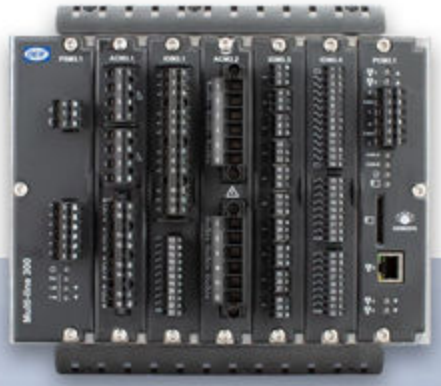
AMC 300

4189341264C

Programmable Automation Controller

User's manual

DEIF Improve Tomorrow



1. Revision

1.1 Revision history

Date	Revision	Changes
2020-12-15	Revision A	The first version of this document.
2021-05-10	Revision B	Re-published in new stylesheet, no content changes.

2. About the User manual

2.1 Intended users of the User manual

The User manual is primarily intended for the operator that performs daily operations with the controller.

The manual includes an overview of tools, software, logs, and the web interface.

2.2 Software versions

The information in this document corresponds to the following software versions.

Table 2.1 Software versions

Software	Details	Version
BSP	Board Support Package	4.0.0.x
CODESYS	CODESYS runtime	3.5.15.0 or later
CODESYS IDE	PC software for development of CODESYS applications	3.5.15.0 or later
CODESYS TSP	AMC 300 CODESYS Target Support Package (TSP)	1.0.1.0

2.3 Technical support

If you need technical support:

1. Technical documentation:
   - Download relevant technical documentation from www.deif.com/documentation.
2. Support:
   - DEIF offers 24-hour support.
   - See www.deif.com for contact details, there may be a DEIF subsidiary located near you.
   - You can also e-mail support@deif.com.
3. Service:
   - DEIF engineers can help with design, commissioning, operating and optimisation.
4. Training:
   - DEIF regularly offers training courses at the DEIF offices worldwide.

You can read more about service and support options on www.deif.com.

2.4 Warnings and safety

2.4.1 Safety during installation and operation

When you install and operate the equipment, you may have to work with dangerous currents and voltages. The installation must only be carried out by authorised personnel who understand the risks involved in working with electrical equipment.

DANGER!

Hazardous live currents and voltages

Do not touch any terminals, especially the AC measurement inputs and the relay terminals, as this could lead to injury or death.

2.4.2 Electrostatic discharge

Protect the equipment terminals from electrostatic discharge when not installed in a grounded rack. Electrostatic discharge can damage the terminals.

2.4.3 Factory settings

The controller is delivered pre-programmed from the factory with a set of default settings. These settings are based on typical values and may not be correct for your system. You must therefore check all parameters before using the controller.

2.4.4 Data security

The AMC 300 includes a firewall.

To minimise the risk of data security breaches we recommend:

- If possible, avoid to expose controllers and networks to public networks and the Internet.
- Use additional security layers like a VPN for remote access.
- Restrict access to authorised persons.

2.4.5 Do not use unsupported hardware modules

Only use the hardware modules that are listed in the Technical specifications. Unsupported hardware modules can make the controller malfunction.

3. Configure AMC 300

3.1 Software

3.1.1 Download AMC 300 software

Download the AMC 300 software from https://www.deif.com/software:

- CODESYS IDE
- AMC 300 CODESYS Target Support package
- AMC 300 firmware (BSP versions)

3.1.2 System requirements

The requirements for the development PC to install the Development packages, PC tools and drivers are:

- Microsoft Windows 10, 32 bit version
- Microsoft Windows 10, 64 bit version (Recommended)

As the AMC 300 supports SSH (Secure Shell) and SCP (Secure Copy) as basic communication protocols, it can be accessed from any system supporting these protocols (if enabled).

NOTE Not all browsers are suitable for this software. We recommend to use Google Chrome or Mozilla Firefox.

3.1.3 PC tools

Bonjour service – mDNS service

We recommend the tool Bonjour service as mDNS service. Download Bonjour service from the official web-site:

- https://support.apple.com/kb/DL999?locale=en_US

PuTTY — SSH client (Linux command shell)

We recommend the free tool PuTTY for Linux command shell access (SSH communication). Download PuTTY from the official web-site:

- https://www.chiark.greenend.org.uk/~sgtatham/putty/

WinSCP – SFTP client (for file transfer)

For secure file transfer (SFTP or SCP communication), for example for configuration and software updating, we recommend the free tool WinSCP. Download WinSCP from the official web-site:

- https://winscp.net/eng/index.php

NOTE Windows PowerShell SSH and SCP are built-in features. Some of the more advanced cryptographic features require Linux, Docker for Windows or WMware.

3.2 Connection

3.2.1 Power connection

To configure and program the AMC 300, apply a 12 or 24 V power supply to the power supply terminals of the PSM3.1/ PSM3.2 module. See the **Installation instructions** for details.

The AMC 300 system software is operational approx. 30 seconds from power on.

NOTE The AMC 300 file system is tolerant to sudden power off, and parameters are automatically stored in the non-volatile memory. No special shutdown procedure is required.

3.2.2 Programming connection

The AMC 300 is configured and programmed via the Ethernet ports on the PCM3·1 module, both for development (direct access) and when installed on site (remote).

The configuration is mainly made via the AMC 300 web page. Special configuration can be made by editing configuration files stored in the AMC 300 file system, and accessed via the SSH (Linux command shell) or SFTP (file transfer).

The PCM3·1 module must be connected to the development computer directly via an Ethernet cable or an Ethernet network. By default, the PCM3·1 only offers secure connections.

By default, all switch ports of PCM3.1 are configured as access ports with VLAN 1. VLAN 1 is configured with mDNS enabled (for example, Bonjour service) and IPv4 and IPV6 in mode Link-local only.

Default hostname: **AMC300**

A PC setup to IPv4 or IPv6 with a Link-local address and mDNS support can access the system web pages on https://amc300.local.

3.2.3 Default user and password

The AMC 300 is by default supplied with one user account (Administrator):

- User name: **admin**
- Password: **admin**

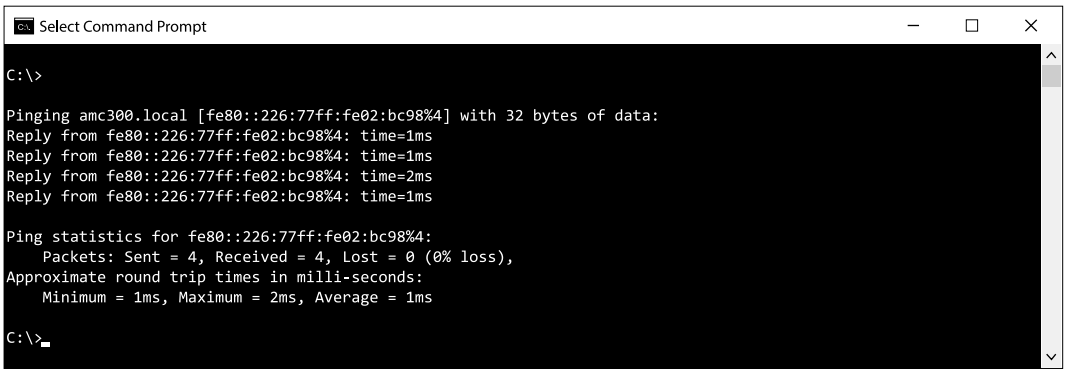
Additional users can be added in the Users menu.

NOTE First time you log in the AMC 300 web page you are prompted to change the password for the admin user.

3.2.4 Test the connection

You can test the connection by sending a 'ping' to the AMC 300. Use the option -6 to force IPv6:

- ping -6 AMC300.local



If there is no connection:

- Check the Ethernet cable
- Check the power to the AMC 300
- Check your PC firewall settings
- Check if the AMC 300 is configured with another IP address than default

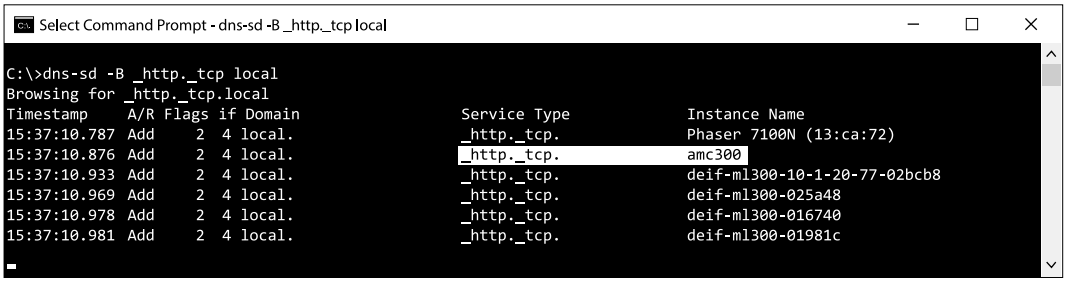
As alternative to access the controller via the hostname, you can use the IPv6 address in the browser. Use the square brackets [ ] to specify an IPv6 address in the URL.

- http://[fe80::226:77ff:fe02:bc98]/

3.2.5 Find network devices

If the hostname is changed from default, you can use the Bonjour service via command dns-sd to view the devices on the network:

- dns-sd -B _http._tcp local

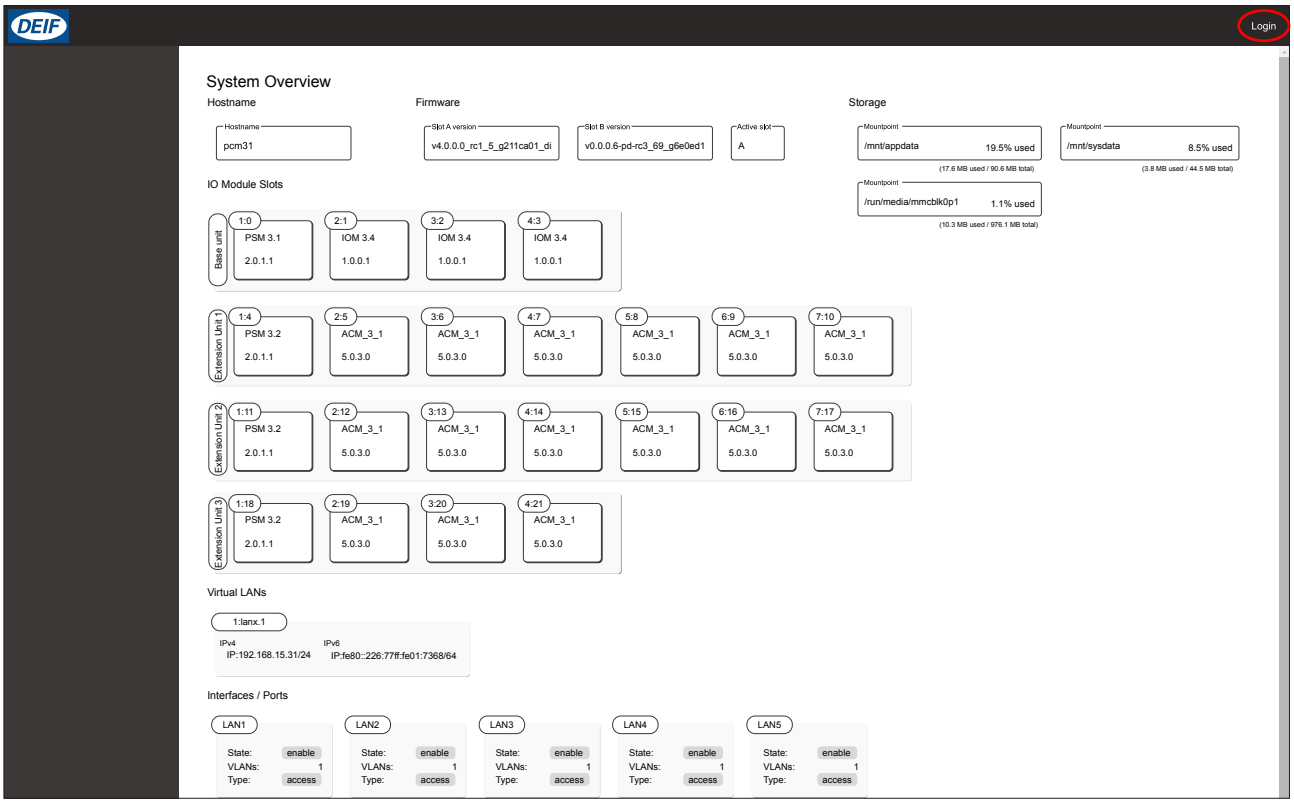


3.3 The system web page

3.3.1 Access to the System web page

To access the AMC 300 system page, open a browser and go to https://amc300.local. If you cannot access the web page, see the section **Test the connection** to resolve the IPv6 network address.

1. Select **Login** in the upper right corner.

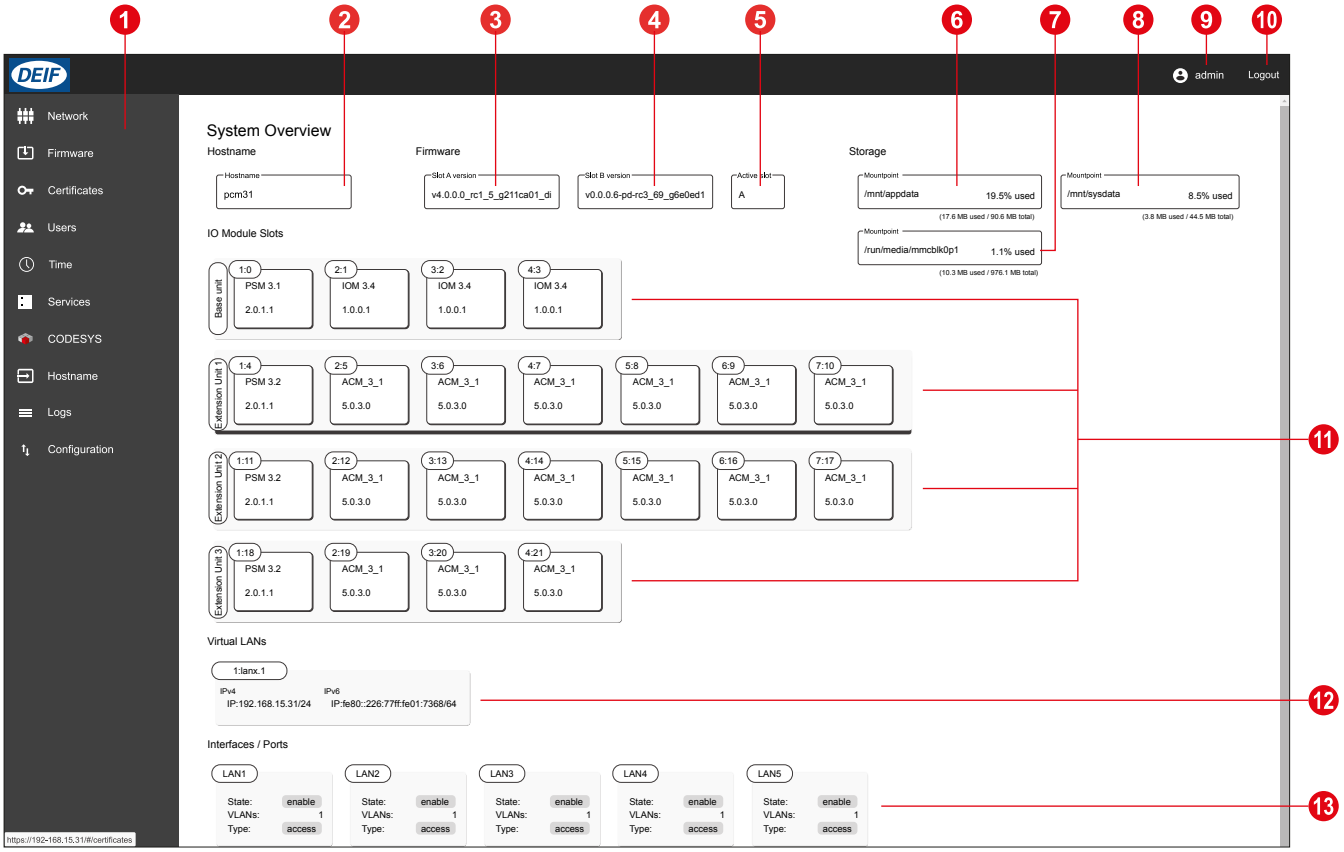


2. Write your user name and password in the pop-up window.

3. Select Login.

3.3.2 Overview of the System web page

When you are logged in, you get an overview of the system:



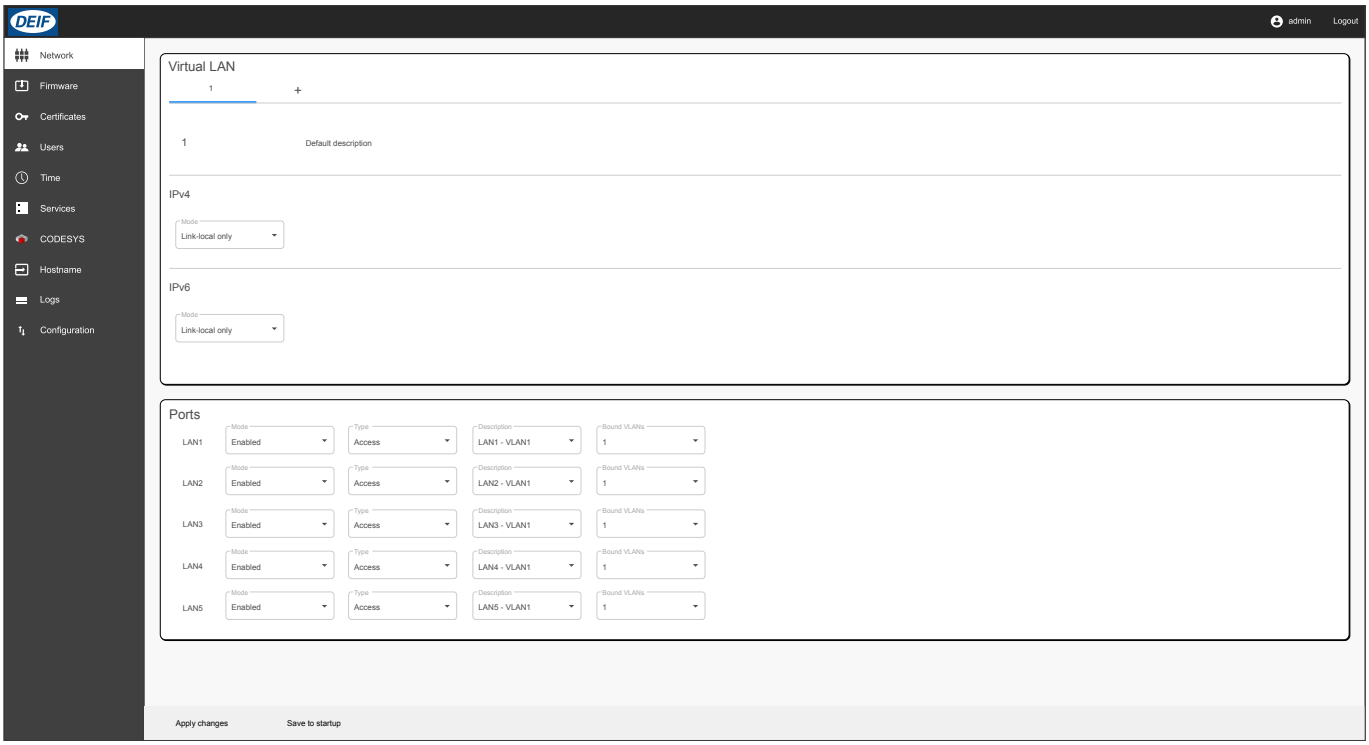
No.	Item	Notes
1	Menu	Select web pages for Network, Firmware, Certificates, Users, Time, Services, CODESYS, Hostname, Logs and Configuration.
2	Host name	Name of the web host.
3	Firmware Slot A	Firmware version for slot A.
4	Firmware Slot B	Firmware version for slot B.
5	Active slot	The active slot.
6	Storage application data	Storage volume for the application data, used and total.
7	Storage SD card	Storage volume for an SD memory card, used and total.
8	Storage system data	Storage volume for the system data, used and total.
9	Active user	Name of the active user.
10	Login/Logout	log in/log out of the system web page.
11	Input/output modules	Available input/output modules in the base unit and expansion units.
12	Virtual LAN	Addresses for IPv4 and IPv6
13	Interfaces/Ports	Available LAN ports.

3.4 Menus

3.4.1 Network

This menu give access to manage Ethernet network configuration, such as ports, VLAN and IP.

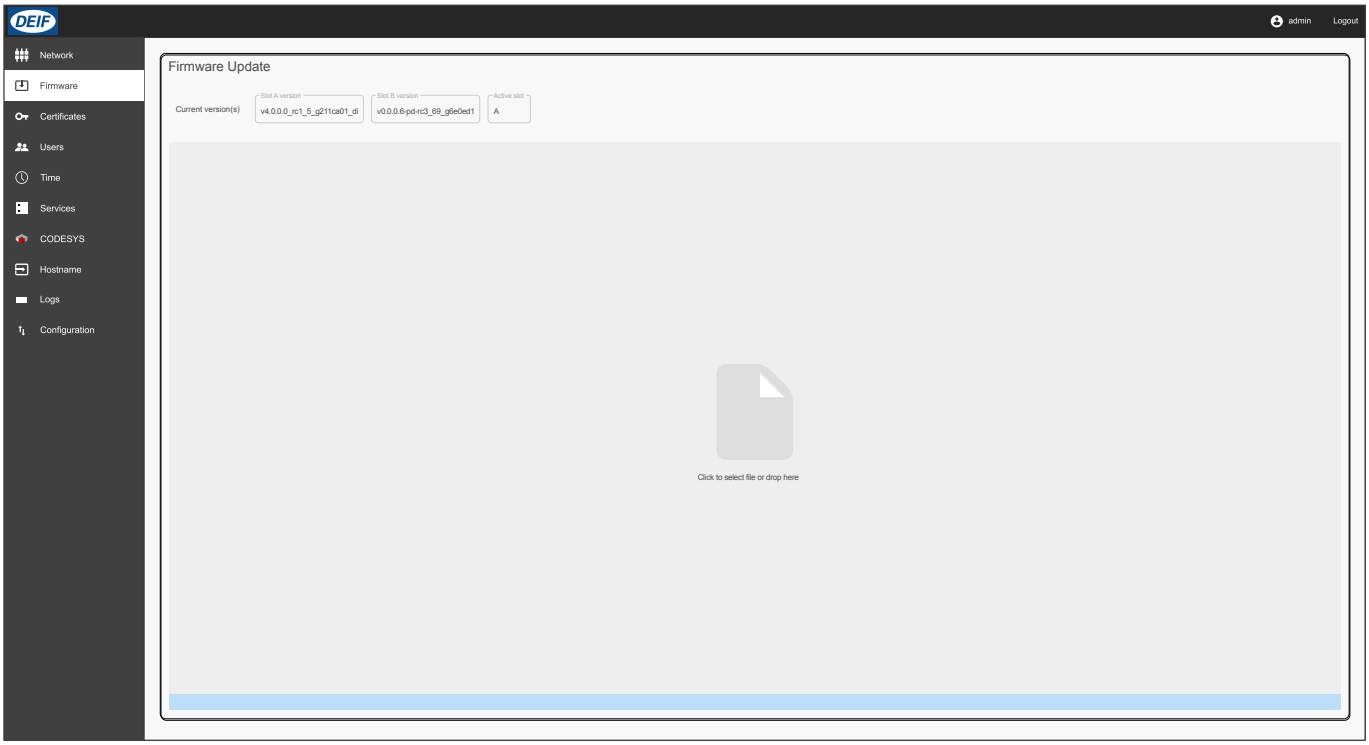
Necessary permissions: **Network management**.



3.4.2 Firmware

This menu gives access to update firmware for the AMC 300.

Necessary permissions: **Firmware update**.



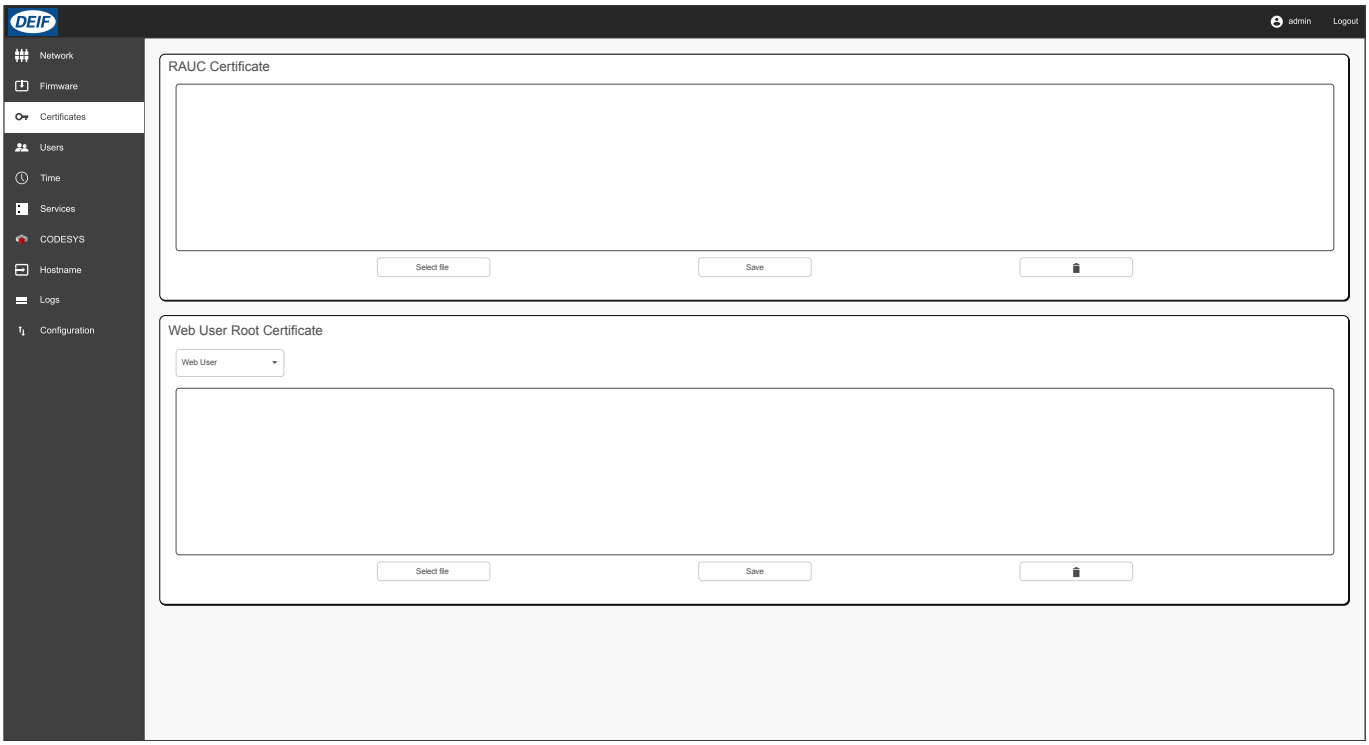
NOTE Updating the firmware does not change the controller configuration.

3.4.3 Certificates

This menu gives access to manage the RAUC and Web User Root CA (mTLS) certificates.

Necessary permissions: **admin user**.

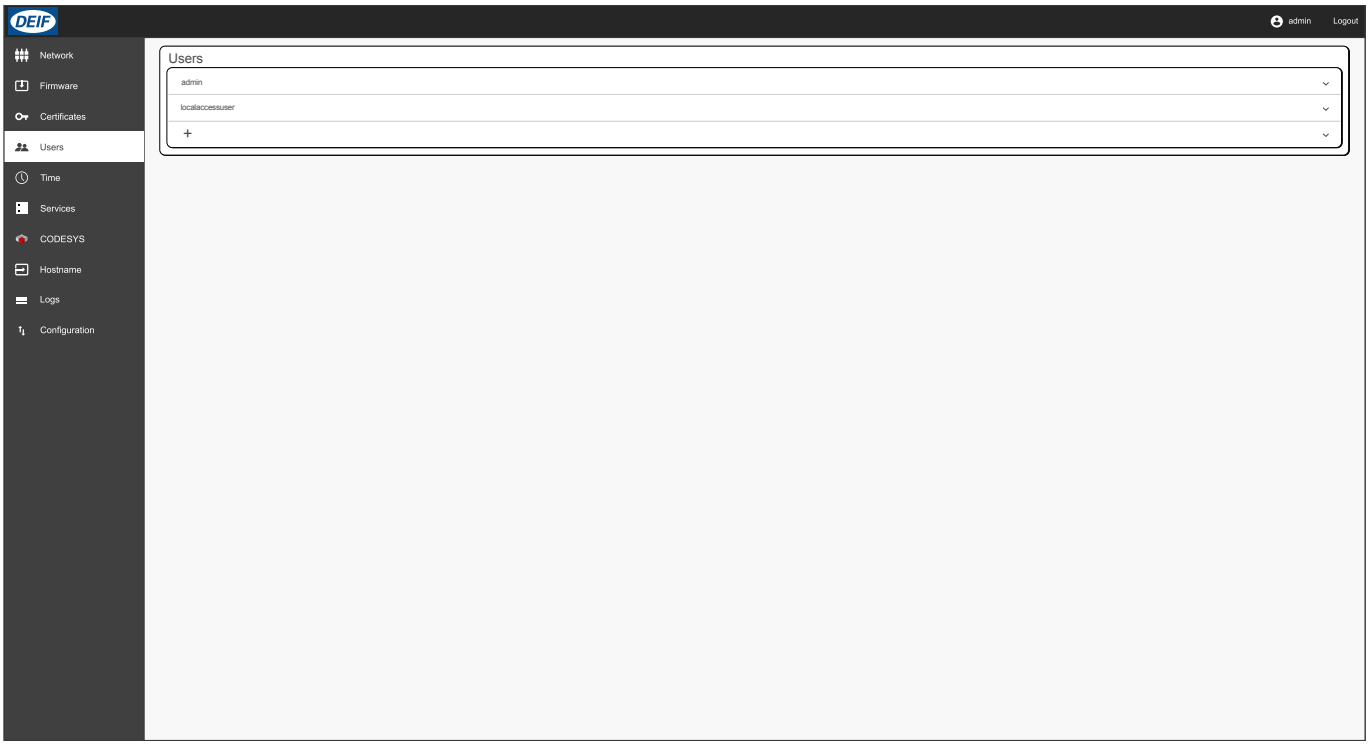
- **RAUC certificate:** Used for validation of the software update. During software upgrade the system validates that the software is signed with this Root CA. The certificate has to be in PEM format.
- **Web User Root Certificate:** Used for authenticating web users that use a client certificate, must be mapped with a user.
  - The REST API checks, if the client certificate is signed with this Root CA certificate.
  - If successful, a JSON Web Token (JWT) is generated and the mapped users permissions are added to the JWT.
  - The certificate has to be in PEM format.



3.4.4 Users

This menu gives access to add, change and delete additional users. If no password is given when a user is created, the system disables the user.

Necessary permissions: **admin user**.

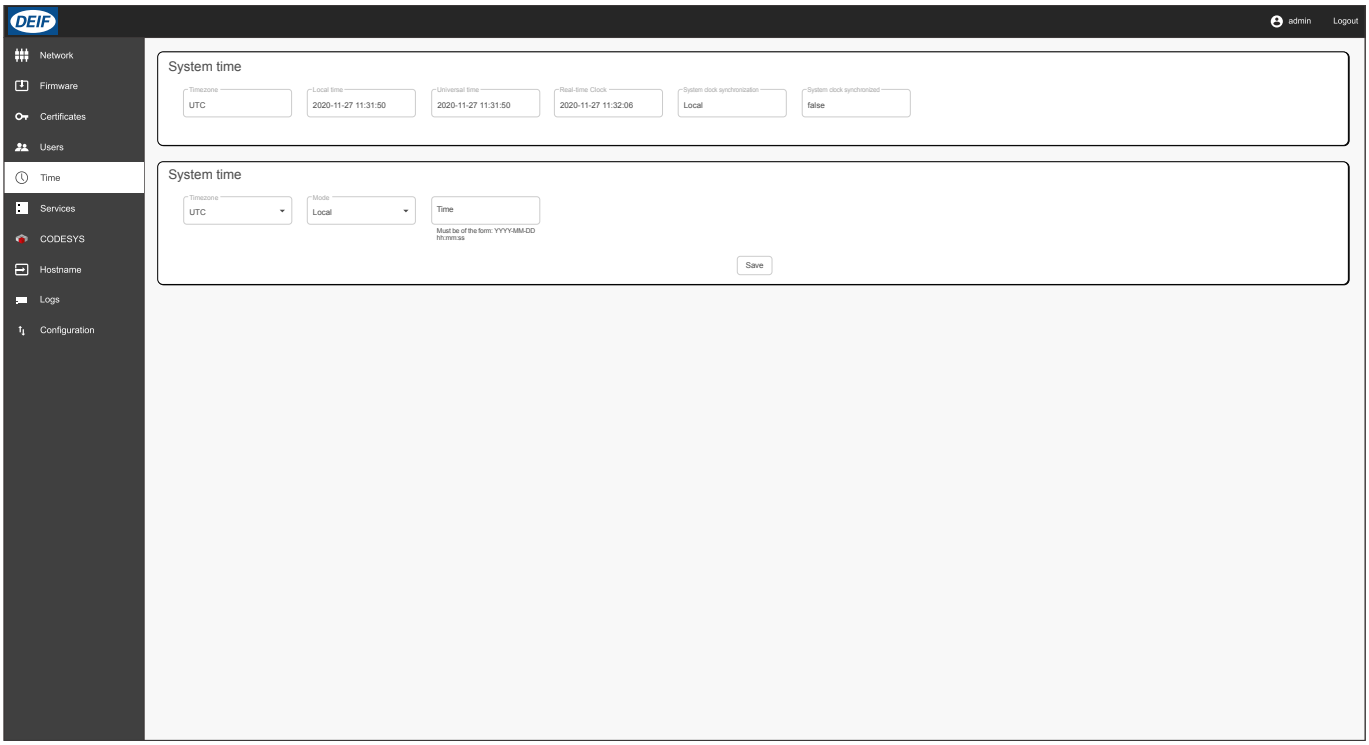


3.4.5 Time

This menu gives access to manage the time settings:

- Timezone and Mode local (no network timesync)
- Client (NTP client)
- Master (NTP Server)

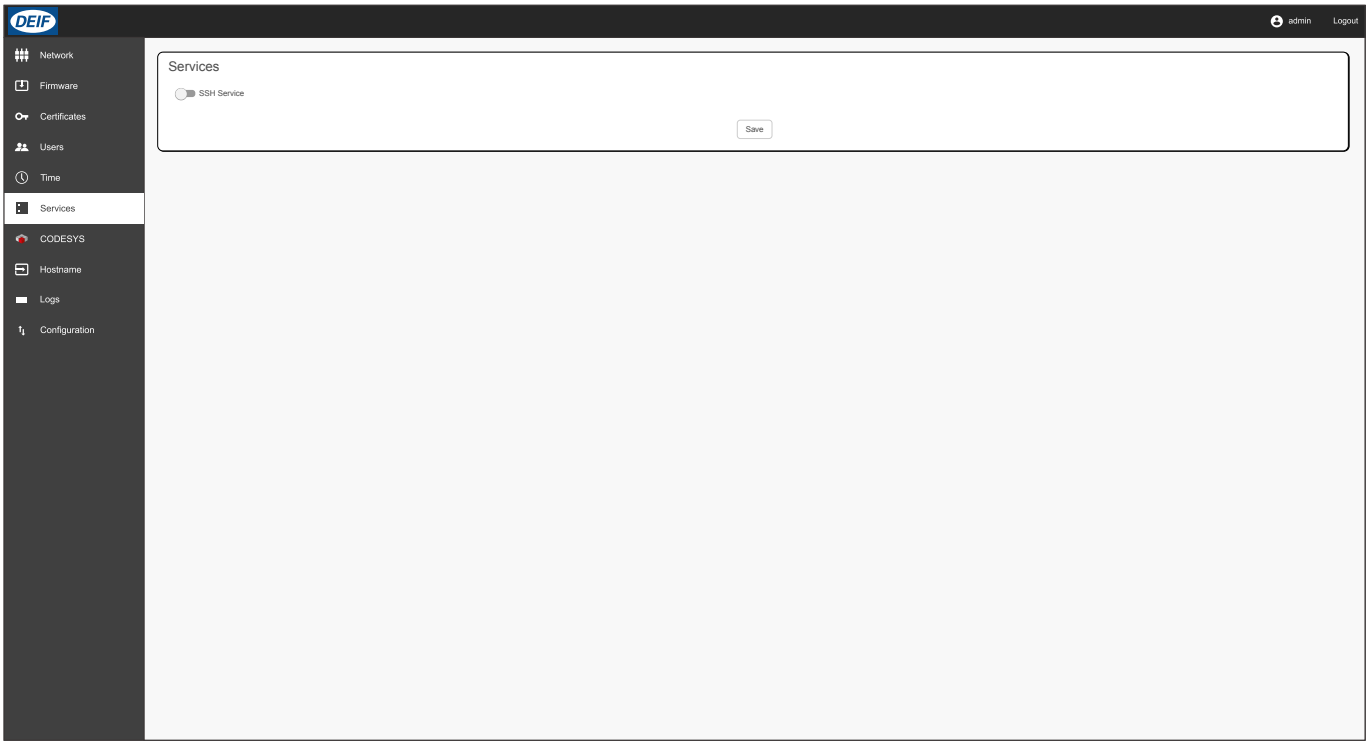
Necessary permissions: **Time setup**.



3.4.6 Services

This menu gives access to enable and disable the SSH service.

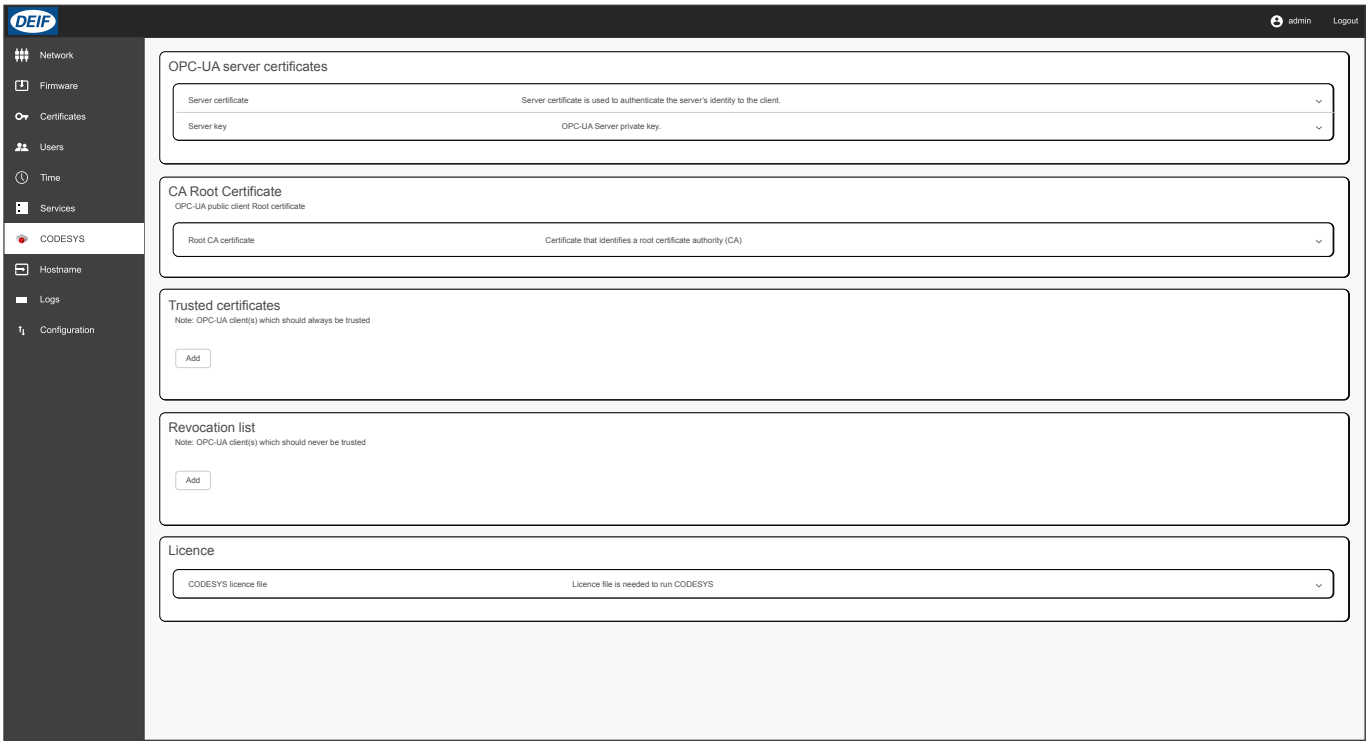
Necessary permissions: **admin user**.



3.4.7 CODESYS

This menu gives access to manage the different types of CODESYS related certificates.

Necessary permissions: **admin user**.



3.4.8 Hostname

This menu gives access to manage the hostname of the AMC 300.

Necessary permissions: **Hostname management**.

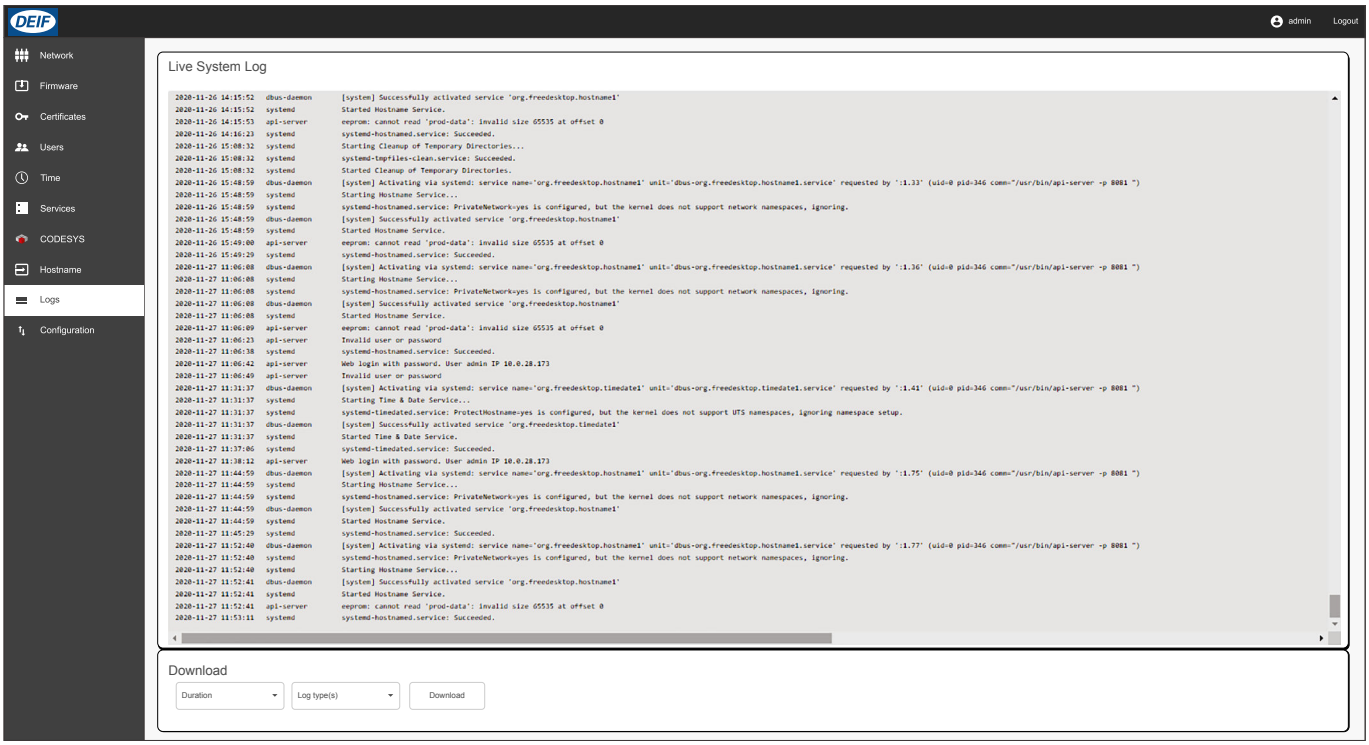
3.4.9 Logs

This menu gives access to see and download different logs:

- Log types
  - CODESYS events: Log contents controlled by the designer of the CODESYS application.
  - CODESYS data: Log contents controlled by the designer of the CODESYS application.
  - Syslog: Log of system messages with information about system events (for example, during system startup or firmware updates). Can be used to determine the health of the overall system.

- Log duration:
  - Latest (4 hours)
  - Last day
  - Last week
  - All

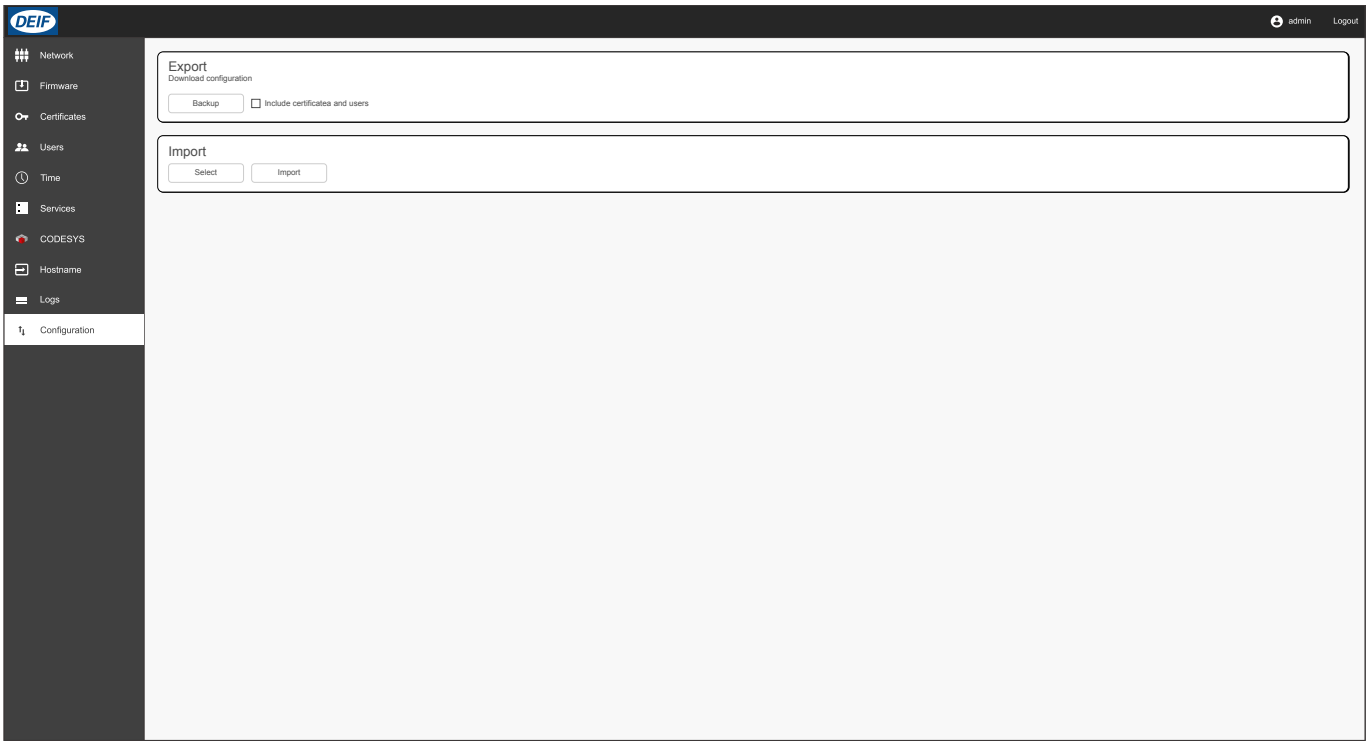
Necessary permissions: **logs**.



3.4.10 Configuration

This menu gives access to export the controller configuration to a backup file, and to import existing configuration backup files.

Necessary permissions: **admin user**.



4. Programming AMC 300

4.1 IEC61131-3 (CODESYS) programming

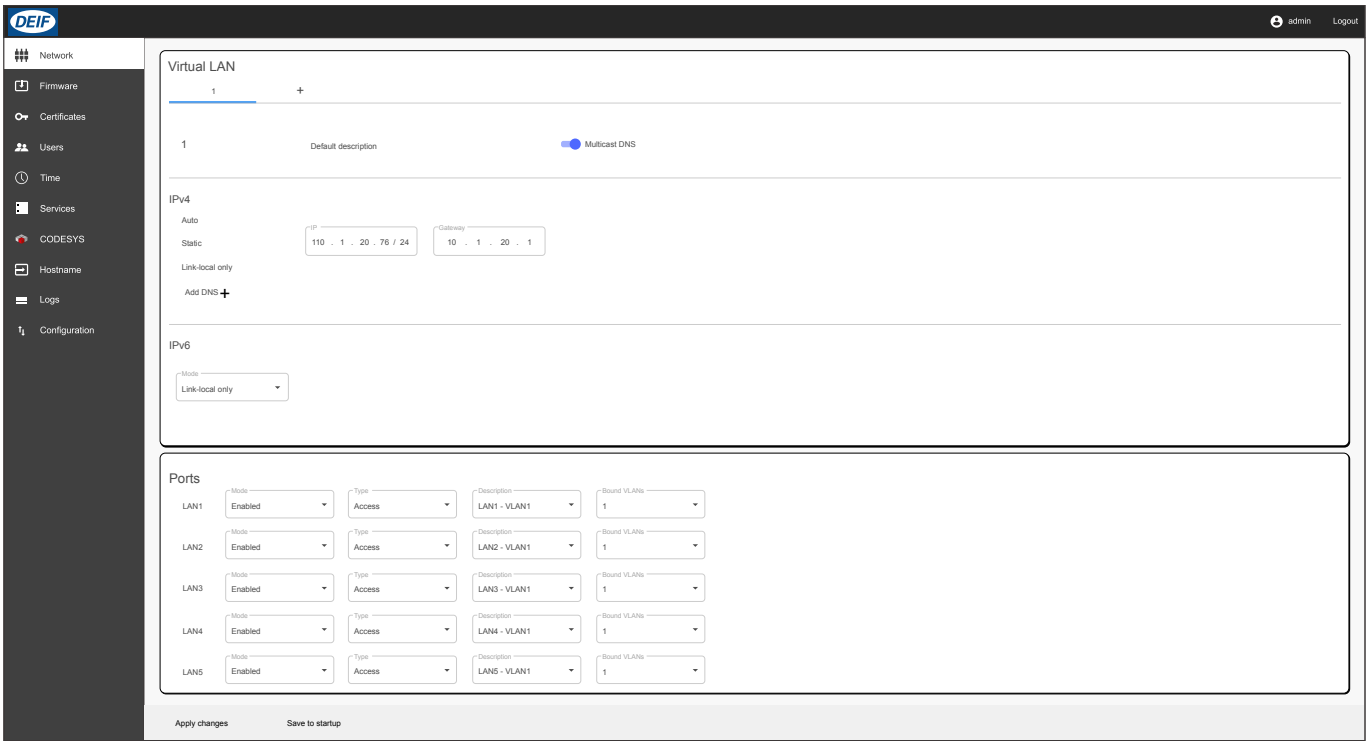
Refer to the document **AMC 300 CODESYS Development package 4186341271** for a guide on how to install the AMC 300 CODESYS Development package and the first steps to get started with it.

5. Additional configuration

5.1 Change advanced network configuration

5.1.1 Change the static IP address

1. Select **Network** in the menu.
2. Select **Static** under IPv4.



3. Fill in **IP** and **Gateway**.
4. a. Select **Apply changes** to save the new static IP address.
   b. Select **Save to Startup** to apply the new static IP address after a controller restart.

CIDR IP addresses

The AMC 300 uses CIDR (or Classless Inter-Domain Routing) as a method for allocating IP addresses and IP routing. The prefix length is the number after/in the IP address and is a different way to set a netmask.

The table shows the relationship between CIDR prefix length and typically used netmasks.

CIDR prefix length	Netmask
8	255.0.0.0
16	255.255.0.0
24	255.255.255.0

5.1.2 Change the hostname

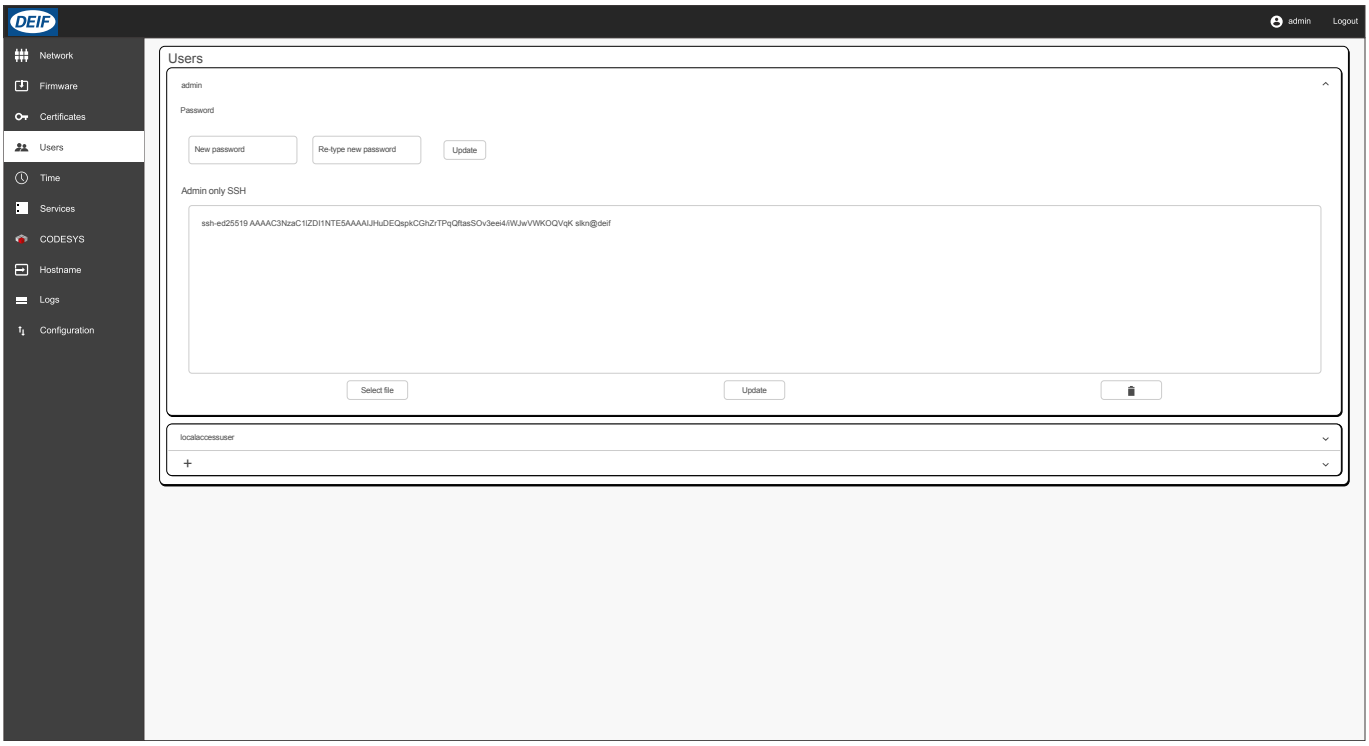
1. Select **Hostname** in the menu.

2. Write the new hostname.
3. Click **Save** to activate the new hostname.

NOTE The hostname must be unique in the network.

5.1.3 Change the user password

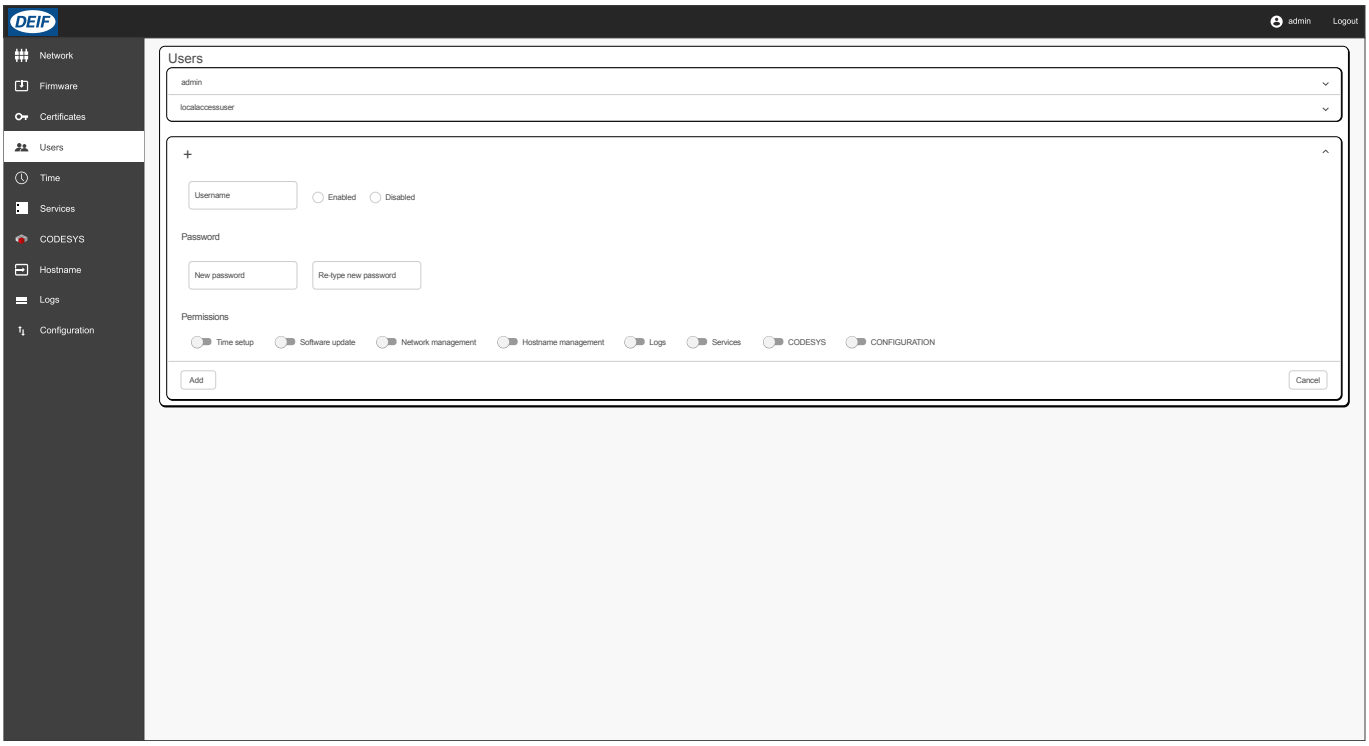
1. Select **Users** in the menu.
2. Expand the settings for the **admin** user.



3. Write the new password in the field **New password**.
4. Write the new password again in the field **Re-type new password**.
5. Select **Update** to activate the new password.

5.1.4 Add new users

1. Select **Users** in the menu.
2. Select **+**.



3. Type in the new user name in the field **Username**.
4. Type in the password in the fields **New password** and **Re-type new password**.
5. Select the permissions for the new user.
6. Select **Add** to save the new user in the system.

Localaccessuser

The localaccessuser is a pre-defined user which has access via localhost (loopback address) and can make API requests over localhost from the CLI or the CODESYS application.

This can be used to show some of the web interface functions inside the CODESYS application, for example log retrieval or time setup functionality.

Permissions for localaccessuser may be managed as for any other user.

The localaccessuser can be deleted, if it is not necessary. If deleted by accident, the local access user can be recreated with the warning that the password must be empty.

The localaccessuser is restored upon a factory reset.

5.2 Enabling SSH (Secure Shell) access

5.2.1 Enabling SSH (Secure Shell) access

SSH login is supported, but only with digital authentication keys. The SSH Service must be enabled in the menu **Services**, and one or more SSH public keys must be added to the admin user. Password authentication is not enabled.

SSH keys of the Ed25519 type are supported. This key type is chosen, because it has many advantages:

- It is fast to generate
- It is fast to verify
- It brings more security
- The keys are smaller, thus easier to transfer and copy/paste.

Key pairs can be generated with OpenSSH on Windows or Linux operating systems.

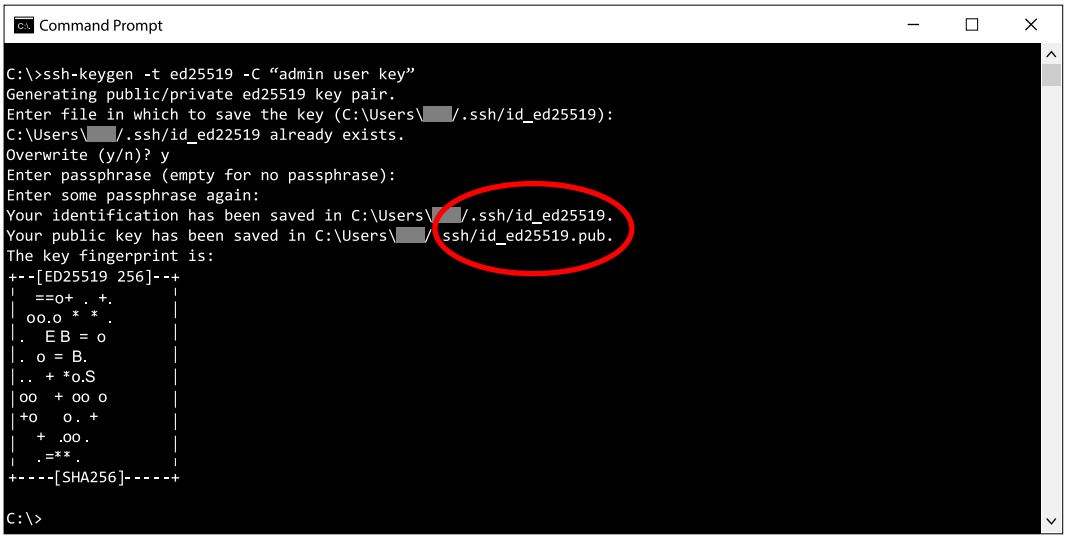
The following describes how to generate the key in Windows, but the method applies for Linux also.

Windows 10 supports Open SSH with SSH Client with “ssh” and key generation with “ssh-keygen” possible via the Windows command line. If this is not enabled, update the Windows version or use the PuTTY method, see the section **Generate Ed25519 authentication key pair using PuTTY**.

5.2.2 Generate an OpenSSH Ed25519 authentication key pair from the Windows command line

Type: ssh-keygen -t ed25519 -C "admin user key"

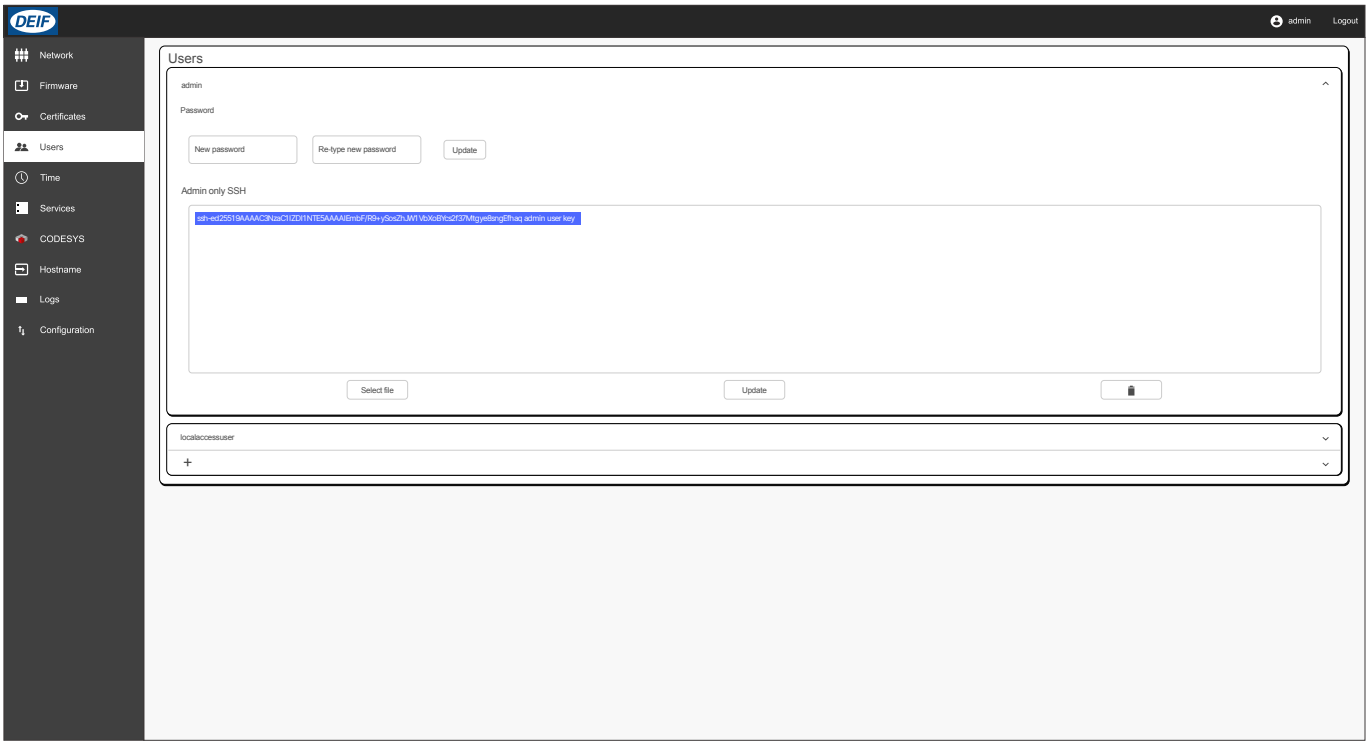
The string after -C is a comment used to identify the admin user and follows the Public key. It could also be the email of the admin user.



- The generated private key is in **C:\Users\[Username]\.ssh\id_ed25519**
- The public key is in **C:\Users\[Username]\.ssh\id_ed25519.pub**

5.2.3 Add an SSH user key to the admin user

1. Select **Users** in the menu.
2. Expand the settings for the **admin** user.
3. Upload or copy-paste the public key id_ed25519.pub in the field **Admin only SSH**.*



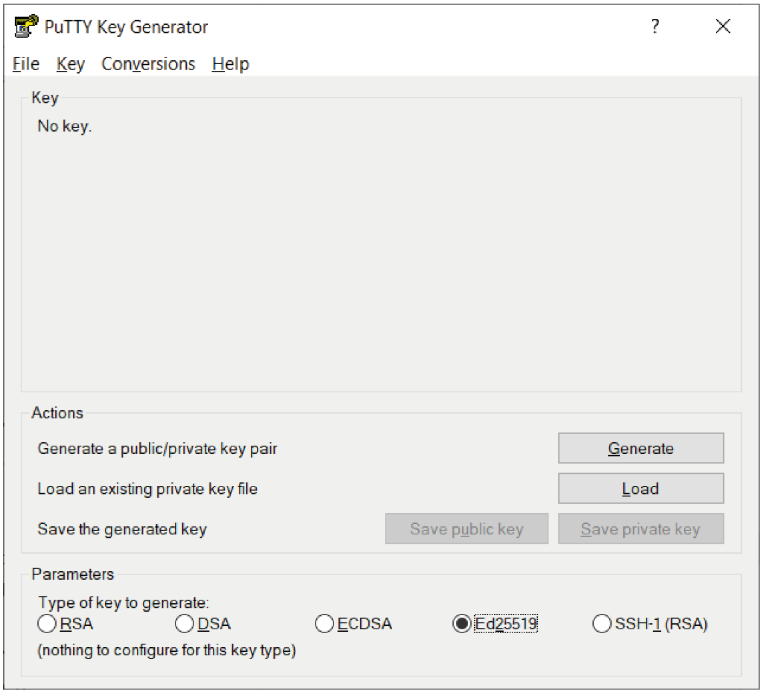
4. Use the OpenSSH client ssh [username]@[hostname], for example, ssh admin@amc300.local to access the controller.

NOTE * Uploading a key replaces all text in the field **Admin only SSH**. To add multiple keys, you must copy-paste each key individually.

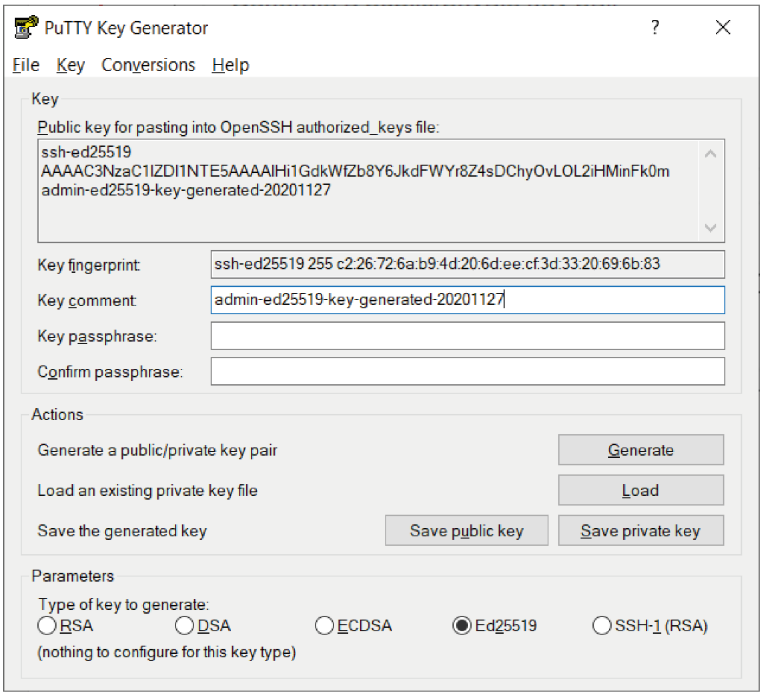
5.2.4 Generate an Ed25519 authentication key pair with PuTTY

An alternative method to demonstrate generating a key pair, is via the Key Generator that comes with PuTTY, called PuTTYgen. PuTTY can create an OpenSSH format Public Key and a PuTTY Private key.

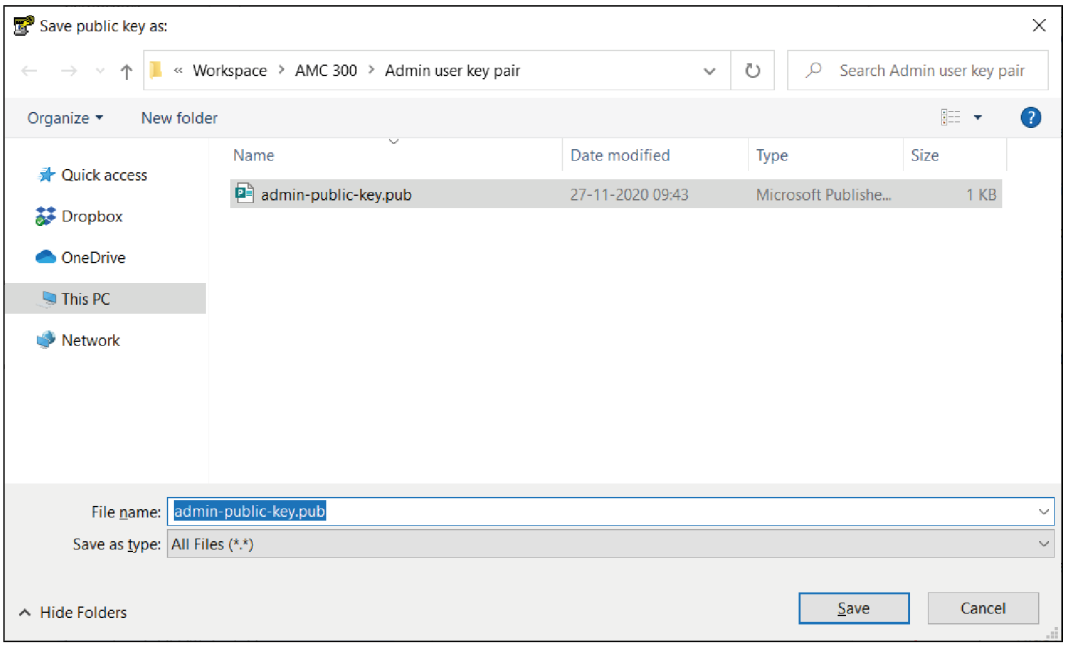
1. Specify the **Type of key to generate** to Ed25519.



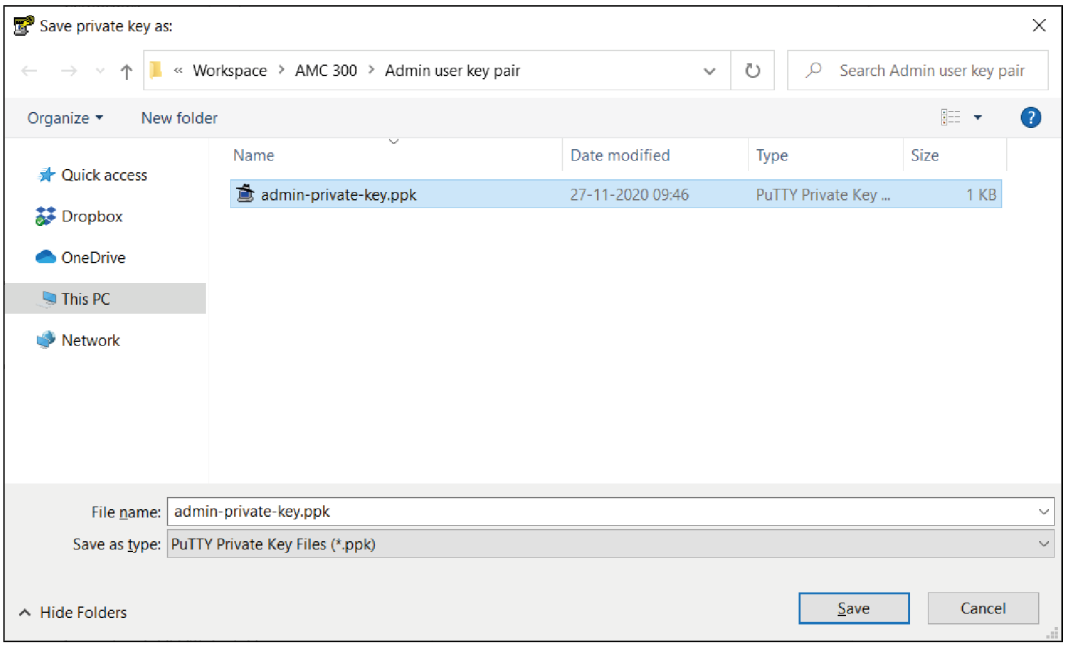
2. Select **Generate**.
3. Follow the instructions on the screen.



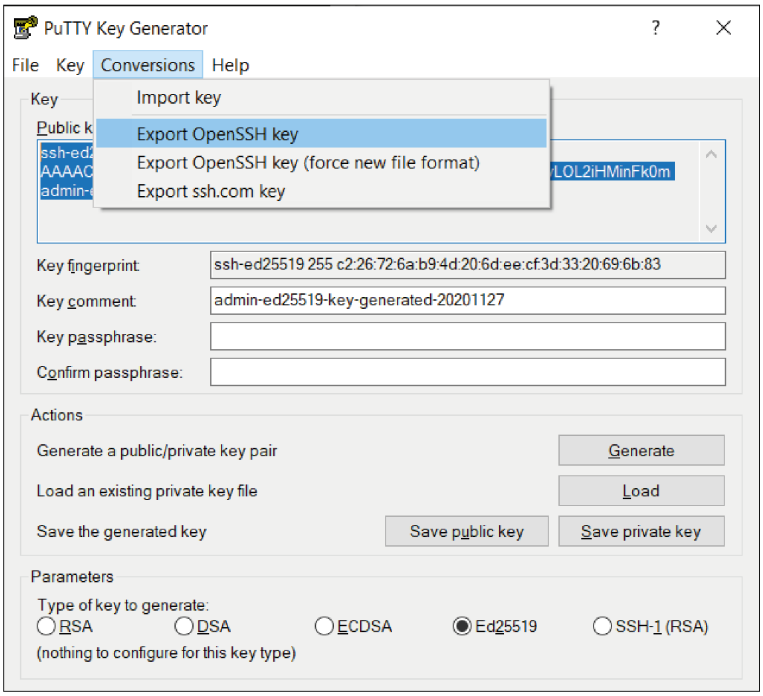
4. Save the generated public key with **Save public key**.

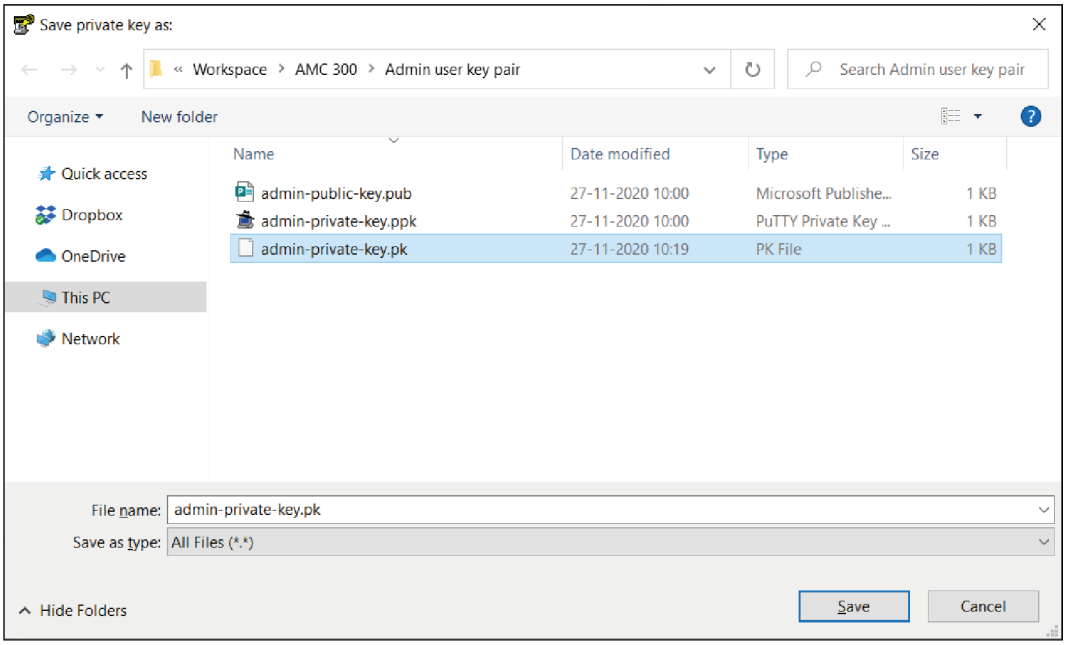


5. Save the generated private key with **Save private key**.



5.2.5 Export an OpenSSH private key

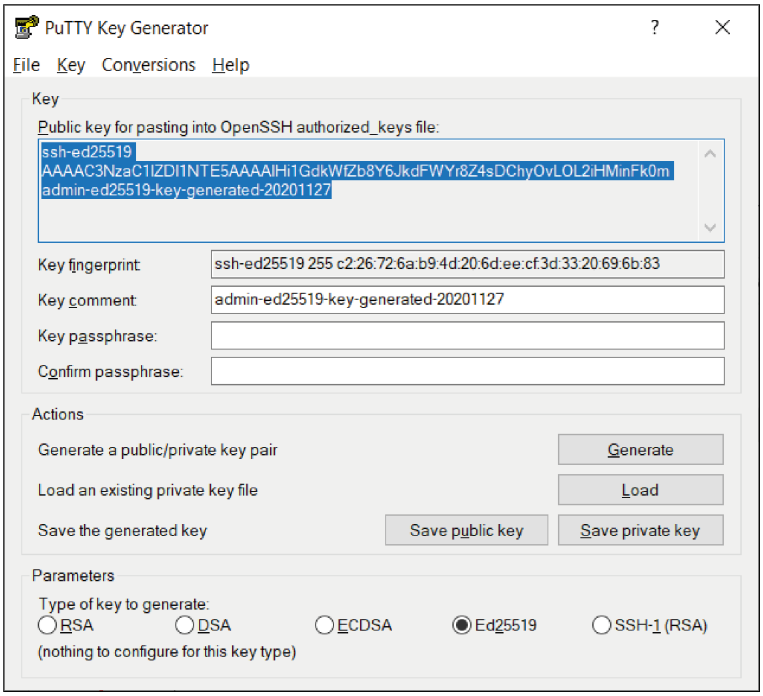




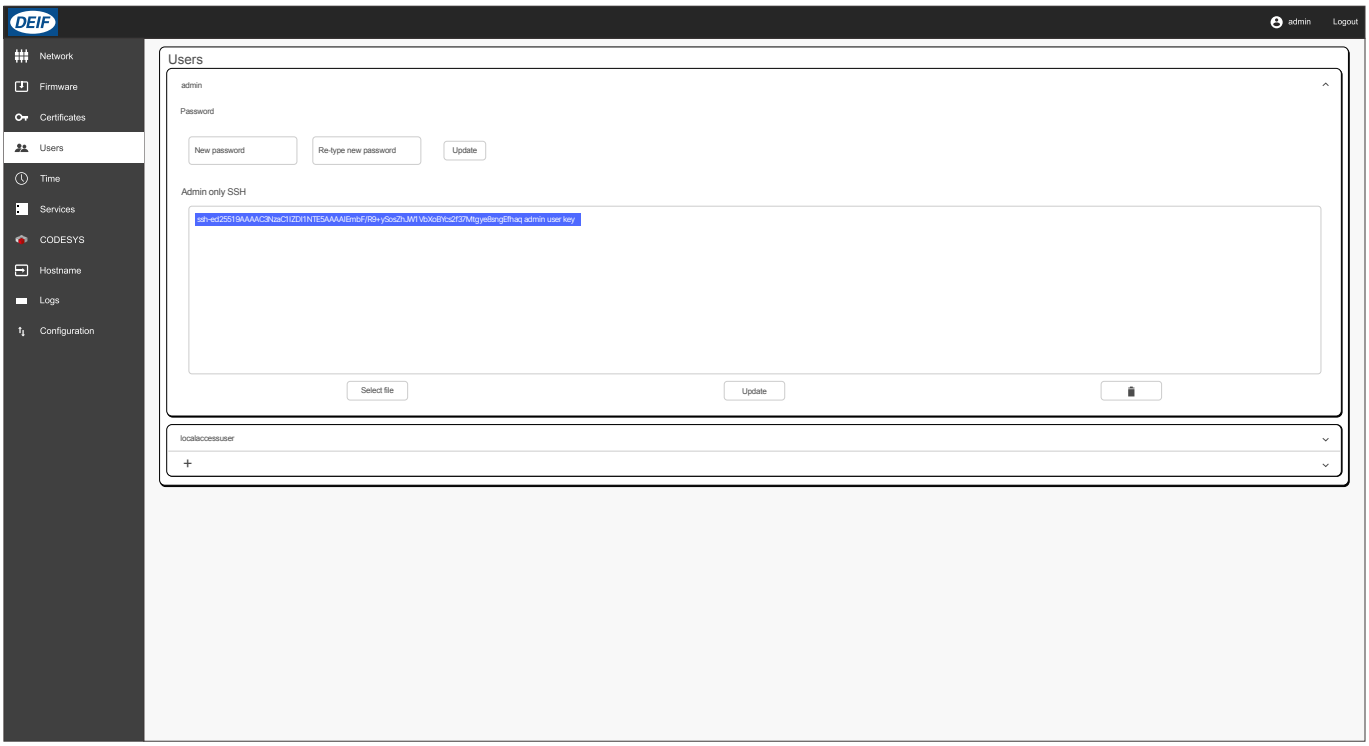
5.3 Adding user keys for SSH (Secure Shell) access

5.3.1 Adding user keys for SSH (Secure Shell) access

1. Mark and copy the generated Public key (OpenSSH format).



2. Select Users in the menu.
3. Expand the **admin** user.
4. Paste the public key into the field **Admin only SSH** (a text line for each key).

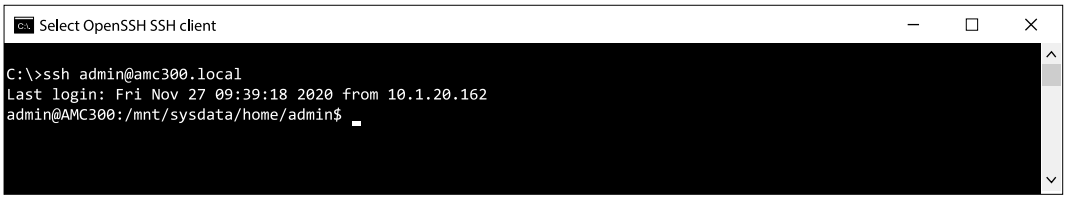


5. Select **Update**.

5.3.2 Using a PuTTY generated key with Windows for SSH (Secure Shell) access

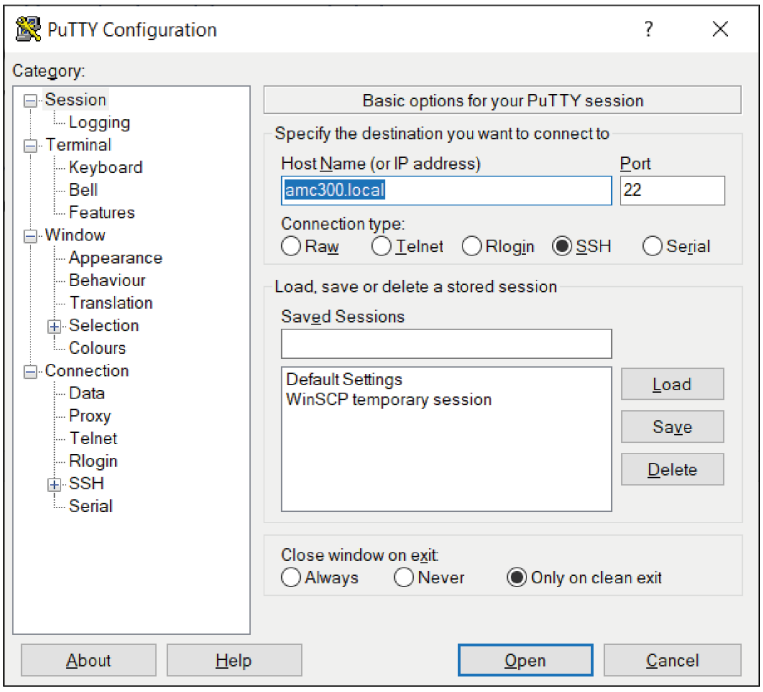
Copy the OpenSSH generated private key to **C:\Users\[Username]\.ssh** and rename it to **id_ed25519**.

You can then access the Secure shell of AMC 300 via ssh [username]@[hostname], for example ssh admin@amc300.local

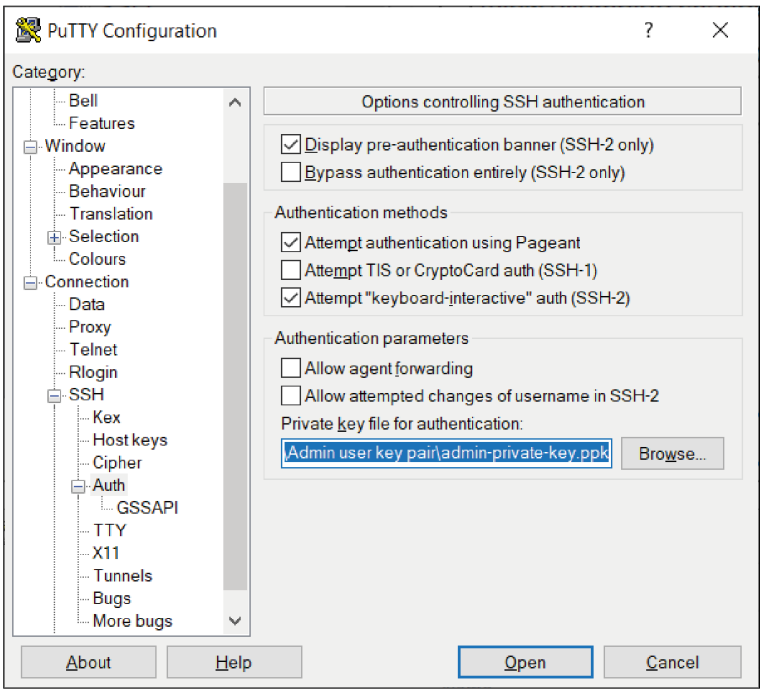


5.3.3 Using PuTTY for SSH access

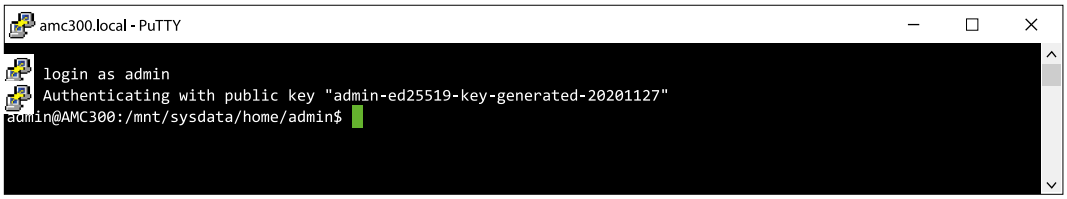
1. Open PuTTY and apply amc300.local as host name.



2. Add the private key in **Auth** and select **Open**:

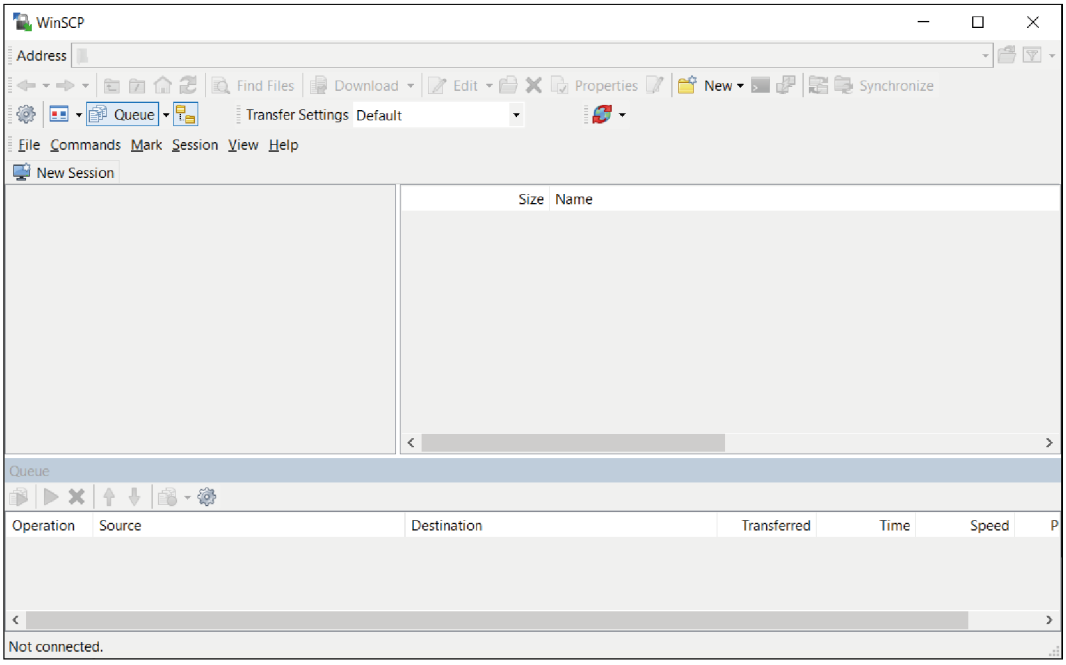


3. Log in with **admin**.

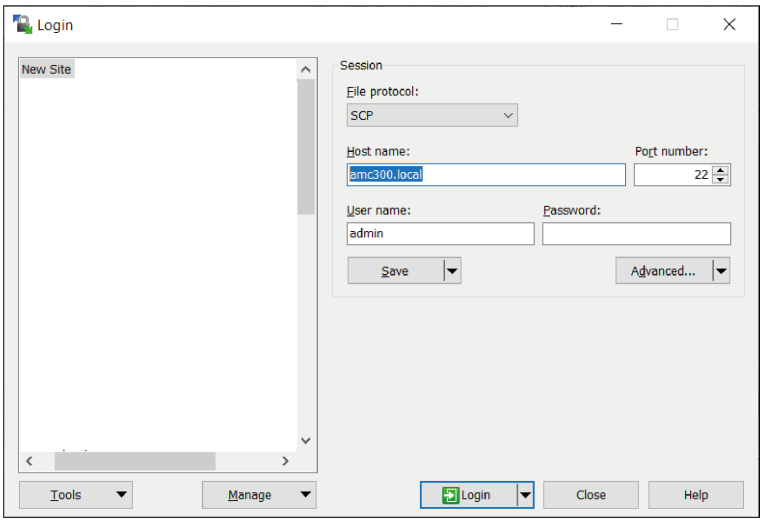


5.3.4 Access via WinSCP

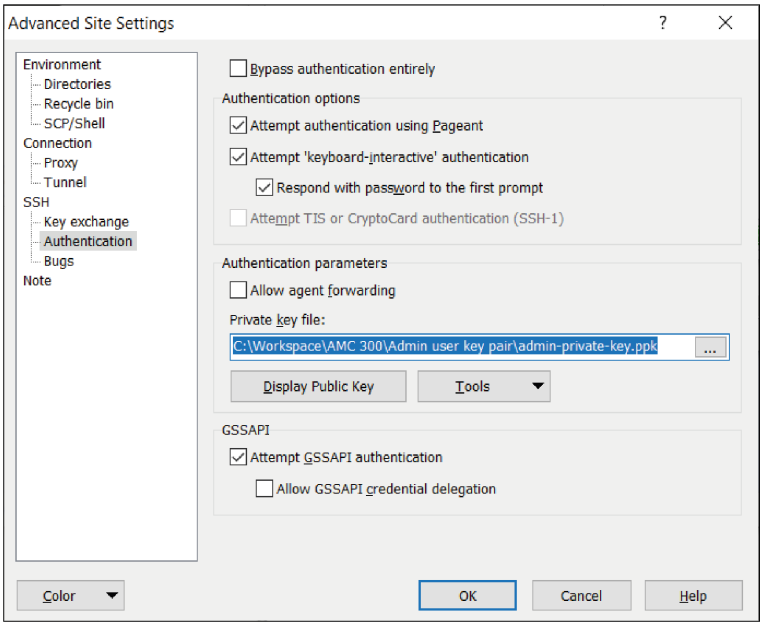
1. Open WinSCP and click new Session:



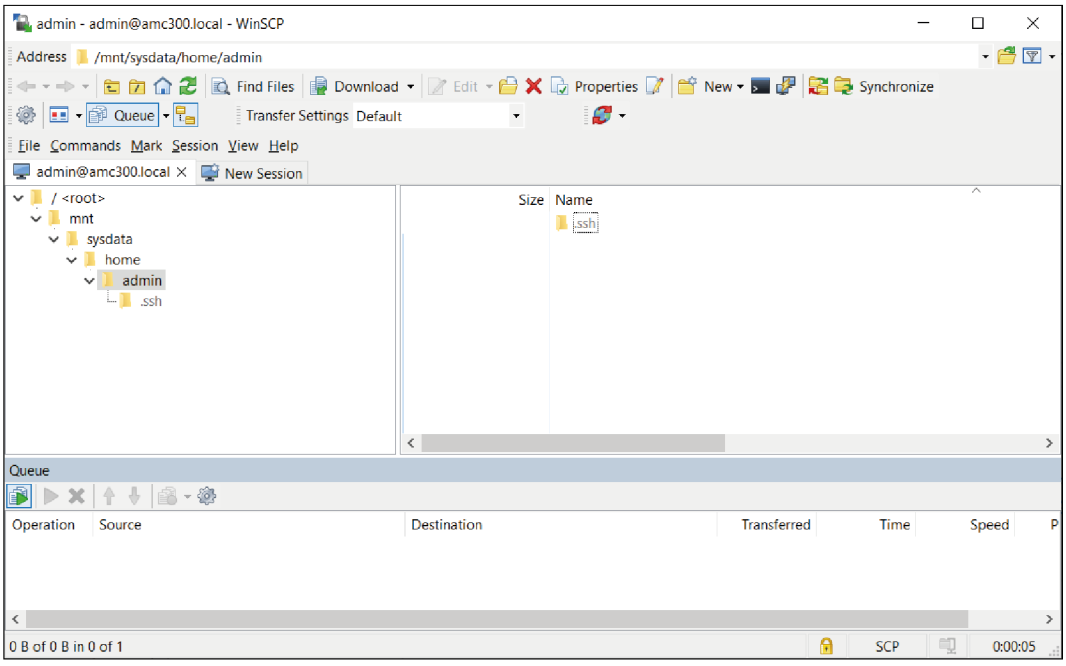
2. Specify File protocol, host name and user name. Because WinSCP and PuTTy share Private key file location, you can continue pressing Login:



3. Go to Advanced and specify the Private key generated:



4. Select Login. You are now connected to the filesystem of the ACM 300:

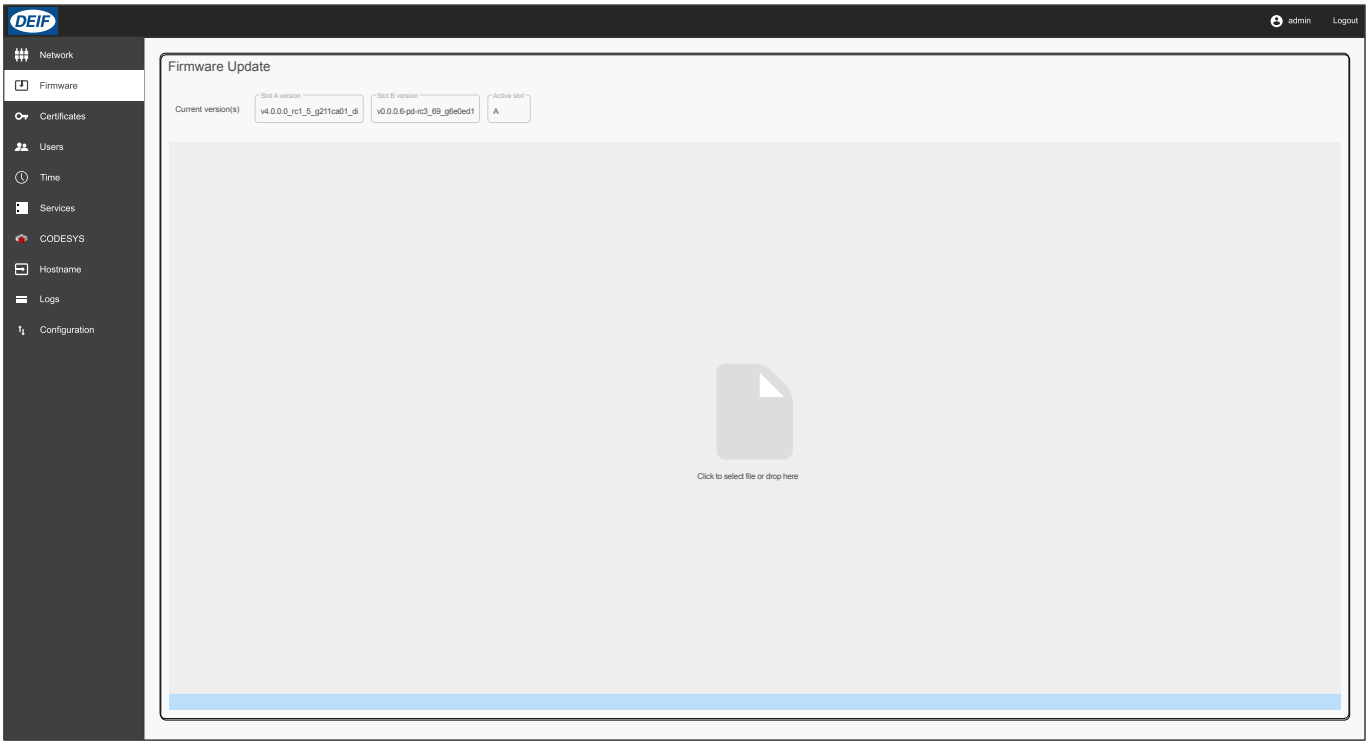


5.4 Set local date and time

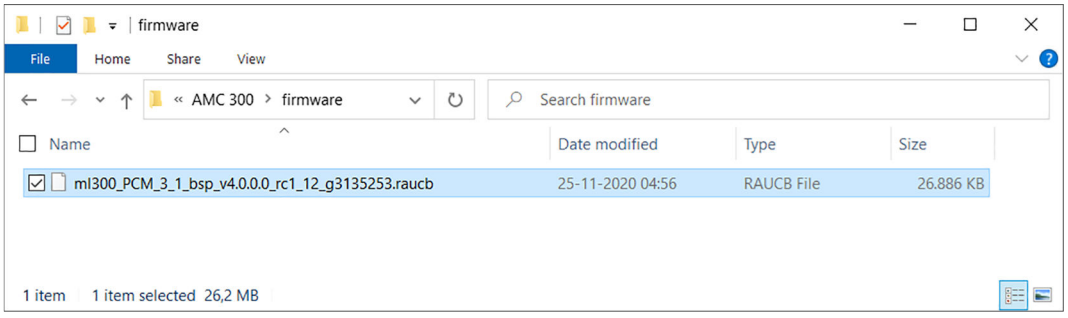
As default, the AMC 300 comes with UTC time. The time in the unit can be set via the System page or via NTP (Network time protocol).

5.5 Update firmware

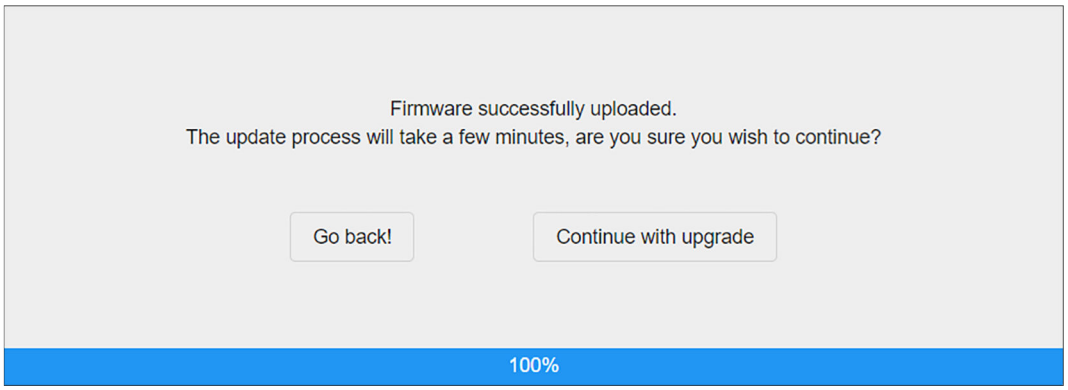
1. Log in to AMC 300
2. Select **Firmware** in the menu



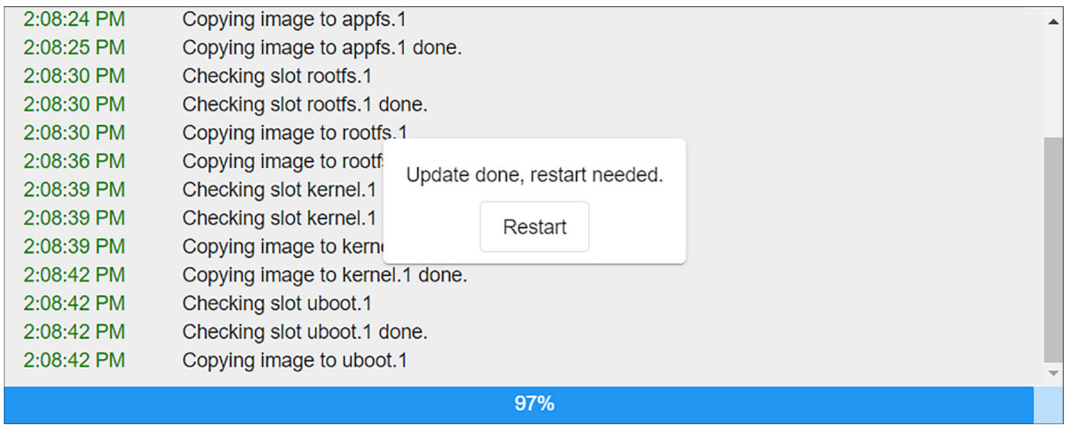
3. Select **Click to select file or drop here**
   - Drag-and-drop a firmware file, or
   - Navigate to the firmware file and select it



4. When the firmware is uploaded, you will be prompted to continue the update



5. Select **Continue with upgrade**
6. When the update is done, you will be prompted to restart the system



7. Select **Restart**.
8. When the system is restarted, you must log in again.

5.6 Create a factory reset

WARNING
Factory reset will restore AMC 300 to its factory settings. Make sure to back up important information before you do the reset.

A factory reset can be performed via REST API (if you have admin access to the controller).

Factory reset via REST API

From CLI:

HOST=https://acm300.local

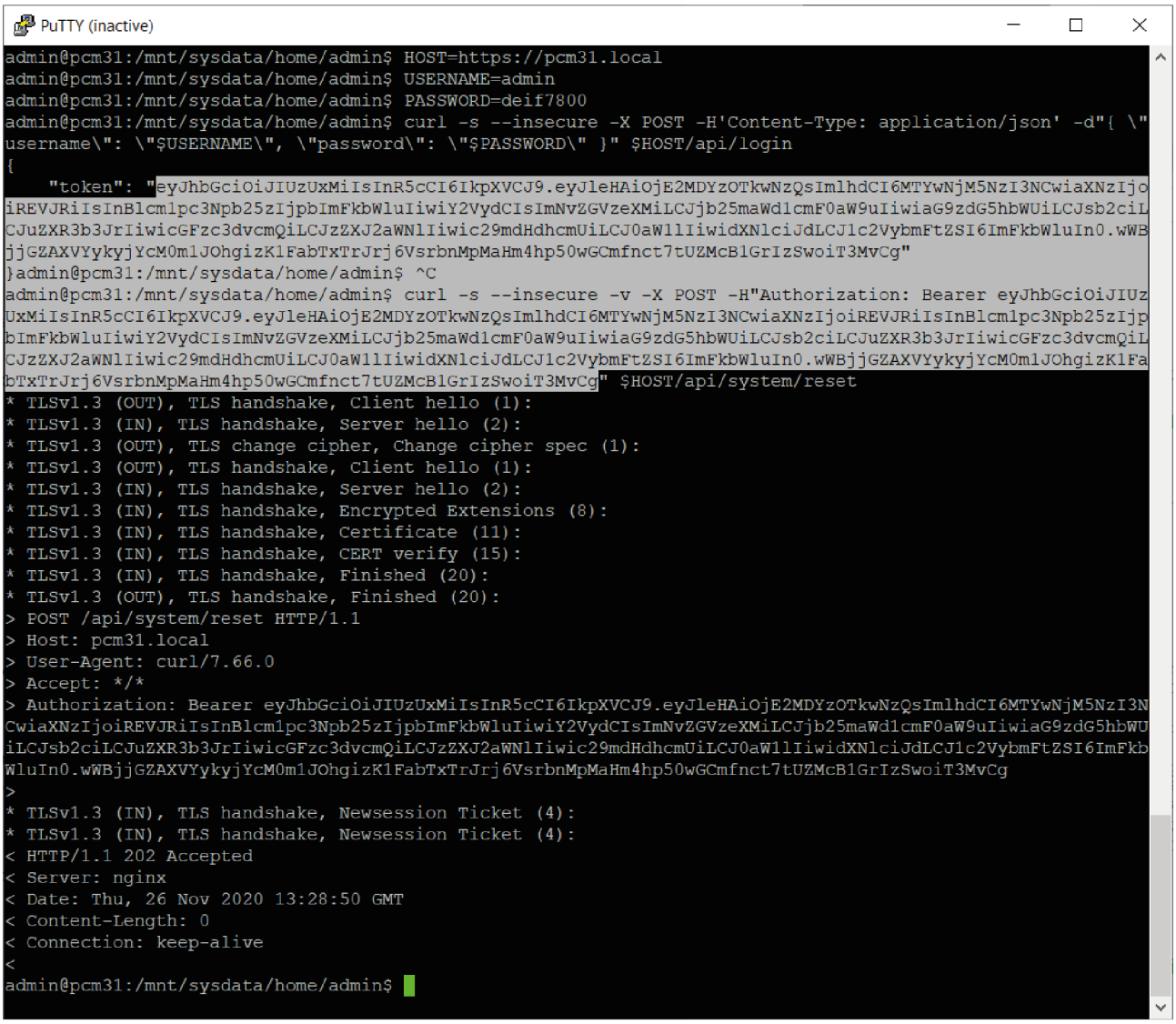
USERNAME=admin

PASSWORD=admin

curl -s --insecure -X POST -H'Content-Type: application/json' -d"{ \"username\": \"$USERNAME\", \"password\": \"$PASSWORD\" }" $HOST/api/login

Insert the string for the token instead of $token.

```
curl -s --insecure -v -X POST -H"Authorization: Bearer TOKEN" $HOST/api/system/reset
```


PuTTY (inactive)
admin@pcm31:/mnt/sysdata/home/admin$ HOST=https://pcm31.local
admin@pcm31:/mnt/sysdata/home/admin$ USERNAME=admin
admin@pcm31:/mnt/sysdata/home/admin$ PASSWORD=deif7800
admin@pcm31:/mnt/sysdata/home/admin$ curl -s --insecure -X POST -H'Content-Type: application/json' -d"{ \"username\": \"$USERNAME\", \"password\": \"$PASSWORD\" }" $HOST/api/login
{
"token": "eyJhbGciOiJIUzUxMiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE2MDYzOTkwNzQsImlhdCI6MTYwNjM5NzI3NCwiaXNzIjoiREVJRiIsInBlcm1pc3Npb25zIjpbImFkbWluIiwiY2VydCIsImNvZGVzeXMiLCJjb25maWd1cmF0aW9uIiwiaG9zdG5hbWUiLCJsb2ciLCJuZXR3b3JrIiwicGFzc3dvcmQiLCJzZXJ2aWNlIiwic29mdHdhcmUiLCJ0aWllIiwidXNlciJdLCJ1c2VybmFtZSI6ImFkbWluIn0.wWBjjGZAXVYykyjYcM0m1JOhgizK1FabTxTrJrj6VsrbnMpMaHm4hp50wGCmfnct7tUZMcB1GrIzSwoiT3MvCg"
}admin@pcm31:/mnt/sysdata/home/admin$ ^C
admin@pcm31:/mnt/sysdata/home/admin$ curl -s --insecure -v -X POST -H"Authorization: Bearer eyJhbGciOiJIUzUxMiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE2MDYzOTkwNzQsImlhdCI6MTYwNjM5NzI3NCwiaXNzIjoiREVJRiIsInBlcm1pc3Npb25zIjpbImFkbWluIiwiY2VydCIsImNvZGVzeXMiLCJjb25maWd1cmF0aW9uIiwiaG9zdG5hbWUiLCJsb2ciLCJuZXR3b3JrIiwicGFzc3dvcmQiLCJzZXJ2aWNlIiwic29mdHdhcmUiLCJ0aWllIiwidXNlciJdLCJ1c2VybmFtZSI6ImFkbWluIn0.wWBjjGZAXVYykyjYcM0m1JOhgizK1FabTxTrJrj6VsrbnMpMaHm4hp50wGCmfnct7tUZMcB1GrIzSwoiT3MvCg" $HOST/api/system/reset
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
* TLSv1.3 (IN), TLS handshake, Server hello (2):
* TLSv1.3 (OUT), TLS change cipher, Change cipher spec (1):
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
* TLSv1.3 (IN), TLS handshake, Server hello (2):
* TLSv1.3 (IN), TLS handshake, Encrypted Extensions (8):
* TLSv1.3 (IN), TLS handshake, Certificate (11):
* TLSv1.3 (IN), TLS handshake, CERT verify (15):
* TLSv1.3 (IN), TLS handshake, Finished (20):
* TLSv1.3 (OUT), TLS handshake, Finished (20):
> POST /api/system/reset HTTP/1.1
> Host: pcm31.local
> User-Agent: curl/7.66.0
> Accept: */*
> Authorization: Bearer eyJhbGciOiJIUzUxMiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE2MDYzOTkwNzQsImlhdCI6MTYwNjM5NzI3NCwiaXNzIjoiREVJRiIsInBlcm1pc3Npb25zIjpbImFkbWluIiwiY2VydCIsImNvZGVzeXMiLCJjb25maWd1cmF0aW9uIiwiaG9zdG5hbWUiLCJsb2ciLCJuZXR3b3JrIiwicGFzc3dvcmQiLCJzZXJ2aWNlIiwic29mdHdhcmUiLCJ0aWllIiwidXNlciJdLCJ1c2VybmFtZSI6ImFkbWluIn0.wWBjjGZAXVYykyjYcM0m1JOhgizK1FabTxTrJrj6VsrbnMpMaHm4hp50wGCmfnct7tUZMcB1GrIzSwoiT3MvCg
>
* TLSv1.3 (IN), TLS handshake, Newsession Ticket (4):
* TLSv1.3 (IN), TLS handshake, Newsession Ticket (4):
< HTTP/1.1 202 Accepted
< Server: nginx
< Date: Thu, 26 Nov 2020 13:28:50 GMT
< Content-Length: 0
< Connection: keep-alive
<
admin@pcm31:/mnt/sysdata/home/admin$