Installing the up.time Controller

Proceed to the appropriate section depending on your Monitoring Station platform:

Installing on Windows

On Windows, the up.time Controller is installed using a graphical installer that guides you through the steps of the installation process.

1. Double-click the executable installer:
   `up.time-controller-installer-<version>.exe`
2. Accept or modify the default install location for the Controller files (`C:\Program Files\uptime software\uptime\controller`), then click **Next**.
3. Accept or modify the default up.time **Controller Port**, then click **Next**.
   This is the port through which the up.time Controller actively listens for API calls. This port number is written to the `<installDirectory>\etc\jetty-ssl.xml` file.
4. Provide keystore configuration details so that the install process can generate the issuer for the Controller's self-signed certificate, and password for the key pair's private key.
5. Click **Next**.
6. Select the database platform that contains your up.time DataStore, then provide the following connection information:
   - **Hostname**
     The name of the system on which the database is running.
   - **Port**
     The port through which the database is listening.
   - **Database Name**
     The name of the database. In typical up.time installations, the database name is `uptime`.
   - **Username**
     The name of the up.time database user, which in a typical installation, is `uptime`.
   - **Password**
     The password for the up.time database user.
7. Click **Next** to accept these database changes, then **Next** to begin the installation process.
8. When the up.time Controller is installed, click **Next**.
9. Optionally **Generate an automatic installation script**, then click **Done**.

Installing on Linux

For information on using the API on Linux Monitoring Stations, contact uptime software Customer Support for more information.

Post-Installation Tasks

These post-installation tasks are highly recommended for all up.time Controller installations.

- If you plan on integrating up.time API examples or other API functions into the up.time web interface, do the following to help prevent several common browser-related warnings when navigating secure and non-secure pages within the same web page:
  1. Enable SSL for the up.time web interface, using the instructions found in Implementing SSL for the Web Interface.
  2. Purchase a valid SSL certificate for the up.time web interface.
- To integrate up.time API examples, you must also enable `lib_curl` on the up.time Monitoring Station:
  1. Stop the `up.time Web Server` service.
  2. Open `<uptimeDirectory>/apache/conf/php.ini` for editing.
  3. Find and remove the semicolon (`;`) from the following line:
     `;extension=php_curl.dll`
  4. Start the `up.time Web Server` service.
- If you are using a Windows Monitoring Station, and intend on using `php_curl` or any of the API examples, you must update the `php_curl.dll` file on your Monitoring Station:
  1. Download the following file to your Monitoring Station: php_curl.dll(credit)
  2. Stop the `up.time Web Server` service.
  3. Replace the existing `<uptimeDirectory>\apache\php\ext\php_curl.dll` file with your downloaded copy.
  4. Start the `up.time Web Server` service.
- Purchase a valid SSL certificate for the up.time Controller. The Controller installs an unsigned and unverified certificate as part of its installation process. For installations in a production environment, a valid key should be purchased and installed on the controller.
- For ease of use, we recommend configuring a simple proxy from the up.time web interface to your controller API location. This will simplify many API programming tasks and help ensure the Controller remains secure. To complete this configuration follow these steps:
  1. On the Monitoring Station, open `<uptimeDirectory>\apache\conf\httpd.conf` for editing.
  2. Find the following section:

```
# proxy settings
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_http_module modules/mod_proxy_http.so
ProxyRequests Off

<Proxy *>
  Order deny,allow
  Allow from all
</Proxy>
ProxyPass /uptime http://HOSTNAME:9996/uptime retry=0
ProxyPassReverse /uptime http://HOSTNAME:9996/uptime
```

3. If you have already enabled SSL on the up.time Web Server, find the following line:

   ```
   ProxyRequests Off
   ```

   Above it, add the add the following line:

   ```
   SSLProxyEngine on
   ```

4. Find the following:

   ```
   ProxyPassReverse /uptime http://HOSTNAME:9996/uptime
   ```

   Below it, add the following, replacing `HOSTNAME:9997` with the hostname and port where your up.time Controller is listening:

   ```
   ProxyPass /api https://HOSTNAME:9997/api retry=0
   ProxyPassReverse /api https://HOSTNAME:9997/api
   ```

5. The section in `httpd.conf` should now look similar to the following:

   ```
   # proxy settings
   LoadModule proxy_module modules/mod_proxy.so
   LoadModule proxy_http_module modules/mod_proxy_http.so
   SSLProxyEngine on

   ProxyRequests Off
   <Proxy *>
     Order deny,allow
     Allow from all
   </Proxy>
   ProxyPass /uptime http://<uptimeMonitoringStation>:9996/uptime retry=0
   ProxyPassReverse /uptime http://<uptimeMonitoringStation>:9996/uptime
   ProxyPass /api https://<uptimeController>:9997/api retry=0
   ProxyPassReverse /api https://<uptimeController>:9997/api
   ```

6. Restart the `up.time Web Server` service to apply these changes.
7. Verify you have correctly configured the proxy by browsing to `https://<uptimeMonitoringStation>/api`. The behavior should be identical to browsing to the up.time Controller at `https://<uptimeController>/api`.