

Applied Systems Ltd

ADMINISTOR'S GUIDE FOR THE NUCLEAR MATERIALS
ACCOUNTING AND CONTROL AUTOMATED SYSTEM
«ATOMIC KEEPER»

Minsk, 2023

CONTENTS

1. SYMBOLS AND ABBREVIATIONS	3
2. GENERAL PROVISIONS	4
2.1. Application area	4
2.2. Main features and functions of NM A&C AS	4
2.3. Administrator's skills	5
3. Basic description of the system architecture	6
3.1. Architecture layout	6
3.2. Software elements	6
3.3. Safety Information for NM A&C AS.	7
4. PREPARATION FOR THE INSTALLATION OF NM A&C AS "ATOMIC KEEPER". INSTALLATION AND CHECK	8
4.1. Preparing to install NM A&C AS	8
4.2. Installing and configuring IIS (Internet Information Services)	8
4.3. Configuring MSSQL Server	11
4.4. Configuring Visio.	17
4.5. Generating a self-signed SSL certificate.....	18
4.6. Installing the AtomicKeeper application	18
4.7. Checking the functionality of the installed software.	22
5. DESCRIPTION OF ADMINISTRATOR OPERATIONS	23
5.1. Login to the system administration page.	23
5.2. Create a user account	23
5.3. Account deactivation	23
5.4. Changing data in a user account.	23
5.5. Reset the password for a user entry.	24
5.6. Viewing the log of user actions (logging).....	24
5.7. Authentication settings.....	24
5.8. Unlock account.	24
6. EMERGENCY ACTIONS	25
6.1. Actions in case of non-compliance with the conditions for the implementation of the technological process, including the case of long-term failures of technical means.....	25
6.2. Actions to restore programs and / or data in case of failure of magnetic storage media or detection of errors in data	25
6.3. Actions in cases of detection of unauthorized data tampering	25
6.4. Actions in other emergencies.....	26

1. SYMBOLS AND ABBREVIATIONS

Abbreviation (symbol)	Decoding (explanation)
NM A&C AS	Nuclear materials accounting and control automated system
NPP	Nuclear power plant
MBA	Material balance area
IC	Isotopic composition
KMP	Key measurement point
IAEA	International Atomic Energy Agency
MBR	Material balance report
ICR	Inventory change report
OS	Operation system
DBMS	Database management system
II	Inventory item
NM	Nuclear material
ICR	Inventory Change Report
MBR	Material Balance Report
PIL	Physical Inventory Listing

2. GENERAL PROVISIONS

The Administrator's Guide for the “Atomic Keeper” nuclear materials accounting and control automated system (hereinafter referred to as the “Guide”) contains step-by-step instructions and explanations on the main operations performed by the system administrator.

2.1. Application area

The nuclear materials accounting and control automated system “Atomic Keeper” (hereinafter referred to as NM A&C AS) is designed to automate procedures for the accounting and control of NM, centralized storage and processing of the data on the handling of NM at an NPP, the formation of reporting and accounting documentation, as well as providing reliable information for planning and implementing activities for the accounting and control of nuclear materials on the territory of the NPP.

2.2. Main features and functions of NM A&C AS

NM A&C AS provides the following key features:

collection, processing and storage of the information on the properties and characteristics of nuclear materials used at a nuclear power plant;
formation and maintenance of accounting and reporting documents;
providing information on the current location and quantity of nuclear materials in their locations.

The main functions of NM A&C AS include:

1. accounting for the characteristics of each accounting unit, maintaining their history of changes;
2. accounting for the location of each accounting unit;
3. registration of operations, works and special procedures performed with accounting units;
4. registration of all movements of accounting units;
5. ensuring the possibility of creating, modifying and applying loading and reloading schemes (during registration of work with the reactor core);
6. formation of working documentation required by NPP specialists before, during or after the performance of work with nuclear materials;
7. providing data on the amount of nuclear materials in all MBAs and KTIs;
8. formation of documentation on the presence of nuclear materials and accounting reports of the established form (ICR, PIL, MBR);
9. maintenance of accounting documents (Main and Auxiliary journals, registration cards, cartograms of nuclear materials placement);
10. support for the possibility of correcting data on the location and isotopic composition of nuclear materials (with reflection in reporting and accounting documents);

11. provision of information support for inspections and physical inventories conducted on the territory of the NPP;
12. Ensuring the verification of input (selected) data for compliance with validation criteria.

2.3. Administrator's skills

The administrator must know:

this Guide and the main Internet technologies;
the relevant terminology of this document;
the basic principles of the sites operation.

The system administrator must have the following knowledge and skills:

setting up and diagnosing of the system operation;
maintenance of technical and system software of the system;
database administration;
data backup and recovery;
provision of routine maintenance and analysis of the results of routine operations.
maintenance and administration of local area networks, TCP/IP protocol;
setting up local area network workstations;
installation, system-wide maintenance and administration;
DBMS administration.

3. BASIC DESCRIPTION OF THE SYSTEM ARCHITECTURE

3.1. Architecture layout

The architecture of the system is implemented according to the MVC pattern (“Model-View-Controller” pattern) with the separation of application data, user interface and control logic into three separate components. Thus, the following levels can be distinguished in the system:

1. User interface level;
2. The level of business logic;
3. Database level.

The top level is the user interface level. At this level, the system contains input / output forms, functions for checking the correctness of input data before they are processed on the server side. The interface is implemented in the HTML5/CSS3 markup language and uses the TypeScript and JavaScript programming languages. The rendering of containers and equipment with their contents on the pages for monitoring the current status of nuclear materials is performed using the canvas element (an element of the HTML5 markup language), designed to create a two-dimensional bitmap image using JavaScript scripts.

At the level of business logic, the system contains program codes that perform the functions of supporting the necessary operations. The business logic layer is written in C#.

The database level consists of tables, views, stored procedures, functions, triggers implemented in the Transact-SQL language and necessary for the full operation of the accounting and control system. The communication between the business logic layer and the database layer happens with the help of O/RM from Microsoft Entity Framework and LINQ syntax.

3.2. Software elements

The system is implemented using the following technologies:

1. NET Framework 4.5;
2. ASP.NET MVC 5;
3. DBMS MS SQL Server;
4. HTML5, CCS3, bootstrap 3
5. C#, Transact-SQL, JavaScript (ES6), TypeScript, AngularJs, Fabric.js

The functioning of the system is provided by the following software:

1. Server part
 - a. OS Windows Server 2019;
 - b. DBMS MS SQL Server 2019;
 - c. Net framework 4.5.1;

- d. IIS.
- 2. Client part
 - a. Operating system Windows 10;
 - b. Web browser MS Edge (15 and above), Chrome (66 and above);
 - c. Tools for creating and editing MS Office documentation (2016 and higher).

3.3. Safety Information for NM A&C AS

All user actions, performed in NM A&C AS, are recorded and stored in the event log indefinitely.

Confidential information, API keys and passwords are not contained in the source code or source code repositories, except for one administrator account (login: admin, password: 123456) used for the initial login to NM A&C AS after its installation. Standard administrator account information is personalized the first time you log in.

User access to the functionality of NM A&C AS is provided using a personal computer and an IP address that is included in the list of trusted IP addresses.

Entering the password in the system interface is hidden and not visible to other persons.

To prevent entering malicious commands, NM A&C AS MK implements validation of user input.

The user session is terminated by the timeout specified by the administrator settings or by pressing the "Exit" button.

4. PREPARATION FOR THE INSTALLATION OF NM A&C AS "ATOMIC KEEPER". INSTALLATION AND CHECK

4.1. Preparing to install NM A&C AS

Preparation for the installation of NM A&C AS includes the installation and configuration of the following software products on the server:

IIS (Internet Information Services)

MS SQL server

MS Visio

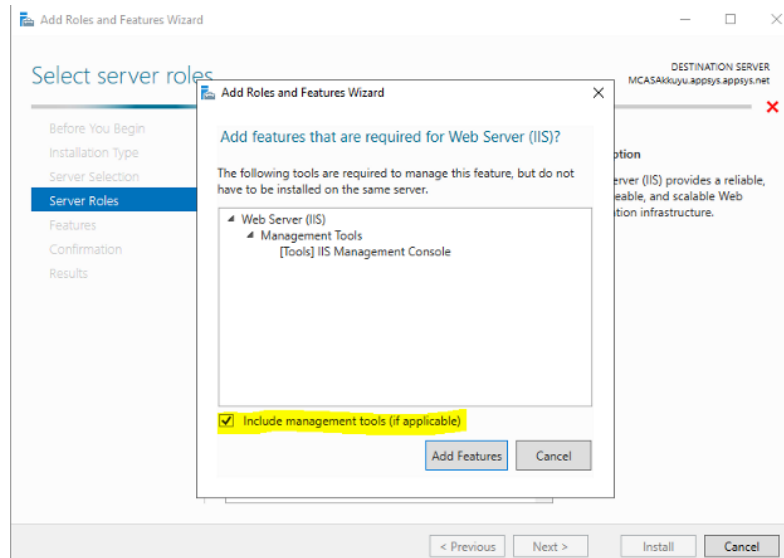
(optional) SSL certificate

Atomic Keeper.

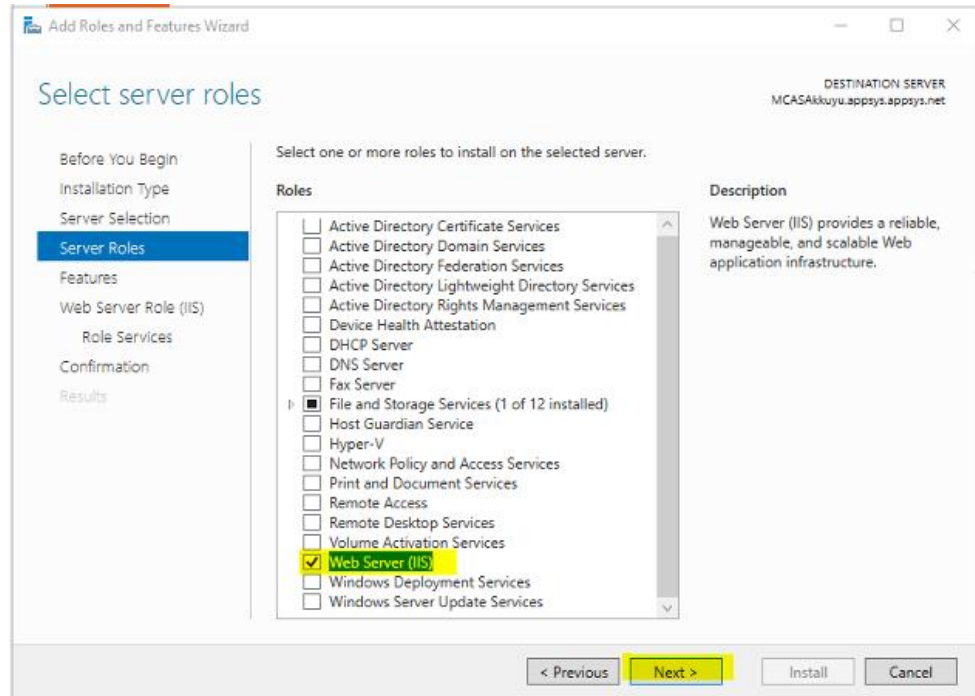
4.2. Installing and configuring IIS (Internet Information Services)

IIS is the built-in software for deploying a web server in Windows. IIS is required to run the AtomicKeeper application and make it available to users. Installing and configuring IIS is performed in the following sequence:

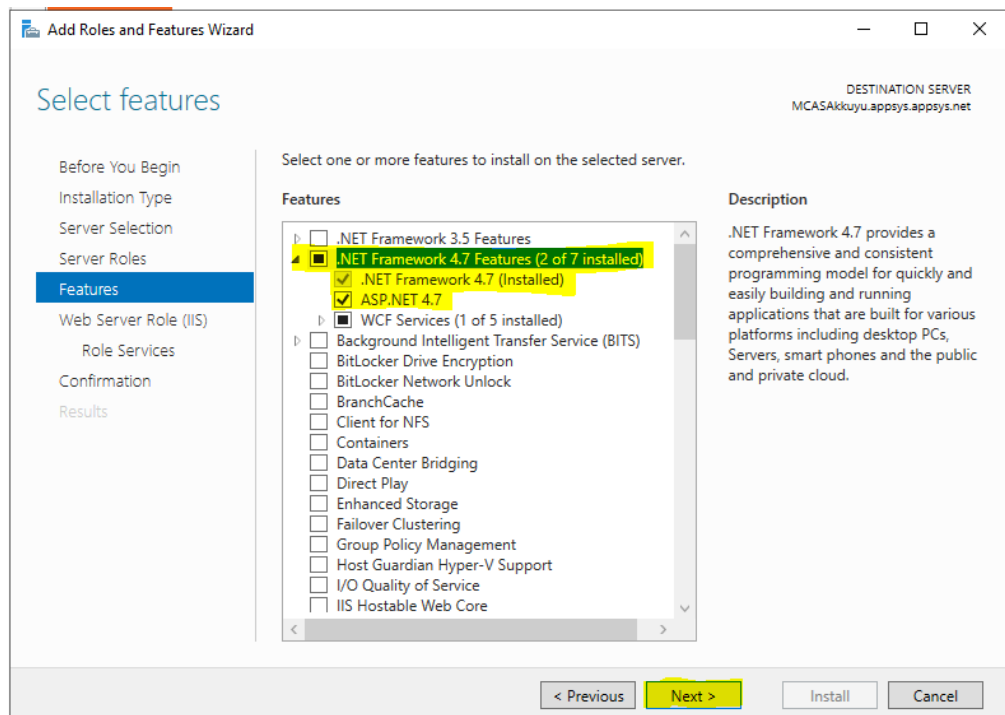
1. Start Windows
2. Press Windows + R
3. Enter appwiz.cpl and press the Enter key.
4. In the left pane, select Turn Windows features on or off.
5. On the Before you begin, Installation Type, Server Selection tabs, click Next.
6. On the Server Roles tab, select Web Server (IIS). Make sure all attachments are selected.
7. In the Add Roles and Features Wizard window that opens, check the Include management tools (if applicable) checkbox and click Add Features:



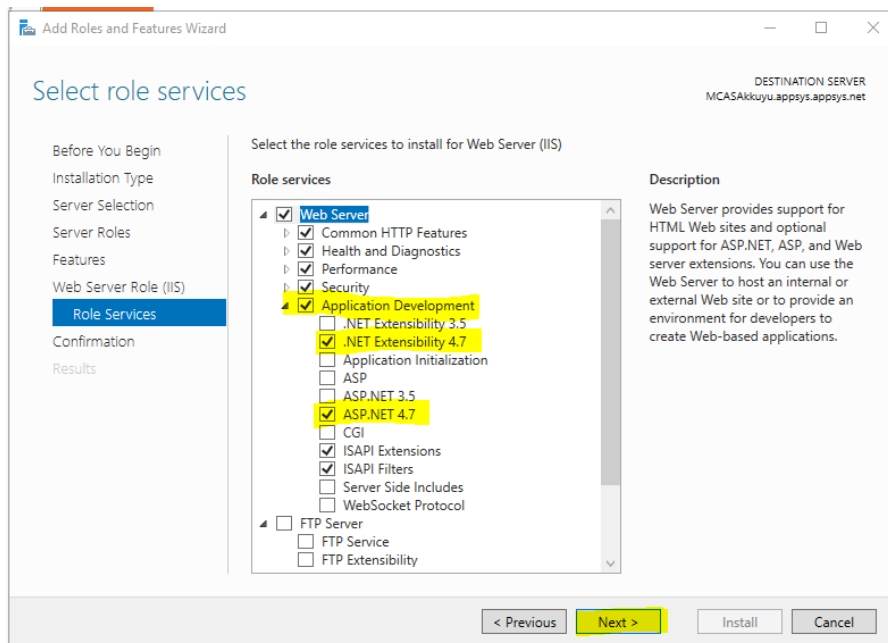
8. Push Next:



9. On the Features tab, expand .NET Framework 4.7 Features and make sure ASP.NET 4.7 and .NET Framework are selected, then click Next:

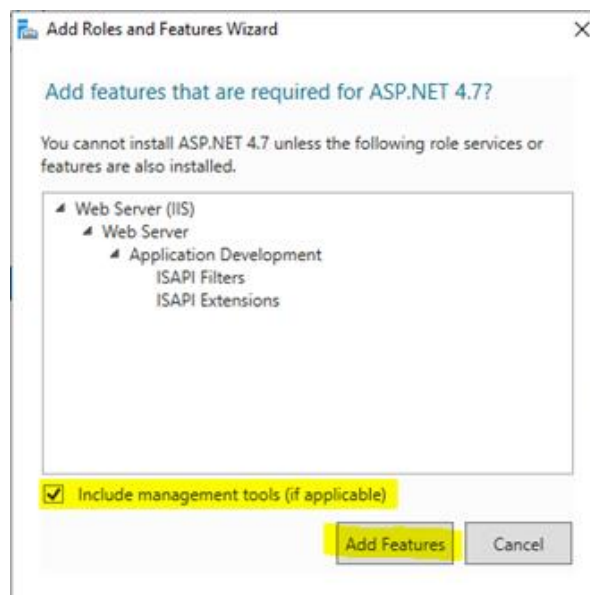


10. Expand Role Services, select Application Development and make sure that .Net Extensibility 4.X и ASP .NET 4.X are selected:



11. Push Next

12. In the window Add Roles and Features Wizard check Include management tools (if applicable) and press Add Features:



13. Push Next

14. On the tab Confirmation push Install.

4.3. Configuring MSSQL Server

SQL Server is software from Microsoft. It is a complex product that contains the functionality necessary for creating and managing databases. Needed here to store data generated or entered by the user while AtomicKeeper is running.

To configure SQL Server, the following prerequisites must be met:

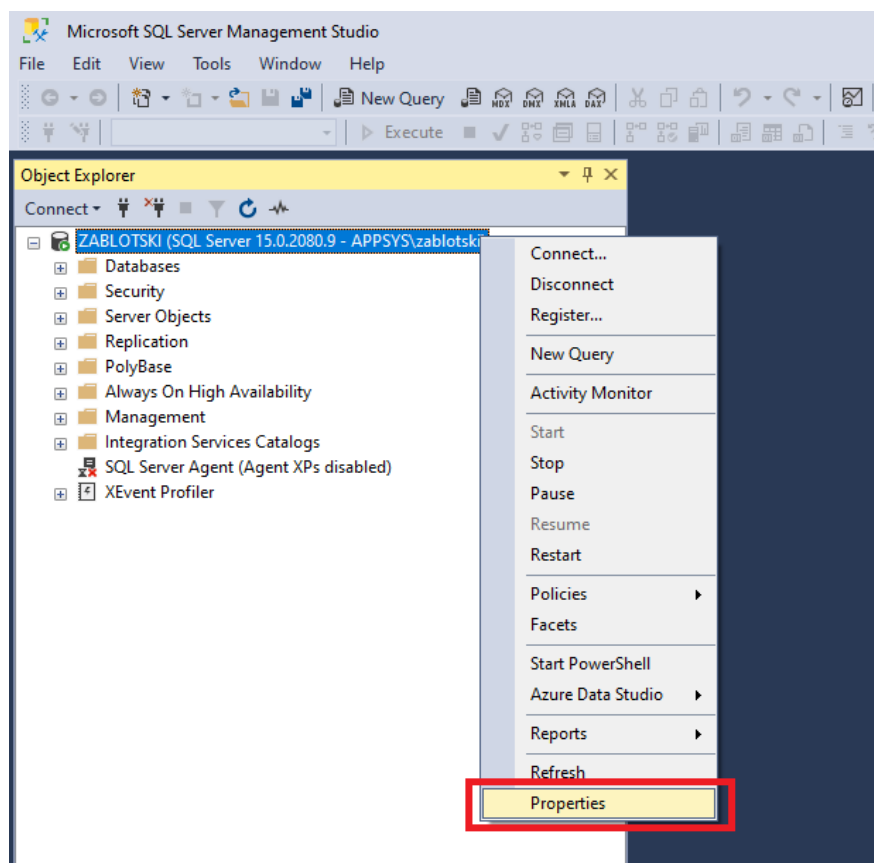
1. SQL Server 2016+ is installed with full functionality (on the Feature Selection tab, the Select All option is activated).

2. SQL Server Management Studio is installed.

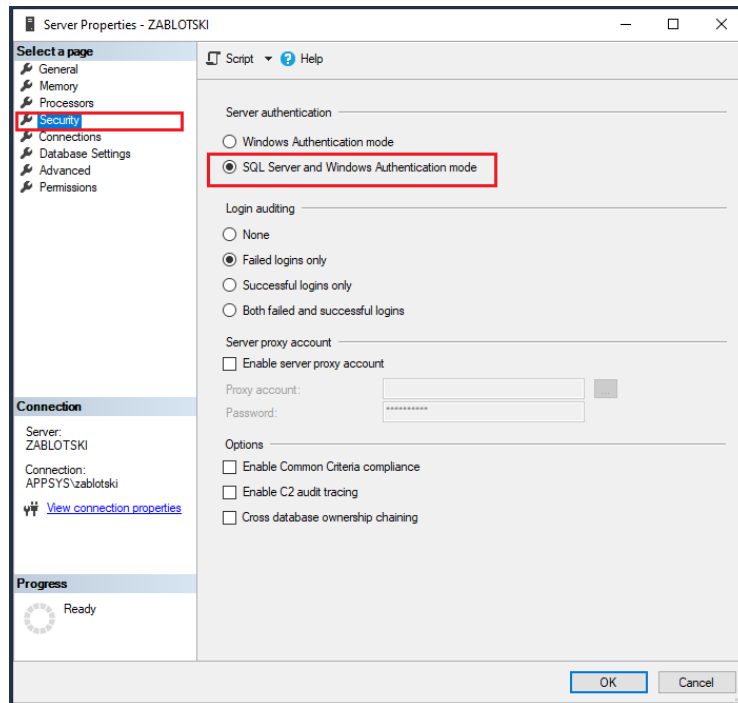
The MSSQL Server setup is performed as follows:

1. Open SQL Server Management Studio.

2. On the Object Explorer page, right-click to highlight the server, then select Properties:



1. On the page **Select a page**, select **Security** → **Server authentication** → **SQL Server and Windows Authentication mode** and push **OK**:



2. In the dialogue **SQL Server Management Studio** push **OK**, allowing the SQL Server to restart.

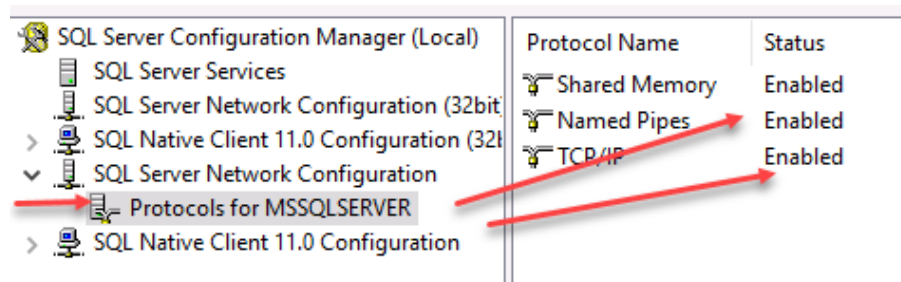
3. In **Object Explorer**, right-click on the server, push **Restart**. Even if **SQL Server Agent** is active at the moment, it should be restarted.

4. Activate the **Named pipes** and **TCP** protocols support.

4.1. Open **SQL Server Configuration Manager**.

4.2. Expand **SQL Server Network Configuration** -> **Protocols for MSSQLSERVER**.

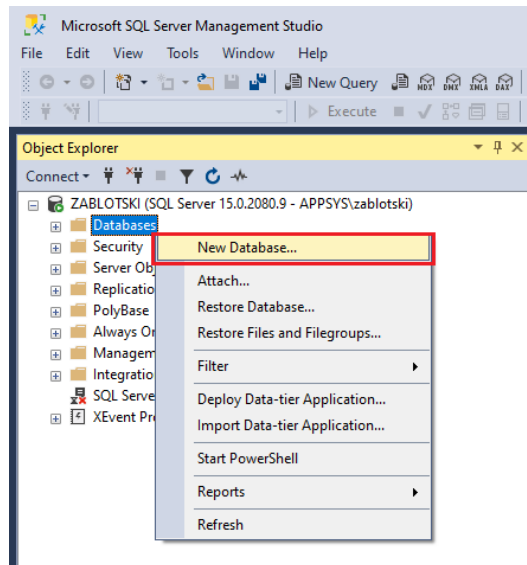
4.3. Enable the support of **Named Pipes** and **TCP/IP** protocols, unless they haven't been checked earlier. For that, right-click the protocol > **Enabled**:



4.4. Restart **SQL Server services** or the computer.

5. Creating a DB:

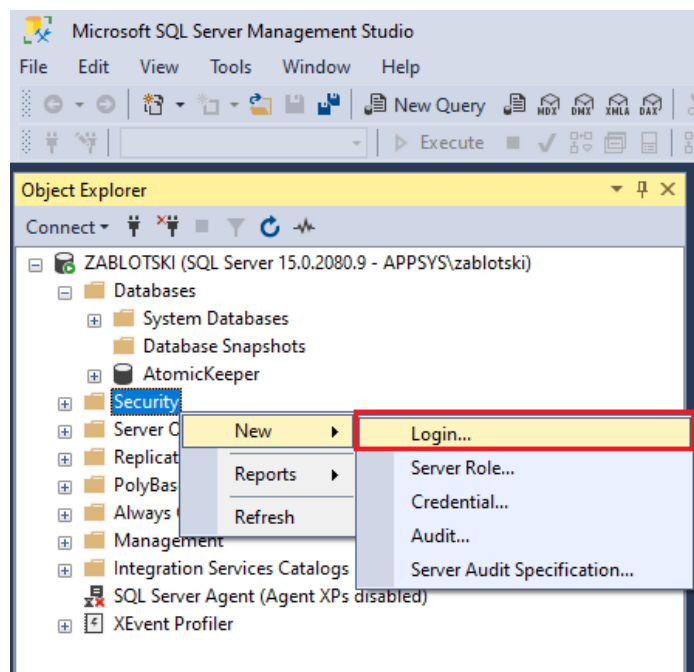
5.1. In **SQL Server Management Studio Object Explorer**, right-click on **Databases > New Database**:



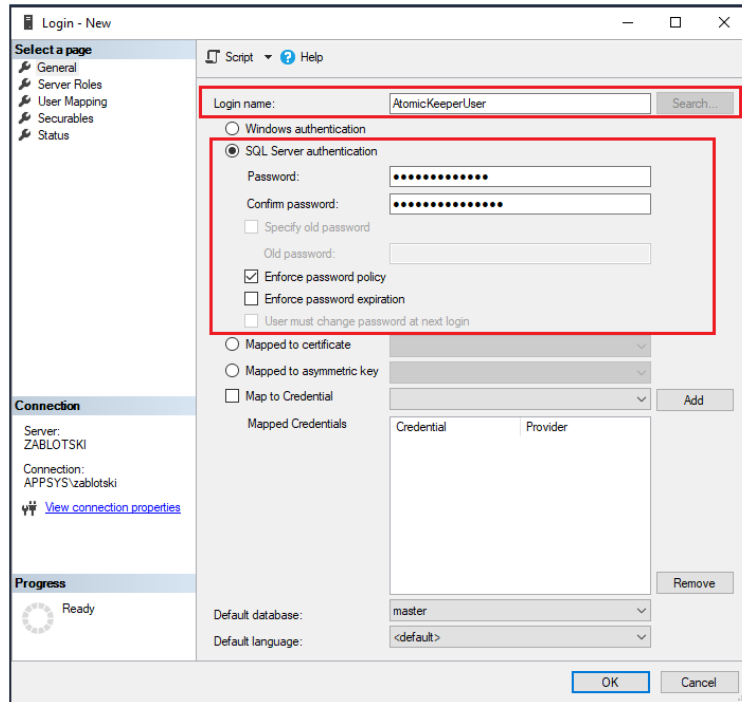
5.2. On the **General** tab, enter a name (any) in the **Database name** field > **OK**.

6. Create Login:

6.1. In **SQL Server Management Studio Object Explorer**, right-click **Security** > **New** > **Login**:



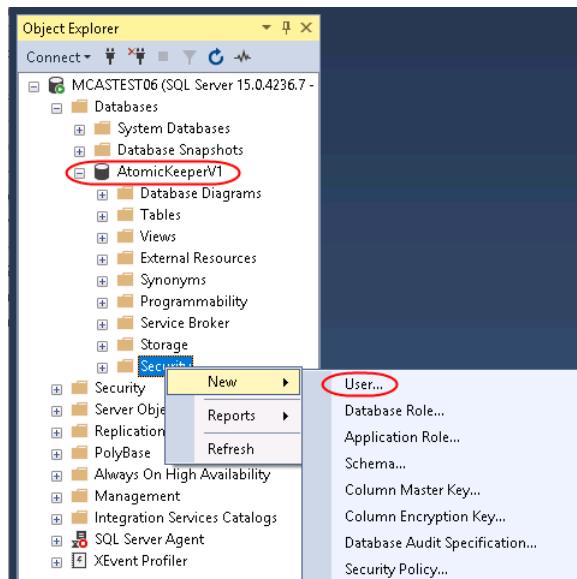
6.2. On the **General** tab, select **SQL Server authentication**, enter **Login name**, fill in the **Password** and **Confirm password** fields. Deactivate the options **Enforce password expiration** and **User must change password at next login**.



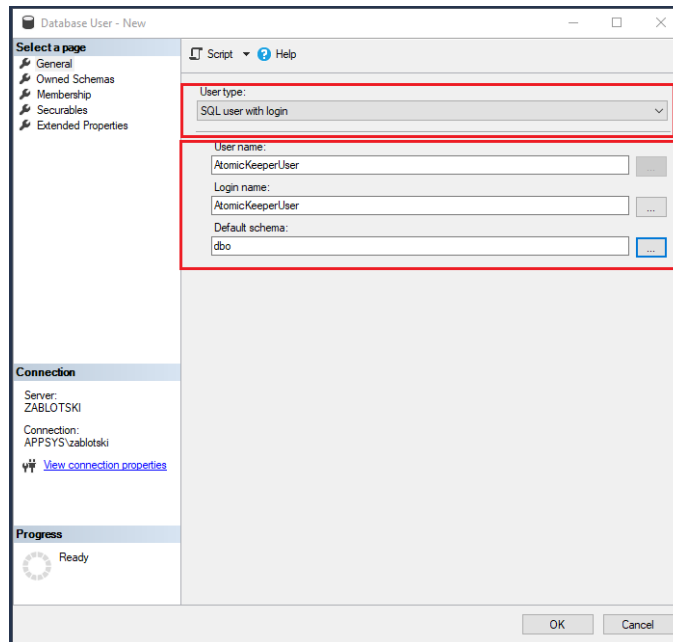
6.3. Push OK

7. Create a Database User.

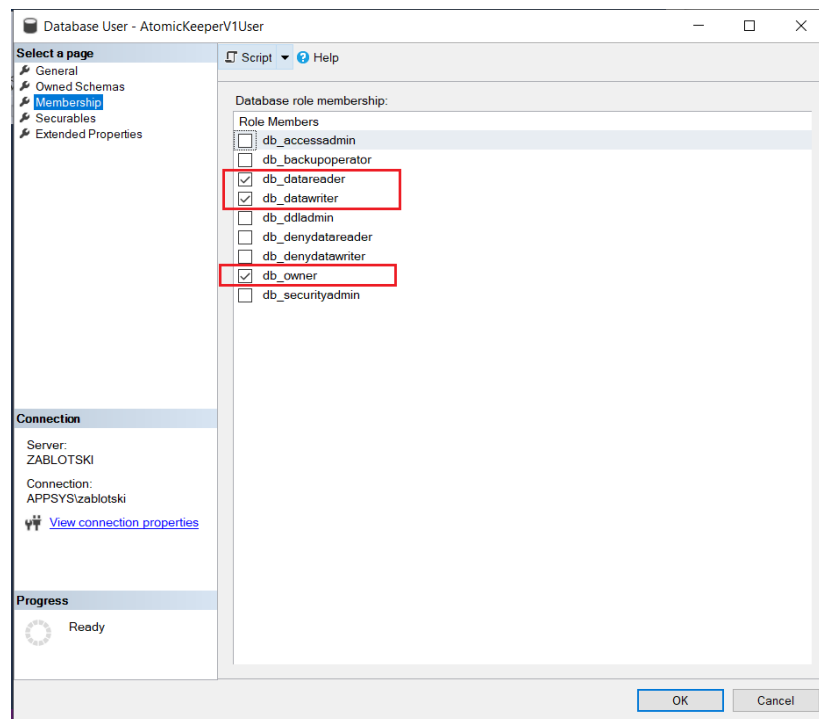
7.1. In **Server Management Studio Object Explorer**, expand the **Databases** section, find your DB on the list and click the **Security** tab, > **New** -> **User**



7.2. On the **General** tab, select **User type** > **SQL user with login**, enter **User name**, in the field **Login name** select **login**, created earlier, in the field **Default schema** select **dbo**:

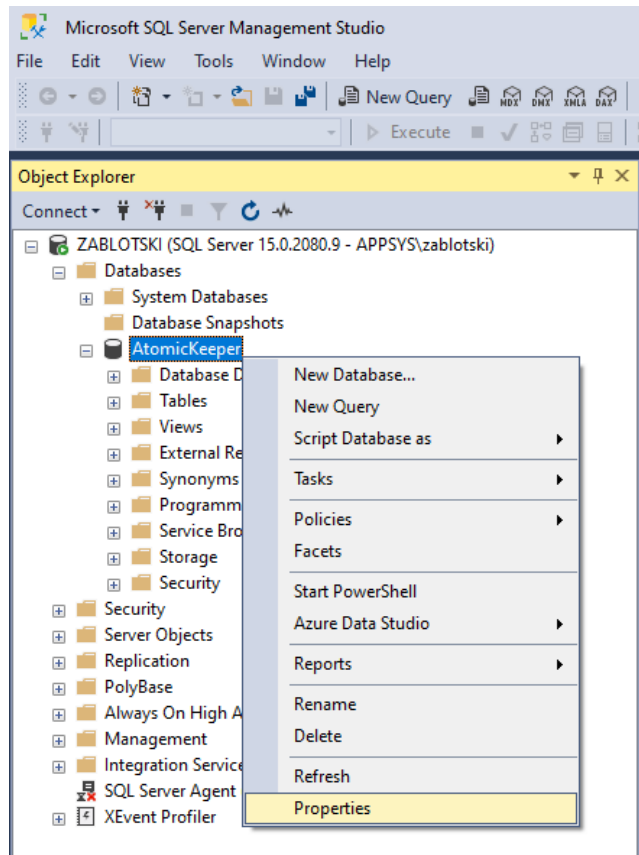


7.3. On the panel **Database role membership** check the roles **db_datareader**, **db_datawriter** and **db_owner**.

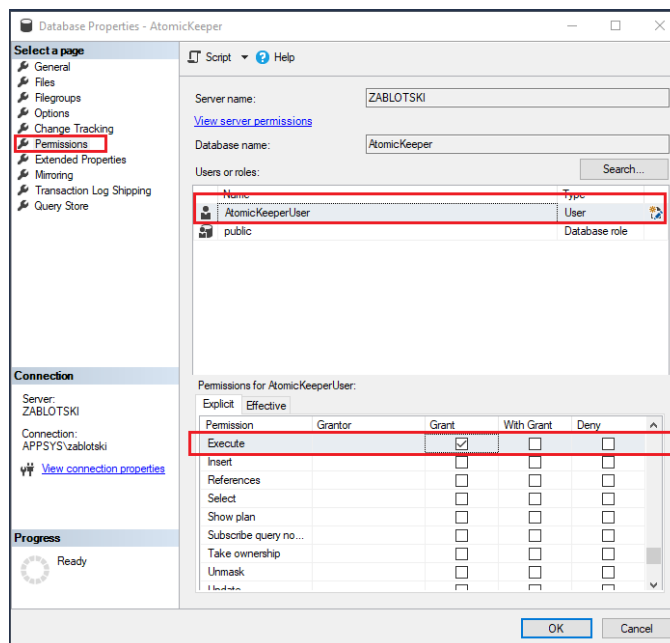


7.4. Push **OK**.

8. Right-click on your DB in **SQL Server Management Studio Object Explorer** > **Properties**:



9. On the left pane **Permissions** select your user name. Then, on the list **Permissions for AtomicKeeperUser** tick the **Grant** in the **Execute** line:



10. Push **OK**.

4.4. Configuring Visio.

MS Visio is software from Microsoft that is needed here to generate and print cartograms.

Prerequisites for using Visio:

The user logs in from **Administrators group**. If the user logs out, Visio stops operating.

Configure Visio as follows:

1. Open **Components Services**:

For Visio 32-bit:

1.1. Open Command Prompt as Administrator.

1.2. Run command: **mmc comexp.msc /32**

For Visio 64-bit:

1.3. Open Command Prompt as Administrator.

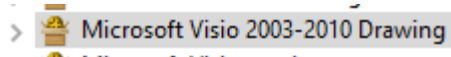
1.4. Run the command: **mmc comexp.msc /64**

2. Configuring **Microsoft Visio DCOM**:

2.1. Open **Component Services > Computers > My Computer > DCOM**

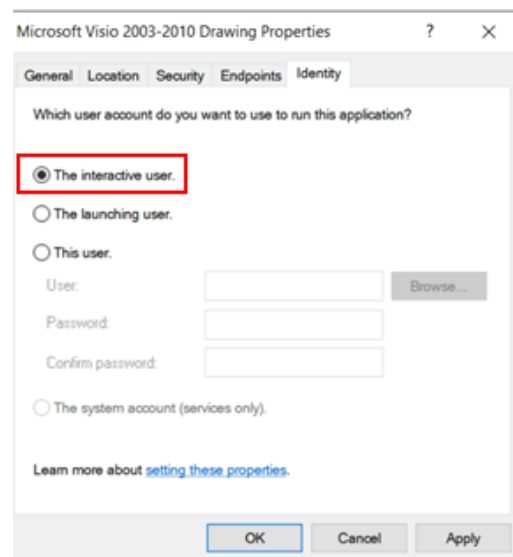
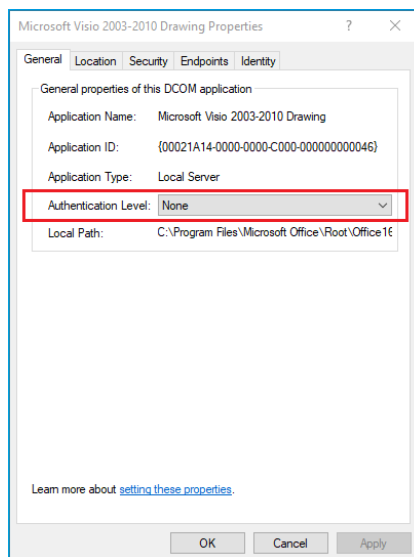
Config.

2.2. Find on the list **Microsoft Visio 2003-2010 Drawing**.



2.3. Right-click on **Properties**.

2.4. On the **General** tab set **Authentication level** to **None**:



2.5. On the **Identity** tab select **The interactive user**.

2.6. Push **Apply** and **OK**.

4.5. Generating a self-signed SSL certificate

In order to ensure secure and confidential data exchange between AtomicKeeper and user PCs, support for the HTTPS protocol has been added to the system. Secure data transfer via the specified protocol is ensured using an SSL certificate. Therefore, an SSL certificate is integrated into the installation package.

The ability to specify a user certificate has been added to the AtomicKeeper installation package. If a user certificate is not specified, the system will be installed with a default certificate ("default SSL certificate"). The default certificate is a self-signed certificate created on the side of the developer company (how to create a self-signed certificate, see the instructions below). The default certificate will be sufficient for security on the internal network. Its only drawback is that users who will connect to AtomicKeeper through a browser will see a warning that the certificate is not trusted. Not only a self-signed certificate, but also any other certificate (domain, public, purchased from a trusted certification organization, etc.) can be used as a user certificate. The only requirement is the format of the certificate. The certificate must be in .pfx format.

Prerequisites for creating a certificate - The **openssl** utility is installed.

To generate a self-signed SSL certificate:

1. open the command prompt (cmd) and run the following commands:

```
openssl req -x509 -sha256 -nodes -days NDAY -newkey rsa:2048 -keyout KEYPATH -out CRTPATH
```

Where the following parameters are used:

- NDAY - certificate validity period in days.
- KEYPATH - path to save the key (example: D:\mycert.key).
- CRTPATH - path to save the certificate (example: D:\mycert.crt).

1.1. Converting a certificate in the format (.crt) and a key (.key) to .pfx format:

Important: after executing the command, the system will ask you to enter and confirm a password to protect the certificate. REMEMBER IT. You will need it for further use of the certificate.

```
openssl pkcs12 -export -out PFXPATH -inkey KEYPATH -in CRTPATH
```

Where the following parameters are used:

PFXPATH - path to save the certificate in the pfx format(e.g. D:\mycert.pfx).

KEYPATH - path to save the key (e.g. D:\mycert.key).

CRTPATH - path to save the certificate (e.g. D:\mycert.crt).

4.6. Installing the AtomicKeeper application

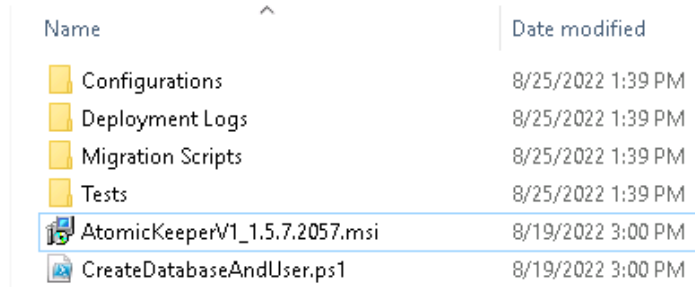
The installation of the AtomicKeeper application can be done in two ways:

Default installation (using UI);

automated installation (via command line).

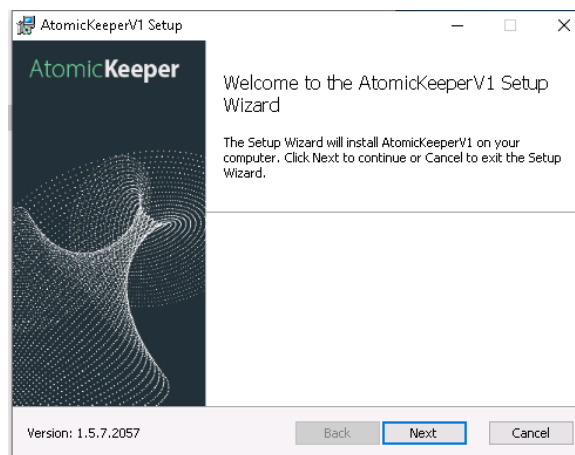
1. Default installation (using UI):

1.1. Unpack the distribution archive ("AtomicKeeperV1_X.X.X.XXXX.zip") to any folder. An example of an unpacked archive looks something like this:

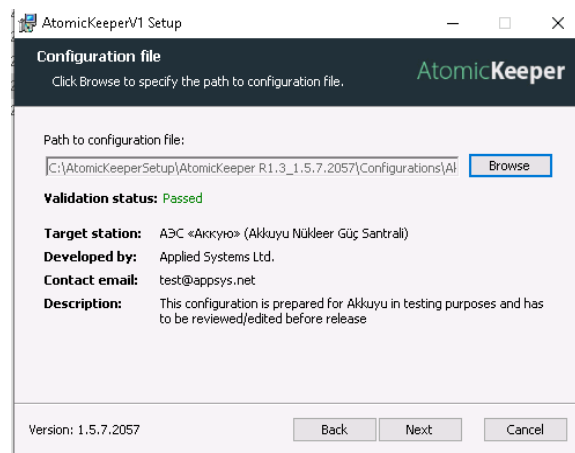


1.2. Run the setup file with the *.msi extension (example: AtomicKeeperV1_1.5.7.2057.msi) by double clicking.

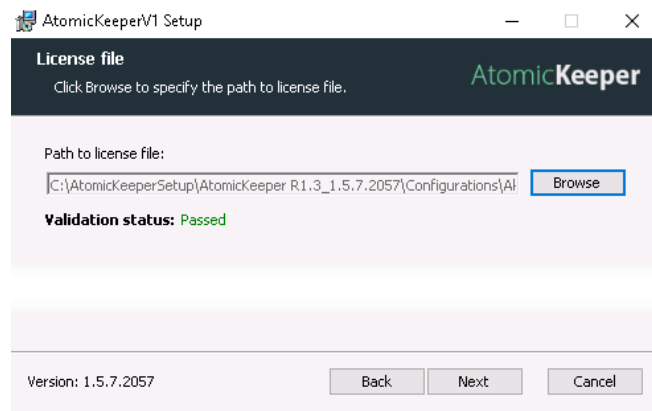
1.3. In the dialog box, click Next.



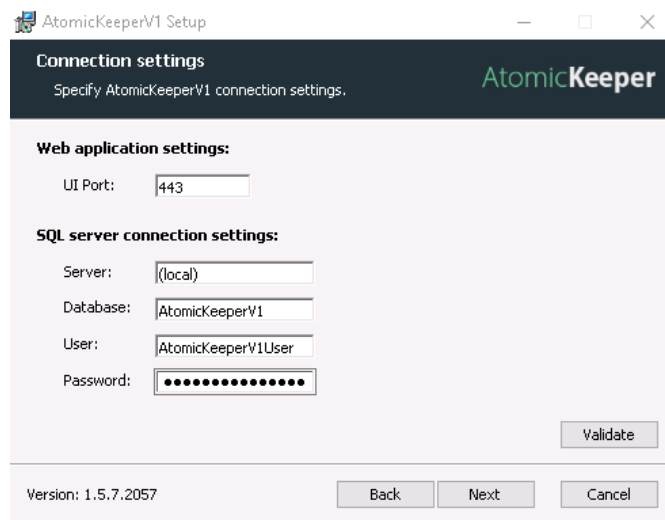
1.4. In the Configuration file dialog that appears, click Browse and specify the path to the Akkuyu.zip configuration file. (The configuration file is in the "Configurations" distribution folder) then click Next. If the configuration file is invalid, the Next button will be disabled.



1.5. In the License file dialog box, click Browse and specify the path to the Akkuyu.lic license file (the license file is in the "Configurations" distribution folder), then click Next. If the license file is invalid, the Next button will be disabled.



1.6. In the Connection settings dialog box, enter the data required to connect to the database (they were created in section 3.3), and then click Next.



UI Port – AtomicKeeper application access port (default 443)

Server – the name of the server where the database is installed (*local* if the database is on the same computer).

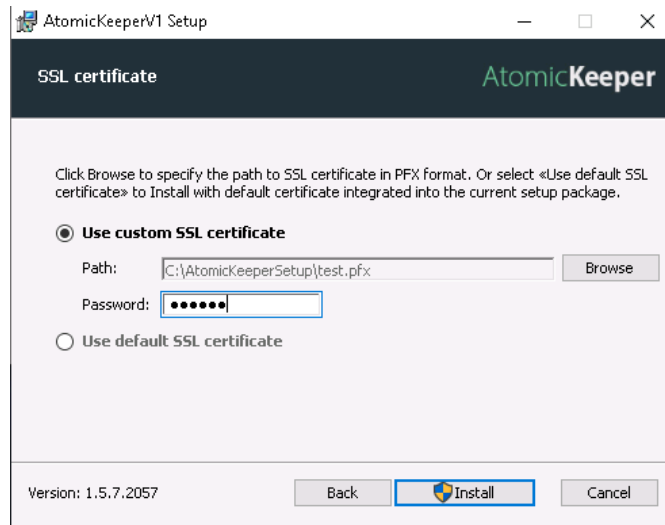
Database - the name of the database

User – the username to connect to the database

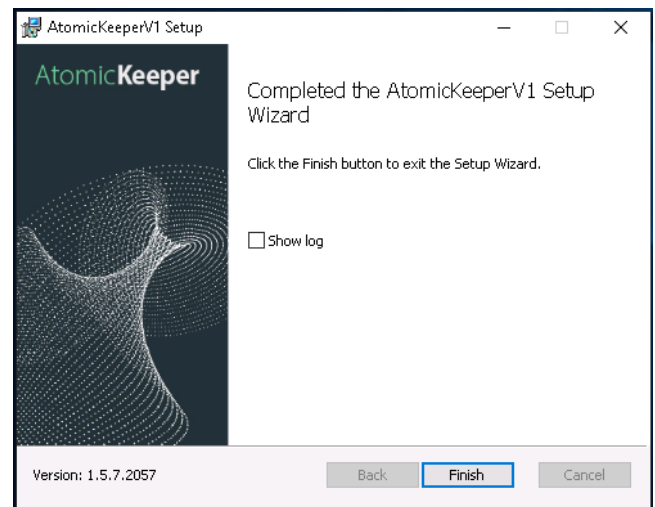
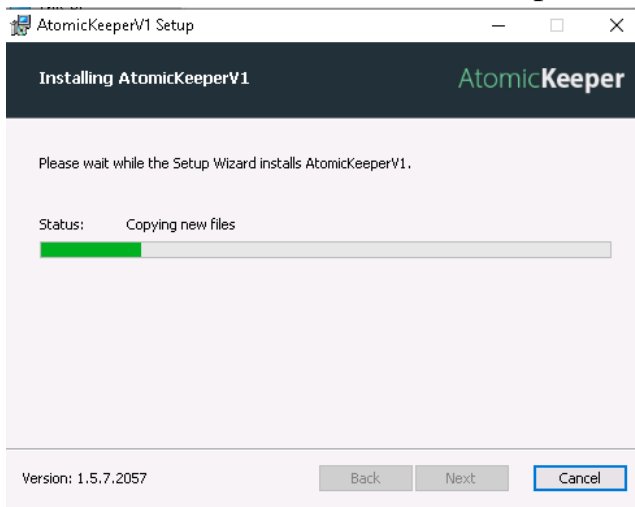
Password – the user password to connect to the database.

1.1. In the **SSL certificate** dialog, activate one of the following options: **Use custom SSL certificate** or **Use default certificate**.

1.7. When using the Use custom SSL certificate option, you will have to specify the path to your certificate in .pfx format (created in section 3.5.), as well as the password that is used to protect the certificate. Then click Install.



1.8. Wait for the installation process to finish.



1.9. Click the **Finish** button.

2. Automated installation.

Automated installation means installation of an application from the command line.

To perform an automated installation, you must:

2.1. Run Command Prompt as Administrator.

2.2. Run the following command:

```
Msiexec /I PATH_TO_MSI /QN /L*V PATH_TO_LOG_FILE Arg1=Value1  
Arg2=Value2 ... ArgN=ValueN
```

Where the following parameters are used:

PATH_TO_MSI - path to the msi file for AtomicKeeper

PATH_TO_LOG is the path to the folder where the log file will be saved.

Argument list:

1. CONFIG_ZIPPATH (default value: empty) - path to the configuration file
2. LICENSE_PATH (default value: empty) - path to the license file

3. USE_DEFAULT_CERT (default value: false) - set to True for installation with default SSL certificate.
4. USER_CERTPATH (default value: empty) – path to SSL certificate in pfx format.
5. USER_CERTPASSWORD (default value: empty) – password for SSL certificate
6. UI_PORT (default value: 80) – port for accessing the WEB application.
7. SQL_SERVER (default value: (local)) is the name of the SQL server.
8. SQL_DBNAME (default value: AtomicKeeperV1) is the name of the database on the SQL server.
9. SQL_USER (default value: AtomicKeeperV1User) is the username for the AtomicKeeperV1 application (needed to connect to the database).
10. SQL_USER_PASSWORD (default value: G#cV-k3X@rj0gPb) – user password used by the AtomicKeeperV1 application to access the database.

4.7. Checking the functionality of the installed software.

After successful installation of the software, it is necessary to check the basic functionality of the administrator.

Validation testing consists of running the tests listed in Appendix A and testing the admin user interface in parallel.

5. DESCRIPTION OF ADMINISTRATOR OPERATIONS

5.1. Login to the system administration page.

To enter the NM A&C AS administration page, you must:

1. Enter the address of the application in the address bar of the browser and press the Enter key. You will be redirected to the system login page.
2. In the **Login** field, enter a login to log in with administrative rights.
3. In the **Password** field, enter a password.
4. Click the **Login** button. You will be taken to the System Administration Page.

5.2. Create a user account

1. Log in to NM A&C AS with administrative rights.
2. Click the "Register" button
3. Register a new user with the role "user":
 - a) enter personal data in the form
 - b) in the **Login** and **Password** fields, specify the authentication parameters for the registered user.
 - c) in the **IP address** field, enter the personal IP address of the computer from which the user will log in. Click the "Register" button.

As a result of performing these actions, a user will be added to the system with the “user (unsigned)” role. The initial password is transmitted by the system administrator to the registered user for the first login. After the first login, the user will be required to enter a new personal password and the role will change to "user".


5.3. Account deactivation

Your account may be deactivated to prevent unauthorized access. The administrator has the option to deactivate the account manually (forcibly) with the following steps:

1. Log in to NM A&C AS with administrative rights.
2. Click on the edit button for the user to be deactivated.
3. Uncheck the "Active" checkbox and click the Edit button.

5.4. Changing data in a user account.

To change a user account, follow these steps:

1. Log in to NM A&C AS with administrative rights.
2. Select the entry you want to change and click on the edit button  , located in the last column. The form for editing the user record will open.
3. Make the necessary changes.
4. Click the Edit button.

As a result of these actions, the user record will be edited.

5.5. Reset the password for a user entry.

1. Log in to NM A&C AS with administrative rights.
2. Select the entry for which you want to change the password and click the edit button. The form for editing the user record will open.
3. Click the *Reset password* link. A form for entering a new password will open.
4. Enter a new password for the initial user entry.
5. Click the **Update Password** button

As a result of these actions, the administrator will reset the user's password, after which the user (during the initial login after resetting the password) will have to enter a new password, then enter a personal password on the page that opens.

5.6. Viewing the log of user actions (logging).


1. Log in to NM A&C AS with administrative rights.
2. On the administration page, open the main navigation menu and select **Audit Log**.
3. A page will open with a list of all actions in the system, indicating the time of the changes made and the user who made the changes.

5.7. Authentication settings.

1. Log in to NM A&C AS with administrative rights.
2. Select **Settings** from the main navigation menu.
3. Set the necessary parameters for authentication.
4. Click **Save**.

5.8. Unlock account.

To prevent unauthorized access, the account can be automatically blocked if the authentication parameters are set in the **Settings**. To unlock a user account, you must:

1. Log in to NM A&C AS with administrative rights.
 1. From the main navigation menu select **Blocked IPs**.
 2. Remove the desired IP Address from the list and, in the main menu, go to **User list**.
3. Press edit button  on the blocked account.
4. Check the box **Active**.
5. Push **Save**.

6. EMERGENCY ACTIONS

The system must ensure correct handling of emergency situations caused by incorrect actions of the administrator, incorrect format or invalid input data values. In these cases, the administrator should be given appropriate alarm messages, and then return to the working state that preceded the incorrect (invalid) command or incorrect data entry. Emergency situations can occur both due to errors in software products, and due to incorrect settings.

The main signs of an emergency are:

1. Absence of the necessary page on the screen.
2. Windows with messages about an emergency.
3. Windows with messages in English.
4. Errors related to the software.

6.1. Actions in case of non-compliance with the conditions for the implementation of the technological process, including the case of long-term failures of technical means

After receiving an error message, you must follow the recommendations indicated in the message, if any, otherwise reload the page, check the network connection. If the error message recurs, please contact NM A&C AS. When contacting the developer, you must specify the course of action that led to the error, including providing the information entered into the system, if an error occurred while entering it, the data of the user's activity log.

6.2. Actions to restore programs and / or data in case of failure of magnetic storage media or detection of errors in data

If magnetic media fails or errors are found in the data, the system administrator must restore the files and data necessary for the correct operation of the system from the latest backup. If the administrator cannot correct errors in the data, the NM A&C AS developer should be contacted. In this case, it is necessary to specify a list of data containing errors and the correct values of distorted attributes

6.3. Actions in cases of detection of unauthorized data tampering

In the event when unauthorized interference with NM A&C AS data is detected, the system administrator must restore the files and data necessary for the correct operation of the system from the latest backup. You should also contact the NM A&C AS developer and describe the signs and the expected nature of the intervention, as well as indicate the list of data subjected to interference.

6.4. Actions in other emergencies

If other emergencies occur while working with NM A&C AS and it is impossible to eliminate them using the administration tools, the database management system, the operating system, you should contact the system developer. In this case, it is necessary to describe the signs of an emergency and the actions that were performed by the user immediately before the occurrence of an emergency. The main possible emergency situations and their solutions are described below.

Emergency situation	Possible loss of information	Method of fixing consequences	Executor
Turn off hardware power	User unsaved data	Re-entering and saving information	User
Hardware failure (excluding hard drive)	User unsaved data	Re-entering and saving information	User
Server operating system failure	All information that has entered the System since the end of the last data backup.	Restoring backup data	Administrator
Hard drive failure	All information that has entered the System since the end of the last data backup.	Restoring backup data	Administrator
Failed to transfer data	Information transmitted	Resending data to the server	User
The required page on the screen is missing	User unsaved data	Reloading the page with the "Refresh" button of the Internet browser; return to the previous page and click again on the link to the required page	User
Exception message windows	User unsaved data	Follow the instructions in the message, if any. If necessary, contact the administrator.	User
Windows with messages in English	User unsaved data	Обратиться к администратору	User

Emergency situation	Possible loss of information	Method of fixing consequences	Executor
Software-related errors	Information entered into the system since the end of the last data backup	Restarting the relevant software, rebooting the server, restoring data from backups	Administrator
Long loading pages of NM A&C AS "Atomic Keeper" software	Missing	Together with the information security staff of the organization, configure the antivirus "Kaspersky Security for Windows Server"	Administrator

