Contents

HTTP and HTTPS

Documented against	**SynchroServer `2.7.9.055`**
Last updated	2026-09-03

> Content unchanged since 2.7.8.051 — the 2.7.9 security work (through 2.7.9.055) did not alter TLS setup, listener ports or the HTTP-to-HTTPS redirect. Renamed only to keep the documentation set on one version.

By default, SynchroServer listens for HTTP requests on port **8080** (`HPORT` in `conf/server.ini`). Both the REST API (`/api/v1/`) and the web interfaces are served over this port.

SynchroServer can also serve **HTTPS natively**. HTTPS is **optional** and **off by default**.

Enabling HTTPS

1. Obtain a certificate and private key in **PEM** format. Either a certificate signed by a public CA (e.g. Let's Encrypt) or a self-signed certificate is supported. The private key must be in **PKCS8** format — that is, the file should begin with `-----BEGIN PRIVATE KEY-----` or `-----BEGIN ENCRYPTED PRIVATE KEY-----`.

   To convert an OpenSSL-style PKCS1 key (`BEGIN RSA PRIVATE KEY`) to PKCS8:

   ```
   openssl pkcs8 -topk8 -nocrypt -in key.pem -out key-pkcs8.pem
   ```

   Place the files anywhere readable by the `synchro` user — by convention under `conf/`:

   ```
   conf/cert.pem
   conf/key.pem
   ```

2. Edit `conf/server-local.ini` and set:

```
UseHTTPS=true
HSPORT=8443
CertPath=/home/synchro/SynchroServer/conf/cert.pem
KeyPath=/home/synchro/SynchroServer/conf/key.pem
```

3. **If the private key is encrypted**, provide the passphrase via one of the following. SynchroServer checks them in this order:

   (a) A `conf/server-secret.ini` file

   ```
   KeyPassword=your-passphrase
   ```

   Set permissions so only `synchro` can read it:

   ```
   chmod 600 conf/server-secret.ini
   ```

   `server-secret.ini` is preserved across upgrades and is never overwritten by `install.sh`.

   (b) The `SYNCHRO_KEY_PASSWORD` environment variable, e.g. in the systemd unit or startup script:

   ```
   SYNCHRO_KEY_PASSWORD=your-passphrase
   ```

   If both are set, `server-secret.ini` wins. If the key is not encrypted, neither is required.

4. Restart SynchroServer. The HTTPS listener becomes available at:

   ```
   https://<host>:8443/
   https://<host>:8443/api/v1/
   https://<host>:8443/SynchroUI/
   ```

Redirecting HTTP to HTTPS

To force HTTPS, set in `server-local.ini`:

```
RedirectHttpToHttps=true
```

Plain HTTP requests on `HPORT` (8080) are then answered with a `301 Moved Permanently` pointing at `HSPORT` (8443). If you do not want a plain HTTP listener at all, firewall off the HTTP port at the OS level — SynchroServer always opens the HTTP port (it is required for the redirect).

Renewing certificates

Replace the files at `CertPath / KeyPath` and restart SynchroServer to pick up the new certificate. There is no need to edit `server.ini`.

Troubleshooting

- **`UseHTTPS=true requires CertPath and KeyPath`** — both paths must be set in `server.ini` (or `server-local.ini`).
- **`Key at ... is PKCS1`** — convert to PKCS8 with the `openssl pkcs8` command shown above.
- **`Encrypted key ... requires a passphrase`** — provide the passphrase via `server-secret.ini` or the `SYNCHRO_KEY_PASSWORD` environment variable.
- **Self-signed certificates** trigger browser warnings; for an internal deployment, install the CA cert on client machines or use a public CA.