On this page

Post-Installation Configuration

After installion, you can make adjustments to the configuration of the DAI server to prepare it for use within your organization.

Add Settings for Self-Signed SSL Certificates

If you've completed an advanced installation and used your own Certificate Authority to sign an SSL certificate, then you must update your configuration after installation.

1. Stop the **Digital Automation Intelligence Service** through the Windows Services manager.
2. Go to `C:\ProgramData\Eggplant\Digital Automation Intelligence\config.yml` and open the `.yml` file in a text editing tool.
3. Add the following entries and save your file:

   config.yml

   ```
   NODE_EXTRA_CA_CERTS: <path to the root Certificate Authority certificate>
   REQUESTS_CA_BUNDLE: <path to the root Certificate Authority certificate>
   ```

4. Restart the **Digital Automation Intelligence** Windows service.

Change the Eggplant DAI Port on Windows

Although Eggplant DAI assigns port 8000 by default during installation, you can specify a different port later:

1. Stop the **Digital Automation Intelligence Service** through the Windows Services manager.
2. Repeat an advanced installation and in steps 3 or 4, depending on your configuration, enter a new port value.
3. When the installation is complete, restart the **Digital Automation Intelligence** Windows service.

Update the Nginx Configuration to Enable TLS 1.2 and 1.3

To protect your DAI server using TLS versions 1.2 or 1.3, update your nginx configuration after installation:

1. Stop the **Digital Automation Intelligence Service** through the Windows Services manager.
2. Open `C:\Program Files\Digital Automation Intelligence\python\tools\Lib\site-packages\eggplant\win_dai_service\resources\nginx.conf.jinja2` in a text editing tool.
3. Find the line: `listen {{SERVER_PORT}} default ssl`
4. On the next line, add a new entry: `ssl_protocols TLSv1.2 TLSv1.3;`. For example:

   ```
   listen {{SERVER_PORT}} default ssl;
   ssl_protocols          TLSv1.2 TLSv1.3;
   ```

5. Save your file and restart the **Digital Automation Intelligence** Windows service.

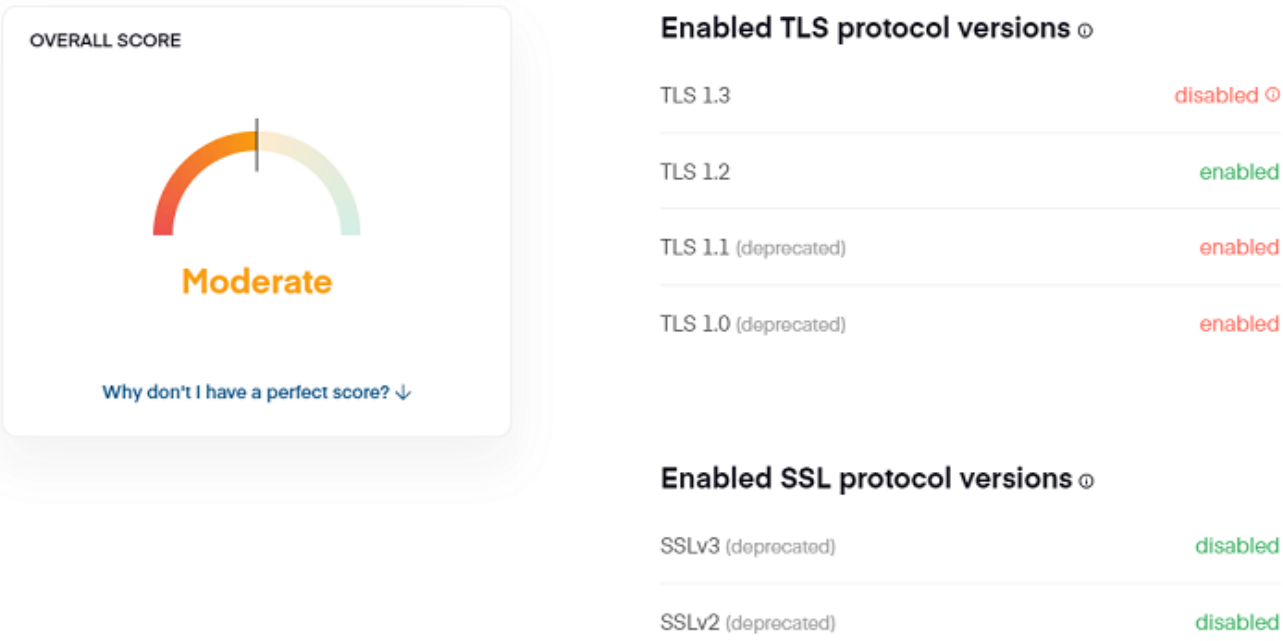
To check that your configuration is correct, use a TLS Checker. For example:

- **Before**

  With default protocols enabled:

https://ec2-54-154-198-175.eu-west-1.compute.amazonaws.com:8000

Copy test URL | Another test →



- **After**

  With only TLS versions 1.2 and 1.3 enabled: