When omitted, it will be a one-legged OAuth scheme (that is, the token returned by the Request URL is already authorized).
Access URL	Enter the URL/endpoint to exchange an authorization token for an access token. This URL is required.

3. Click [OK] to validate your input and add it to the request.

Technical Note: If OAuth 1.0 authentication is used and an API is mapped with a WADL that includes a POST method with "representation" elements, that POST method element should not contain query parameters or query strings. Similarly, you must not add any query parameters in the Add Parameter dialog, otherwise the resulting OAuth 1.0 token validation will fail.

OAuth 2.0

It is also possible to use the OAuth 2.0 authentication method. The OAuth 2.0 method defines four base grant types: Authorization Code, Implicit, Resource Owner Password Credentials, and Client Credentials.

With OAuth 2.0, the Grant Type you choose affects the process flow. For the Authorization Code and Implicit grant types, the flow is as follows:

1. The browser redirects the user to the specified authorize endpoint.

2. User authenticates and grants access to the application via the service provider.

3. Once access has been granted or denied, the service provider will redirect the

user back to the specified page as defined by redirect_uri.

4. The access tokens are retrieved from the URI fragment as attached by the

service provider.

The Resource Owner Password Credentials and Client Credentials grant types do not involve any redirection. The Resource Owner Password Credentials grant type allows for an access token to be retrieved directly via username and password. With the Client Credentials grant type, access tokens are requested by providing the Client ID and Client Secret to the Token Endpoint.

1. Choose OAuth 2.0 from the Service Authentication drop-down list.

2. Complete the following fields:

Setting	Description
Grant Type	Choose from one of the following: • Authorization Code: This grant type is designed to authorize a client via an intermediary server, where instead of requesting authorization directly from the resource owner, the client directs the resource owner to an authorization server. • Implicit: This grant type is designed for clients implemented in the web browser. Note: There are additional security risks associated with this grant type. • Resource Owner Password Credentials: This option grants access using the username and password of the resource owner. This grant type does not involve any redirection as it allows for an access token to be retrieved directly by providing a username and password. • Client Credentials: This grant type does not involve any redirection. Access tokens are requested by providing the Client ID and Client Secret to the Token Endpoint.
Client ID	Enter the ID assigned to the user from the service provider. This may be the same as the API key generated on the portal when registering an application.
Client Secret	Enter the client secret assigned by the service provider. This field does not appear when the Implicit Grant Type is selected.
Scope	Enter the "scope" or permission of the access. For example, “scope = read” can mean that access is read only. Refer to the service provider for a list of available scopes and requirements. Depending on the service provider, this may be a required field.
Authorize Endpoint	Enter the URL/endpoint to authorize a request token. This field does not appear if the Resource Owner Password Credentials or the Client Credentials Grant Type is selected.
Token Endpoint	Enter the endpoint from which the client will obtain an access token. This field does not appear when the Implicit Grant Type is selected.
Username	Enter the username to be used to obtain the token. This method should only be used in a high trust environment. The Username field only appears if Resource Owner Password Credentials is selected.
Password	Enter a password to be used to obtain the token. This method should only be used in a high trust environment. The Password field only appears if Resource Owner Password Credentials is selected.

3. Click [OK] to validate your input and add it to the request.