MAGIC AC1 XIP

Secure Login Update
from Version 5.x

Contact:

Phone +49 911 5271-110
Email support@avt-nbg.de

AVT Audio Video Technologies

- The previous simple and unencrypted password protection was intended to avoid misconfiguration by users.
- Through the new Audio over IP technique the systems are increasingly connected directly to the Internet, thus increasing the risk that criminal hackers take over the systems and cause costs to the users.
- In order to prevent this risk, we have integrated a multi-level password security with the new Secure Login, which is described in the following.

Why Secure Login?

- To achieve a as high as possible security with a suitable password, the following requirements have to be fulfilled:
  - The password length must be 8 characters at least and 16 maximally
  - The password must contain:
    - At least one letter
    - At least one digit
    - At least one special sign
- The password is encrypted by means of the standardized, symmetrical encryption method AES-256 (Advanced Encryption Standard)
- Each device uses an individual code
- There is no in-house Backdoor Password
- An automatic user logout is carried out
  - After an ADMIN or USER Login, if no action is carried out within 5 minutes
  - 60 seconds before the automatic logout, an alarm is displayed

Password Security

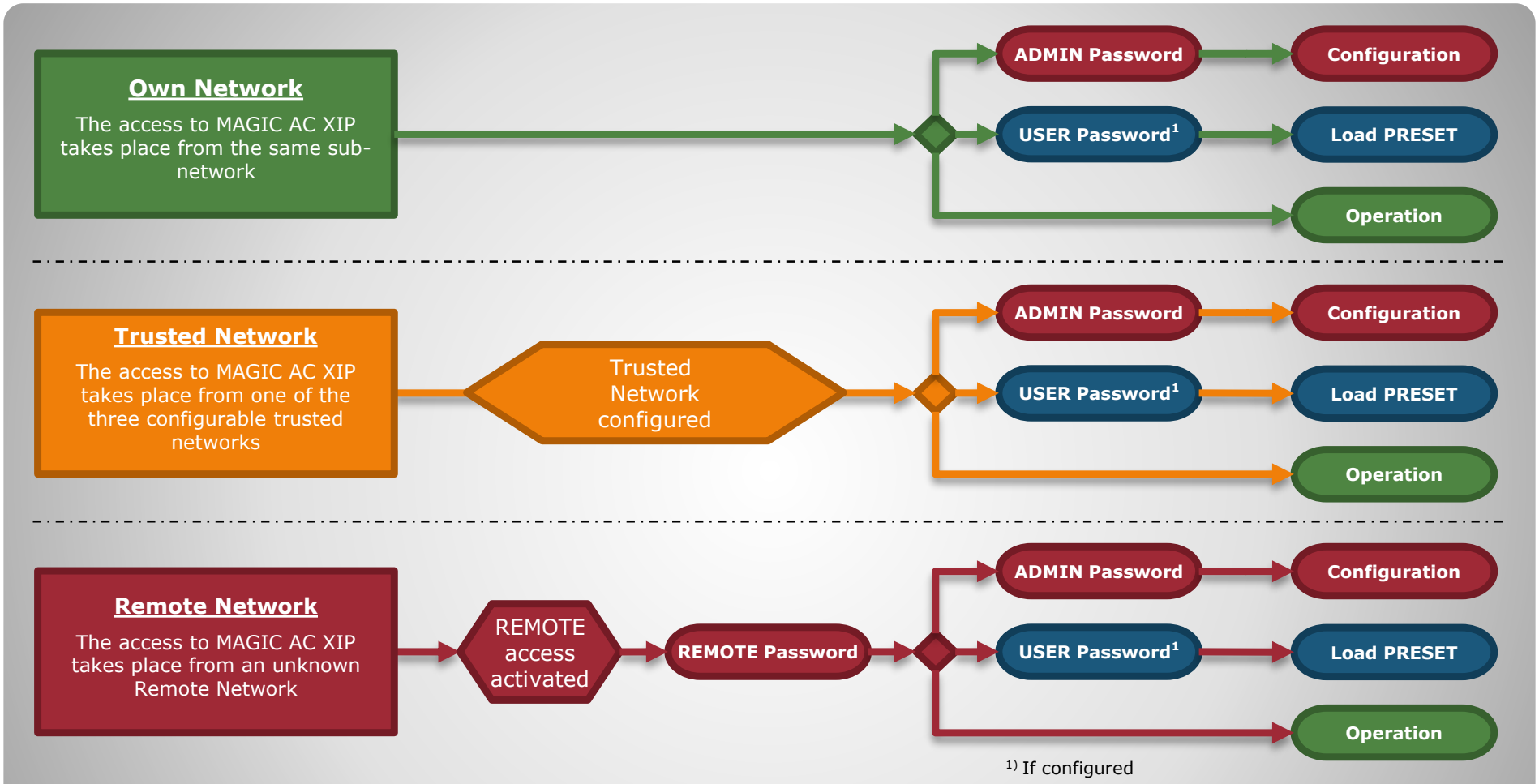
- The entry of an ADMIN password is compulsory

  The request is issued in case of:

  - **Initial operation**
    - After starting the system the command prompt for the ADMIN password shows on the display
    - An entry of the ADMIN password is only possible directly on the device
  - **At first-time Software Update to Version 5.x or higher**
    - The entry takes place via the PC software
    - A confirmation on the device is not necessary

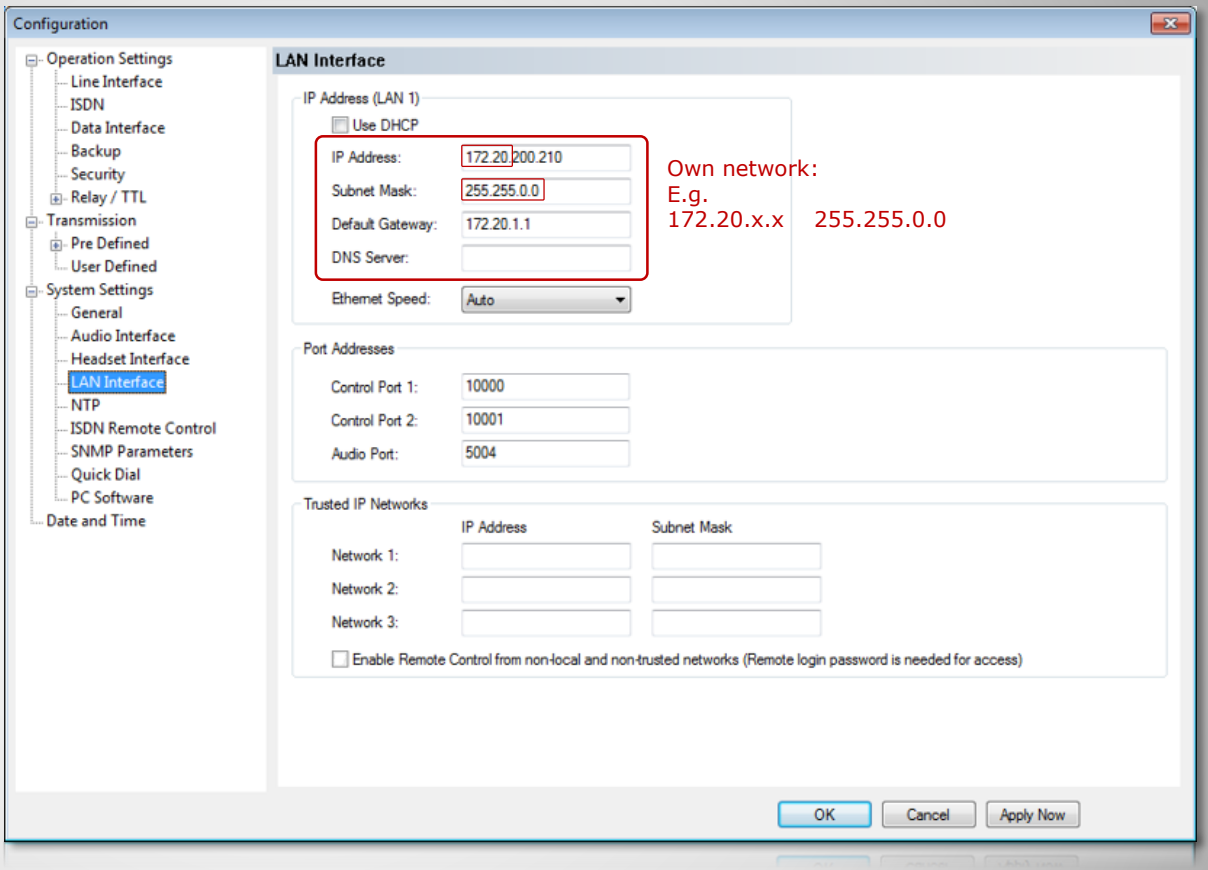
- A change of the ADMIN password via the PC software requires:
  - Login with old password
  - Edit new password
  - Verification of password
  - **Local** confirmation on the device

Compulsory ADMIN Password



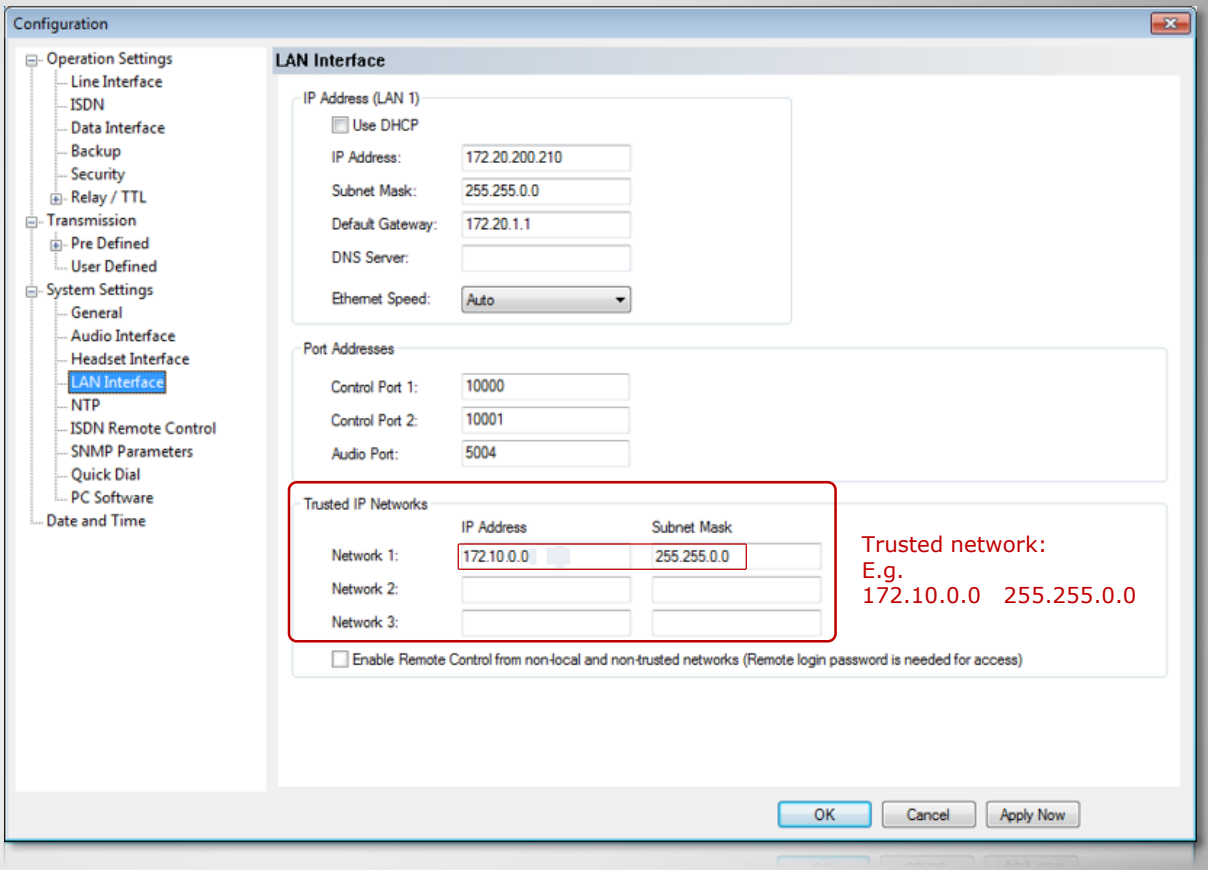
Access from different networks

- The access authorization for PCs in the own network is identical to the previous access with a firmware smaller than V5.x
  - ADMIN password for configuration
  - USER password for loading Presets
  - No password for status display and operation



Own Network

- The access authorization for PCs from a trusted network is identical to the access from the own network
  - ADMIN password for configuration
  - USER password for loading Presets
  - No password for status display and operation
- The access is only possible if the network from which the access is intended has been entered in the device under ***Trusted IP Networks***
  - Format specification for networks, e.g.:
    - 192.168.96.0 255.255.255.0
    - 172.16.0.0 255.255.0.0
- Up to <u>three</u> trusted networks can be defined <u>additionally</u> to the own network

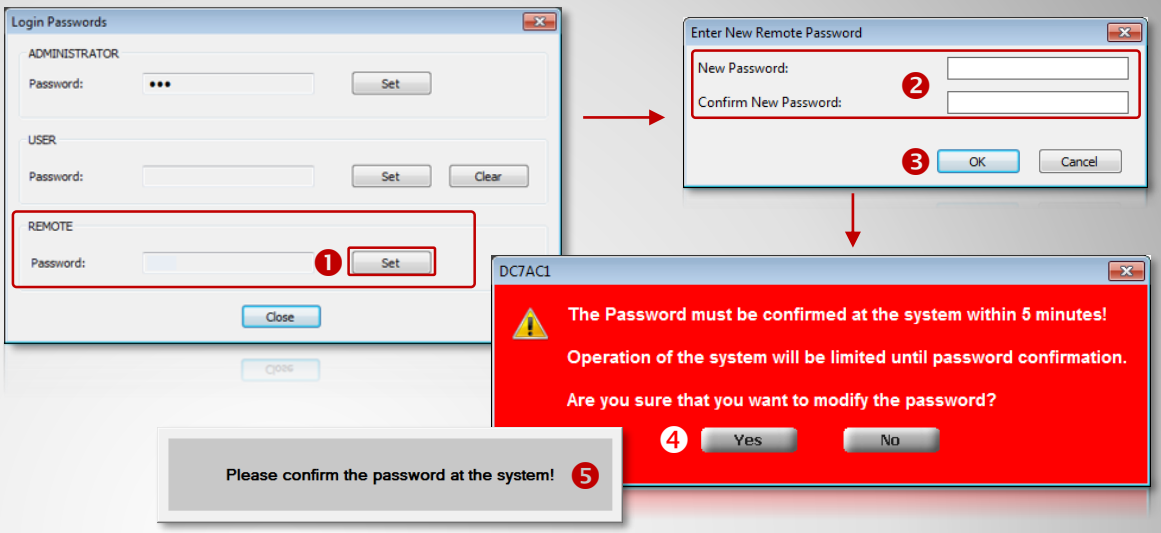


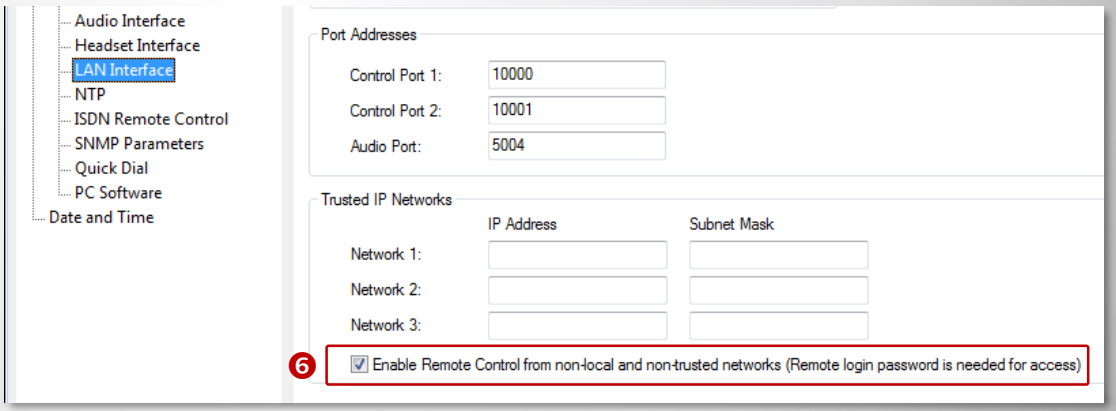
Trusted Networks

- For access from Remote Networks a REMOTE password is required
- The device can be operated after the entry of the REMOTE password
- For the remote configuration of the device the ADMIN password is required
- Setup of the remote access via display/keypad on the device
  - Login with ADMIN password under
    - MENU → LOGIN
  - Setup of a REMOTE password under
    - MENU → SYSTEM SETTINGS → ETHERNET REMOTE ACCESS → REMOTE PASSWORD
  - Enabling the access for Remote Networks
    - MENU → SYSTEM SETTINGS → ETHERNET REMOTE ACCESS → REMOTE ACCESS ENABLE

Remote Networks (1)

- Setup of the REMOTE password on the PC
  - Device and PC must be located in the own or a trusted network
  - Select ***Configuration → Login Passwords*** in the PC software
  - After clicking on ***Set*** (❶) at ***REMOTE Password*** the entry mask for the setup of the REMOTE password is displayed
  - Enter the requested REMOTE password under ***New Password*** and confirm with ***Confirm New Password*** (❷)
  - After clicking the ***OK*** button (❸) a warning notice appears, saying that the password on the device must be confirmed
  - After clicking the ***Yes*** button (❹) the REMOTE password must be confirmed on the device within 5 minutes (❺)
- Enabling the access for Remote Networks
  - Please finally set the option ***Enable Remote Control from non-local and non-trusted networks*** (❻) on the ***LAN Interface*** page in order to activate the Remote access





Remote Networks (2)

- The following restrictions apply to third-party software, which use the AVT control protocol for our systems:
  - A control/operation is only possible in the own network or via the trusted networks
  - A device cannot be configured any longer, as the ADMIN password is required
- If you have forgotten the password
  - The password protection can only be reset on the device by clicking on ***MENU*** → ***LOGIN*** → soft key ***FACTORY SETTINGS***
    - AVT has no Backdoor Password to re-establish the access
    - The AVT Support has no possibility to read out your password in another way

Third-Party Software Forgotten Password