

TLS and SSL Configuration

Configure the FrameworkX runtime HTTP server to serve HTTPS traffic using a PFX file or a Windows certificate store thumbprint.

Reference Installation TLS and SSL Configuration



New in 10.1.5. HTTPS is a supported baseline for cloud and SaaS deployment. The runtime auto-upgrades port 80 to 443 when certificate entries are present.

Location under review. Final placement pending the next doc pass.

The 10.1.5 runtime loads its HTTPS configuration from the service JSON file next to each runtime executable. Set the certificate path or thumbprint there, then restart the service.

The same configuration format applies to every runtime HTTP server: TStartup, TWebServices, TSecureGateway, and RuntimeMCPHttp.

[Configuration File](#)
[Certificate Properties](#)
[Example Configurations](#)
[Encrypting the Certificate Password](#)
[Verification](#)

Configuration File

Each runtime service reads its certificate configuration from a JSON file named after the process, located in the MachineSettings folder. When no file exists in MachineSettings, the runtime falls back to the assembly folder.

Service	Config File
TStartup	TStartup.json
TWebServices	TWebServices.json
TSecureGateway	TSecureGateway.json
RuntimeMCPHttp	RuntimeMCPHttp.json

Certificate Properties

Set the properties below under appSettings.trPCServer. Two input modes are supported: a PFX file path plus password, or a thumbprint pointing at the Windows LocalMachine\My store.

Property	Description	Example
CertFileName	Full path to a PFX file.	C:\Certs\plant1.pfx
CertPass	PFX password. Wrap the value in # characters to use the built-in encrypted form.	#0XF3A1B...#
CertHash	Thumbprint of a certificate installed in the LocalMachine\My store. Use when you prefer the Windows certificate store over a file path.	F1A20B9C3D4E5F6A7B8C9D0E1F2A3B4C5D6E7F8A

Per-Port Variants

Append _<port> to any property name to scope it to a specific listener port. A per-port value wins over the bare property on the matching listener. Use per-port entries when a single service hosts multiple listeners.

Example Key	Effect
CertFileName_443	PFX used by the listener on port 443.
CertPass_443	Password for the port 443 PFX.
CertHash_8443	Store thumbprint for the listener on port 8443.

Automatic Port 80 to 443 Upgrade

When the configured port is 80 and the file contains CertFileName_443 or CertHash_443, the runtime switches the listener to 443 and enables TLS automatically. This avoids a dedicated HTTPS config entry when the only listener is the web-facing port.

Example Configurations

PFX File

```
{
  "appSettings": {
    "portNumber": 443,
    "tRPCServer": {
      "CertFileName": "C:\\\\Certs\\plant1.pfx",
      "CertPass": "#0XF3A1B...#"
    }
  }
}
```

Windows Certificate Store

```
{
  "appSettings": {
    "portNumber": 443,
    "tRPCServer": {
      "CertHash": "F1A20B9C3D4E5F6A7B8C9D0E1F2A3B4C5D6E7F8A"
    }
  }
}
```

Port 80 Auto-Upgrade

```
{
  "appSettings": {
    "portNumber": 80,
    "tRPCServer": {
      "CertFileName_443": "C:\\\\Certs\\plant1.pfx",
      "CertPass_443": "#0XF3A1B...#"
    }
  }
}
```

The runtime starts on port 443 instead of 80.

Encrypting the Certificate Password

The runtime accepts a plain password inside `CertPass`. For deployments where the password goes into source control or configuration management, use the built-in encrypted form:

1. In Designer, open the runtime service settings dialog.
2. Paste the plain password into the **CertPass** field.
3. Click **Encrypt**. Designer rewrites the value wrapped in # characters.
4. Copy the wrapped value into the service JSON file.

The runtime detects the `#. . . #` wrapping and decrypts the value at startup.

Verification

1. Restart the runtime service after saving the JSON file.

2. In the runtime trace log, look for the line `Started listen port: <port> :: SSL: True`. Any other value indicates the certificate failed to load.
3. Open `https://<host>:<port>/health` in a browser. A valid TLS handshake plus a JSON health body confirms the certificate is active.

Common Errors

Log Line	Cause	Fix
Invalid certificate file configuration	The PFX path is wrong or the password is incorrect.	Verify <code>CertFileName</code> and <code>CertPass</code> . Re-export the PFX if needed.
HTTPS handshake fails with no common cipher.	Client and server TLS protocol versions do not overlap.	Confirm the OS supports TLS 1.2 or later. Windows Server 2012 R2 requires the SChannel update.
Browser warns about an untrusted certificate.	The PFX is self-signed or the issuing CA is not installed on the client.	Install the CA chain on the client, or issue a certificate from a trusted public CA.

In this section...