elcomplus

SmartICS Installation and Start Guide

June 2020

Revision History

Revision	Description	Date
2.0	Initial release of the document. The document is compliant with SmartICS 2.0.	June 2020

Contents

About This Document

The document describes processes of the environment preparation for the SmartICS installation, its installation and the beginning of the configuration. It is indended for Customer's system administrators.

Additional Information

The document does not contain information about SmartICS configuration and use. The corresponding information is available in the embedded help of the product.

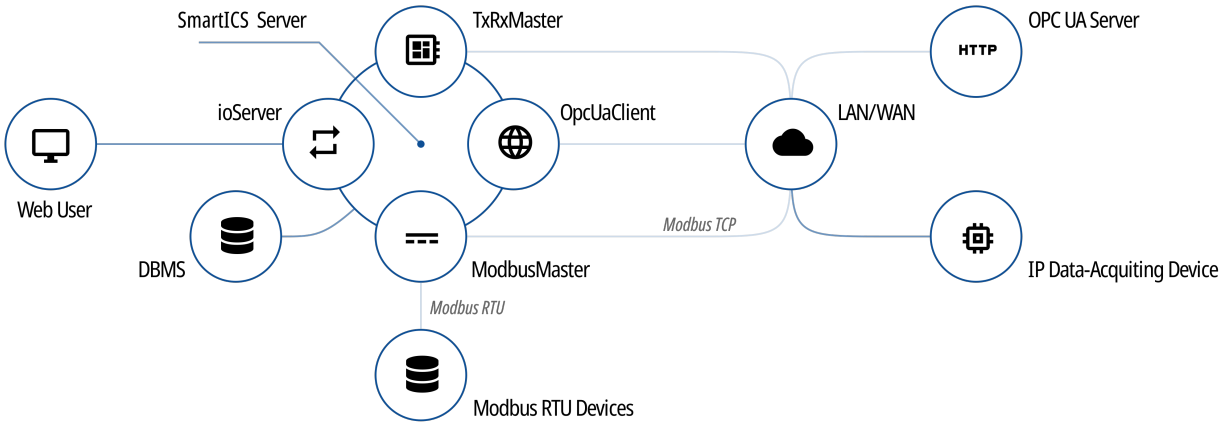
This document does not contain information that is related to the Windows computer administration. It also does not contain information related to the data-acquiring device configuration (including the AdapTel devices). The only exception is the information that is necessary for SmartICS configuration. The information can be obtained from the following sources:

Source	Description
Microsoft Docs	Microsoft documentation storage for users, developers, and IT specialists.
AdapTel. System Planner	Document that describes the process of the AdapTel device configurarion. AdapTel is a product developed and released by Elcomplus LLC.

If you require an assistance in devices and/or services configuration, or computer administration, submit a request to the SmartPTT Technical Support Center.

1 Overview

SmartICS is a client–server software for telemetry data acquisition and remote control in civil engineering.



SmartICS is a web application.

1.1 Components

The following information is related to the key SmartICS components.

SmartICS Server

SmartICS Server (software component) provides the following features:

- Data aggregation from various devices and services.
- Logging events to the database..
- Information delivery from the database to the SmartICS user.
- User commands provision to devices.

On the computer, the server is represented as a Windows service named **SmartICS**. Start of the service is required for SmartICS operation and server configuration access. The access is provided by the ControlCenter web application.

When user is authorized in ControlCenter, they are provided with access to the SmartICS internal services. The services provide the following functions:

Service	Description
ioServer	SmartICS GUI and DBMS connection to the server.
OpcUaClient	Connection to HTTP servers that implement Unified Architecture specification as recommended by OPC Foundation.
ModbusMaster	Connection to devices and data exchange with them over the Modbus TCP or Modbus RTU protocols.

Service	Description
TxRxMaster	Connection to and data exchange with the AdapTel devices.

For details, see the ControlCenter embedded help.

Database Management System

Database Management System (DBMS) provides the following functions:

- Logging events that involve SmartICS Server (includes device data and user commands).
- User settings storage (dashboards, widgets, profile settings and more).

SmartICS uses Microsoft SQL Server as DBMS. Other DMBS are not supported. For information on compatible SQL versions and editions, see Compatible Products.

1.2 Features and Capabilities

SmartICS provides the following capabilities:

- Supervisory control in communication systems based on AdapTel devices;
- Data exchange over the Modbus protocol.
- Connection to HTTP servers that implement Unified Architecture proposed by OPC Foundation.
- Flexible role model with configurable permissions and device access.
- Demonstration mode (24 hours long) with on-demand extension.

WARNING
Demonstration mode is **not** intended for real system maintenance. For this purpose, order a license.

SmartICS provides the following user features:

- Data observation.
- Visual and audible notifications when parameter values are out of normal mode limits.
- Remote control commands.
- Event logging.
- Data analysis using filtered event log and trendlines; data export to CSV.

For SmartICS administrators, the following features are available:

- User account creation and management.
- Device parameters adjustment and dashboard creation.
- Process diagrams creation.
- SmartICS backups creation and management.

1.3 System Requirements

Hardware and software that is intended to host SmartICS must comply with specific requirements. The requirements are described in the following sections.

1.3.1 Host Requirements

SmartICS has certain requirements to hardware and software. The following minimum requirements are intended for demonstration purposes and should cover a configuration with 20 devices. If you have any questions related to the SmartICS host specifications for your system, contact Elcomplus LLC representative in your region.

Minimum Hardware Requirements

Parameter	Value
Processor	Intel Core i3-6100
Memory (RAM)	4 GB
Disk	parameters: 7200 rpm (HDD)
	free space: 11 GB
Network Adapter	Ethernet, 10/100/1000 Mbps
I/O Ports	1 video output (at least for installation)
	(Optional) 1 keyboard input*
	(Optional) 1 pointing device input (mouse or trackball)**
	(Optional) 1 audio output for the audible alarm notifications.
	1 installation package delivery port (USB or DVD/R)
Monitor	display size: 15″
	screen resolution: 1368 × 768 px.

* Physical keyboard can be replaced with the Windows virtual (screen) keyboard.

** Pointing devices can be replaced with touchscreen.

Minimum Operating System Requirements

Parameter	Value
OS Family	Windows
OS Architecture	64-bit operating system only
OS Versions and Editions	Windows 10 Pro (version 1809)
	Windows 10 Enterprise 2016 LTSC

If you have any questions about SmartICS compatibility with another operating systems, submit a request to the SmartPTT Technical Support Center.

1.3.2 Cohabit Installation

SmartICS can be installed on the same host (computer) with the database management system (DBMS) software. In this case, hardware and software specifications must be reviewed due to the increased load. For details, contact Elcomplus LLC representative in your region.

1.3.3 Compatible Products

SmartICS is compatible with the following products:

Product Type	Details
Web Browsers	Google Chrome, Mozilla Firefox
Database Management System	family: Microsoft SQL Server
	products: 2014 Express, 2008 R2 Enterprise

Other Products

SmartICS is compatible with the data-acquiring device named AdapTel that is developed and released by Elcomplus LLC. For details, see the “AdapTel” webpage (smartptt.com/products/adaptel).

1.3.4 Networking Requirements

SmartICS provides specific requirements to the local network connection.

Parameter	Value
Packet Loss	<2,5 %

Parameter	Value
Two-Way Delay	< 90 ms
Jitter	< 90 ms

For information on requirements to the IP channel used by data acquisition devices, see the corresponding device documentation.

1.4 Internationalization

SmartICS user interface is available in the following languages:

- English
- French
- German
- Italian
- Portuguese (Brazil)
- Russian
- Spanish

User interface can be changed in the user profile settings.

2 Preliminary Configuration

Before the SmartICS installation, additional environment configuration must be performed. The following sections outline the necessary configuration actions.

2.1 Addressing

SmartICS requires Internet Protocol version 4 (IPv4) support. It does not support IPv6.

SmartICS can be installed on a computer with several active IP addresses. For some purposes, it may require explicitly stating an IP address.

SmartICS partly supports domain names. Using domain names may require DNS Server support in the Customer Enterprise Network or modification of Windows system files (for example, *%WINDIR%\system32\drivers\etc\hosts*).

Since several SmartICS parameters require explicit IP addresses, those IP addresses must be fixed for SmartICS host, network devices, and more. For this, static IP addressing can be used. Alternatively, IP addresses can be associated with device MAC addresses using Dynamic Host Controller Protocol (DHCP) and the corresponding DHCP Server.

2.2 Authorization and Security

The following information provides brief description of the authentication and authorization details.

SmartICS Server Access

Access to SmartICS Server configuration is password-protected. User authentication is performed by SmartICS itself. No tools that are specific to the operating system are required.

SmartICS GUI Access

Access to SmartICS GUI requires user login and password. User authentication is performed by SmartICS itself. No tools that are specific to the operating system are required.

DBMS Access

SmartICS authorization in database is implemented in one of the following ways:

- Based on the local user and group lists (referred to as Windows NT Authentication). This method is applicable if the following conditions are met:
  - Both DBMS and SmartICS Server are installed on the same computer.
  - DBMS provides users with rights to create and manage databases.
- Based on domain user and group lists (referred to as Windows NT Authentication too). This method is applicable if the following conditions are met:
  - DBMS and SmartICS Server are installed on computers connected to the same domain of the Windows Active Directory.
  - DBMS provides users with rights to create and manage databases.

- Based on DBMS users. This method is applicable if the following conditions are met:
  - User authentication is allowed in DBMS.
  - User accounts are created in DBMS; corresponding users are able to create and manage databases.
  - User accounts are active; user accounts do not require password change at first logon; user account passwords do not expire until the system maintenance is ended.

2.3 Disk Space

SmartICS uses disk space in the following way:

- SmartICS components take ~130 MB of the disk space.
- Size of the installed DBMS depends on its version and edition.
- Database size grows as the number of logged events increases; maximum database size depends on the following conditions:
  - Some DMBS forbid unlimited database growth. For example, Microsoft SQL Server Express 2014 limits the database size to 10 GB.
  - Some DBMS allow to modify the maximum database size. For details, see the documentation of the corresponding DBMS.
- SmartICS backup size is determined by the number of users, dashboards, cards, and widgets. As a rule, its size does not exceed hundreds of kilobytes.

Important
Backup size increases dramatically if multiple image cards with background images are used.

To estimate the required disk space and prepare a suitable drive, all of these aspects must be taken into account.

If you require an assistance in disk space estimation, contact Elcomplus LLC representative in your region.

2.4 NTP Services

NTP Servers provide time synchronization between network devices using Network Time Protocol (NTP). It is recommended to configure SmartICS host in the following way:

SmartICS Host Role	NTP Server	Condition
NTP Client	DBMS Host	DBMS Host is already configured as the NTP Server.
NTP Client	OPC Server	OPC Server is already configured as the NTP Server.
NTP Server	SmartICS Server Host	No NTP Server is configured for DBMS, OPC Server.

To configure Windows computer as the NTP Server, the corresponding service (W32Time) must be configured and started. In other cases, NTP Server must be configured as instructed for the corresponding hardware/software.

To configure Windows computer as the NTP Client, address of the NTP server must be entered in the date and time settings. At some domain configurations, corresponding settings can be unavailable. To resolve the issues, contact your system administrator.

2.5 Power-Saving Mode

In Windows, power-saving mode can be configured (sleep mode, hibernation, or automatic turnoff). This mode must be turned off on SmartICS computer.

Automatic screen lock can be left unchanged as it does not affect SmartICS service operation.

2.6 Database Configuration

Database management system (DBMS) can be configured before and after the SmartICS installation. It is recommended to configure it **before** the SmartICS installation.

In the document, the minimum DBMS configuration is presented. For all the procedures, the following applications are used:

- Microsoft SQL Server Configuration Manager (included in the standard DBMS installation package).
- Microsoft SQL Server Management Studio (**not** included in the standard DBMS installation package).

All of those applications have a graphical user interface.

DBMS configuration includes the following actions:

- DBMS autostart configuration. For details, see Configuring DBMS Autostart.
- Remote access configuration. For details, see Configuring Remote DBMS Access.
- User account creation. For details, see Adding SQL Server Users.
- Memory consumption management. For details, see Limiting DBMS Memory Use.
- Network traffic allowance for remote DBMS. For details, see Firewall Configuration for DBMS.

All screen captures in the procedures are taken from Microsoft SQL Server Express in Windows 10. They can be visually different from what the Customer will see in their DBMS configuration.

2.6.1 Configuring DBMS Autostart

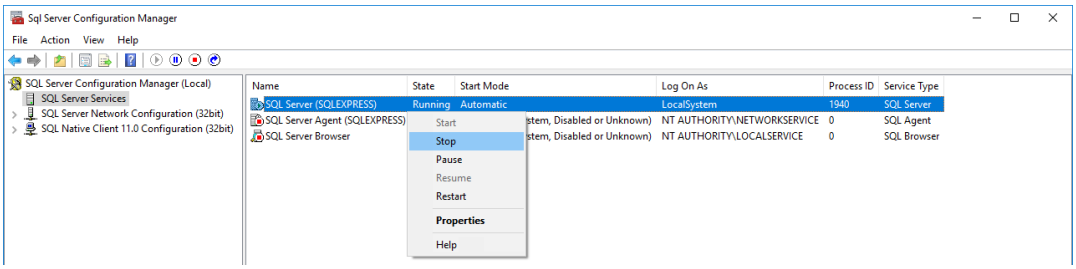
Follow the procedure to configure automatic start of the DBMS service after computer restart. This will reduce the time of system startup after DBMS host restart.

Prerequisites:

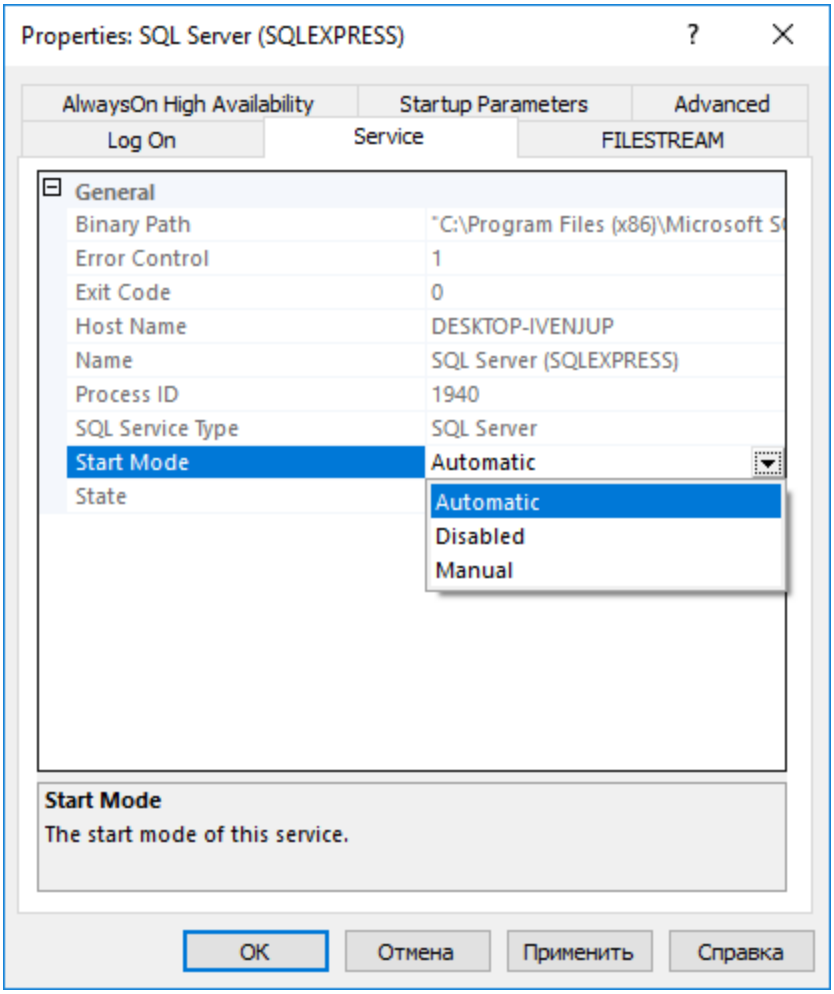
Start SQL Server Configuration Client (SSCC) on the DBMS host. For details, see SQL Server Configuration Manager in the *Microsoft Docs* portal.

Procedure:

1. In SSCC, in the left pane, expand **SQL Server Configuration Manager (Local)**, and then click **SQL Server Services**.
2. Stop DBMS services:
   a. In the right pane, right-click **SQL Server**, and then select **Stop** from the action menu.



   b. Repeat step 2a for **SQL Server Browser**.
3. Configure DBMS autostart:
   a. Right-click **SQL Server**, and then select **Properties** from the action menu.
   The **Properties: SQL Server** window appears.



   b. In the window that appears, open the **Service** tab.
   c. On the tab, in the **Start Mode** list, click the current value, and then select *Automatic*.

d. In the **Properties: SQL Server** window, click **OK** to apply changes and close the window.

4. Repeat step 3 for the **SQL Server Browser** service.
5. Start DBMS services:
   a. In the right pane, right-click **SQL Server**, and then select **Start** from the action menu.
   b. Repeat step 5a for **SQL Server Browser**.

2.6.2 Configuring Remote DBMS Access

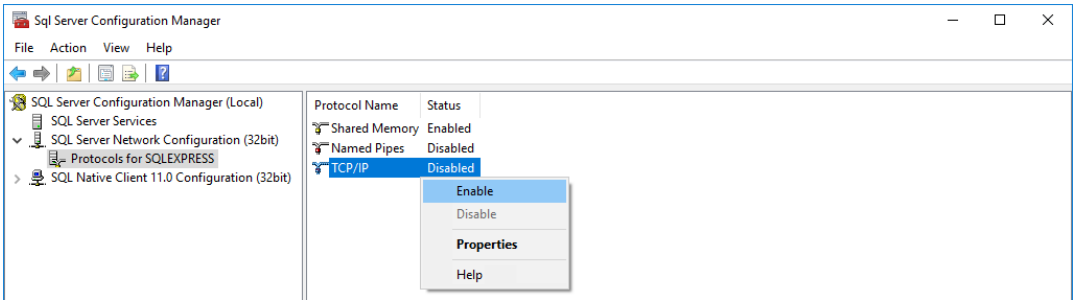
Follow the procedure to allow remote access to the DBMS.

Prerequisites:

Start SQL Server Configuration Client (SSCC) on the DBMS host. For details, see SQL Server Configuration Manager in the *Microsoft Docs* portal.

Procedure:

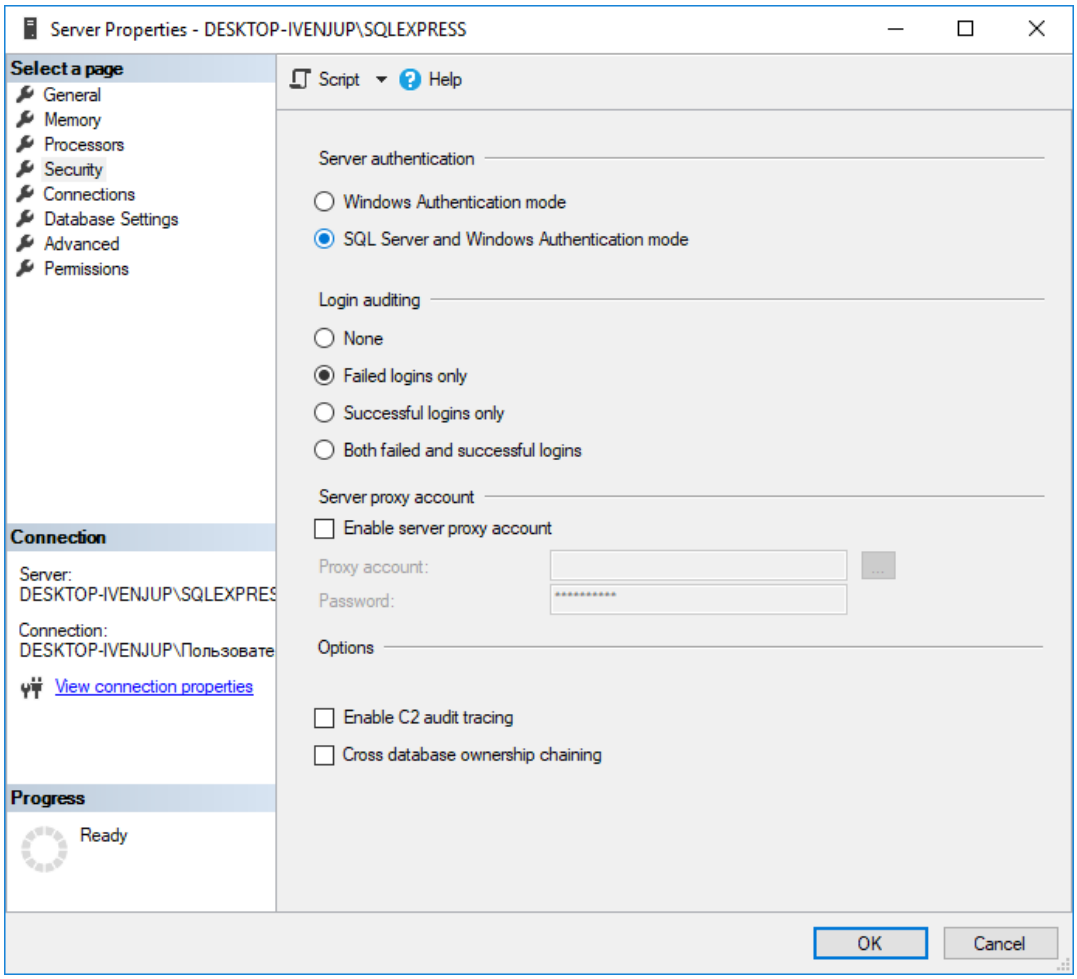
1. Allow the TCP/IP protocol for communication with DBMS:
   a. In SSCC, in the left pane, expand **SQL Server Configuration Manager (Local)** → **SQL Server Network Configuration**, and then select **Protocols for <DBMS Name>**.



   b. In the right pane, right-click **TCP/IP**, and then select **Enable** from the actions menu.
   c. In the warning dialog box, click **OK**.
   d. Restart DBMS:
      i. In the left pane, click **SQL Server Services**.
      ii. In the right pane, right-click **SQL Server**, and then select **Restart** from the actions menu.
2. Start SQL Server Management Studio (SSMS), and then connect to the required DBMS.
3. Open the **Object Explorer** panel.
4. On the panel, right-click **<Computer Name>\<DBMS Name>**, and then select **Properties** from the action menu.
   The **Server Properties** window appears.

5. In the window that appears, modify authentication settings:

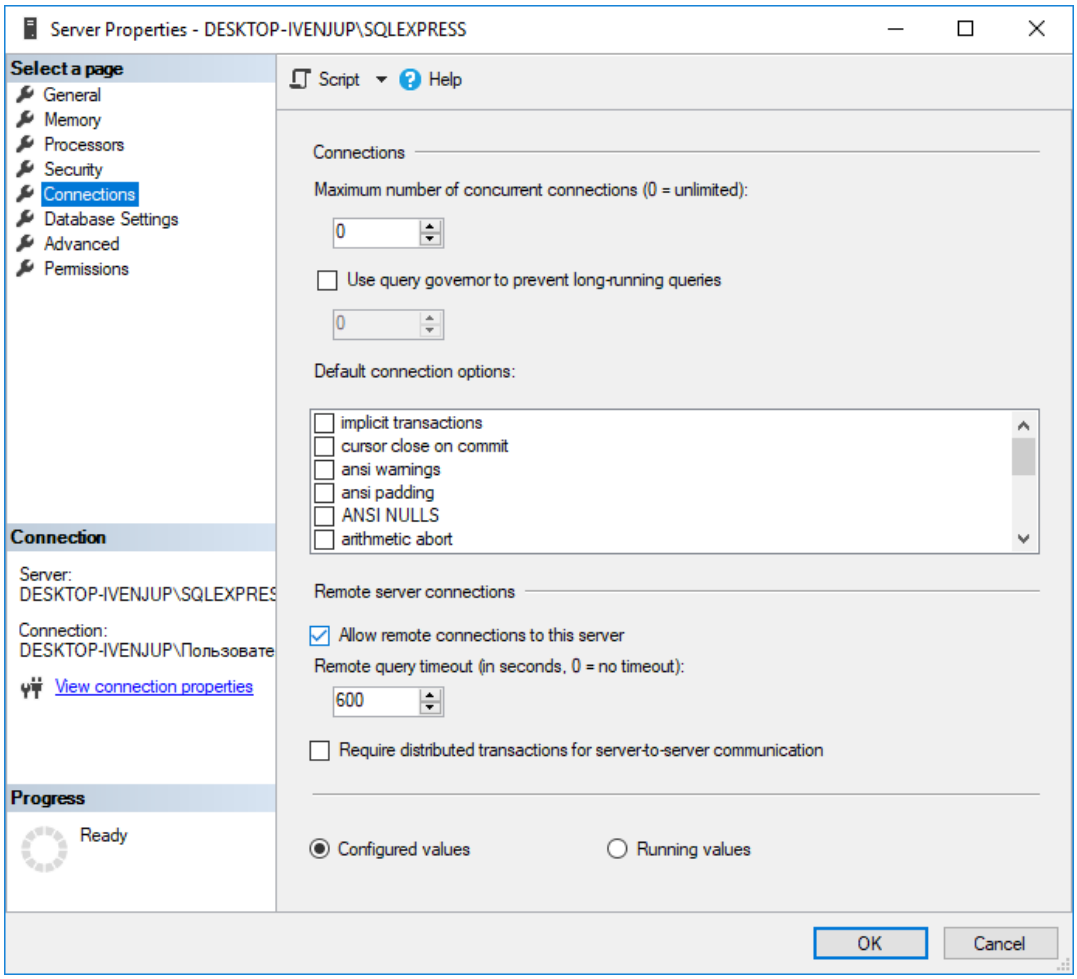
   a. In the left pane of the window, click **Security**.
   Security settings appear in the right pane.



   b. In the right pane, click **SQL Server and Windows Authentication mode**.

6. Configure the remote access parameter for the DBMS:

   a. In the left pane, click **Connections**.



   b. In the right pane, in the **Maximum number of concurrent connections** field, enter one of the following values:

To allow unlimited number of connections,	enter *0*.
To limit the maximum number of simultaneous connections,	enter the required number of connections.

   c. In the right pane, in the **Remote server connections** area, select **Allow remote connections to this server**.

   d. *(Optional)* In the **Remote query timeout** field, enter the request timeout.

   e. Click **OK** to apply changes and close the window.

7. On the **Object Explorer** panel, right-click **<Computer Name>\<DBMS Name>**, and then select **Restart** from the actions menu.

2.6.3 Adding SQL Users

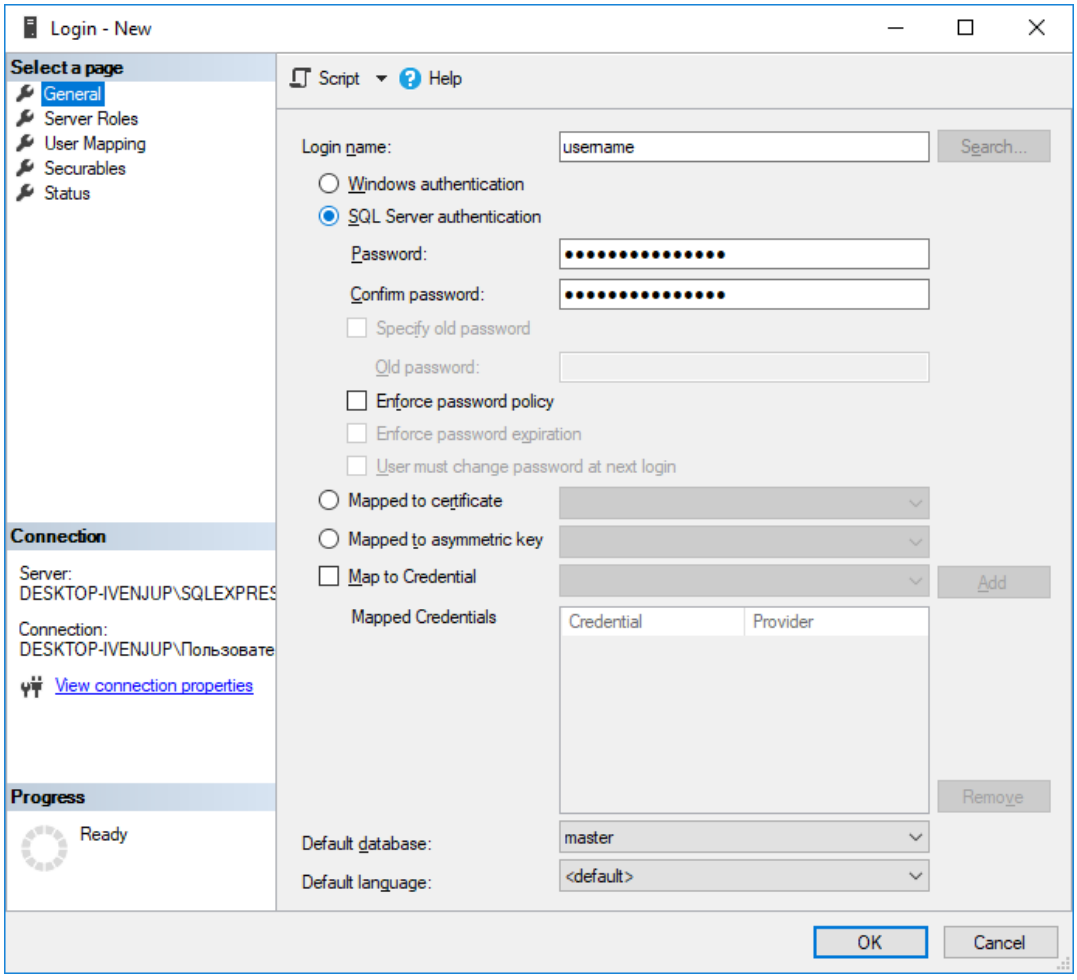
Follow the procedure to add a user account to the SQL service and use its credentials for DBMS authentication.

Prerequisites:

- Determine user login and password.
- Connect to the DBMS using SQL Server Management Studio (SSMS).

Procedure:

1. In SSMS, open the **Object Explorer** panel.
2. On the **Object Explorer** panel, expand **<Computer Name>\<DBMS Name>** → **Security**.
3. Right-click **Logins**, and then select **New Login** from the actions menu.
   The **Login - New** window appears.
4. In the window that appears, set user credentials:
   a. In the left pane, click **General**.



   b. In the right pane, in the **Login name** field, enter user login.
   c. Click **SQL Server authentication**.
   d. In the **Password** field, enter user password.

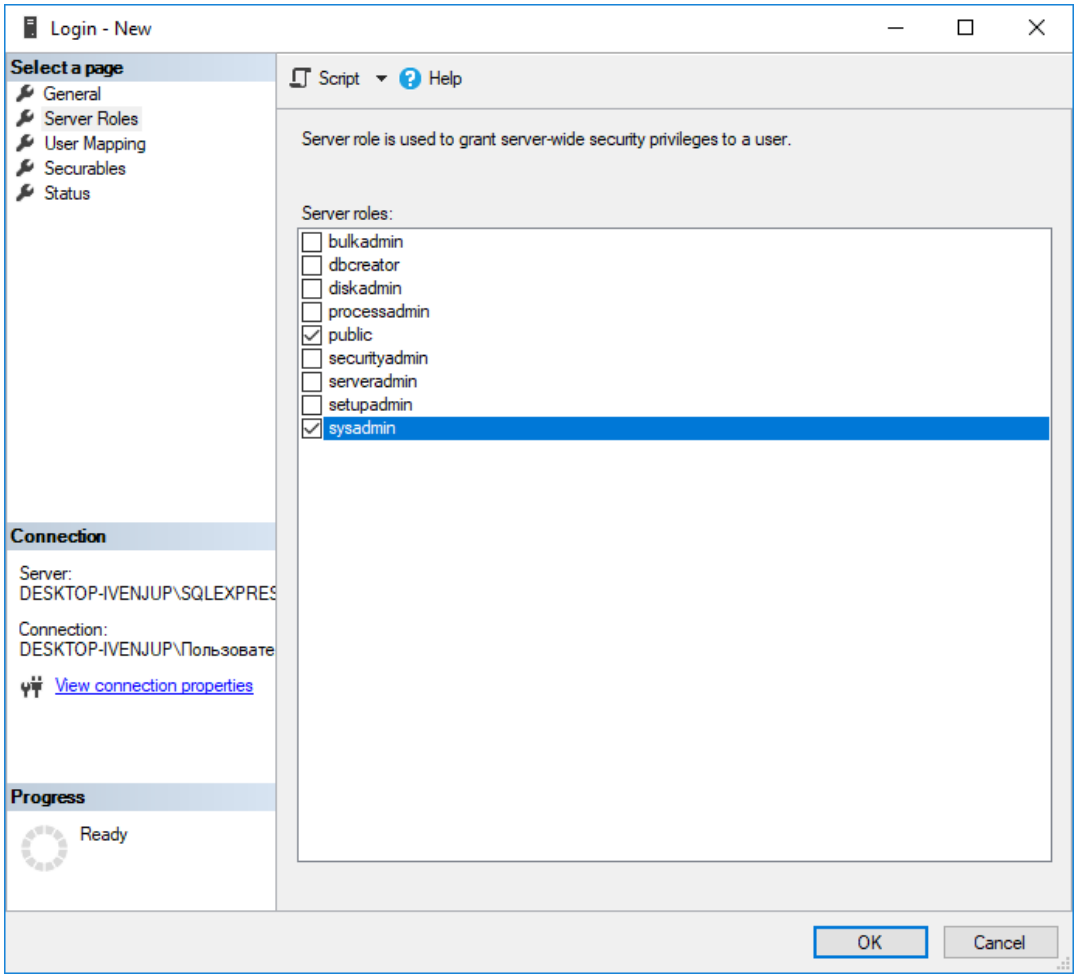
e. In the **Confirm password** field, enter user password again.

f. Modify password policy settings:

To make password policy settings compliant with the operating system settings,	perform the following actions: 1. Select **Enforce password policy**. 2. Clear **Enforce password expiration**. 3. Clear **User must change password at next login**.
To turn off password policy for the user,	clear **Enforce password policy**.

5. Configure user rights:

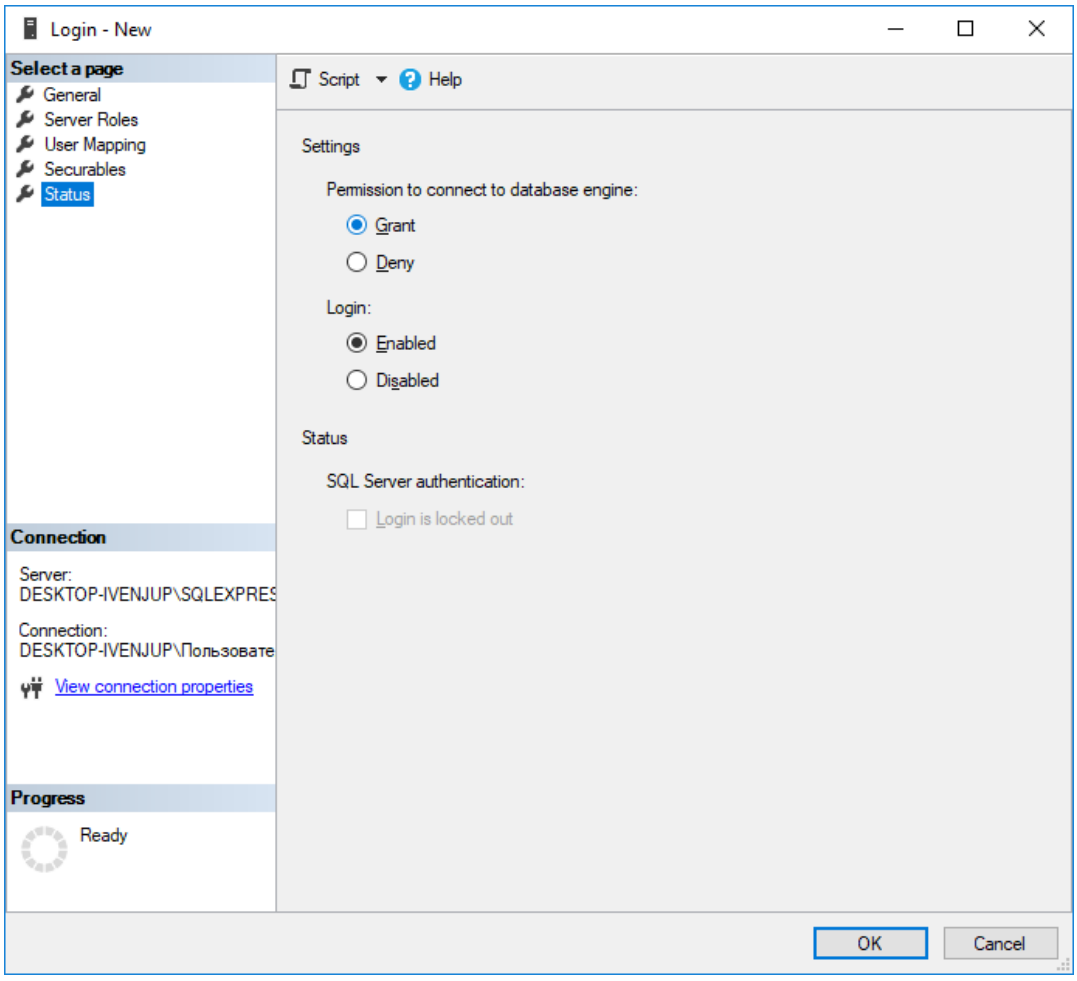
a. In the left pane, click **Server Roles**.



b. In the right pane, in the **Server Roles** area, select **sysadmin**.

6. Configure user status:

   a. In the left pane, click **Status**.



   b. In the right pane, in the **Permission to connect to database engine** area, click **Grant**.

   c. In the **Login** area, click **Enabled**.

7. In the **Login - New** window, click **OK** to create the user account and close the window.

8. On the **Object Explorer** panel, right-click **<Computer Name>\<DBMS Name>**, and then select **Restart** from the actions menu.

2.6.4 Limiting DBMS Memory

Follow the procedure to limit the size of Random-Access Memory (RAM) used by DBMS. By default, DBMS is able to consume all the available RAM. This may result in a serious decrease in computer performance, especially if DBMS is installed on the same computer as another server application.

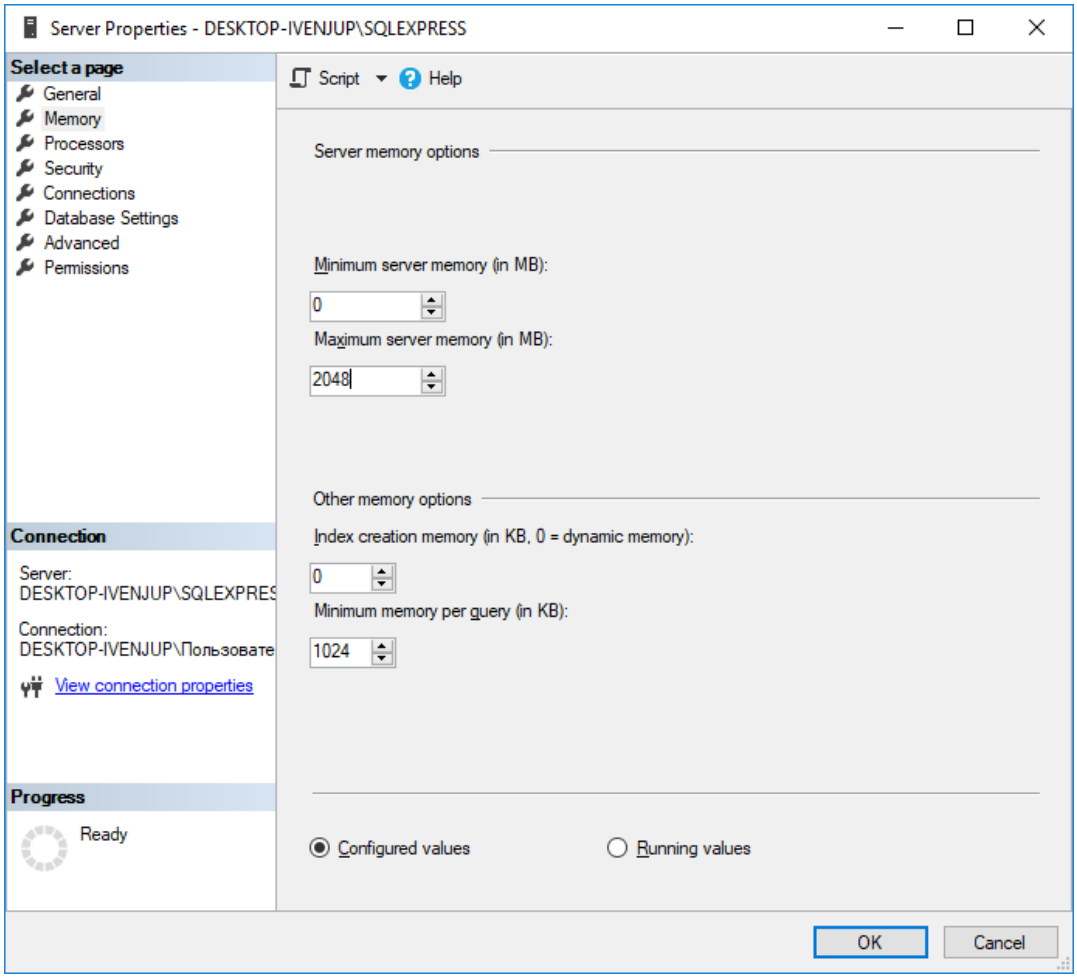
WARNING
Modify the settings only after consultation with your system administrator.

Prerequisites:

Connect to the required DBMS using SQL Server Management Studio (SSMS).

Procedure:

1. In SSMS, open the **Object Explorer** panel.
2. On the panel, right-click **<Computer Name>\<DBMS Name>**, and then select **Properties** from the actions menu.
   The **Server Properties** window appears.



3. In the window that appears, in the left pane, click **Memory**.
4. In the right pane, in the **Maximum server memory** field, enter the maximum RAM size that will be available to DBMS.
5. In the **Server Properties** area, click **OK**.
6. On the **Object Explorer** panel, right-click **<Computer Name>\<DBMS Name>**, and then select **Restart** from the actions menu.

2.6.5 Firewall Configuration for DBMS

If firewall software is turned on in the DBMS host, incoming and outgoing network traffic could be blocked. It is known that network traffic can be blocked even if Windows Firewall is turned off and no other firewall software is installed on the computer.

To allow network traffic, firewall software must be configured to allow network traffic for the following network ports:

Port Number	Transport Protocol
1433	TCP
1434	UDP

If you require assistance in firewall configuration, submit a request to SmartPTT Technical Support Center.

3 Installation and Start

SmartICS installation is performed using an application with graphical user interface. Automatic installation as well as installation using command interface is unavailable.

3.1 Installing Software

Follow the procedure to install SmartICS on a new computer.

Prerequisites:

- Authorize in Windows as administrator.
- Copy the installation file to the computer.
- *(Optional)* If DBMS is configured, obtain the following parameters:
  - Full DBMS address (includes host name and the Windows service name).
  - Credentials that are required for authorization in DBMS (if SQL authorization will be used).

NOTE
DMBS connection can be performed during SmartICS configuration. For details, see SmartICS GUI embedded help.

Procedure:

1. Start the installation file.

2. In the welcome window, select the installation language:
   a. To the right of the **Язык установки/Setup language**, click the current language.
   b. In the dialog box, select the desired language, and then click **Apply**.

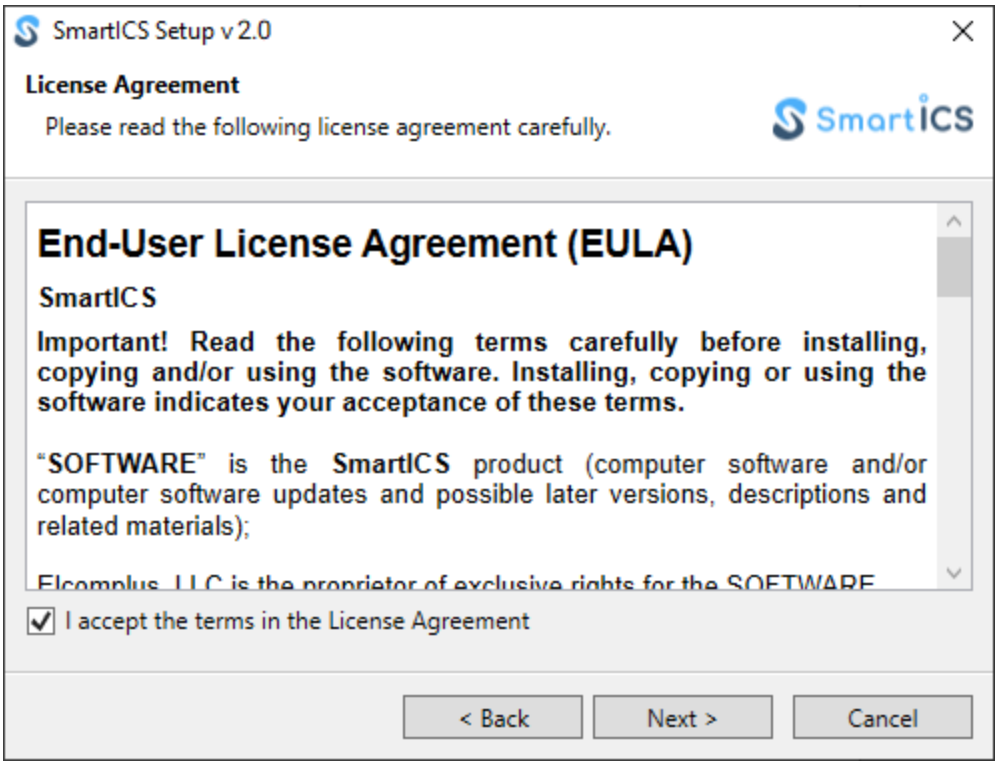
c. In the welcome window, click **Next**.

3. If .NET Framework needs to be installed, agree to install it.

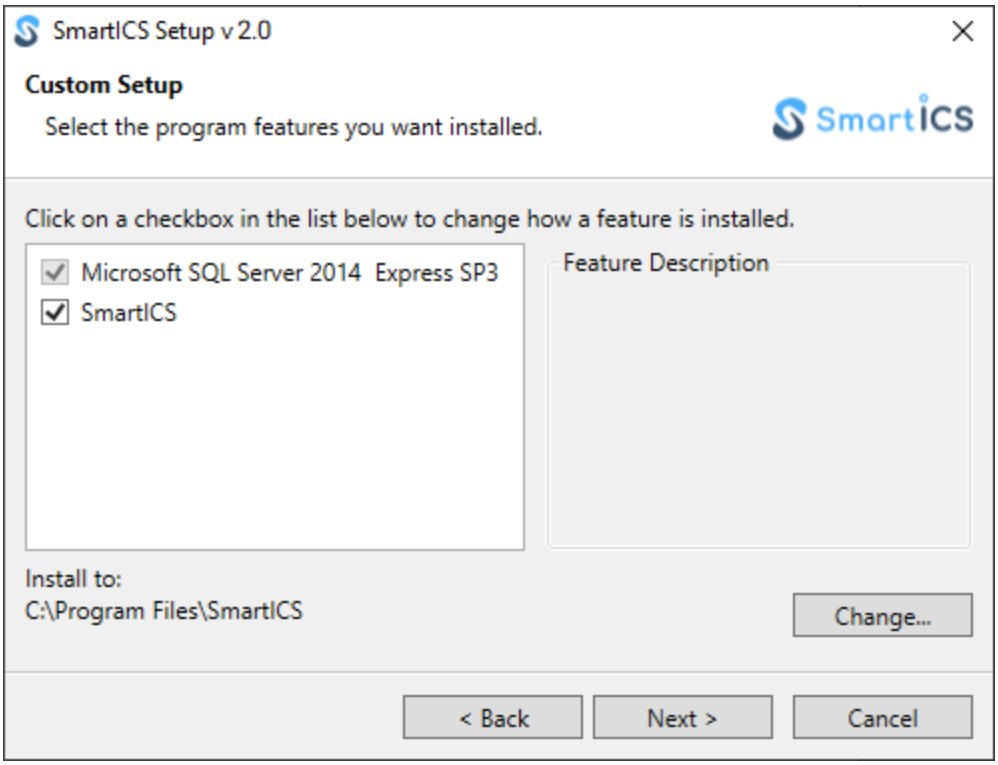
WARNING
In Windows 8.1, computer must be restarted **right after** the .NET Framework is installed. For other Windows operating systems, restart is optional.

4. After .NET Framework installation and computer restart (if required), start the installation file again.

5. Select the language again. Then click **Next**.
The **License Agreement** window appears.



6. In the windows that appears, select **I accept the terms in the License Agreement**, and then click **Next**.
The **Custom Setup** window appears.



7. In the window that appears, configure components that must be installed:

   a. Select the desired component.

NOTE
If a component is already installed, it will appear unavailable (disabled) and selected. It will not be re-installed.

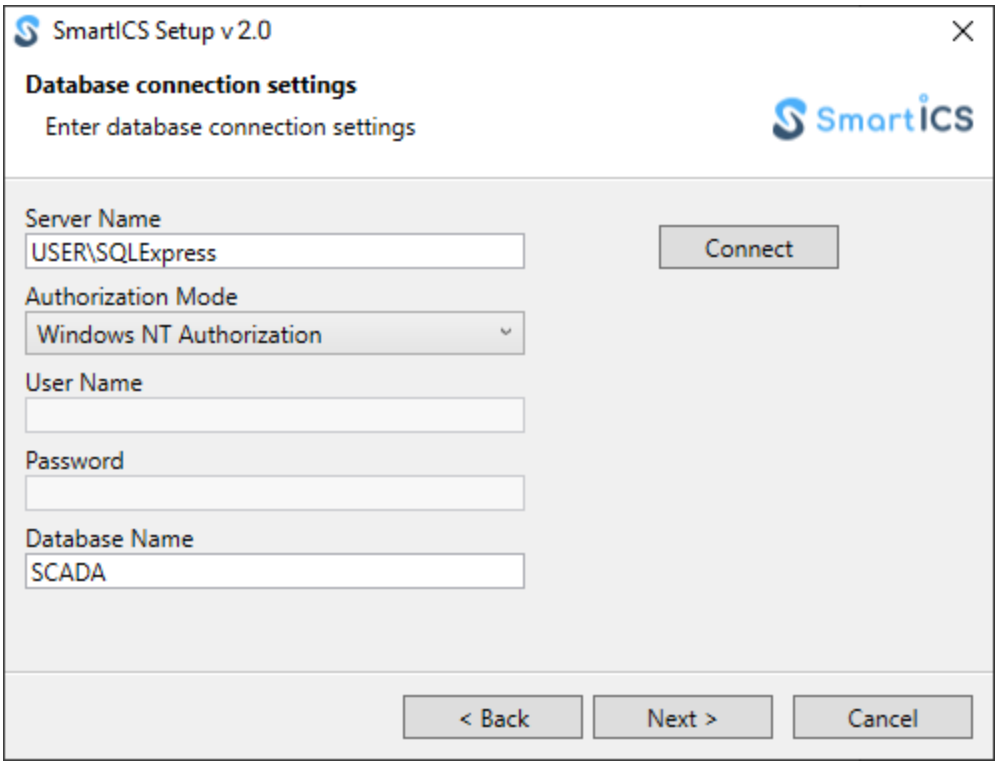
   b. *(Optional)* For each of the desired components, change the destination folder:

      i. Click **Change**.

      ii. In the dialog box, select the desired path, and then click **Open**.

Important
It is recommended to leave default paths unchanged.

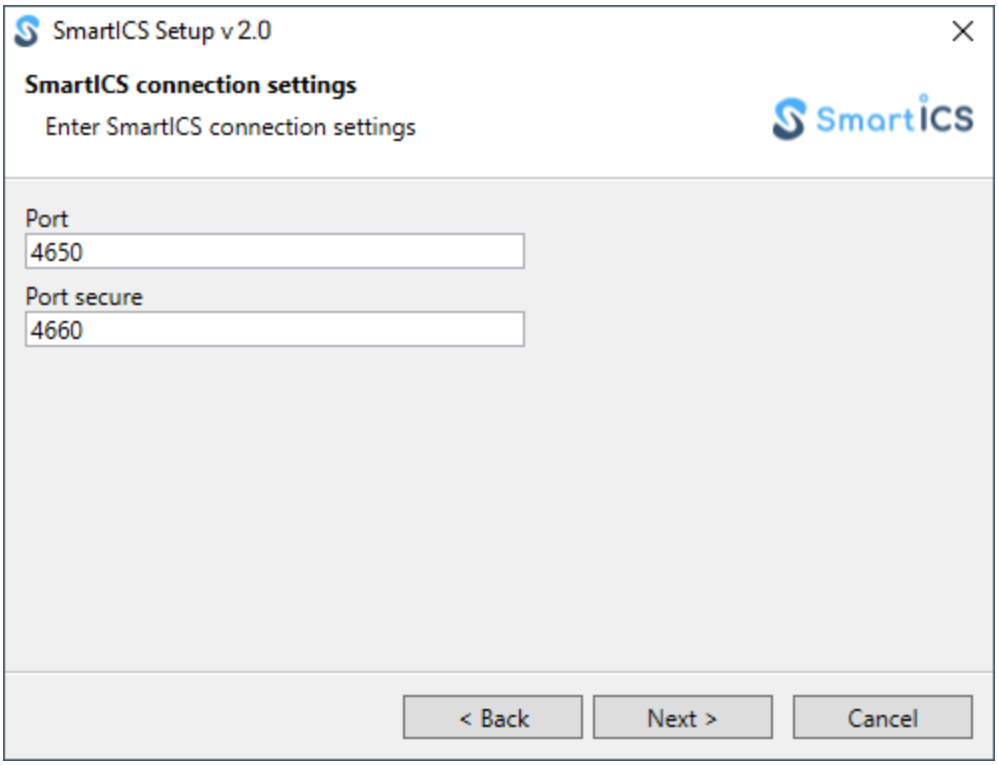
   c. In the **Custom Setup** window, click **Next**.
   The **Database Connection Settings** window appears.



8. *(Optional)* In the window that appears, configure the connection to DMBS:
   a. In the **Server Name** field, enter the full DBMS name in the following format: *<DBMS host address>\<DBMS server name>*.
   b. Configure authorization in DMBS:

To use local or domain user accounts,	from the **Authorization Mode** list, select *Windows NT Authorization*.
To use SQL user accounts,	perform the following actions: 1. From the **Authorization Mode** list, select *SQL Server Authorization*. 2. In the **User Name** field, enter the user name (login). 3. In the **Password** field, enter the password.

   c. In the **Database Name** field, enter the name of the desired (new or existing) database.
   d. Click **Connect** to authorize in DBMS.
9. Click **Next**.
   The **Connection Settings** window appears.



10. In the window that appears, configure the connection between SmartICS GUI and SmartICS Server:
    a. In the **Address** field, enter the IP address of the computer where SmartICS is installed.
    b. In the **Port** field, enter the port number that will be used for connection.
11. Click **Next**.
    The **Ready to Install** window appears.
12. In the window that appears, view the summary. If it is correct, click **Install**.
    After the installation, the **Setup Completed** window appears.
13. In the window that appears, click **Finish** to close the installation program.

Postrequisites:

- Restart the computer to guarantee that SmartICS will operate properly on the computer.
- If DBMS was not configured by the installation start, configure DBMS.

3.1.1 Antivirus Configuration

If computer hosts antivirus software, SmartICS executable files may be blocked. To avoid this, the following files must be added to the antivirus ignore list:

- \<installation directory>\Server\App\ioServer\ioServer.exe
- \<installation directory>\Server\App\ControlCenterWin\ControlCenterWin.exe
- \<installation directory>\Server\App\OpcUaClient\OpcUaClient.exe
- \<installation directory>\Server\App\ModbusMaster\ModbusMaster.exe
- \<installation directory>\Server\App\TxRxMaster\TxRxMaster.exe

To determine DBMS files that must be allowed in the antivirus software, submit a request to the SmartICS Technical Support Center.

3.2 Authorizing in SmartICS Server

Follow the procedure to access SmartICS Server settings.

Prerequisites:

Install Chrome or Chromium web browser.

Procedure:

1. Start the web browser.
2. In the address field, enter `<http://SmartICS IP address>:8079`
   Authorization page opens.
3. In the web page that appears, in the **Password** field, enter the password. For the first logon, enter *elcomplus*

Postrequisites:

Change the default password. For details, see ControlCenter embedded help.

3.3 Creating First User

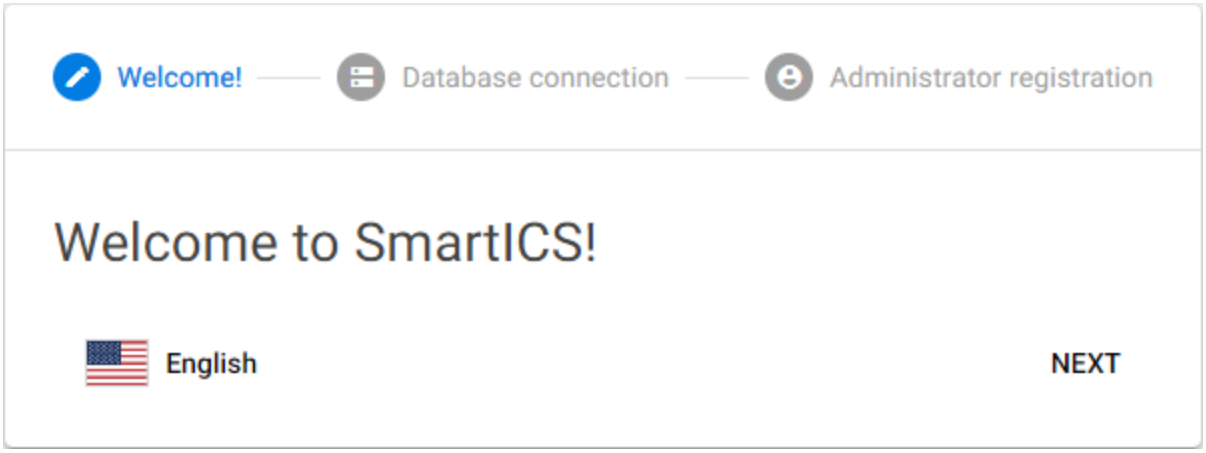
Follow the procedure to create a first user.

Prerequisites:

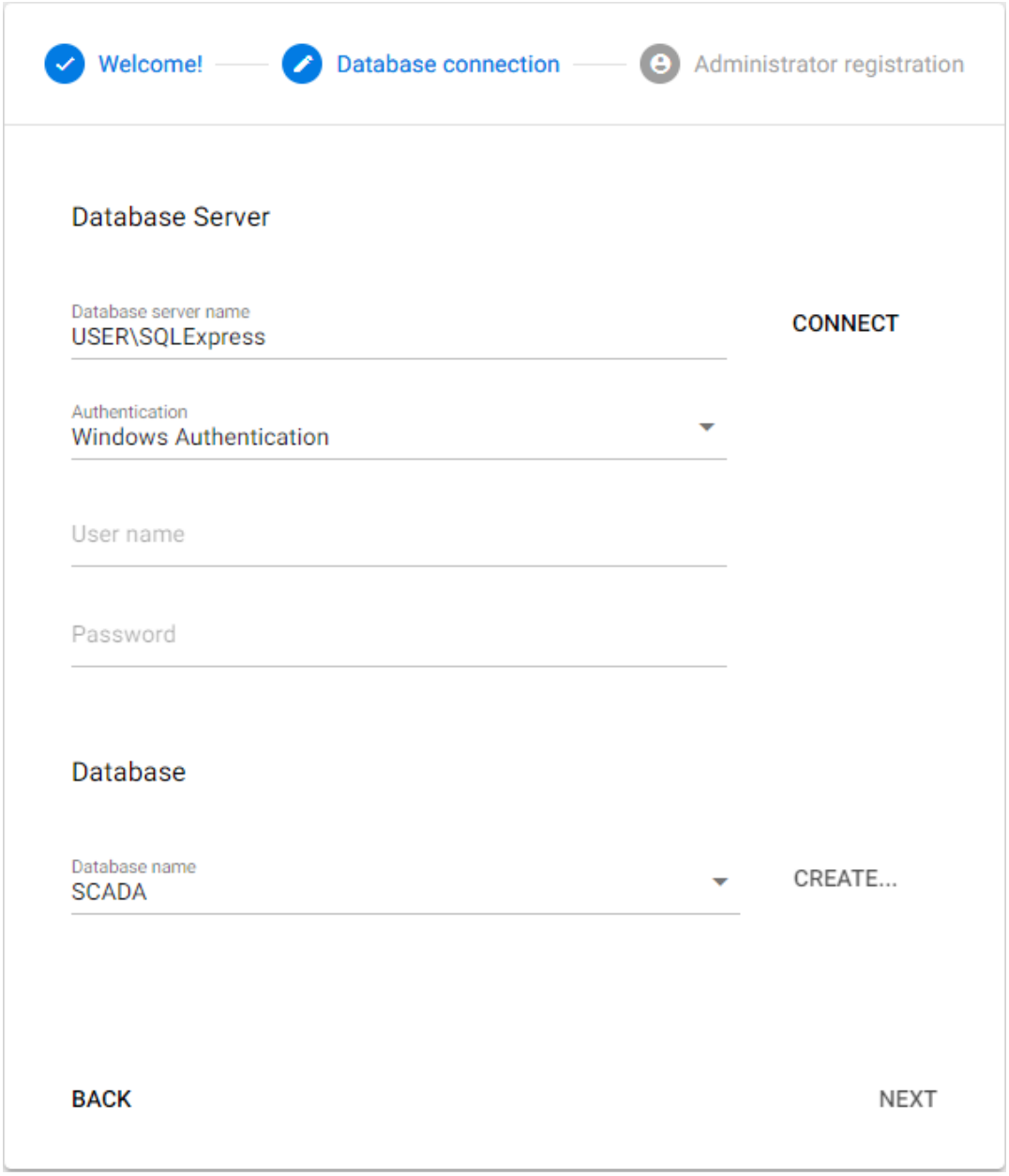
- Ensure that the computer is restarted after the SmartICS installation.
- Ensure that the SmartICS services are running.
- Install a compatible web browser. For details, see Compatible Products.
- Obtain the IP address of the SmartICS host.
- Determine the first web user credentials (login and password).

Procedure:

1. In the address field of the browser, enter *<https://SmartICS IP address>:5001*
   The configuration wizard appears.



2. *(Optional)* In the webpage, select the language:
   a. Click the current language (text and/or icon).
   b. From the list that appears, select the required language.
3. Click **Next**.
   DBMS connection settings appear.



Important
Initial settings are equal to those that were set during the SmartICS installation. If you entered the valid settings during the installation, skip steps 4–6.

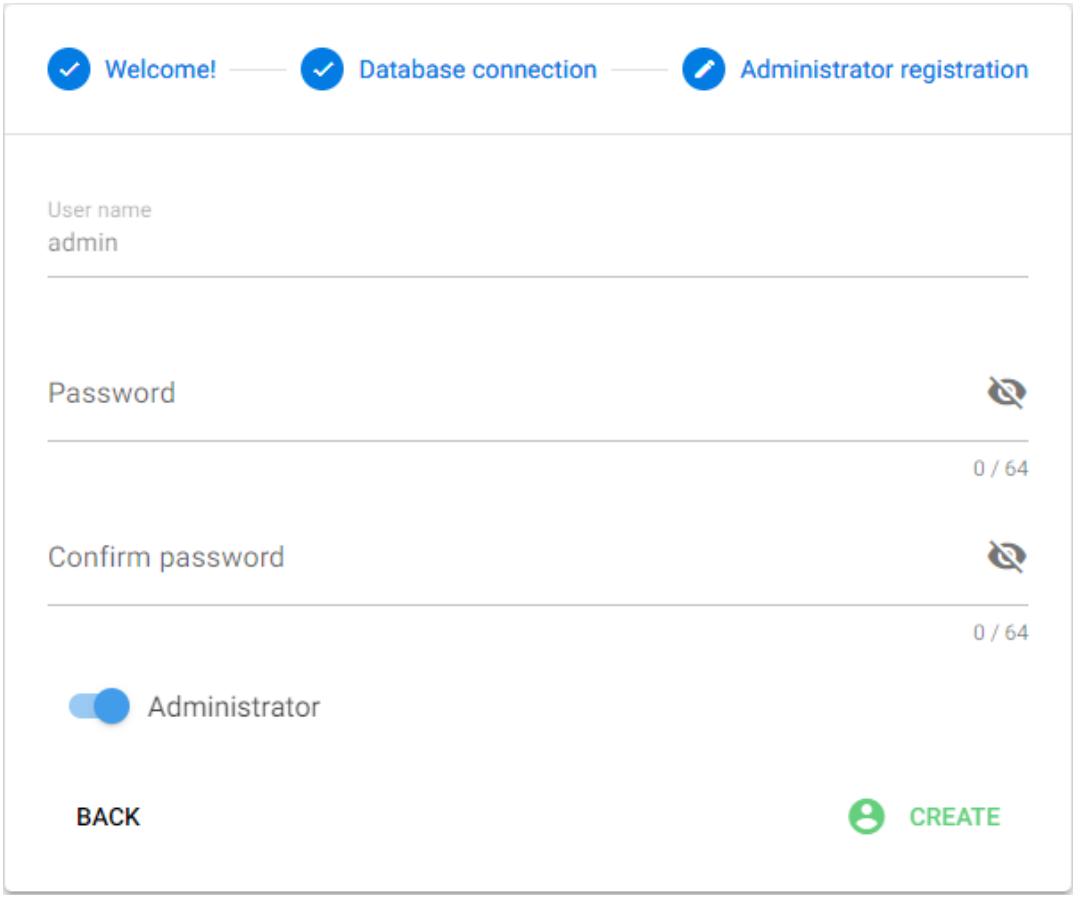
4. In the webpage that appears, in the **Database Server** area, in the **Database server name** field, enter the full DBMS name in the following format: *<DBMS host address>\<DBMS server name>*.
5. Configure SmartICS authorization in DBMS:

To use operating system/domain accounts,	from the **Authentication** list, select *Windows Authentication*.
To use DBMS (SQL) accounts,	perform the following actions: 1. From the **Authentication** list, select *SQL Server Authentication*. 2. In the **User name** field, enter the user name (login). 3. In the **Password** field, enter the user password. 4. *(Optional)* In the right part of the **Password** field, click **View password (👁‍🗨)** to validate the entered password.

6. In the same page, in the **Database** area, configure the database:

To create a new database,	perform the following actions: 1. Click **Create**. 2. In the dialog box, enter the database name, and then click **OK**.
To connect an existing SmartICS database,	from the **Database name** list, select the required database.

7. In the webpage, click **Next**.
First user account settings appear.



8. In the webpage that appears, set the user password:
   a. In the **Password** field, enter the first user password.
   b. In the **Confirm** field, enter the user password again.
   c. Click **Register ( )**.

Postrequisites:

Authorize in SmartICS to start its configuration. For details, see Logging on to SmartICS.

3.4 Logging on to SmartICS

Follow the procedure to log on to the SmartICS over the web interface.

Prerequisites:

- Create the first web user. For details, see Creating First User.
- Obtain user password.

Procedure:

1. In the address field of the browser, enter *<https://SmartICS IP address>:5001*
   Authorization webpage opens.
2. In the webpage, in the **User name** field, enter the user name (login). At the first authorization, enter *admin*
3. In the **Password** field, enter the user password.

4. *(Optional)* In the right part of the **Password** field, enter **Show password ( )** to validate the entered password.
5. Click **Login ( )**.

Postrequisites:

Configure SmartICS using the embedded help information. For details, see Embedded Help.

3.5 Embedded Help

Each SmartICS component contains the embedded help.

ControlCenter embedded help provides the following information:

- Minimum required procedures for SmartICS Server configuration.
- Context help for several ControlCenter controls.

SmartICS GUI embedded help provides the following information:

- Minimum required procedures for SmartICS administration and use.
- Context help for SmartICS GUI controls.

Context help can be accessed by selecting **Help ( )** in the **Help ( )** menu on the Toolbar, clicking the **Help ( )** icon on any element of SmartICS, or pressing F1.

4 Troubleshooting

This chapter provides information about the typical problems that Customer may experience during the SmartICS installation, configuration, and maintenance. For each problem, resolution and/or workaround is provided.

4.1 Failed to Install the Software

In some cases SmartICS fails to install install on the computer. This can be indicated in the following way:

- Installation program reports on the installation failure.
- SmartICS services fail to start.
- User is unable to access ControlCenter or SmartICS GUI.

This may occur for the following reasons:

- SmartICS is installed on the computer with 32-bit architecture (may also refer to as “x86 architecture”). This architecture type is **not** supported.
- SmartICS is installed in the operating system that does not comply with the system requirements. For details, see Host Requirements.
- Undefined error occurred during the installation. To resolve this issue, repair the software. For details, see <% TARGETTITLE%>.

4.2 Failed to Connect to ioServer

In some cases SmartICS user will see the stylized warning that SmartICS GUI is failed to connect to ioServer. This may occur for the following reasons:

- ioServer is stopped.
- SmartICS is not connected to DBMS.
- SmartICS database is not created.

ioServer Start and Restart

Start and restart of the SmartICS internal services required to perform the following actions:

1. ControlCenter authorization.
2. Restart/start of the corresponding service.

For details, see the ControlCenter embedded help.

Connection to DMBS

Connection to the DMBS service after the SmartICS installation requires to perform one of the following actions:

- Configuration of the DMBS connection in ControlCenter. For details, see the ControlCenter embedded help.
- Configuration of the DBMS using web interface. For details, see Creating First User.

Database Creation

SmartICS database creation is available at two stages:

- During the SmartICS installation.
- During the first web user creation. For details, see Creating First User.

4.3 Issues with DBMS

In some cases, SmartICS users may experience issues with the connection to DBMS and authentication in it. This occurs due to various reasons.

Several DBMS

It is possible that multiple DBMS versions and/or editions are installed on the same computer. For instance, it may occur when a third-party clients are installed on it. Using the same ports, sharing libraries, and occasional attribute matches may cause the problem.

To resolve the issues, it is highly recommended to move each DMBS version and edition into the different host.

Requirements Violation

DMBS must comply with the SmartICS system requirements. For details, see Compatible Products.

If you require to provide the SmartICS operation with a different Microsoft SQL Server version/edition, contact Elcomplus LLC representative in your region.

DBMS Host Unavailability

DBMS can be installed on a remote computer. Typical reasons of the host unavailability are as follows:

- Issues in the DBMS host network card.
- Issues in the SmartICS network card.
- Issues with the firewall configuration on any of those hosts.

To diagnose and reveal the reason of the DMBS unavailability, the following actions must be performed:

- DBMS host availability must be checked (for example, using the `PING` command).
- SmartICS host availability must be checked.
- Firewall settings must be checked.

If no issues is revealed, contact the customer's system administrator. If no problems is found in the computer system, submit a request to the SmartPTT Technical Support Center.

DBMS Service Stop

SmartICS disconnects from DBMS if the corresponding Windows service is stopped automatically or manually. To restore the connection, the service must be started. After the start, it is recommended to ensure that the service is running and not stopping again.

NOTE
To start the service, administrator right may require.

Additionally, it is recommended to configure the automatic DBMS start after the operating system of its host is restarted. For details, see Configuring DBMS Autostart.

Credential Modification

Authorization issues may occur if the user account settings were modified. The following changes may affect the aithorization failure:

- Password change.
- Password expiration.
- Removal of the DBMS administrator permissions from the user.

4.4 Rapid Disk Space Decrease

In some cases SmartICS users may notice the rapid decrease of the free disk space. In particular, it can be noticed when DBMS and SmartICS Server are installed on the same computer.

In this case, the current database size must be checked. If it is close to its maximum (depends on DBMS version and database settings), the reason of the disk space consumption can be in the log file increase. The file will contain messages that inform the reader about unavailability .

Contact Information

The document describes the product developed by Elcomplus LLC. The official company's website is www.elcomplus.com.

For contact information with the Elcomplus LLC representatives, see www.elcomplus.com/contacts.

Technical Support

Customer support is provided by SmartICS Support Center.

To contact a support engineer, email to support@smartics.io.

In America, customer support is provided by Elcomplus, Inc. To contact support engineers, use the following contact information:

- Phone: +1 786-362-5525
- Email: miami@smartptt.com
- Mailbox: 290 NW 165th St, Ste P-200, 3rd Flr
  Miami, FL, 33169, USA

Customer Documentation

This document is authored and published by Elcomplus LLC. If you have any comments and suggestions on it, please email them to support@smartics.io.