

# SensorView Installation Best Practices

This guide provides instructional information to ensure SensorView is configured in a secure manner.

## Install Location

SensorView can be installed to any location on the host, excluding a NAS (Network Addressable Storage) device.

## Configuring HTTPS

### Installing a SSL certificate

During installation there will be a prompt to select a pre-existing website to install SensorView. SensorView will inherit the security configuration associated with this website, (i.e., if the web site is configured to support HTTPS then SensorView will support HTTPS).

The recommended setting for SensorView is to be installed on a website utilizing HTTPS to secure login credentials. For instructions on configuring a website to use HTTPS refer [here](#) [1].

### Forward HTTP requests to HTTPS

If the configured website supports both HTTP and HTTPS connections it is recommended to configure SensorView to forward all HTTP connections to HTTPS. In order to achieve this, the following modification must be made. Please create a back-up of the configuration file before modifying the configuration file.

1. Open C:\Program Files\SensorSwitch\SensorView\App\Active\WebUI\web.config in any text editor (i.e., Notepad, Word, etc.).  
*Note: The location of the "SensorSwitch" folder may vary based on customization of the installation directory.*

2. Locate and edit the following line:

```
<forms requireSSL="false" loginUrl="Login.aspx" timeout="30" protection="All" slidingExpiration="true" cookieless="UseCookies"/>
```

#### Change false to true:

```
<forms requireSSL="true" loginUrl="Login.aspx" timeout="30" protection="All" slidingExpiration="true" cookieless="UseCookies"/>
```

3. Save the file, refresh (or reopen) the SensorView web application.

**Warning:** Modifying SensorView's configuration file improperly can cause serious problems which may require SensorView to be re-installed. It is recommended a backup of the configuration file is created prior to modifying it.

## Network Configuration

nLight utilizes AES-128 encryption to secure communication and SensorView. The default passkey is *sensorswitch1234*. After installation we recommend changing the default passkey; refer [here](#) [2] for tips on selecting a strong passkey.

### Changing the Gateway Password passkey:

1. Open SensorView and log in as an administrative user
2. Navigate to *Admin*
3. Navigate to *Setup->Gateway Password*
4. Change the passkey, select *Save*
5. Update passkey on each nGWY device

- nGWY1 devices are already communicating with SensorView and the passkey will automatically be updated
- nGWY2 devices need to be updated directly from the nGWY2 GFX via the instructions below:
  1. Locate the nGWY2 GFX touch screen unit
  2. Select the padlock keep on the top left corner of the screen, and enter pin code 1234 and select enter (ent)
  3. Select *Gateway Setup->Set Network Password*
  4. Enter the same password that was previously entered into SensorView

## User Account Management

SensorView ships with a default administrator account and password complexity requirements. After installing SensorView it is recommended to change the password for additional security.

Changing the administrator (default) password:

1. Log into SensorView as the administrator (default is administrator/admin)
2. Select the *Users* tab at the top right of the screen
3. In the drop down, check that *administrator* is the current user being modified, if not select it
4. Input the new password and select *Save*

## Password complexity

The password complexity requirements can be modified. Detailed below are the instructions.

1. Open *C:\Program Files\SensorSwitch\SensorView\App\Active\WebUI\web.config* in any text editor. Note: The location of the "SensorSwitch" folder may vary based on customization of the installation directory.
2. Edit the following lines to specify password length and number of symbols per password
  - `<add key="MinPasswordLength" value="Insert minimum length here">`
  - `<add key="MinNonAlphaCharacters" value="Insert number of symbols here">`

**Warning:** Modifying SensorView's configuration file improperly can cause serious problems which may require SensorView to be re-installed. It is recommended a backup of the configuration file is created prior to modifying it.

## Application updates

- Best practice is to keep SensorView up to date with the most recent version provided by Acuity Controls. Notifications about new application updates are available within SensorView on the *Overview->Available Updates* section.
- If an outbound network filter is being used it is recommended to whitelist *nlight.sensorswitch.com* in order for new application updates to be retrieved.

## References

[1] <https://support.microsoft.com/kb/324069?wa=wsignin1.0>

[2] <http://windows.microsoft.com/en-us/windows-vista/tips-for-creating-a-strong-password>