
CHAPTER 1 - INSTALLATION	3
1.1. GENERAL REQUIREMENTS	3
1.2. CONSISTENT INSTALLATION PROCESS	4
1.3. ADMINISTRATION SERVER SPECIFICS	7
1.4. CAMERA SERVER SPECIFICS	8
1.5. AFTER INSTALLATION	9
1.6. CONFIGURATION PARAMETERS OF THE ADMINISTRATION SERVER	10
1.7. CONFIGURATION PARAMETERS OF THE CAMERA SERVER	11
1.8. CONFIGURATION PARAMETERS OF THE CAMERA CLIENT	12
1.9. AUTOMATIC UPDATES	12
1.10. 32-BIT AND 64-BIT APPLICATION VERSIONS	13
1.11. MULTIPLE NETWORK ADAPTERS	14
1.12. MOBILE CLIENT INSTALLATION	15
1.13. WEB CLIENT AND SECURITY	16
1.14. NEURAL NETWORKS INSTALLATION	18
1.15. INSTALLING THE BROWSER COMPONENT	18
1.16. LICENSE PLATE RECOGNITION INSTALLATION	19
1.17. IPV6 COMPATIBILITY	20
CHAPTER 2 - STARTING UP FOR THE FIRST TIME	21
2.1. FIRST LOGIN AND PROVIDING THE LICENSE KEY	21
2.2. ATEAS ID INSTALLATION IDENTIFIER	26
2.3. CERTIFIED INSTALLATIONS	27
2.4. BASIC SETUP WIZARD	29
2.5. CUSTOM SERVER NAMES	31
2.6. VERSION INFORMATION	32
2.7. INFORMATION ABOUT PMA	34
2.8. OFFLINE LOGIN	35
2.9. APPLICATION MAIN MENU	36
2.10. APPLICATION AUTOMATIC STARTUP	37
2.11. SEARCHING, FILTERING AND SORTING THROUGHOUT THE APPLICATION	37
2.12. TERMINAL CLIENT ACCESS	38
2.13. PROTOCOLS	39



CHAPTER 3 - HELP	40
3.1. DOCUMENTATION AND HELP	40

Chapter 1 - Installation

1.1. General requirements

A Microsoft operating system is required to run ATEAS Security products. The entire ATEAS Security system installation is very simple and only takes several minutes. The installation requires you to be logged on as administrator under Windows. If required by the installer, .NET framework generation 4 needs to be installed with the minimum version of 4.6.1. The ATEAS Screen Recorder can cope with 4.0 version, which makes it possible to use it for older computers.

NOTE

In most cases the .NET framework will already be part of your operating system.

ATEAS Security system also comes with an automatic update engine. Downloading and installing the new administration server (ATEAS Administrator) directly from the client application is the only user action required. All other applications will be updated automatically.

Each edition of the ATEAS Security product requires the installation of three basic ATEAS Security applications:

1. ATEAS Security Administrator – ATEAS Security system server, central login to system or a central camera server and event management.
2. ATEAS Security Server – ATEAS Security camera server, communication with cameras or video servers. Responsible for video and audio stream management, recordings and event evaluation.
3. ATEAS Security Observer – client application, the only user interface application in the system. It provides full access to the system and its administration (completely adjusts the behavior of servers, cameras, recordings etc.).

Apart from these applications, several additional add-ons or components are offered, such as the ATEAS Screen Recorder application, emulating a camera on a standard computer, or the ATEAS Security LPR Engine for detecting vehicles license plates.

The START and HOME edition installs both server applications on a single computer. The client application can be installed to a location of your choice (on the same computer where both server

applications are installed). However, compared to the PROFESSIONAL edition, system access is limited to only two simultaneous accesses.

The PROFESSIONAL edition sees the ATEAS Security Administrator and ATEAS Security Server are generally installed on a camera system computer (server), where recording and event management will proceed. ATEAS Security Observer is then installed on a corresponding number of client workstations which will access the system.

The UNLIMITED edition installation is identical to the installation of the PROFESSIONAL edition, with the only difference being the ATEAS Server application can be installed on additional computers (servers), to which additional cameras or video servers can be connected.

1.2. Consistent installation process

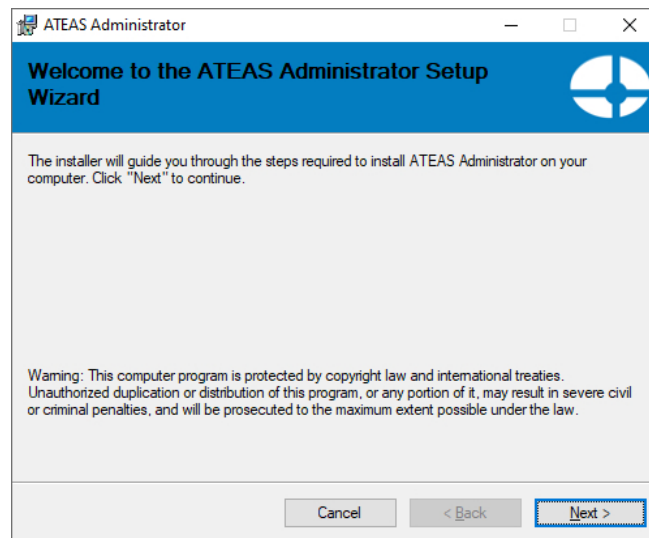
All three applications are installed identically using the same installation wizard. Links to the installation for all of these applications including other important links can be found directly on the page that automatically opens after inserting or connecting the installation media. The following links are available:

- first chapter of the product documentation on system installation,
- installing the system administration server,
- installing the system camera server (32-bit and 64-bit edition),
- installing the client application (32-bit and 64-bit edition),
- access to clients for iOS and Android in their respective stores (free),
- installing applications for computer monitoring.

Camera servers, client applications and all other applications can also be installed using the administration server web page. Compared to the links that are directly on the installation media home page, this page also contains links to important documents, complete product documentation in print quality and an ATEAS API demo application.

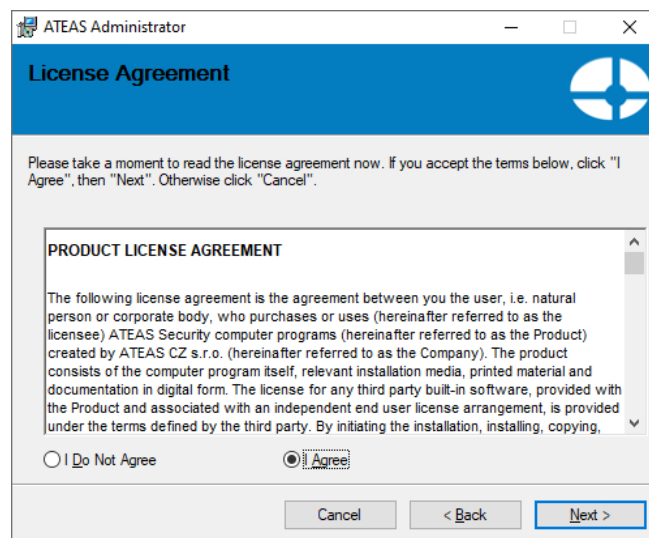
All three applications can be installed in any order. Now, we will go through the ATEAS Security Administrator installation process. The installation process of the two other applications is completely identical to this installation with only a few minor differences, described further in this chapter.

Step 1 – Installer welcome screen.



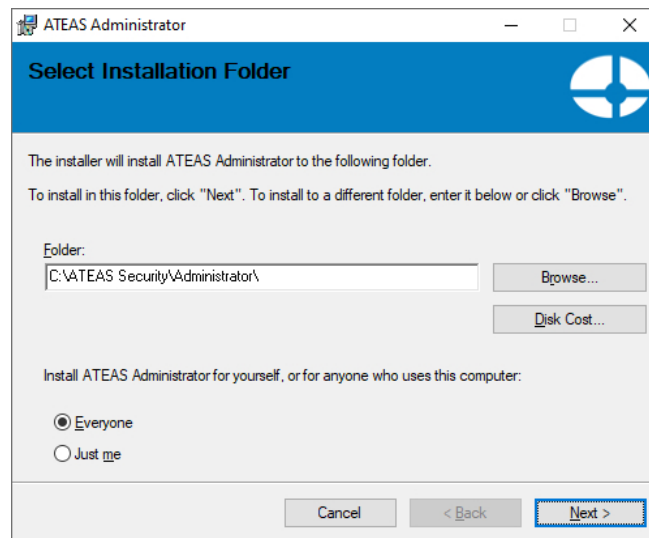
Continue installation by pressing the **NEXT** button.

Step 2 – License agreement.



Check the I agree radio button and continue with installation by pressing the **NEXT** button.

Step 3 – Installation folder selection.



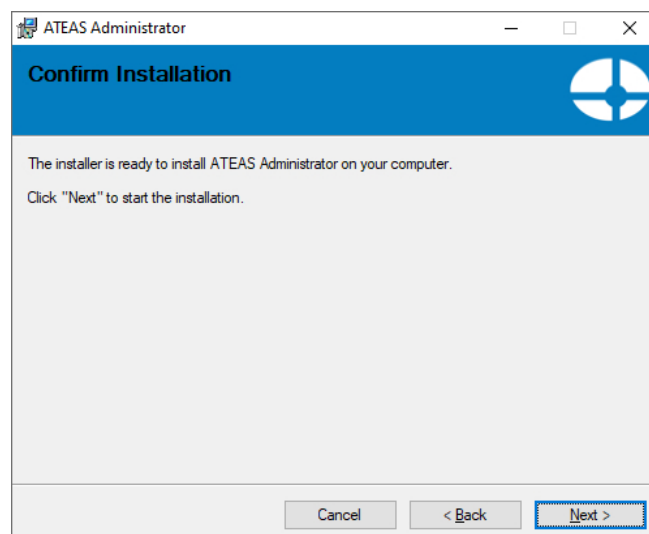
CAUTION

If you wish to make the ATEAS Security software available to all Windows users (this refers mainly to the client application), check the Everyone radio button.

This part of the installation requires selecting a destination folder, where the application shall be installed. Changing the hard drive can be easily accomplished by re-writing the beginning letter in the text field labeled Folder.

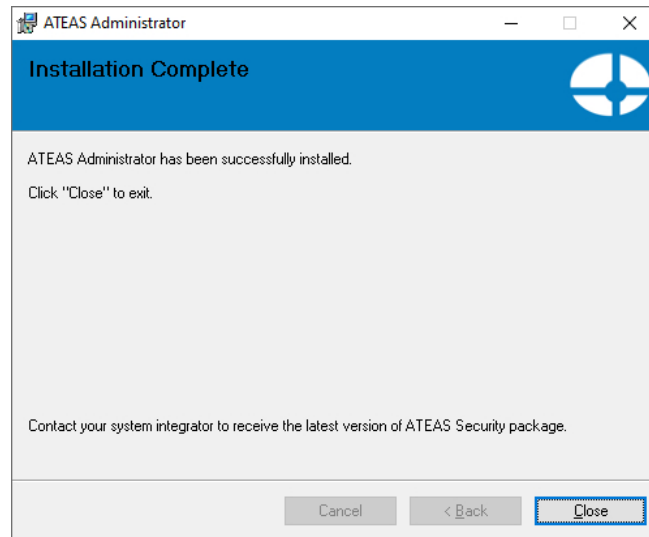
Continue the installation by pressing the **NEXT** button.

Step 4 – Installation confirmation.



Continue the installation by pressing the **NEXT** button.

Step 5 – Finishing installation.



The Installation is finished by pressing the **CLOSE** button.

1.3. Administration server specifics

When installing the administration server, an additional dialog appears before the start of the installation process, informing the user that if you are upgrading an existing installation the system cannot be activated if no ATEAS PMA service is active. Make sure that the ATEAS PMA service has been activated for the respective ATEAS ID before starting the installation process on an existing installation.

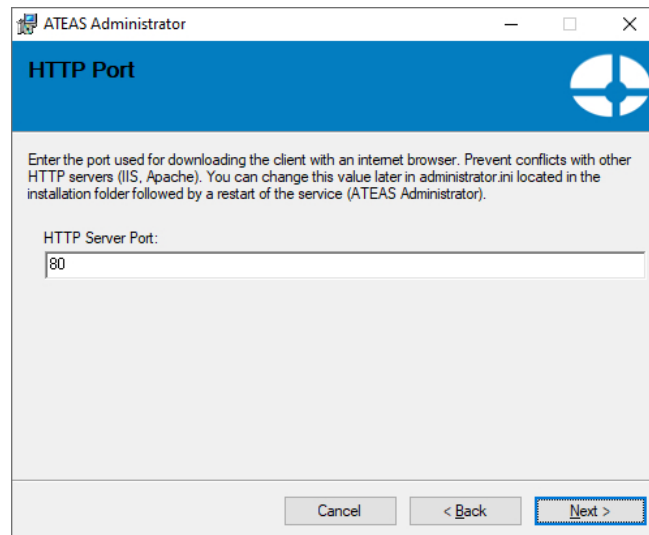
NOTE

In the START edition, new versions of the product can be installed without any restrictions.

A dialog box will appear during the administration server installation, where the user can enter a numerical value for the designated HTTP port, used by the administration server for communicating with web browsers. Both control or data communication ports are listed in the appendix. Nevertheless, a client application can be easily installed or downloaded from a web browser; therefore a CD is not required.

NOTE

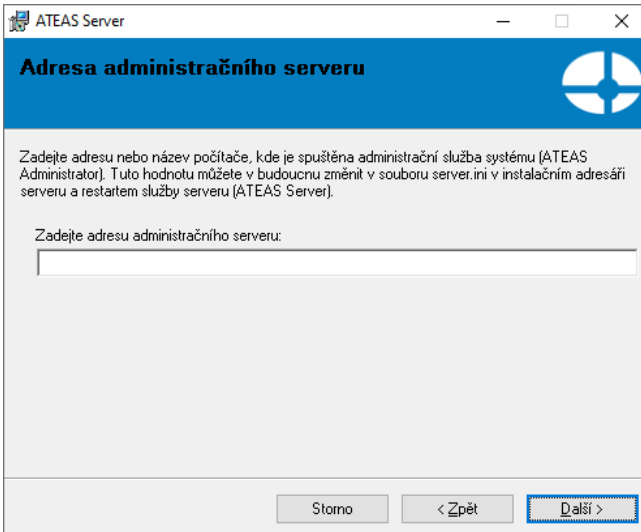
A camera server can be also downloaded or installed from a web browser. However, only an administrator can add a new camera server to the system.



The default value of the HTTP port is set to 80. In this case, the administration server can be accessed from the web browser using its address, e.g. 10.0.0.1. In case another port is used, the user must add this port to the address (e.g. 10.0.0.1:999). The HTTP port must not be used by any other application or server such as Apache, IIS, etc. This value can be changed at any time in administrator.ini, using the HTTPPORT key found in the installation folder. This action requires the ATEAS Administrator service be restarted.

1.4. Camera server specifics

The camera server installation will ask for the address or name (computer name or DNS) of the administration server. Every single camera server must be connected to the administration server. There is only one administration server in each system.



Please consider the following rules and recommendations when filling in the address:

HOME and PROFESSIONAL editions: The administration server address is consistent with the camera server address since both server applications are installed on one computer (server). Therefore, fill in the local IP address of the computer or server (e.g. 10.0.0.1 or 192.168.1.1, etc.).

UNLIMITED edition: A limitless amount of camera servers can exist in the local network, WAN or internet. Fill in the address to establish a connection with the administration server. This address may either be an address in a local area network or the WAN address of the NAT-enabled router, which redirects the communication to the administration server.

NOTE

For proper server service operation in the NAT environment, see network configuration. There are certain ports that need to be open for ATEAS Security applications.

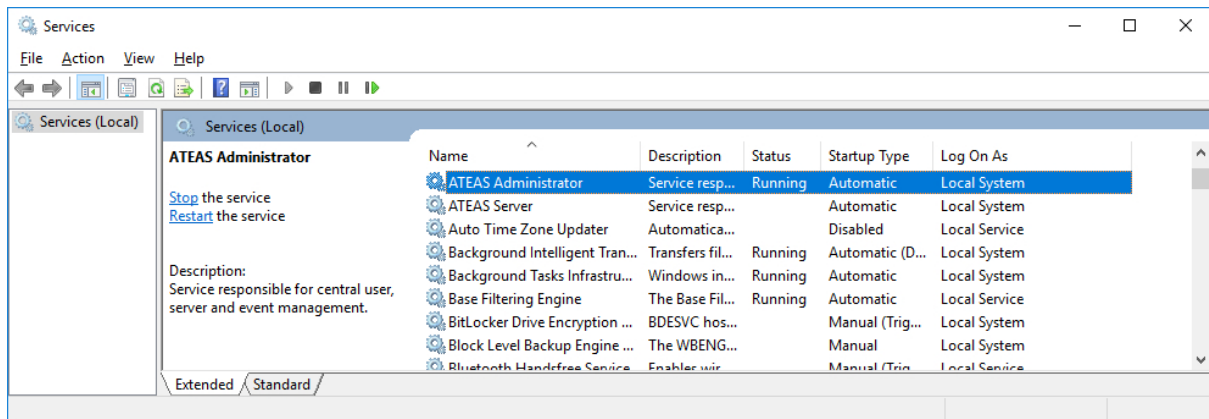
This value can be changed in server.ini using the ADMIN key, found in the installation folder. This action requires ATEAS Server service to be restarted.

1.5. After installation

Server applications (ATEAS Administrator and ATEAS Server) are installed on your computer or server as services with no user interface. All system controls, system management and settings are executed within the ATEAS Observer client application environment. The installer will automatically

create a corresponding program group in the Start Menu that will include the ATEAS Observer shortcut, also appearing on the desktop.

After the installation, both server applications are started automatically and their startup value is set to automatic (see the following picture), meaning both applications are started automatically at Windows startup (regardless of whether a user is logged on or not) and terminated at Windows shutdown.



This is how you navigate to the services window:

English operating system: Start – Control panel – Administrative tools – Services.

1.6. Configuration parameters of the administration server

The configuration parameters of the administration server are located in the administrator.ini file in the administration server installation folder. These parameters can be configured directly in this file using any text editor. The administration server service shall always be restarted for changes to be applied.

HTTPPORT (default value 80): This parameter is automatically set to the value entered during installation and specifies the port on which the administration server displays the home page of your camera system, runs the web client, and manages automatic system updates.

HTTPSPORT (default value 443): This parameter specifies the port on which the administration server displays the homepage of your camera system and runs the web client via the secured http protocol.

WEBCLIENT (default value OFF): Permits or denies web access to the system (value OFF or ON).

WEBCLIENTFORCESSL (default value OFF): Permits or denies unsecured web client operation. If this parameter is set to ON, the web client will only be able to run with a secured http protocol and the address will always begin with https://.

1.7. Configuration parameters of the camera server

The configuration parameters of the camera server are located in the server.ini file in the camera server installation folder. These parameters can be configured directly in this file using any text editor. The camera server service shall always be restarted for changes to be applied.

ADMIN (default value 127.0.0.1): This parameter specifies the name or address of the administration server in the system, to which the given camera server shall connect and be a part of. This value is automatically set to the value entered during installation.

LOCALIP (not used by default): The parameter can be used to select the proper network interface for establishing a connection with the administration server of the system, which would ensure the camera server is properly identified. However, this is only used in rare situations when the camera server is unable to automatically determine the use of network interfaces. For more information see the Multiple network adapters chapter.

MULTICASTSOURCEIP (not used by default): This parameter allows you to select a network interface that will be used for multicast transmission. For more information see also the Multiple network adapters chapter.

FORCEDSERVERID (not used by default): Camera servers are commonly identified within the system based on their address, which gives them a unique number in the system, assigned by the administrator. This parameter can be used to distinguish multiple server connections from the same address.

DLNA item (not used by default): This item determines the network interface for broadcasting video via DLNA standard. If not populated, an interface is chosen automatically.

WANKEY item (not used by default): This item defines the unique camera server key for camera server connection in cloud mode.

HTTPPORT item (default value 8080): Specifies the http port number of the camera server service, which might be used by some other systems e.g. when downloading media from body worn cameras.

HTTPUSER item (default value root): Specifies the username when authenticating to the http server.

HTTTPASS item (default value pass): Specifies the password when authenticating to the http server.

1.8. Configuration parameters of the camera client

The configuration parameters of the camera client are located in the observer.ini file found in the client installation folder. Updates can be made directly to this file via text editor. The client must be restarted with each update.

MUTEXLEVEL (default value 1): The item specifies that a mutex system object is used to prevent a duplicate launch of the client. If the client is launched in terminal mode (e.g. using desktop virtualization technology with GPU acceleration), depending on the selected virtualization depth, this protection may need to be disabled by setting the value to 0. For more information, see also the GPU acceleration chapter.

1.9. Automatic updates

The installation of ATEAS Security applications installation is very quick and simple supporting comfortable automatic system updates. Automatic updates are available for both camera servers (ATEAS Server service) and system clients (ATEAS Observer). Only the system administration service (ATEAS administrator) requires reinstallation in terms of the full system update. The rest of the system will be updated automatically. The new version of the system (administration server) can either be obtained directly via ATEAS installation medium, available in ISO format, or can be downloaded directly from the new system version check window. See Version information chapter for more information.

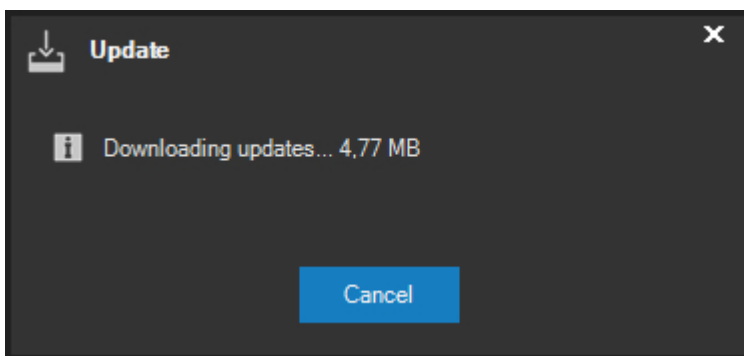
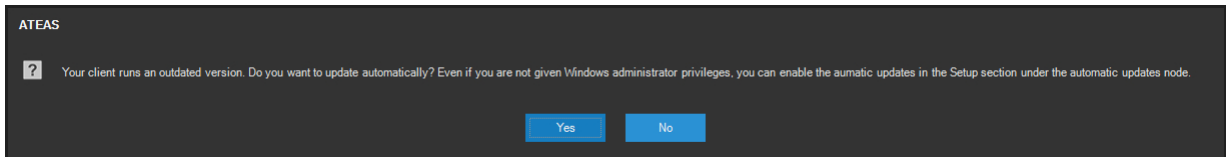
NOTE

When reinstalling the system administration server, the old version of the product is automatically replaced, thus a manual uninstall is not necessary.

Camera servers, disconnected during the system administration core installation (basic functions are not interrupted), are capable of downloading and executing updates, after automatic reconnection to the Administration server, followed by a restart of the service.

Automatic updates make life easier especially on large systems with many clients or for UNLIMITED edition users with many camera servers, capable of executing the update and restarting themselves automatically (after the administration server service has been updated).

System clients are disconnected during the system administration core reinstallation and need to be logged in again. After the login process, the client is capable of downloading and executing the automatic update. The client automatic update process is guided by a very simple update wizard as follows.



CAUTION

In order for the automatic update process to run successfully, the administration server requires the HTTP port be available, making it possible to download the update package. The port (see the network ports appendix) is implicitly set to 80 and may be changed in administrator.ini.

NOTE

If the computer involved is included in the video wall (i.e. the user currently logged in is created as a video wall account), the update will automatically start without having to confirm the dialog by pressing **YES**, because the video wall computers do not necessarily have peripheral devices connected.

1.10. 32-bit and 64-bit application versions

Both the 32-bit and 64-bit version of the camera server service (ATEAS Server) and client application (ATEAS Observer) are available on the installation media home page. 32-bit editions can be installed

on both 32-bit and 64-bit Windows operation systems. 64-bit editions of the application are only compatible with a 64-bit operation system. There are no significant (i.e. measurable under all circumstances) differences in the application performance between the 32-bit and 64-bit version of the application running on a 64-bit operating system. Therefore, only extreme configurations can benefit from 64-bit editions, where a 32-bit address space would not suffice (under 4 GB RAM).

NOTE

The system administration server is available as a 64-bit application only.

Editions can be replaced as necessary. Uninstalling the 32-bit edition of the application and installing the 64-bit edition into the same directory is possible and all settings will be adopted by the current installation. Moving from the 64-bit to 32-bit edition of the application in the same manner is also possible.

NOTE

It is imperative the edition remains the same for automatic updates of camera servers and clients. During the automatic update, a 32-bit edition is always updated to a 32-bit edition, a 64-bit edition to a 64-bit edition. Thus, if we decide to change the edition on a computer, this change must be performed manually.

1.11. Multiple network adapters

If there are multiple network adapters used on a single computer, the entire system operation will remain automatic with no need of additional configuration. Multiple network adapters on a single computer may be used, for example, for both the physical (different active network devices) and virtual (via VLAN) separation of camera and client networks. Since the administration server does the verification of all camera servers being connected to the system, you must respect the principle according to which camera servers connect to the administration server using the address by which they are recognized by the system. Providing the camera server is part of two networks (e.g. 10.0.0.X and 10.0.1.Y with a subnet mask of 255.255.255.0) and the administration server is in the 10.0.0.X network, the camera server has to be added to the system including the address within network 10.0.0.X. The camera server will then automatically choose the corresponding network interface to establish the connection with the administration server. If the administration server is installed on the same computer as the camera server, described above, any interface may be used for their

interconnection and identification (however, the address in the ADMIN key in the server.ini file has to correspond to the address used during the camera server system registration (addition)).

The only theoretical exception, lacking practical impacts, could be the case, when a camera server may establish a connection to the administration server from several network interfaces. In this case, to ensure valid camera server identification, it might be necessary enter this address to the LOCALIP key in server.ini, followed by a restart of the camera server service. In the majority of cases, the LOCALIP key can be left empty.

Providing the above stated principals are observed, the system shall function flawlessly also on a server (computer) with more than two network interfaces. If there are multiple separated networks on multiple network interfaces, via which clients will access the system, these clients must have the profile set to REMOTE. With this profile, the client automatically uses the administration server address, used during the login, for the camera server address.

With some users having the LOCAL profile and the relevant camera server having multiple network interfaces, it may be necessary to specify the network interface that will be used for multicast transmission. This is possible with the MULTICASTSOURCEIP key in the server.ini file. In the majority of cases, this key can be left empty.

CAUTION

Multiple network adapters (interfaces) in a computer running a camera server must not be confused with defining LAN and WAN addresses for a server intended for remote connections from the WAN or Internet.

1.12. Mobile client installation

The application for mobile access to the system can be launched or installed using the links on the installation CD or from your system's administration server address.

The iOS application requires the iOS operation system, installed on Apple devices - iPhone, iPad. The application is started after being downloaded from the App Store. The application is free to download.

The Android OS application requires the Android operating system, installed on various types of smart phone and tablet devices. The application is started after being downloaded from the Android application online store (Google Play). The application is free to download.

The Android application can also be installed on devices such as televisions or displays running the Android operating system, controlled via remote controller or as part of a video wall. The same APK used for the mobile phone or tablet can be used for the installation. If the application detects it has been launched on a television or other display, it automatically selects the optimized user interface.

NOTE

Some Android displays do not feature a display recognition option and the application will be launched with the phone interface. In this case, during the installation, you must use the APK, which includes the interface for televisions and display only.

1.13. Web client and security

After the administration server installation, if the web client operation is permitted via the `WEBCLIENT` parameter in the `administration.ini` configuration file, it is possible to access the homepage of your camera system on the given ports (`http` or `https`) and run the web client.

The ATEAS Security architecture is based on optimizing transmissions to ensure data is transmitted to the client directly from the camera server and not through the administration server. Therefore, if the user logs in to the camera system from his local branch and views the cameras of the respective branch, the user will be logged into the central server, however, data will be transmitted using the shortest route directly from the server located at his branch towards the client.

This principle is also fully applied when using the web client.

CAUTION

Therefore, when using the web client it is important for the camera server ports designated for web access to be available - 8507 for unsecured and 8508 for secured communication.

If the user attempts to access the system web page via secured `http` protocol (`https://`) or the use of secured communication is enforced via the `WEBCLIENTFORCESSL` parameter, your camera system shall have the necessary certificates installed to allow such access.

NOTE

These can be test certificates issued for free or by you directly, as well as any commercial certificates issued by a certification authority that verifies your identity.

Since the certificate must always be issued for the respective server, name, address, or domain, the proper certificates for your system cannot be included in the camera system installation. Test certificates `ateas_root.pfx` and `ateas_127_0_0_1.pfx` are found in the `ssl` subfolders of your administration and camera server and can be used to test the secured version of the web client. The first certificate is the ATEAS test root certificate and the second is a certificate based on this root certificate, issued for the "127.0.0.1" server.

NOTE

After installing these test certificates, your browser will accept the connection and trust the server only when accessing the "127.0.0.1" address, i.e. only directly from the computer where the server is installed.

Installing certificates for the camera system

The certificate for your server (administration or camera) can be installed easily by copying the certificate in PFX (Personal Information Exchange) format directly into the `ssl` folder in the installation folder of the respective server and restarting the server.

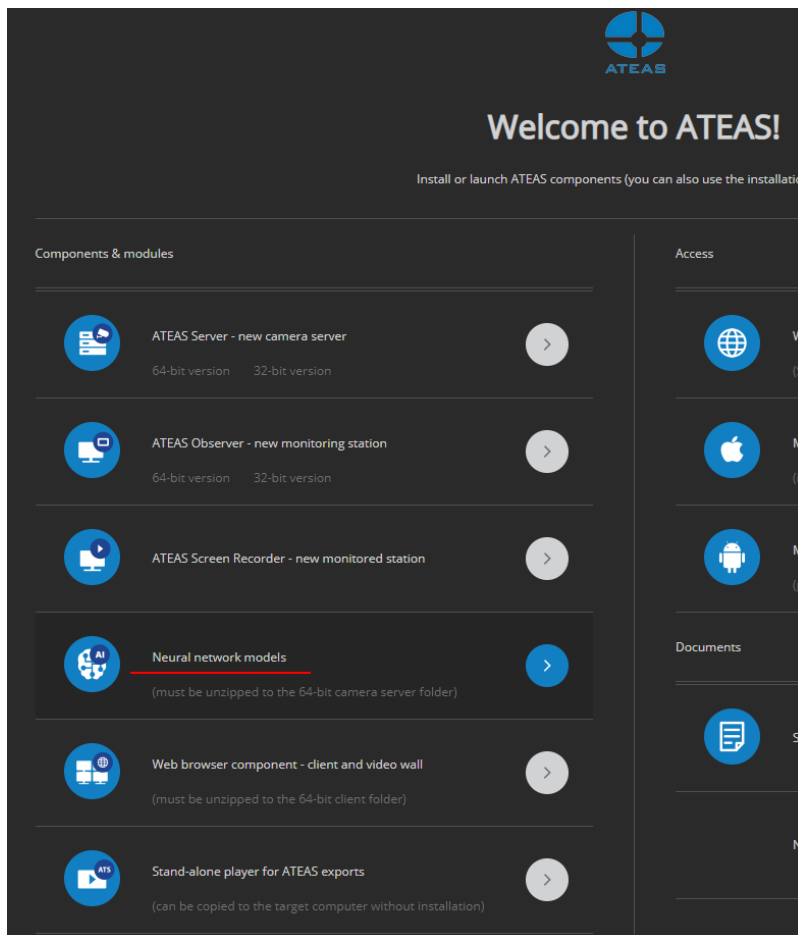
If certificate data is password protected, the password can be passed to the administration or camera server service via the `-ssl` parameter at service startup. For more information, see the Parameterized application launch chapter.

NOTE

The password for the delivered testing certificates is „ateas“. You don't need to pass this password using the `ssl` switch, unless a different password has already been used with this switch.

1.14. Neural networks installation

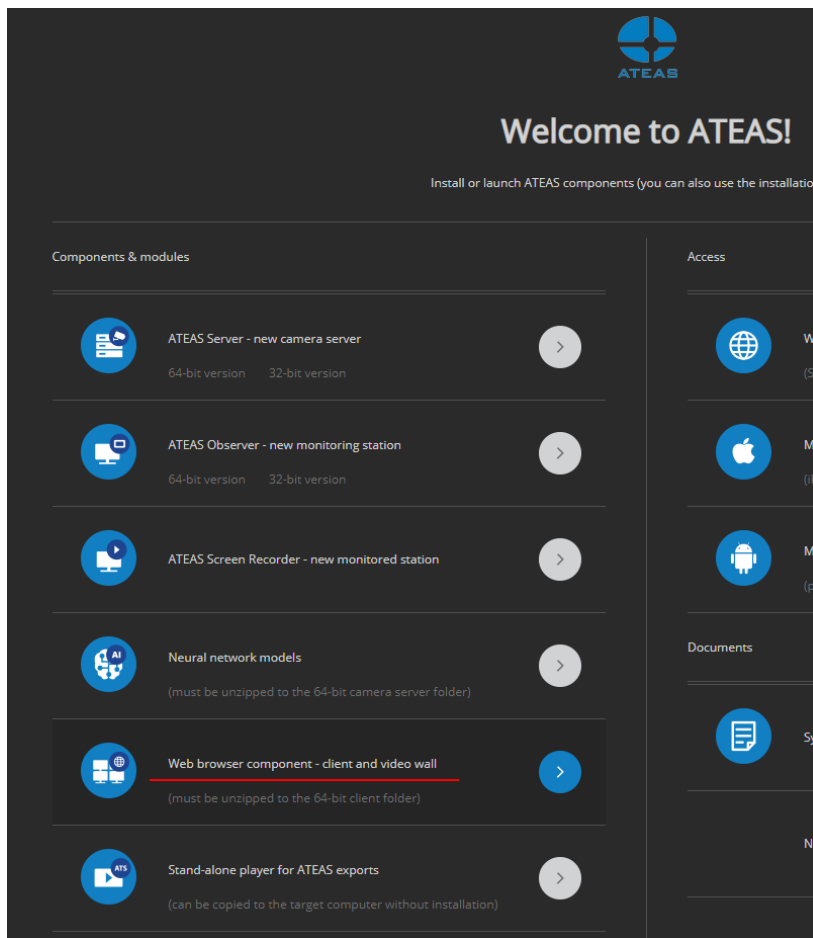
A neural network can easily be installed by downloading the archive directly from the system administration server website and unpacking the contents of the archive to the installation directory of the camera server designated to be equipped with artificial intelligence and analysis capability features.



After the installation, you can continue in server administration section by pressing the **DNN** button.

1.15. Installing the browser component

Apart from cameras ATEAS client or the video wall can also display any web based content. For this purpose, a web browser component must be added to the client that is available on the administration server website.



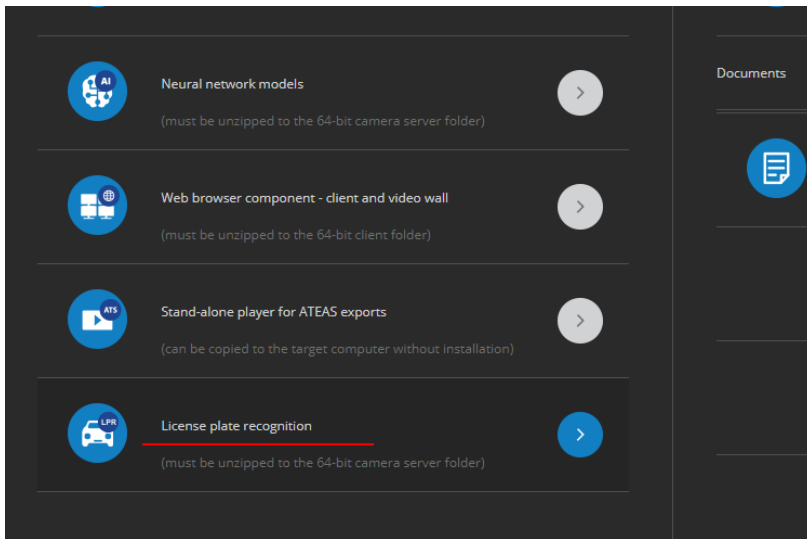
The archive must be unzipped to the ATEAS client installation folder.

NOTE

The web browser component can only be used with the 64-bit version of the client and can't be used with an Android powered display device, which can be part of the video wall.

1.16. License plate recognition installation

License plate recognition can easily be installed by downloading the archive directly from the system administration server website and unpacking the contents of the archive to the installation directory of the camera server designated to be equipped with this feature.



After the installation, you can continue in add-on administration section on the LPR tab.

NOTE

An additional license is required for license plate recognition.

1.17. IPv6 compatibility

The actual exhaustion of public IPv4 addresses is the key driving force behind the evolving use of IPv6 addresses. The first to be affected by the transition to IPv6, in terms of camera systems, will be the users accessing the system from IPv6 (mobile) networks, in which IPv4 addresses will no longer be assigned to the devices. Therefore, ATEAS also supports the IPv6 protocol for communication between system components (users, servers, cameras).

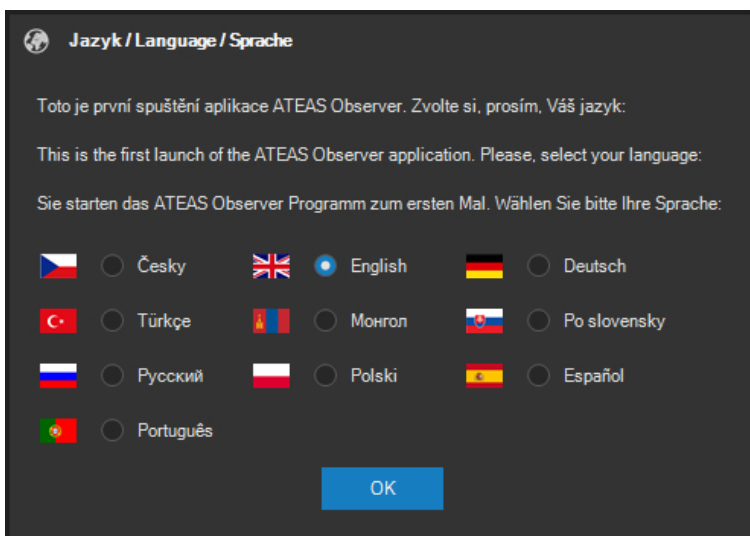
Chapter 2 - Starting up for the first time

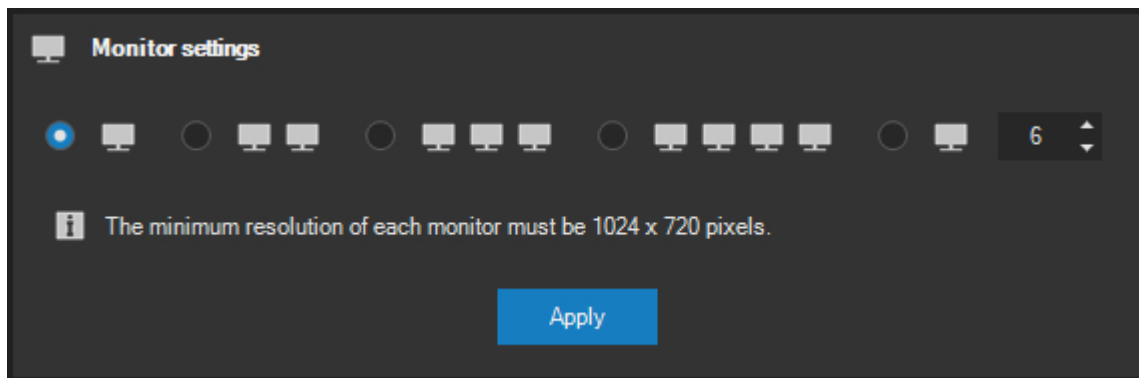
2.1. First login and providing the license key

NOTE

For more information about license activation and obtaining the activation key, please read the Product activation and license key upgrade subchapter (found under the administration section). If your system has not been activated yet, this information is available at the address of your administration server (using a web browser). This subchapter also includes information interesting to hackers.

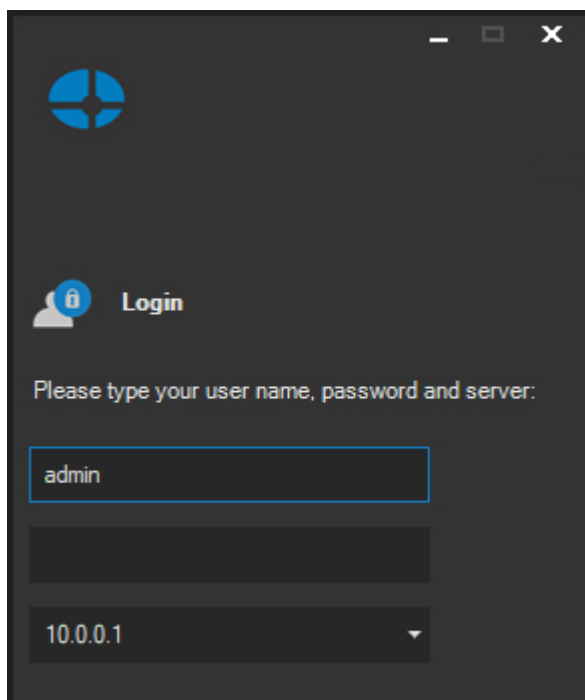
Several basic application setup dialogs are displayed when running the application for the first time on a given workstation (language selection and multiple monitor settings). In both cases, it is necessary to select one of the options and continue by pressing the **OK** or **APPLY** button (the language might be preselected according to your system's settings). Further information about monitor settings can be found in the documentation section regarding local application settings, where these options may be changed.



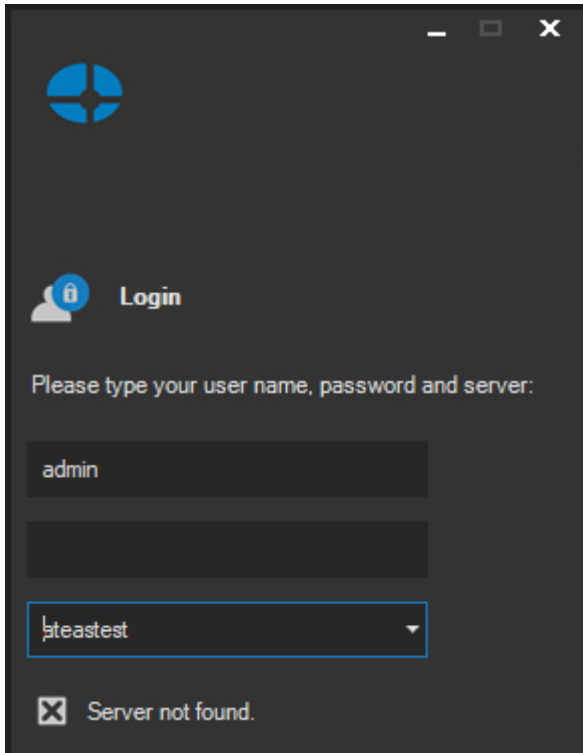


After the client application (ATEAS Security Observer) is started, the system will require the user to enter his username, password and server to log in. The system uses a predefined administrator account **admin** with the password **admin**. The system does not accept identical usernames and passwords, so the user must change his password after the first login. You can enter either the IP address or the name of the server where the ATEAS Security administration server is currently running. After the user is successfully authenticated, the server name or address is saved and does not need to be entered again in the future.

The client application remembers the last login. When logging on again, not only is the server information automatically filled in, but a list of recently used servers is also available. It is possible to select any given item from the list or use the auto-complete function when typing via the keyboard. The drop-down list is always sorted according to the server login dates, in descending order starting with the most recently used names or addresses.



The application always states the cause of an unsuccessful login, as seen in the following picture:



The most common reasons for unsuccessful authentication include:

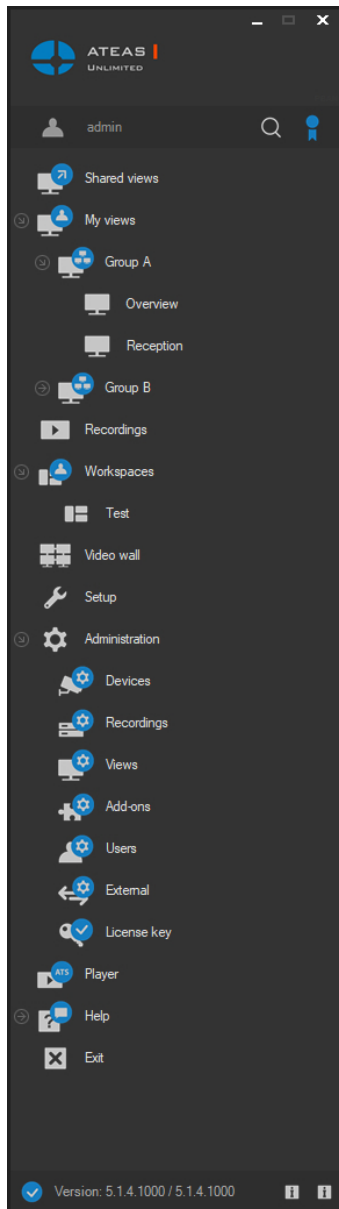
- incorrect username or password, note that passwords are always case sensitive, the system administrator may reset your password when necessary,
- incorrect address or server name,
- network connection problems,
- exceeding the limit of simultaneous client accesses as per the actual license,
- invalid (outdated) client application version,
- duplicate login.

The system does not accept identical usernames and passwords and will ask the user to change the password following the first login as admin (this also applies to passwords reset by the administrator or logging on with a new user account for the first time). The following is an overview of rules that shall be considered when creating a new system password:

- the minimum password length is 4 characters (providing the system administrator did not modify the user policy, which requires the minimum length to be higher or for the required password to be strong),

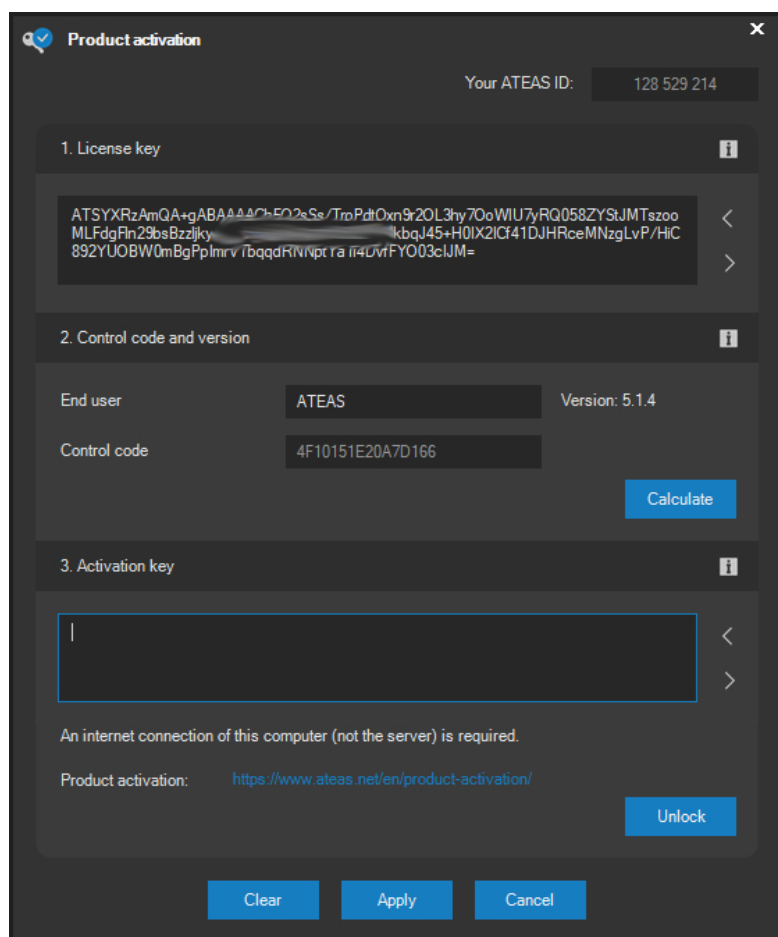
- passwords are case sensitive,
- entering a password identical to the username is not possible (regardless of case sensitivity).

The application main menu will appear after the login is successful. You will also see a logo corresponding to the currently installed product edition (HOME, PROFESSIONAL, UNLIMITED) and a small administration server connection indicator will appear at the bottom.



Connections to all camera servers and to the administration server are maintained automatically and can be recovered on break up. The administration server connection status is indicated by a symbol located in the bottom left corner of the main menu window.

After the initial client application startup, the administrator shall enter his license number, otherwise it will not be possible to continue working with the system. One license number is entered for the entire system and does not require re-entering for the installation of additional client applications or servers.



The license key number you purchased shall be entered in the License key section. This license number can be copied or inserted from the license file that was attached to the activation e-mail. Importing the license key from the license file can be performed via the white up-arrow button. More information is provided in the product activation documentation section in the full version of this document, which is also available at your administration server address.

If you don't have a license, you can activate the software by typing START which enables you to add four cameras free of charge without any time limitations and add the license key later without reinstalling.

After entering the license key, the name of the license end user shall be entered followed by pressing **CALCULATE** to generate the control code.

CAUTION

A valid end user name must be entered. System users can display the name at any time and, provided the name is incorrect, they shall request the name to be corrected. A system with an invalid end user name is considered to be improperly licensed.

NOTE

The end user name is a precaution that increases the security of providing licenses. The end user names are not monitored or saved in any way, nor are they transmitted to the licensing server during system activation.

NOTE

Besides the end user name of the license, the control code calculation also includes basic information about the computer on which the administration server is installed.

Apart from the license number, it is necessary to obtain the activation key. This can be done either online by clicking the **UNLOCK** button or using the links at the bottom of the window. You must have an internet connection to access ATEAS servers (not necessary for computers with ATEAS software equipment installed).

This dialog can be closed without entering a license number by clicking the **CANCEL** button.

CAUTION

If no license number is entered, the client application will close after clicking the **CANCEL** button.

2.2. ATEAS ID installation identifier

After the license key has been entered and the system has been activated, the ATEAS ID will be displayed in the top right corner of the license dialog. This ID serves as a unique and permanent

identifier of your software copy and shall be used for all technical and process matters regarding your installation. The ATEAS ID is a nine character numerical identifier.

The ATEAS ID also facilitates installation management for installation companies, for ATEAS ID stays the same for all standard system operations:

- The license key (along with the activation key) is updated when the system is expanded, nevertheless, the assigned ATEAS ID remains the same.
- When the system is moved to a different hardware configuration and the license is deactivated, the control code for your license (along with the activation key) is updated, nevertheless, the assigned ATEAS ID remains the same.
- Upgrading to a newer version of the system results in the activation key changing with the reactivation process, nevertheless, the ATEAS ID remains the same.

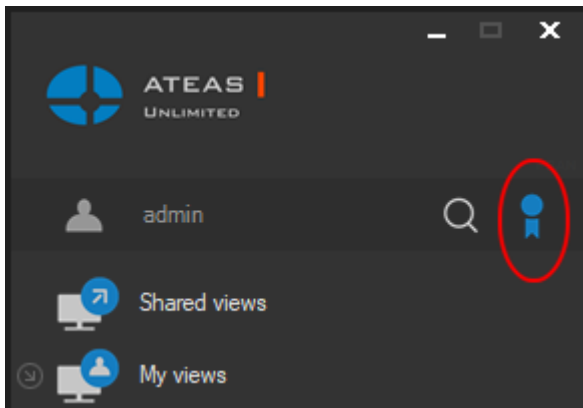
2.3. Certified installations

Your installation can be certified. This indicates the installation was carried out by a company that meets the requirements for performing certified installations, which in particular include undergoing various levels of authorized administrator ATEAS training sessions. An installation certificate is generated and automatically uploaded to the system during the license key activation process. The certificate is an XML file uploaded to the certificates subfolder under the installation folder of your administration server.

NOTE

A certificate is also generated for manual license key activations performed on the ATEAS webpage. A download link is created to download the certificate. This file must be placed in the folder stated above. This must then be followed by a restart of the administration server.

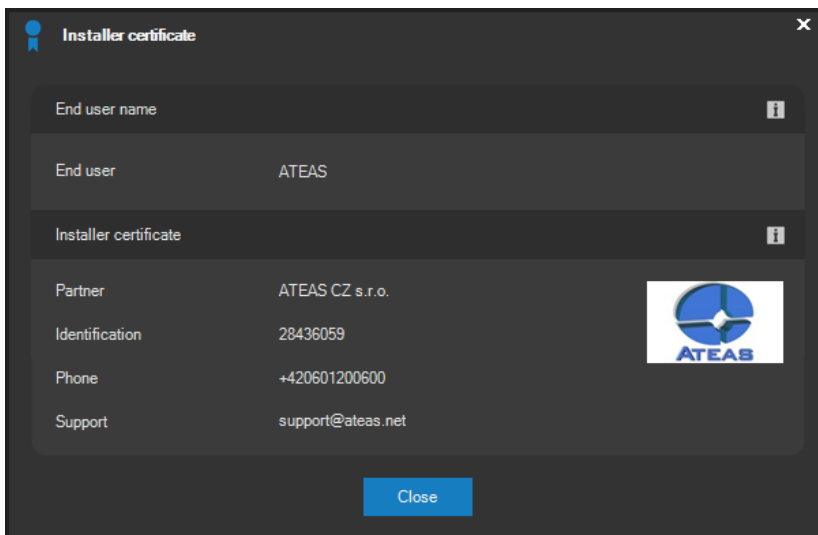
A bold certificate symbol in the top left corner of the window with the application main menu indicates your system is a certified installation.



In addition, the certificate includes the following features:

- The certificate is digitally signed directly on ATEAS servers and cannot be created by anybody else.
- A certificate is linked and issued to a specific ATEAS ID and is non-transferable.
- The certificate contains the installation partner's credentials as well as their ID including logo. Optional data includes phone or online support contacts.

This data can be displayed at any time by clicking on the certificate icon.



Besides the certificate of the installation partner, this dialog also displays the end user name. In order to create a control code for your installation, a valid end user name shall be entered during system activation.

CAUTION

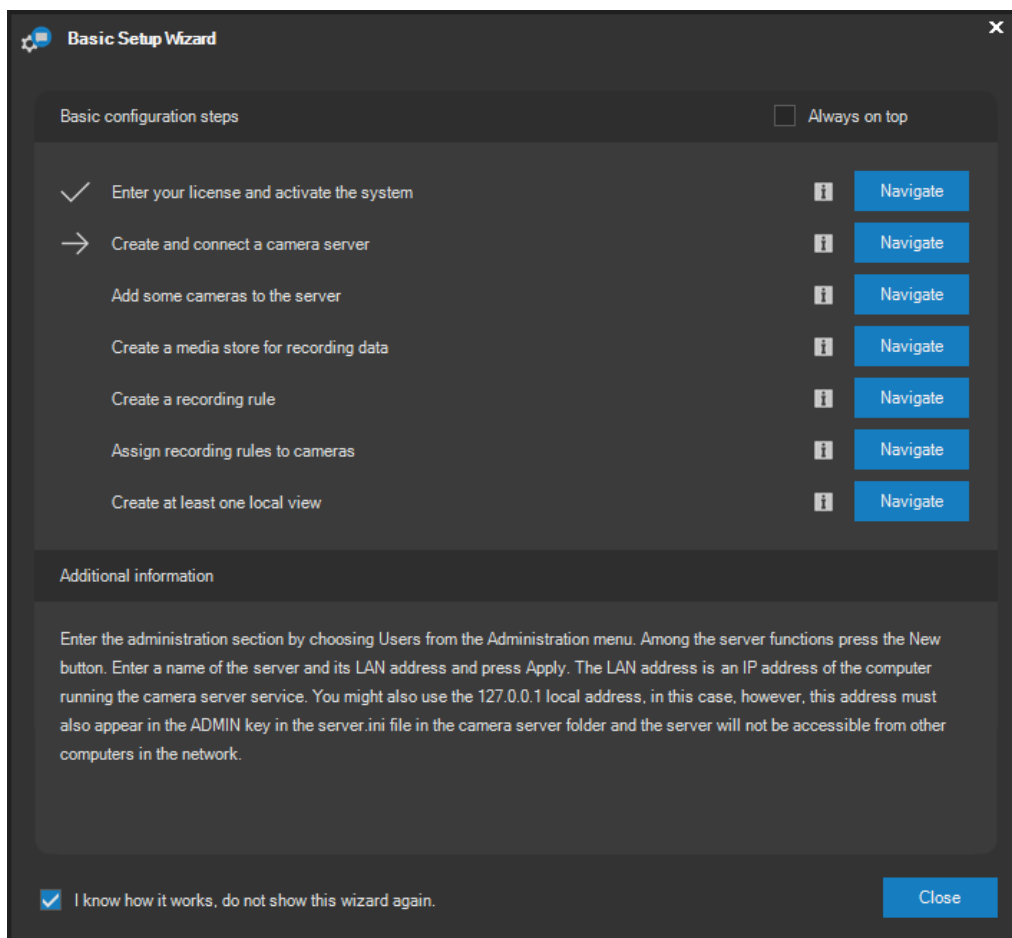
If your installation shows a different end user name, you should contact your installation partner to rectify such situation. A system with an invalid end user name is considered to be improperly licensed.

NOTE

If the installation partner's certificate is not available in the system, the certificate icon in the main menu is grey and no certificate can be displayed. However, end user data will always be displayed for a licensed product, not for the START edition.

2.4. Basic Setup Wizard

The Basic Setup Wizard will automatically be launched after the user successfully logs in to the system for the first time. This wizard will guide you through several basic steps normally required to get the fundamental functions of the camera system up and running. These functions, for example, include adding cameras, setup recordings or creating a live view.



The setup wizard is well organized into several basic steps covering license entry and system activation, creating a camera server, adding cameras to the server, creating a media store for recording data and creating a recording rule, assigning recording rules to cameras and creating at least one local camera view. During the setup process, the wizard displays information stating which steps have already been carried out and which step is the next to be performed.

Detailed information on how to perform each step is displayed at the bottom of the wizard window. A **NAVIGATE** button is also available for each step, which automatically opens the respective window with the settings required for the given action. The blue button with the information icon will provide additional information for any of the steps.

If you do not wish to use the wizard for system setup, it can be deactivated by activating the checkbox on the bottom edge of the window. In this case the wizard will no longer appear.

NOTE

The wizard can be reactivated at any time by manually selecting Setup Wizard from the Help menu.

NOTE

The wizard is shown automatically only for the master system administrator (administrator number 1), authorized to perform all steps in the installation wizard. This is only the case should any of the setup steps not be carried out. If all steps have been carried out, the wizard will not appear.

NOTE

The wizard can be loaded by other system administrators manually, but will not appear automatically. The wizard cannot be opened by standard system users.

The wizard window is displayed in front of all other opened windows, ensuring you always have the current setup step in front of you. However, the wizard on top feature can be disabled by deactivating the Always on top option.

2.5. Custom server names

When logging in, the text field for entering the server supports both the server IP address, as well as the server name (e.g. DNS name or local network name). These names are then displayed in the drop-down list, which shows the history of recent successful logins sorted in chronological order with the names of the most recently used names shown first.

NOTE

The history can contain up to 25 login items.

Based on experience, logging in to various camera systems using a single client can create a confusing list of IP addresses, which seemingly cannot be assigned to specific systems. These can be substituted with aliases.

NOTE

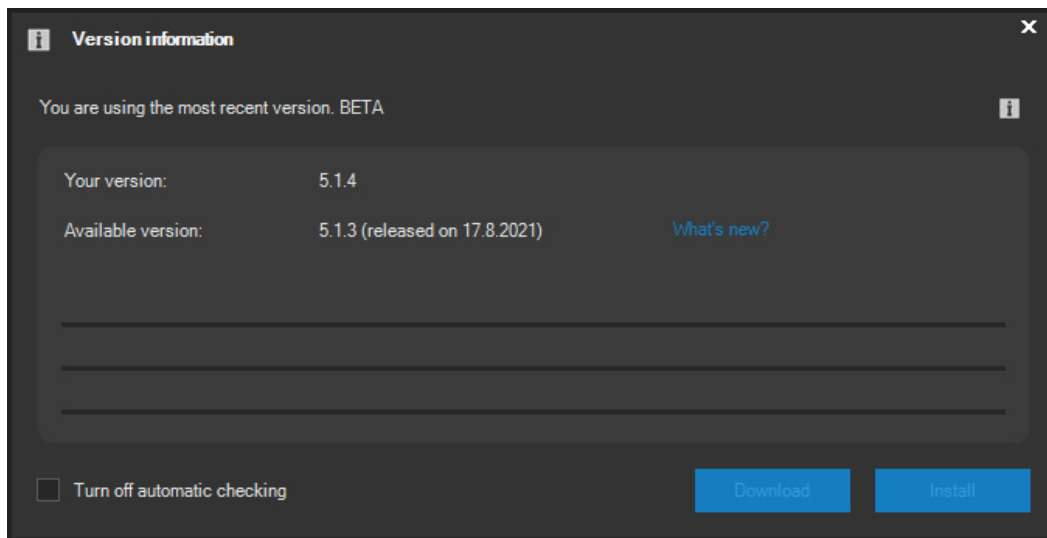
In this case we mean logging into multiple different camera systems, each of which has a custom licensed administration server. We are not referring to the situation in which multiple servers exist within a single camera system. Here, the users of course perform a single sign on, granting them access to all servers in an UNLIMITED edition simultaneously.

Custom logon server names (alias names) can be created under Settings, in the Login history section, where this feature is described. In addition to this, the alias can also be created by direct entry immediately when logging in by adding the alias into parentheses behind the actual network name or server address, e.g. 10.0.0.10 (alias).

The alias names created in local settings section or by following the procedure specified in the previous paragraph can then be used in the same manner as network names. The alias names just need to be entered into the server field when logging in.

2.6. Version information

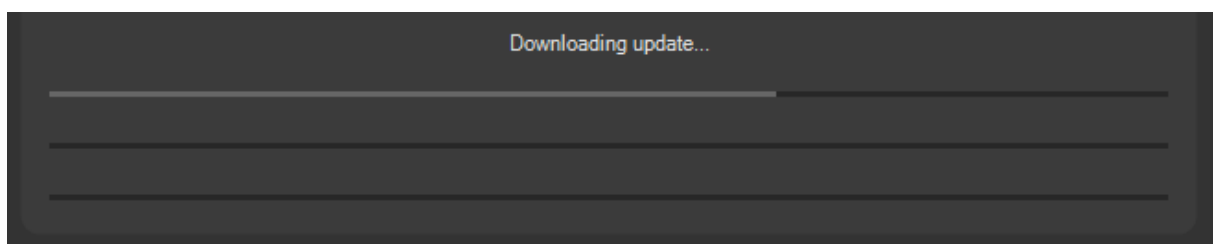
Icons with an information symbol are located in the bottom part of the main menu window in the right bottom corner (besides the connection with administration server status and current version information). Providing the computer running the client application is currently connected to the internet, it is possible to verify the newest available version of the ATEAS platform by clicking on icon on the right.



The client application contacts ATEAS servers and determines the currently newest version available along with its release date. Furthermore, it will also display information whether or not you are using the current or older product version. The window also contains a link to the ATEAS website where, upon signing in with ATEAS Login credentials, the newest installation medium image is available for download, along with a link to the page containing a description of added features and new options available in new ATEAS versions.

The client application is configured to automatically check for a newer version by default. You will be notified of a newer version. This automatic control can be switched off by checking the relevant option on the bottom edge of the window and by clicking the **CLOSE** button.

If a new system version is available, a user with master administrator rights can download the new version by clicking the **DOWNLOAD** button. The first row shows the downloading progress.



NOTE

The latest system version will be downloaded, only if your ATEAS PMA entitles you to do so and you can activate it.

After the downloading process is complete, the integrity of the downloaded file is checked. The progress of this check can be seen in the second row. The third row shows the progress of uploading the update to the system administration server.

NOTE

Therefore camera system servers do not need to be connected to the internet during the auto-update process.

After the update has been uploaded to the administration server, click the **INSTALL** button to initiate the reinstallation of the system administration server. The reinstallation process disconnects the client. After the client is automatically connected, the client may require an update along with the need to activate the new version of the system. The Automatic updates chapter describes this process together with the auto-update process of all camera servers.

NOTE

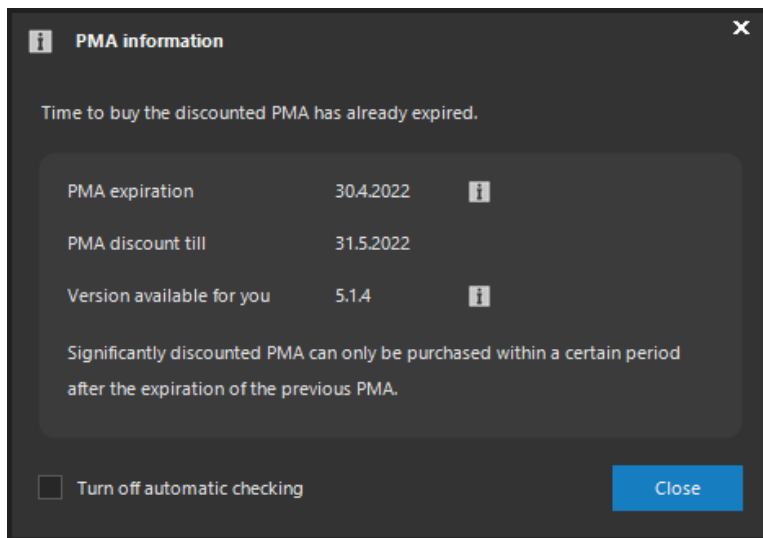
You can successfully activate the new version upon installing only providing you have the right to do so (free update by purchasing a license number or independent contract on PMA product support).

NOTE

The client application version is displayed on the bottom of the application's main menu window followed by the version of the system the client has logged on to. Since release 4.0.2, the client application has backward compatibility and can access older system versions, however no older than version 4.0.1.

2.7. Information about PMA

The symbol on the left, within the group of information symbols located in the bottom right corner of the window displaying the main menu, is used for verifying the PMA status of your installation.



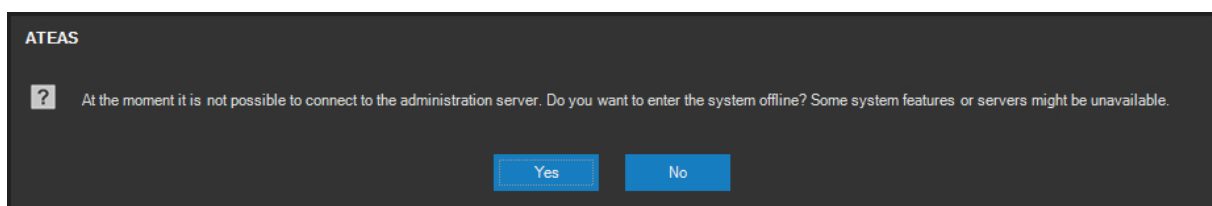
ATEAS PMA guarantees updates for your system to the most recent version available. In order to update the system, an ATEAS PMA service must be active. More favorable conditions are available to those who renew PMA on a regular basis. Thus, if the application is connected to the internet, you can check the PMA expiration date and the PMA renewal date directly in your application. With every new license purchase there is a 2-year PMA included.

The client application is configured to automatically check for expiration by default. You will be notified prior to the expiration date. This automatic control can be switched off by checking the relevant option on the bottom edge of the window and by clicking the **CLOSE** button.

Version available for you displays the maximum system version that you can install and activate. Had your ATEAS PMA already expired, this version can be lower than the most recent system version.

2.8. Offline login

In the event that the administration server cannot be accessed, it is possible to enter the system offline (no connection to the administration server). The application will provide this option after failing to establish a connection with the administration core or upon using up the preconfigured amount of login attempts when using the automatic login feature.



By selecting **YES**, you will be able to access the system offline, providing you entered your username and password correctly. The user is given the last available set of rights and restrictions after logging on offline.

NOTE

For this reason, logging on offline will not be possible if the user has not performed a proper online login previously on the given station.

After logging on to the system offline, you will always be able to use functions for managing the local snapshot database and locally saved sequences, exported from camera server media databases. UNLIMITED edition additionally enables online access to some camera servers within the system, including live access to cameras and their recordings. However, the system administrator must explicitly enable this feature. See subchapter Basic server management for more information.

CAUTION

For security reasons, only the last user logged online on the respective computer can access the system offline.

2.9. Application main menu

The application main menu will appear after a successful login. It contains the following items:

Shared views – views defined by administrators with access granted to all users.

My views – views defined by users with no access for other users.

Recordings – access to camera recordings.

Workspaces – this option includes the layout of several live windows including views or the map window, it is activated within the workspace setup section.

Video wall – this option enables access to the video wall or to remote monitors providing a video wall is configured by the administrator.

Setup – local workstation setup.

Administration – camera management and setup, recordings, views and video wall, add-ons, users, rights and server management, integration possibilities and license number upgrade (activation).

Help – opens the product documentation.

Exit – closes the application.

The current user is displayed above the main menu as well as a button for activating the menu search. This is especially handy, when there are many shared or private live views possibly organized in a multi-level tree structure.

2.10. Application automatic startup

The startup value for ATEAS Administrator and ATEAS Server services is set to automatic by default and does not require user action to be run (except for restarting).

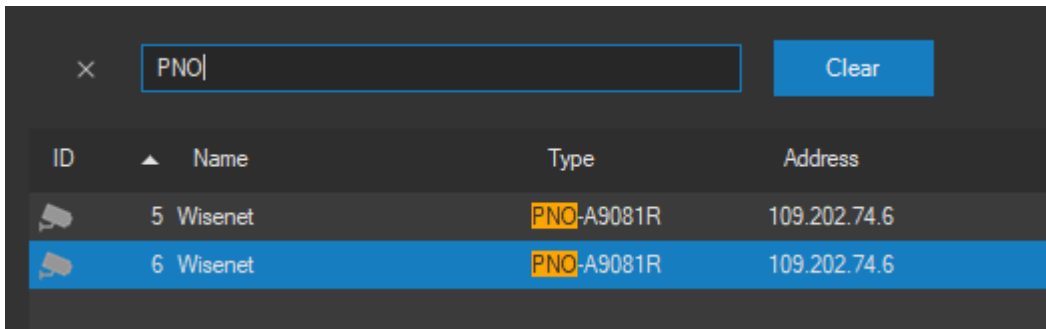
Using the local setup, the ATEAS Observer client application may be started automatically after Windows startup and can automatically authenticate a specific user. Automatic workspace loading also enables the opening of predefined views and their correct positioning on relevant monitors. See the local settings chapter for more information.

CAUTION

Be very careful when using the automatic login feature. Users logged in automatically do not have to enter their password, which can lead to their account being abused. Therefore, it is highly recommended to only use the automatic login function for universal users with low permission levels.

2.11. Searching, filtering and sorting throughout the application

Various segments of the client application produce system data lists – e.g. list of cameras, users, servers, events, external elements and many more. The data is presented either in table view or list view with tree structure. The CTRL-F key combination can be used in all of these structures to activate searching via the integrated search panel.



ID	Name	Type	Address
5	Wisenet	PNO-A9081R	109.202.74.6
6	Wisenet	PNO-A9081R	109.202.74.6

By entering text into the search field, data rows in the table are automatically filtered. Only the data rows that meet the search criteria will be displayed. The following rules apply for searching and filtering:

- All table columns are automatically searched for the entered text.
- Entering multiple words separated by a space, searches for all data rows with at least one column containing at least one of the search words (logical OR).
- To search for data rows containing multiple words, the word should be prepended with a + symbol (logical AND).
- An entire phrase containing spaces can be searched by adding quotation marks to the entire searched phrase.
- To restrict the search to a specific column, enter the column name followed by a colon before the search phrase.
- The searched phrases are automatically highlighted within the filtered data rows.
- All entered search words can be removed by pressing **DELETE**.

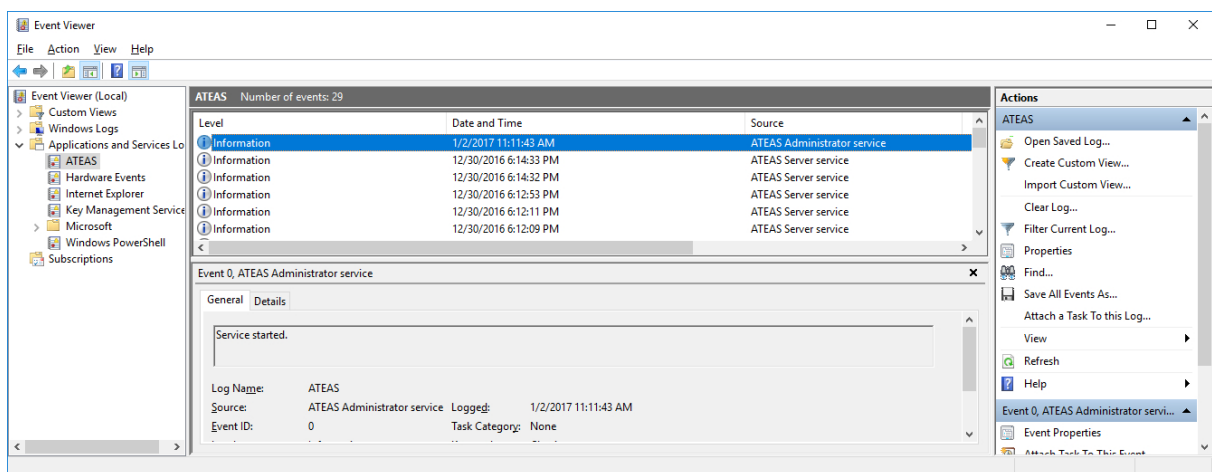
Lists can be sorted by simply clicking on the header of the relevant column. Clicking the column header again will change the sorting from ascending to descending and vice versa. Use the SHIFT key to select and sort according to multiple columns.

2.12. Terminal client access

Desktop virtualization technology indisputably has great benefits for the operation of information systems within enterprise solutions. Since ATEAS applications support GPU acceleration technologies (client and server), camera systems can now also be fully integrated into the architecture. The client application can utilize the acceleration via server GPUs (Tesla) and can be run for a larger number of clients with GPU acceleration. Without this acceleration, multiple launches of the client, demanding smooth high definition video, would immediately overload the server processors. For more information, see the GPU acceleration chapters.

2.13. Protocols

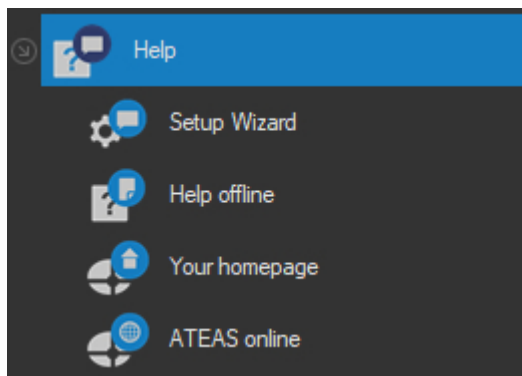
A new event protocol labeled ATEAS is created upon finishing the installation of any ATEAS Security application. All significant circumstances related to the application run are recorded to this protocol. The protocol can be found in the Control panel – Administrative tools – Event Viewer section. In case of any suspicious or non-standard behavior, this protocol may contain important diagnostic data. Besides the system protocol logging, managed by the Windows operating system, ATEAS Security writes its own system log related to the camera system, available in the user administration section. The log contains a history overview, filtering and a live spy window feature.



Chapter 3 - Help

3.1. Documentation and help

There are several links available in the submenu as follows.



System administrators can run the Setup Wizard to guide them through basic steps for the initial setup.

The Help offline link opens the complete offline product documentation in PDF or CHM file format. Your homepage opens the administration server homepage in your default web browser (internet connection is not required), where besides the complete press quality documentation, other documents and system applications installers can be found.

The last link will redirect you to the manufacturer's homepage (internet connection required), providing contact information and enabling users to log into the partner section.