

Authentication



- [Authentication Methods](#)
 - [Authorization Map](#)
 - [User Configuration Map](#)
-

NATS authentication is multi-level. All of the security modes have an [accounts](#) level with [users](#) belonging to those accounts. The decentralized JWT Authentication also has an *operator* to which the accounts belong.

Each account has its own independent subject namespace: a message published on subject 'foo' in one account will not be seen by subscribers to 'foo' in other accounts. Accounts can however define exports and imports of subject(s) streams as well as expose request-reply services between accounts. Users within an account will share the same subject namespace but can be restricted to only be able to publish-subscribe to specific subjects.

Authentication Methods

The NATS server provides various ways of authenticating clients:

- [Token Authentication](#)
- [Plain Text Username/Password credentials](#)
- [Bcrypted Username/Password credentials](#)
- [TLS Certificate](#)
- [NKEY with Challenge](#)
- [Decentralized JWT Authentication/Authorization](#)

Authentication deals with allowing a NATS client to connect to the server. Except for JWT authentication, authentication and authorization are configured in the `authorization` section of the configuration. With JWT authentication the account and user information are stored in the [resolver](#) rather than in the server configuration file.

Authorization Map

The `authorization` block provides *authentication* configuration as well as [authorization](#):

Property	Description
<code>token</code>	Specifies a global token that can be used to authenticate to the server (exclusive of user and password)
<code>user</code>	Specifies a single <i>global</i> user name for clients to the server (exclusive of token)
<code>password</code>	Specifies a single <i>global</i> password for clients to the server (exclusive of <code>token</code>)
<code>users</code>	A list of user configuration maps. For multiple username and password credentials, specify a <code>users</code> list.
<code>timeout</code>	Maximum number of seconds to wait for client authentication
<code>auth_callout</code>	Enables the auth callout extension

User Configuration Map

A `user` configuration map specifies credentials and permissions options for a single user:

Property	Description
<code>user</code>	username for client authentication. (Can also be a user for tls authentication)
<code>password</code>	password for the user entry
<code>nkey</code>	public nkey identifying an user
<code>permissions</code>	permissions map configuring subjects accessible to the user

📄 #3

📄 cocobook-sync 📄 2026-10-28 11:13:58 UTC

📄 cocobook-sync 📄 2026-10-29 01:42:39 UTC