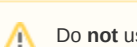
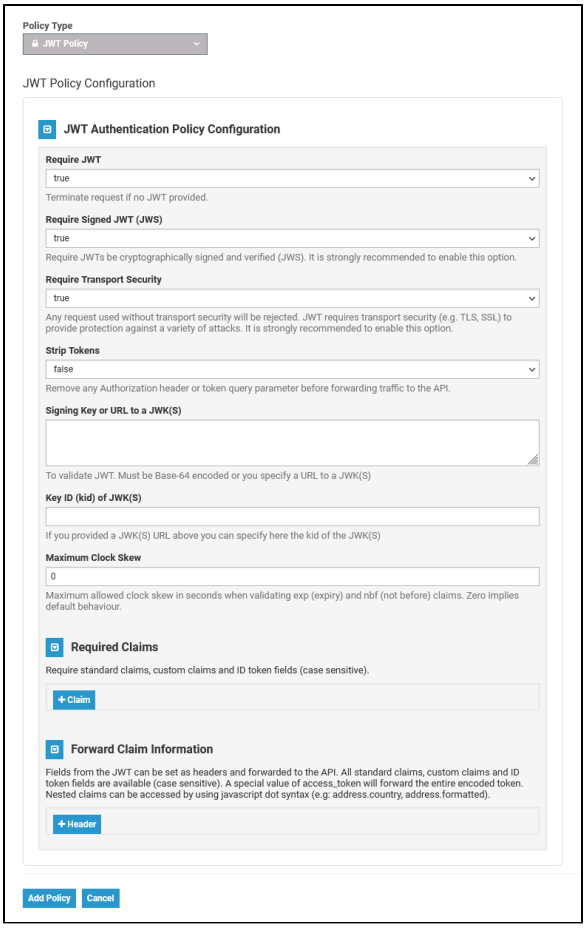
# JWT

The **JWT Policy** helps you to validate JSON Web Tokens (JWT) by providing a signing key or a JSON Web Key Set (JWK(S)). You can also require claims and strip them to forward them as header to the backend API.



Do **not** use the **JWT** policy together with the other authentication policies Keycloak OAuth and BASIC Authentication. The chaining of these policies does not currently work, but this may change in future versions.






Use the links in the field description to access more information on the related subjects.

## Configuration Options

| Option | Description | Possible Values | Default |
|---|---|---|---|
| **Require JWT** | Specify whether request should be terminate if no JWT is provided.<br><br>Make sure that this option is true if you want to use this policy for authentication. | • true: Terminate request if no JWT is provided (default).<br>• false: Do not terminate request if no JWT is provided. | true |

**On this Page:**



**Related Pages:**

- Policies
  - Assigning Policies
  - Policy Configuration
- API Management Best Practices
  - API Security: Authentication and Authorization

| | | | |
|---|---|---|---|
| **Require Signed JWT (JWS)** | Specify whether JWTs must be cryptographically signed and verified (JWS).<br><br>⚠ It is strongly recommended to enable this option. | • true: Require JWTs be cryptographically signed and verified (JWS, default).<br>• false: Do not require JWTs be cryptographically signed and verified. | true |
| **Require Transport Security** | Specify whether requests without transport security will be rejected. JWT requires transport security (e.g. TLS, SSL) to provide protection against a variety of attacks.<br><br>⚠ Please disable the TLS check if you are using Scheer PAS 21.1 or a newer version, because all PAS components are running behind a proxy server. | • true: Reject any request without transport security (default).<br>• false: Do not reject requests without transport security. | false |
| **Strip Tokens** | Specify whether Authorization header or token query parameter should be removed before forwarding traffic to the API. | • true: Remove any Authorization header or token query parameter before forwarding traffic to the API.<br>• false: Do not remove Authorization header or token query parameter before forwarding traffic to the API (default). | false |
| **Signing Key or URL to a JWK(S)** | Specify a signing key or a URL to a JWK(S) to validate JWT. | Must be a Base-64 encoded string or a URL to a JWK(S). | - |
| **Key ID (kid) of JWK(S)** | Specify the key id of the JWK(S) if you provided a JWK(S) URL. | a valid string | - |
| **Maximum Clock Skew** | Specify the maximum allowed clock skew in seconds when validating exp (expiry) and nbf (not before) claims. | a valid integer | 0 |
| **Required Claims** | Specify a list of required claims. If a required claim is not present, access will be rejected. | All standard claims , custom claims and id token fields are available (case sensitive). A special value of **access_token** will forward the entire encoded token. Nested claims can be accessed by using javascript dot syntax (e.g: *address.country* , *address.formatted*). | - |
| **Forward Claim Information** | Specify a list of fields from the JWT to be forwarded to the API as a header. | All standard claims , custom claims and id token fields are available (case sensitive). A special value of **access_token** will forward the entire encoded token. Nested claims can be accessed by using javascript dot syntax (e.g: *address.country* , *address.formatted*). | - |