JWT

# JWT#

Work with JSON web tokens in your n8n workflows.

Credentials

You can find authentication information for this node here.

## Operations#

• Decode

• Sign

• Verify

## Node parameters#

This node can be used as an AI tool

This node can be used to enhance the capabilities of an AI agent. When used in this way, many parameters can be set automatically, or with information directed by AI - find out more in the AI tool parameters documentation.

• Credential to connect with: Select or create a JWT credential to connect with.

• Token: Enter the token to Verify or Decode.

• If you select the Sign operation, you'll also have this parameter:  
Use JSON to Build Payload: When turned on, the node uses JSON to build the claims. The selection here influences what appears in the Payload Claims section.

• Use JSON to Build Payload: When turned on, the node uses JSON to build the claims. The selection here influences what appears in the Payload Claims section.

## Payload Claims#

The node only displays payload claims if you select the Sign operation. What you see depends on what you select for Use JSON to Build Payload:

• If you select Use JSON to Build Payload, this section displays a JSON editor where you can construct the claims.

• If you don't select Use JSON to Build Payload, this section prompts you to Add Claim.

You can add the following claims.

### Audience#

The Audience or aud claim identifies the intended recipients of the JWT.

aud

Refer to "aud" (Audience) Claim for more information.

### Expires In#

The Expires In or exp claim identifies the time after which the JWT expires and must not be accepted for processing.

exp

Refer to "exp" (Expiration Time) Claim for more information.

### Issuer#

The Issuer or iss claim identifies the principal that issued the JWT.

iss

Refer to "iss" (Issuer) Claim for more information.

### JWT ID#

The JWT ID or jti claim provides a unique identifier for the JWT.

jti

Refer to "jti" (JWT ID) Claim for more information.

### Not Before#

The Not Before or nbf claim identifies the time before which the JWT must not be accepted for processing.

nbf

Refer to "nbf" (Not Before) Claim for more information.

### Subject#

The Subject or sub claim identifies the principal that's the subject of the JWT.

sub

Refer to "sub" (Subject) Claim for more information.

## Node options#

### Decode node options#

The Return Additional Info toggle controls how much information the node returns.

When turned on, the node returns the complete decoded token with information about the header and signature. When turned off, the node only returns the payload.

### Sign node options#

Use the Override Algorithm control to select the algorithm to use for verifying the token. This algorithm will override the algorithm selected in the credentials.

### Verify node options#

This operation includes several node options:

• Return Additional Info: This toggle controls how much information the node returns. When turned on, the node returns the complete decoded token with information about the header and signature. When turned off, the node only returns the payload.

• Ignore Expiration: This toggle controls whether the node should ignore the token's expiration time claim (exp). Refer to "exp" (Expiration Time) Claim for more information.

exp

• Ignore Not Before Claim: This toggle controls whether to ignore the token's not before claim (nbf). Refer to "nbf" (Not Before) Claim for more information.

nbf

• Clock Tolerance: Enter the number of seconds to tolerate when checking the nbf and exp claims. This allows you to deal with small clock differences among different servers. Refer to "exp" (Expiration Time) Claim for more information.

nbf

exp

• Override Algorithm: The algorithm to use for verifying the token. This algorithm will override the algorithm selected in the credentials.

## Templates and examples#

Browse JWT integration templates, or search all templates