Installing the Monitoring Station

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

Installing on Windows

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

1. Ensure you are logged in to the Monitoring Station system as the local administrator.
   up.time may not function properly if the Monitoring Station is installed when you are logged in as a domain or non-local administrator.
2. Double-click the executable installer:
   `up.time-<version#>-windows.exe`
3. On the introduction screen, click **Next**.
4. On the **License Agreement** screen, carefully read all of the up.time end-user license agreement, then click the **accept** check box, and click **Next**.
5. Accept or modify the default install location for the Monitoring Station files (`C:\Program Files\uptime software\uptime`), then click **Next**.
   This is the location of the core up.time components (i.e., the Data Collector and Web server), as well as the Controller; the DataStore location is set in the next step.
6. Accept or modify the default install location for the DataStore (`C:\Program Files\uptime software\uptime\datastore`), then click **Next**.
   Because the DataStore can grow very large (in excess of 100 GB), you can install the DataStore on another file system if you are monitoring a large number of systems and retaining data for extended periods.
7. On the **Configuration Options** page, in the **Web Server Settings** section, optionally configure the up.time Web server:
   - **Web Server Name**
     The hostname of the system through which users will access the Web server's user interface. This name is written to the `<installDirectory>\apache\conf\httpd.conf` file, which contains configuration information for the Web server used by up.time.
   - **Web Server Port**
     The port through which the Web server for the Monitoring Station will listen for requests. The port number is written to the `httpd.conf` file.
8. Configure the up.time **Controller Settings**:
   - **Controller Port**
     This is the port through which the up.time Controller actively listens for API calls. This port number is written to the `<installDirectory>\controller\etc\jetty-ssl.xml` file.
   - **SSL Distinguished Name**
   - **SSL Passphrase**
     Provide keystore information so that the install process can generate the issuer for the Controller's self-signed certificate. This information includes a distinguished name and passphrase. By default, the distinguished name is the Controller hostname, which is a mandatory attribute; make this as complete as needed (e.g., `CN=hostname,O=Organization,OU=ITServices,ST=California,C=US`). The passphrase must be at least six characters long.
9. In the DataStore Settings section, optionally configure the Database Port through which the DataStore will listen for requests.
   The port number is written to the `uptime.conf` file
10. Select the Start menu location and user access option, then click **Next**.
11. Click **Next** to begin the installation.
    The installation process will take several minutes.
12. When the software is installed, click **Finish**.
    The following occurs:
    - the Web server and DataStore services are started
    - the DataStore is populated with default data
    - the Data Collector is started
    - the Controller service is left in a stopped state
    - the Monitoring Station user interface is launched in your default browser
13. Proceed to the Post-Installation Tasks section.

Installing on Linux

On Linux, the up.time Monitoring Station installer is a console application.

1. Ensure you have logged in to the Monitoring Station system as `root`.
2. Type the following command:
   `sh up.time-<version>-linux.bin`
   It can take up to several minutes for the components of the installer to be extracted from the `.bin` file.
3. On the `Introduction` page, press **Enter** to continue.
4. On the `License Agreement` page, carefully read all of the up.time end-user license agreement. Press **Enter** to scroll through the agreement.
5. At the `DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT? (Y/N)` prompt, type **y** and press **Enter**.
6. `Choose Install Folder`: Accept the default install directory for the Monitoring Station files (`/usr/local/uptime`) or enter a new, absolute path, then press **Enter**.
   This is the location of the core up.time components (i.e., the Data Collector and Web server), as well as the Controller; the DataStore location is set in the next step.

> The `uptime` user account must be able to access the specified directory.

7. `Choose DataStore Path`: Accept the default install directory for the DataStore (`/usr/local/uptime/datastore`) or enter a new, absolute path, then press **Enter**.
   Because the DataStore can grow very large (in excess of 100 GB), you can install the DataStore on another file system if you are monitoring a large number of systems and retaining data for extended periods.
8. `DataStore Port`: Accept the default DataStore port (`3308`) or enter a new one, the press **Enter**.
   This is the port through which the DataStore will listen for requests. The port number is written to the uptime.conf file.
9. `Web Server Name`: Accept the default hostname for up.time's Web server component or enter a new one, then press **Enter**.
   This is the name of the system through which users will access the up.time Web interface. This name is written to the `<installDirectory>/apache/conf/httpd.conf` file, which contains configuration information for the Web server used by up.time.
10. `Web Server Port`: Accept the default Web server port (`9999`) or enter a new one, then press **Enter**.
    This is the port through which the Web server will listen for requests. The port number is written to the `httpd.conf` file.
11. `Uptime Controller Port`: Accept the default up.time Controller port (`9997`) or enter a new one, then press **Enter**.
    This is the port through which the up.time Controller listens for API calls. The port number is written to the `<installDirectory>/controller/etc/jetty-ssl.xml` file.
12. `Keystore Configuration`: Provide keystore information so that the install process can generate the issuer for the Controller's self-signed certificate.
    a. `Distinguished Name`: Accept the default distinguished name (the hostname of the installation system) or enter a new one, then press **Enter**.
       Only the common name (`CN`) attribute is required, but you can make the name as complete as needed (e.g., `CN=hostname, O=Organization, OU=ITServices, ST=California, C=US`).
    b. `Keystore Password`: Enter and confirm a password.
       This password must be at least 6 characters long.
13. `Pre-Installation Summary`: Review the configured options, then press **Enter**.
    The installation process will take several minutes.
14. When the installation is complete, press **Enter**.
    The following occurs:
    - the Web server and DataStore are started
    - the DataStore is populated with default data
    - the Data Collector is started
    - the Controller service is left in a stopped state
15. Press **Enter** again to exit the installer.
16. Proceed to the Post-Installation Tasks section.

Installing on a VMware vCenter Server

On VMware vSphere, the up.time vApp is installed on a VMware vCenter Server as an OVF template.

Deploy the up.time OVF Template

1. Download the latest up.time Virtual Appliance from the uptime software website: http://www.uptimesoftware.com/download-vmapp.php.
   The archive consists of the up.time OVF template and the virtual disk image.
2. Unzip the contents of the archive onto a file system that is accessible by the vSphere Client.
3. In the vSphere Client, select **File > Deploy OVF** Template to initiate the **Deploy OVF Template** wizard.
4. Specify the location of `up.time.ovf`.
5. Review the up.time OVF template details, and the end-user license agreement.
6. Optionally edit the name of the up.time virtual appliance, and its location in the VMware vCenter inventory hierarchy.
7. Specify where the up.time OVF template is to be deployed, whether it's a host, host within a cluster, or a resource pool.
8. Select a datastore used by the destination cluster or host where the up.time virtual appliance and virtual disk file will be stored.
9. Select the disk format for the virtual disk file:
   - thin provisioned format, where storage is allocated on demand (3.3 GB required)
   - thick provisioned format, where all required storage is allocated up front (10 GB required)
10. Map the up.time virtual appliance network with an inventory network by selecting one from the **Destination Networks** column.
11. Optionally configure the network settings for the up.time virtual appliance.
12. Review your settings and click **Finish** to begin importing the virtual appliance into your VMware vCenter inventory.
    The vSphere Client will update you on the template deployment progress, as the up.time VM is created, and its virtual disk is deployed.

Configure up.time Virtual Appliance

1. **Power On** the up.time VM.
2. After the up.time appliance has started (this could take a few minutes), click the **Console** tab.
3. Set the correct timezone.

> Even if you are using up.time for evaluation purposes, it is important that you set the timezone to ensure it integrates correctly with other parts of your infrastructure.

4. Note the Monitoring Station IP address, then proceed to the Post-Installation Tasks section.

Post-Installation Tasks

After installing the up.time Monitoring Station, you will need to do the following:

- set up the administrator account and SMTP server when you first log in
- install the license for up.time
- add systems
- add users

Set Up the Administrator Account and SMTP Server

Once the Monitoring Station has been installed, connect to it using the hostname and port defined during the installation process: `http://<hostname>:<port>`

The first user to log into up.time should be the system administrator. The administrator account has the default user name `admin`, and at first login, you will have to set the password and email address for this administrator account. To set up the administrator account, do the following:

1. Access the Monitoring Station in a supported Web browser:
   `http://<hostname>:<port>`
   Where `<hostname>` is the name or IP address of the system that is running the up.time Monitoring Station. For example:
   http://localhost:9999
2. At the up.time login screen, enter the password for the administrator in the **Password** field.
3. Re-enter the password in the **Confirm Password** field.
4. Enter an appropriate address in the **Administrator's Email** field.
5. Enter your SMTP hostname in the **SMTP Server** field.
   up.time needs this information configured immediately in order to send alerts. You can modify this information after installation (see SMTP Server for more information).
6. Click the **Login** button.
   You have set up up.time's main administrator account.

Install a License to Use up.time

See License Information for more information.

Add Systems

The fastest way to begin monitoring your infrastructure is to use Auto Discovery to efficiently assemble a monitored inventory.

Afterward, you can fine-tune your monitored inventory. See Managing Your Infrastructure for more information.

Add Users

You will need to create user roles (e.g., for administration, alert investigation, and report access) and assign individual users or user groups to them. See User Management for more information.

Secure the up.time Virtual Appliance

If you have installed up.time as a VMware virtual appliance, the default user ID and password used to access the virtual OS is `root` and `uptime`, respectively. This level of access is required for system-level up.time tasks such as custom scripting, debugging, and working with the database. For security purposes, it is strongly recommended that you change the default root-level password provided for the up.time virtual appliance OS.

Secure the up.time Controller

If you are planning to use the up.time Controller, there are further steps to consider. See Controller Security for more information.