

Programmable Automation Controller

User's manual



1. Revision

1.1 Revision history	4
2. About the User manual	
2.1 Intended users of the User manual	5
2.2 Software versions	
2.3 Technical support	5
2.4 Warnings and safety	5
2.4.1 Safety during installation and operation	5
2.4.2 Electrostatic discharge	6
2.4.3 Factory settings	
2.4.4 Data security	6
2.4.5 Do not use unsupported hardware modules	6

3. Configure AMC 300

3.1 Software	7
3.1.1 Download AMC 300 software	7
3.1.2 System requirements	7
3.1.3 PC tools	7
3.2 Connection	8
3.2.1 Power connection	
3.2.2 Programming connection	
3.2.3 Default user and password	
3.2.4 Test the connection	
3.2.5 Find network devices	
3.3 The system web page	
3.3.1 Access to the System web page	
3.3.2 Overview of the System web page	
3.4 Menus	
3.4.1 Network	
3.4.2 Firmware	
3.4.3 Certificates	
3.4.4 Users	
3.4.5 Time	
3.4.6 Services	
3.4.7 CODESYS	
3.4.8 Hostname	19
3.4.9 Logs	
3.4.10 Configuration	

4. Programming AMC 300

4.1 IEC61131-3 (CODESYS) programming	
5. Additional configuration	
5.1 Change advanced network configuration	
5.1.1 Change the static IP address	
5.1.2 Change the hostname	
5.1.3 Change the user password	
514 Add new users	26

5.1.4 Add new user	S	
5.2 Enabling SSH (Se	cure Shell) access	
5.2.1 Enabling SSH	(Secure Shell) access	27

5.2.2 Generate an OpenSSH Ed25519 authentication key pair from the Windows command line	27
5.2.3 Add an SSH user key to the admin user	
5.2.4 Generate an Ed25519 authentication key pair with PuTTY	29
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	32
5.3.2 Using a PuTTY generated key with Windows for SSH (Secure Shell) access	
5.3.3 Using PuTTY for SSH access	
5.3.4 Access via WinSCP	
5.4 Set local date and time	
5.5 Update firmware	
5.6 Create a factory reset	

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 2.1Software 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.





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

Select Command Prompt	_	×
C:\>		
Pinging amc300.local [fe80::226:77ff:fe02:bc98%4] with 32 bytes of data: Reply from fe80::226:77ff:fe02:bc98%4: time=1ms Reply from fe80::226:77ff:fe02:bc98%4: time=1ms Reply from fe80::226:77ff:fe02:bc98%4: time=2ms Reply from fe80::226:77ff:fe02:bc98%4: time=1ms		
<pre>Ping statistics for fe80::226:77ff:fe02:bc98%4: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 1ms, Maximum = 2ms, Average = 1ms</pre>		
C:\>_		\sim

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

Select Command Prompt - dns-sd -B _http_tcp local		-	□ ×	
				^
C:\>dns-sd -B _httptcp local				
Browsing for _httptcp.local				
Timestamp A/R Flags if Domain	Service Type	Instance Name		
15:37:10.787 Add 2 4 local.	_httptcp.	Phaser 7100N (13:ca:72)		
15:37:10.876 Add 2 4 local.	_httptcp.	amc300		
15:37:10.933 Add 2 4 local.	_httptcp.	deif-ml300-10-1-20-77-02bcb8		
15:37:10.969 Add 2 4 local.	_httptcp.	deif-ml300-025a48		
15:37:10.978 Add 2 4 local.	_httptcp.	deif-ml300-016740		
15:37:10.981 Add 2 4 local.	_httptcp.	deif-ml300-01981c		
				v

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.

DEF		Login
	System Overview Firmware Storage Hostname Firmware Storage	
	IO Module Slots	
	$ \begin{bmatrix} 1.4 \\ PSM 3.2 \\ 20.1.1 \\ ggg \\ ggg$	
	1:11 PSM 3.2 2:12 ACM 3.1 5:15 ACM 3.1 C:17 ACM 3.1 20.1.1 5:0.30 5:0.30 5:0.30 5:0.30 5:0.30 5:0.30 5:0.30 6:16 ACM 3.1 5:0.30	
	118 PSM 3.2 2.19 ACM_3_1 4.21 20.1.1 50.3.0 50.3.0 4.21 50.3.0	
	Virtual LANs 1.1anx.1 IPv4 IP-192.188.15.31/24 IP-192.188.05.31/24 IP-192.088.05.088.05.31/24 IP-192.07.07.0	
	Interfaces / Ports LAN1 LAN2 LAN3 LAN4 LAN5 State: enable State: enable State: enable VLANs: 1 VLANs: 1 VLANs: 1 VLANs: 1 VLANs: 1 Type: access Type: access Type: access Type: access	

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

Login	
Password	
Cancel	Login

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.

DEIF		🔒 admin Logout
Network	Virtual I AN	
Firmware		
O- Certificates		
Sta Users	1 Default description	
• • • • • • • • • • • • • • • • • • •	IPv4	
. Services		
CODESYS	Link-sodi ony •	
Hostname	Pv6	
Logs		
t ₁ Configuration	Link-local only *	
	Ports characterized constraints characterized to the characterized to th	
	LANI Enabled * Access * LANI-VLANI * 1 *	
	LANZ TOTAL TOTAL CONTRACT CONT	
	LNG Enabled * Access * UNG-VLAN1 * 1 *	
	LANA Fanahier V Georgian Baury LANa Georgian Baury LANa Company	
	LANS Enabled Access LANS-VLAN1	
	Apply changes Save to startup	

3.4.2 Firmware

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

Necessary permissions: Firmware update.

DEIF	e admin Logaut
+++ Network	Firmware Update
Firmware	Current version(s) Str.A version
Or Certificates	
Users	
Services	
CODESYS	
🚍 Hostname	
Logs	
t ₁ Configuration	
	Gik to asket file or deep here

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.

		😫 admin Logou
Network	RAUC Certificate	
Firmware		
O- Certificates		
21 Users		
() Time		
Services		
CODESYS		
- Hostname	Seted file Save	
💻 Logs		
I ₁ Configuration	Web User Root Certificate Web User Select file Select file Select file	

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.

DEIF	🔂 admin Logov	a
tit Network	Users	
Firmware	admin v	
O- Certificates	localaccesuser	
Ja Users	\	
() Time		
Services		
CODESYS		
Hostname		
Logs		
t ₁ Configuration		

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.

DEIF	e admin	Logout
### Network	System time	
Firmware	* Timesone - Local fine - Ubiversal fine - Filed - fine Clock - Splatn dok synchronization - Splatn dok synchronization 1 trg - 2000 41 07 41/0.5 E0 - 2000 41 07 41/0.5 E0	
Or Certificates		
22. Users		2
() Time	System time	
Services	UTC Local Local Local Marte of the time YYYYAMADD	
CODESYS	hhunnas	
Hostname	ane	
Logs		
1 Comiguration		

3.4.6 Services

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

Necessary permissions: admin user.

DEIF	🔁 admin Logout
tt Network	Sanviras
Firmware	De Moda De Ssi Service
O- Certificates	
👥 Users	Sare
() Time	
Services	
CODESYS	
Hostname	
Logs	
t ₄ Configuration	

3.4.7 CODESYS

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

Necessary permissions: admin user.

DEP	😝 admin Lopour
Network	OPC-UA server certificates
E Firmware	Server certificate Server certificate is used to authenticate the server's identity to the client. 🗸
O- Certificates	Server key OPC-UA Server private key.
Time	
Services	CA Root Certificate PPC-UA public elient Root certificate
CODESYS	Root CA certificate that identifies a root certificate authority (CA)
Hostname	
Logs	Trusted certificates Note: OPC Und ciently which should always be trusted
t ₁ Configuration	
	Revocation list Note: CPC-UA-clerit(s) which should never be trusted Add
	Licence
	CODESYS licence file Licence file is needed to run CODESYS 🗸

3.4.8 Hostname

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

Necessary permissions: Hostname management.

DEIP	🔁 admin Logour
Network	Hostname
Firmware	Hottaura
Or Certificates	510
22. Users	Save
() Time	
Services	
CODESYS	
Hostname	
Logs	
t ₁ Configuration	

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.

DEI					🕒 admin <u>Loo</u> o	ut
	-				<u> </u>	L
***	Network	(
		Live System I	_og			
•	Firmware					
		2020-11-26 14:15:1	2 dbus-daemon	Lystem) Successmily activate service org.freedestop.nostname: Started Mostname Service.	1	
0 (Certificates	2020-11-26 14:15:5	3 api-server	ceptors combined involves invalid size 65535 at offset 0		
		2020-11-26 14:16:1	13 systemd	systemd-hostnamed.service: Succeeded.		
22.1	Users	2020-11-26 15:08:1	12 systemd	Starting Cleanup of Temporary Directories		
		2020-11-26 15:08:3	12 systemd	systemd-tmpfiles-clean.service: Succeeded.		
0.	Time	2020-11-26 15:08:1	12 systemd	Started Cleanup of Temporary Directories.		
Ŭ		2020-11-26 15:48:1	dbus-daemon	[system] Activating via systemid: service name="org.freedesktop.hostname1" unit="dbus-org.freedesktop.hostname1.service" requested by "11.13" (uid=0 pid=346 comm="jusr/bin/api-server" -p 8081 ") fraction (uid=0 pid=346 comm="jusr/bin/api-server" -p 8081 ")		
	Sonicor	2020-11-26 15:48:5	9 systemd	suited hostmand.ever/scie: PrivateNetworksves is configured, but the kernel does not support network namespaces, impring.		
	00141003	2020-11-26 15:48:5	9 dbus-daemon	[system] Successfully activated service 'org.freedesktop.hostname1'		
		2020-11-26 15:48:5	9 systemd	Started Hostname Service.		
	CODESYS	2020-11-26 15:49:6	00 api-server	eeprom: cannot read 'prod-data': invalid size 65535 at offset 0		
_		2020-11-26 15:49:3	19 systemd	systemd-hostnamed.service: Succeeded.		
Ð 1	Hostname	2020-11-27 11:06:0	18 dbus-daenon	[system] Activating via systemd: service name='org.freedesktop.hostname1' unit='dbus-org.freedesktop.hostname1.service' requested by ':1.36' (uid=0 pid=346 comm="/usr/bin/api-server -p 8081 ")		
		2020-11-27 11:06:0	N8 systemd	Starting Nostmand Service		
	Logs	2020-11-27 11:00:0	8 dhus-daenoo	systemutnostnameuservice: rrivatenetwerkeyes is contigured, out one kernet does not support network namespaces, ignoring. Exotent Successfully artivated extraction instrument:		
		2020-11-27 11:06:0	8 systemd	Started Hostname Service.		
ti d	Configuration	2020-11-27 11:06:0	9 api-server	eeprom: cannot read 'prod-data': invalid size 65535 at offset 0		
		2020-11-27 11:06:3	13 ap1-server	Invalid user on password		
		2020-11-27 11:06:1	18 systemd	systemd-hostnamed.service: Succeeded.		
		2020-11-27 11:06:4	12 apl-server	Web login with password. User admin IP 10.0.28.173		
		2020-11-27 11:06:4	19 api-server	Invalla user or password		
		2020-11-27 11:31:1	7 cous-daemon	[system] Activating via system) service name: org.treedesktop.timedatei unit: dous-org.treedesktop.timedatei.service requested by :1.41 (uiu-e pin-346 comm: /usr/oin/api-server -p semi -) trarting Thus & hats conv(n		
		2020-11-27 11:31:3	7 systemd	system's text of the service: ProtectHostname-ves is configured, but the kernel does not support UTS namespaces, ignoring namespace setup.		
		2020-11-27 11:31:3	7 dbus-daemon	[system] Successfully activated service 'org.freedesktop.timedate1'		
		2020-11-27 11:31:3	17 systemd	Started Time & Date Service.		
		2020-11-27 11:37:0	6 systemd	systemd-timedated.service: Succeeded.		
		2020-11-27 11:38:1	12 ap1-server	Web login with password. User admin IP 10.0.28.373		
		2020-11-27 11:44:5	9 dbus-daenon	[system] Activating via systemd: service name*org.freedesktop.hostname1* unit=*dbus-org.freedesktop.hostname1.service* requested by ':1,75' (uid=0 pid=346 comm=*/usr/bin/api-server -p 8081 *)		
		2020-11-27 11:44:5	9 systemd	starting mostmam service		
		2020-11-27 11:44:5	9 dbus-daemon	[system] Successfully activated service 'org_freedesktop.hostname1'		
		2020-11-27 11:44:5	9 systemd	Started Hostname Service.		
		2020-11-27 11:45:2	19 systemd	systemd-hostnamed.service: Succeeded.		
		2020-11-27 11:52:4	tê dbus-daemon	[system] Activating via systemd: service name='org.freedesktop.hostname1' unit='dbus-org.freedesktop.hostname1.service' requested by ':1.77' (uid=0 pid=346 comm="/usr/bin/api-server -p 8081 ")		
		2020-11-27 11:52:4	40 systemd	systemd-hostnamed.service: PrivateNetwork=yes is configured, but the kernel does not support network namespaces, ignoring.		
		2020-11-27 11:52:4	lð systend	Starting Hostmane Service		
		2020-11-27 11:52:4	t cous-damon	Lystem] Successfully activates service org.freedes.cop.nostname1		
		2020-11-27 11:52:4	41 apl-server	eeroem cannot read 'prod-data': invalid size 65535 at offset 0		
		2020-11-27 11:53:1	11 systemd	systemd-hostnamed.service: Succeeded.		
					Ψ.	
		4			·	
)	
		Download				
		Duration	-	a(c) Transad		
		Sudion	. Log typ			
_						
)	
		-				-

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.

DEID	😝 admin Logout
tt Network	Export
Firmware	Download configuration
O- Certificates	Badup Indude certificates and users
21 Users	Import
() Time	Select Import
Services	
CODESYS	
- Hostname	
💻 Logs	
t ₄ Configuration	

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.

DEIF	e ad	imin Logout
H Network	Virtual LAN	
Or Certificates	1 +	
St Users	1 Default description	
 Time Services CODESYS Hostname Logs Configuration 	IPv4 Ado State 110 . 1 . 20 . 76 / 24 Link-locat only Add DNS +	
	Link-local only	
	Ports	
	LANI Enabled Implies Implie	
	LAN2 Access Construction Constr	
	LAN3 (Mode - 75pe - Cecesption - Access - LAN3 - VLAN1 + 1 + 1	
	LANA Caces Caces LANA LANA LANA LANA LANA LANA LANA LAN	
	LANS Enabled Tree Conception Tree Conception Con	
	Apply changes Save to startup	

- 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.

DEI	😝 admin Lopout
+++ Network	Hostname
E Firmware	Hoteland Hoteland
O- Certificates	519
21 Users	Save
() Time	
Services	
CODESYS	
Hostname	
Logs	
t ₁ Configuration	

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.

DEIF		😫 admin Logout
Network	Users	
Firmware	admin	
O- Certificates	Pasavord	
31 Users	New password Re-type new password Update	
() Time	Admin only SSH	
Services		
CODESYS	aan ooson is verenoonsoo naar na caareen naacaareen naar moor ny sanggoon	
- Hostname		
Logs		
t↓ Configuration		
	Select file Update	
	locatoroesser	<u> </u>
	+	~

- 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 +.

DEIF		3 admin Lo	gout
Network	Users		ר
Firmware	admin	Ý	
O- Certificates	localiscossuser		1
21 Users	(+		ıl -
() Time			1
Services	Usemane Enabled Disabled		1
CODESYS	Password		1
Hostname	New password Re-type new password		1
Logs			
t ₁ Configuration	Permissions		
			1
	Adi	Cancel	j]
			1

- 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.*

		🔒 admin L
k (Users	
e	admin	^
	Password	
	New password Re-type new password Update	
	Admin Unity SSH Ind-wr/SSI MAAACNING'I 7711/1755444.65-b764-96-771.MTM-MCR/CF773.05148/0576-01110-1000 km/	
	Select file Update	
	+	~
	+	

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

OpenSSH SSH client	-	×
		^
C:\>ssh admin@amc300.local		
Last login: Fri Nov 27 09:39:31 2020 from fe80::a5aa:bff1:3d76:f4bb%lanx.1		
admin@AMC300;/mnt/sysdata/home/admin\$		
		\sim

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.

		?
e <u>K</u> ey Con <u>v</u> ersions <u>H</u> elp		
Key No key.		
Actions Generate a public/private key pair		<u>G</u> enerate
Load an existing private key file		Load
Save the generated key	Save p <u>u</u> blic key	<u>S</u> ave private key
Save the generated key Parameters	Save p <u>u</u> blic key	<u>S</u> ave private key

2. Select Generate.

3. Follow the instructions on the screen.

PuTTY Key Generato	r		?	\times
File Key Conversions	<u>H</u> elp			
Key				
Public key for pasting ir	to OpenSSH authorized_	keys file:		
ssh-ed25519 AAAAC3NzaC1IZDI1N admin-ed25519-key-ge	TE5AAAAIHi1GdkWfZb8 merated-20201127	Y6JkdFWYr8Z4sDChyOvl	-OL2iHMinFk0m	
Kov fingornrint	esh-od25519.255 c2:26	72:6a:b9:4d:20:6d:ee:cf3d	-33-20-69-66-83	4
Key ingerprint.	SSIFed25515255 C2.20.	72.0a.D5.40.20.00.ee.cl.50	.55.20.05.00.05	_
Key <u>c</u> omment	admin-ed25519-key-ge	nerated-20201127		
Key p <u>a</u> ssphrase:				
Confirm passphrase:				
Actions				
Generate a public/priva	ite key pair		<u>G</u> enerate	
Load an existing private	e key file		<u>L</u> oad	
Save the generated ke	y .	Save p <u>u</u> blic key	Save private key	
Parameters				
Type of key to generate <u>RSA</u>	e: <u>D</u> SA O <u>E</u> CDS this key type)	GA	() SSH- <u>1 (</u> RSA)	

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

Save public key as:					×
$\leftarrow \rightarrow \uparrow \uparrow$	$ < $ Workspace $ \rightarrow $ AMC 300 $ \rightarrow $ Admin user key pair	~	じ 、 Search A	dmin user key pai	r
Organize 🔻 New	v folder				?
🖈 Quick access	Name	Date modified	Туре	Size	
	admin-public-key.pub	27-11-2020 09:43	Microsoft Publishe	1 KB	
Dropbox					
OneDrive					
🧢 This PC					
🗳 Network					
File <u>n</u> ame:	admin-public-key.pub				~
Save as <u>t</u> ype:	All Files (*.*)				~
∧ Hide Folders			<u>S</u> ave	Cancel	

5. Save the generated private key with $\ensuremath{\textbf{Save private key}}$.

😴 Save private key as	is:				Х
A A A	« Workspace > AMC 300 > Admin user key pair	~	ひ 。 Search A	dmin user key pair	
Organize 🔹 Nev	w folder			-	?
+ Quick accord	Name	Date modified	Туре	Size	
	🗋 admin-private-key.ppk	27-11-2020 09:46	PuTTY Private Key	1 KB	
 OneDrive 					
🧢 This PC					
😻 Network					
File <u>n</u> ame:	admin-private-key.ppk				~
Save as <u>t</u> ype:	PuTTY Private Key Files (*.ppk)				V
∧ Hide Folders			<u>S</u> ave	Cancel	

5.2.5 Export an OpenSSH private key

	V Key Generato	,			2 X
ing runn					: ^
File Key	Conversions	Help			
Key	Import k	ey			
Public	k Export C	penSSH key			
ssh-eo	Export O	penSSH key	(force new	file format)	1 OL 2iHMinEk0m
admin	Export se	h.com key			
					· · · ·
Key fin	gerprint	ssh-ed25519) 255 c2:26:72	2:6a:b9:4d:20:6d:ee:cf:3	d:33:20:69:6b:83
Key <u>c</u> o	mment	admin-ed25	519-key-gene	erated-20201127	
Key pa	ssphrase:				
Confirm	n passphrase:				
Actions					
Genera	ate a public/priva	te key pair			Generate
Load a	in existing private	key file			Load
Save the generated key Save public key Save private key					<u>S</u> ave private key
Parame	eters				
Type o <u>R</u> S/	of key to generate A O [: <u>)</u> SA	⊖ <u>e</u> cdsa	• Ed <u>2</u> 5519	⊖ SSH- <u>1</u> (RSA)
(nothing	g to conligure for	inis key type)			

🚰 Save private key as	:					Х
← → ∽ ↑ 🖡	« Wo	rkspace > AMC 300 > Admin user key pair	~	ර , P Search A	Admin user key pa	ir
Organize • New	/ folder	r			•== •	?
1.0.11		Name	Date modified	Туре	Size	
r Quick access		<table-of-contents> admin-public-key.pub</table-of-contents>	27-11-2020 10:00	Microsoft Publishe	1 KB	
Dropbox		🏂 admin-private-key.ppk	27-11-2020 10:00	PuTTY Private Key	1 KB	
OneDrive		admin-private-key.pk	27-11-2020 10:19	PK File	1 KB	
🐚 This PC						
🧼 Network						
File <u>n</u> ame:	admin	ı-private-key.pk				
Save as <u>t</u> ype:	All File	15 (*.*)				
∧ Hide Folders				<u>S</u> ave	Cancel	

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).

PuTTY Key Generato	r		? >
le <u>K</u> ey Con <u>v</u> ersions	<u>H</u> elp		
Key			
Public key for pasting in	to OpenSSH authorized	keys file:	
ssh-ed25519			A
AAAAC3NzaC112D11N admin-ed25519-key-ge	rerated-20201127	Y6JkdFWYr8Z4sDChyOvl	LOL2IHMinFk0m
			*
Key fingerprint	ssh-ed25519 255 c2:26	:72:6a:b9:4d:20:6d:ee:cf:3d	1:33:20:69:6b:83
Key <u>c</u> omment	admin-ed25519-key-ge	enerated-20201127	
Key p <u>a</u> ssphrase:			
Confirm passphrase:			
Actions			
Generate a public/priva	te key pair		<u>G</u> enerate
Load an existing private	key file		Load
0		Onus aublis have	O avec a situate have
Save the generated key	/	Save p <u>u</u> blic key	Save private key
Parameters			
Type of key to generate		-	-
	<u>D</u> SA <u>E</u> CD	SA () Ed <u>2</u> 5519	() SSH- <u>1</u> (RSA)
(nothing to configure for	this key type)		

- 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).

DEIF		🙁 admin 🛛 L	ogout
Network	Users		<u>ה</u>
J Firmware	admin	^	
Or Certificates	Pasavord		
🚨 Users	New password Re-type new password Update		
() Time			
Services	vb.w/55/10.11.17.39.0/1771/10754.11.0/m/5.620/50/70.101.19/0/676/2000 selection into law.		
CODESYS			
- Hostname			
Logs			
t ₄ Configuration			
	Select file Update		
			김.
		~	
			IJ

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

Select OpenSSH SSH client	-	×
		^
C:\>ssh admin@amc300.local		
Last login: Fri Nov 27 09:39:18 2020 from 10.1.20.162		
admin@AMC300:/mnt/sysdata/home/admin\$		
		\sim

5.3.3 Using PuTTY for SSH access

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

Repuiring Configuration		í X
Category:		
 Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection 	Basic options for your PuTTY s Specify the destination you want to connect Host Name (or IP address) amc300.local Connection type: Raw I lenet Rlogin Ssvgd Sessions	ession to Port 22 SH () Se <u>r</u> ial
Colours Connection Data Proxy Telnet Rlogin SSH Serial	Default Settings WinSCP temporary session	Load Sa <u>v</u> e Delete
	Close window on exit. Always Never Only on o	clean exit

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

🕵 PuTTY Configuration		?	\times
Category:			
Bell Features Window Appearance Behaviour Translation Selection Colours Onnection Proxy Telnet Blogin	Options controlling SS Display pre-authentication bar Bypass authentication entirely Authentication methods Authentication using P Attempt authentication using P Attempt TIS or CryptoCard aut Attempt "keyboard-interactive Authentication parameters Authentication parameters Allow agent forwarding	H authentication Iner (SSH-2 only) (SSH-2 only) ageant h (SSH-1) " auth (SSH-2)	
SSH - Kex - Host keys - Cipher - Auth - GSSAPI - TTY - X11 - Tunnels - Bugs - More bugs	Allow attempted changes of us Private <u>k</u> ey file for authentication: Admin user key pair\admin-priva	sername in SSH-2 <u>te-key.ppk</u> Br	o <u>w</u> se
<u>A</u> bout <u>H</u>	р <u>О</u> р	en <u>C</u>	ancel

3. Log in with **admin**.

Pamc300.local - PuTTY	_	×
		^
🚰 login as admin		
🛃 Authenticating with public key "admin-ed25519-key-generated-20201127"		
admin@AMC300:/mnt/sysdata/home/admin\$		
		×

5.3.4 Access via WinSCP

1. Open WinSCP and click new Session:

-							
💫 WinSCP					-		×
Address						6	- 7
	🗈 🗊 🏠 🧭 🙀 Find Files 📄 Downloa	d 🕶 📝 Edit 🕶 🚔 🗙	🕞 Properties 📝 督 N	ew 🕶 📰 🧬 🔛 😳	Synchronize		
🍥 🗉 -	🖗 Queue 👻 🏣 🛛 Transfer Settings Defau	lt 🔹	<i>🛃</i> 🗸				
<u>F</u> ile <u>C</u> omm	ands <u>M</u> ark <u>S</u> ession <u>V</u> iew <u>H</u> elp						
🛒 New Ses	sion						
		Size	Name				
		<					>
Queue							
🖗 🕨 🗙	↑ ↓ iii • ∅						
Operation	Source	Destination		Transferred	Time	Speed	Р
							,
Not connecte	d						
Hot connecte	u.						

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

New Site	^	Session Elle protocol:	
		Host name: amc300.local	Port number:
		User name: Passw admin	ord:
		<u>S</u> ave ▼	A <u>d</u> vanced
<	×		
Tools 💌	<u>M</u> anage 🔻	Login 🗸	Close Help

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

dvanced Site Settings		?	×
Environment Directories Recycle bin Connection Proxy Tunnel SSH Key exchange Authentication	Bypass authentication entirely Authentication options Attempt authentication using Pageant Attempt 'keyboard-interactive' authentication Respond with password to the first prompt Attempt TIS or CryptoCard authentication (SSH-1)		
– Bugs Note	Authentication parameters Allow agent forwarding Private key file: C:\Workspace\AMC 300\Admin user key pair\admin-private Display Public Key Tools	e-key.ppk	
	GSSAPI		
<u>C</u> olor ▼	OK Cancel	I I	<u>H</u> elp

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

🌯 admin - admin@amc300.local - WinSCP			-		Х
Address 📜 /mnt/sysdata/home/admin				-	-
🛛 🔶 🔹 🖈 🏠 🕼 🧭 🖍 Find Files 🛛 🙀 Download	1 🗸 📝 Edit 👻 🔂 🗶 🔂 Properties 📝 📑 Ne	ew 🕶 📰 🧬 🔀 🚔	Synchronize		
🔅 💷 🛪 📝 Queue 🛪 🏪 🛛 Transfer Settings Defaul	t 🔹 💋 -				
<u>File</u> <u>Commands</u> <u>Mark</u> <u>Session</u> <u>View</u> <u>H</u> elp					
📮 admin@amc300.local 🗶 😴 New Session					
<pre>> / <root></root></pre>	Size Name			^	
	<				>
Queue					
Operation Source	Destination	Transferred	Time	Speed	P
0 B of 0 B in 0 of 1			SCP	0:00	:05

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

Finance Forware Update Forware Update Contractors	DEIP	👌 admin Logov
I ranze I ra	Network	Firmware Update
• Centralize • Centralize • Less • The • Contralized • Contralized </th <th>Firmware</th> <th>(Stat wation (Statis wation (Addw statis)</th>	Firmware	(Stat wation (Statis wation (Addw statis)
 kuns kuns<th>Or Certificates</th><th>Current version(s) v4.0.0.0_rct_5_g211ca01_d A</th>	Or Certificates	Current version(s) v4.0.0.0_rct_5_g211ca01_d A
Image: Content in a	🚨 Users	
 Services CODESYS Noticearro Logic Configuration 	() Time	
 CODESYS Mostaure Loga Configuration 	Services	
 kottano kottano kottano configuration 	CODESYS	
Logs Configuration	Hostname	
Configuration Civic Confi	Logs	
	t Configuration	Cick to select file or dicp here

3. Select Click to select file or drop here

- Drag-and-drop a firmware file, or
- Navigate to the firmware file and select it

📕 🕑 📜 🔻 firmware			- 0	×
File Home Share View				~ ?
\leftarrow \rightarrow \checkmark \uparrow \blacksquare $<$ AMC 300 $>$ firmware \checkmark \circlearrowright	Search firmware			
Name ^	Date modified	Туре	Size	
mi300_PCM_3_1_bsp_v4.0.0.0_rc1_12_g3135253.raucb	25-11-2020 04:56	RAUCB File	26.886 KB	
1 item 1 item selected 26,2 MB				

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

Firm The update process will take	ware successfully uploaded. e a few minutes, are you sure you wish to continue?				
Go back!	Continue with upgrade				
100%					

5. Select Continue with upgrade

6. When the update is done, you will be prompted to restart the system

				_	
2:08:24 PM	Copying image to appfs.1			•	
2:08:25 PM	Copying image to appfs.1 done.				
2:08:30 PM	Checking slot rootfs.1				
2:08:30 PM	Checking slot rootfs.1 done.				
2:08:30 PM	Copying image to rootfs.1				
2:08:36 PM	Copying image to rootf	Lindete dono, restart needed			
2:08:39 PM	Checking slot kernel.1	opuale done, restart needed.			
2:08:39 PM	Checking slot kernel.1	Restart			
2:08:39 PM	Copying image to kerne	rtotart			
2:08:42 PM	Copying image to kernel.1 done.				
2:08:42 PM	Checking slot uboot.1				
2:08:42 PM	Checking slot uboot.1 done.				
2:08:42 PM	Copying image to uboot.1			-	
070					
97%					

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 -sinsecure -X POST -H'Content-Type: application	n/ison'	-d"{	\ "
username\": \"\$USERNAME\", \"password\": \"\$PASSWORD\" }" \$HOST/api/login			
"token": "eyJhbGciOiJIUZUXMIISInR5cCI6IkpXVCJ9.eyJleHAiOjE2MDYzOTkwNzQSImlhdCI6MTYwNjM5h iREVJRiISInBlcm1pc3Npb25zIjpbImFkbWluIiwiY2VydCISImNvZGVzeXMiLCJjb25maWdlcmF0aW9uIiwiaG9zdG CJuZXR3b3JrIiwicGFzc3dvcmQiLCJzZXJ2aWNlIiwic29mdHdhcmUiLCJ0aWllIiwidXNlciJdLCUIc2VybmFtZSI6 jjGZAXVYykyjYcM0mlJOhgizKIFabTxTrJrj6VsrbnMpMaHm4hp50wGCmfnct7tUZMcB1GrIzSwoiT3MvCg" }admin@pcm31:/mnt/sysdata/home/admin\$ ^C	VzI3NCw ShbWUiL ImFkbWl	iaXNzI CJsb2c: uIn0.wW	jo iL WB
admin@pcm31:/mnt/sysdata/home/admin\$ curl -sinsecure -v -X POST -H"Authorization: Bearer UXMiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE2MDY2OTkwNzQsImlhdCI6MTYwNjM5NzI3NCwiaXNzIjoiREVJRiIsInBlc bImFkbWluIiwiY2VydCIsImNvZGVzeXMiLCJjb25maWdlcmF0aW9uIiwiaG9zdG5hbWUiLCJsb2ciLCJuZXR3b3JrIiv CJzZXJ2aWNlIiwic29mdHdhcmUiLCJ0aW11IiwidXNlciJdLCJ1c2VybmFtZSI6ImFkbWluIn0.wWBjjGZAXVYykyjYc bTxTrJrj6VsrbnMpMaHm4hp50wGCmfnct7tUZMcB1GrIzSwoiT3MvCg" \$HOST/api/system/reset	eyJhbG m1pc3N vicGFzc M0m1JC	ciOiJIU [pb25zI] :3dvcmQ;)hgizK1]	UZ jp iL Fa
<pre>* TLSv1.3 (OUT), TLS handshake, Client hello (1): * TLSv1.3 (IN), TLS handshake, Server hello (2):</pre>			
* TLSv1.3 (OUT), TLS change cipher, Change cipher spec (1):			
* TLSV1.3 (UN), 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):			
> POST /api/system/reset HTTP/1.1			
> Host: pcm31.local			
> User-Agent: curl/7.66.0			
<pre>> Accept: */* > Authorization: Bearer eyJhbGciOiJIUzUxMiISInR5cCI6IkpXVCJ9.eyJleHAiOjE2MDYzOTkwNzQsImlhdCl CwiaXNzIjoiREVJRiISInBlcm1pc3Npb25zIjpbImFkbWluIiwiY2VydCIsImNvZGVzeXMiLCJjb25maWd1cmF0aW9u iLCJsb2ciLCJuZXR3b3JrIiwicGFzc3dvcmQiLCJzZXJ2aWNlIiwic29mdHdhcmUiLCJ0aW11IiwidXNlciJdLCJ1c2V WluIn0.wWBjjGZAXVYykyjYcM0m1JOhgizK1FabTxTrJrj6VsrbnMpMaHm4hp50wGCmfnct7tUZMcB1GrIzSwoiT3Mv0 ></pre>	6MTYwN iwiaG9 /ybmFtZ Cg	jM5NzI zdG5hbW SI6ImF	3N WU kb
* 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: U			
<			
admin@pcm31:/mnt/sysdata/home/admin\$			
			\sim