ETAPE de remise en état CPU AXC F 2152

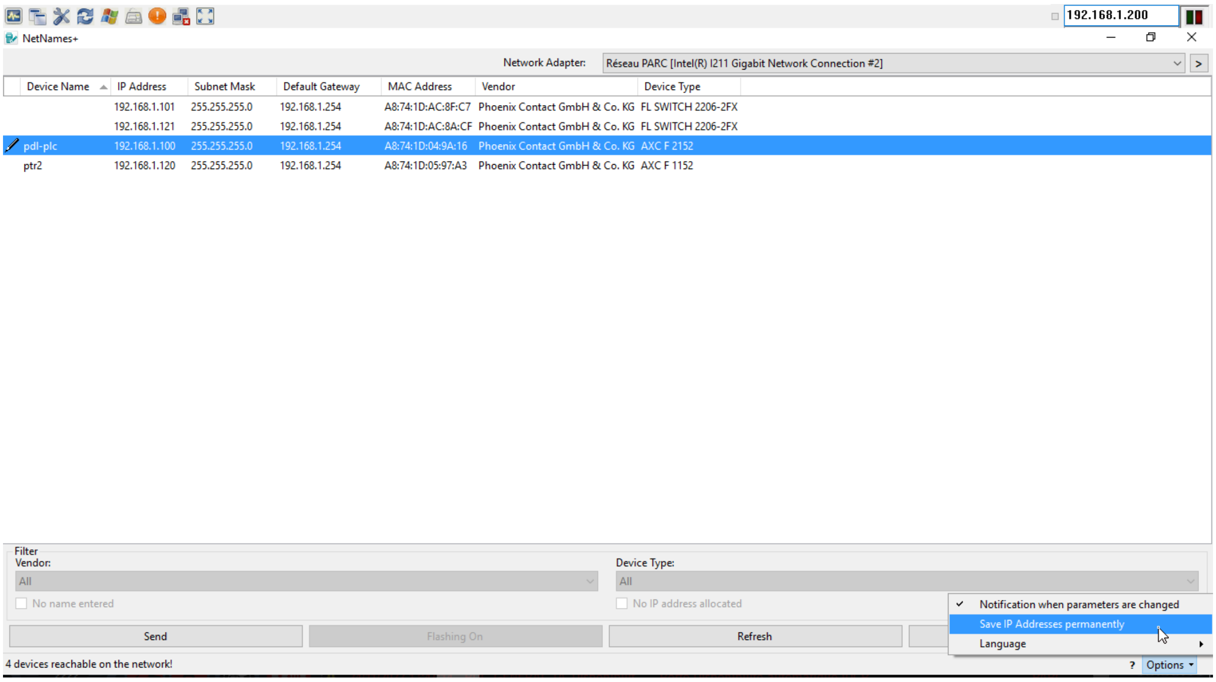
Vérifier si le logiciel NetNames+ 1.50 est installé sur le pc du site.

1) Récupérer le mot de passe par défaut de la CPU :
   a) Sous putty en mode admin
   b) Setting a root user password
   c) Se logger en root sous putty
   d) Taper cat /etc/device_data/phoenixsign/production_data , ce fichier contient une balise « DEFAULT_PASSWORD » contenant le mot de passe

2) Installer la licence de développement AVEVA procédure Wiki : Il faut préalablement un compte AVEVA
   https://wikiai.aifrance.com/doku.php?id=technique:supervision:aveva_edge_indusoft:installation_licence

3) Lancer NetNames en selectionnant le network adapter sur le réseau PARC.
   a) Selectionner la CPU AXC F 2152
   b) Modifier son adresse IP, masque de sous réseau et gateway si nécessaire.

   ATTENTION AVANT ENVOIE BIEN COCHER « Save IP Adress permanently »



Network Adapter: Réseau PARC [Intel(R) I211 Gigabit Network Connection #2]

Device Name	IP Address	Subnet Mask	Default Gateway	MAC Address	Vendor	Device Type
	192.168.1.101	255.255.255.0	192.168.1.254	A8:74:1D:AC:8F:C7	Phoenix Contact GmbH & Co. KG	FL SWITCH 2206-2FX
	192.168.1.121	255.255.255.0	192.168.1.254	A8:74:1D:AC:8A:CF	Phoenix Contact GmbH & Co. KG	FL SWITCH 2206-2FX
pdl-plc	192.168.1.100	255.255.255.0	192.168.1.254	A8:74:1D:04:9A:16	Phoenix Contact GmbH & Co. KG	AXC F 2152
ptr2	192.168.1.120	255.255.255.0	192.168.1.254	A8:74:1D:05:97:A3	Phoenix Contact GmbH & Co. KG	AXC F 1152

Filter
Vendor: All
Device Type: All
□ No name entered
□ No IP address allocated

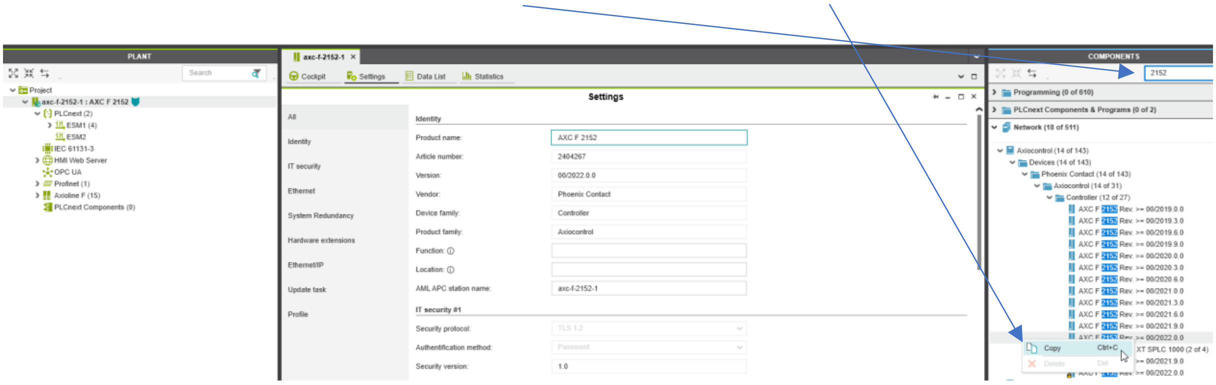
Send
Flashing On
Refresh
✓ Notification when parameters are changed
Save IP Addresses permanently
Language
?
Options

4 devices reachable on the network!

4) Vérifier la connexion à la page web de l'automate : https://192.168.1.100/wbm en utilisant l'utilisateur admin et le mot de passe par défaut précédemment récupéré.

5) Changer le mot de passe utilisateur Admin avec le mot de passe standard d'AI.
6) Refaire le chargement du firmware
7) Modifier la version de CPU en relation avec la version firmware.

Pour cela, taper Dans le menu **COMPONENTS** « 2152 » et cliquer droit puis copier



Settings

All / Identity / IT security / Ethernet / System Redundancy / Hardware extensions / Ethernet/IP / Update task / Profile

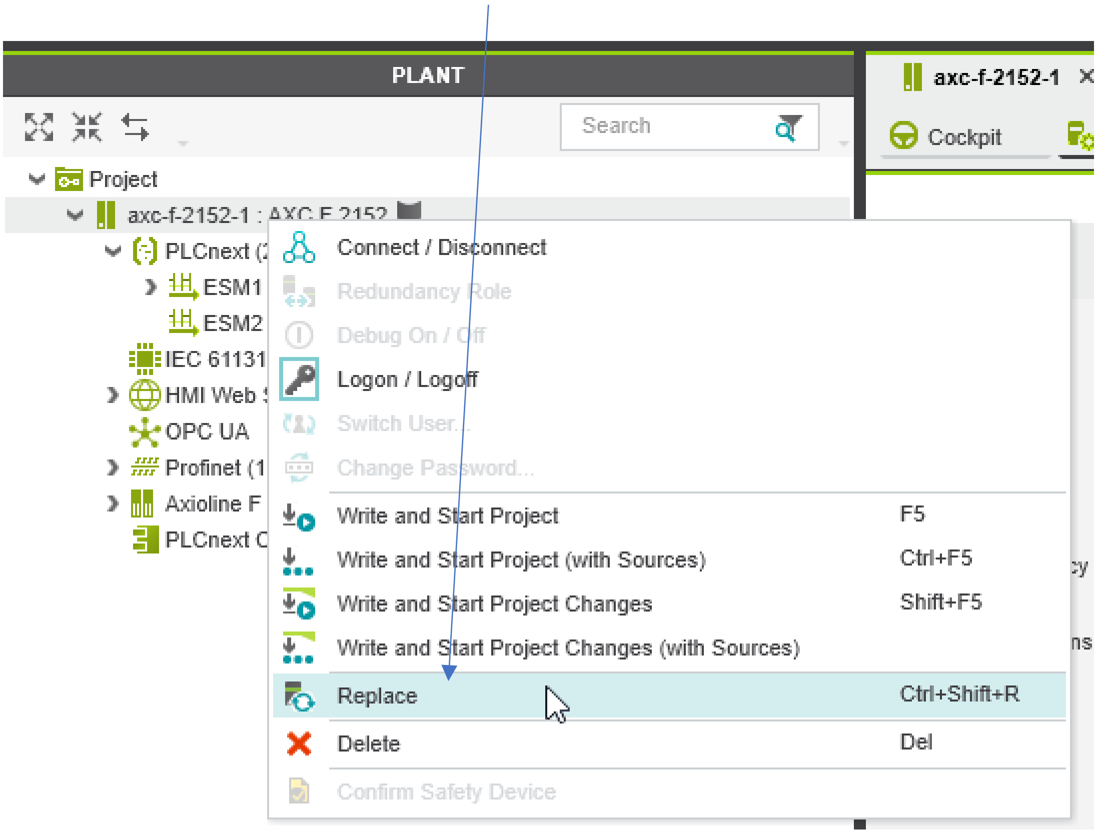
Identity

Product name: AXC F 2152
Article number: 2404267
Version: 00/2022.0.0
Vendor: Phoenix Contact
Device family: Controller
Product family: Axiocontrol
Function:
Location:
AML APC station name: axc-f-2152-1

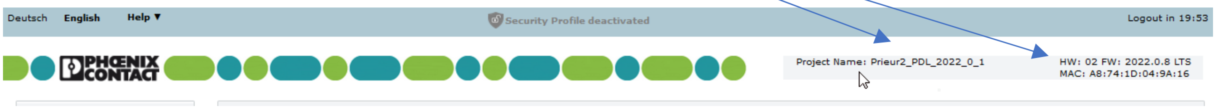
IT security #1

Security protocol: TLS 1.2
Authentification method: Password
Security version: 1.0

Puis cliquer droit sur la CPU et faire « **Replace ».**



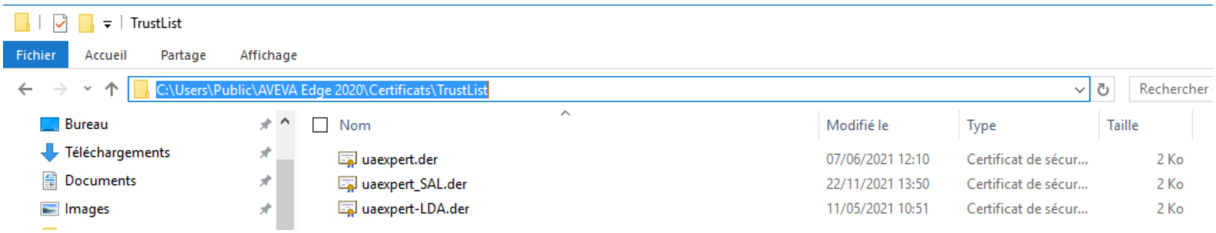
8) Vérifier la connexion à la page web de l'automate : https://192.168.1.100/wbm
Et vérifier que nom de projet et le firmware apparaît bien



Project Name: Prieur2_PDL_2022_0_1

HW: 02 FW: 2022.0.8 LTS
MAC: A8:74:1D:04:9A:16

9) Arrêter la supervision si ce n'est pas le cas.
10) Supprimer le résidu de certificat depuis l'explorateur windows :

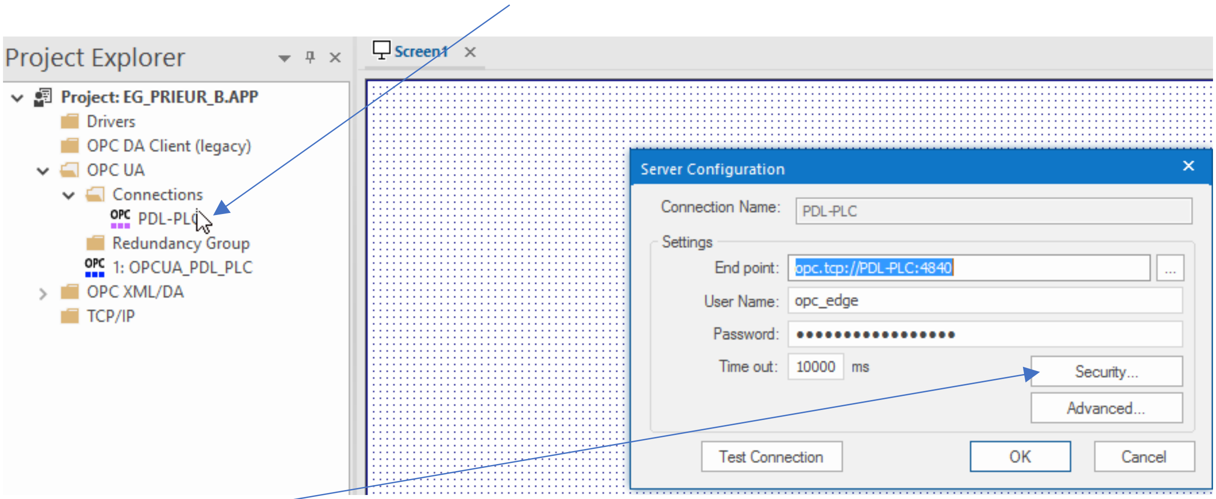


TrustList

C:\Users\Public\AVEVA Edge 2020\Certificats\TrustList

Nom	Modifié le	Type	Taille
uaexpert.der	07/06/2021 12:10	Certificat de sécur...	2 Ko
uaexpert_SAL.der	22/11/2021 13:50	Certificat de sécur...	2 Ko
uaexpert-LDA.der	11/05/2021 10:51	Certificat de sécur...	2 Ko

Depuis AVEVA studio ouvrir la connections OPC



Project Explorer

- Project: EG_PRIEUR_B.APP
  - Drivers
  - OPC DA Client (legacy)
  - OPC UA
    - Connections
      - PDL-PLC
    - Redundancy Group
    - 1: OPCUA_PDL_PLC
  - OPC XML/DA
  - TCP/IP

Server Configuration

Connection Name: PDL-PLC

Settings

End point: opc.tcp://PDL-PLC:4840

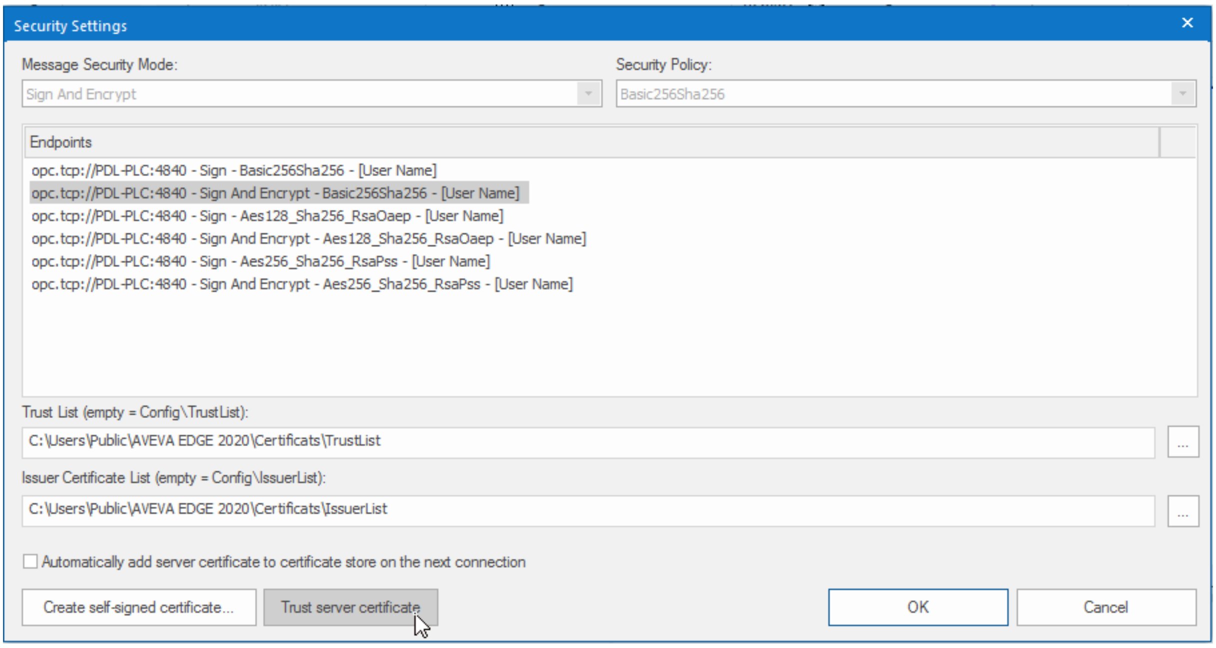
User Name: opc_edge

Password: ●●●●●●●●●●●●●●●●●

Time out: 10000 ms

, puis Security

Sélectionner le type de cryptage du certificat et cliquer sur « **Trust server certificate** » pour générer le certificat.



Security Settings

Message Security Mode: Sign And Encrypt

Security Policy: Basic256Sha256

Endpoints

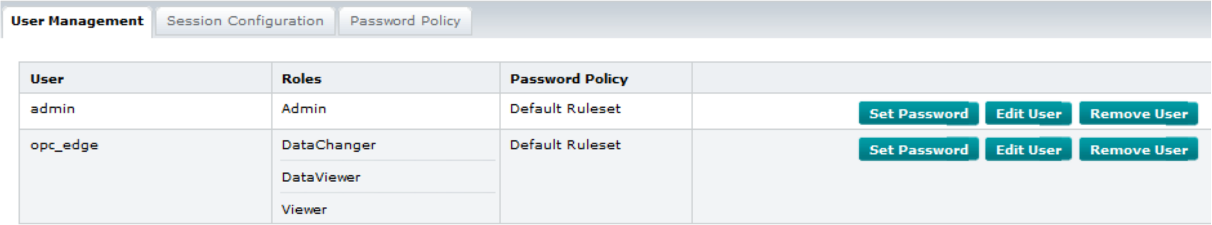
opc.tcp://PDL-PLC:4840 - Sign - Basic256Sha256 - [User Name]
opc.tcp://PDL-PLC:4840 - Sign And Encrypt - Basic256Sha256 - [User Name]
opc.tcp://PDL-PLC:4840 - Sign - Aes128_Sha256_RsaOaep - [User Name]
opc.tcp://PDL-PLC:4840 - Sign And Encrypt - Aes128_Sha256_RsaOaep - [User Name]
opc.tcp://PDL-PLC:4840 - Sign - Aes256_Sha256_RsaPss - [User Name]
opc.tcp://PDL-PLC:4840 - Sign And Encrypt - Aes256_Sha256_RsaPss - [User Name]

Trust List (empty = Config\TrustList): C:\Users\Public\AVEVA EDGE 2020\Certificats\TrustList

Issuer Certificate List (empty = Config\IssuerList): C:\Users\Public\AVEVA EDGE 2020\Certificats\IssuerList

☐ Automatically add server certificate to certificate store on the next connection

11) Depuis la page Web de l’automate, créer l’utilisateur opc_edge et attribuer les rôles : Datachanger, Dataviewer, Viewer.



User	Roles	Password Policy
admin	Admin	Default Ruleset
opc_edge	DataChanger DataViewer Viewer	Default Ruleset

Firmware update

Beginning with firmware version 2019.0 LTS, you can **update the firmware** conveniently via the Web-based Management of your controller.

For older firmware versions, you can start the firmware update via the `sudo update-plcnext` shell script, which you will find in the file system of the controller.

- Download the **.zip* firmware file from the download area of your controller.
- Unzip the **.zip* firmware file.
- Run the **.exe* setup file.
- Follow the instructions in the installation wizard.
- Open an SFTP client software (e.g., **WinSCP**).
- Log in as an administrator (default access data is User name: admin; Password: printed on the controllers' housing)
- Copy the **.raucb* update file to the */opt/plcnext* directory (home directory of the Linux user "admin").
- Open the shell using a command line tool (e.g., PuTTY or Tera Term).
- Log in as administrator.
- Issue the update command: The name of the update script is the same for every controller:`sudo update-plcnext`. The script is available in the directory under */usr/sbin/*. Under */usr/sbin/*, you will also find symbolic links with the respective product designation in the name, e.g., `sudo update-axcf2152`.

The script executes the following operations:

1. Stopping the PLCnext Technology process.
2. Performing the firmware update.
3. Rebooting the system and deleting the firmware container.

The same goes for downgrading to a former firmware version.

Note:

Known for firmware 2020.6 or newer on all supported PLCnext Control devices:

After downgrading the firmware, it is recommended to reset to **Default setting Type 1** (see **Factory Reset**). This is not necessary when updating the firmware.

Reset to default setting type 1 and type 2

You can reset the controller to the default settings using a shell script. Here, a distinction is made between two types of default settings:

- **Type 1:**
  All user-specific data is deleted (settings, programs, users, etc.). The current PLCnext Technology firmware remains unchanged.
- **Type 2:**
  In addition to the user-specific data (type 1), the firmware of the controller is reset to default state.

The script is available in the controller file system. The name of the factory reset script is the same for every controller: `sudo recover-plcnext`

You will find the script under */usr/sbin/*. When calling the script, specify the desired reset type, e.g., `sudo recover-plcnext 1` for type 1 default settings.
Under */usr/sbin/*, you will also find symbolic links with the respective product designation in the name, e.g.,
`recover-axcf2152 1` for type 1 default settings of a PLCnext Control AXC F 2152.

Note: You can also reset your controller to type 1 and type 2 default settings via the device-specific operating elements (e.g., reset button or operating display). For additional information, please refer to the corresponding **user manual**.

The type 1 default settings can also be restored via the **Cockpit** editor in PLCnext Engineer.

Note: Files that are stored outside the ***upperdir*** directory are not deleted during a reset to default setting type 1 or type 2 (e.g. PLCnext apps may not be installed and OCI images are not installed in the upperdir directory).

So in this case not necessarily all user files are deleted and a reset to default setting type 2 does not necessarily restore the controller to factory default state.

All licenses, and especially licenses that are bound to the device, are retained.

Controlling the firmware

The `plcnext` script in the */etc/init.d* directory controls the firmware.

You can control the firmware with the following commands:

Shell command	Description
`sudo /etc/init.d/plcnext stop`	Stops all PLCnext firmware processes
`sudo /etc/init.d/plcnext start`	Starts all PLCnext firmware processes
`sudo /etc/init.d/plcnext restart`	Restarts all PLCnext firmware processes

Connecting to the controller

Default System Use Notification

If you connect to the controller via SSH or SFTP (e.g. using WinSCP), you will receive the following system use notification for your attention:

```
Hinweis:
Dieses Geraet darf nur von autorisierten Benutzern fuer autorisierte
Zwecke verwendet werden. Ihre Anmeldeinformationen und alle
Benutzeraktionen auf diesem Geraet koennen ueberwacht,
aufgezeichnet, kopiert und auditiert werden.
Durch die weitere Verwendung dieses Geraets erklaeren
Sie sich mit diesen Bedingungen einverstanden.

Notice:
This device may only be used by authorized users for authorized
purposes. Your credentials and all user actions on this device can
be monitored, recorded, copied and audited. By continuing to use
this device, you agree to these terms.
```

The text is also displayed when logging in to the controller via PLCnext Engineer.

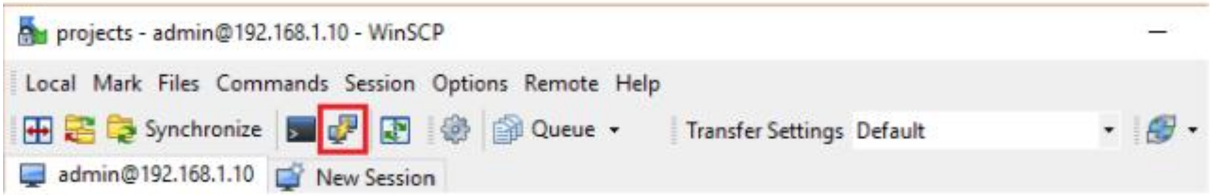
The displayed text is stored in a *.txt* file on the controller by default and can be changed or replaced if necessary. The file can be found on the file system of the controller under */opt/plcnext/config/System/Um/UmSystemUseNotifcation.txt*. To change the file, you must be logged in as Linux user `admin`.

From firmware version 2021.0 LTS on you also have the possibility to edit the **System Use Notification** via the WBM of the controller.

For executing commands on the controller

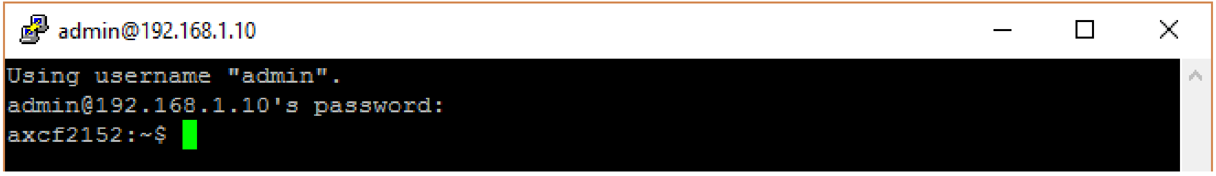
Using a Windows® PC

- If already connected to the controller using WinSCP, open the console by clicking the **Open in PuTTY** button:



Otherwise you may also use PuTTY directly.

- At the prompt, enter the admin user's password:



```
Using username "admin".
admin@192.168.1.10's password:
axcf2152:~$ 
```

You're ready to issue Linux® commands.

User rights

Default user

PLCnext Controls are supplied with a preset **admin user** and a default password that is printed on the controller's housing. This enables access to the most important functions.

`admin` user

When a PLCnext user logs into the SSH console with the **`admin`** user, the user is also recognized with the same name and password by the Linux system. The user is therefore assigned to the **`plcnext`** Linux group. Files that this user may read, write to and/or execute are assigned to the **`plcnext`** group file system.

`plcnext_firmware` user

The **`plcnext_firmware`** user is another major user in the Linux system. It is permanently integrated and is used for starting the PLCnext firmware processes. In the Linux system, the user has the rights to execute all the operations required.
In addition to the Linux user rights, the PLCnext Technology firmware also has its own user management. Its configuration is described in **User Authentication**.

Override with `sudo`

Executing Linux commands that require higher rights is made possible for the users via `sudo`. Which Linux commands the PLCnext users are allowed to execute via `sudo` is being configured in the Linux system.

Default rights settings

The following rights are available:

Rights	`plcnext` **group**	**admin**	`sudo` **required**
Setting and inspecting IP settings (including `ifconfig`, `ping`, `netstat`, etc.)	✓	✓	✓ (for `ifconfig`)
Configuring the **firewall**	✓	✓	–
Starting/stopping the firewall (`init` script)	✓	✓	✓
Inspecting the firewall with `nft`	✓	✓	✓
Configuring VPN (IPsec and OpenVPN™)	–	✓	–
Starting/stopping VPN services (IPsec and OpenVPN™)	–	✓	✓
Editing the ***Default*** PLCnext folder for individual ACF, ESM, GDS configurations, and **.so*	✓	✓	–
Starting/stopping the PLCnext Technology firmware processes `sudo /etc/init.d/plcnext start|stop|restart`	–	✓	✓
Reading PLCnext log files	✓	✓	–
Calling and configuring TOP/HTOP	✓	✓	–
Firmware update via update script with `sudo update-plcnext-`	–	✓	✓
Configuring the NTP server	✓	✓	–
Setting the root password with `passwd`	–	✓	✓
Requesting the system time with `date`	✓	✓	–
Setting the system time with `sudo date -s`	✓	✓	✓

Restarting/shutting down the controller with `reboot` or `shutdown`	–	✓	✓
Write access to */opt/plcnext* and */opt/plcnext/projects*	✓	✓	–
Recording network traces with `tcpdump`	✓	✓	✓
Starting the `gdbserver` with root rights (see **here** how to do that)	–	✓	✓
Resetting to factory defaults with `sudo recover-plcnext 1` (see also **Factory reset**)	–	✓	✓

Root rights

For some commands you require advanced rights. To this end, the root user password needs to be set while the root user itself already exists under the Linux® system.

Risk of personal injury or damage to equipment

With active `root` user access, the controller must not be used for live operation.

Before live operation of the controller return to an appropriate user role and remove the `root` user password.

Security Note: With `root` user access, you can make unlimited changes on the controller. Root rights are therefore **only** suitable for qualified application programmers and software engineers with relevant experience.

- **Avoid** making changes to the PLCnext Technology firmware or Operating System itself. If changes are neccessary, see **Overlay File System** for details.
- **Do not** supply the device with an already set password for the `root` user.
- **Remove** the root password as soon as `root` user access is not required any more.

Setting a root user password

- **Connect to the controller** via its IP address and log in as `admin` user. The default password for the user printed on the controller's housing.
- Enter this command: `sudo passwd root`.
- Enter the `admin` user's password to authorize this command.
- Enter a **new** password for the `root` user (minimum 5 characters, preferably consisting of upper-case and lower-case letters plus numbers).
- Confirm the new password by entering it again.
  Show the screenshot

Using the root user

- **Connect to the controller** via its IP address and log in as `admin` user. The default password for the `admin` user is printed on the controller's housing.
- Switch to the `root` user with the `su -` command and the `root` user's password.
- Perform the activities that need the `root` user's rights.
- Once you have executed all the activities as the `root` user, change back to the previous user role (e.g., `admin`) using the `exit` command.

Removing the root password

If the `root` user is no longer required, remove the password. This prevents unauthorized users from modifying the firmware.

- Connect to the controller via its IP address and log in as `admin` user. The default password for the user printed on the controller's housing.
- In the shell or command line interface, enter this command: `sudo passwd -d root`.

After that, the `root` user stays present on the controller. Before using it again you have to set a new password.

Recommended: The easiest way to undo changes to the `root` user is a reset to default setting type 1. This will also remove the `root` user's password.

Directories of the firmware components

You can access the controller via SFTP or via SSH, view the directories and files in the Linux file system (on the internal flash memory and on the SD card), and modify them if necessary.

Directories and files that Phoenix Contact provides (also through firmware updates) are stored on the internal flash memory of the controller.

If you make changes to the directories or files, the Linux operating system generates an overlay file system. The storage location depends on whether you operate the controller with or without an **SD card**.

Operation without an SD card

Note: Phoenix Contact recommends operating the PLCnext Control device with an SD card if it supports SD card operation. For some PLCnext Control devices, operation with an SD card is mandatory. Refer to the user manual of your PLCnext Control device.

If you make changes to the directories or files on the internal flash memory, the Linux operating system generates an overlay file system there.

Operation with an SD card

Note: Phoenix Contact recommends operating the PLCnext Control device with an SD card if it supports SD card operation. For some PLCnext Control devices, operation with an SD card is mandatory. Refer to the user manual of your PLCnext Control device.

If you operate the controller with an SD card, it generates the overlay file system on the SD card.
Settings that you have configured by yourself (for example, network configuration, configured bus configuration, PLCnext Engineer project, etc.) are also saved to the SD card.

Major directories on the internal file system

Directory in the root file system	Contents
/usr/local/lib	Directory for storing additional open-source libraries that customized C++ programs use (see **C++ programming**).
/usr/share/common-licenses	License information on the individual Linux packages of the controller.

/opt/plcnext	Home directory of the `admin` Linux user and working directory of the device firmware. Files written by the application program are stored in this directory if the specified file name does not contain a storage path.
/opt/plcnext/config 2019.9, 2020.0 LTS, 2020.3	Directory for storing configuration files that are not project-specific.
/opt/plcnext/config/System/Um ≥ 2020.6	Directory for storing configuration files of the User Manager. • *UmSystemUseNotifcation.txt*: The file contains the Default System Use Notification that is displayed if you connect to the controller via SSH or SFTP (for example, using WinSCP). **Click here** for more information.
/opt/plcnext/logs	Directory for storing the log files of the Diagnostic Logger as well as the database of the Notification Logger This directory contains the *Output.log* file. It contains information on the startup behavior of the firmware, status, and error messages as well as warning notes that help you find the source of error. **Click here** for more information. In addition, you will find the diagnostic log file of the`plcnextapp` command line tools (*plcnextapp.log*) as well as the log files of the UA server (uatrace.log, uatrace_1.log).
/opt/plcnext/projects	Directory for storing project directories and files
/opt/plcnext/projects/Default	Directory for storing project directories and files downloaded manually by the user
/opt/plcnext/projects/PCWE	Directory for storing PLCnext Engineer projects PLCnext Engineer exclusively manages all files and subdirectories in this directory. **Note:** **Do not make any changes** to this directory.
/opt/plcnext/Security	Directory for storing certificates of `IdentityStores` and `TrustStores` , which the WBM manages.

/opt/plcnext/Security/Certificates/https	Directory for storing the HTTPS certificate **Note:** Certificate setting **From firmware 2021.0 LTS** Up to firmware 2020.6, the HTTPS certifcate and its related private key were located as files on the file system of the controller. These files have been replaced by symbolic links. Therefore, when updating the firmware, the existing certificate and key files are moved to _/opt/plcnext/Security/IdentityStores/HTTPS-self-signed-Backup/*.*_and symbolic links are created at the original location pointing to this backup. On the WBM **Certificate Authentication** page you can either select to use an existing IdentityStore or to use self-signed certificates. When using an existing IdentityStore the symbolic links are changed and refer now to the specified IdentityStore. When using self-signed certificates a self-signed certificate is generated at _/opt/plcnext/Security/IdentityStore/HTTPS-self-signed/*.*_and the symbolic links refer to that IdentityStore. When creating a self-signed certificate via the **Certificate Authentication** WBM page, the */opt/plcnext/Security/IdentityStores/HTTPS-self-signed-Backup* directory is not modified. **Up to firmware 2020.6** The HTTPS certificate and its related private key are located as files in the following directories of the controller file system: • */opt/plcnext/Security/Certificates/https/https_cert.pem* • */opt/plcnext/Security/Certificates/https/https_key.pem* You can exchange these files by your own certificate and key.

/opt/plcnext/Security/TrustStores	Directory for storing the `TrustStores` configured in WBM. Each subdirectory corresponds to the name of a `TrustStore`. A `TrustStore` directory contains the following subdirectories: • trusted: The directory contains CA certificates that are trusted. • issuers: The directory contains CA certificates that are not automatically trusted but that are necessary for creating a certificate chain. • trusted/crl: The directory contains files with CRLs for the CA certificates. • issuers/crl: The directory contains files with CRLs for issuer certificates. **Note:** The firmware internally uses the */opt/plcnext/Security/TrustStores/Empty/*`TrustStore`. **Do not** make any changes to the directory, the subdirectories, or the files of the */Empty*`TrustStore`.
/opt/plcnext/Security/IdentityStores	Directory for storing the `IdentityStores` configured in the WBM. Each subdirectory corresponds to the name of an IdentityStore. An IdentityStore contains identities (X.509 certificates with associated private key). An IdentityStore directory contains the following files: • *certificate.pem*: The file in PEM format contains the X.509 certificate of the identity. The file may additionally contain several certificates of the certificate chain. • *key.pem*: The file in PEM format contains the private key for the certificate. • *tpmkey.pem*: The file contains the private key linked to the TPM (Trusted Platform Module) of the controller.
/opt/plcnext/apps	All active apps downloaded from the PLCnext Store to the controller are mounted in this directory.

	Each active app is mounted with the name of the app identifier in a subdirectory. The entire content of the app container is available in this directory (read-only). The PLCnext Store manages the directory. Do not make any changes to this directory.
/opt/plcnext/installed_apps	Directory for storing all installed app containers The directory belongs to the PLCnext Store.
/opt/plcnext/appshome	Directory for storing and managing app data The PLCnext Store and the installed apps manage the directory. Do not make any changes to this directory.
/opt/plcnext/lttng	Directory for storing the default configuration files for tracing via LTTng
/opt/plcnext/lttng_traces	Directory for storing trace files The directory is created during runtime of the trace controller when the trigger function for storing the trace files is called for the first time. Each time the trigger function of the memory is called, a new subdirectory (trace directory) for storing the current trace data is created. The designation of a trace directory is structured as follows: `YYYYMMDD_hhmmss` For example: ***/opt/plcnext/lttng_traces/20190418_190615/<trace_data>*** The memory operates as a ring memory. When exceeding the maximum storage space, the oldest trace directory is deleted.
/opt/plcnext/backup	Directory for download changes operations The directory is used for creating a backup of the project directory (***/opt/plcnext/projects/***). In the event of an error, the contents of the backup directory are restored. The backup directory is created following the

	first successful project download and following every successful project download.
/opt/plcnext/retaining	Directory for storing remanent data
/opt/plcnext/retaining/backups ≥ 2021.0 LTS	Directory for storing backup files that contain the retain variable values and its corresponding retain CRC along with the project name. Up to 10 backup files are stored before the oldest file is deleted. The criterion is the file name. You can find more information about the backup and restore feature in the topic **Extended retain handling**.
/opt/plcnext/shadowing	Directory for internal storage of copies of C++ user libraries that have been configured in PLCnext Engineer and downloaded.
/opt/plcnext/profinet	Directory for storing temporary PROFINET® files

Using SFTP to access the file system

You can access the file system via the SFTP protocol. Use a suitable SFTP client software for this (for example, WinSCP).

Access to the file system via SFTP requires authentication with a user name and password. The following access data is set by default with administrator rights:

- **User name:** admin
- **Password:** is printed on the PLCnext Control

SSH login as root user

By default, the SSH login as a `root` user is prevented for security reasons. Nevertheless, they are some cases where the SSH login as the `root` user is necessary to perform commands that are reserved for the `root` user under a secure SSH connection.

To log in as a root user, the **root user password** must be set.

Security Note: With `root` user access, you can make unlimited changes on the controller. Root rights are therefore **only** suitable for qualified application programmers and software engineers with relevant experience.

- **Avoid** making changes to the PLCnext Technology firmware or Operating System itself. If changes are neccessary, see **Overlay File System** for details.
- **Do not** supply the device with an already set password for the `root` user.
- **Remove** the root password as soon as `root` user access is not required any more.

To enable or disable direct login via SSH for the `root` user, you have to configure this in the *sshd_config* file as shown here:

Activating SSH login as root user

- **Connect to the controller** and log in as the `root` user.
- Open the */etc/ssh/sshd_config* file with a suitable editor.
- In the `# Authentication:` section, enable the `PermitRootLogin yes` entry that is commented out by default.
- Restart the SSH service with `/etc/init.d/sshd restart`.

Deactivating SSH login as root user

- **Connect to the controller** and log in as the `root` user.
- Open the */etc/ssh/sshd_config* file with a suitable editor.
- Change the `PermitRootLogin yes` entry in the `# Authentication:` section to a comment again.
- Restart the SSH service with `/etc/init.d/sshd restart`.