

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.

Configuration Options

JWT

Basic Configuration

Signing key or salt, to a JWK(S) *

https://nrmc[redacted]keys/look/health/PAS/protocol/openid-connect/certs

To validate JWT, must be Base64 encoded or you specify a URL, to a JWK(S).

Currently, self-signed certificates are not supported.

Key ID (kid) of JWK(S)

If you provided a JWK(S) URL, above, you can specify the kid of the JWK(S) here.

Required Claims

Require standard claims, custom claims and ID token fields (case sensitive). 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 the .JavaScript dot syntax (e.g. address.country, address.formatted).

<input type="checkbox"/>	Claim	Value
<input type="checkbox"/>	user.email	email

AddDelete

Forward Claim Information

Fields from the JWT can be set as headers and forwarded to the API. 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 the .JavaScript dot syntax (e.g. address.country, address.formatted).

<input type="checkbox"/>	Header	Field
<input type="checkbox"/>	Header *	Field *

AddDelete

Advanced Configuration

☒ Require Signed JWT (WSJ)
Require JWT's to be cryptographically signed and verified (WSJ). It is strongly recommended to enable this option.

☐ Strip Tokens
Remove any Authorization header or token query parameter before forwarding traffic to the API.


Maximum Clock Skew *

0

Maximum allowed clock skew in seconds when validating exp (expires) and nbf (not before) claims, uses system default behavior.

CancelBackNext

Basic Configuration

Option	Description	Possible Values	Default
Signing Key or URL to a JWK(S)	<p>Specify a Base-64 encoded signing key or a URL to a JWK(S) to validate JWT.</p> <div>  Self-signed certificates are currently not supported. </div>	<ul style="list-style-type: none"> a Base-64 encoded string or a URL to a JWK(S) 	FQDN path automatically set for your PAS installation
Key ID (kid) of JWK(S)	Specify the key id of the JWK(S) in this field if you provided a JWK(S) URL.	a valid string	-

Required Claims

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 the JavaScript dot syntax (e.g. `address.country`, `address.formatted`).

Option	Description	Possible Values	Default
Claim	Specify a list of required claims. If a required claim is not present, access will be rejected.	a string	-
Value	Determines the content of the claim.	a string	-

Click **Add** to create more rows in the table. Click **Delete** to remove selected rows.

On this Page:

- Configuration Options
 - Basic Configuration
 - Required Claims
 - Forward Claim Information
 - Advanced Configuration

Related Pages:

- Policies
 - Attaching Policies

Forward Claim Information

Fields from the JWT can be set as headers and forwarded to the API. 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 the JavaScript dot syntax (e.g: `address.country`, `address.formatted`).

Option	Description	Possible Values	Default
Field	Specify a list of fields from the JWT to be forwarded to the API as a header.	a string	-
Header	Holds the value of the Field .	a string	-
Click Add to create more rows in the table. Click Delete to remove selected rows.			

Advanced Configuration

Option	Description	Possible Values	Default
Require Signed JWT (JWS)	Specify whether JWTs must be cryptographically signed and verified (JWS). It is strongly recommended to enable this option.	<ul style="list-style-type: none">• enabled• disabled	enabled
Strip Tokens	Enable if the Authorization header or token query parameter should be removed before forwarding traffic to the API.	<ul style="list-style-type: none">• enabled• disabled	disabled
Maximum Clock Skew	Specify the maximum allowed clock skew in seconds when validating exp (expiry) and nbf (not before) claims. 0 implies default behavior.	a valid integer	0