Local Licensing Server

The Local Licensing Server User Guide

TME18866-001

Last updated: April 2023

Schneider Electric

Table of Contents

Getting Started

The Schneider Electric Local Licensing Server (LLS) allows you to activate and manage licenses for PowerChute Network Shutdown v5.0 and above. This document details how to install the Local Licensing Server to be used for these products.

For more license information on PowerChute, see the PowerChute Licensing FAQ on the APC website.

Download the Local Licensing Server

1. Visit Knowledge Base article FAQ000256668 and download the required LLS files.
2. View the checksum of the server zip file by running the following command in a command prompt: `<certUtil -hashfile <File-Name.zip> SHA256>`
3. Compare this checksum against the one provided in the “sha256sums” file. The two checksums should match, if they don’t, re-download the files and try again.
4. Unzip the contents.
5. Copy the server folder to a local directory on the machine you intend to install it on.

Prerequisites

You must have Java installed on your PC and Java must be found on the path. The JAVA_HOME environment variable must also be set to the Java installation directory.

Windows

Installing the LLS

To install the Local Licensing Server on Windows, follow the steps below:

1. Install Java 11 and set JAVA_HOME and Java Path variables. It is recommended you download the latest LTS version of Java 11.
2. Navigate to the server folder with command prompt running as administrator.
3. Run `<install.bat>` from this command prompt.

```
C:\Users\user\server>install.bat
Installing service FNLS-SCHNEIDR
Service FNLS-SCHNEIDR successfully started

Enter your new admin password for LLS
Your password must meet the following condtions:
1 At least 8 characters (with a maximum of 64 characters)
2 At least one digit
3 At least one upper-case character
4 At least one special character examples:, ^ * $ - + ? _ & = ! % { } / # @
5 No whitespace
Password:
```

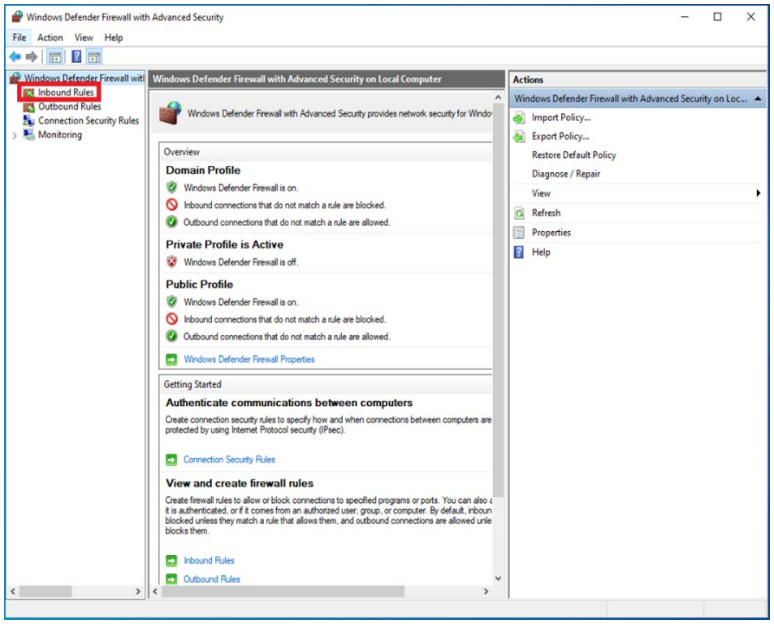
4. Enter and confirm your administrator password for the LLS. This password must meet the following requirements:
    - At least 8 characters (maximum of 64 characters)
    - At least one digit
    - At least one upper-case character
    - At least one special character (for example, ^ * $ - + ? _ & = ! % { } / # @)
    - No whitespace

5. A successful installation will look like this:

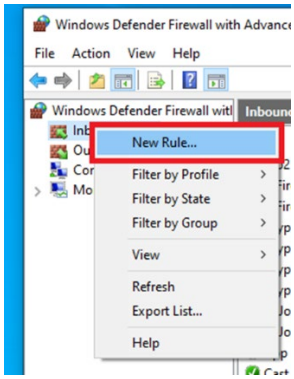
```
C:\Users\user\server>install.bat
Installing service FNLS-SCHNEIDR
Service FNLS-SCHNEIDR successfully started

Enter your new admin password for LLS
Your password must meet the following condtions:
1 At least 8 characters (with a maximum of 64 characters)
2 At least one digit
3 At least one upper-case character
4 At least one special character examples:, ^ * $ - + ? _ & = ! % { } / # @
5 No whitespace
Password: Passw0rd!
Re-enter Password: Passw0rd!
Waiting for LLS to come online...
Password changed successfully
```

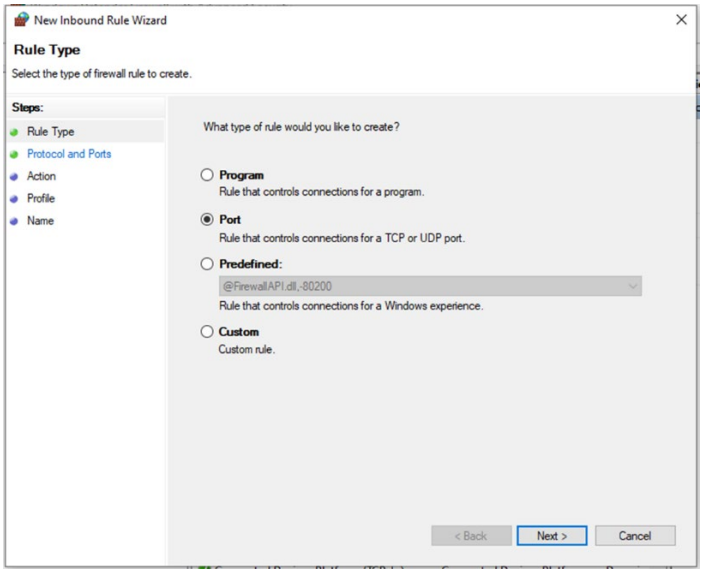
6. You need to create a new inbound rule for port 7070 in “Windows Defender” to allow access to the LLS from outside the device.
   Note: This step is not required if you are running the LLS locally on the same machine as PowerChute Network Shutdown.
    - Open “Windows Defender Firewall with Advanced Security”. Select **Inbound Rules** and right click on it again.



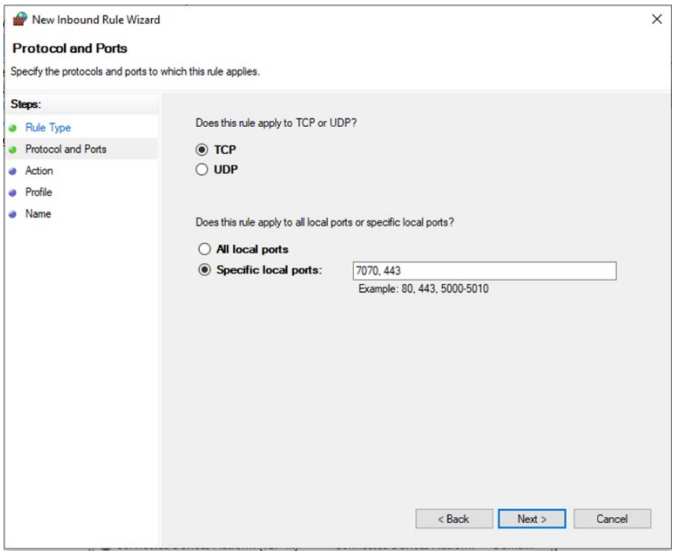
- Select **New Rule**.



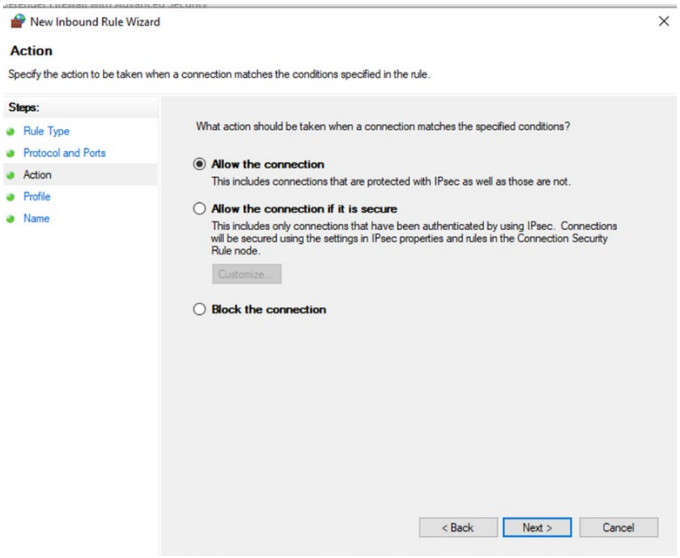
- Select port.



- On the following page, ensure **TCP** is selected and enter the ports you want to open. By default, the LLS uses port 7070 for HTTP and port 443 for HTTPS on Windows.



- Choose to **Allow the Connection** on the “Action page”.



- Proceed through the rest of the wizard.
- On the final page, allocate an identifiable name to the rule. Click **Finish** to open your ports and allow communication to the LLS.

Using HTTPS

Firewall

As with the HTTP implementation you will need to open the HTTPS port in the windows firewall inbound rules. By default, port 443 is used for HTTPS but his can be changed as needed. See Installing the LLS on Windows.

Certificate generation

To use HTTPS for the Local Licensing Server you are required to provide certificates, “openssl” is the tool used to generate certificates.

In this example the host name of the server is going to be “llshostname.com”. This can be changed to suit the hostname of your Local Licensing Server.

1. Create an “lls.ext” file in the folder you’re going to create the certificates in with the following contents:

```
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:FALSE
subjectAltName = @alt_names
[alt_names]
DNS.1 = llshostname.com
```

2. winpty openssl genrsa –aes256 -out lls.key 2048
3. winpty openssl req -key lls.key -new -out lls.csr
4. winpty openssl x509 -signkey lls.key -in lls.csr -req -days 365 -out lls.crt
5. winpty openssl req -x509 -sha256 -days 1825 -newkey rsa:2048 -keyout rootCA.key -out rootCA.crt
6. winpty openssl x509 -req -CA rootCA.crt -CAkey rootCA.key -in lls.csr -out lls.crt -days 365 -CAcreateserial -extfile lls.ext
7. winpty openssl pkcs12 -inkey lls.key -in lls.crt -export -out llscert.pfx
8. copy the llscert.pfx to the LLS server directory

Create the keystore, and adding the LLS-server cert

Use the command below to create the keystore, and add "llscert.pfx" created above to the keystore for the LLS server, You will be asked to provide a keystore password, this will be needed at a later stage: `keytool -v -importkeystore -srckeystore llscert.pfx -srcstoretype PKCS12 -destkeystore servercert.jks -deststoretype JKS`

Adding keystore Path to LLS

1. The “local-configuration.yaml” file is located in the server directory. It is the same file you created in the keystore above. Open the file in an editor.
2. In the “local-configuration.yaml” file, you are required to edit the “https-in” section:
   - Set Enabled to **True**.
   - Set the path to the keystore you created.
   - Add the keystore-password.
3. The “local-configuration.yaml” file should look like this:

```
# HTTPS server mode
https-in:
  # Set to true to enable
  enabled: true
  # HTTPS listening port
  port: 1443
  # Path to keystore
  keystore-path: servercert.jks
  # Keystore password. You can obfuscate this with java -jar flexnetls.jar -password your-password-here
  keystore-password: your-password-here
  # Enable the below line for TLS 1.3
  # tlsCipherSuites: MODERN
```

4. You can now restart the LLS and connect to it over HTTPS.

Note: “servercert.jks” must be present in the same location where the “local-configuration.yaml” file is stored.

Disabling HTTP on LLS

To disable the LLS from using HTTP you must also change the port option at the top of the "local-configuration.yaml" file to 0. This must be uncommented before changing it.

```
# local-configuration.

# HTTP listening port. Default is 7070. You can bind to an interface with this syntax: '[127.0.0.1].7070'.
port: 0

```

Adding self-signed certificate to Java CACERTS keystore

When the Local Licensing Server is configured to use HTTPS with a self-signed certificate, you are required to add the certificate to your Java cacerts keystore to interact with the Local Licensing Server. To complete this, follow the steps below:

1. Copy your certificate (rootCA.crt in the example provided) onto the device running the Local Licensing Server.
2. To add the certificate into the Java keystore, run the following command from an administrative command prompt in the same directory as the certificate: `keytool -import -trustcacerts -cacerts -storepass changeit -noprompt -alias LLSCert -file rootCA.crt`
   Note: The default java cacerts keystore password is "changeit" you may need to change this if it has been changed on your system.
3. Add the hostname of the Local Licensing Server to the windows hosts file. See **Adding LLS hostname to the host's file**.
4. Your device can now interact with the Local Licensing Server over HTTPS using the "flexnetlsadmin.sh" scripts provided.

Activating Licenses

When the LLS has an internet connection

The below command can be used to activate licenses on the LLS via command prompt. It should be run from the server folder:

```
flexnetlsadmin.bat -server https://<hostname>:443/api/1.0/instances/~ -authorize admin <admin password> -activate -id <activation ID> -count <quantity>
```

When the LLS does not have an internet connection

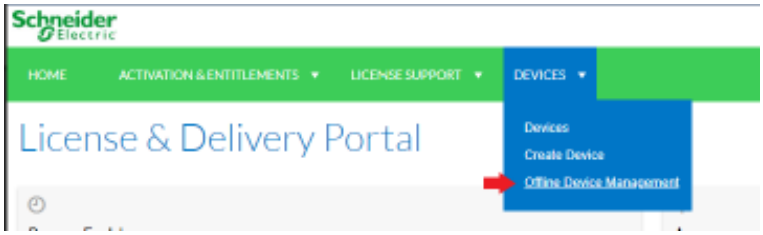
When the LLS is not connected to the internet, you are required to manage the request and response files manually, to move the licenses from the Cloud Licensing Server to the Local Licensing Server.

To generate the request file, follow the command below from the server folder:

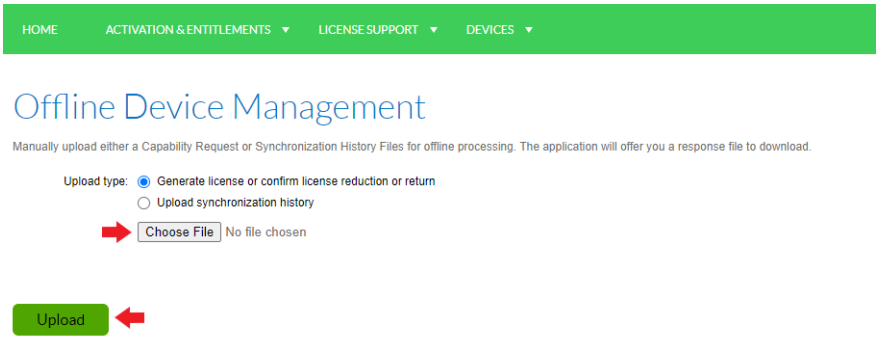
```
flexnetlsadmin.bat -server https://<hostname>:443/api/1.0/instances/~ -authorize admin <admin password> -activate -id <activation Id> -count <quantity> -o request.bin
```

This command will create the request file "request.bin" in the server folder. Copy this file over to a machine that with internet access and open the URL here.

1. Log in with the same activation ID used to generate the request.
2. Navigate to **Devices > Offline Device Management**.

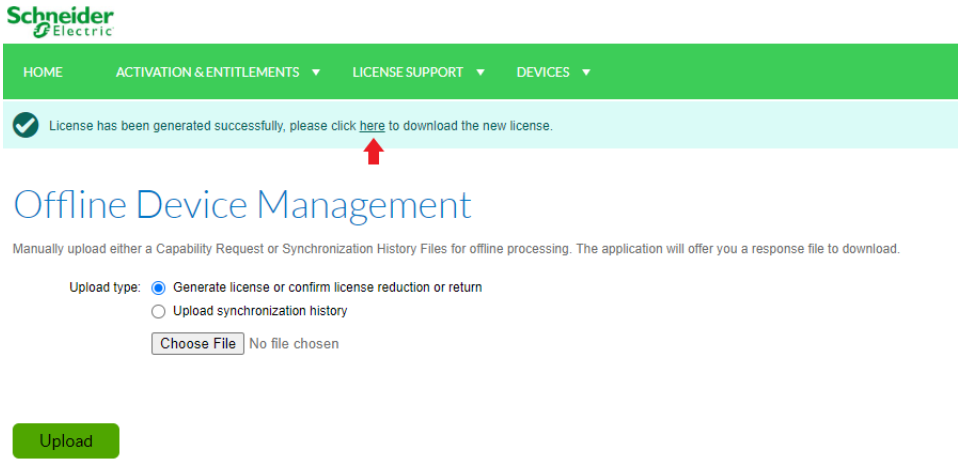


3. You will be directed to the page below. Click **Choose File**.
4. Select the “request.bin” file generated in the previous step and then click on **Upload**. This will upload the request file and generate a response file.



5. When the response has been generated, a dialog will appear at the top of the screen prompting you to download the response file. Click the link to download the file. The file should be named “capabilityResponse.bin”.

Note: This file is only valid for 30 days after generation.



6. Copy the response file onto the device that the LLS is running on and place it in the server folder.
7. Run the following command to process the response file: `<flexnetlsadmin.bat -server https://<hostname>:443/api/1.0/instances/~ -authorize admin <admin password> -activate -load capabilityResponse.bin>`
8. The LLS will then have the active licenses. To validate this, choose to “View active Licenses" in Interacting with the LLS.

Interacting with the LLS

The following commands can be run from the server folder.

Action	Command
Stop the service	`flexnetls.bat -stop`
Start the service	`flexnetls.bat -start`
View active licenses and quantity available	`flexnetlsadmin.bat -server https://<hostname>:443/api/1.0/instances/~ -authorize admin <admin password> -licenses -verbose`
Change admin password	`flexnetlsadmin.bat -server https://<hostname>:443/api/1.0/instances/~ -authorize admin <current admin password> -users -edit admin <new admin password>` **Note:** The default password provided with the LLS is Admin@123, this will be changed to a user defined password during the installation process.

Uninstalling the LLS

You are required to remove any licenses present on the LLS before you begin uninstallation. This can be done by following the same command used to activate licenses onto the LLS, except the quantity used is 0.

`<flexnetlsadmin.bat -server http://localhost:7070/api/1.0/instances/~ -authorize admin <password> -activate -id [Activation ID] -count 0>`

Note: If HTTP has been disabled, use the configured HTTPS port.

Using the provided script

Run `<uninstall.bat>` from the server folder as an administrator to automatically uninstall the LLS.

Manually

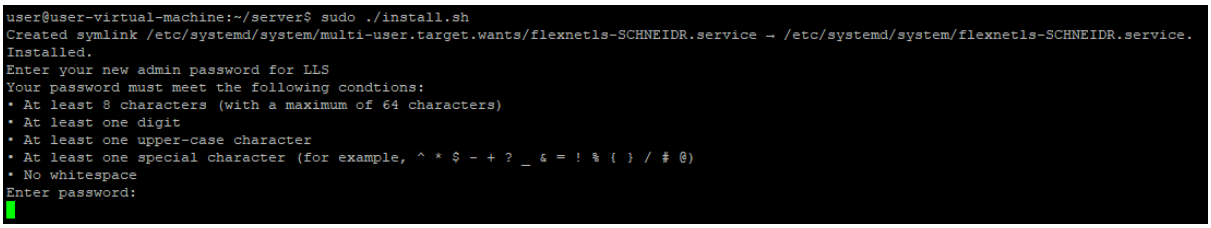
- Run `<flexnetls.bat -stop>` from the server folder as an administrator.
- Run `<flexnetls.bat -uninstall>` to remove the LLS.
- To remove all remaining server files, go to **C:\Windows\ServiceProfiles\NetworkService\ flexnetls** and delete the “SCHNEIDER” folder.
  Note: If C: is not your main drive, change this as appropriate.

Ubuntu

Installing the LLS

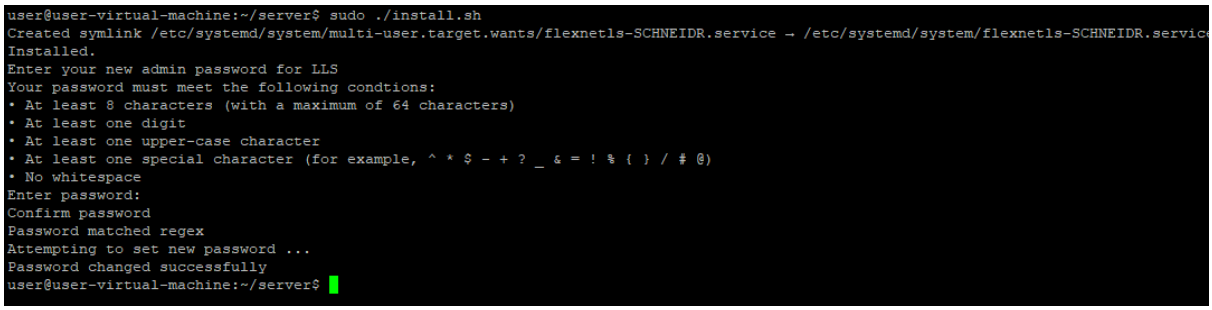
To install the Local Licesning Server on Ubuntu, follow the steps below:

1. Install Java <sudo apt-get install openjdk-11-jre> on Ubuntu. It is recommended that you download the latest LTS version of Java 11.
2. Run <sudo ./install.sh> in a terminal from the server folder.



4. Enter and confirm your administrator password for the LLS. This password must meet the following requirements:
    - At least 8 characters (with a maximum of 64 characters)
    - At least one digit
    - At least one upper-case character
    - At least one special character (for example, ^ * $ - + ? _ & = ! % { } / # @)
    - No whitespace

5. A successful installation will look like this:



Using HTTPS

Certificate Generation

To use HTTPS for the Local Licensing Server you are required to provide certificates, “openssl” is the tool used to generate certificates.

In this example, the name of the host server is “llshostname.com”. This can be changed to suit the hostname of your Local Licensing Server.

1. Create a “lls.ext” file in the folder you’re going to create the certificates in with the following contents:

```
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:FALSE
subjectAltName = @alt_names
[alt_names]
DNS.1 = llshostname.com
```

2. openssl genrsa –aes256 -out lls.key 2048
3. openssl req -key lls.key -new -out lls.csr
4. openssl x509 -signkey lls.key -in lls.csr -req -days 365 -out lls.crt
5. openssl req -x509 -sha256 -days 1825 -newkey rsa:2048 -keyout rootCA.key -out rootCA.crt
6. openssl x509 -req -CA rootCA.crt -CAkey rootCA.key -in lls.csr -out lls.crt -days 365 -CAcreateserial -extfile lls.ext
7. openssl pkcs12 -inkey lls.key -in lls.crt -export -out llscert.pfx
8. copy the llscert.pfx to the LLS server directory

Create the keystore, and adding the LLS-server cert

Use this command to create the keystore and add llscert.pfx created above to the keystore: `keytool -v -importkeystore -srckeystore llscert.pfx -srcstoretype PKCS12 -destkeystore servercert.jks -deststoretype JKS`

Adding keystore Path to LLS

1. The “local-configuration.yaml” file is located at **/opt/flexnetls/SCHNEIDR**
2. In the “local-configuration.yaml” file you need to enable **https-in**.
3. Add the keystore path and keystore-password, it should look like this:

```yaml
# HTTPS server mode
https-in:
  # Set to true to enable
  enabled: true
  # HTTPS listening port
  port: 1443
  # Path to keystore
  keystore-path: servercert.jks
  # Keystore password. You can obfuscate this with java -jar flexnetls.jar -password your-password-here
  keystore-password: your-password-here
  # Enable the below line for TLS 1.3
  # tlsCipherSuites: MODERN
```

4. The Local Licensing Server defaults to 1443 on Ubuntu to avoid issues on Linux with port numbers less than 1024. Any port number above 1024 can be used.
5. You can now restart the LLS and connect to it over HTTPS.
   Note: “servercert.jks” must be present in the same location where the “local-configuration.yaml” file is stored.

Disabling HTTP on LLS

To disable the LLS from using HTTP you must also change the port option at the top of the "local-configuration.yaml" file to 0. This must be uncommented before the change.

```
# local-configuration.

# HTTP listening port. Default is 7070. You can bind to an interface with this syntax: '[127.0.0.1].7070'.
port: 0

```

Adding self-signed certificate to Java CACERTS keystore

When the Local Licensing Server is configured to use HTTPS with a self-signed certificate, you are required to add the certificate to your Java cacerts keystore to interact with the Local Licensing Server. To complete this, follow the steps below:

1. Copy your certificate (rootCA.crt in the example provided) onto the device running the Local Licensing Server.
2. Add the certificate into the Java keystore by running the following command from a terminal in the same directory as the certificate: `<sudo keytool -import -trustcacerts -cacerts -storepass changeit -noprompt -alias LLSCert -file rootCA.crt>`
   Note: The default java cacerts keystore password is "changeit" you may need to change this if it has been changed on your system.
3. Add the hostname of the Local Licensing Server to the windows hosts file. See **Adding LLS hostname to the host's file**.
4. Your device can now interact with the Local Licensing Server over HTTPS using the "flexnetlsadmin.sh" scripts provided.

Activating Licenses

When the LLS has an internet connection

The below command can be used to activate licenses on the LLS via command prompt, it should be run from the server folder:

```
./flexnetlsadmin.sh -server https://<hostname>:1443/api/1.0/instances/~ -authorize admin <admin password> -activate -id <activation ID> -count <quantity>
```

When the LLS does not have an internet connection

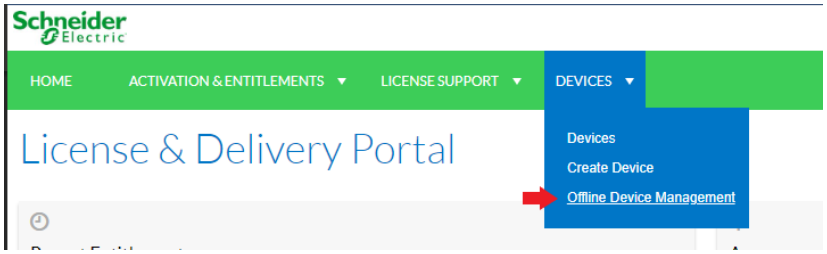
When the LLS is not connected to the internet, you are required to manage the request and response files manually, to move the licenses from the Cloud Licensing Server to the Local Licensing Server.

To generate the request file, execute the following command from the server folder:

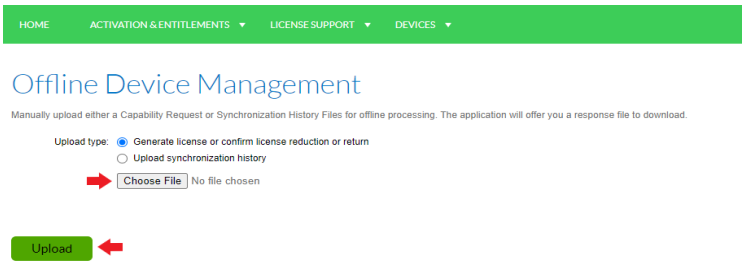
```
.flexnetlsadmin.sh -server https://<hostname>:1443/api/1.0/instances/~ -authorize admin <admin password> -activate -id <activation Id> -count <quantity> -o request.bin
```

This command will create the request file (request.bin) in the server folder. Copy this file over to a machine with internet access and open the URL here.

1. Log in with the same activation ID used to generate the request.
2. Navigate to **Devices > Offline Device Management**.

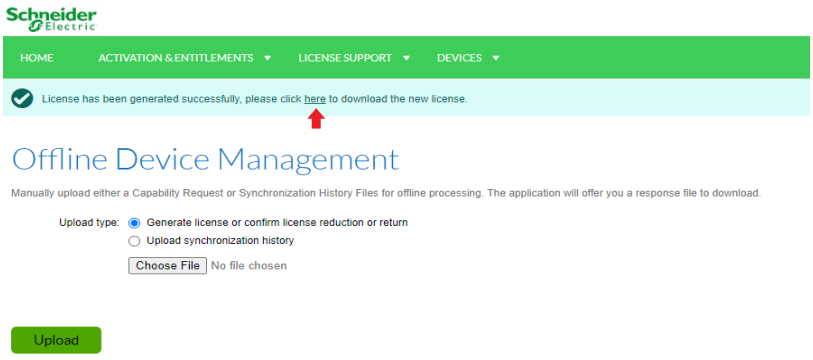


3. You will be directed to the page below. Click **Choose File**.
4. Select the “request.bin” file generated in the previous step and then click on **Upload**. This will upload the request file and generate a response file.



5. When the response has been generated, a dialog will appear at the top of the screen prompting you to download the response file. Click the link to download the file. The file should be named “capabilityResponse.bin”.

Note: This file is only valid for 30 days after generation.



6. Copy the response file onto the device that the LLS is running on and place it in the server folder.
7. Run the following command to process the response file: `./flexnetlsadmin.sh -server https://<hostname>:1443/api/1.0/instances/~ -authorize admin <admin password> -activate -load capabilityResponse.bin`
8. The LLS will then have the active licenses. To validate this, see the command to “View active Licenses” in Interacting with the LLS.

Interacting with the LLS

Action	Command
Stop the service	`sudo systemctl stop flexnetls-SCHNEIDR.service`
Start the service	`sudo systemctl start flexnetls-SCHNEIDR.service`
Review service status	`sudo systemctl status flexnetls-SCHNEIDR.service`
View active licenses and quantity available	`./flexnetlsadmin.sh -server https://<hostname>:1443/api/1.0/instances/ ~-authorize admin <admin password> -licenses -verbose`
Change administrator password	Enter the below command into the server folder: `./flexnetlsadmin.sh -server https://<hostname>:1443/api/1.0/instances/ ~-authorize admin <current admin password> - users -edit admin <new admin password>` **Note:** The default password provided with the LLS is Admin@123, this will be changed to a user defined password during the installation process.

Uninstalling the LLS

You are required to remove any licenses present on the LLS before you begin the uninstallation. This can be done by following the same command used to activate licenses onto the LLS, except the quantity used is 0.

```
./flexnetlsadmin.sh -server https://<hostname>:1443/api/1.0/instances/ ~-authorize admin <current admin password> - users -edit admin <new admin password>
```

Note: If HTTP has been disabled, use the configured HTTPS port.

Using the provided script

Run `<sudo ./uninstall.sh>` from the server folder as an administrator to automatically uninstall the LLS.

Manually

Run the following commands in this order:

`sudo systemctl stop flexnetls-SCHNEIDR.service`	To shutdown the service.
`sudo systemctl disable flexnetls-SCHNEIDR.service`	To disable the service from starting on system reboot.
`sudo rm /etc/systemd/system/flexnetls-SCHNEIDR.service`	
`sudo rm -r /etc/systemd/system/flexnetls-SCHNEIDR.service.d`	
`sudo rm -r /opt/flexnetls/SCHNEIDR`	
`sudo rm -r /var/opt/flexnetls/SCHNEIDR`	

Configuring the LLS

All user configurable settings for the LLS are found in the “local-configuration.yaml” file. The HTTP port number can be changed from this file if necessary.

This file can be found at:

- **Windows:** In the server folder where you installed LLS.
- **Linux:** In the /opt/flexnetls/SCHNEIDR/ directory.

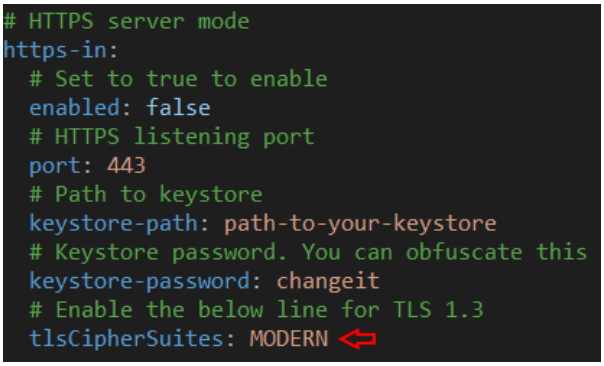
Disabling TLS 1.2

The LLS is configured to use both TLS 1.2 and TLS 1.3 by default. TLS 1.2 allows communication with PowerChute and Network Management Cards while TLS 1.3 will only work on PowerChute.

To disable TLS 1.2, follow the steps below:

Note: Disabling TLS 1.2 will only allow communication with PowerChute, not the NMC.

1. Stop the LLS service and open the “local-configuration.yaml” file.
2. Go to the line **#tlsCipherSuites: MODERN** and uncomment it.
3. Restart the LLS service again. TLS 1.3 will be enabled.



PowerChute

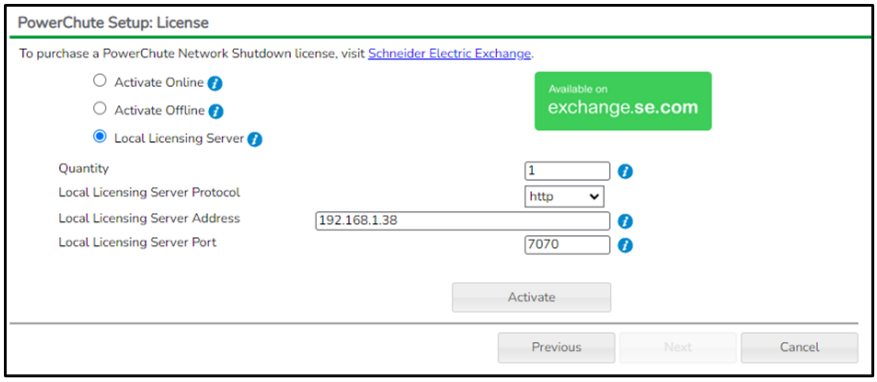
If you have multiple installations of PowerChute Network Shutdown which do not have access to the internet, it is recommended that you install a Local Licensing Server. This will allow you to license PowerChute from your licensing server hosted inside your offline network.

To connect to the LLS, there are three input fields required:

1. **Protocol:** The default protocol is set to HTTPS. This can be changed via the drop down menu.
2. **Address:** The address can be an IP address or a hostname.
3. **Port number:** The default port for the LLS is 443. If your LLS is configured for a different port this should be changed accordingly.

Note: Licenses are requested from the LLS using feature names, no activation ID is required.

Once the required fields are inputted, select **Activate.**



Adding LLS hostname to the host's file

If the SSL certificate you created is not using the hostname of your device that is running the LLS, you are required to enter the new hostname into the host's file.

1. Open the host's file on the device that is running PowerChute.
    - **Windows:** C:\Windows\System32\drivers\etc\hosts
    - **Ubuntu:** /etc/hosts
2. Where the hostname is used, input: <Ip Address of LLS> <hostname>

Adding HTTPS Certificate

To add a HTTPS certificate, follow the steps below:

Note: Before you add the certificate, you are required to set your user-defined password to the PowerChute-keystore.

1. Stop the PowerChute Network Shutdown service from running.
2. Copy the certificate into the **APC > PowerChute > group1** folder.
3. To add the rootCA into the PowerChute-keystore, run the following command as an administrator in the above directory.
    - **Windows:** `C:\Program Files\APC\PowerChute\jre_x64\bin\keytool.exe" -importcert -file <certificate> -keystore PowerChute-keystore`
    - **Linux:** `/opt/APC/PowerChute/jre-11.0.11/bin/keytool -importcert -file <certificate> -keystore PowerChute-keystore`
4. Restart the PowerChute Network Shutdown service and proceed to the configuration wizard.

Troubleshooting Issues

- The LLS must be running on internet time, otherwise there will be issues if switching between using the LLS and CLS as local device time may drift slightly

- If switching between different Local Licensing Servers, ensure they are running on the same time and in the same time zone otherwise issues will arise with requests being out of order.

- The error message that Java is not recognised as an internal or external command means that the environmental variable entry for the Java directory is missing. Depending on the Java installation you have installed, you should find a JAVA_HOME or JRE_HOME variable already being set. Add either %JAVA_HOME%\bin or %JRE_HOME%\bin to the PATH environmental variable to make Java available from any directory.

- The LLS will continue to allow licensing of new clients until the end of the licenses grace period. The CLS stops new clients at the start of the grace period.

- Once a license has expired on the LLS, it will not be visible to clients and the message "Unable to obtain license(s) from the Local Licensing Server" will be displayed. Please ensure you have licenses available on your Local Licensing Server.

- If there are multiple licenses on the LLS, the Local Licensing Server will return the license with the earliest expiry date first. If one license does not have enough quantity to cover a PowerChute Network Shutdown request quantity, then the Local Licensing Server will return what is available from the first license.

- If the LLS fails to start correctly after configuring it to use HTTPS, ensure that no other process is using port 443. If the port is already in use, change the HTTPS port that the LLS is using in the "local-configuration.yaml" file.