Protect Platform authentication

To make calls to Protect Platform APIs that work in conjunction with the Protect Platform, you must provide authentication details with each request. Telesign offers the following authentication choices:

- Basic
- Bearer

This page explains overall security requirements, describes each authentication method, explains how to implement each.

Each Protect Platform API endpoint supports either one or both of these methods; see the reference documentation for an endpoint to check which auth methods it supports.

Overall security requirements

Protocol

You must use the HTTPS protocol for every request to Telesign. HTTP is not supported.

TLS and certificates

Transport Layer Security (TLS) is required for all connections through the Application Load Balancer (ALB). The listener is configured to enforce modern TLS policies (for example, **TLS 1.3 with fallback to TLS 1.2**) and requires a valid ACM-issued certificate.

We strongly recommend relying on **standard PKI certificate path validation**. The ALB does not explicitly support locally pinned certificate validation.

> ! WARNING:
>
> Using locally pinned certificates can cause unexpected service disruptions when ACM certificates are rotated or renewed.

DNS regions

To ensure optimal performance and compliance, services are deployed in multiple geographic regions. Each region has a specific DNS endpoint that must be used when sending requests. Selecting the correct region helps reduce latency and ensures that your traffic remains within the desired geographic boundaries.

Region Name	Region	DNS
US East (N. Virginia)	us-east-1	https://us-east-1.di-platform.telesign.com
Asia Pacific (Jakarta)	ap-southeast-3	https://ap-southeast-3.di-platform.telesign.com
Asia Pacific (Mumbai)	ap-south-1	https://ap-south-1.di-platform.telesign.com

Basic authentication

A request using Basic authentication sends an encoded string that includes your User name, Password and API Key.

How to implement it

1. Obtain your API credentials (username, password, and API key) from the DI portal.
2. Add an Authorization header to your request.

> 📘 NOTE:
>
> Basic credentials must be sent encoded in Base64 using the format `username:password`.

cURL

```
curl POST --location 'https://<DNS Region>/authenticationmanager/v1/authenticate/api' \
--header 'X-Api-Key: ABC12345yusumoN6BYsBVkh+yRJ5czgsnCehZaOYldPJdmFh6NeX8kunZ2zU1YWaUw/0wV6xfw==' \
--header 'Content-Type: application/json' \
--header 'Authorization: Basic
RkZGRkZGRkYtRUVFRS1EREReLTEyMzQtQUIxMjM0NTY3ODkwOlRFOHNUZ2c0NXl1c3Vtb042QllzQlZraCt5Uko1Y3pnc25DZWhaYU9ZbGRQSmRtRmg2TmVYC
\
--data '{
  "productId": 2
}'
```

3. Send your request. The reference documentation for each endpoint specifies what to expect in the response for an authentication failure or authentication success.

JSON

```
{
  "accessToken":
"RkZGRkZGRkYtRUVFRS1EREReLTEyMzQtQUIxMjM0NTY3ODkwOlRFOHNUZ2c0NXl1c3Vtb042QllzQlZraCt5Uko1Y3pnc25DZWhaYU9ZbGRQSmRtRmg2TmVY
  "expirationTimeSeconds": 27788
}
```

Bearer authentication

To use Bearer authentication, you must first generate a Bearer token using Basic authentication.

> 📘 NOTE:
>
> **Rate limit restriction**: To prevent abuse and ensure fair usage, each token can make **up to a specific number of requests every range of time (seconds).** If you exceed this limit of five petitions within 30 seconds, the server will respond with a **429 Too Many Requests** error, indicating that you've hit the rate cap.

How to implement it

1. **Obtain a access token**:
   - Send a request using Basic authentication as shown in the previous section.
   - The response will include an accessToken along with its `expirationTimeSeconds`.

Example response:

JSON


```
{
  "accessToken":
"RkZGRkZGRkYtRUVFRS1EREReLTEyMzQtQUIxMjM0NTY3ODkwOlRFOHNUZ2c0NXl1c3Vtb042QllzQlZraCt5Uko1Y3pnc25DZWhaYU9ZbGRQSmRtRmg2TmVY
  "expirationTimeSeconds": 27788
}
```


2. **Use the access token**:
   - Extract the `accessToken` value from the response.
   - Include it in the `Authorization` header of subsequent requests to access the products.
     The format must be:

     ```
     Authorization: Bearer
     RkZGRkZGRkYtRUVFRS1EREReLTEyMzQtQUIxMjM0NTY3ODkwOlRFOHNUZ2c0NXl1c3Vtb042QllzQlZraCt5Uko1Y3pnc25DZWhaYU9ZbGRQSmRtRmg2T
     ```

3. **Access token expiration**:
   - The token is only valid for the duration specified in `expirationTimeSeconds`.
   - Once expired, you must request a new token again using Basic authentication. `.

Updated 22 days ago

← Authentication

Try the API Explorer →