Secure your Backend Services

WSO2 API Cloud allows you to turn your backend services into managed APIs through which subscribers can consume your backend services. According to the architecture of WSO2 API Cloud, all API calls that go out to your backend services go through the Cloud’s API Gateway. The API Gateway handles user requests, user authentication via OAuth, enforces security policies etc.

The API Gateway has the ability to intercept API requests and apply various security policies and mechanisms to secure the connection between the API Gateway and your backend service. Upon validation of a policy, the Gateway passes Web service calls to the actual backend.

In this tutorial, you learn the different ways in which you can secure the link between WSO2 API Cloud and the backend services of the APIs in the API Cloud.

Let's get started.

- Using basic authentication
- Using digest authentication
- Using a custom authorization token
- Using Mutual SSL (certificate-based API Gateway)
- Whitelisting IPs

Using basic authentication

One of the simplest ways to enforce access control to Web resources is using a username and password (i.e., basic authentication).

1. Secure your backend services using a username and password.

   Next, design your API in WSO2 API Cloud in a way that the API sends the authentication details with the request that is going to the backend.

2. Log in to the API Publisher and click the Edit icon of the API that points to a public backend service you secured. For example:
3. Go to the **Implement** tab of the API, and click the **Show More Options** link. Then, set the **Endpoint Security Scheme** to **Secured**, the **Endpoint Auth Type** to **Basic Auth** and give the credentials that you used to secure your backend service.

You have now configured the API to send the basic auth credentials with a request that goes to the backend.

**Using digest authentication**

Digest authentication is similar to basic authentication, but is more secure, and prevents replay attacks. It applies an MD5 cryptographic hash using nonce values (a one-time-use string) to the credentials before sending them to the backend.

1. Secure your backend services using digest authentication.
   Next, design your API in WSO2 API Cloud in a way that the API sends the authentication details with the request that is going to the backend.
2. Log in to the API Publisher and click the **Edit** icon of the API that points to a public backend service you secured. For example:
3. Go to the Implement tab of the API, and click the Show More Options link. Then, set the Endpoint Security Scheme to Secured, the Endpoint Auth Type to Digest Auth and give the credentials that you used to secure your backend service.

You have now configured the API to send the digest auth credentials with a request that goes to the backend.

**Using a custom authorization token**

Rather than using credentials, you can pass a token (usually a string or a series of numbers) to the backend with the API calls. This custom authorization token which should be recognized and validated by your backend in order to be granted access. For a step-by-step tutorial, see Pass a Custom Authorization Token to the Backend.

**Using Mutual SSL (certificate-based API Gateway)**

In Mutual SSL, also known as certificate-based mutual authentication, trust between the API Cloud and your backend services are established by verifying a provided certificate so that both parties are sure of each other's identity. The diagram below depicts this scenario:
To set up, provide a trusted certificate to the WSO2 Cloud team as follows:

1. Log in to the API Cloud and click the **Support** menu at the top.

2. Submit a request to the WSO2 Cloud team with your backend hostname.

3. You get a response email from WSO2. After that is received, send us the backend certificate with which you want to configure mutual SSL (e.g., your_backend_cert.crt).

4. We add your certificate to WSO2 servers and send you our public certificate.

5. You add the public certificate to your backend servers.

### Whitelisting IPs

You can secure your backend in such a way that it only accepts calls proxied by the API Cloud. **Configure your network to accept the IPs of trusted sources such as WSO2 API Cloud.** This makes your backend services accessible to API consumers who make the requests via the API Cloud.

To get started, click the **Support** menu in the **API Cloud** interface and submit your request. WSO2 will respond with the IP range that you need to whitelist.