



AEMON and AECONF



AEMON: AEOS Monitoring and configuration tool

AECONF: AEPU - IP configuration tool

User Manual



0 CONTENTS

1.	INTRODUCTION	4
2.	INSTALLATION of AEMON and AECONF	4
3.	CONFIGURING THE AEPU	5
3.1.	AEpu configuration with AEconf	5
3.2.	Hosts file distribution using AEconf	5
3.3.	AEpu configuration using Hyperterminal (or putty)	6
4.	STARTING UP AEMON	8
4.1.	Menu overview	9
5.	LOADING AEPU	12
5.1.	Check version number of software of AEpu	12
5.2.	Load new software to AEpu using AEmon	12
5.3.	Load new software to AEpu using .bat scripts	13
5.4.	Check / set date and time of AEpu	13
5.5.	Deploying AEbc's	13
6.	CONFIGURATING AEMON	14
6.1.	Determine how the AEpu's must be selected	14
6.1.1.	Lookup servers	14
6.1.2.	AEpu lookup server check and change	15
6.1.3.	AEpu information	15
6.2.	Check connected hardware	16
6.3.	Detailed hardware settings	17
6.4.	Configure the AEpu	17
6.4.1.	Deploy configuration over more than one AEpu	19
6.5.	Changing default values of a behaviour component	19
6.5.1.	Bindings	20
6.6.	Configuring the AEpu using the graphical configuration editor	22
6.6.1.	State Monitor	24
6.6.2.	Options	24
6.6.3.	Printing	24
6.7.	Groups	25
7.	LOGGING	26
7.1.	AEmon logging	26
7.2.	AEpu logging	26
7.3.	View events	27
8.	UPLOADING FIRMWARE	28
8.1.	Naming of firmware.	28
8.2.	Restrictions at loading firmware	28
8.3.	Loading new firmware	29
9.	SECURE COMMUNICATION	30
10.	SYSTEM INFORMATION	31
10.1.	Configuration overview	31
10.2.	Used components	31
10.3.	What hardware is used	31
10.4.	Remote bindings	31
10.5.	Check consistency	31
10.6.	AEpu information, including date and time	32
11.	TESTING PORT USAGE	33
11.1.	Testing ports from AEmon to AEpu	34
11.2.	Testing ports from AEsServer to AEpu	35

12. EXAMPLES	36
12.1. Standard Door with combined Emergency Unlock	36
12.2. Generating an Alarm at Emergency Unlock using InputGuard	37
12.3. InputGuard combinations	38
13. HELPFUL HINTS	39
13.1. Right mouse button	39
13.2. Saving data (configuration) to disk	39
13.3. AEpack addresses	39
13.4. Expanding AEpack hardware information	39
13.5. Configuring without having a connection	39
13.6. Automatic AEpu discovery	39
13.7. Lookup services	39
13.8. InterAEpu functionality	39
13.9. AEpu hosts file using AEconf	39
13.10. AEpu hosts file distributing over all AEpu's	40
13.11. Rebooting AEpu using batch script	40
14. CONFIGURATION OF ACCESSPOINTS	41
14.1. Actions on AEmon	41
14.2. Actions on AEsServer	41
14.3. Deleting AccessPoints	41
15. FIRST TIME USE ON AESERVER	42
15.1. Short procedure how to get started with AEOS	42
16. MENU OVERVIEW	44
17. FILES AND DIRECTORIES	46

Intelligent Security & Fire

1. INTRODUCTION

The AEmon program is used as configuring tool for AEOS AEpacks, AEmon also contains several debug functions.

AEmon is needed to configure the AEpacks and Access points. Only after the Access points are configured and deployed they can be detected in the AEOS user interface.

AEconf is an helpful program to make the correct (IP) settings for the AEpu (instead of using hyperterminal or putty).

2. INSTALLATION of AEMON and AECONF

For the installation see the AEOS software CD. AEmon and AEconf are part of the installation.

AEpu's are connected using the network. This manual describes the use of AEmon. How the correct network settings must be made is described in the *AEOS installation manual* and also at chapter 'AEpu configuration'.

Remark: The software version of the AEpu **must** be the same as AEmon and the AEservr.

With version 2.1 this can be done with AEmon, see chapter 5.

See the AEOS installation CD how this version can be checked and eventually updated.

For using InterAEpu communication and automatic discovery of one or more lookup services should be present (See chapter 6.1).

Intelligent Security & FIDO

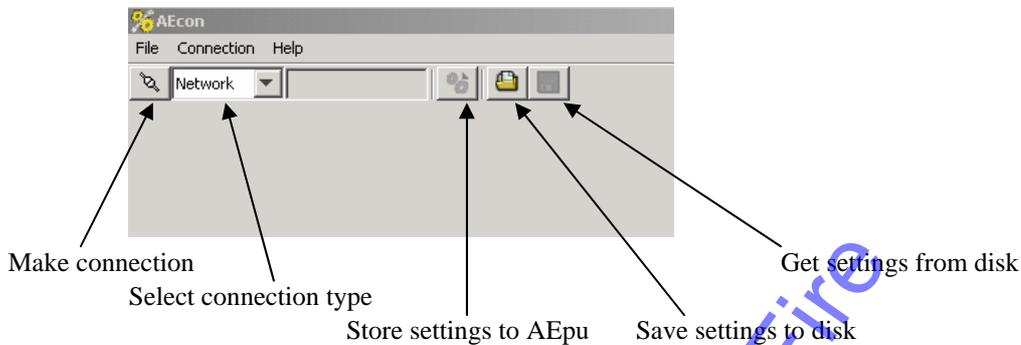
3. CONFIGURING THE AEPU

The network settings for the AEpu can be done by using AEconf (Preferable) or Hyperterminal (Attention: don't use the backspace).

3.1. AEpu configuration with AEconf

AEconf is installed together with AEmon.

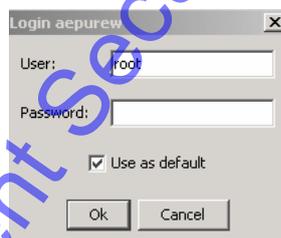
Starting up AEconf shows next screen, on which you can decide how to connect with this AEpu.



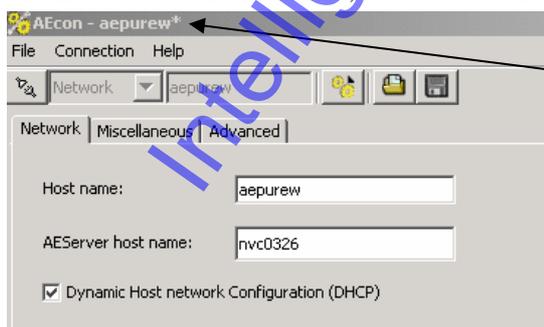
- Select how the AEpu must be connected with AEconf
 - Network (using cross cable on address 192.168.1.1)
 - Or on the host name of the AEpu
 - Serial (connect Null Modem cable to AEpu COM1)



- Make connection with this AEpu (pressing the connection icon)
- Now you first have to login to this AEpu (root – grolle)



- The data will be read from this AEpu and shown. Only the data that is important is shown (e.g. if DHCP is selected the IP-addresses are not shown, these are now non important)



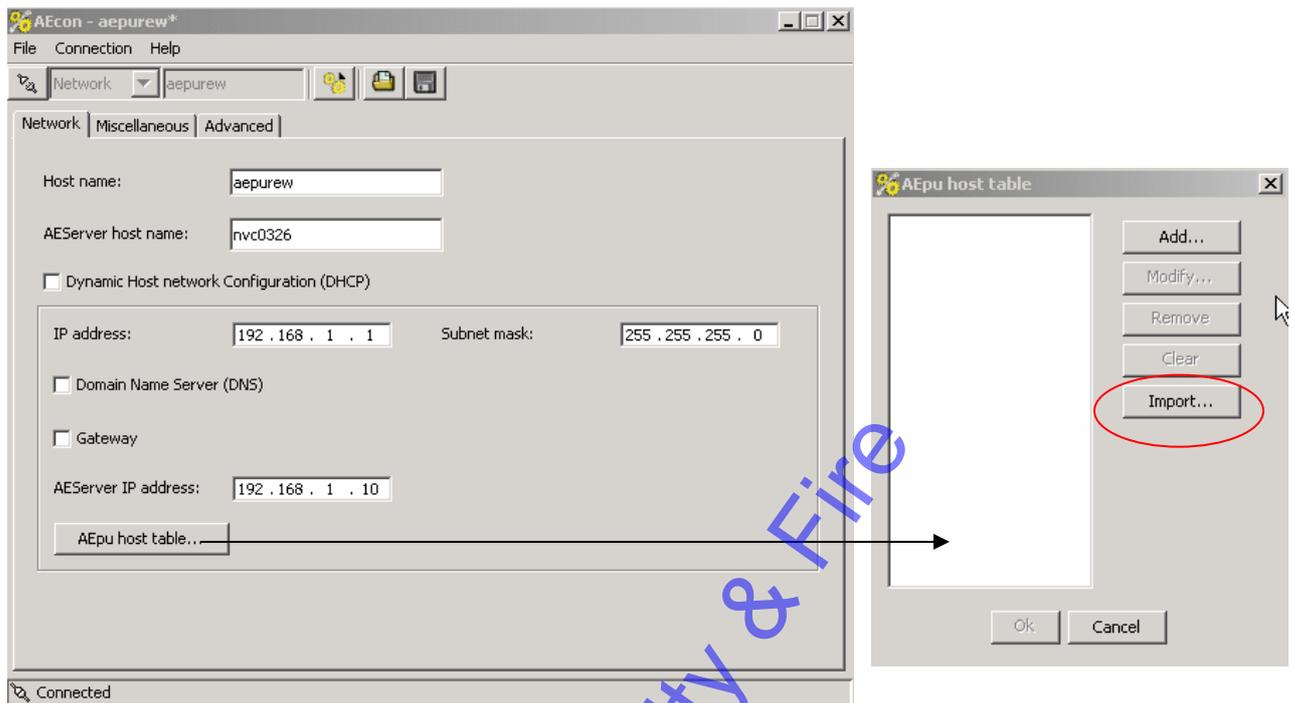
AEpu name, * behind the name indicates that data is changed

- On each tab specific settings can be made. Be careful with the Advanced settings. Only AEOS qualified users are allowed to change these.
- After the changes sent the data to the AEpu by clicking on 

3.2. Hosts file distribution using AEconf

If no DNHC and DNS is used, all AEpu names and IP-address combinations must be added to the AEpu if these AEpu's are using inter AEpu-functionality.

The hosts table can manually be filled, but also by importing the hosts file from the server (also on the server the AEpu names and IP-address must be known).



Remark: Make also a copy of the settings to disk. For all next AEpu's this AEpu configuration file can be used, only the AEpu name and IP address (depending of the network settings) have to be changed then. Both the IP settings and the hosts file will be saved (as two separate files).

3.3. AEpu configuration using Hyperterminal (or putty)

Network and other settings must be initial made using serial connection:

- Connect Null Modem cable to AEpu COM1
- Start Hyperterminal, using following settings:
 - Bits per second: 115200
 - Data bits 8
 - Parity None
 - Stop bits 1
 - Flow Control None
- Use VT100 emulation at Hyperterminal
- Hyperterminal connects now to AEpu and after 'Enter' it returns with login prompt `<aepu_name> login`
- Log on to the AEpu (use correct password)
- After correct login the AEpu prompt appears: #.
- Type `config` for starting the configuration program: between brackets the currents setting is given:

Remark: during configuration the AEpu processes are stopped, so no actions on AEpacks connected to this AEpu are executed!

Config:

- *Host name of this AEpu [aepu_3]:*
- *Use dynamic host network configuration (DHCP) (n/y) [no]*

No:

- *IP address of this AEpu [172.16.17.222]:*
- *Network address and range [172.16.1.0/24]:*

This is a new notation of subnet mask: 255.255.0.0. To calculate this:

E.g.: IP address: 172.16.17.128 and subnetmask was before: 255.255.0.0

Now the network address and range becomes: 172.16.0.0/16

/16 Number of '1' at beginning of string (255=8 '1', so 255.255 = 16)

- 172.16 Logical AND of 255 and 172 (=172) and 255 and 16 (=16)
- Use domain name server (DNS) (n/y) [no]:
 - Use a gateway (y/n) [no]:
 - Yes:
 - Host name of network gateway [aeserver]:
 - IP address of the gateway [172.16.17.100]:
 - Use virtual private network (VPN) (y/n) [no]:
 - Host name AEserv [aeos]:
 - IP address AEserv [192.168.1.10]:
 - Select the proper timezone [Amsterdam]:
Depending on the location where this AEpu is placed the correct timezone must chosen.
 - Add a new aepe (y/n):
Is needed for inter AEpu communication (behaviour components use inputs or outputs form AEpacks located on another AEpu. For using this also the jini services must running on this computer
 - Name of the AEpu:
 - IP address of the AEpu:
 - Add a new aepe (y/n):

Next time config is used it is asked if the added AEpu's must be kept.

After the last command the AEpu is restarted.

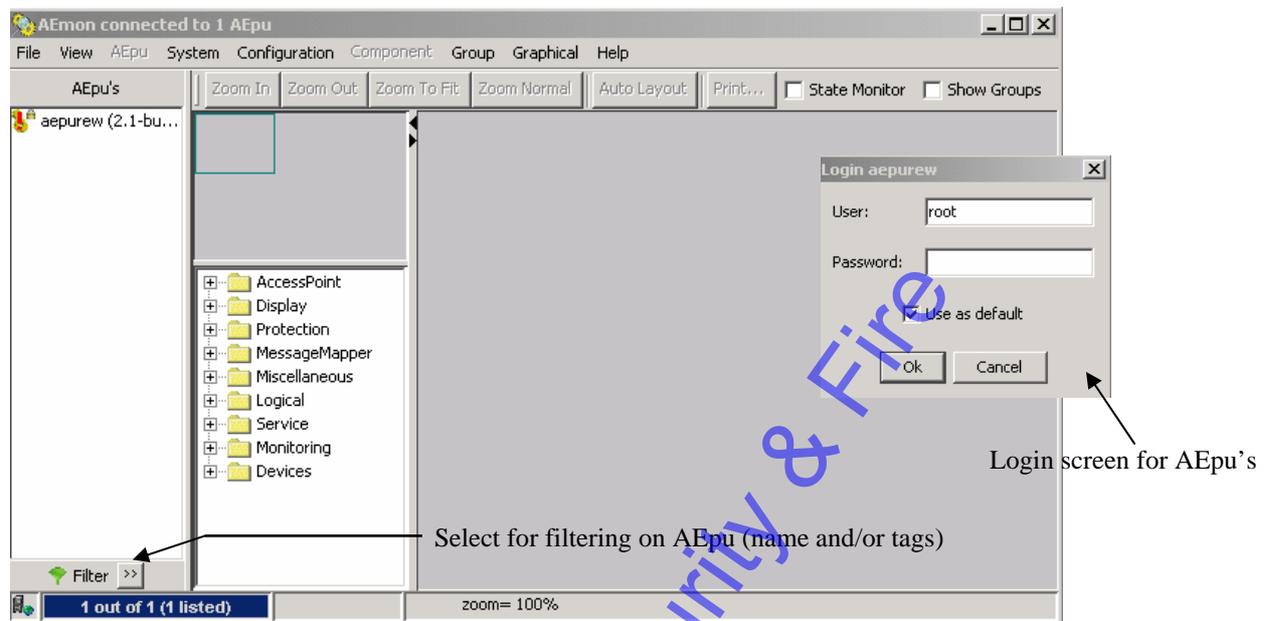
If the correct network settings are made, then the AEpu is also reachable using 'telnet' or equivalent program.

Intelligent Security & Fire

4. STARTING UP AEMON

After installation AEmon can be started using 'Start - Programs – AEOS – AEmon'. If so configured, AEmon will automatically connect to the AEpu's. For starting up AEmon, **no** password is required. Only if interactions with an AEpu are executed, you need to give the correct password for this AEpu. After clicking on an AEpu the password dialog will appear.

The small lock at the AEpu icon shows that this AEpu is 'locked', so a password is required to access this AEpu.



At the login screen for the AEpu you can activate *Use as default* to use this login and password for each AEpu (this will prevent you from filling in each time this password)

4.1. Menu overview

Following menu's are available, some depending if connected to an AEpu:

- **File**

Connections to select AEpu's or show all selected AEpu's (automatic AEpu discovery, Lookup service)
Can be done using the name of the AEpu (e.g. AEpu_Frontdoor) or the IP address (e.g. 192.12.12.61) or automatically by selecting the appropriate lookup services.

A filter can be applied to select one a set of all AEpu's in the system for the defined lookup services

More than one Lookup service can be used.

Prereferences : make your own personalised settings to work with AEmon.

AEpu Define logout time at AEpu and AEpu upload location

Behaviour State if every time you deploy you want to see the overview what to deploy and confirm this. Also can be stated that each time you deploy a configuration on an AEpu the current configuration must be automatically saved.

Graphical Settings for using the graphical configuration interface

Exit

- **View**

Configuration (F1 key)

Shows the behaviour component editor used for inspecting/configuring the behaviour components of the selected AEpu. Depending on menu item *Graphical Mode* the standard (non graphical) or graphical editor is shown. Selecting *View-Configuration* enables the following menu's:

Configuration, Component, Groups

Log (F2 key)

Enables the different log functions in the AEpu and gets the results, see chapter 7.2 for more information. Selecting *View-Log* enables the *Log* menu.

Hardware (F3 key)

Shows the hardware configuration (AEpacks, including firmware version) and their settings.

Graphical Mode

If checked the graphical behaviour component editor is shown when selecting *View-Configuration*

Events

Live event data generated by the selected AEpu is shown in the bottom pane of the AEmon window, see chapter 7.3 for more information.

Program Log (F4 key)

Program Log shows the internal AEmon logging in a separate window, see chapter 7.1 for more information.

- **AEpu**

Properties

Tags Define additional information to an AEpu divided over 3 different tags. These tags can e.g. be used for filtering at location, etc
These Tags are stored at the AEpu and belong to the AEpu configuration.

Lookup services

Select Lookup services for the selected AEpu

Secure shell

Login to the operating system on this AEpu (only for qualified AEmon users !).

Software update

Upload AEpu software to this AEpu (software versions of AEservers and AEpu's must all be equal to each other), see chapter 5

- **System**

Report

Generates a system wide report in a separate Report window.

Remote bindings

Reports what components use inter AEpu functionality, see chapter 10.4

Component statistics

Amount of used behaviour components (AEbc's) , see chapter 10.2

Consistency

Checks the component configuration if any inconsistency is detected (e.g. double used inputs), see chapter 10.5

AEpu information (CTRL+I key)

Retrieves AEpu specific information, see chapter 10.6

Host name resolving

Checks if hostnames involved in inter-aepe communication can be resolved in the appropriate AEpu's,

*Show**Hardware utilization*

Show the system wide utilization of AEpack inputs and outputs

*Tools**Port scanner*

Shows if the used ports (IP / TCP) are free

Firmware control

View/change AEpack firmware, see chapter 8.3

Secure communication

View/change secure communication state, see chapter 9

Change AEpu password

Change the AEpu's password (only for qualified AEmon users !)

Update AEu software

Upload AEpu software to all or a set of AEpu's, see chapter 5

Batch processing

Perform batch actions over all or a set of AEpu's (e.g. save or deploy configuration, see 6.4.1)

- **Configuration** (Only in *Configuration* view)

New

Loads an empty behaviour component configuration.

*Open**from file*

Opens a configuration file which was previously stored on hard disk

from AEpu

Retrieves configuration data from selected AEpu.

Close

Closes the loaded configuration

Save

Saves the configuration to disk

*Report**Components*

Lists all components in the configuration

Consistency

Checks the consistency of the configuration.

Deploy (CTRL+E key)

Deploys (makes active) loaded configuration in the selected AEpu

- **Component** (Only in *Configuration* view)

New

Adds new behaviour component to the configuration

Open (from file)

Opens a component file which was previously stored on hard disk

Save

Saves the component to disk

Report

Generates report of this component.

Copy (CTRL+C key)

Copies the selected component into the internal clipboard.

Paste (CTRL+V key)

Pastes the copied component into the loaded configuration

Rename

Renames the selected component

Modify

Modifies the hardware map for the selected component

Delete (DEL key)

Removes the selected component from the loaded configuration

Properties (CTRL+P key)

Show properties of a selected AEbc

- **Group** (Only in *Configuration* view)
 - Create*
Adds the selected components as a new component group to the group library
 - Organize*
Organize group library including renaming, removing or changing group description.
 - Apply*
Loads the component defined by the selected group into the loaded configuration
- **Graphical** (Only in *Configuration* view with *View-Graphical mode* selected)
 - Zoom in*
Increase view scale.
 - Zoom out*
Decrease view scale.
 - Zoom to fit*
Fits the view scale in such a way that all nodes are shown
 - Zoom normal*
Sets view scale to 100%.
 - Auto layout*
Arrange the node positions automatically.
 - Page Setup*
Sets page paper size, orientation and margins for printing
 - Print preview*
Preview the configuration (or selected part) for printing
 - Print*
Prints the configuration or a part of it in case of selection
 - Options*
View/change graphical options
- **Log** (Only in *Log* view)
 - Get* (CTRL+G key)
Retrieves log data from selected AEpu
 - Save*
Saves retrieved log data to disk
 - Go to most recent*
Scrolls the view to the most recent log record
- **Help**
 - About*
Shows version number of AEmon

Intelligent Security & Fire

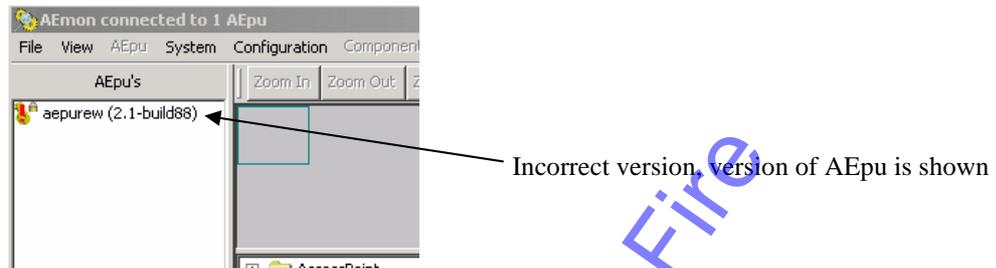
5. LOADING AEPU

The software versions of AEpu's, AEservers and AEMON must be identical. For each new AEpu following actions must be done: (see also the *AEOS installation manual*)

5.1. Check version number of software of AEpu

Make connection to the AEpu (see AEOS installation guide), and after correct settings according the installation guide have been made check the version number (command *version*). The version of the AEpu software **must** be equal to the AEservers version and AEMON version.

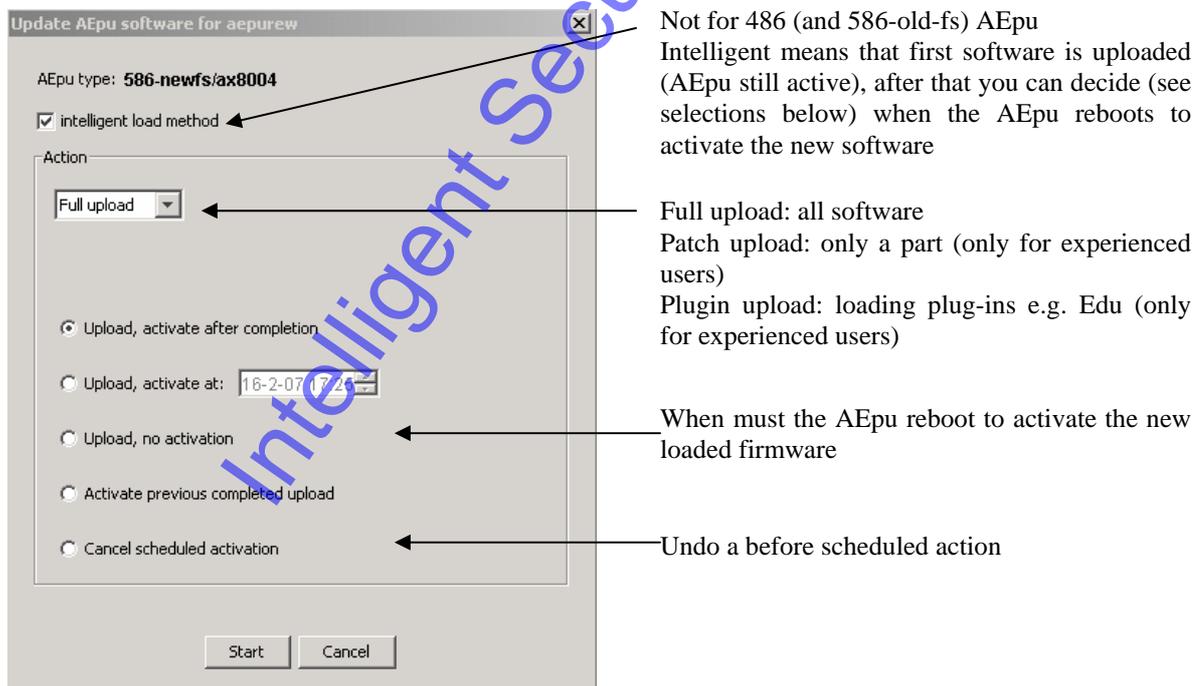
After AEMON is started, in the left part of the screen the detected AEpu's are shown including the status of the software version.



5.2. Load new software to AEpu using AEMON

Using AEMON the AEpu;s can be loaded with the correct software on different ways:

- Select an AEpu, use right mouse button, select option *Software update*. Next screen will appear:



Remark: Activation: A reboot is only performed if AEpu system files have changed, else the application in only stopped and started to activate the update. In the latter case the AEpu down-time is much shorter.

- Go to *System – Update AEpu software*. Make a selection for which AEpu's (with AEpu groups) you want to update at once. The above screen will appear. After activation of the Start button the upload process is activated.

5.3. Load new software to AEpu using .bat scripts

During installation AEpu software and scripts for uploading is stored on the server. See *AEOS Installation manual* for uploading new software to AEpu. (*load_aepu <aepu-name> root grolle*)

5.4. Check / set date and time of AEpu

As most actions on the AEpu are related to time and date be sure date and time is correct.

Date and time are normally set during the upload scripts. To set the new date and time a script is available on the CD. Date and time can also be checked with AEmon.

5.5. Deploying AEbc's

AEbc's must be deployed on this AEpu and linked at the AEservers.

Intelligent Security & Fire

6. CONFIGURATING AEMON

For making a configuration next steps must be taken:

- Determine how the AEpu's must be chosen: using lookup server (preferred) or manually (*File - Connections*)
- Select the AEpu to be configured
- Eventually check the connected hardware (*View - Hardware*)
- Configure the AEbc's (*View - Configuration*)

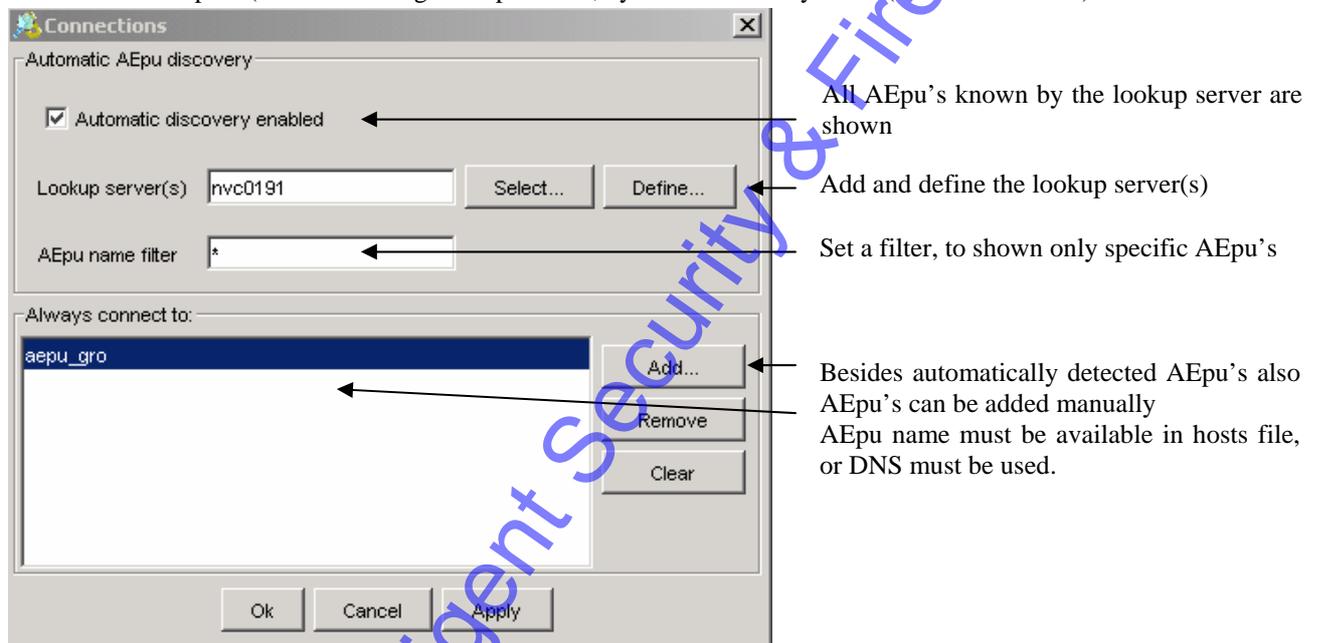
6.1. Determine how the AEpu's must be selected

AEpu's which should be displayed are selected in *File - Connections* by:

- Lookup servers
- Filtering on AEpu name or Tags
- Manual added AEpu names into AEMON

File - Connections

Select AEpu's (automatic using lookup servers, by IP address or by name (hosts file or DNS))



Apply Adds the changes
OK Adds the changes and closes this window

After *OK* those AEpu's which can be discovered at the network are shown. The more AEpu's are present, the longer this can take, so be careful when choosing 'Automatic discovery enabled'

6.1.1. Lookup servers

The lookup servers are used to link AEpu's to AEOS. There can be more than one lookup server active in one system.

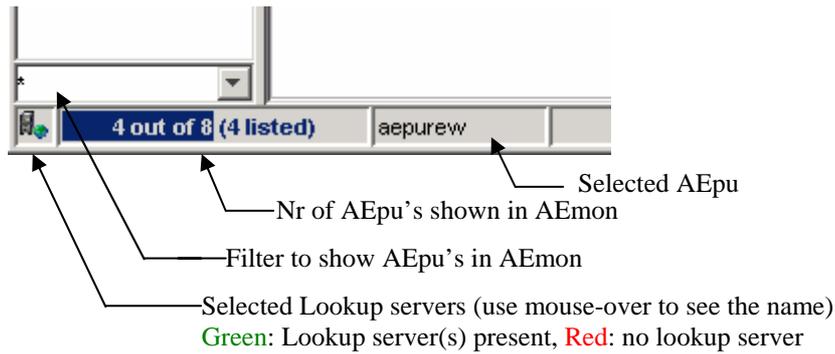
- *Define* Make a list of lookup servers from which later can be used to make a choice from which lookup servers the AEpu's must be shown
 Lookup servers can be added, removed and with *Find all* lookup servers on the network are shown
- *Select* Select from which Lookup servers the AEpu's must be shown (by moving the lookup servers from the left to the right window)

If AEpu's are shown in the left part, use the right mouse button to check/change the lookup server for this AEpu.

Remark: AEpu's are only shown in AEMON if the AEpu name is known (name must be present in the *hosts file* of the PC where AEMON is running or use DNS)

More information about the lookup servers can be found in the *AEOS Advanced Installation Manual*.

At the left bottom of AEMON information about the lookup server(s) can be found:



6.1.2. AEPu lookup server check and change

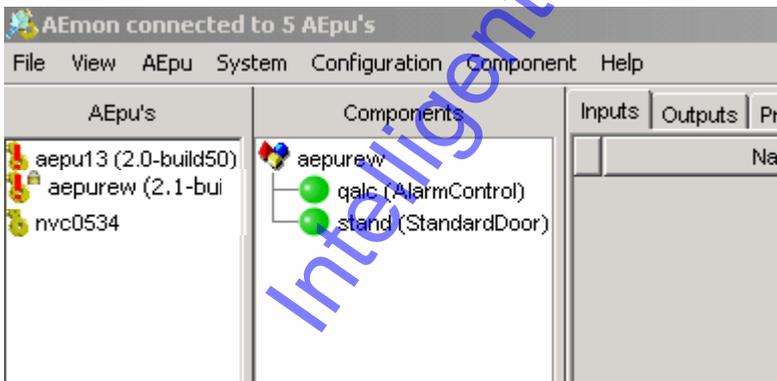
By using right mouse button on an AEPu (or at *AEPu – Properties – Lookup services*), the Lookup services for this AEPu can be checked and changed



Attention: Be careful with changing the lookup services, this may only be done by qualified personnel.

6.1.3. AEPu information

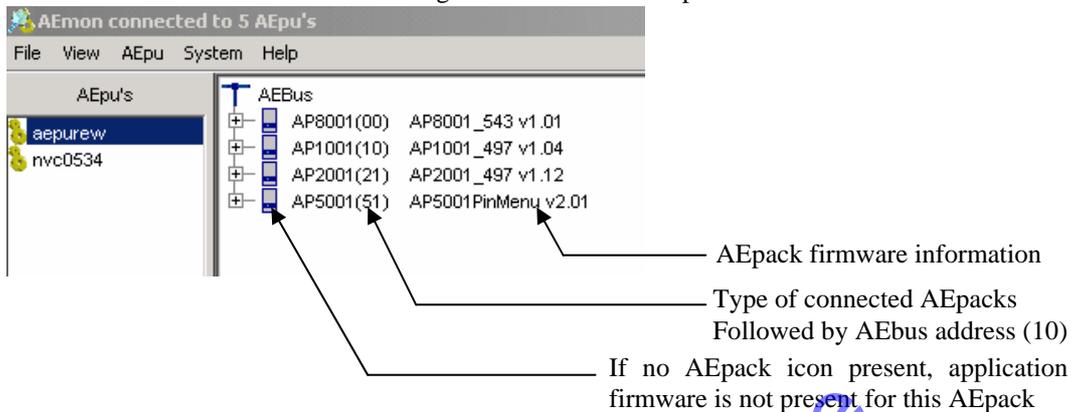
In the left all available AEPu's (as seen by the lookup servers and those manually added) are shown. If the AEPu version is unequal to the AEMON version this will be shown (!)



At above figure the above AEPu **aepu13 (2.0-build50)** has a different version of the software than AEMON (AEPu has 2.0 build50, AEMON can be checked at Help). At all locations the software version must be equal ! AEPu **aepurew (2.1-bui)** is locked, you have first log in to this AEPu to retrieve his data.

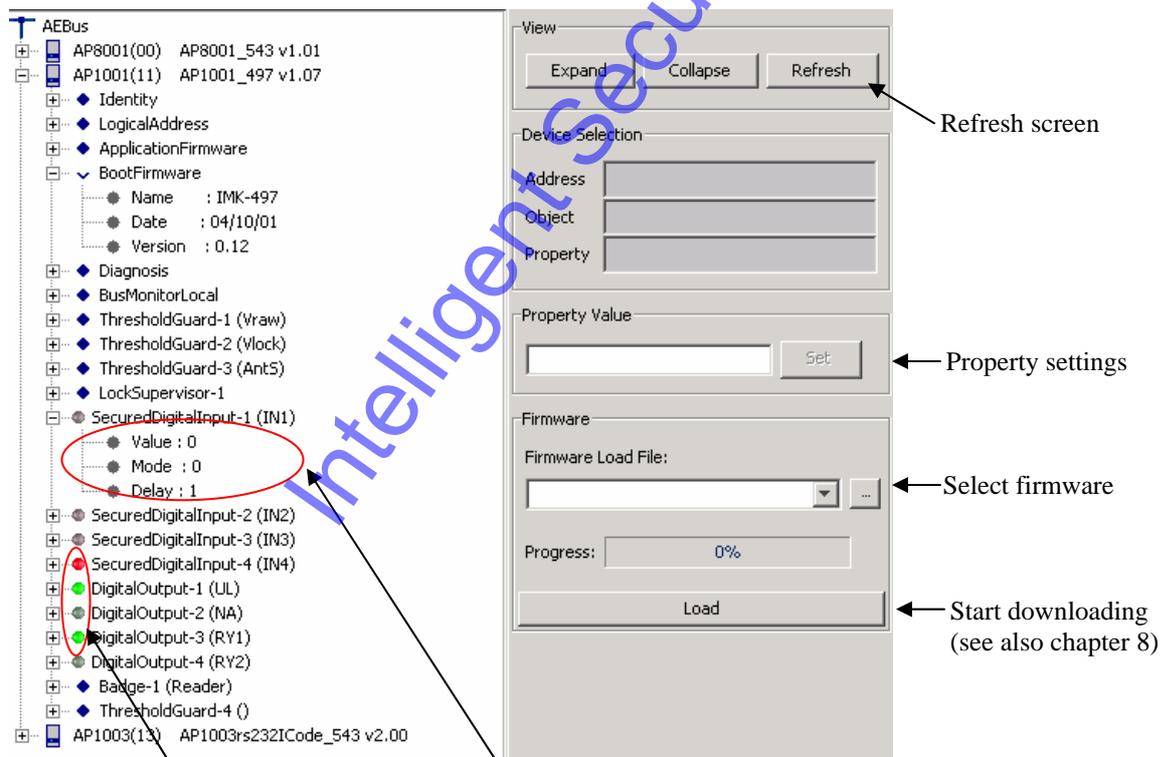
6.2. Check connected hardware

- *View – Hardware* (use F3 key)
Shows the connected hardware including addresses on this AEpu.



By expanding the AEPacks (click on +) more information is given. For each AEPack their characteristics and corresponding settings are given. The right part of the screen is used to change these settings. See figure below. E.g.:

- **ApplicationFirmware:** Firmware (name, version, state) of this AEPack. New firmware can now also be loaded.
- **BootFirmware:** Firmware (name, version, state) of the bootstrapper.
- All other items are for certified personal only, and are not discussed here. (You can always open them, but never try to change these, only if told so by Nedap Groenlo)



Detailed information about property
Status inputs / outputs (identical as on AEPacks: (use *Refresh* button))

- Green: Passive / output activated
- Red: Active
- Orange: Sabotage
- Grey: Not used

6.3. Detailed hardware settings

Attention: Never change these settings, only if asked for by qualified personal

At **Inputs** (SecuredDigitalInputs) following information is given: (also represented with colours)

- Value: 0: Input is passive
1: Input is active
- Mode: 0: Normally closed
1: Normally open
2: Secured Normally closed
3: Secured Normally open
- Delay Debounce value

Remark: Value 0 or 1 represents status of this input. If input is closed and the setting of this input (mode) is Normally closed, than his status will be passive.

At above situation IN1 is at hardware level (physical input) closed, IN2 is open.

At **Outputs** (Digital Outputs) following information is given: (also represented with colours)

- State: 0: Output is passive
255: Output is continuous active
1-254: Output is active during this time (x 100 msec)
- Behaviour: 0: Normal
1: Blinking rate

6.4. Configure the AEpu

View – Configuration (use F1 key)

Default view is the classic view; you can change to the graphical mode by *View – Graphical mode*. (see also 6.6)

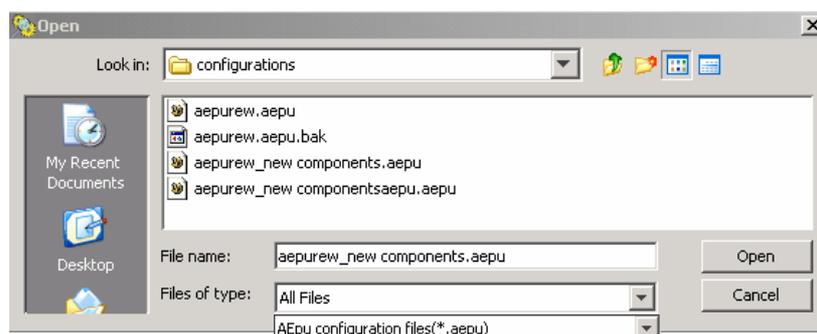
Each AEpu must know what action it must perform and how inputs and outputs are linked to an AEbc. This is done in the configuration part of AEmon. Here you can add and change components (AEbc's) and deploy them. More information about the AEbc's can be found in the corresponding *AEbc manuals*.

For generating a configuration on an AEpu following actions must be taken:

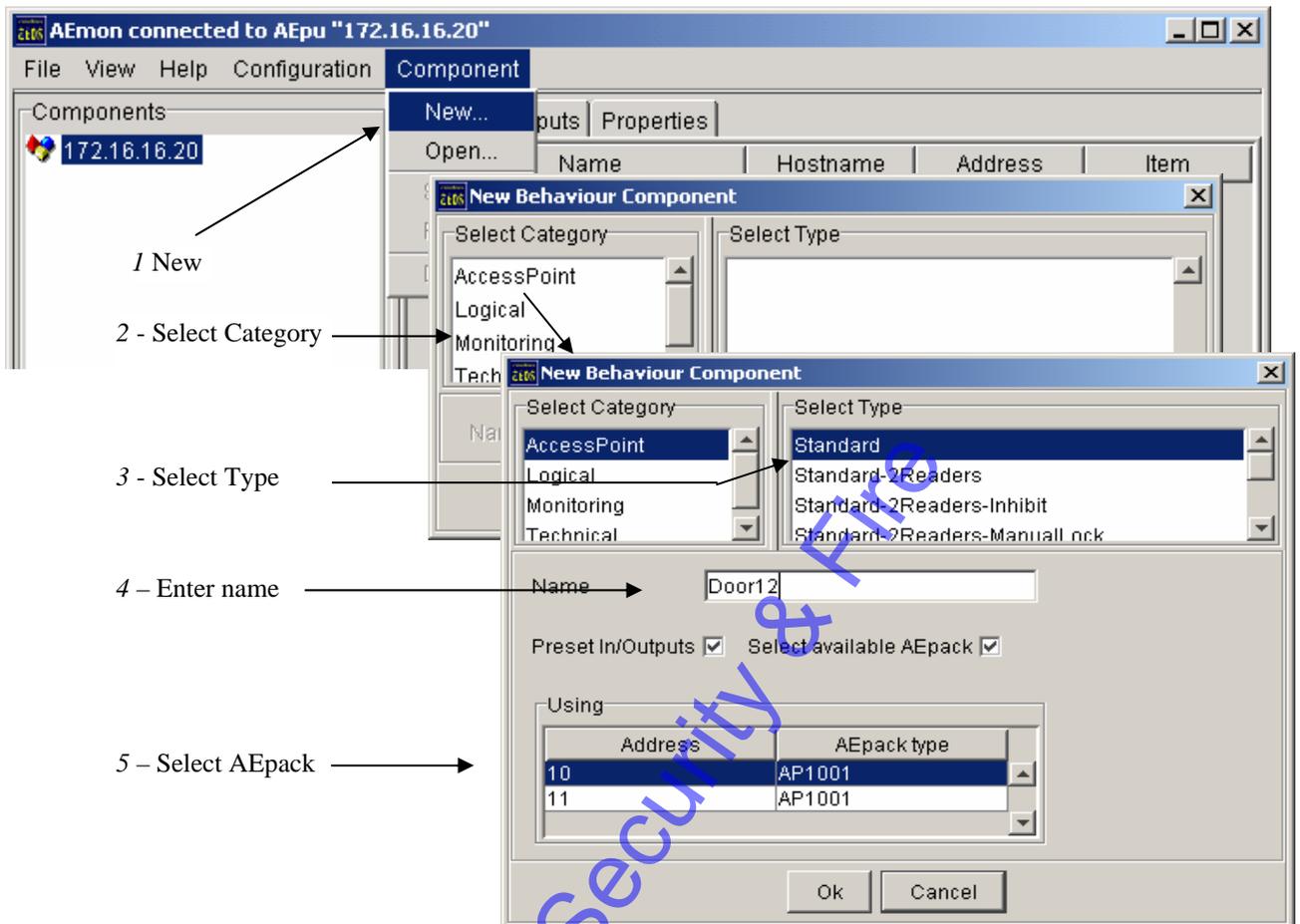
- Select the AEpu
- Select at Components New
- Select Category of AEbc and AEbc type
- Use if necessary Presettings and select available AEpac
- AEbc is now added at AEmon, settings can be changed
- Deploy AEbc to AEpu, AEbc is now active on AEpu

An configuration is after been deployed saved on the AEpu, and can also been saved on disk as backup (*View – Configuration – Save*)

If the configuration is saved automatically (see *Prereferences*), AEmon makes also a back up of the 'old' configuration file. At the *configurations* directory you can select only the *AEpu configuration files (*.aepu)* or *All files*. The latest shows also the *.bak* files



AEmon will for each selected component check the hardware for corresponding AEPacks



After selecting *Component – New* a new box appears on which following selections can be made:

- *Select Category* The behaviour components have been divided into different categories
- *Select Type* Depending on the software version various behaviour components can be selected
- *Name* Give a logical name to this behaviour component (e.g. Front Door)
This name is later on presented in AEOS frontend
- *Preset In/Outputs* Must all settings of this behaviour component be default or not. If not all settings must be made manually (default then all settings are 'Not Defined')
- *Select available AEPacks* If selected the available AEPacks connected to this AEpu are shown when online. Otherwise address and AEPack type must be set manually.
- *Address* The logic address as set on the AEPack
- *AEPack type* The correct type of AEPack

Use the OK button to add the new behaviour component. Now the Inputs, Outputs and Properties can be changed. Are all settings correct, than the AEbc(s) can be deployed. During deployment AEmon checks if there are any inconsistencies on Inputs or Outputs for this AEpu.

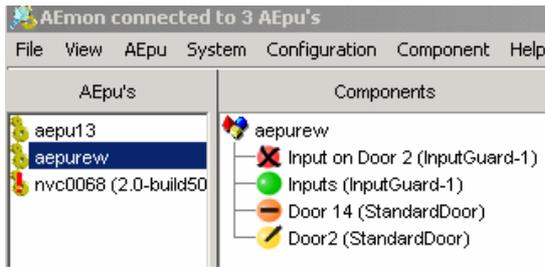
Attention: The OK button is only active if all needed data for this behaviour component is filled in.

If AEpu is not online the available AEPacks are not shown (*Select available AEPacks* is OFF).

Not all components have presets available. In this case the *Preset In/Outputs* is OFF.

Now the new behaviour components are added in the left screen, in front an icon is representing their status:

-  Orange: Component added, but not deployed
-  Green: Component deployed
-  Yellow: Changes made on deployed component and not newly deployed
-  Red: Component deleted at AEmon, but not yet deployed



At normal situation all components should be deployed. Deployed means that the information from AEMON is transferred to the AEPU.

6.4.1. Deploy configuration over more than one AEPU

System – Batch processing
 Select option: *Deploy configuration*.

With this option you can deploy an existing (or pre-defined) configuration over all (or using the filtering some) AEPU's. Depending on the selected option you can *Add to each AEPU configuration* or erase the current configuration.

Attention: If *Rename Components* is used (before adding the to be added components can be renamed), be sure that after renaming an *Enter* has been given.,

6.5. Changing default values of a behaviour component

After adding a behaviour component several settings can be changed, using the right part of the AEMON screen. Select the component on the left side and the tab with properties on the right side. The default values are shown.

The main screenshot shows the 'Properties' tab for the 'Door2 (StandardDoor)' component. It contains a table with the following data:

Name	Hostname	Address	Item	
Unlock	localhost	12	AP1001.RY1	1
Unlock Indication	localhost	12	AP1001.UL	
Not Authorized Indication	localhost	12	AP1001.NA	
Not Authorized	localhost	12	AP1001.RY2	

Annotations point to various parts of the interface:

- AEPU name**: Points to 'aepurew' in the Components list.
- Icon about status of information**: Points to the colored icons next to the component names.
- Select binding**: Points to the 'Inputs' tab.
- Characteristics**: Points to the 'Name' column in the table.
- Select Item (online-)**: Points to the 'Item' column.
- Binding**: Points to the 'Address' column.
- Component(s) linked to this output**: Points to the 'Utilized' column.

Two smaller windows are shown below:

- Change Output Binding aepurew.Door2.Unlock Indication**: Shows a table with 'Current' and 'New' sections. The 'Current' section shows 'localhost (aepurew)' with address '12', type 'AP1001', and detail 'UL'. The 'New' section has a 'Component' tab with a list of items.
- Select Item**: A dialog box with 'AEPack Type' set to 'AP1002' and 'Detail' set to 'Reader-1'.

Additional annotations for the 'Change Output Binding' window:

- Free item**: Points to the 'HF Disable' item in the 'New' list.
- Utilized=where used: click on button for more information**: Points to the 'Utilized' column in the 'New' list.

Remarks:

- AEpac information is only given if AEpu is **online**.
- For Output Bindings only hardware can be linked, for Input Bindings also Output or components can be linked (select *Hardware*)
- Bindings can be made locally or remote, by activating *List remote* and eventually enter a *Hostname filter pattern*, so that not all AEpu's are listed in the overview for the bindings.
- If inconsistencies are programmed, the amount of Utilized components is represented in **Red**

6.5.1. Bindings

A *Binding* represents the link between the logical input/output of a behaviour component and the hardware device (physical input/output). This physical input/output can be on the same AEpac, but also on another AEpac and even on an AEpac connected to another AEpu.

For more information see the *AEbc_UserManual*.

Bindings can only be changed as above when the AEpu is **online** (use button at front of binding). If AEpu is **offline** then the bindings can not be changed using above screen, but must be changed using the main screen (see aside). This is because there is no AEpac information available for AEmon (no AEpu's connected).

		Inputs	Outputs	Properties	
	Name	Hostname	Address	Item	
...	Unlock	localhost	12	AP1001.RY1	1
...	Unlock Indication	localhost	12	AP1001.UL	
...	NotAuthorized Indication	localhost	12	AP1001.NA	
...	NotAuthorized	localhost	12	AP1001.RY2	
...	Direct Door Alarm				

For each behaviour component specific characteristics can be changed. See the *AEbc manuals* for detailed information.

- *Inputs* and *Outputs*
 - *Name*: Description of variable
The hardware device is addressed by using the following variables:
 - *Hostname*: Name of the AEpu (can be local or any other AEpu in the network. Name or IP address must be given.)
 - *Address*: Logical address (set by the two rotating switches) of the AEpac this physical input/output is located. Can be also on another AEpac.
If during the configuration '*Preset*' is active, all addresses will be default filled in, otherwise they will be '*Not Defined*'.
It can occur that more output functions are present than outputs available, their variables are presented than as '*Not Defined*'.
 - *Item*: The physical input or output (hardware device) of this variable of the behaviour component
 - *Connected to component*: The last column represents the number of components linked to this output.
- *Properties*: Depending of the behaviour specific properties can be changed.
 - Properties can also be show by using CNTR – P on the selected AEbc.
 - Only the properties for those inputs been linked are shown. Properties of unused inputs are not shown

- Below the properties of a standard AccessPoint are given. In the column 'Value' the settings can be changed

The screenshot shows a software interface with a 'Properties' tab. A table lists various properties with their names, values, and units. An arrow points from the 'Nedap-XS badge' value in the 'Identifier type' row to a dialog box titled 'Identifier Type'. This dialog box shows a dropdown menu with options: XSBadge, WiegandBadge, OmronBadge, BarcodeBadge (highlighted), and MifareBadge. A second dialog box below it shows 'BarcodeBadge' selected, with fields for 'Length' (6), 'Starts at position' (0), and 'Count in digits' (unchecked).

Name	Value	Units
Identifier type	Nedap-XS badge	
Verifier type	No Verification	...
Unlock time	5000	ms
Minimum unlock time	500	ms
NotAuthorized time	3000	ms
Door open alarm time	20000	ms
Input contact debounce time	50	ms
Direct door alarm enabled	<input type="checkbox"/>	
Direction mode	0	0=None 1=In 2=Out
Registrate passage only when opening door	<input type="checkbox"/>	
Read badge while door is open	<input type="checkbox"/>	
Blocking time	0	s (0-32767)
Blocking time direction sensitive	<input type="checkbox"/>	
Door Opened normally closed	<input checked="" type="checkbox"/>	
Door Opened sabotage alarm enabled	<input type="checkbox"/>	
Door Opened state when binding fails	No Change	
Events enabled	...	
Test mode enabled	<input type="checkbox"/>	

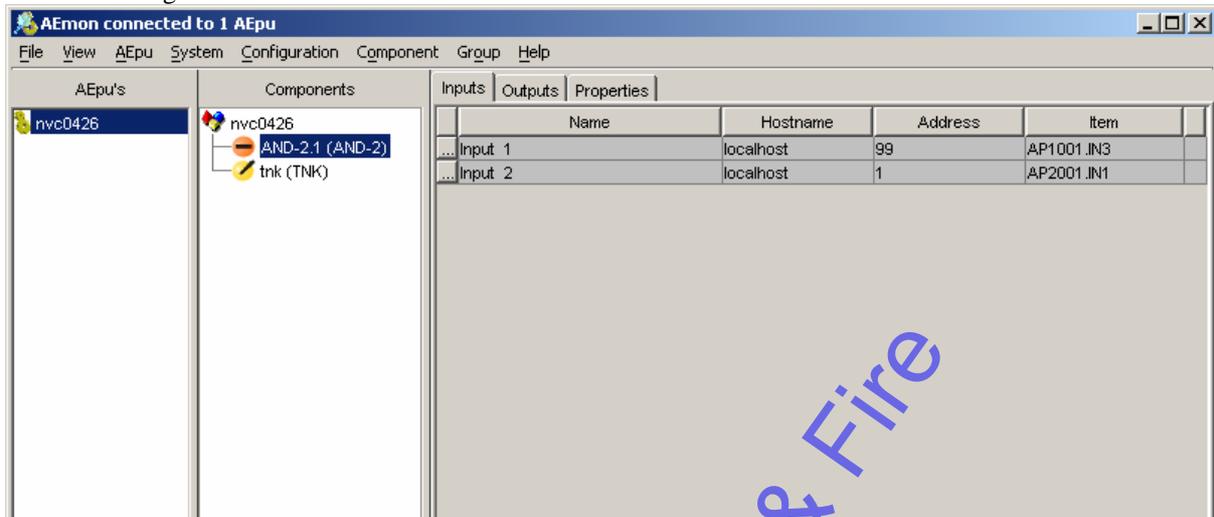
Specific points

- After changing one of more Properties, the changed Property is represented in **bold**. Using right mouse button allows you to undo this change. It is also possible to change more than one property at once and after that perform the deploy.
- At the left bottom of this screen the button *Apply to* can be selected to sent this changes to all or some selected AEbc's over all or some AEpu's
The deployment of the changed AEbc's is done automatically (if desired the current configuration can be saved before the deployment)
Only the **selected items** will be *Applied to* the selected AEpu's (so not the changed bold items)!
Selecting more than one Property can be done by clicking on the items and holding Shift button.
At the *Details* you can check which Properties are where changed.
- Identifier type: Which identifier must be read, for some identifiers the number of digits and the starting position must be filled in. Starting position 0 means from the first character.
The *Generic* Type can be freely defined, needs qualified personal to do so.
Attention: At AEOS the setting for the identifier **must** be corresponding AEmon.
- Door Opened Input Sabotage Alarm Enable: If secured inputs are connected (using double loop principle) the variable *xxx Sabotage Alarm Enable* must be *Yes*
- Test mode enabled During test time all presented badges will be valid. Starting / ending testmode will be reported to the AEservers. Test mode is limited to a timeout (on badge reading)

6.6. Configuring the AEpu using the graphical configuration editor

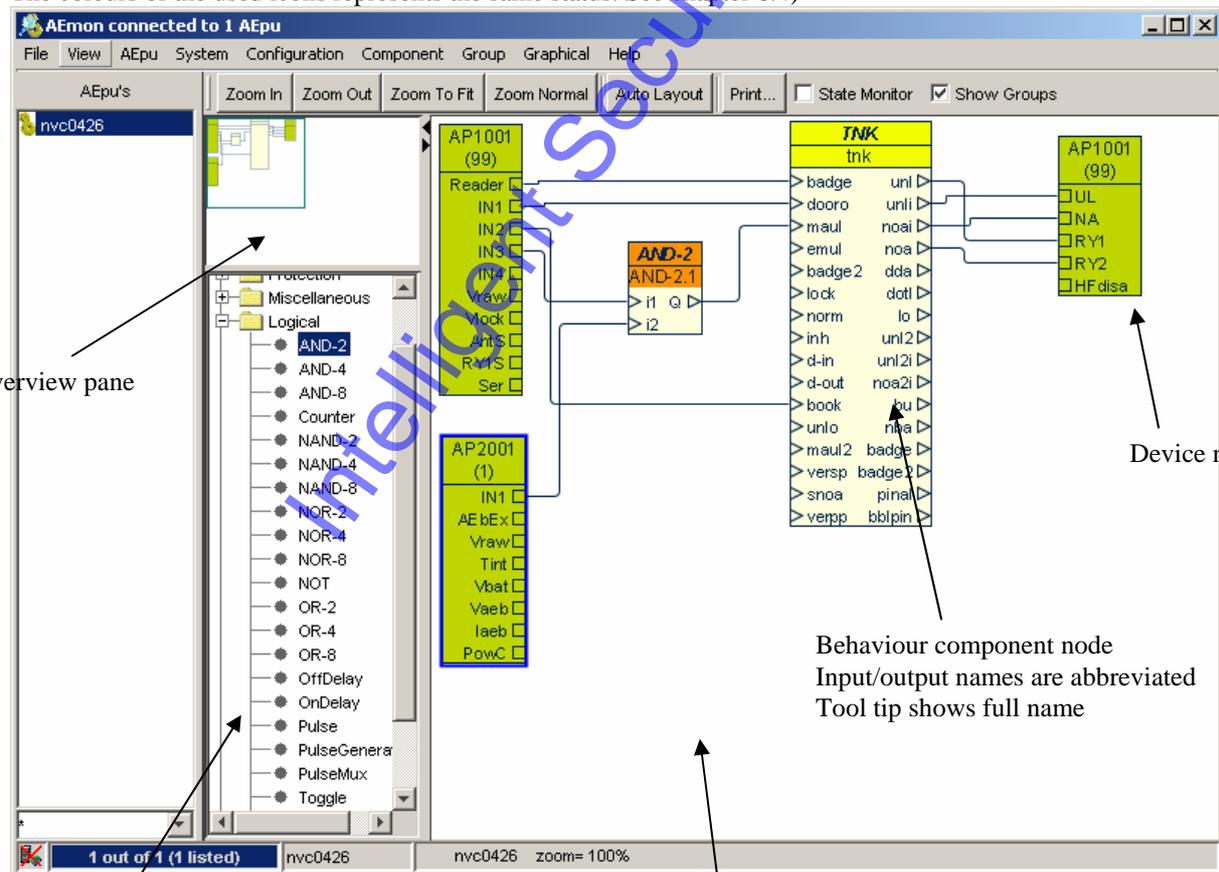
When the *View-Graphical mode* menu item has been selected the AEpu can be configured using the graphical editor. The following two screen shots show the difference between the standard and graphical editor:

Standard configuration editor



Graphical editor with same configuration.

The colours of the used icons represents the same status. See chapter 6.4)



Overview pane

Device node

Behaviour component node
Input/output names are abbreviated
Tool tip shows full name

Components/devices can be drag'n dropped into the editor panel

Editor pane

The graphical configuration representation consists of nodes which are connected to each other by links. Links represent the bindings as described in chapter 6.5.1 Changing a link (create, re-link or delete) will automatically change the bindings of the underlying behaviour component(s).

When a configuration is loaded into the editor for the first time, the nodes locations in the view are unknown and an automatic layout algorithm will be used to determine node locations.

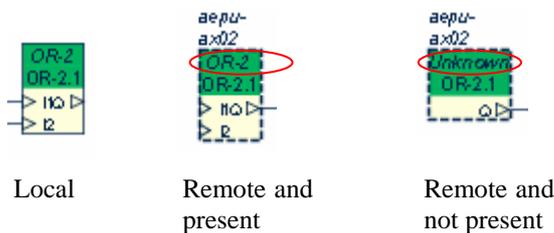
Graphical layout preserving is done by saving node locations. Layout of links will not be saved, links are always drawn automatically after node positioning and their layout depends on node positions and the defined layout type (see graphical options 6.6.2).

Node location are preserved in two ways:

- When an AEpu is selected the node locations are automatically saved/restored using a file named '[aepu-name].loc'
- When saving the configuration (*Configuration – Save*) the node locations are saved into the configuration file. When loading from file (*Configuration – Open – from File*) the saved locations are applied.

Behaviour component node

The colour of each node header {Green/Yellow/Orange/Red} corresponds with the icons described in chapter 6.4 and indicates the same status. A behaviour component can be either local (present on the selected AEpu) or remote (maybe present on another AEpu), this is shown as follows:



Local

Remote and present

Remote and not present

A link to a remote node can not be drawn directly, right clicking the port allows the user to open the well known *Change binding* dialog (chapter 6.5) and select a remote device or component.

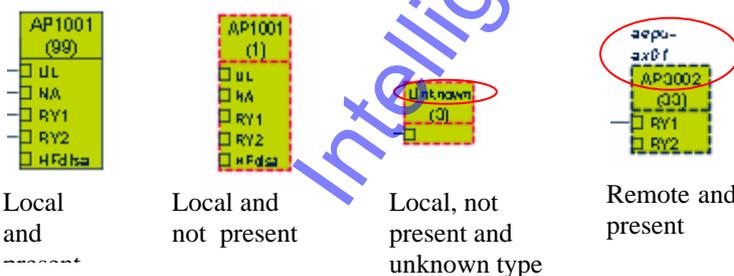
If working offline there are two ways to create a remote link:

- A remote device can be created by drag'n drop a device and then changing its host name by right clicking its node
- Switch to the standard editor, enter the host name manually and switch back to the graphical editor

A remote component is shown for clearness only, it can not be altered.

Device node

This node represents the input or output part of an AEPack and can have the following states:



Local and present

Local and not present

Local, not present and unknown type

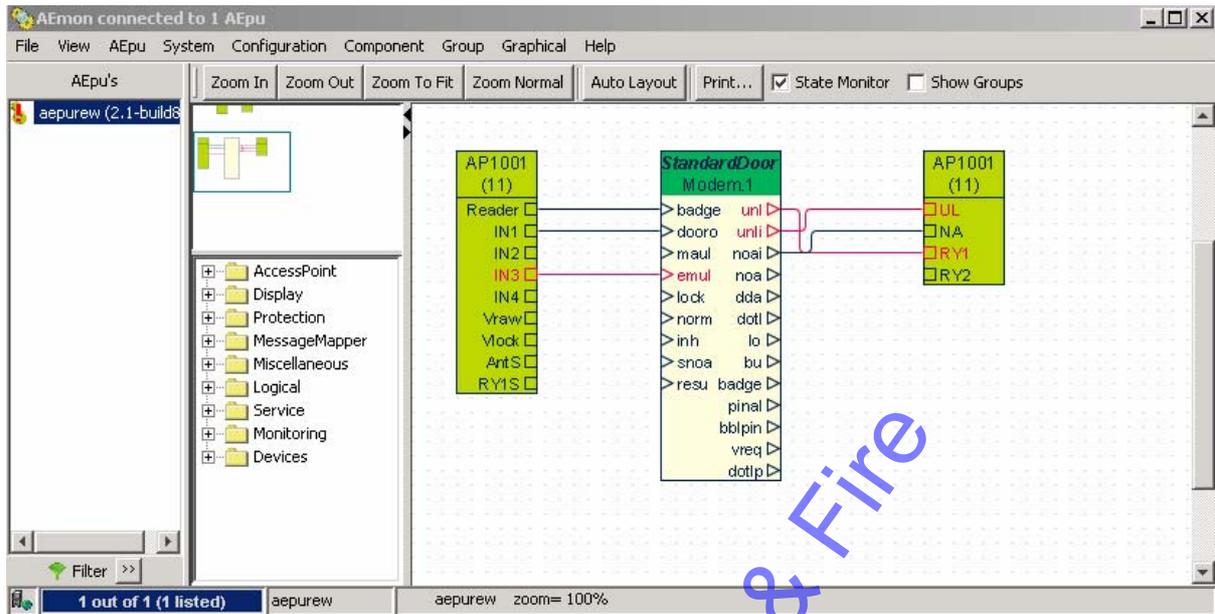
Remote and present

The device type can be unknown when a live AEpu configuration is retrieved from an AEpu and the addressed AEPack is not present in the AEpu.

Right clicking a device node allows the user to open a properties dialog where device address and host name can be changed.

6.6.1. State Monitor

The state monitor makes it possible to watch real-time logical state changes in a graphical way:



A logical '1' is indicated by a red link, a logic '0' by a dark blue line. The underlying mechanism makes use of the same AEpu events as the *View – Events* functions described in 7.3. For this reason this monitor function will take some AEpu performance!

! Only digital signals are monitored.

6.6.2. Options

The option dialog (*Graphical – Options*) contains the following options:

- Snap Grid
- Grid height and width
- Grid style: Invisible, Dots, Crosses or Lines
- Drags real-time, if enabled (=default) a node is really moved while dragged by the user. Whenever there is a matter of a performance problem (e.g. with very large configurations) it is advisable to disable this function.
- Orthogonal links, if enabled (=default) a link will consist of segments that are all either horizontal or vertical. Furthermore the algorithm will try to avoid crossing nodes or overlapping other links. When disabled a link only consists of two end-segments and straight line between them. Orthogonal links can take a lot of processor power specially in large configurations.
- Print scale

6.6.3. Printing

Beware that the both *Graphical – Print* and *Graphical – Print preview* functions are selection sensitive: if a part of the view has been selected only the selection will be printed, this is not indicated in the platform dependant Print dialog.

Please notice the Print scale option in *Graphical – Options*

6.7. Groups

A group is defined as a number of behaviour components, including all their property settings and graphical node positions.

A group is stored into library file 'groups.dat' and is identified by a user definable type string. An optional description can also be stored with the group.

Creating a group (graphical editor only)

By selecting components in the graphical editor and entering the *Group - Create* menu option. The loaded configuration will not be modified by creating a group.

Renaming/Deleting a group

Modify and delete options in the *Group - Organize* dialog

Apply a group

Using *Group - Apply* the user can insert a group into the configuration by selecting a group from the library and defining a group name.

Grouping implementation

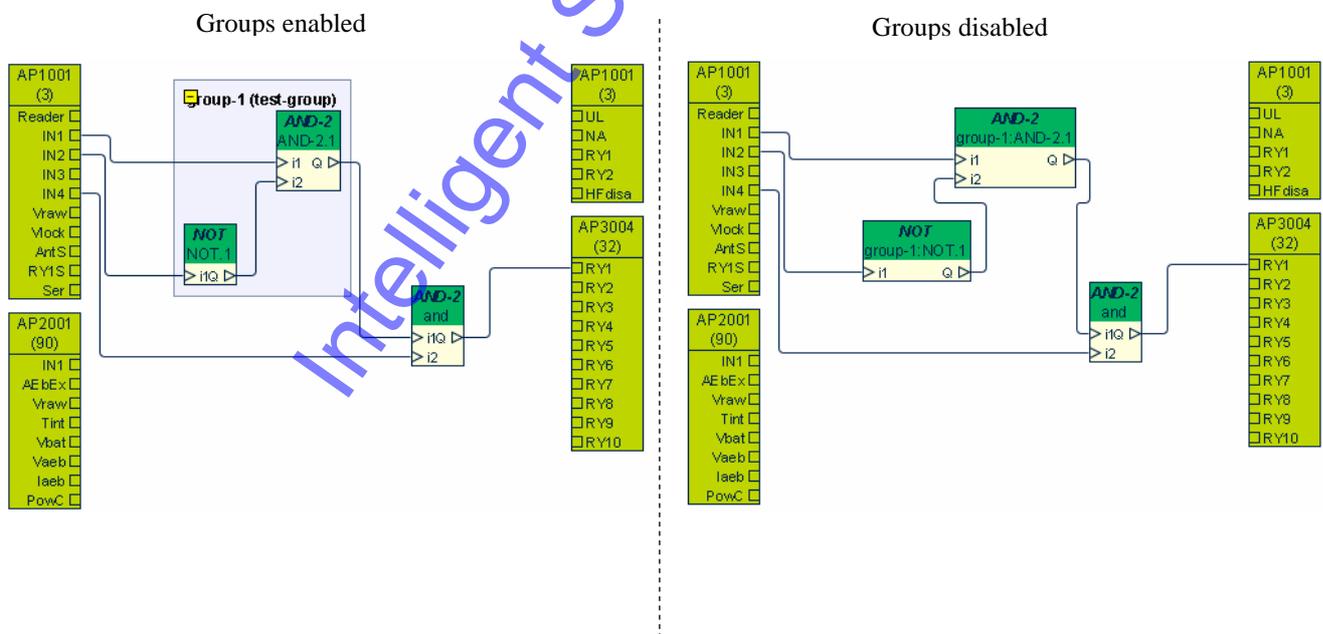
The grouping information is not explicitly stored¹ into the AEpu. This is realized by using a component naming convention, a component which is part of a group is always named as:

[group name]:[behaviour name]

In this way the AEmon is able to retrieve group information for an AEpu configuration. If the 'group type' is present in its library the corresponding graphical node positions can also be retrieved.

¹ Except the group type which is shown in the graphical editor which will be stored in the AEpu, if an AEpu does not contain the group type information it will not be displayed.

Graphical behaviour editor view with applied group (group name = group-1, group type = "test-group") and option 'Show Groups' enabled and also groups disabled.



7. LOGGING

The AEpu keeps a lot of debug information (logging data is stored in a buffer; first in first out). Logdata can be very useful in case of problems or to sent to Nedap to help understanding a specific problem. Also the AEpu logging can give some additional data about carriers detected at accesspoints.

7.1. AEmon logging

- *View - Programlog* (use F4 key) will give in a separate screen all logging of AEmon, with type of data, date, time and additional information.

Explanation:

- **Warnings** are represented in **green**
- **Errors** in **red**
- **Debug** information in **black**

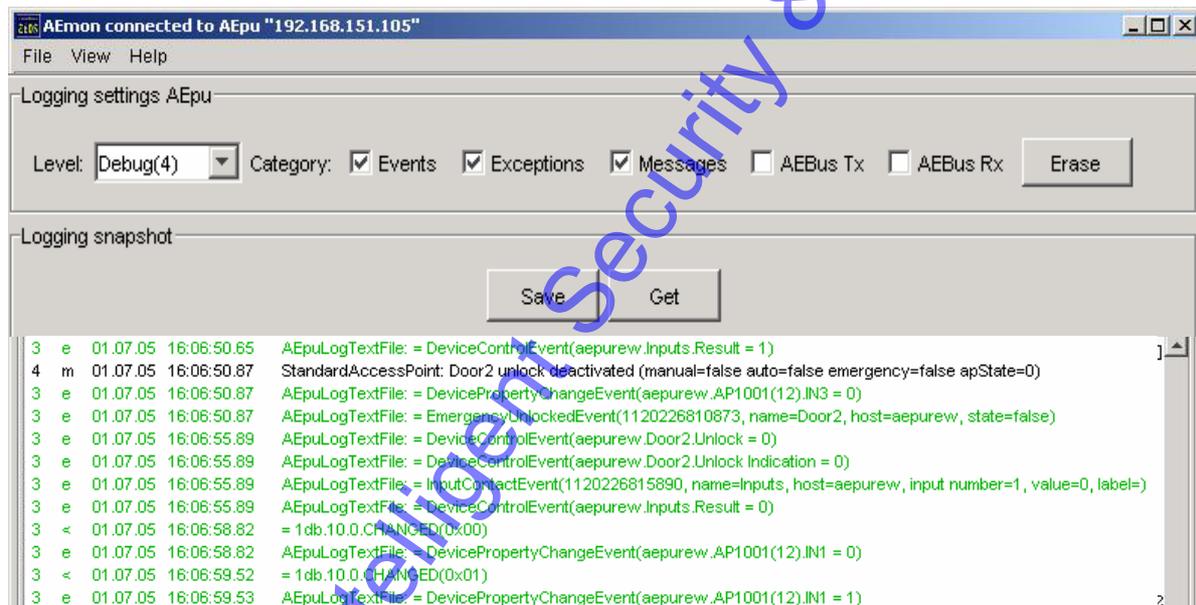
Saving the Program log can only by select all (Cntr All) and than Copy this data to e.g. Notepad.

Clearing the Program log: use right mouse button and select *Clear*

The logging data shown in the window is also written into file 'aemonlog'

7.2. AEpu logging

- Select the AEpu (*File - Connect*) and go to the logging screen (*View - Log*) (use F2 key)



↑ Date and time of message
 ↑ Type of logging record
 ↑ Debug level
 ↑ Additional information about this message

Explanation:

- *Debug level* 1: Error 2: Warning 3: Info 4: Debug
- *Date and time* Date and time of the AEpu, time up to 1 msec.
- *Type of logging record* m message
e event
x exception
> Bus signal towards AEpac
< Bus signal towards AEpu
- *Additional information* for each event gives more information about this event.

The log file is depending of the settings of the AEpu. To check the logfile use the button 'Get' and all data of the AEpu buffer will be shown. To get new data you always have to use the 'Get' button. Data is not been refreshed lively on screen. If new logging must be started use *Erase* to clean up the logging buffer of the AEpu.

Logged data can be saved locally on your PC using the 'Save' button.

Remark: Be aware the more options are activated the more data will be collected. E.g. Rx and Tx data can interferer with the correct timing of the AEpu (a lot of data has to be collected).

7.3. View events

View – Events

In a separate screen all events (all data over the AEBus and inside the AEpu) is real time displayed. Depending of the selected logging level some of this data is also shown at the AEpu logfile.

Attention: Opening this screen will take some performance of the AEpu!

```
1120220917755 InputContactEvent(1120220917755, name=Inputs, host=aepurew, input number=1, value=1, label=)
1120220917756 Inputs.Result = 1
1120220918386 AP1001(12).IN3 = 0
1120220918389 EmergencyUnlockedEvent(1120220918389, name=Door2, host=aepurew, state=false)
1120220923405 Door2.Unlock = 0
1120220923405 Door2.Unlock Indication = 0
1120220923406 InputContactEvent(1120220923406, name=Inputs, host=aepurew, input number=1, value=0, label=)
1120220923407 Inputs.Result = 0
```

Explanation:

- **Green** Outputs of components
- **Blue**: Hardware inputs
- **Red** Errors / infrastructure
- **Black**: Application events (are also sent to the AEs server)

Clearing the Events screen: use right mouse button and select *Clear* (this will not clear the AEpu log)

8. UPLOADING FIRMWARE

Beside the software on the AEpu (uploaded using upload scripts on the AEservers), which must be equal to the version of AEmon and the AEservers, also the AEpacks are equipped with firmware. This AEpack firmware is responsible for all communication between AEpack and AEpu.

The AEpack firmware is depending on:

- Type AEpack
- Type of application on this AEpack (for AP1003 each protocol has its own firmware)
- Type of uProcessor used at this AEpack (e.g. 496, 543)
- Type of kernel used at this AEpack (kernel with version 1 ('small') or with version 2 ('large'))
The kernel is the BIOS of the AEpack.

All above information can be checked at *View – Hardware* (see chapter 6.2)

The firmware is included with the AEOS CD, the latest version can be found on www.nedap.net

8.1. Naming of firmware.

General the AEpack firmware is build up as follows:

```

AP1003wieg32_543v202.mhx
AP1003                type AEpack
    wieg32            application indication (this is for wieg32 protocol)
        543          uProcessor
            v202     version of this firmware, version represents also the type of kernel
    
```

Other examples:

- AP1002_548v207.mhx AP1002 (Handsfree reader) version 2.07 for uProcessor type 548
- AP4007s09_543v200.mhx s09 indicates that this is customer specific firmware for AP4007
- AP2001_497v112.mhx AP2001 (Power Supply, version 1.12 for uProcessor type 497
- AP4003wieg37s04_543v202.mhx Customer specific firmware with wiegand37 protocol

Remark:

Use the latest version of software; in case of problems check www.nedap.net for changes on the firmware. The first part of the version number (e.g. v2.08) represents the used kernel.

- v2.xx Firmware is developed for 'large' kernel
- v1.xx Firmware is developed for 'small' kernel

8.2. Restrictions at loading firmware

Following restrictions must be taken in mind (AEmon checks on these points and gives a warning if incompatibility is detected):

1. Firmware must be corresponding the AEpack type (firmware for the AP1002 differs from e.g. AP1003)
2. Type of uProcessor must be identical
3. Version of firmware to be loaded is depending of used kernel
 - *AEpacks except AP4000 series:* Application version v1.xx can be loaded into AEpack with kernel version 1 and kernel version 2, application version v2.xx **may only** be loaded into kernel version 2

Kernel	Application version	
	v1.xx	V2.xx
v1.xx ('small')	Yes	No
v2.xx ('large')	Yes	Yes

- *AP4x00 series:* Applications with version v1.xx **may only** be loaded into AEpacks with kernel version 1.xx, applications with version 2.xx can be loaded into AEpacks with kernel version 1.xx and 2.xx

Kernel	Application version	
	v1.xx	V2.xx
v1.xx ('small')	Yes	Yes
v2.xx ('large')	No	Yes

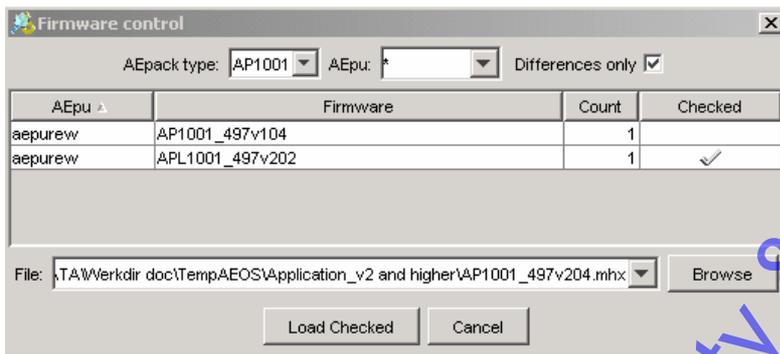
8.3. Loading new firmware

New firmware can be loaded using menu *View – Hardware* (see chapter 6.2): select the AEpack and the new application firmware (Firmware load file), use *Load* button to start downloading. The progress bar shows the status of the download process.

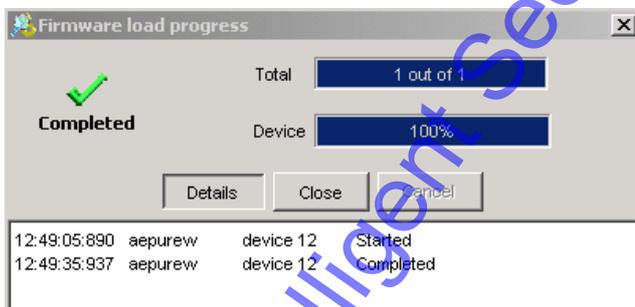
For selecting the firmware, default **only** the firmware suitable for this AEpack will be shown (otherwise select *All Files*).

At menu *System – Firmware control* all available AEpacks of one selected type (e.g. all AP1001's) known at AEmon are uploaded. This uploading goes simultaneously pro AEpu, thus saving a lot of time.

After selecting the AEpack and the firmware to be downloaded AEmon automatically checks if this firmware can be downloaded on the AEpacks following the firmware restrictions (see chapter 8.2). The result is given at column *Checked*. With *Load Checked* the firmware will be uploaded only to the *Checked* AEpacks.



A process bar will be shown; activating *Details* gives exact information which devices for which AEpu's are uploaded. Errors will be reported.

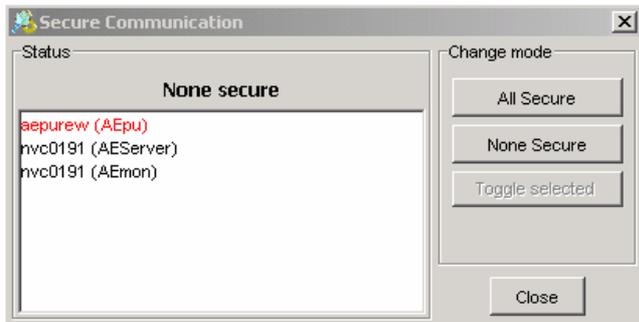


9. SECURE COMMUNICATION

More detailed information is described in the *AEOS Advanced Installation Manual*.
Communication between AEpu's and server can be made secure, using SSL.
During installation default SSL certificates are loaded.

Attention: This function may only be used by qualified AEOS personal. Incorrect usage can result that the devices cannot be reached any longer!

Using *System – Secure communication...* the communication can be toggled between *Secure* and *None Secure*.
(Setting to *None Secure* can only be activated if communication is already secure.)



If device name is in red, this device cannot be changed.

Intelligent Security & Fire

10. SYSTEM INFORMATION

Several information can be retrieved from AEmon, using reports. Reports can be saved on disk.

10.1. Configuration overview

At *Configuration – Report – Components* an overview of the complete configuration is reported (hardware bindings and properties of each AEbc)

Using *Component – Report* gives an overview for this single AEbc.

10.2. Used components

At *System – Report – Component Statistics* an overview is generated of all components (AEbc's) used on AEpu's connected to AEmon, as well as a totalization over all AEpu's.

10.3. What hardware is used

At *System – Show – Hardware utilization* all available and used hardware inputs and outputs are shown, also the amount of inputs that are still free.

Selections can be made pro hardware type and AEpu name (using filtering)

10.4. Remote bindings

At *System – Report – Remote bindings* an overview is generated of all remote bindings (connections to and from other AEpu's)

10.5. Check consistency

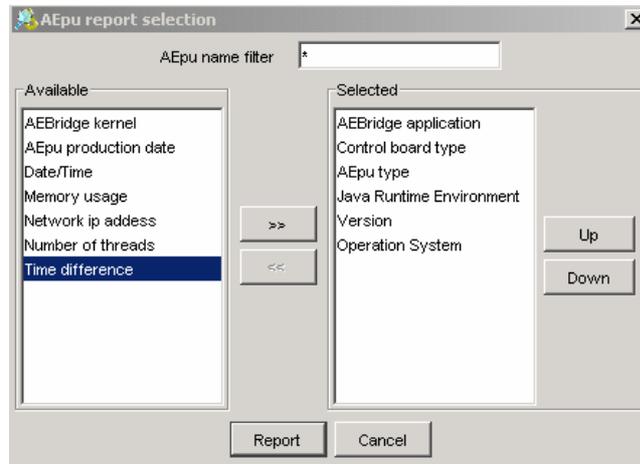
At *System – Report – Consistency* all AEpu's connected to AEmon are checked for inconsistent use of inputs and outputs.

With *Configuration – Report – Consistency* only the selected configuration is checked.

Intelligent Security & Fire

10.6. AEpu information, including date and time

At *System – Report – AEpu information* AEpu items can be selected from which the report must be generated:



- | | |
|---------------------------------------|--|
| • AEBridge kernel: | Kernel version of the AEpu |
| • AEBridge application: | Application version of the AEpu firmware (not the AEOS software version) |
| • AEpu production date: | Production date of this AEpu (Year code, month code, day) |
| • AEpu type: | e.g. AP8001, AP4801 |
| • Control board type: | e.g. 486, 586, PC |
| • Date/Time: | Date and time of the AEpu |
| • Time Difference: | Between AEpu and PC where AEmon is running |
| • Memory usage: | Total memory / free memory |
| • Network ip address: | e.g 192.168.1.1 |
| • Operating System: | Operating system of the AEpu including version number |
| • Version: | AEOS software version on this AEpu |
| • SSL supported: | Is SSL on this AEpu |
| • Jave Runtime Environment: | Only for Nedap developers |
| • Number of threads: | Only for Nedap developers |
| • Socket connection time-outs | Only for Nedap developers |
| • Socket read time-outs | Only for Nedap developers |
| • Socket failures | Only for Nedap developers |
| • Socket max connection time 24 hours | Only for Nedap developers |
| • Socket max connection time week | Only for Nedap developers |
| • Socket connection time counters | Only for Nedap developers |

11. TESTING PORT USAGE

For using this item, you need to know the aspects and differences of IP and TCP, port numbers and protocols. AEOS uses different ports. In some situations these ports can be used by another system or blocked by e.g. a firewall. For more information about the used ports check the *AEOS Advanced Installation Manual*.

For the more experience users it is also possible to perform these tests directly on the AEpu (e.g. using the secure shell), by using the command *portscan*

```
portscan [-verbose] [-route] <hostname> [<port>][:][<port>]...
```

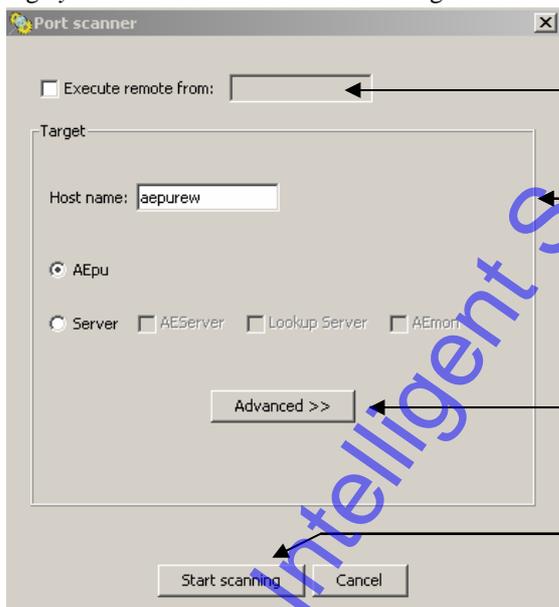
- *verbose* Gives additional information
- *route* Identical with AEMON port scanner, *Basic* mode = only IP connection
No - *route*: TCP connection is tested (*Advanced* mode)

There are two tests available:

- **Basic:** Test on IP level with fixed set of target ports.
If not correct you will see errors of *No route to host*
- **Advanced:** Test on IP or TCP level with user definable set of target ports, connect to application
If not correct you will see errors of *Connection refused*

This test can be executed locally, but also remote, so e.g. from AEMON to an AEpu, but also from the AEpu to AEMON (activate *Execute remote from*).

Using *System – Tools – Port scanner* will give next screen:



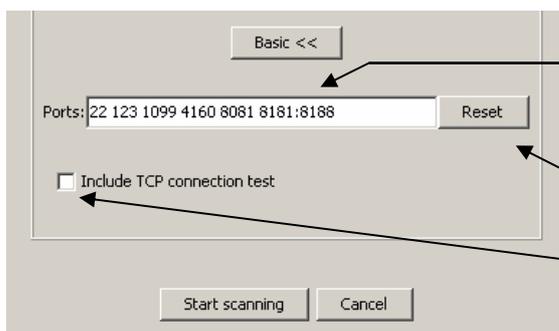
Execute test locally or remote. In this case it is executed locally from this PC (*nvc0191*)

Target information, to which device the connection must be checked.
Depending on the device the test will differ.

Basic Test fixed target ports
Advanced Test on user definable ports, optional also on TCP level, see below

Start test, a report will be generated with the results

Activating *Advanced* will give next addition:



Port numbers that must be tested.

- Ports are separated by spaces;
- Ranges are separated by :

In this case the tested ports are: 23, 123, 1099, 4160, 8081, 8181, 8182, 8183, 8184, 8185, 8186, 8187, 8188

Reset port numbers to default.

Check if applications at above ports can be reached at TCP level.

11.1. Testing ports from AEmon to AEpu

Settings as above

PC with AEmon (*nvc0191*)



AEpu (*aepurew*)



Result from Basic test

Result from Advanced test with *TCP connection test* activated

Scanning ports...			
Completed		13 out of 13	
21.02.07 16:49:51	aepurew	port 22	ok
21.02.07 16:49:52	aepurew	port 123	ok
21.02.07 16:49:52	aepurew	port 1099	ok
21.02.07 16:49:53	aepurew	port 4160	ok
21.02.07 16:49:53	aepurew	port 8081	ok
21.02.07 16:49:53	aepurew	port 8181	ok
21.02.07 16:49:53	aepurew	port 8182	ok
21.02.07 16:49:53	aepurew	port 8183	ok
21.02.07 16:49:53	aepurew	port 8184	ok
21.02.07 16:49:54	aepurew	port 8185	ok
21.02.07 16:49:55	aepurew	port 8186	ok
21.02.07 16:49:56	aepurew	port 8187	ok
21.02.07 16:49:56	aepurew	port 8188	ok

Scanning ports...			
Failed		13 out of 13	
21.02.07 16:51:43	aepurew	port 22	ok
21.02.07 16:51:44	aepurew	port 123	Connection refused: connect
21.02.07 16:51:44	aepurew	port 1099	ok
21.02.07 16:51:45	aepurew	port 4160	Connection refused: connect
21.02.07 16:51:45	aepurew	port 8081	ok
21.02.07 16:51:45	aepurew	port 8181	ok
21.02.07 16:51:45	aepurew	port 8182	ok
21.02.07 16:51:45	aepurew	port 8183	ok
21.02.07 16:51:45	aepurew	port 8184	ok
21.02.07 16:51:46	aepurew	port 8185	Connection refused: connect
21.02.07 16:51:47	aepurew	port 8186	Connection refused: connect
21.02.07 16:51:48	aepurew	port 8187	Connection refused: connect
21.02.07 16:51:48	aepurew	port 8188	ok

Remark: At the right screen (tested with *TCP connection test* activated) the red lines indicate that the failed are not used by this AEpu application.
 E.g. port 4160 is only used on an AEpu where a lookup service is deployed.
 Port 123 is used by the NTP process but uses UDP, so there is no TCP listener
 Ports 8185 – 8187 are not in use (there is a range specified, but this does not mean that they are all used).

Intelligent Security & Compliance

11.2. Testing ports from AEserver to AEpu

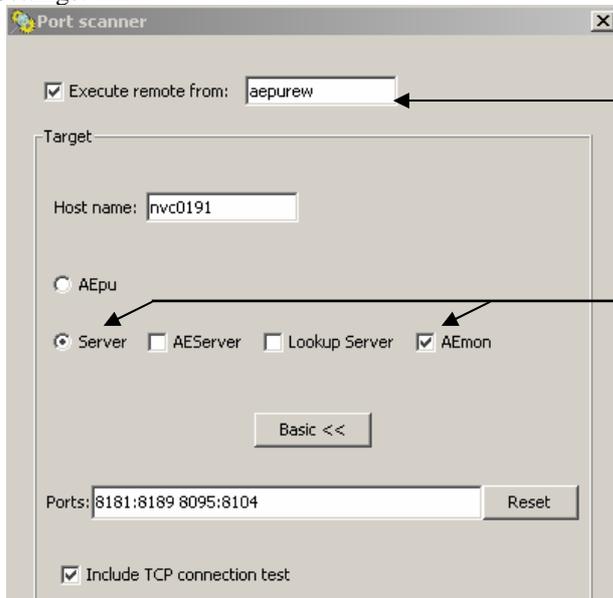
AEpu (*aepurew*)



PC with AEmon (*nvc0191*)



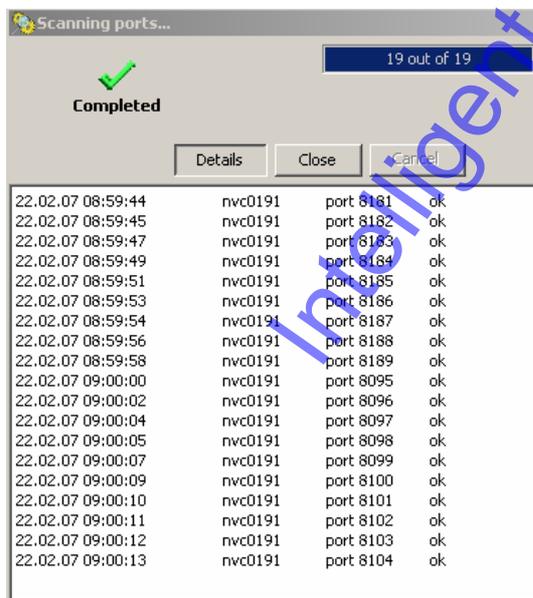
Settings:



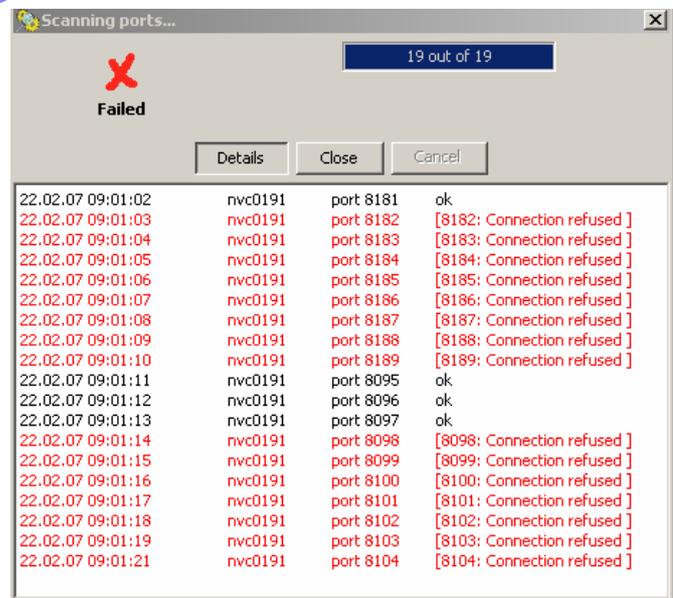
Test is performed from *aepurew*

Target is now the sserver (*nvc0191*) on which only AEmon is active, so only the ports for AEmon are tested.

Result from Basic test



Result from Advanced test with *TCP connection test* activated



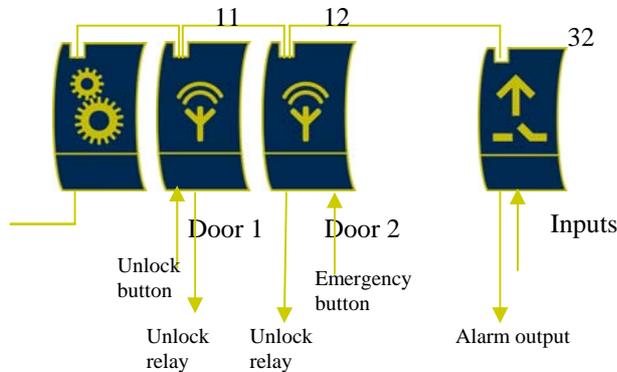
Remark: At the right screen (tested with *TCP connection test* activated) the red lines indicate that the failed are not used by this server application. Ports 8182 – 8189 and 8098 – 8104 are not in use (there is a range specified, but this does not mean that they are all used).

12. EXAMPLES

12.1. Standard Door with combined Emergency Unlock

For more information see also the *AEbc_UserManual*.

At the example below for Door 1 and Door 2 the Unlock Relay and Door Contact are default. The Emergency Unlock is connected to the second AP1001 (address 12), this emergency unlocks both Door 1 and Door 2.



From the default configuration the Emergency Input is deleted. It was for both doors at IN3.

Components		Inputs	Outputs	Properties	
		Name	Hostname	Address	Item
aepurew	Door1 (StandardDoor)	... Badge	localhost	11	AP1001.Reader-1
		... Door Opened	localhost	11	AP1001.IN1
		... Manual Unlock	localhost	11	AP1001.IN2
		... Emergency Unlock			
		... Lock			
		... Normal			
		... Inhibit			
		... Verification Serial Port			
		... Suppress NA			
		... Verification Pin Port			

To use one hardware (physical) input to two logical inputs, an InputAdapter has to be added. The Emergency Unlock is connected to AEpack 11 IN4:

Components		Inputs	Outputs	Properties	
		Name	Hostname	Address	Item
aepurew	EmUnl (InputAdapter)	... Input	localhost	11	AP1001.IN4
	Door1 (StandardDoor)				
	Door2 (StandardDoor)				

The Emergency Unlock from both doors is now connected to the Output of the Input Adapter (at *Change input bindings* select tabblad *Component* and select the output of this InputAdapter)

Change Input Binding aepurew.Door1.Emergency Unlock				
Current				
Hostname	Address/Name	Type	Detail	Utilized
localhost (aepurew)	EmUnl	Miscellaneous:InputA...	Output	2
New				
Hardware Component				
<input type="checkbox"/> List remote				
Hostname	Address/Name	Type	Detail	Utilized
localhost (aepurew)	EmUnl	InputAdapter	Output	2
localhost (aepurew)	Door2	StandardDoor	Unlock	
localhost (aepurew)	Door2	StandardDoor	Unlock Indication	

At Door1 and Door2 now the Emergency Unlock is linked to the *Output* of component *EmUnl*

Components		Inputs	Outputs	Properties		
		Name	Hostname	Address	Item	
<ul style="list-style-type: none"> EmUnl (InputAdapter) Door1 (StandardDoor) Door2 (StandardDoor) 	...	Badge	localhost	11	AP1001_Reader-1	
	...	Door Opened	localhost	11	AP1001.IN1	
	...	Manual Unlock	localhost	11	AP1001.IN2	
	...	Emergency Unlock	localhost	EmUnl	Output	
	...	Lock				
	...	Normal				
	...					

The output of the input adapter is now linked to two other components; this is represented by the 2 at the last column. (When components it is not possible to link directly an Output to a Component. Linking to components can only be done from the input side.)

Components		Inputs	Outputs	Properties		
		Name	Hostname	Address	Item	
<ul style="list-style-type: none"> EmUnl (InputAdapter) Door1 (StandardDoor) Door2 (StandardDoor) 	...	Output				2
	...					

Remark: In above example all AEpacks are located at the same AEpu (localhost). If Inputs or Outputs from another AEpu (Hardware or Components) must be used, they can be selected at *Change input bindings* select *List Remote* and select the correct AEpu and Input or Output.

12.2. Generating an Alarm at Emergency Unlock using InputGuard

If at above configuration an relais must be activated as soon as the Emergency Unlock is activated, the Input Adapter can be replaced by an InputGuard. For this example, the Output of the InputGuard is linked to AP1001 12 Relays 2 to activate an external alarm. Also the InputGuard generated an Event.

Input for InputGuard is located at AP1001 12 IN4

Components		Inputs	Outputs	Properties		
		Name	Hostname	Address	Item	
<ul style="list-style-type: none"> EmergencyCheck (InputGuard-1) Door1 (StandardDoor) Door2 (StandardDoor) 	...	Input 1	localhost	11	AP1001.IN4	
	...	Inhibit				
	...					

Output for generating alarm is linked to AP1001-RY2, the component output is also linked to 2 other components.

Components		Inputs	Outputs	Properties		
		Name	Hostname	Address	Item	
<ul style="list-style-type: none"> EmergencyCheck (InputGuard-1) Door1 (StandardDoor) Door2 (StandardDoor) 	...	Result	localhost	12	AP1001.RY2	2
	...	Sabotaged				
	...					

At the doors the Emergency unlock is linked to the output (*Result*) of the InputGuard (*EmergencyCheck*):

Components		Inputs	Outputs	Properties		
		Name	Hostname	Address	Item	
<ul style="list-style-type: none"> EmergencyCheck (InputGuard-1) Door1 (StandardDoor) Door2 (StandardDoor) 	...	Badge	localhost	11	AP1001_Reader-1	
	...	Door Opened	localhost	11	AP1001.IN1	
	...	Manual Unlock	localhost	11	AP1001.IN2	
	...	Emergency Unlock	localhost	EmergencyCheck	Result	
	...					

12.3. InputGuard combinations

InputGuards can be used to generate alarmmessage and also hardware alarms. Default an InputGuard is deployed on a AP3002, but also inputs or outputs from other AEPacks can be used.

At the configuration below some inputs are used from the AP3002 (InputGuard-4 *FirstFloorWindows*), other from the AP1001 on which also AccessPoints are deployed (InputGuard-4 *FirstFloorDoors*)

Inputs for InputGuard on AP3002, Inhibit input is not used.

Components		Inputs	Outputs	Properties																								
		<table border="1"> <thead> <tr> <th>Name</th> <th>Hostname</th> <th>Address</th> <th>Item</th> </tr> </thead> <tbody> <tr> <td>... Input 1</td> <td>localhost</td> <td>32</td> <td>AP3002.IN1</td> </tr> <tr> <td>... Input 2</td> <td>localhost</td> <td>32</td> <td>AP3002.IN2</td> </tr> <tr> <td>... Input 3</td> <td>localhost</td> <td>32</td> <td>AP3002.IN3</td> </tr> <tr> <td>... Input 4</td> <td>localhost</td> <td>32</td> <td>AP3002.IN4</td> </tr> <tr> <td>... Inhibit</td> <td></td> <td></td> <td></td> </tr> </tbody> </table>			Name	Hostname	Address	Item	... Input 1	localhost	32	AP3002.IN1	... Input 2	localhost	32	AP3002.IN2	... Input 3	localhost	32	AP3002.IN3	... Input 4	localhost	32	AP3002.IN4	... Inhibit			
Name	Hostname	Address	Item																									
... Input 1	localhost	32	AP3002.IN1																									
... Input 2	localhost	32	AP3002.IN2																									
... Input 3	localhost	32	AP3002.IN3																									
... Input 4	localhost	32	AP3002.IN4																									
... Inhibit																												

Outputs for InputGuard on AP3002, both Result and Sabotaged are used.

Components		Inputs	Outputs	Properties												
		<table border="1"> <thead> <tr> <th>Name</th> <th>Hostname</th> <th>Address</th> <th>Item</th> </tr> </thead> <tbody> <tr> <td>... Result</td> <td>localhost</td> <td>32</td> <td>AP3002.RY1</td> </tr> <tr> <td>... Sabotaged</td> <td>localhost</td> <td>32</td> <td>AP3002.RY2</td> </tr> </tbody> </table>			Name	Hostname	Address	Item	... Result	localhost	32	AP3002.RY1	... Sabotaged	localhost	32	AP3002.RY2
Name	Hostname	Address	Item													
... Result	localhost	32	AP3002.RY1													
... Sabotaged	localhost	32	AP3002.RY2													

Properties: For inputs several settings can be made: Important is to check how the AEbc should act if the link to the hardware input fails: *Input status when binding fails* (important if other AEpu's AEPacks are used to link the input)

Components		Inputs	Outputs	Properties																								
		<table border="1"> <thead> <tr> <th>Name</th> <th>Value</th> <th>Units</th> </tr> </thead> <tbody> <tr> <td>Event Mode</td> <td>0</td> <td>0=all, 1=change,...</td> </tr> <tr> <td>Input Contact Debounce Time</td> <td>50</td> <td>ms</td> </tr> <tr> <td>Input 1 normally closed</td> <td><input type="checkbox"/></td> <td></td> </tr> <tr> <td>Input 1 sabotage alarm enabled</td> <td><input type="checkbox"/></td> <td></td> </tr> <tr> <td>Input 1 label</td> <td></td> <td></td> </tr> <tr> <td>Input 1 state when binding fails</td> <td>No Change</td> <td></td> </tr> <tr> <td>Input 2 normally closed</td> <td><input type="checkbox"/></td> <td></td> </tr> </tbody> </table>			Name	Value	Units	Event Mode	0	0=all, 1=change,...	Input Contact Debounce Time	50	ms	Input 1 normally closed	<input type="checkbox"/>		Input 1 sabotage alarm enabled	<input type="checkbox"/>		Input 1 label			Input 1 state when binding fails	No Change		Input 2 normally closed	<input type="checkbox"/>	
Name	Value	Units																										
Event Mode	0	0=all, 1=change,...																										
Input Contact Debounce Time	50	ms																										
Input 1 normally closed	<input type="checkbox"/>																											
Input 1 sabotage alarm enabled	<input type="checkbox"/>																											
Input 1 label																												
Input 1 state when binding fails	No Change																											
Input 2 normally closed	<input type="checkbox"/>																											

There is no need to use an input module (AP3002) for the InputGuard. The user is free to select any of the unused inputs for generating the alarms with the InputGuards. Above e.g. the free inputs of the AP1001 are used.

Components		Inputs	Outputs	Properties																								
		<table border="1"> <thead> <tr> <th>Name</th> <th>Hostname</th> <th>Address</th> <th>Item</th> </tr> </thead> <tbody> <tr> <td>... Input 1</td> <td>localhost</td> <td>10</td> <td>AP1001.IN3</td> </tr> <tr> <td>... Input 2</td> <td></td> <td></td> <td></td> </tr> <tr> <td>... Input 3</td> <td>localhost</td> <td>10</td> <td>AP1001.IN4</td> </tr> <tr> <td>... Input 4</td> <td></td> <td></td> <td></td> </tr> <tr> <td>... Inhibit</td> <td></td> <td></td> <td></td> </tr> </tbody> </table>			Name	Hostname	Address	Item	... Input 1	localhost	10	AP1001.IN3	... Input 2				... Input 3	localhost	10	AP1001.IN4	... Input 4				... Inhibit			
Name	Hostname	Address	Item																									
... Input 1	localhost	10	AP1001.IN3																									
... Input 2																												
... Input 3	localhost	10	AP1001.IN4																									
... Input 4																												
... Inhibit																												

13. HELPFUL HINTS

13.1. Right mouse button

At several positions the right mouse button can be used for some commands. Just try it. (e.g to deploy the configuration).

13.2. Saving data (configuration) to disk

Saving data to disk (Configuration – Open from file) makes it easy to copy a certain configuration to other AEpu's without adding all data.

Before changing the AEbc configuration you can also automatically let's AEmon save the configuration. (See *File – Preferences*) The existing configuration in this directory will be renamed to .aepu.bak.

13.3. AEpack addresses

We strongly advise to take the following hardware addresses on the AEpacks to make your system easier to maintain.

- Readers (AP1001, AP1005) 1 x (10 .. 19)
- Power Supply (AP2001, AP2003) 2 x (20 .. 29)
- Output / Input modules (AP3004, AP3002) 3 x (30 .. 39)

13.4. Expanding AEpack hardware information

Use the *Enter* key to expand / collapse the information on the screen (*View – Hardware*)

13.5. Configuring without having a connection

It's not needed to have a connection to the AEpu you want to configure. It's also possible to prepare all data without an AEpu and save the configuration to disk. If the AEpu later on is present, the configuration file can be deployed.

If the configuration is build, addresses have to add manually, there is no link to the hardware.

13.6. Automatic AEpu discovery

Using 'Automatic AEpu discovery' at the start screen of AEmon means that anywhere an Lookup server must be available (e.g. at the AEmon PC).

Lookup server present in network:

- Yes: Automatic AEpu discovery is possible
AEpu names and IP addresses must also be at the hosts file of the AEmon PC (and AEservers PC)
InterAEpu communication is possible
- No: Automatic AEpu discovery is NOT possible
Use AEpu names and IP addresses in hosts file of the AEmon PC
InterAEpu can be programmed, but not be tested (can only be used if the server is available)

13.7. Lookup services

Default the lookup service will be installed when installing the complete server. If a the lookup server must be installed, than choice 'Custom setup' and select AEmon and Jini and Java.

13.8. InterAEpu functionality

InterAEpu functionality is only possible if there is a Lookup server running. Also using InterAEpu can only be used with AEpu names, so no IP addresses may be used when configuring the InterAEpu functionality. (See also 'Automatic AEpu discovery' above)

AEpu's with are communicating with any other AEpu must be known on both sides. (using 'Config' or AEconf)

13.9. AEpu hosts file using AEconf

The AEpu hosts file is needed for InterAEpu functionality when no DHCP or DNS is available. With AEconf the hosts file of the server easily can be imported and distributed to the AEpu's.

13.10. AEpu hosts file distributing over all AEpu's

See also chapter 13.9. At above chapter is described how to load the hosts file to one AEpu.

Below the procedure (only for AEOS certified personal) is described how to distribute the hosts file over all (or a group selected) AEpu's at once, using *System – Update AEpu software*.

Procedure:

- Make correct *Hosts file*: Use e.g. AEdconf to get the hosts file from an AEpu. Check this hosts file to be sure it is correct.
- Make on the server (or PC where AEmon is running) at the upload directory the folder `\data\patch\etc` (complete path is `.\AEOS\scripts\upload\data\patch\etc`)
Default directory for upload: `C:\AEOS\scripts\upload`, see *Prereferences*.
- Place the before generated hosts file in this directory
- Go to *System – Update AEpu software*. Make a selection for which AEpu's (with AEpu groups) you want to upload this new hosts file.
- After activation of the *Start button* the upload process is activated.
- To activate the new hosts file, the AEpus now must be rebooted.

13.11. Rebooting AEpu using batch script

In some situations it can be necessary to reboot a amount of AEpu's (e.g. to activate the new loaded hosts file). Below procedure is only for AEOS certified personal.

- Make a report in AEmon (*System – Report – AEpu information*) with no items selected (move all items to the left side). You will now get a list of all AEpu's.
- Save this file
- Use e.g. notepad or another editor to add following data to each line:
`start plink -pw grolle root@aepunaam reboot`
- Save this file as a .bat file
- Use a dos prompt to execute this file (all AEpu's in this file will now reboot)

Intelligent Security & Fire

14. CONFIGURATION OF ACCESSPOINTS

To configure accesspoints in the AEservers the following actions must be taken:

14.1. Actions on AEmon

Add new AccessPoints using the AEmon and make all correct settings (including the properties). Most settings can be used as default.

After adding all Accesspoints for one AEpu, save the file on disk.

14.2. Actions on AEservers

- Go to *Config – view infrastructure*
At the left bottom a line is displayed *there are unconfirmed accesspoints* Click on this link and all by AEmon added Accesspoints will be shown.
- Activate (checkbox) the Accesspoints you want to add and click the *Add* button
- Go to *Maintain Entrances* to define the entrances

14.3. Deleting AccessPoints

Deleting AccessPoints at an AEpu which are already assigned at AEOS is not possible with AEmon. This restriction is necessary for the AEservers. If however AccessPoints must be deleted at the AEpu and you're sure no problems can occur at the AEservers, AEmon must be started with the '-e' option (*aemon.bat -e*). When an AccessPoint is now deleted an additional message is given and if you still want to delete this AccessPoint it now is possible.

Intelligent Security & Fire

15. FIRST TIME USE ON AESERVER

After installation of the software on the AEs server following steps are advised to be taken to use AEOS (see also the AEOS software):

- Add *Access points* as mentioned above (actions on AEmon and AEs server)
- Maintain *Day/time schedules*
 - Eventually maintain *Templates* (combination of day/time schedules and entrances)
- Announce employees
 - Chose template (or schedule and entrance)
 - Chose identifier type and number
 - Add / Modify employee

At chapter 15.1 you can find a very short instruction how to get AEOS operational, step by step.

This list below describes only in short how to get started with AEOS. For detailed information (and you will need that) check always the corresponding manuals:

- AEpack Installation sheets (e.g. AP1001_InstallSheet_E)
- AEOS Installation Manual_E
- AEmon AEconf User Manual_E
- AEOS Checklist (checklist for handling AEOS projects)
- Etc ...

If anywhere in this process problems arise, check the documentation if all is been correct installed and all actions have been correctly performed. Depending of the problem, but at AEmon with the *log* functions you can also get some additional information, and also the *server log* of AEOS can give additional information.

15.1. Short procedure how to get started with AEOS

1. Use the *AEOS Checklist* to be prepared

SERVER PART

2. Check if the server is according the specifications, depending of AEOS and the database both running on the same server or separate servers
3. Install SQL Database (or Oracle) (see *AEOS Installation Manual*)
Install the latest service packs for Windows and the database
4. Check correct working of the database.
For SQL: start the Query analyzer check if you can login with *sa* and corresponding password. If this is not working solve this first!
5. Don't install the USB (or parallel) hardware key (contains the unique license number) before AEOS is complete installed!
6. Install AEOS (see *AEOS Installation Manual*) from CD (use *setup.exe*)
If certain settings are not clear, leave them as default!
7. With AEOS 2.1 the USB drivers are automatically installed.
Version before AEOS 2.1: Install the sentinel drivers from CD
8. Place now the USB (or parallel) hardware key
9. Optional: Check at the server if the services are available and set to automatic (these services are automatically installed)
 - *AEOS Application service*
 - *AEOS Lookup service*
10. Reboot the server, depending of the server AEOS will be started at 2-5 minutes (check *server.log* to check if server is started)
11. User browser (<http://<pc-name>:8080>) to start up the AEOS user interface
12. If no login screen appears (or an error message), check the *server.log* for more information what could be wrong and solve this first.
13. If login is successful you now only get one menu option, for loading the license file.
Load the correct license file (corresponding to the hardware key).
Logout and login again for activating the license file. If the license file is correct loaded all menu options are now available.

HARDWARE PART

14. We assume all hardware (AEpacks antenna's, etc) are connected conform specifications (see *AEpack_Installation Sheet*)
15. Check hardware using the ALT (AEpack Local Test) mode. First repair any defects.

AECONF PART (Network settings)

16. Configure the network settings of the AEpu using AEconf and RS232 or Cross cable (instead of AEconf also Hyperterminal or putty can be used). (See *AEmon AEconf User Manual*)
17. Check if name of AEpu must be known at the server (*hosts file* if no DHCP / DNS is used)
18. Check IP connection between AEpu and server by
 - Opening dos box on server and execute *ping* to AEpu (ping <aepuname>, not the IP address)
 - Login to AEpu (use *putty*) and execute *ping* to the server (ping <servername>, not the IP address)Use ping with AEpu-name and server-name, not on IP address (AEOS is name-based!)

AEMON PART

19. Start up AEmon
20. If ping from both sides was ok, the AEpu must appear now at AEmon
21. Upload correct software version to this AEpu (see *AEmon AEconf User Manual*)
22. Configure the AccessPoint AEbc to this AEpu (see *AEmon AEconf User Manual*), connect for starting only the *badge input* and the *UNLock output* to the corresponding hardware

AESERVER PART, ISSUE BADGE

23. Check in AEOS if there is an *unconfirmed accesspoint*, with the name of the AccessPoint deployed before. Confirm this unconfirmed accesspoint.
24. Make an *Entrance* and link the before confirmed accesspoint to this Entrance (see *AEOS User Manual*)
25. Define the *Identifier type* to be used. The identifier type is depending of the cards to be read (see *AEOS User Manual*)
26. Define a *Day/Timezone* which is always valid: 24 hours, each day (e.g. a free period of 1 day which is valid form 00:00 to 00:00. (see *AEOS User Manual*)
27. Define a *Template* with the combination of the before defined Entrance and Day/Time schedule
28. Open the *Event Monitor* with filter *all events*
29. Present a badge to the antenna (and check if the ID-led on the AEpack blinks)
If the ID-led of the AEpack is not blinking than this first must be solved. No ID-led on the AEpack means that no data is received or understood by the AEpack.
30. Check at the *Event Monitor* if the message *Not authorized badge* with card type and card number is shown
If noting appears, the Event Monitor (AEOS) has no connection with the AEpu.
If an 'undefineable' string appears, the firmware of the AEpack could be wrong, or the Identifier type is not defined correctly.
31. Add a person (*Employee – new*) and give him access to this Entrance using the before defined *Template* with the correct badge number.
32. Present this badge to the antenna and check at the *Event Monitor* if the person name with *Authorized badge* is been shown
33. Now you're able to issue a badge, the rest can be done also.

16. MENU OVERVIEW

Below find a link to this manual where there items are described.

File

<i>Connections</i>	6
<i>Preferences</i>	4.1
<i>Exit</i>	

View

<i>Configuration (F1)</i>	6.4
<i>Log (F2)</i>	7.2
<i>Hardware (F3)</i>	6.2
<i>Graphical mode</i>	6.6
<i>Events</i>	7.3
<i>Program Log (F4)</i>	7.1

AEpu

<i>Properties</i>	
<i>Tags</i>	4.1
<i>Lookup services</i>	6.1
<i>Secure shell</i>	4.1
<i>Software update</i>	5

System

<i>Report</i>	
<i>Remote bindings</i>	10.4
<i>Component statistics</i>	10.2
<i>Consistency</i>	10.5
<i>AEpu information (CTRL+I)</i>	10.1
<i>Host name resolving</i>	4.1
<i>Show</i>	
<i>Hardware utilization</i>	10.3
<i>Tools</i>	
<i>Port scanner</i>	11
<i>Firmware control</i>	8
<i>Secure communication</i>	9
<i>Change AEpu password</i>	4.1
<i>Update AEpu software</i>	5
<i>Batch processing</i>	6.4.1, 13.10

Configuration

<i>New</i>	6.4
<i>Open</i>	
<i>from file</i>	6.4
<i>from AEpu</i>	6.4
<i>Close</i>	
<i>Save</i>	6.4
<i>Report</i>	
<i>Components</i>	10.1
<i>Consistency</i>	10.5
<i>Deploy (CTRL+E)</i>	

Component	
<i>New</i>	6.4
<i>Open</i>	
<i>Save</i>	
<i>Report</i>	10.1
<i>Copy (CTRL+C)</i>	
<i>Paste (CTRL+V)</i>	
<i>Rename</i>	
<i>Modify</i>	
<i>Delete (Delete)</i>	
<i>Properties (CTRL+P)</i>	
Group	6.7
<i>Create</i>	
<i>Organize</i>	
<i>Apply</i>	
Graphical	6.6
<i>Zoom in</i>	
<i>Zoom out</i>	
<i>Zoom to fit</i>	
<i>Zoom normal</i>	
<i>Auto layout</i>	
<i>Page setup</i>	
<i>Print preview</i>	
<i>Print</i>	
<i>Options</i>	
Log	
<i>Get (CTRL+G)</i>	7.2
<i>Save</i>	7.2
<i>Go to most recent</i>	7.2
Help	
<i>About</i>	

Intelligent Security & Fire

17. FILES AND DIRECTORIES

All files/directories listed created by AEmon are stored in directory [aeos install-dir]\scripts, so if the default install directory has been chosen this will be "c:\aeos\scripts"

Overview of all AEmon files/directories:

Item	Description
aemon.dat	Settings/options
aemonlog/aemonlog-i	Program log (max size 1Mbyte)
locators.dat	List of lookup servers
locators.dat.bup	List of lookup servers backup
groups.dat	Component group library
configurations	Default directory where configuration (*.aepu) files are stored
components	Default directory where component (*.aebc) files are stored
Firmware	Directory containing all AEpack firmware load files
logs	Default directory where log files are stored
[name].aepu	Saved configuration with optionally all associated graphical node locations
[name].aepu.bak	Backup file for previous saved configuration when using option 'Auto save configuration deployment' or executing Batch processing -> Save configuration
[name].aebc	Saved component
[aepu-name].loc	Graphical node locations for a particular AEpu

Intelligent Security & Fire