

OCSP Stapling



- [Advanced Configuration](#)
 - [Caching of Staples](#)
-

Supported since NATS Server version 2.3

[OCSP Stapling](#) is honored by default for certificates that have the [status_request Must-Staple flag](#).

When a certificate is configured with OCSP Must-Staple, the NATS Server will fetch staples from the configured OCSP responder URL that is present in a certificate. For example, given a certificate with the following configuration:

```
[ ext_ca ]
...
authorityInfoAccess = OCSP;URI:http://ocsp.example.net:80
tlsfeature = status_request
...
```

The NATS server will make a request to the OCSP responder to fetch a new staple which will then be presented to any TLS connection that is accepted by the server during the TLS handshake.

OCSP Stapling can be explicitly enabled or disabled in the NATS Server by setting the following flag in the NATS configuration file at the top-level:

```
ocsp: false
```

Note: When OCSP Stapling is disabled, the NATS Server will not request staples even if the certificate has the Must-Staple flag.

Advanced Configuration

By default, the NATS Server will be running in OCSP `auto` mode. In this mode the server will only fetch staples when the Must-Staple flag is configured in the certificate.

There are other OCSP modes that control the behavior as to whether OCSP should be enforced and the server should shutdown if the certificate runs with a revoked staple:

Mode	Description	Server shutdowns when revoked
auto	Enables OCSP Stapling when the certificate has the must staple/status_request flag	No
must	Enables OCSP Staping when the certificate has the must staple/status_request flag	Yes
always	Enables OCSP Stapling for all certificates	Yes
never	Disables OCSP Stapling even if must staple flag is present (same as <code>ocsp: false</code>)	No

For example, in the following OCSP configuration, the mode is set to `must`. This means that staples will be fetched only for certificates that have the Must-Staple flag enabled as well, but in case of revocation the server will shutdown rather than run with a revoked staple.

In this configuration, the `url` will also override the OCSP responder URL that may have been configured in the certificate.

```
ocsp {
  mode: must
  url: "http://ocsp.example.net"
}
```

If staples are always required, regardless of the configuration of the certificate, you can enforce the behavior as follows:

```
ocsp {
  mode: always
  url: "http://ocsp.example.net"
}
```

Caching of Staples

When a `store_dir` is configured in the NATS Server, the directory will be used to cache staples on disk to allow the server to resume in case of restarts without having to make another request to the OCSP responder if the staple is still valid.

```
ocsp: true
```

```
store_dir: "/path/to/store/dir"
```

```
tls {
```

```
    cert_file: "configs/certs/ocsp/server-status-request-url.pem"
```

```
    key_file: "configs/certs/ocsp/server-status-request-url-key.pem"
```

```
    ca_file: "configs/certs/ocsp/ca-cert.pem"
```

```
    timeout: 5
```

```
}
```

If JetStream is enabled, then the same `store_dir` will be reused and disk caching will be automatically enabled.

```
### #1
```

```
□ cocobook-sync ### 2026-10-28 11:14:16 UTC
```

```
□ cocobook-sync ### 2026-10-28 11:14:16 UTC
```