Applied Systems Ltd

ADMINISTRATOR'S GUIDE FOR THE MODULE ON ACCOUNTING FOR NUCLEAR MATERIALS AT LOFs OF THE AUTOMATED SYSTEM FOR ACCOUNTING AND CONTROL OF NUCLEAR MATERIALS «ATOMIC KEEPER»

Minsk, 2023

CONTENTS

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

1. GENERAL PROVISIONS

The Administrator's Guide for the “Atomic Keeper” v.2.0 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.

1.1. Application area

The nuclear materials accounting and control automated system “Atomic Keeper” (hereinafter referred to as NM A&C AS 2.0) 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.

1.2. Main features and functions of NM A&C AS 2.0.

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 2.0 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. formation of working documentation required by NPP specialists before, during or after the performance of work with nuclear materials;
6. providing data on the amount of nuclear materials in all MBAs and KTIs;
7. formation of documentation on the presence of nuclear materials and accounting reports of the established form (ICR, PIL, MBR);
8. maintenance of accounting documents (Main and Auxiliary journals, registration cards, cartograms of nuclear materials placement);
9. provision of information support for inspections and physical inventories conducted on the territory of the NPP;
10. Ensuring the verification of input (selected) data for compliance with validation criteria.

1.3. 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.

2. BASIC DESCRIPTION OF THE SYSTEM ARCHITECTURE

2.1. 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:

- User interface level;
- The level of business logic;
- 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.

2.2. Software elements

The system is implemented using the following technologies:

1. NET 6;
2. ASP.NET Core 6;
3. DBMS MS SQL Server or PostgreSQL;
4. HTML5, CSS3
5. C#, Transact-SQL, TypeScript, JavaScript, Angular 12.

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

1. Server part

1.1. Для Windows:

OS Windows Server 2019;

DBMS MS SQL Server 2019 or PostgreSQL 14;

1.2. For Linux:

Linux Astra Smolensk 1.6;
PostgreSQL 9.X
2. Client part
OS Windows 10;
Web browser Chrome (105 and above);
Tools for creating and editing MS Office documentation (2016 and higher).

2.3. Safety Information for NM A&C AS 2.0

All user actions, performed in NM A&C AS 2.0, are recorded and stored in the event log indefinitely. To avoid audit log overflow and loss of records due to lack of disk space, the administrator needs to timely control the sufficient amount of memory on the server where NM A&C AS 2.0. (see 5.4).

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: admin) 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.

NM A&C AS 2.0 uses the following user roles:

Role	Purpose
Administrator	Performs the administrative functions of the NM A&C AS 2.0 described in chapter 4.
Commissioner	Assigned to the user for editing (adding/changing/deleting) information (if possible) in the sections of the "References" module.
Expert	Assigned to the user to perform the basic functionality of NM A&C AS 2.0. related directly to the accounting and control of NM SQ.

To separate the system files and configuration files belonging to NM A&C AS 2.0, as well as to separate the event log from user data, you need to install the NM A&C AS 2.0 and the database to different locations (directories, system partition, etc.). The exported event log should also be stored separately.

The modern Oauth 2.0 protocol is used for user authentication.

User access to NM A&C AS 2.0 functionality is provided by 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 people.

To prevent entering malicious commands into NM A&C AS 2.0 the validation of user-entered data is implemented.

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

3. PREPARATION FOR THE INSTALLATION OF NM A&C AS 2.0 "ATOMIC KEEPER". INSTALLATION AND CHECK

Preparation for the installation of NM A&C AS 2.0 includes installation and configuration on the server of the following software products (depending on the OS Windows or Linux):

MS SQL server (Windows only) or PostgreSQL

(optional) SSL certificate

SW NM A&C AS «Atomic Keeper» v.2.0.

3.1. Preparation for installation and installation of "Atomic Keeper" v.2.0 for Windows.

3.1.1. Configuring MSSQL Server

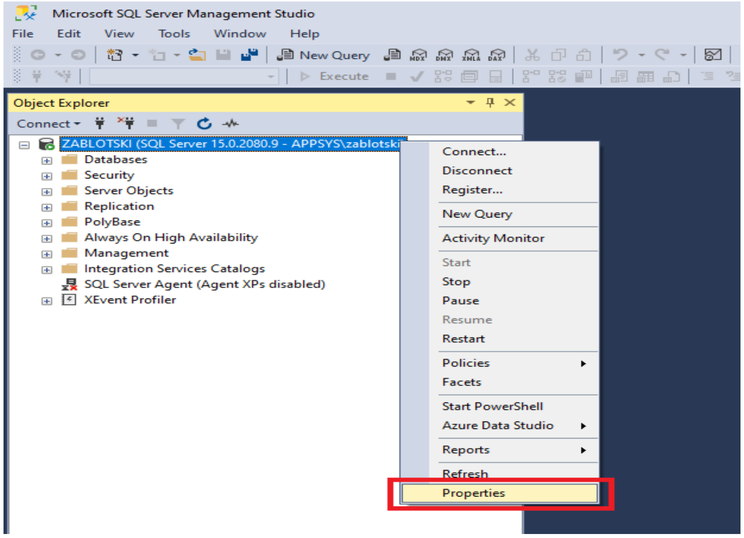
SQL Server is software from Microsoft. It is a complex product that contains the functionality necessary for creating and managing databases. Needed here to store data generated or entered by the user while AtomicKeeper is running.

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

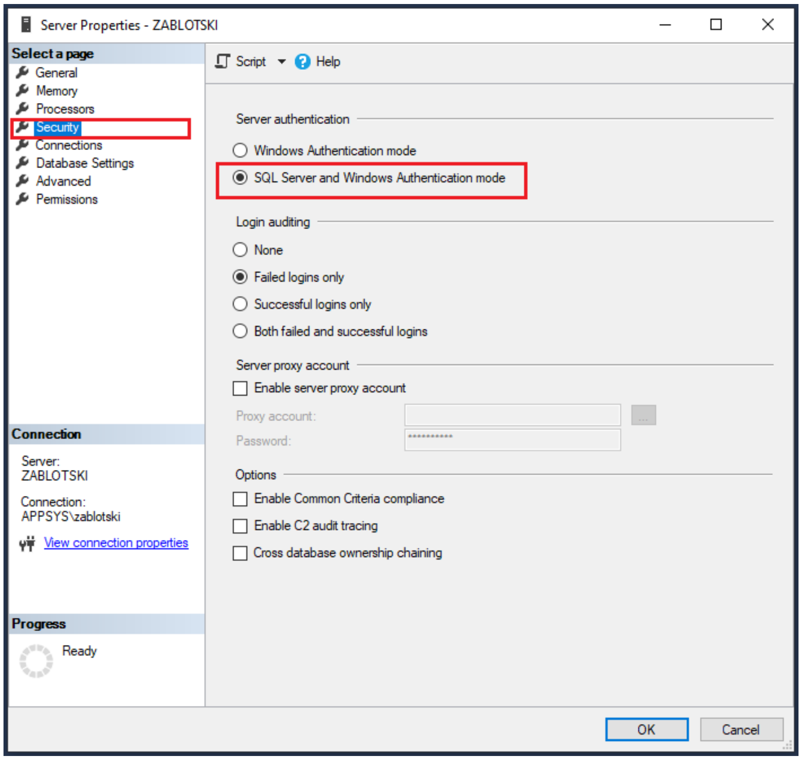
1. **SQL Server 2016+** is installed with full functionality (on the **Feature Selection** tab, option **Select All** is activated).
2. **SQL Server Management Studio** is installed.

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:**



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



Server authentication

○ Windows Authentication mode
● SQL Server and Windows Authentication mode

Login auditing

○ None
● Failed logins only
○ Successful logins only
○ Both failed and successful logins

Server proxy account

□ Enable server proxy account

Proxy account:

Password: **********

Options

□ Enable Common Criteria compliance
□ Enable C2 audit tracing
□ Cross database ownership chaining

Connection

Server:
ZABLOTSKI

Connection:
APPSYS\zablotski

View connection properties

Progress

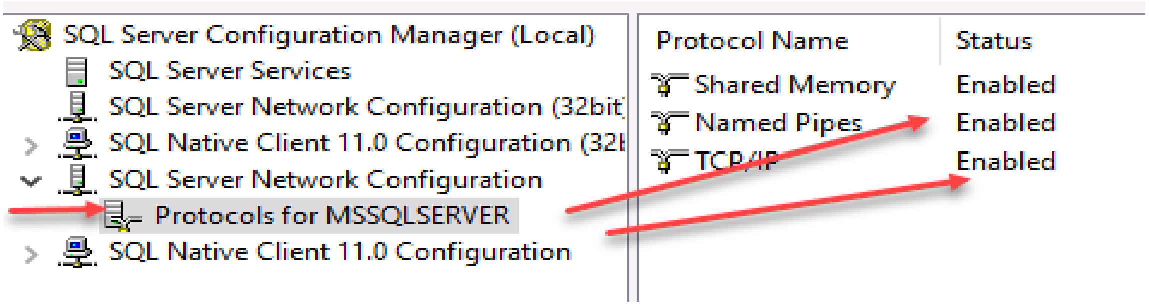
Ready

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

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**:


SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration (32bit
SQL Native Client 11.0 Configuration (32l
SQL Server Network Configuration
Protocols for MSSQLSERVER
SQL Native Client 11.0 Configuration

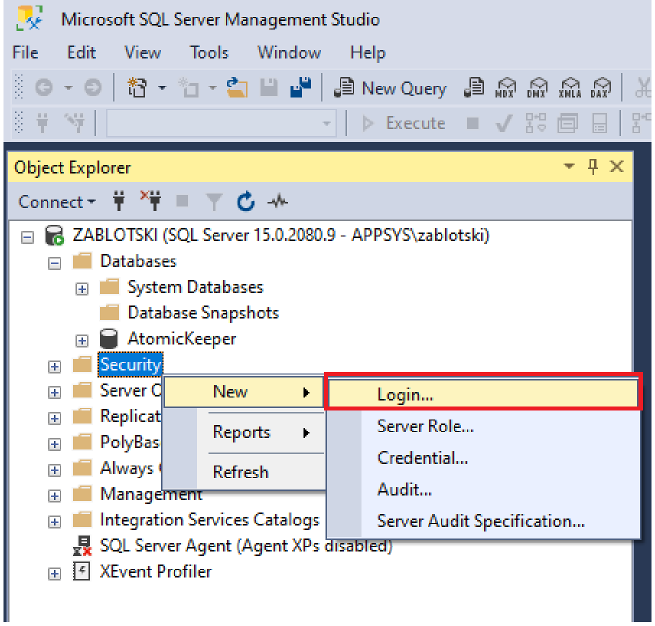
Protocol Name	Status
Shared Memory	Enabled
Named Pipes	Enabled
TCP/IP	Enabled

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

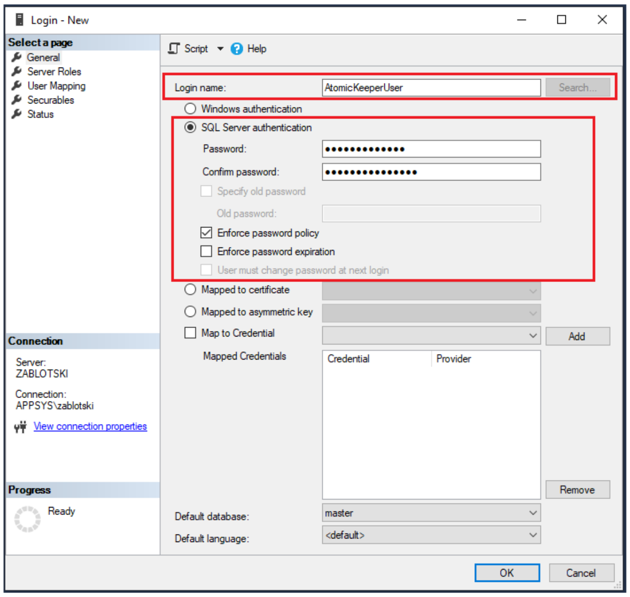
5. Create a user for SQL:

5.1. Launch SQL Server Management Studio.

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



5.3. 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**.



Login name: AtomicKeeperUser

○ Windows authentication

● SQL Server authentication

Password: ••••••••••••••

Confirm password: •••••••••••••••

□ Specify old password

Old password:

☑ Enforce password policy

□ Enforce password expiration

□ User must change password at next login

○ Mapped to certificate

○ Mapped to asymmetric key

□ Map to Credential

Mapped Credentials

Credential	Provider

Default database: master

Default language: <default>

Server: ZABLOTSKI

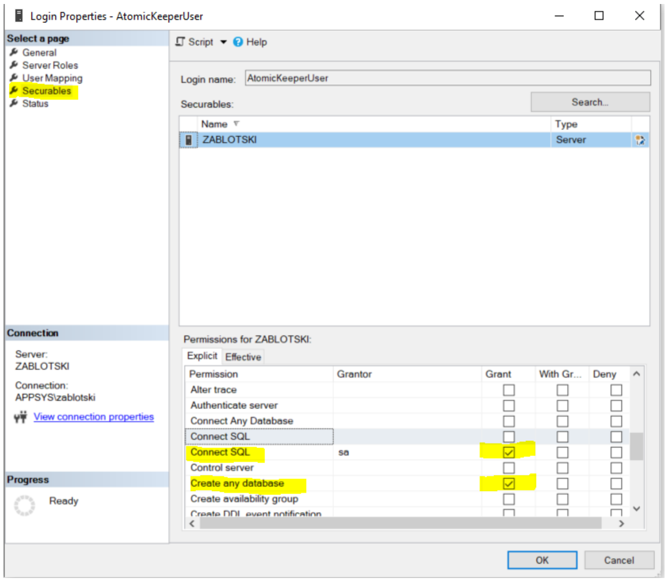
Connection: APPSYS\zablotski

5.4. Push **OK.**

5.5. In **Object Explorer** expand **Security** > **Logins**. Найдите здесь созданного пользователя на шаге 5, щелкните его правой кнопкой мыши и перейдите в раздел **Properties** > **Securables**.

5.6. In **Securables** enable the permissions **Create any database** and **Connect SQL**, unless they are already on. Push **OK.**

NOTE. After installing AtomicKeeper, the rights to create a database might be disabled.



Login name: AtomicKeeperUser

Securables:

Name	Type
ZABLOTSKI	Server

Server: ZABLOTSKI

Connection: APPSYS\zablotski

Permissions for ZABLOTSKI:

Explicit | Effective

Permission	Grantor	Grant	With Gr...	Deny
Alter trace		□	□	□
Authenticate server		□	□	□
Connect Any Database		□	□	□
Connect SQL		□	□	□
Connect SQL	sa	☑	□	□
Control server		□	□	□
Create any database		☑	□	□
Create availability group		□	□	□
Create DDL event notification		□	□	□

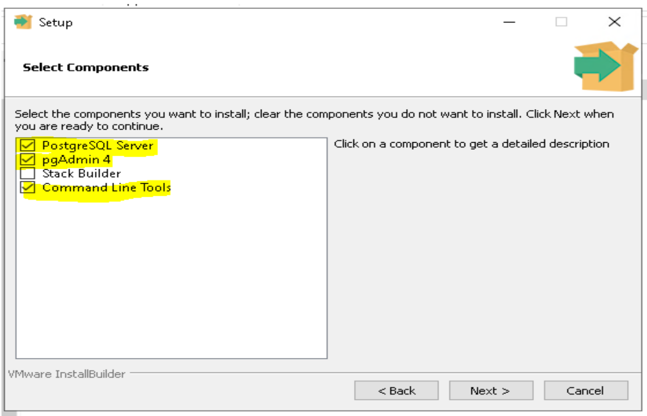
3.1.2. Configuring PostgreSQL.

PostgreSQL is a powerful open-source object-relational database system that uses and extends the SQL language, combined with many features to securely store and scale the most complex data workloads. PostgreSQL has many features designed to help developers build applications, and to help administrators protect data integrity and create fault-tolerant environments, and also help manage their data no matter how big or small the data set is.

1. Setting up PostgreSQL.

1.1. Download and run the installation package Postgresql 14.x.

1.2. During the installation process, select the following features: **PostgreSQL Server, pgAdmin 4, Command Line Tools.**

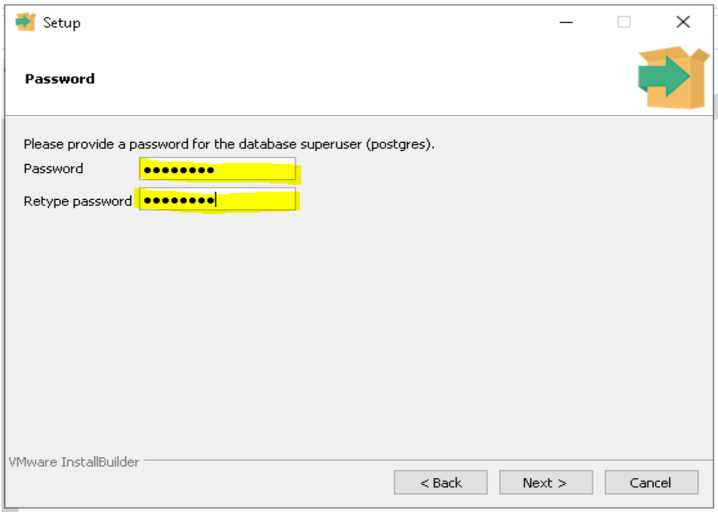


Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.

☑ PostgreSQL Server
☑ pgAdmin 4
□ Stack Builder
☑ Command Line Tools

Click on a component to get a detailed description

1.3. In the **Password** dialog box, enter the *PostgreSQL* password (this password will be your master password when you first log in) and click the **Next** button.



Please provide a password for the database superuser (postgres).

Password ••••••••

Retype password ••••••••

1.4. In the "Port" dialog box, leave the default value (5432), click **Next** and complete the installation.

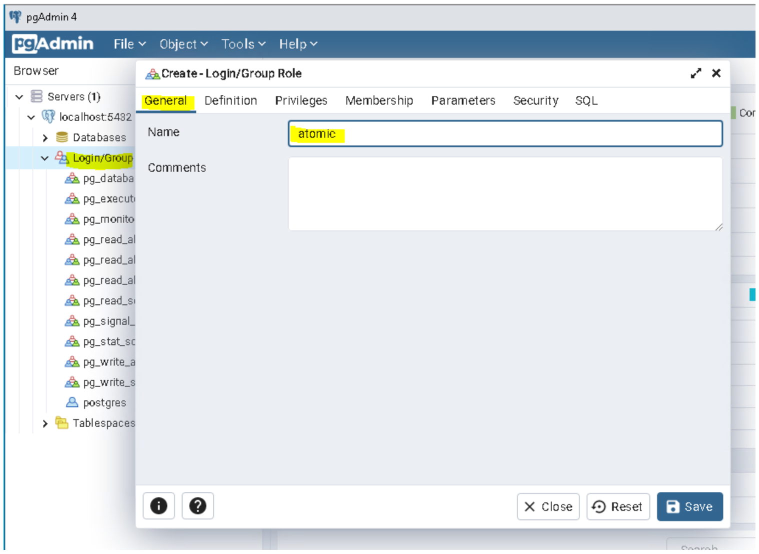
2. Create a database user.

2.1. Run the pgAdmin utility (installed from the Postgresql installation package).

2.2. Connect to the localhost server via pgAdmin (when you first log in, enter the master password specified in paragraph 1.3).

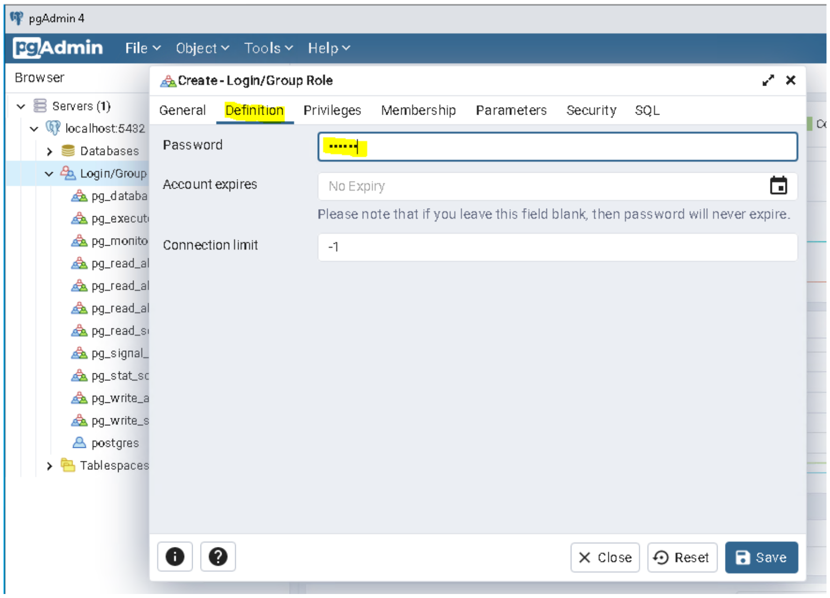
2.3. Create a user (right-click the **Login/Group** tab and select **Create Login/Group Role**):

2.4. On the **General** tab, enter the username (for example: atomic)



Name atomic

2.5. On the **Definition** tab, enter the password (**Connection limit** is equal to -1, **Account expires** is left empty (means no expiration)).



Password ••••••

Account expires No Expiry

Please note that if you leave this field blank, then password will never expire.

Connection limit -1

2.6. On the **Privileges** tab, enable the following switches: **Can login** and **Create databases** and click the button **Save.**

3.1.3. Generating a self-signed SSL certificate

In order to ensure the secure and confidential communication between NM A&C AS 2.0 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.

There is a possibility to specify a user certificate. 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 NM A&C AS 2.0. through a browser, they 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, you need to:

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

1.1. Create a self-signed certificate (.crt) and a key (.key):

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

Where the following parameters are used:

NDAYS - 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).

1.2. 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 pfx format (example: D:\mycert.pfx).

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

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

3.1.4. Installation «Atomic Keeper» v.2.0.

Installation of the application "Atomic Keeper" v.2.0. divides into two parts:

a. platform installation;

b. configuration setting;

and can be done in two ways:

1) the default installation (using UI) provides a user-friendly interface for easy navigation through the installation process;

2) automated installation (via command line).

1. Default installation (using UI):

Platform installation

The platform is an integral part of the "Atomic Keeper" v.2.0 installation and is used to install and configure the following parameters:

a. installing common configuration files;

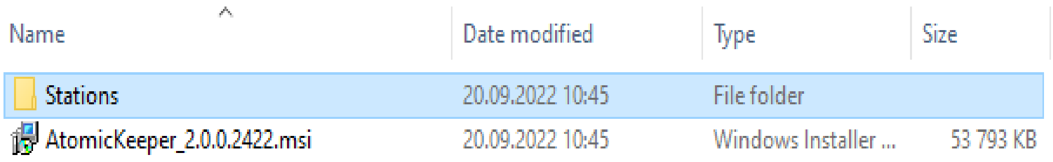
b. installation of binary files and libraries;

c. setting up and checking the connection to the database;

d. configuring and checking application access settings.

1.1.1. To install the Atomic Keeper Platform v.2.0, do the following:

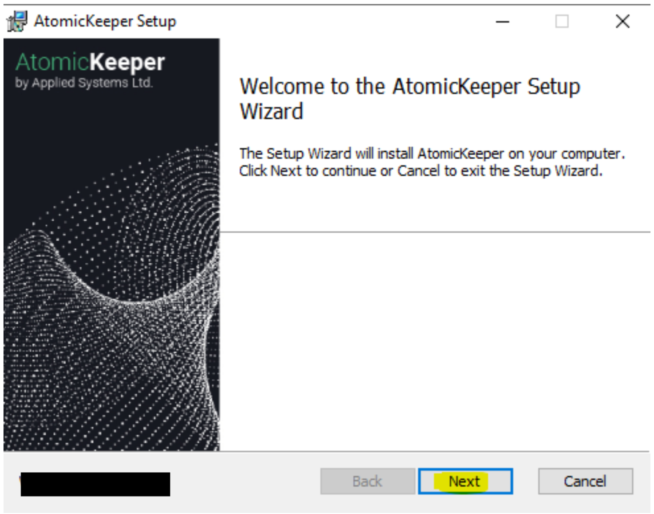
1) Unpack the distribution archive ("AtomicKeeper_X.X.X.XXXX.zip") to any folder. An example of an unpacked archive looks like this:



Name	Date modified	Type	Size
Stations	20.09.2022 10:45	File folder	
AtomicKeeper_2.0.0.2422.msi	20.09.2022 10:45	Windows Installer ...	53 793 KB

2) Run the setup file with *.msi extension (example: AtomicKeeper_2.0.0.2422.msi) by double clicking.

3) In the dialog box, click **Next**.



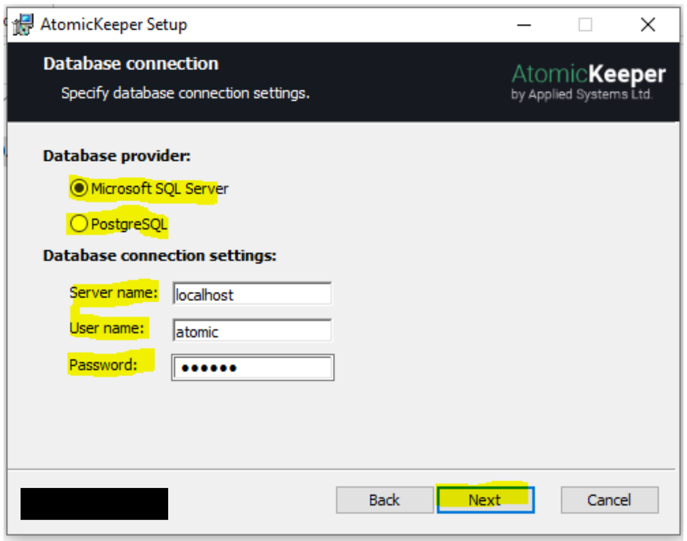
AtomicKeeper Setup

Welcome to the AtomicKeeper Setup Wizard

The Setup Wizard will install AtomicKeeper on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

[redacted]

4) In the **Database connection** dialog, enter the settings for connecting to the corresponding database



AtomicKeeper Setup

Database connection

Specify database connection settings.

Database provider:

● Microsoft SQL Server

○ PostgreSQL

Database connection settings:

Server name: localhost

User name: atomic

Password: ••••••

[redacted]

Database provider – database provider depending on the one selected in clause 4.1.

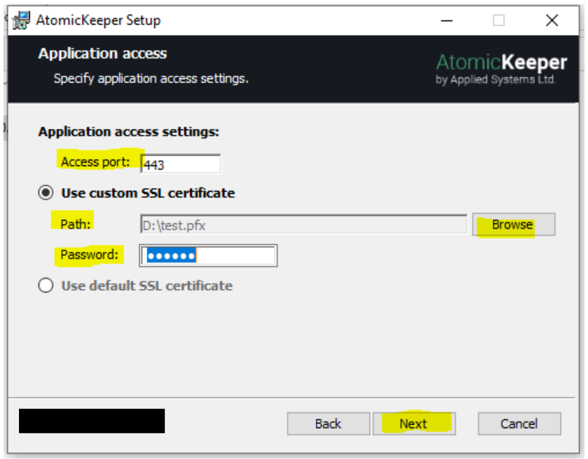
Server name – the name of the server where the database is installed ((local) if the database is on the same machine).

User name - username to connect to the database

Password - user password to connect to the database.

5) In the Application access dialog box, enter the port for accessing the web application and activate one of the following options: Use custom SSL certificate or Use default certificate and click the Next button. 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. Using the Use default

SSL certificate option means use the default SSL certificate to use the built-in self-signed certificate.



AtomicKeeper Setup

Application access

Specify application access settings.

Application access settings:

Access port: 443

● **Use custom SSL certificate**

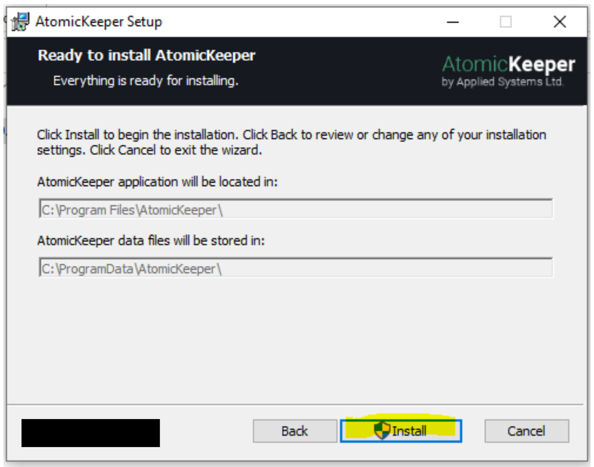
Path: D:\test.pfx

Password: ••••••

○ Use default SSL certificate

[redacted]

6) In the **Ready to install** dialog, click **Install**.



AtomicKeeper Setup

Ready to install AtomicKeeper

Everything is ready for installing.

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

AtomicKeeper application will be located in:

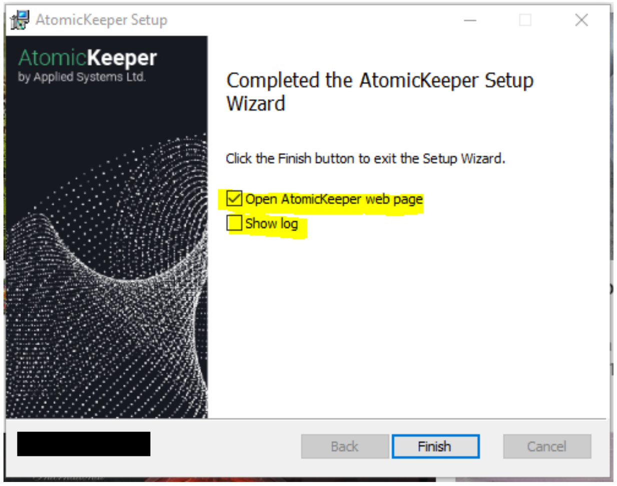
C:\Program Files\AtomicKeeper\

AtomicKeeper data files will be stored in:

C:\ProgramData\AtomicKeeper\

[redacted]

7) Wait for the installation process to complete and in the **Final** dialog box, optionally selecting the **Show log** and **Open AtomicKeeper** web page options, checking the appropriate checkbox, and clicking **Finish**:



AtomicKeeper Setup

Completed the AtomicKeeper Setup Wizard

Click the Finish button to exit the Setup Wizard.

☑ Open AtomicKeeper web page

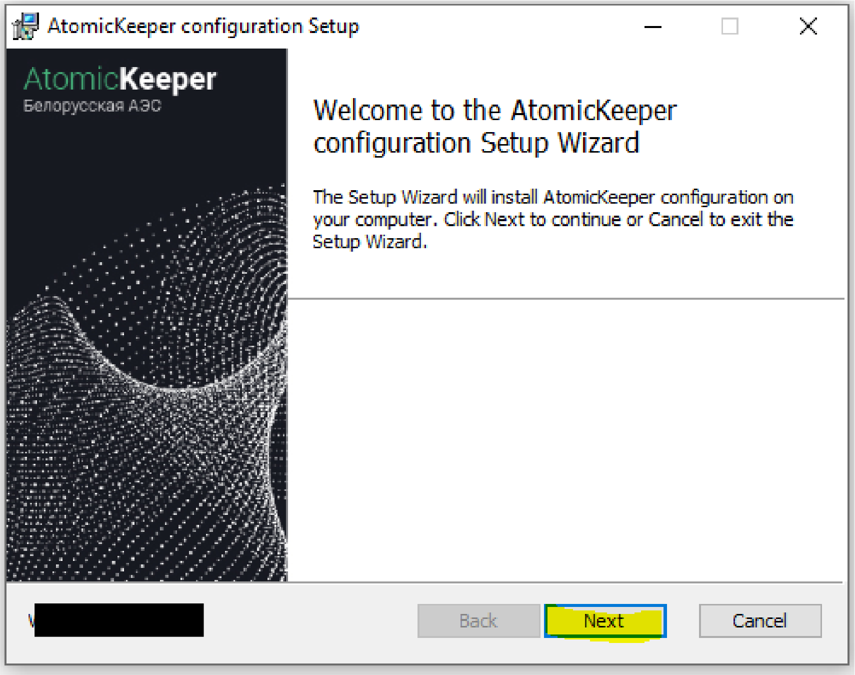
☐ Show log

[redacted]

1) Installing Atomic Keeper v.2.0 configuration Make sure that the Platform installation is completed successfully.

2) Go to the Stations folder in the unpacked distribution folder and run the installation configuration file (for example: AtomicKeeper_Akkuyu_x.x.x.x.msi).

3) In the dialog box, click Next.

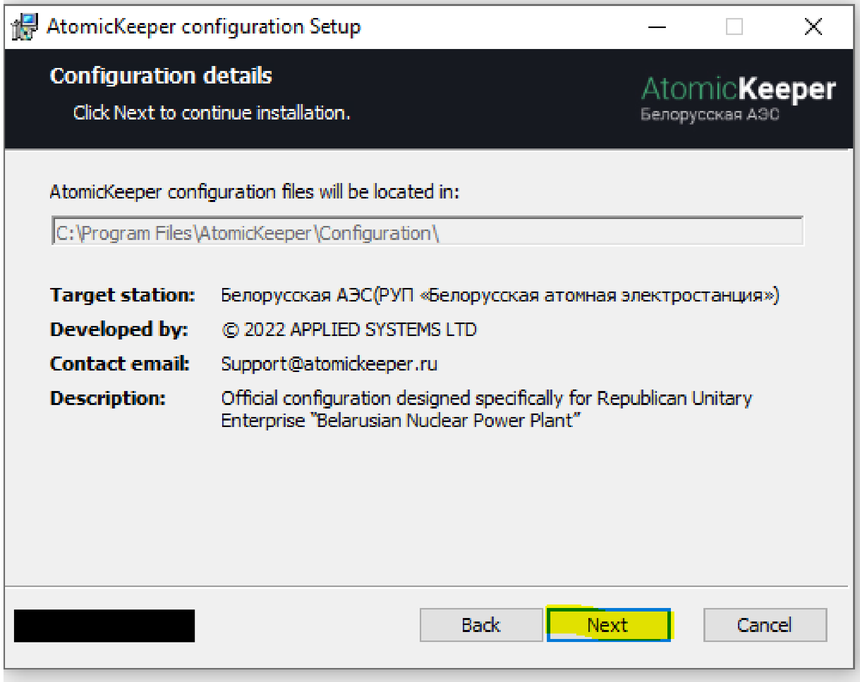


Welcome to the AtomicKeeper configuration Setup Wizard

The Setup Wizard will install AtomicKeeper configuration on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

[redacted]

4) 4) In the **Configuration details** dialog that appears, click **Next**



Configuration details

Click Next to continue installation.

AtomicKeeper configuration files will be located in:

C:\Program Files\AtomicKeeper\Configuration\

Target station: Белорусская АЭС(РУП «Белорусская атомная электростанция»)

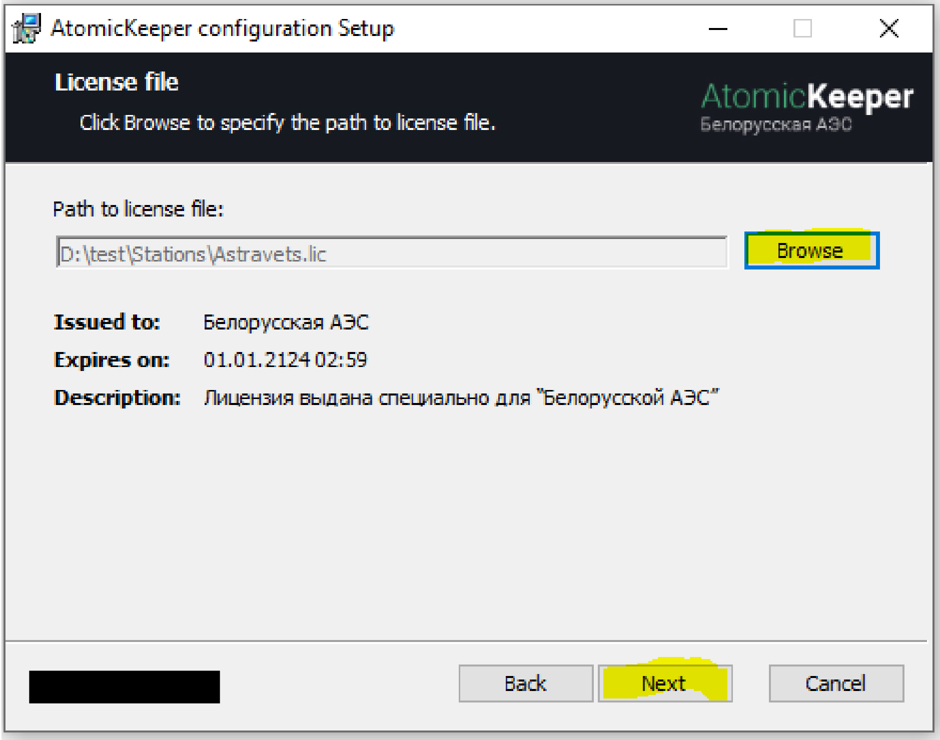
Developed by: © 2022 APPLIED SYSTEMS LTD

Contact email: Support@atomickeeper.ru

Description: Official configuration designed specifically for Republican Unitary Enterprise "Belarusian Nuclear Power Plant"

[redacted]

5) In the **License file** dialog box, click **Browse** and specify the path to the license file (for example: Akkuyu.lic) located in the Stations distribution folder, then click **Next**. If the license file is invalid, the **Next** button will be disabled.



License file

Click Browse to specify the path to license file.

Path to license file:

D:\test\Stations\Astravets.lic

Issued to: Белорусская АЭС

Expires on: 01.01.2124 02:59

Description: Лицензия выдана специально для "Белорусской АЭС"

[redacted]

6) In the **Ready to install** dialog, click the **Install** button.

7) Wait until the end of the installation process and in the **Final** dialog box, optionally selecting the **Show log** option (Show the installation log) by checking the appropriate box, click the button **Finish**:

2. Automated installation (via command line).

To perform an automated installation, you must:

2.1. Platform installation:

2.1.1. Run *Command Prompt* as Administrator.

2.1.2. Run 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 msi file AtomicKeeper_X.X.X.X..msi.

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

Argument list:

1) **USE_DEFAULT_CERT** (default: False) - set this value to True to install msi with default SSL certificate.

2) **CERTIFICATE_PATH** (default: empty) — a path to a custom SSL certificate in pfx format.

3) **CERTIFICATE_PASSWORD** (default: empty) — password for the user's SSL certificate.

4) **ACCESS_PORT** (default: 443) – a port for accessing the web application via a browser.

5) .**DB_PROVIDER** (default: MSSQL. Possible values: MSSQL or POSTGRESQL) - database provider.

6) **DB_SERVER** (default: localhost) - SQL server name.

7) **DB_USER** (default: atomic) - username for connecting the "Atomic Keeper" application to the database.

8) **DB_PASSWORD** (default: atomic) is the user password used by Atomic Keeper to connect to the SQL database.

2.2. Setting up the configuration NM A&C AS 2.0:

2.2.1. Run the *Command Prompt* as Administrator.

2.2.2. Run 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 msi file (example: AtomicKeeper_Akkuyu_
x.x.x.x.msi).

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

Argument list:

1) **LICENSE_PATH** (default: empty) – path to the license file.

3.2. Preparation for and installation of "Atomic Keeper" v.2.0 for Linux Astra Smolensk 1.6

3.2.1Configuring PostgreSQL

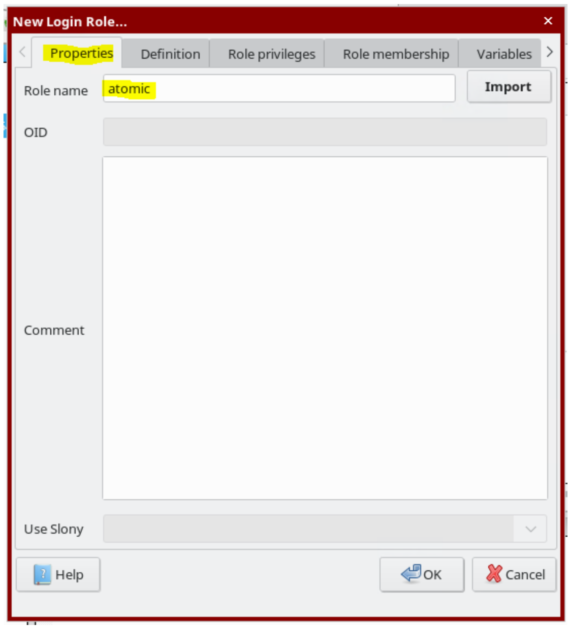
1. Set up PostgreSQL.

2. Create a database user:

2.1. Open the *pgAdmin* utility.

2.2. Expand the **Servers** tab, then expand the **localhost** tab. Find the "Login Roles" section, right-click on it and select "New Role...".

2.3. In the window that opens, on the "Properties" tab, enter the username in the "Role Name" field, for example *atomic*.



New Login Role...

Properties | Definition | Role privileges | Role membership | Variables

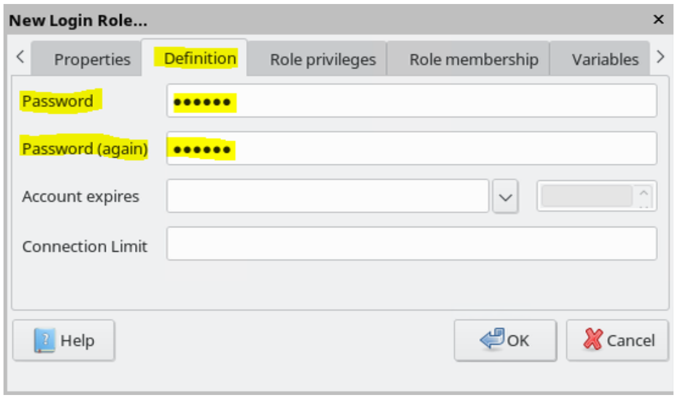
Role name: atomic

OID:

Comment:

Use Slony:

2.4. On the "Definition" tab, enter the password for the user in the "Password" field and confirm it in the " Password (again)" field.



New Login Role...

Properties | Definition | Role privileges | Role membership | Variables

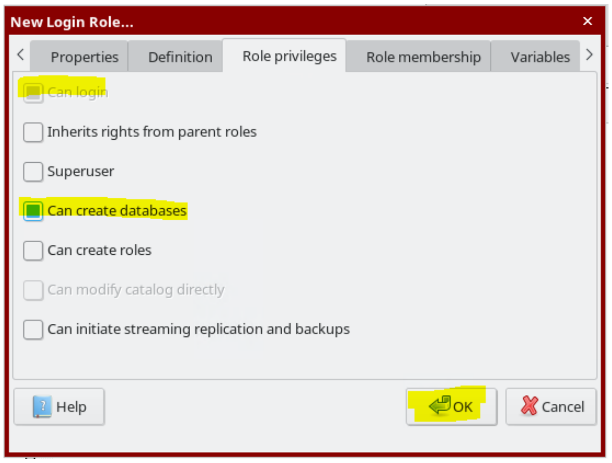
Password: ••••••

Password (again): ••••••

Account expires:

Connection Limit:

2.5. On the "Role Privileges" tab, select "Can Login" (if not selected) and "Can create databases". Then click **OK**:



New Login Role...

Properties | Definition | Role privileges | Role membership | Variables

☑ Can login

□ Inherits rights from parent roles

□ Superuser

☑ Can create databases

□ Can create roles

□ Can modify catalog directly

□ Can initiate streaming replication and backups

3.2.2 «Atomic Keeper» v.2.0 installation

Installation "Atomic Keeper" v.2.0 consists of three parts:

1. Platform installation:

1.1. Create a folder for installation under *Linux Astra Smolensk 1.6*. (for example: AtomicKeeper). This folder will be named **InstallDir**

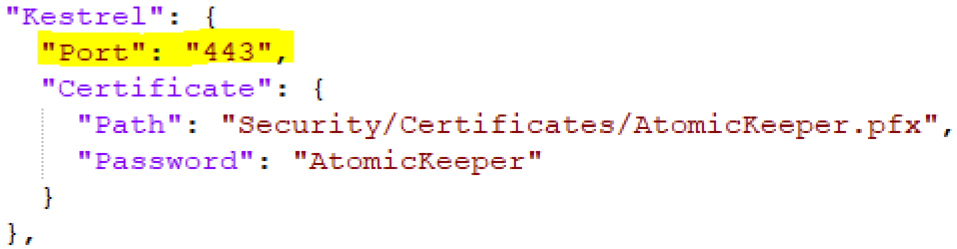
1.2.Copy all files from the folder **Setup.Linux/Platform** into **InstallDir**.

1.3.Configure access settings for the web application:

Note: The steps in the list below are optional and you can skip them if you want to use the default settings (Default access port 443):

1.3.1. Open file **appsettings.json** in **InstallDir.**

1.3.2. Find the "Port" section and replace the default value (443) with whatever port number you want to be used for *NM A&C AS 2.0.*



```
"Kestrel": {
  "Port": "443",
  "Certificate": {
    "Path": "Security/Certificates/AtomicKeeper.pfx",
    "Password": "AtomicKeeper"
  }
},
```

Note: If the port is set to 443, port 80 will also be available for *NM A&C AS 2.0* to enable automatic redirection from HTTP to HTTPS.

1.3.3. Save changes in the file *appsettings.json*.

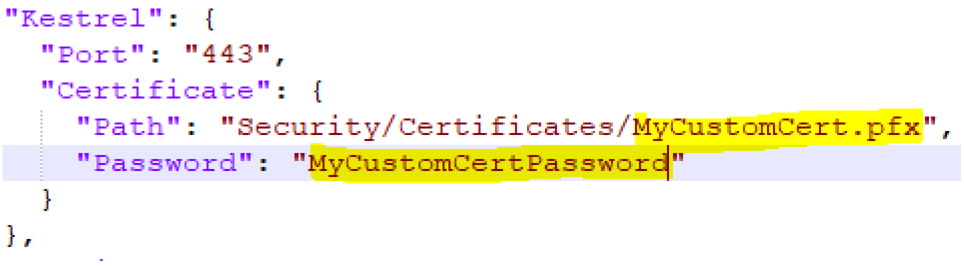
1.4.Installing a custom SSL certificate:

Note: By default, a self-signed certificate is already built into the system.

1.4.1. Copy your own certificate in PFX format into the folder **InstallDir/Security/Certificates**.

2) Open file **appsettings.json** in **InstallDir**.

3) Find section *Certificate*, set the name of the user certificate in the *Path* subsection, and the password for the certificate in the *Password* subsection:



```
"Kestrel": {
  "Port": "443",
  "Certificate": {
    "Path": "Security/Certificates/MyCustomCert.pfx",
    "Password": "MyCustomCertPassword"
  }
},
```

1.5. Configure database connection settings:

Note: The user was created in PostgreSql according to the instructions described in paragraph 3.2.1.

1.5.1. Open *appsettings.json* file in *InstallDir*.

1.5.2. In all subsections of the *ConnectionStrings* section, replace the default user ID and password with the corresponding username and password of the user that was created in PostgreSql.

2. Setting the configuration

2.1. Copy content from the folder **Setup.Linux/Configurations/Target_Station** into the folder **InstallDir/Configuration**.

Target_Station — the name of the station for which you want to set the configuration. (Example: to set the configuration **Akkuyu**, you need to copy the content of **Setup.Linux/Configurations/Akkuyu** into **InstallDir/Configuration)**.

2.2. Install the license:

2.2.1. Copy the license file from **Setup.Linux/Licenses/Target_Station.lic** to the folder **InstallDir/Configuration**.

Target_Station — the name of the station for which you want to install the license. (Example: to install a license **Akkuyu**, you need to copy the content of **Setup.Linux/Configurations/ Akkuyu.lic** to **InstallDir/Configuration)**.

3. Launching Atomic Keeperv.2.0

3.1. Grant the execute permissions to the executable file **AtomicKeeper.Bootstrapper**:

3.1.1. Open the command prompt and go to **InstallDir**.

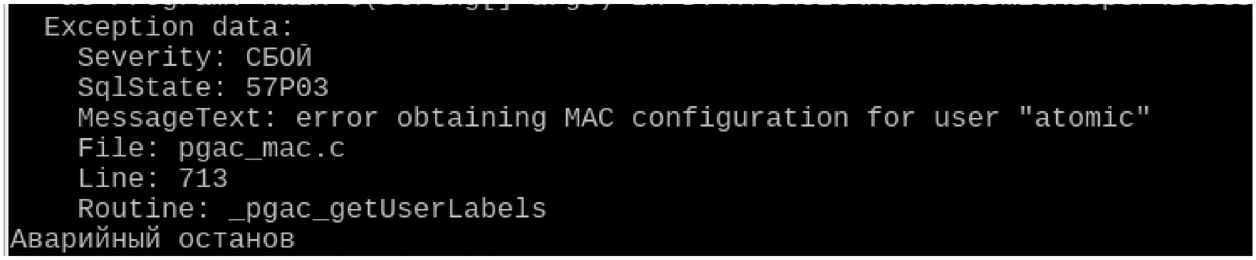
3.1.2. Execute the command: *sudo chmod +x ./AtomicKeeper.Bootstrapper*

3.2.Run the executable **AtomicKeeper.Bootstrapper:**

3.2.1. Open the command prompt and go to **InstallDir.**

2. Run the command *sudo ./AtomicKeeper.Bootstrapper*

Note: the first time you run it, you may receive an error message "failed to get MAC configuration for user xxx".



```
  Exception data:
    Severity: СБОЙ
    SqlState: 57P03
    MessageText: error obtaining MAC configuration for user "atomic"
    File: pgac_mac.c
    Line: 713
    Routine: _pgac_getUserLabels
Аварийный останов
```

This message means that the *Postgresql* installed missed some settings. To correct this error, it is necessary, in the file */etc/parsec/mswitch.conf*, parameter *zero_if_notfound* set into *yes*.

3.3. Checking the functionality of the installed software

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

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

4. DESCRIPTION OF ADMINISTRATOR OPERATIONS

4.1. Login to the system administration page

To login to the *NM A&C AS 2.0* administration page, it is necessary:

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 the login to log into the system with the "Administrator" role.
3. In the **Password** field, enter a password.
4. Click the **Login** button. You will be taken to the System Administration Page.

4.2. Create a rights group for users

Rights groups are used to provide certain users with the Expert role with the necessary rights to perform certain NM SQ accounting and control operations in NM A&C AS 2.0.

1. Log in to NM A&C AS 2.0 with the "Administrator" role.
2. Go to the "Permission groups" tab.
3. Click the "Add" button and enter the information about the name of the created rights group.
4. Select from the list of areas, the required area of which will be owned by users in the created group.
5. In the right part of the page, select the necessary rights from the list for users of the created group in the selected area.
6. Click the **Save** button.

4.3. Create a user account with the "Commissioner" role

A user with the " Commissioner " role has access only to the "References" module and is enabled for editing information in it.

1. Log in to *NM A&C AS 2.0* with the "Administrator" role.

2. Go to the "List of users" tab and click the "Add" button.

3. Register a new user with the Commissioner role:

a. in the *Login* and *Temporary password* fields, specify the data for authentication of the registered user;

a) add the IP address of the user's computer;

b. other fields with personal data are optional;

c. press the **Save** button.

As a result of these actions, a user will be added to the system with the Customizer 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.

4.4. Creating a user account with the “Expert” role

1. Log in to NM A&C AS 2.0 with the "Administrator" role.
2. Go to the "List of users" tab and click the "Add" button.
3. Register a new user with the Expert role:

a. in the *Login* and *Temporary password* fields, specify the data for authentication of the registered user;

b) add the IP address of the user's computer;

b. select the full name of the user who will own the account from the list (the list of employees and their data is registered by a user with the "Setter" rights in the "Directories" module);

c. Select a rights group for a user;

d. Push the **Save** button.

As a result of these actions, a user will be added to the system with the Expert role. The initial password is passed on 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.

4.5. Account deactivation

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

1. Log in to NM A&C AS 2.0. with the "Administrator" role.
2. Go to the "List of users" tab.
3. Select the user to be deactivated in the table and press the button in the "Actions" column (deactivate).
4. Confirm deactivation by pressing the button 💾.

4.6. Changing data in a user account

To change information in a user account, follow these steps:

1. Log in to NM A&C AS 2.0 with the "Administrator" role.
2. Go to the "List of users" tab.
3. Select in the table the user whose information you want to change and in the column "Actions" press the button ✎ (change).
4. Make the necessary adjustments for the selected user and click the **Save** button.

4.7. Resetting a User Entry Password

1. Log in to NM A&C AS 2.0 with the "Administrator" role.
2. Go to the "List of users" tab.
3. Select the user in the table who needs to reset the password and click the button in the "Actions" column (reset the password).

4. In the dialog box, enter a new initial password for the user or select the password suggested by the system.

5. Push the **Save** button.

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

4.8. Viewing the log of user actions (logging)

1. Log in to NM A&C AS 2.0. with the "Administrator" role.
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.

The event log can be filtered for a specific specified period, and it is also possible to export the log data to a *.xlsx file.

4.9. Authentication Settings

1. Log in to NM A&C AS 2.0 with administrative rights.
2. Select **Settings** on the main navigation menu.
3. Set the necessary parameters for authentication.
4. Click **Save**.

4.10. Unlock an account

In order to prevent unauthorized access, the account may be automatically blocked when the authentication parameters are set in the Settings. To unlock a user account, you need to do as follows:

1. Log in to NM A&C AS 2.0. with the "Administrator" role.
2. From the main navigation menu, select the IP Addresses tab and select Blocked.
3. Remove the required IP Address from the list and go to the User List in the main menu.
4. Go to the "List of users" tab, select the user in the table who needs to activate access, press the button 👤 (activate) in the deactivated account.
5. Press the button 💾 (Save).

5. EMERGENCY ACTIONS

The system must ensure the 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.

5.1. 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.

5.2. 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.

5.3. 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.

5.4. 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
Entries are not added to the audit log due to insufficient memory	Information about user actions in the audit log	Increase memory on the server where "Atomic Keeper" v.2.0 is installed by adding additional larger hard drives or cleaning up junk files to free up the required amount of memory.	Administrator
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
Turn off hardware power	User unsaved data	Re-entering and saving information	User
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

Emergency situation	**Possible loss of information**	**Method of fixing consequences**	**Executor**
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
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