Enterprise Application

Configuration Manual

Version 4.5

SICK
Sensor Intelligence.

Part Number: XXXX
Publication: XXXX
Release Date: XX/XX/XXXX

Copyright © 2025

SICK

150 Royall St

Suite 104

Canton, MA 02021

Software Versions

Software / Tool	Function	Version
Enterprise Application	• Extended compatibility to all SICK products and external applications using a new heartbeat JSON and MQTT topic for dynamic data integration. • Introduced a multi-level Tree View dashboard with zoom, pan, breadcrumb navigation, dynamic data-type selection, and a draggable Summary & Filters panel. • Added a dedicated page to display and manage offline products with search and refresh capabilities. • Added a dedicated page for downloading PDF reports directly from the EA server. • Added OpenID authentication with JWT assertion support alongside Database and LDAP options. • Added a Notification Logs page to track notifications for troubleshooting and auditing. • Improved facility configuration with bulk add/edit/delete, inline edits, and MQTT connections via IP-address lists. • Enhanced List View with data-type filters, health/performance pagination, and a draggable Summary & Filters panel. • Enhanced Map View with a redesigned cluster-info modal, autocomplete for region/country, dynamic product-state display, and a Summary & Filters panel. • Increased maximum notification frequency to one hour.	4.5

Contents

1 About This Manual

1.1 Purpose of the Configuration Manual

This Enterprise Application (EA) 4.5 Configuration Manual provides comprehensive instructions for administrators and technical users to set up and configure the EA 4.5 software for Analytics functionality. It covers all necessary steps to install, configure, and maintain the system, including product management, MQTT connectivity, authentication, notifications, and license application. This manual is designed to ensure that EA 4.5 is properly deployed to aggregate and process real-time data from SICK products and facility servers, enabling robust analytics for enterprise operations.

1.2 Add a New Group

Use the **Create Group** dialog to define a new user group. Groups control which users have access to specific roles and privileges, such as equipment monitoring, maintenance management, or production reporting.

1. In the **Manage Groups** interface, select the **Add** icon in the top-right corner.
   The **Create Group** dialog appears.

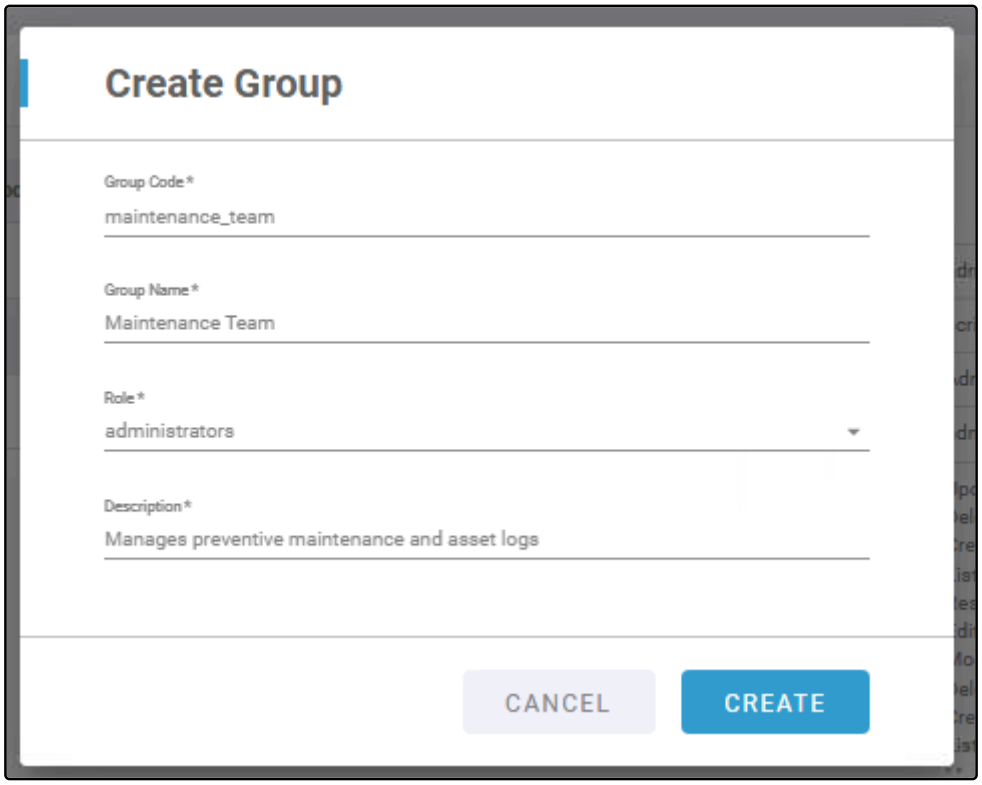


Figure 1

2. Fill in the required fields:

©SICK All rights reserved

Field	Description	Example Input
Group Code	Unique system-friendly identifier (use lowercase and underscores).	maintenance_team
Group Name	Display name that users will see.	Maintenance Team
Role	The role to assign to the group (choose from the existing list).	administrators
Description	A short explanation of the group's responsibilities.	Manages preventive maintenance and asset logs

3. Select **Create** to add the group or **Cancel** to close the dialog without saving.

4. A snackbar message confirms the result:
   "Group created successfully."

5. The new group now appears in the **Group Table**, and its details are available in the **Group Details Panel**.

1.3 Related Documentation

For information on using **EA 4.5** features, such as navigating the dashboard, viewing product data, or performing enterprise searches, refer to the **EA 4.5 User Manual**. The User Manual complements this Configuration Manual by detailing how to interact with the **EA 4.5** interface and leverage its analytics capabilities.

1.4 SICK Support Contact Information

For assistance with EA 4.5 installation, configuration, or troubleshooting, contact SICK support:

- **Sales and Product Support:** Visit www.sick.com
- **Technical Support:** Access the SICK Support Portal at https://supportportal.sick.com/
- **Address:** 150 Royall St suite 104, Canton, MA 02021, United States

©SICK All rights reserved

2 Security and Usage Disclaimer

Overview

This section outlines important security, operational, and usage considerations for the product. The operating entity is responsible for ensuring that the product is deployed, configured, and maintained in a secure and controlled environment.

Network Services and Protocols

A diagram and list of all network services and protocols used by the product are available in the product-specific Release Notes at:

https://support.sick.com

The listed services and protocols represent the best available knowledge. No service or protocol has been intentionally omitted.

Network Security

The operating entity must implement appropriate measures to protect the operating environment and network infrastructure. This includes ensuring secure and trustworthy communication between the product and all connected systems and devices.

Physical Access Protection

The product is not intended for use in easily accessible or public areas.

- Protect the product from unauthorized physical access
- Restrict access even for personnel present in the working area
- Ensure that only authorized individuals can access the product

Protection of Installation Environment

The operating entity must prevent unauthorized access to the area in which the product is installed and operated.

Protection of Transmission Media

Transmission media (for example, data cables and network connections) must be protected against unauthorized access, interception, or tampering.

Data Protection and Privacy

The product is technically capable of identifying individuals or capturing personal data. The operating entity is responsible for ensuring compliance with applicable data protection and privacy regulations.

Protection Against External Force

The product is not designed to protect data or functionality against external force, tampering, or vandalism.

Access Control and User Management

The operating entity must configure access credentials and permissions according to the principle of least privilege. Only the minimum required access rights should be assigned.

External Systems and Services

The product may interact with external systems such as:

- Analytics systems

©SICK All rights reserved

- FTP servers accessed by the product

These integrations must be secured appropriately.

Cryptographic Data Handling

The product does not store cryptographic secrets that would allow it to access other systems or devices.

Intended Use Limitations

- Safety-critical applications
- Control or authorization of physical access

Responsibility Statement

The operating entity is solely responsible for securing the product, its environment, and ensuring compliant usage.

Important

Failure to implement appropriate security and access control measures may result in unauthorized access, data breaches, or misuse of the product.

©SICK All rights reserved

3 System Components

SICK EA works together with the existing key components in your Facility to collect and report on system data. These are:

- The EA software
- PC/server to host EA
- Client computers
- Active Facilities

3.1 EA software

EA software receives and processes data received from Facilities, captured from SICK sensors and controllers. All data sent from connected systems is stored in the Facility database EA receives data from Facility using **MQTT** publish-subscribe-based messaging protocol. The host PC supports the EA client dashboard requests. All user access to the database is provided through the **EA dashboard**.

3.2 PC/server host

EA software is installed on your host PC/server. All collected system data from the Facility is requested in the host PC. EA configuration data is saved in this PC.

3.3 Client computers

The client computer is any PC connected to the EA network. EA's client dashboards are **HTML5 web applications**. The client dashboards connect to the EA to access Facility data and provide a powerful user experience. Client computers provide a platform for the EA interface ("**dashboard**"), to provide access to Facility information and database information stored on the host PC. The dashboard makes it possible to quickly search, view, and export information obtained from the auto identification solution.

3.4 Active Facilities

EA retrieves Facility data using **MQTT** publish-subscribe-based messaging protocol. To view Facility state and data for each Facility linked to EA application, we need an active Facility,

©SICK All rights reserved

4 System Architecture

The illustration below provides a visual representation of EA architecture, and illustrates how the system components work together to provide a robust and comprehensive analytical tool for your auto ID systems.

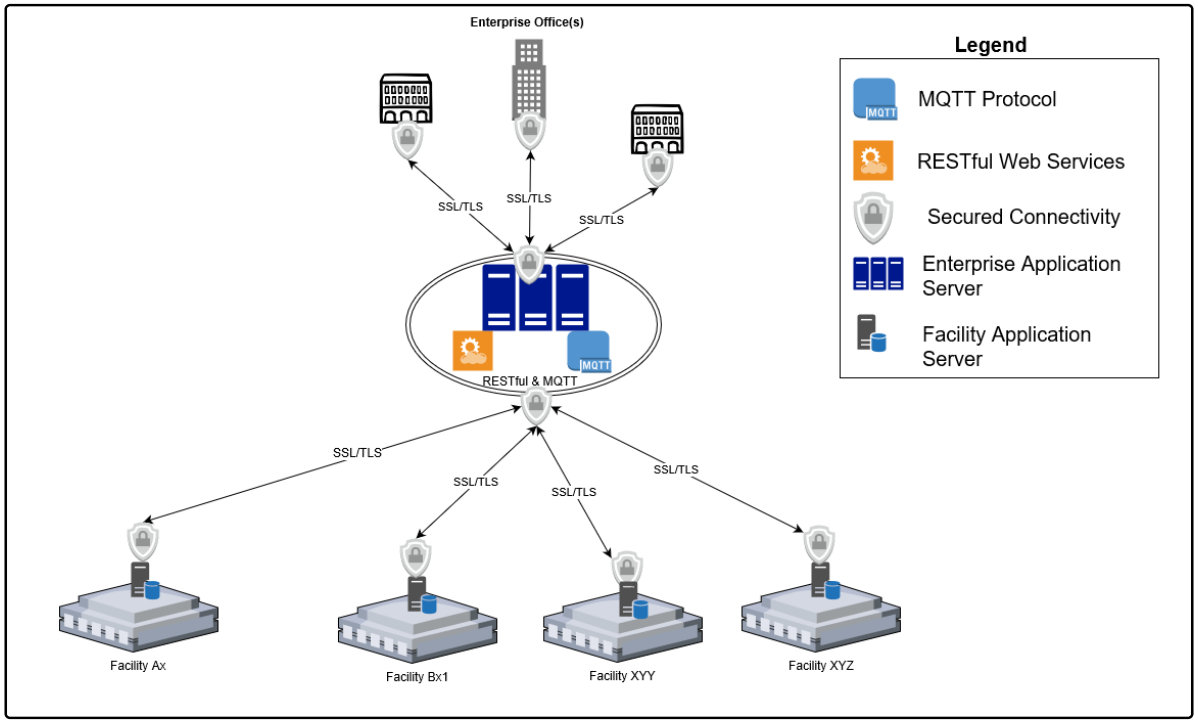


Figure 2

©SICK All rights reserved

5 Hardware Requirements

The following minimum system hardware requirements must be met prior to installation. Note that these are minimum requirements; final hardware configuration is application dependent. Data and storage duration is application dependent.

Component	Specification
Operating System	Windows 7 (64 bit), Windows 10 (64 bit), Windows Server 2012 R2 (64 bit), Windows Server 2016 (64 bit), Windows Server 2008 R2 Standard
Required Disk Space	Depends on application. Minimum 500 MB. Key factors include number of systems and sensors connected, number of objects per day, number of days for storage.
Processor	Depends on application. Minimum Intel Core i7-6700TE (quad-core 2.40 GHz)
Monitor Resolution	1920 x 1080 pixels, 16:9 aspect ratio for best results
Supported Browsers	Google Chrome, Mozilla Firefox, Internet Explorer 11, Microsoft Edge
Note	**Note:** This software can be integrated with most anti-virus software. Certain user-defined ports need to be exempted from file scanning: • 2008 (TCP communications) • 8441, 8442, 8443 (HTTPS) • 8080, 8081, 8181 (REST and WebSocket communications) • 8406, 3306 (Database communications) The software is available with installation packages Java 8 (JRE) and MySQL 5.7.

©SICK All rights reserved

6 Installation

This section provides instructions for installing the SICK Enterprise Application (EA) to enable real-time monitoring and analytics of SICK products.

6.1 To Launch the Installer on Windows

1. Double-click the executable file (for example, **SICK_Enterprise-4.5.exe**).

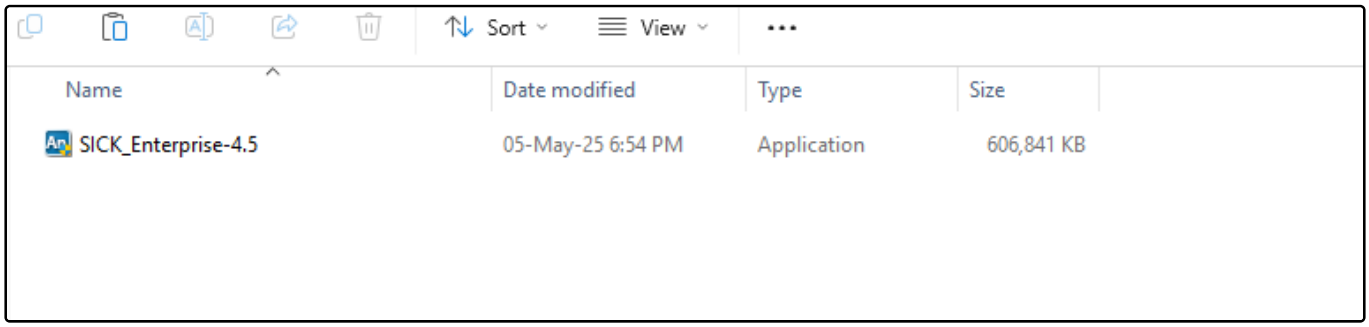


Figure 3

2. The **InstallAnywhere** dialog will be displayed, showing a progress bar as the installer prepares.

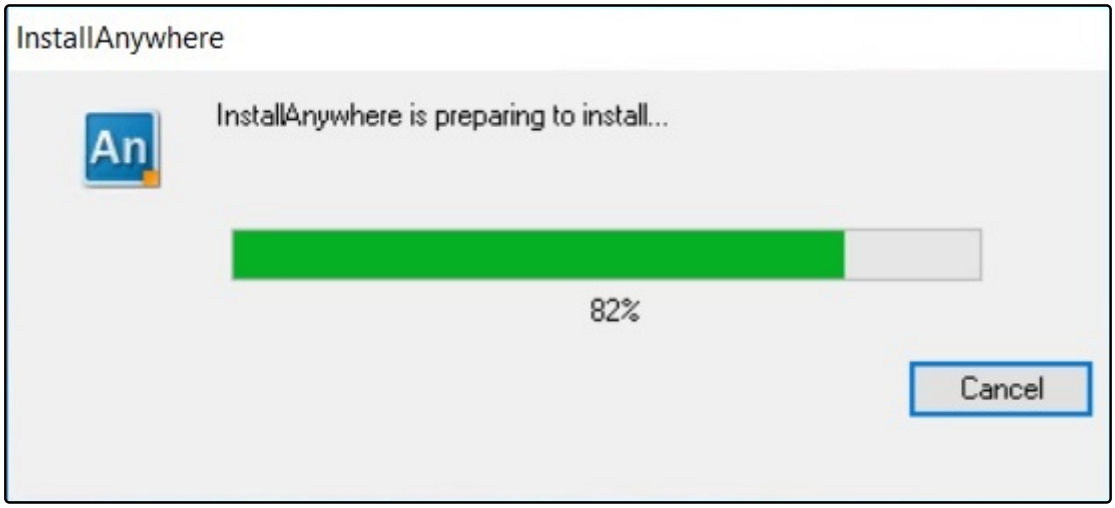


Figure 4

3. Once the progress on the **InstallAnywhere** dialog reaches 100%, the **Enterprise Application Installation Wizard** will launch with the **Introduction** screen. Click **Next** to proceed.

©SICK All rights reserved

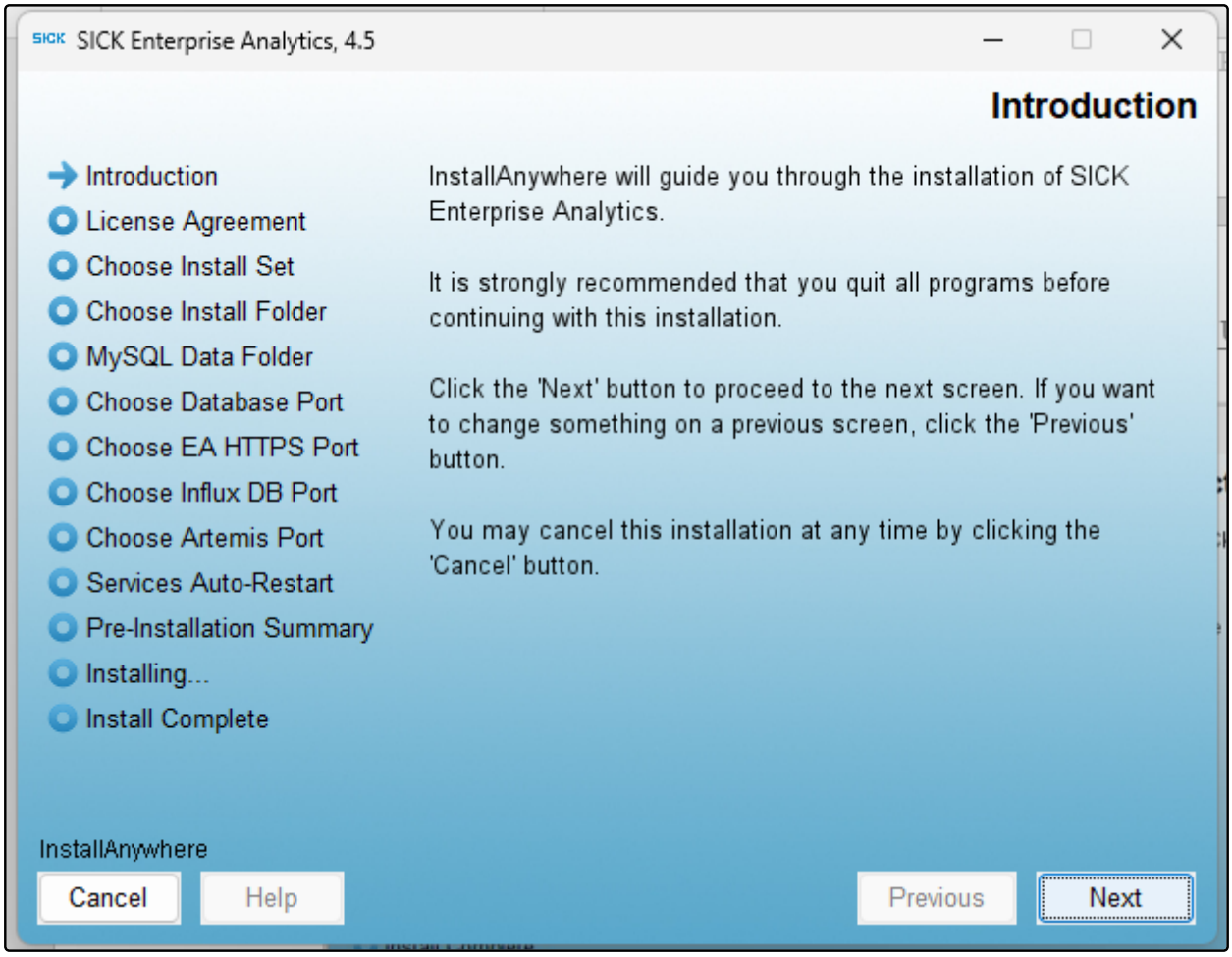


Figure 5

4. The **License Agreement** screen prompts you to read the End User License Agreement (EULA) and agree to its terms. Review the terms, select the checkbox to acknowledge agreement, and click **Next**.

©SICK All rights reserved

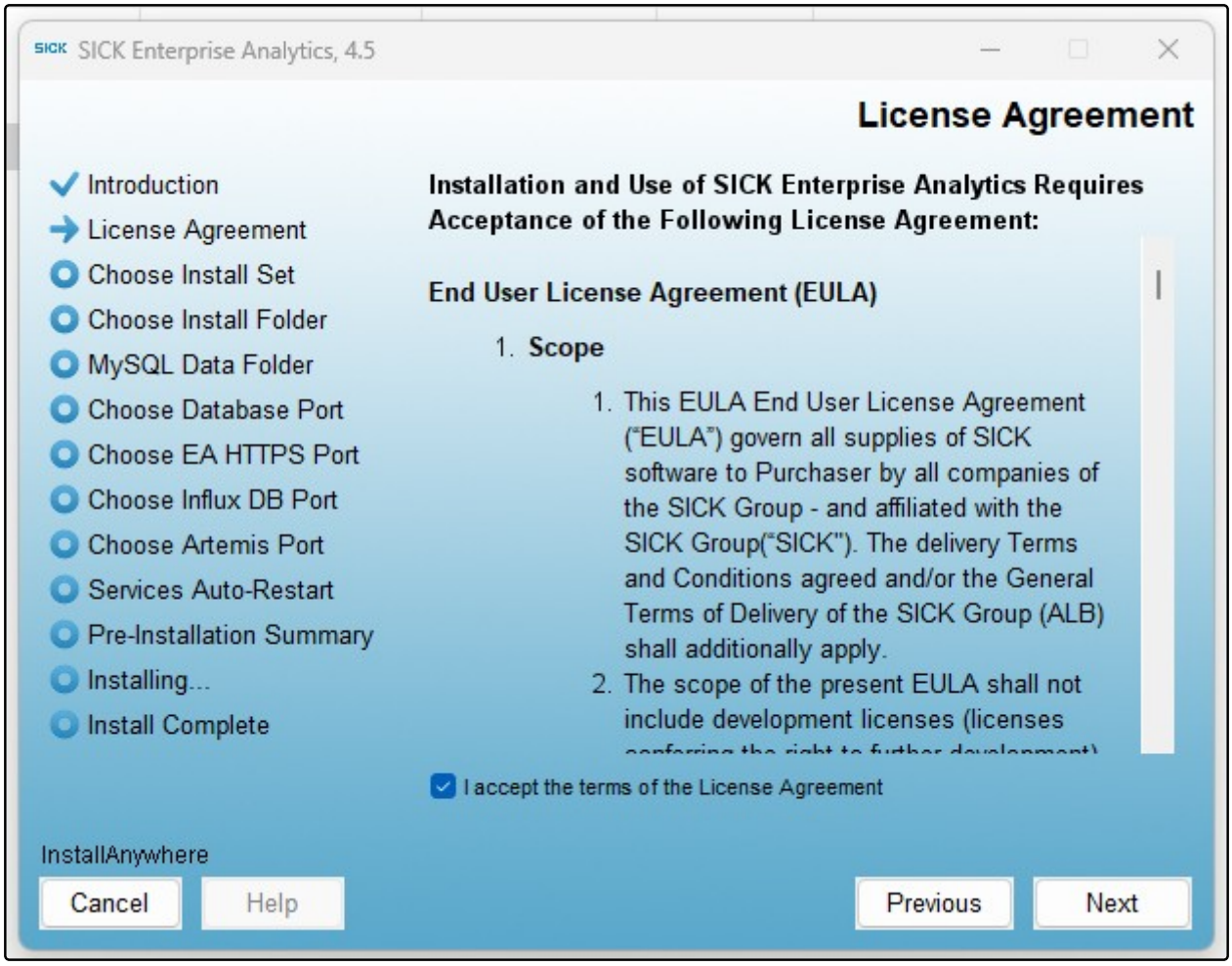


Figure 6

5. The **Choose Install Set** screen appears:
   - **Full Installation**: Installs all features for the SICK Enterprise Analytics (EA) application.
   - **Custom Installation**: Allows you to customize which features to install. Select the desired option and click **Next**.

©SICK All rights reserved

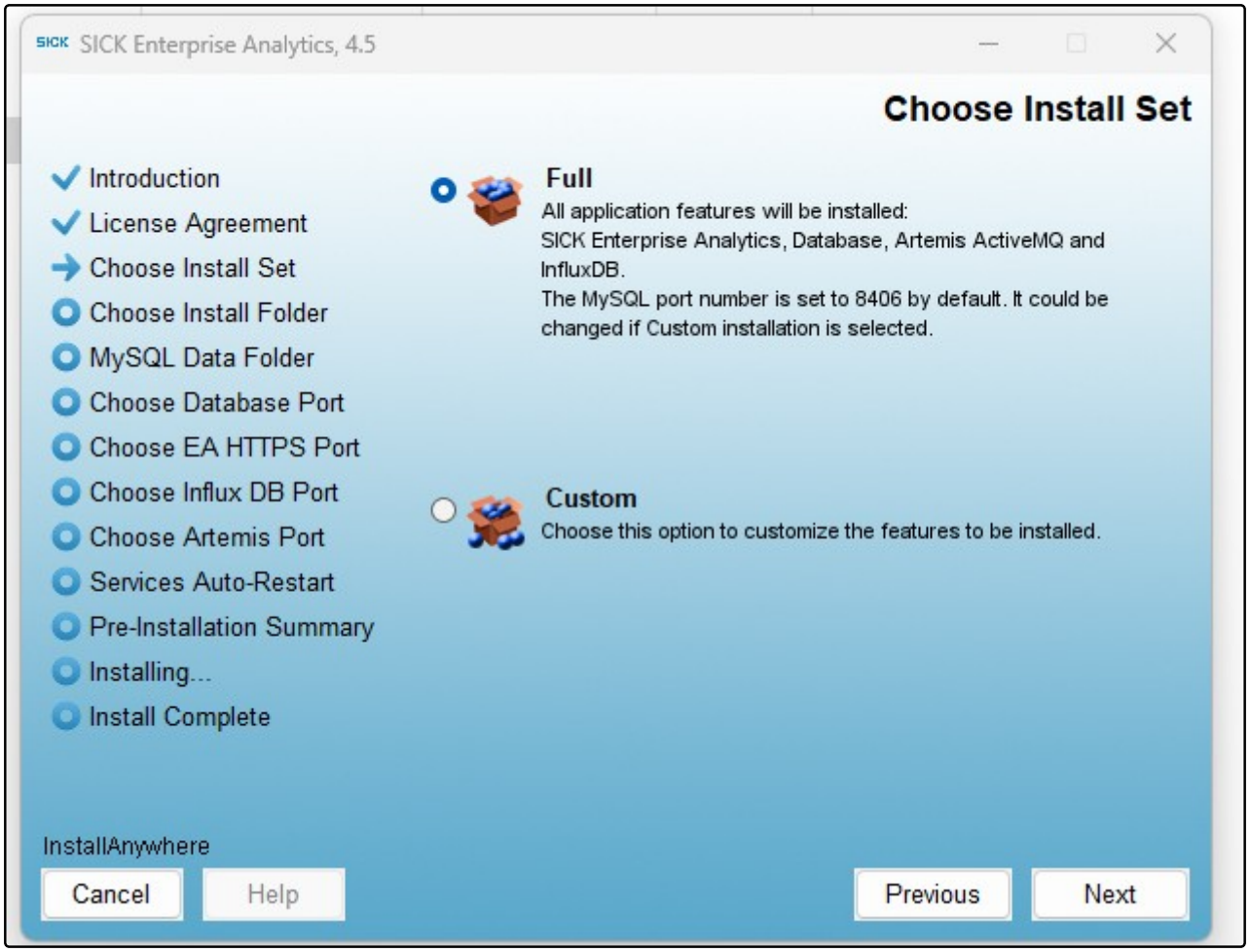


Figure 7

©SICK All rights reserved

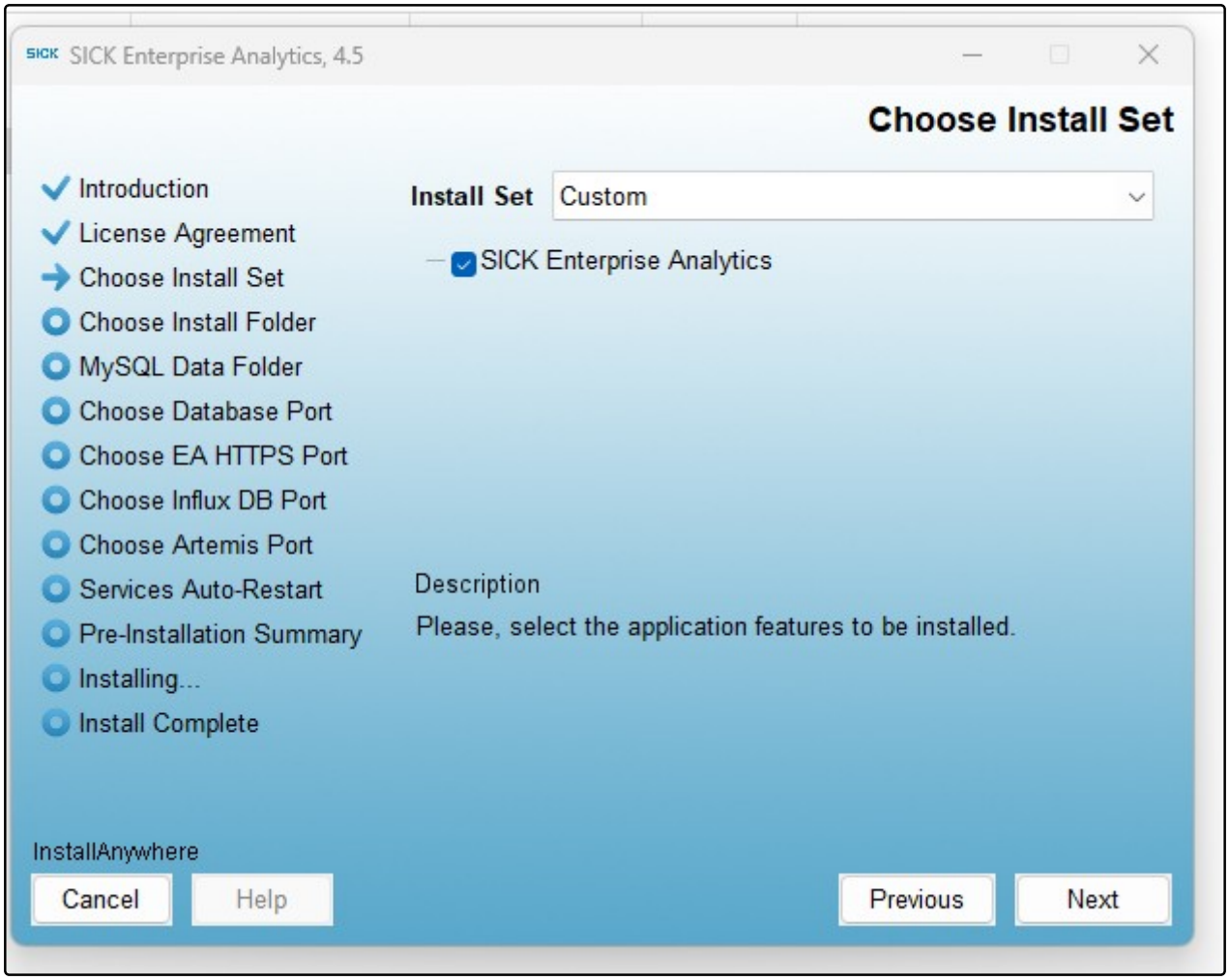


Figure 8

6. The **Choose Install Folder** screen appears:
   - The default path is **C:\Program Files\SICK\Enterprise Application**. Click **Next** to use this location.
   - To change the directory, click **Choose...**, or **Restore Default Folder**.

©SICK All rights reserved

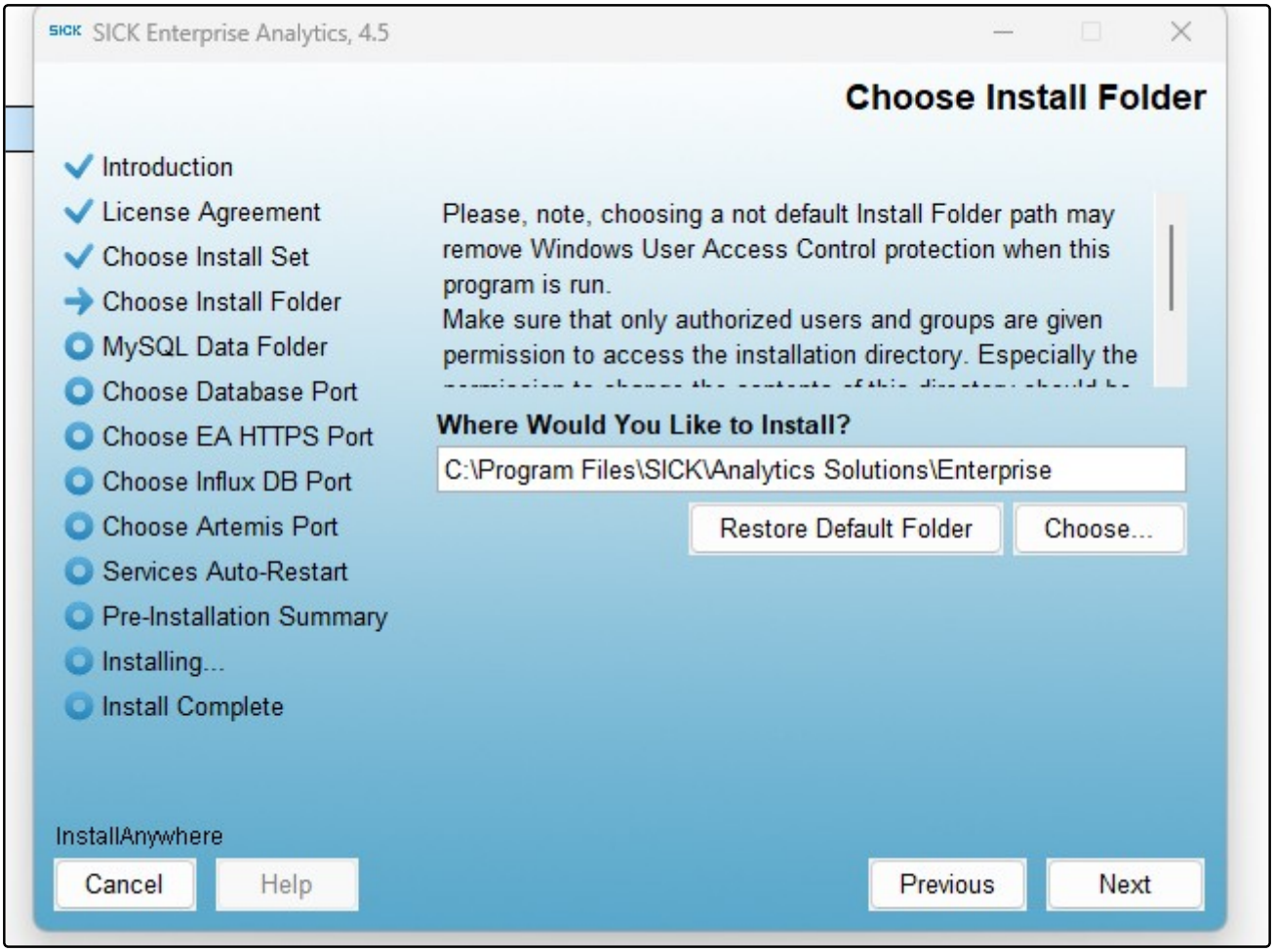


Figure 9

7. The **MySQL Data Folder** screen appears:
   - The default path is **C:\Program Files\SICK\Enterprise Application\MySQL**. Click **Next** to use this location.
   - To change, click **Choose...**, or **Restore Default Folder**.

©SICK All rights reserved

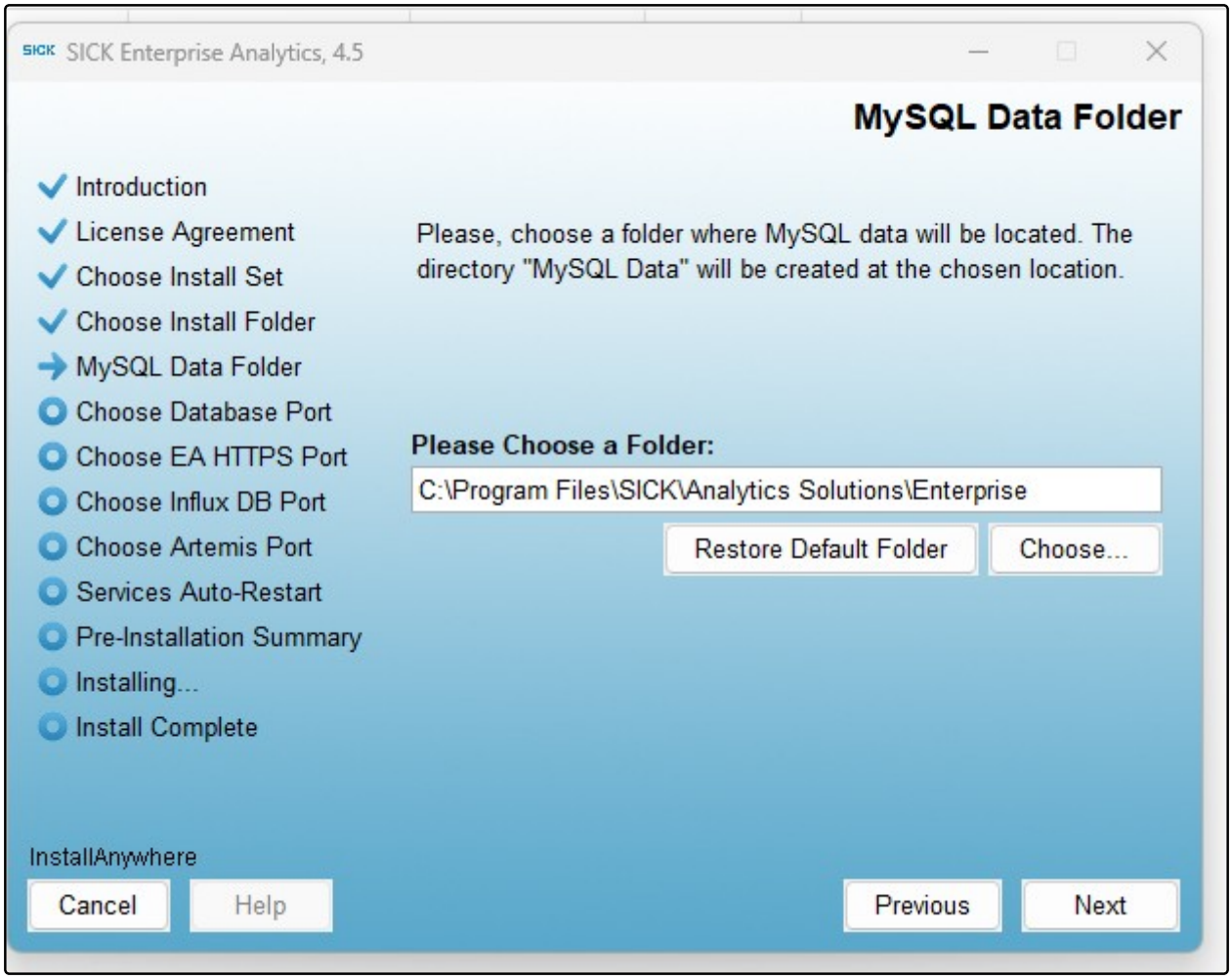


Figure 10

8. The **Choose Database Port** screen appears, prompting you to enter a valid port number for the MySQL database connection:
   - The default port is **8406**.
   - Valid Range: **1024** to **65535**. Ensure the selected port is not in use by another application.
   - Click **Next** to proceed or **Previous** to return to the previous screen.

©SICK All rights reserved

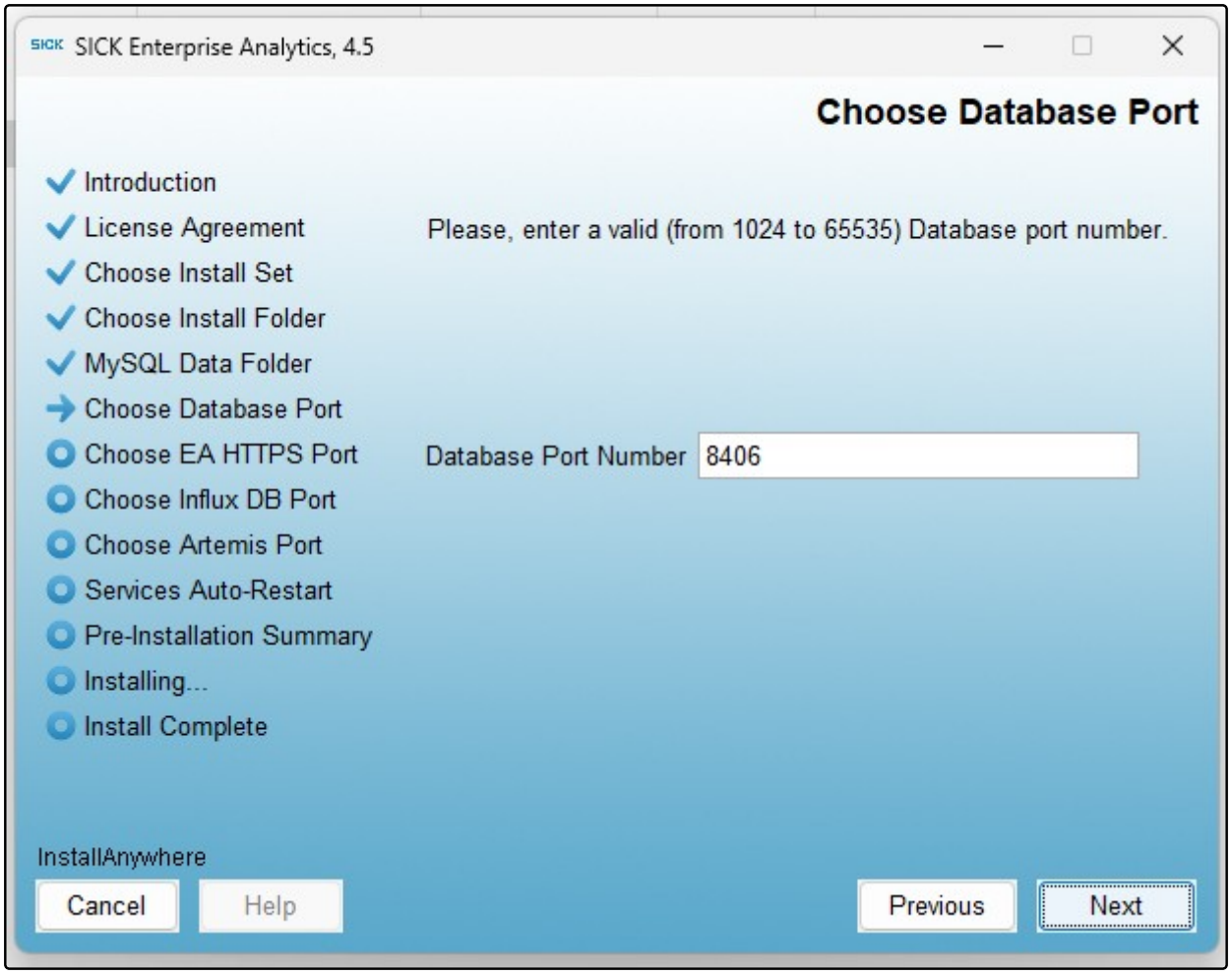


Figure 11

9. The **Enable Services Auto-Restart on Failure** screen appears:
   - **Checked** (default): The system restarts services automatically.
   - **Unchecked**: Use this if services are managed manually.

©SICK All rights reserved

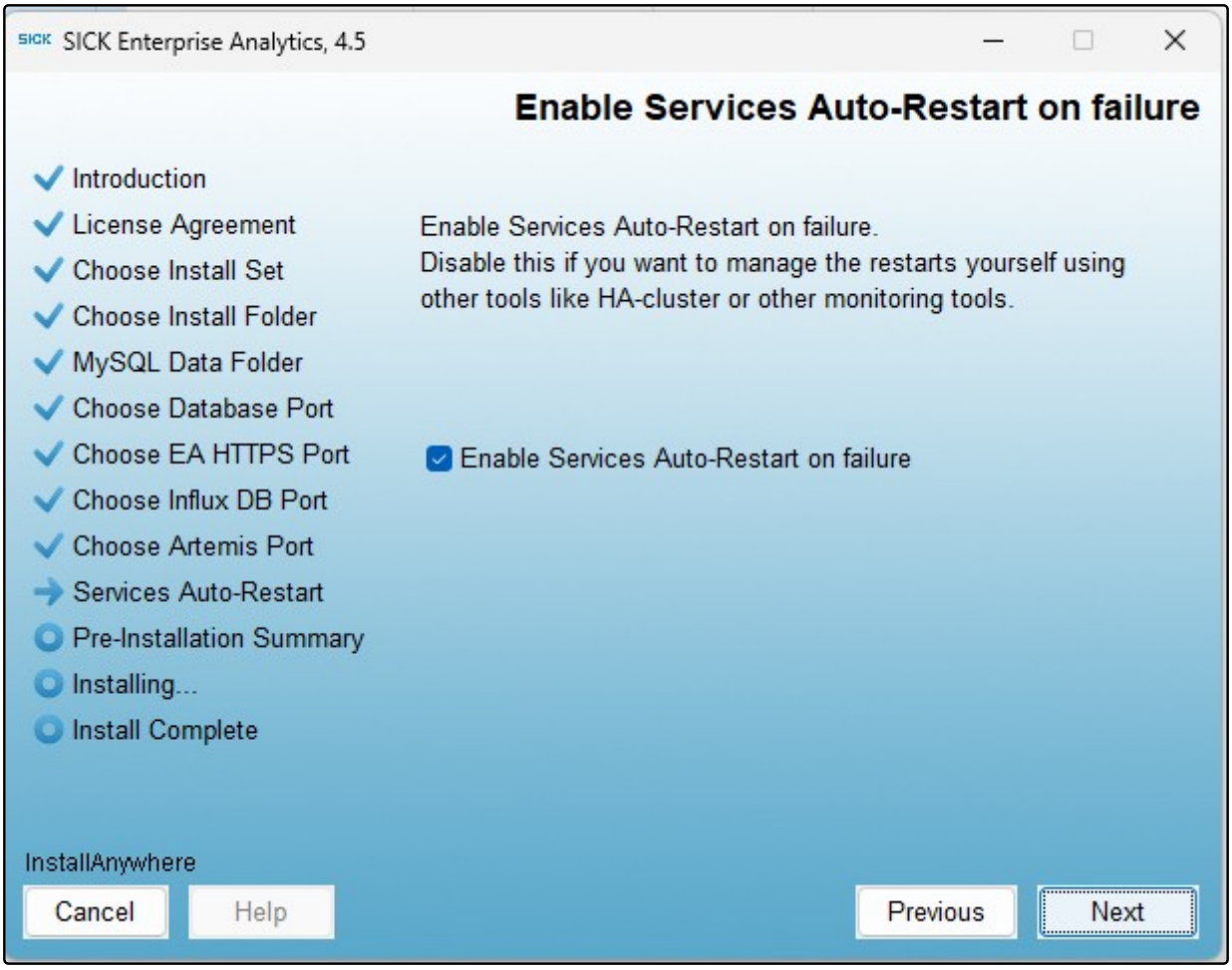


Figure 12

10. The **Manage Product Windows Services as a User** screen appears:
    - Check the **Manage Product Windows Services as a User** checkbox to enable the fields.
    - In the **Domain** field, enter the domain (e.g., **RPCDOMAIN**).
    - In the **User Name** field, enter the username (e.g., **gMSA03**).
    - For a Group Managed Service Account (gMSA), append **$** to the username (e.g., **gMSA03$**).
    - Click **Next** to proceed.

©SICK All rights reserved

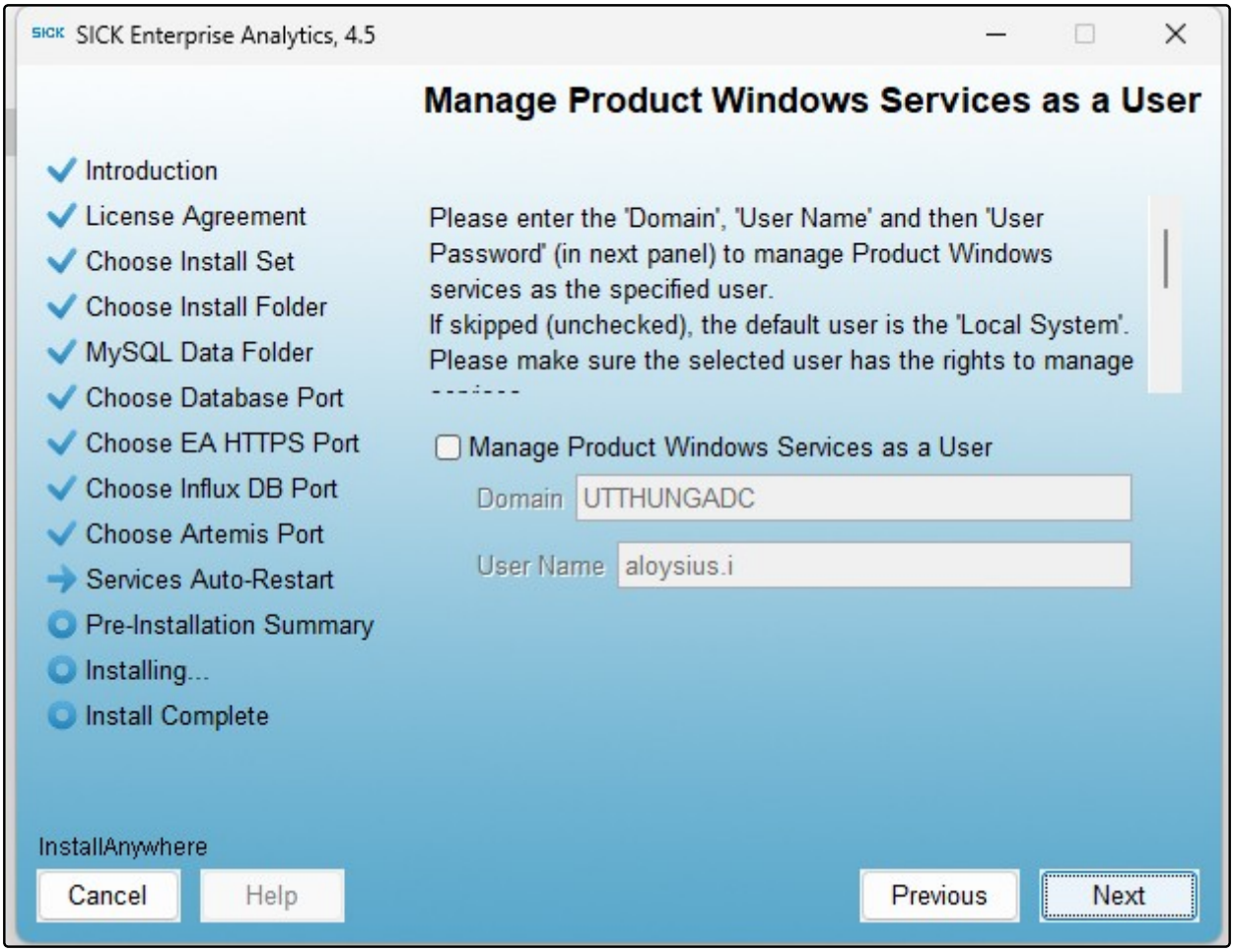


Figure 13

11. The **Certificate Properties File** screen appears:
    - **Choose…**: Browse to and select the required `cert.properties` file (for example, `C:\certupdates\cert.properties`).
    - **Restore Default File**: Use the default certificate properties file if no custom file is provided.

    Click **Next** to proceed.

©SICK All rights reserved

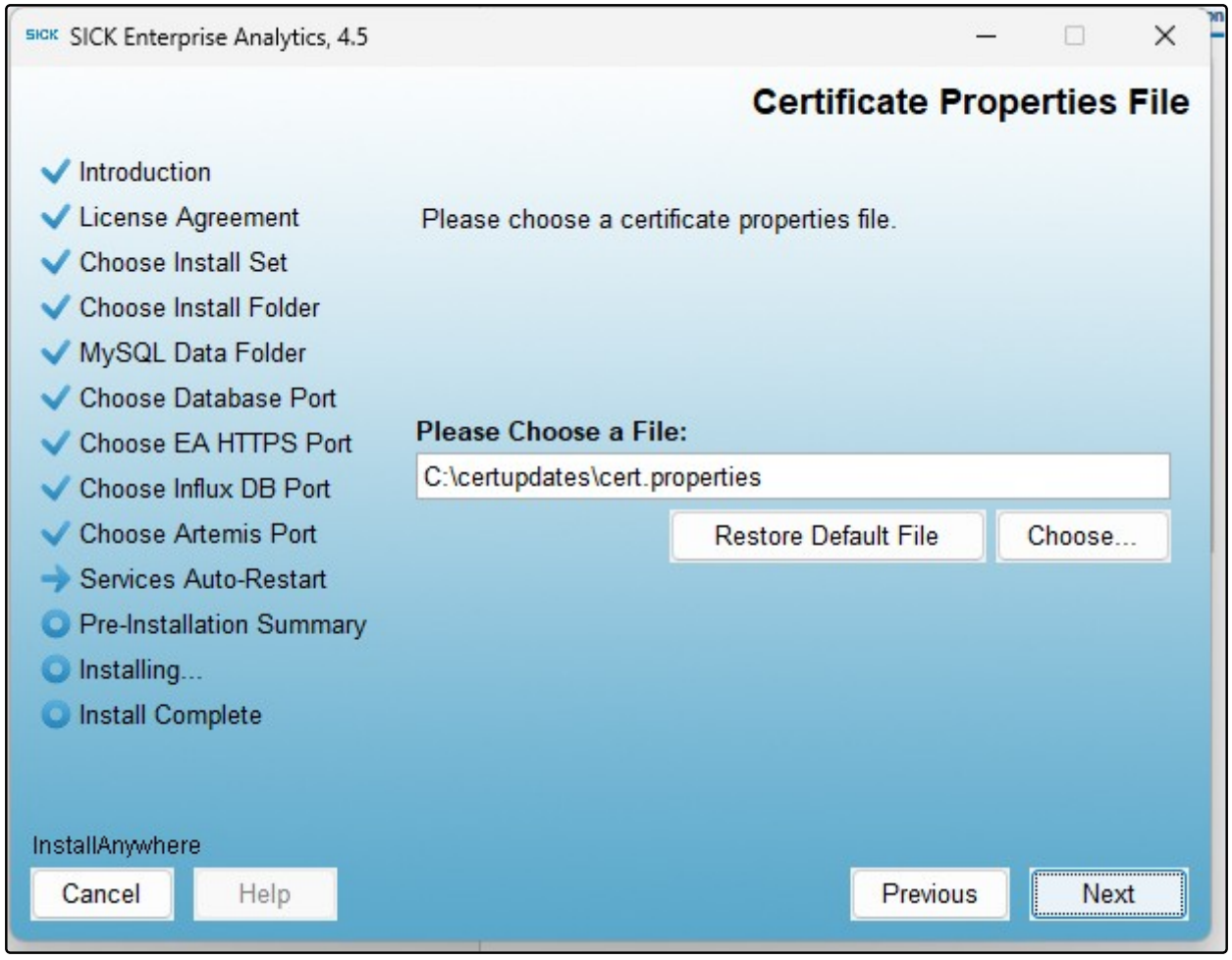


Figure 14

12. Review all details on the **Pre-Installation Summary** page and click **Install** to begin the installation.

©SICK All rights reserved

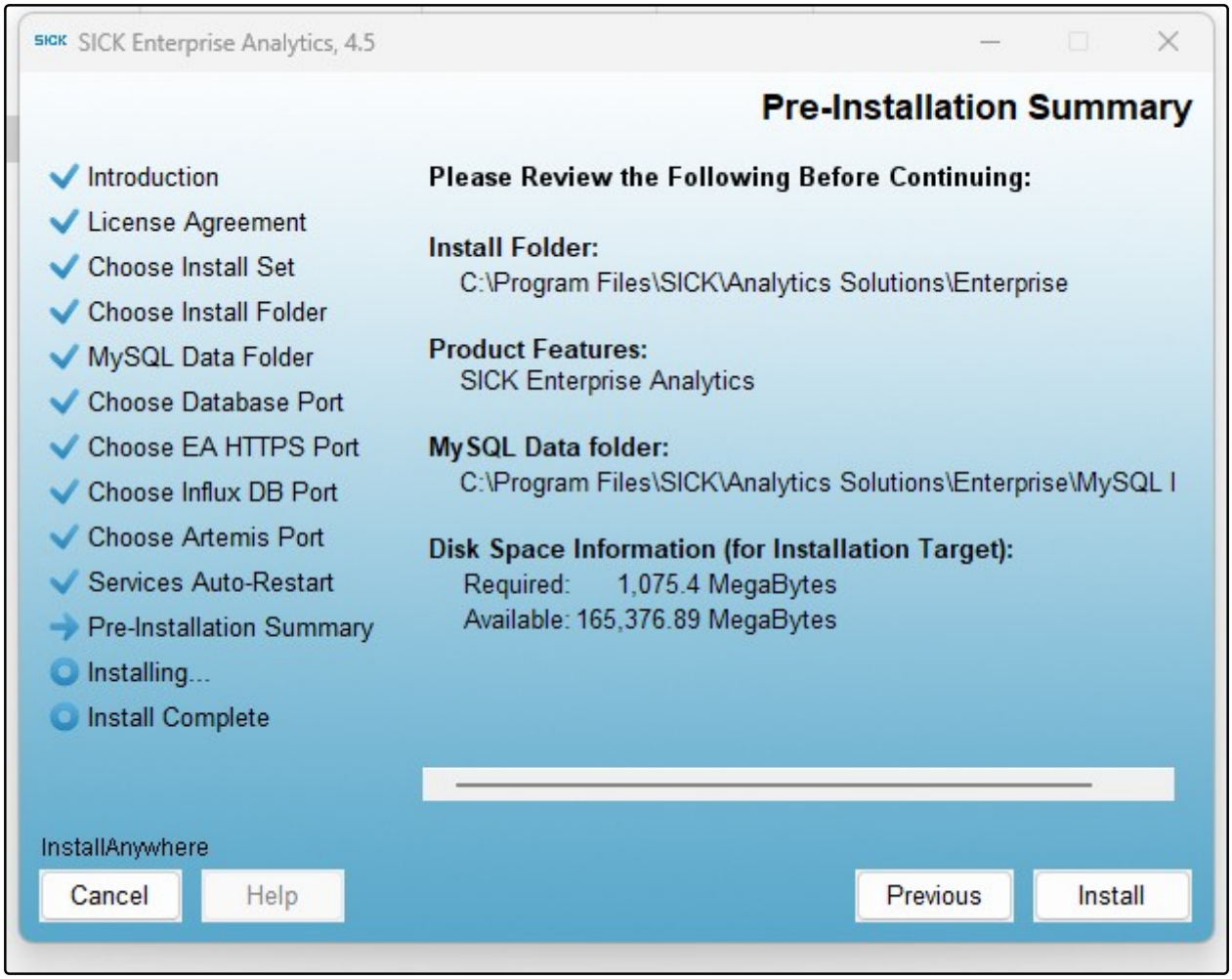


Figure 15

13. The installation begins. You can track progress using the progress bar at the bottom of the screen.

©SICK All rights reserved

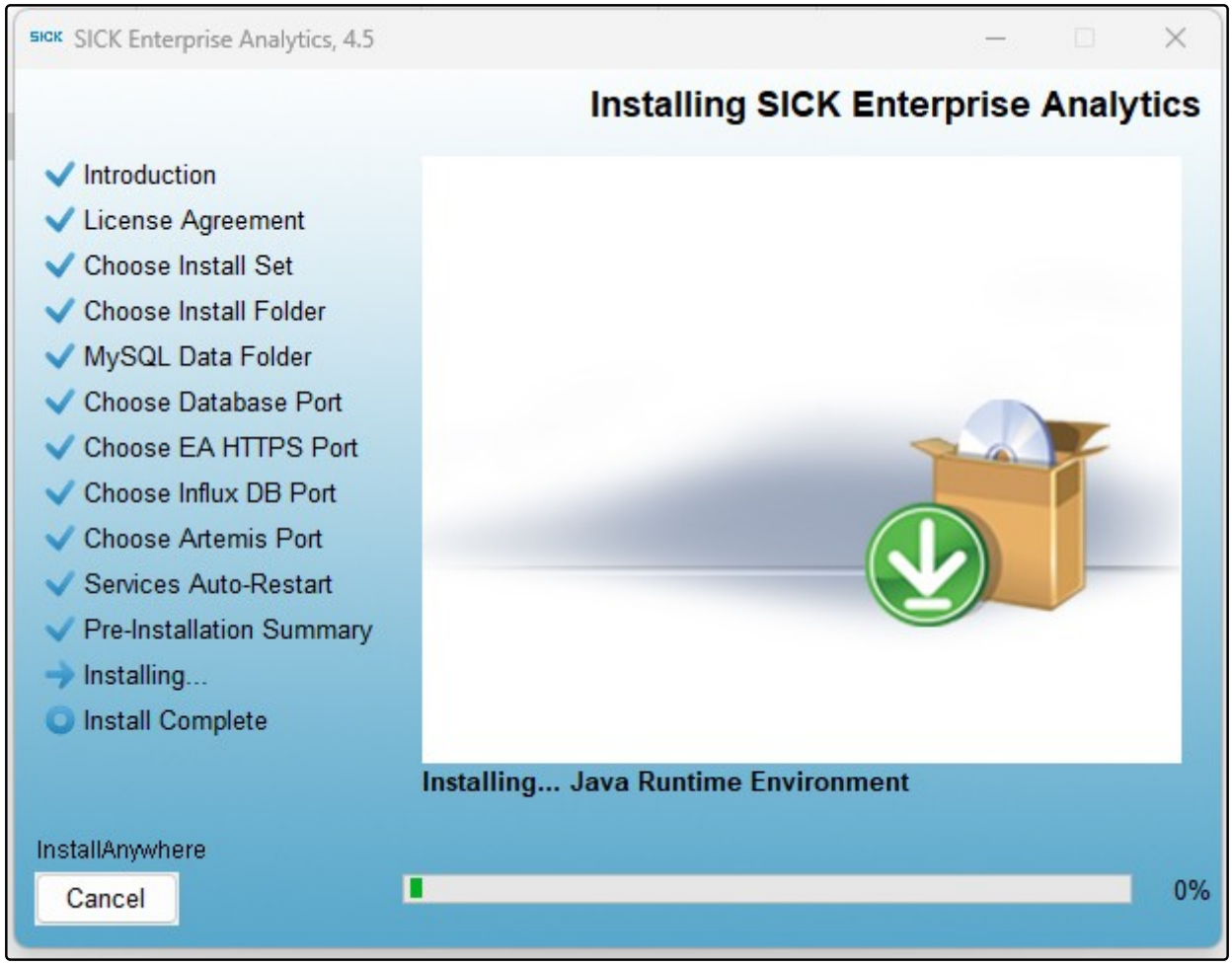


Figure 16

14. Once installation is complete, the **Install Complete** window appears. Click **Done** to finish.

©SICK All rights reserved

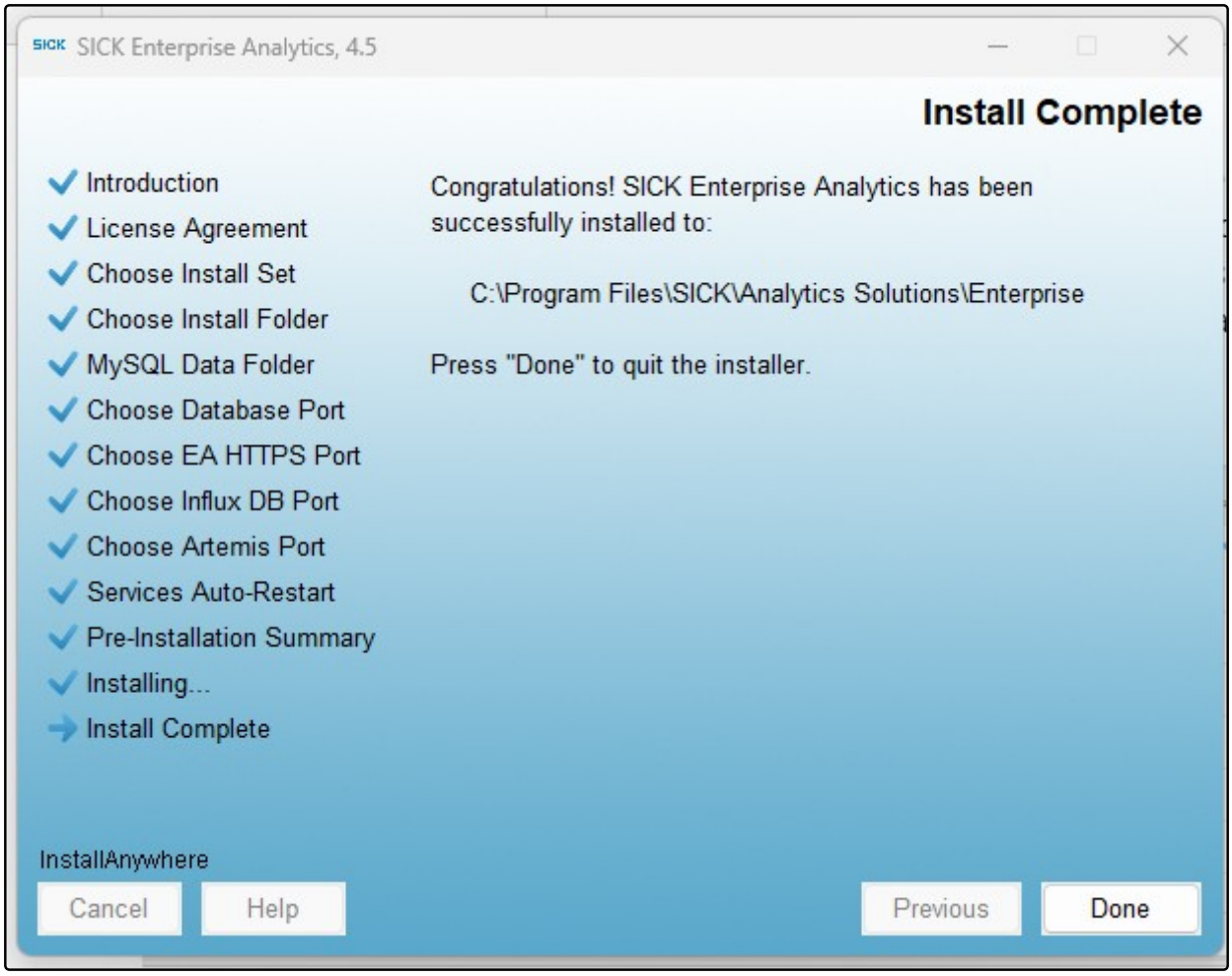


Figure 17

6.2 To Launch the Installer on Linux

This section explains how to install SICK Enterprise Application (EA) on a Linux system.

1. The **Launch Installer** step:
   - Navigate to the folder where the installer `.bin` file is located.
   - Open a Terminal in that location.
   - Make the file executable: `chmod +x SICK_Enterprise_Application-4.5.bin`
   - Launch the installer with sudo: `sudo ./SICK_Enterprise_Application-4.5.bin`
   - Wait for the **InstallAnywhere** installer to start.

©SICK All rights reserved

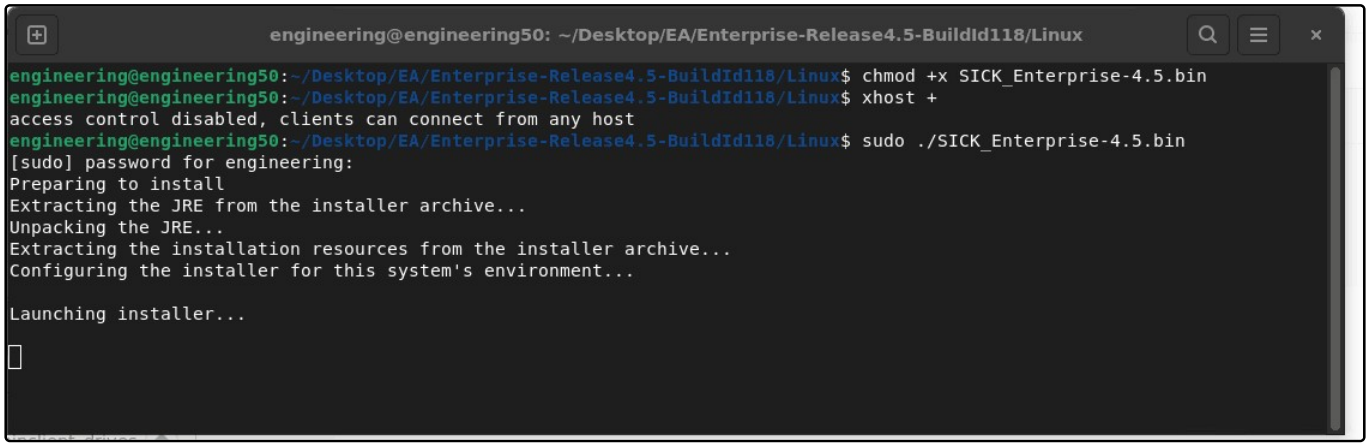


Figure 18

2. The **Introduction** screen appears:
   - Provides an overview of the installation process.
   - Close all running applications before continuing.
   - Click **Next** to proceed.

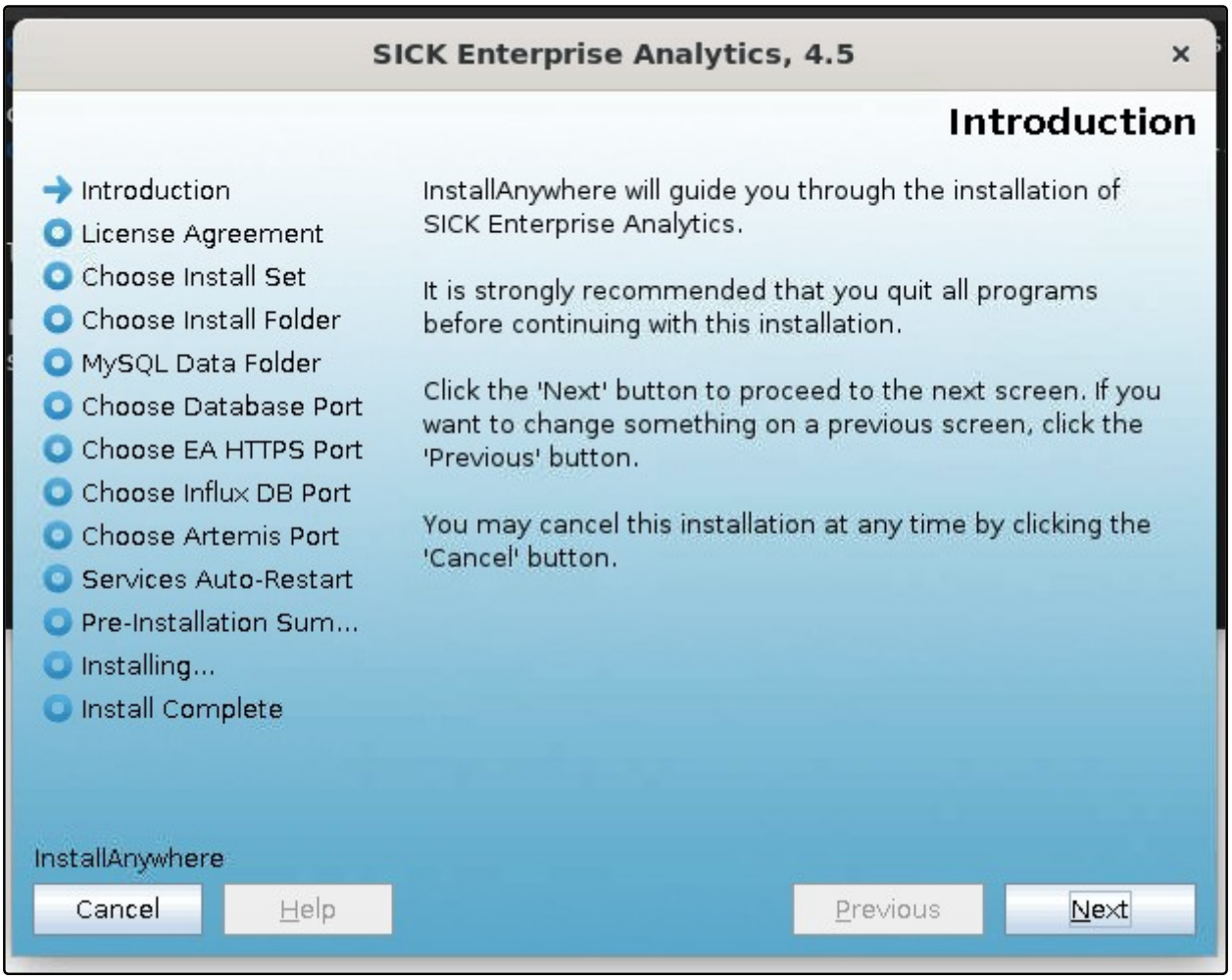


Figure 19

©SICK All rights reserved

3. The **License Agreement** screen appears:
   - Displays the End User License Agreement (EULA).
   - Read the terms and select the checkbox to acknowledge agreement.
   - Click **Next** to proceed.

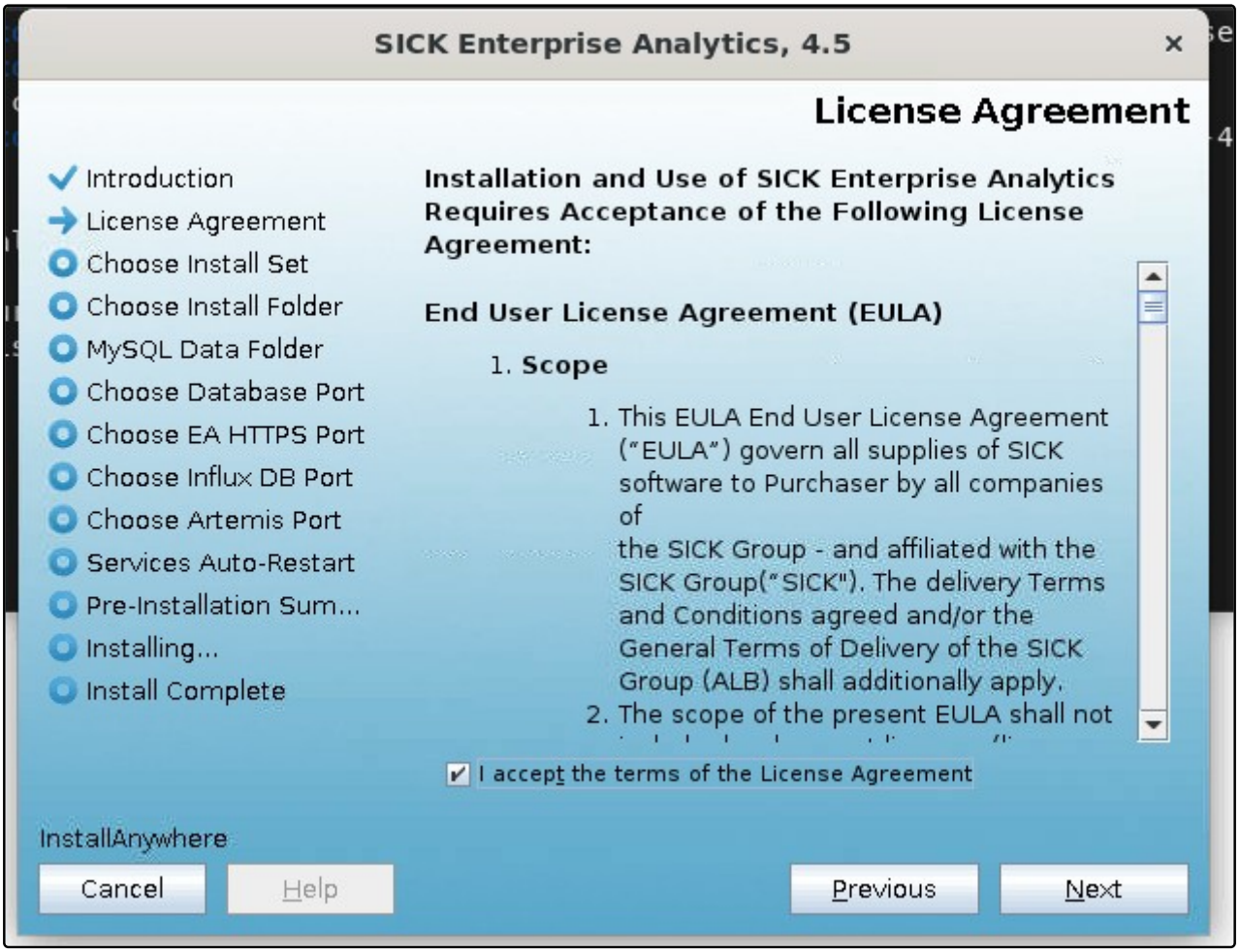


Figure 20

4. The **Choose Install Set** screen appears:
   - **Full**: Installs all EA features.
   - **Custom**: Allows selective installation of components.
   - Click **Next** to proceed.

©SICK All rights reserved

Figure 21

5. The **Choose Install Folder** screen appears:
   - Select the installation directory (for example, `/opt/SICK/EnterpriseApplication`) or provide a custom path.
   - Click **Next** to continue.

©SICK All rights reserved

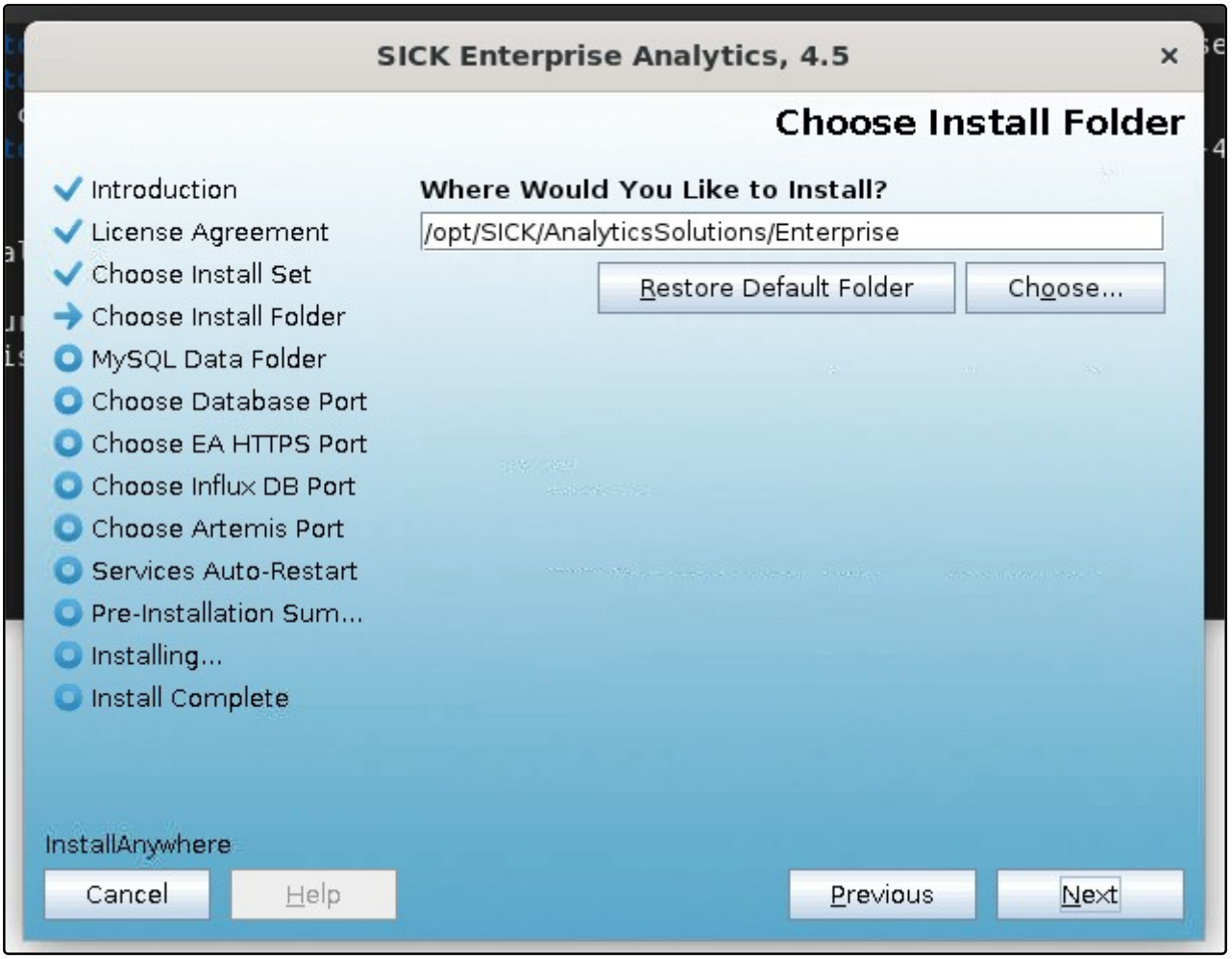


Figure 22

6. The **Specify MySQL Data Folder** screen appears:
   - Choose a folder for MySQL data storage (for example, `/var/lib/mysql`).
   - Click **Next** to proceed.

©SICK All rights reserved

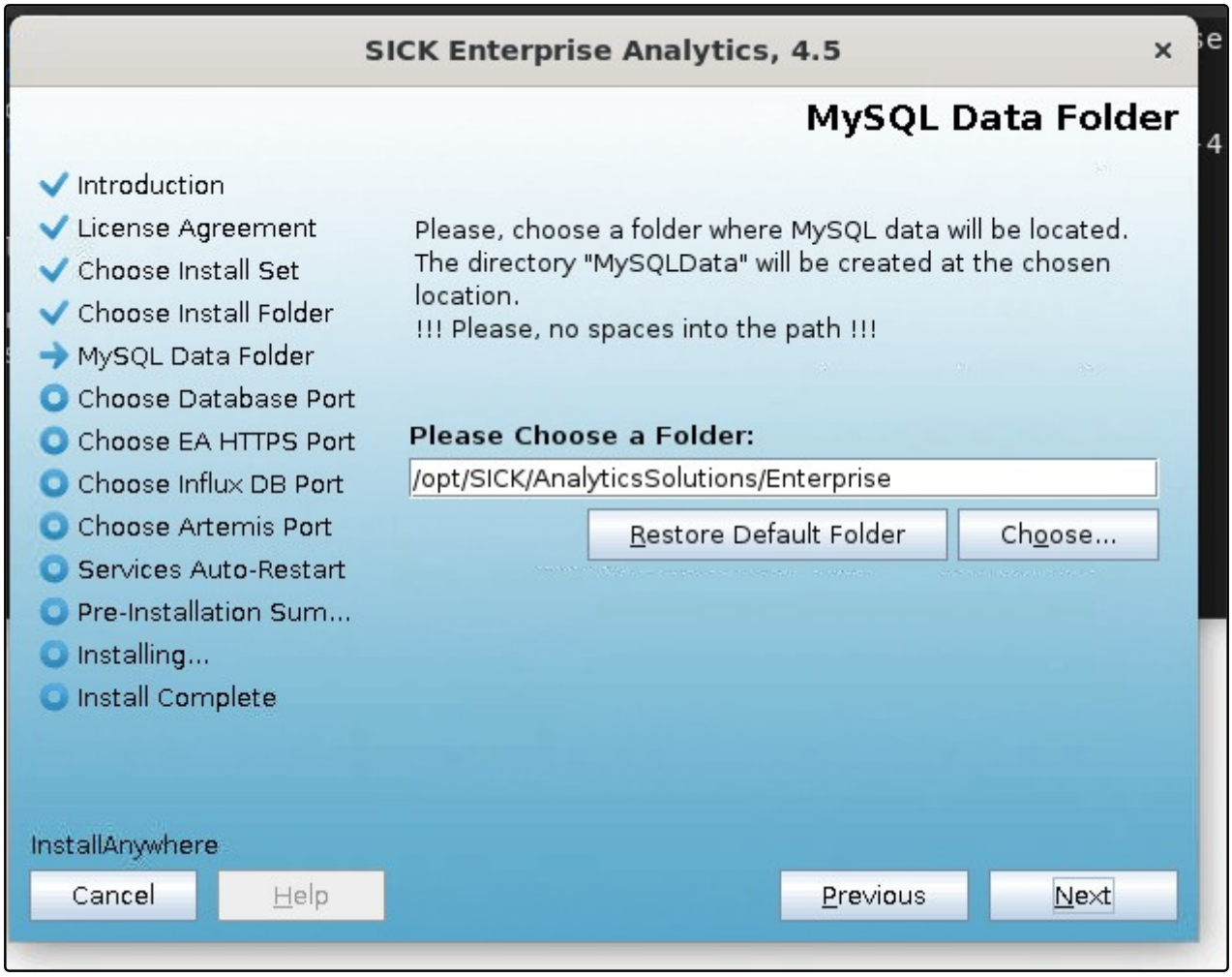


Figure 23

7. The **Pre-Installation Summary** screen appears:
   - Product Name (Enterprise Application 4.5)
   - Install Folder
   - Disk Space (Required & Available)
   - Verify the details and click **Install** to begin.

©SICK All rights reserved

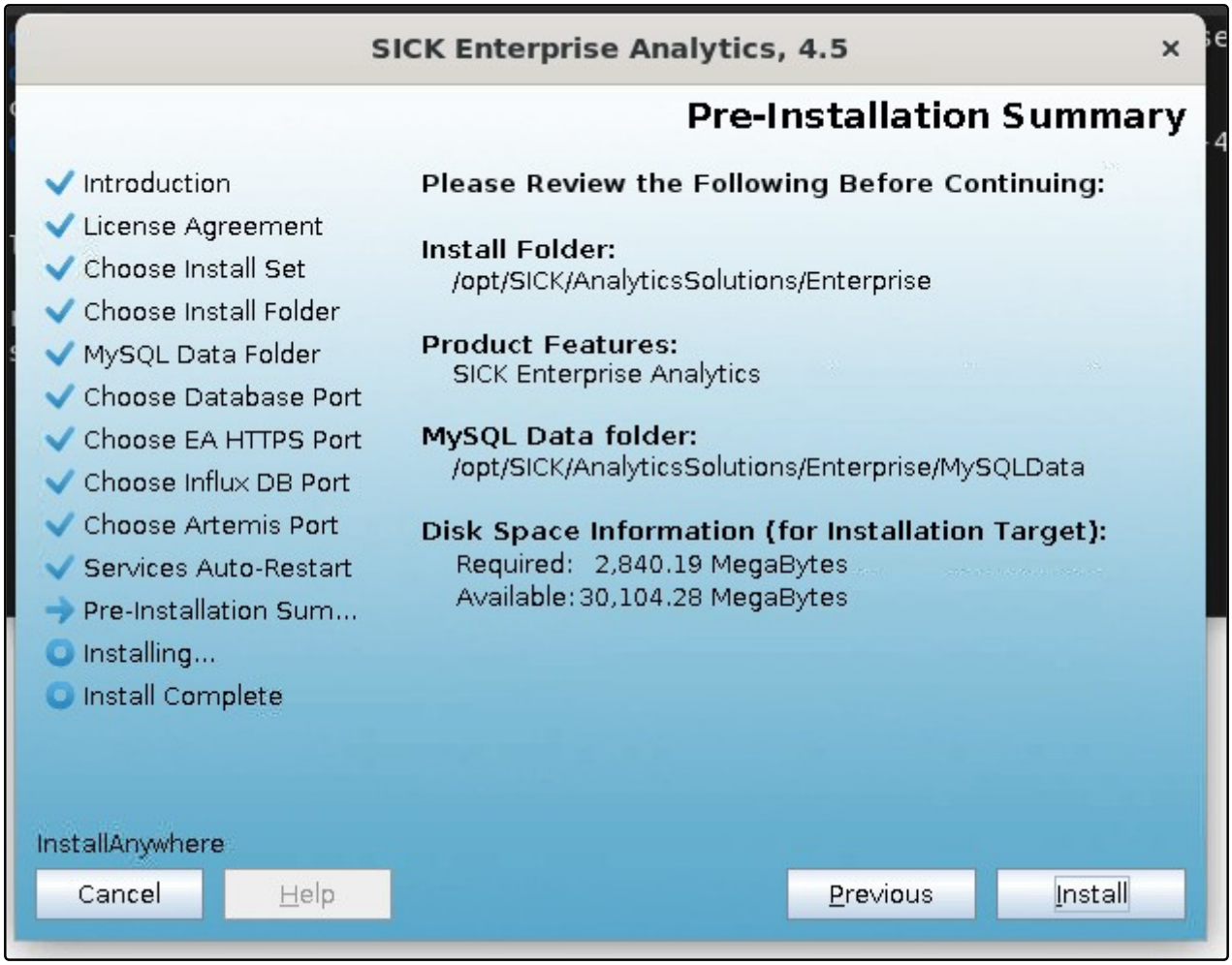


Figure 24

8. The installation begins:
   - The installer copies files and configures services.
   - A progress bar shows the installation status.
   - Wait until it reaches 100%.

©SICK All rights reserved

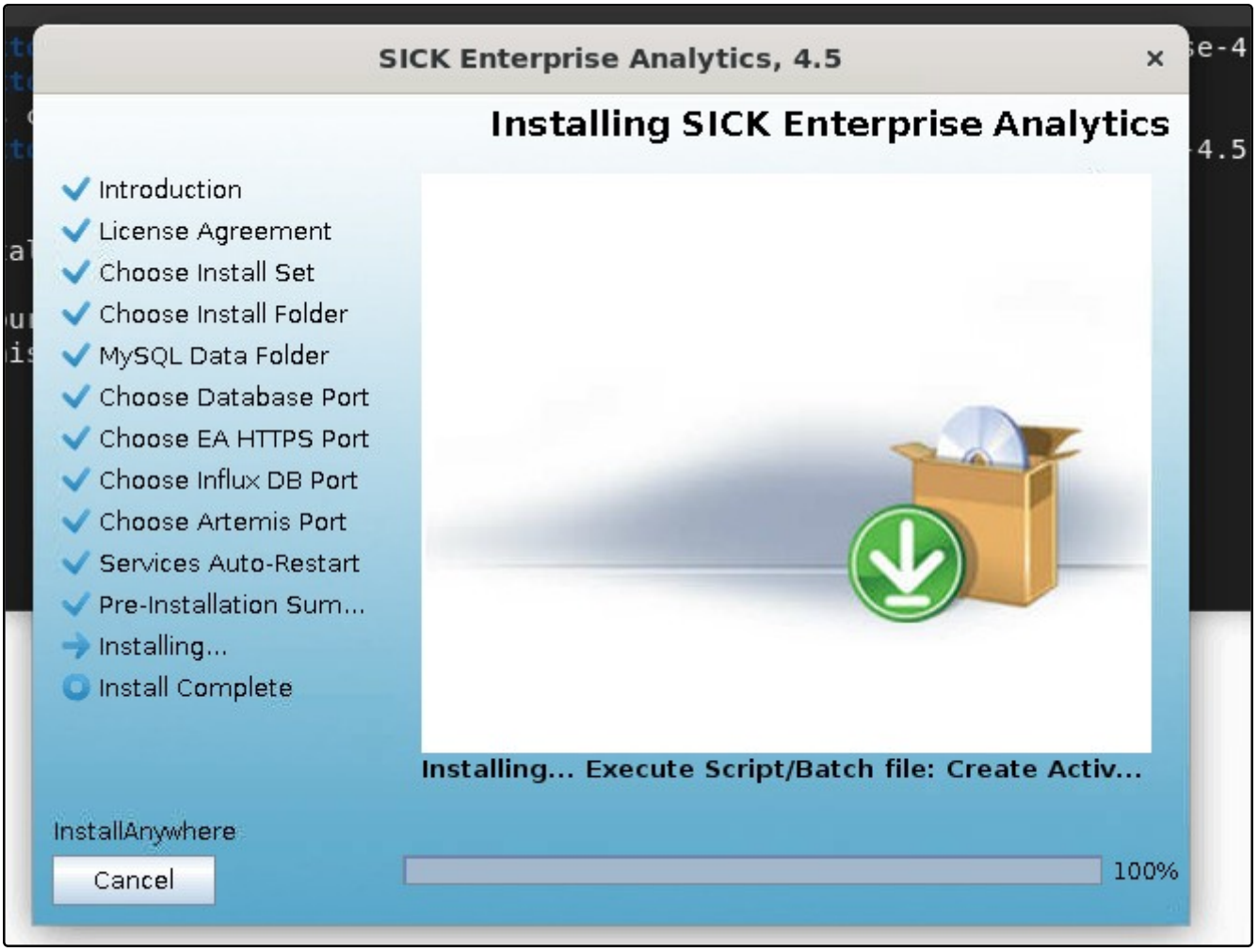


Figure 25

9. The **Install Complete** screen appears:
   - Confirms successful installation of EA.
   - Displays the installation directory for reference.
   - Click **Done** to exit the installer.

©SICK All rights reserved

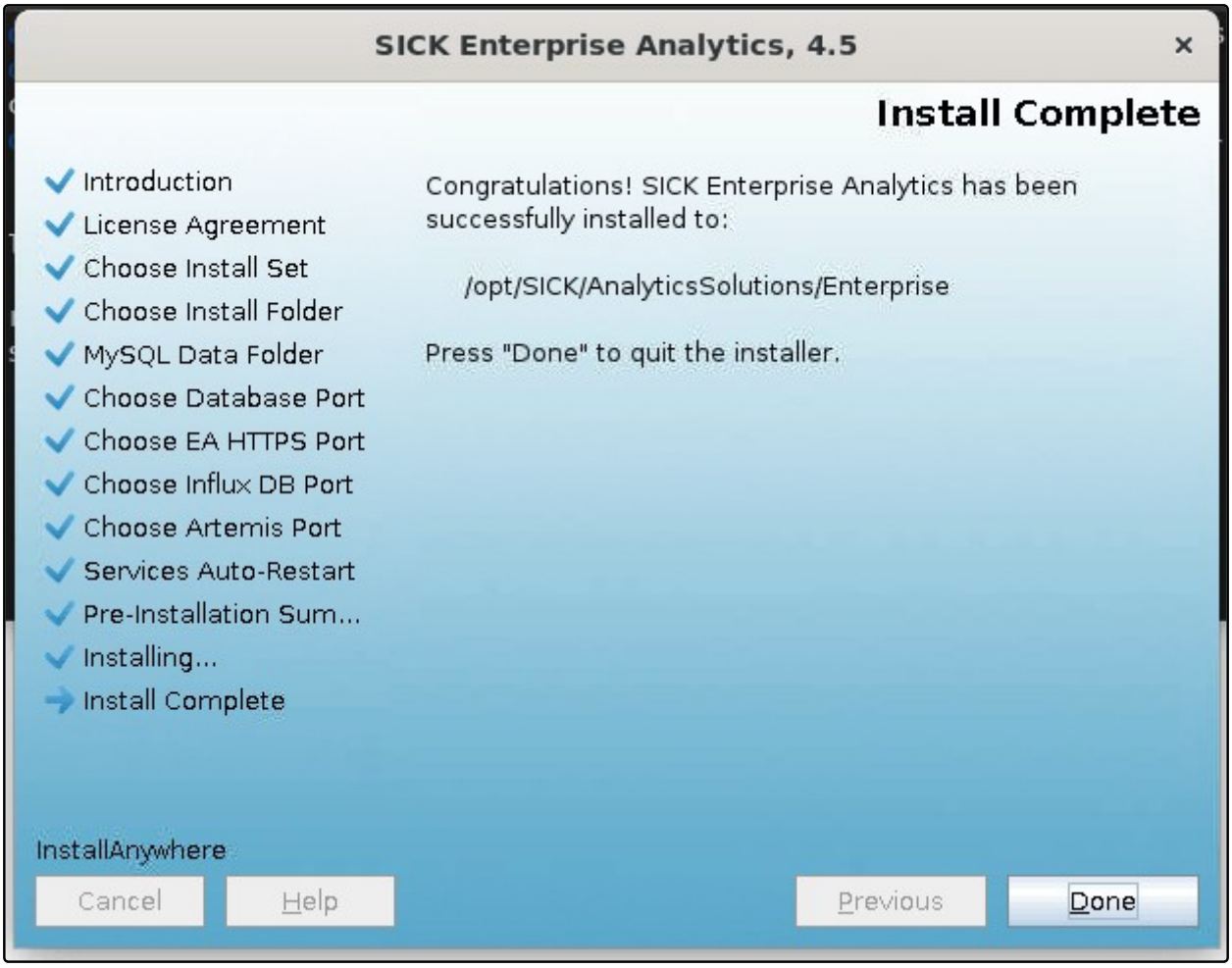


Figure 26

6.3 To Launch the Patch Installer on Windows

This section explains how to apply a software patch to update or fix SICK Enterprise Application (EA).

1. Double-click the patch executable file (for example, **SICK_Enterprise-4.5-Patch.exe**).

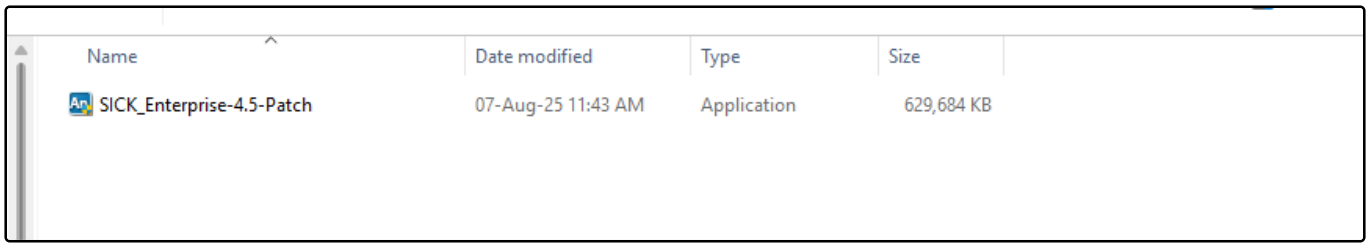


Figure 27

2. The **InstallAnywhere** dialog will be displayed, showing a progress bar as the patch installer prepares.

©SICK All rights reserved

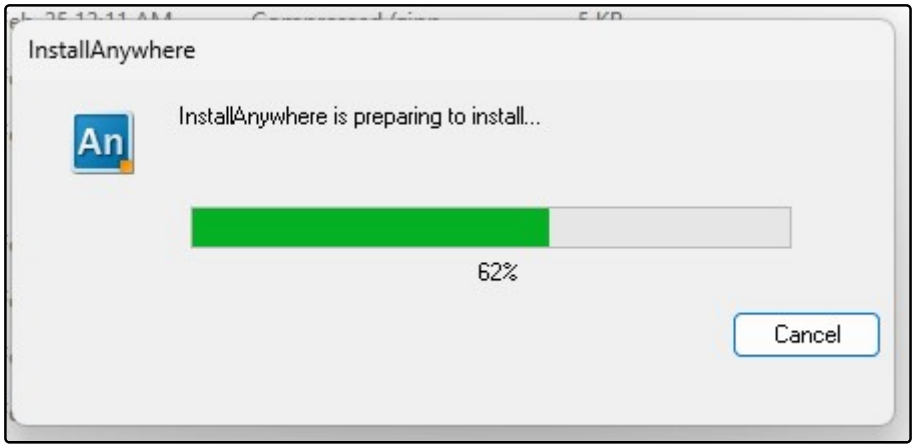


Figure 28

3. Once the progress on the **InstallAnywhere** dialog reaches 100%, the **Patch Installation Wizard** will launch with the **Introduction** screen. Click **Next** to proceed.

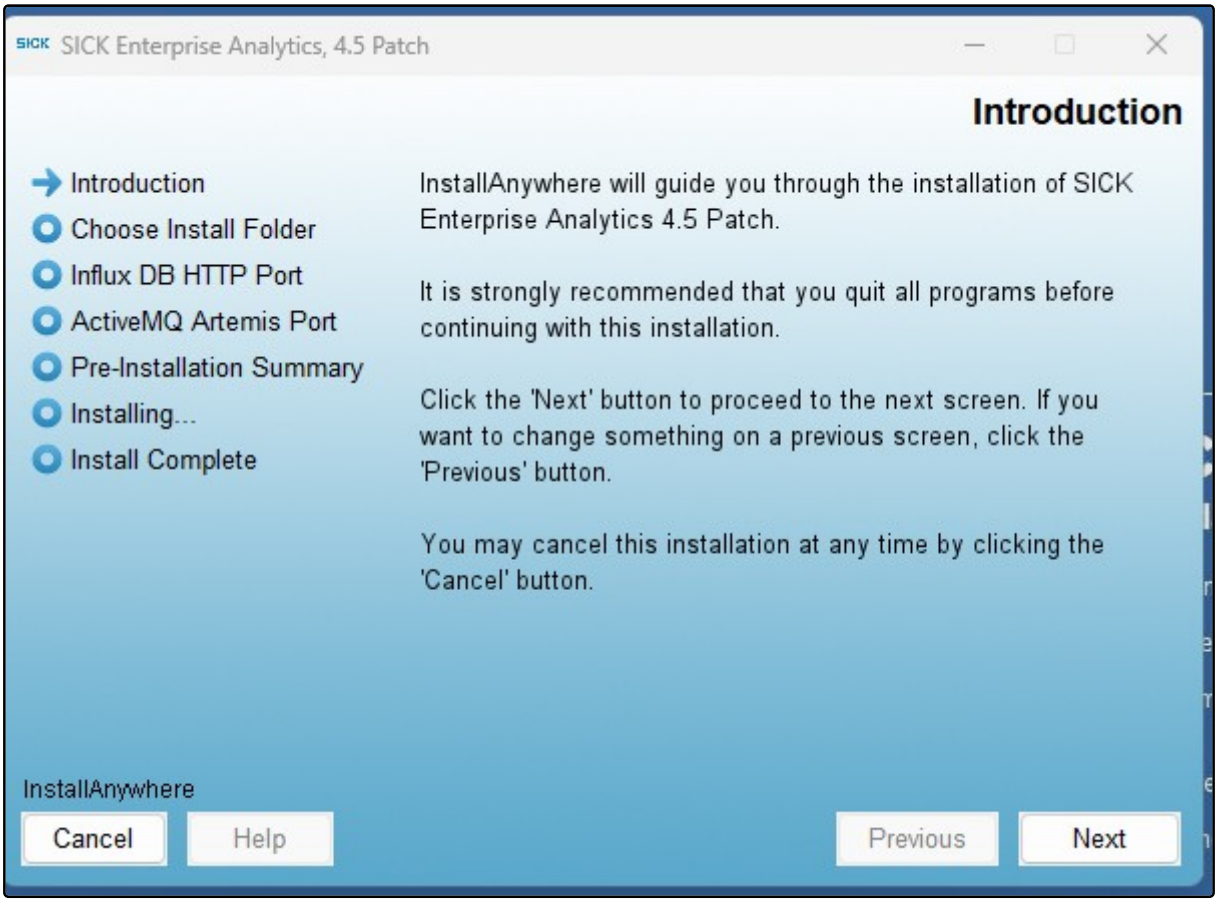


Figure 29

4. The **Pre-Installation Summary** screen appears. Review the following information:
   - Product Name (Enterprise Application 4.5)
   - Install Folder
   - Disk Space Information (Required & Available Space)

   Verify the details and click **Install** to begin.

©SICK All rights reserved

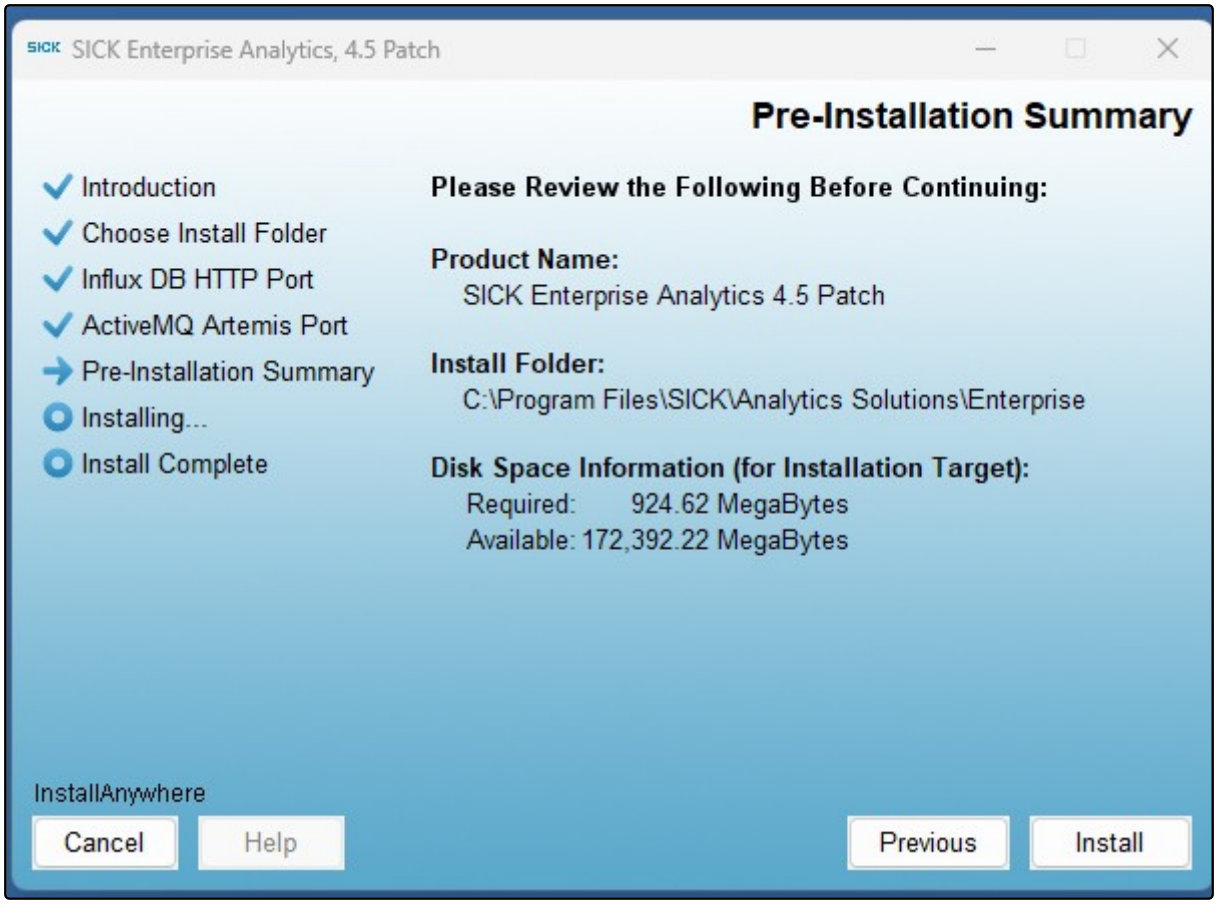


Figure 30

5. The patch installation begins. A progress bar at the bottom of the screen shows the status. JRE and dependent libraries may also be updated if required.

©SICK All rights reserved

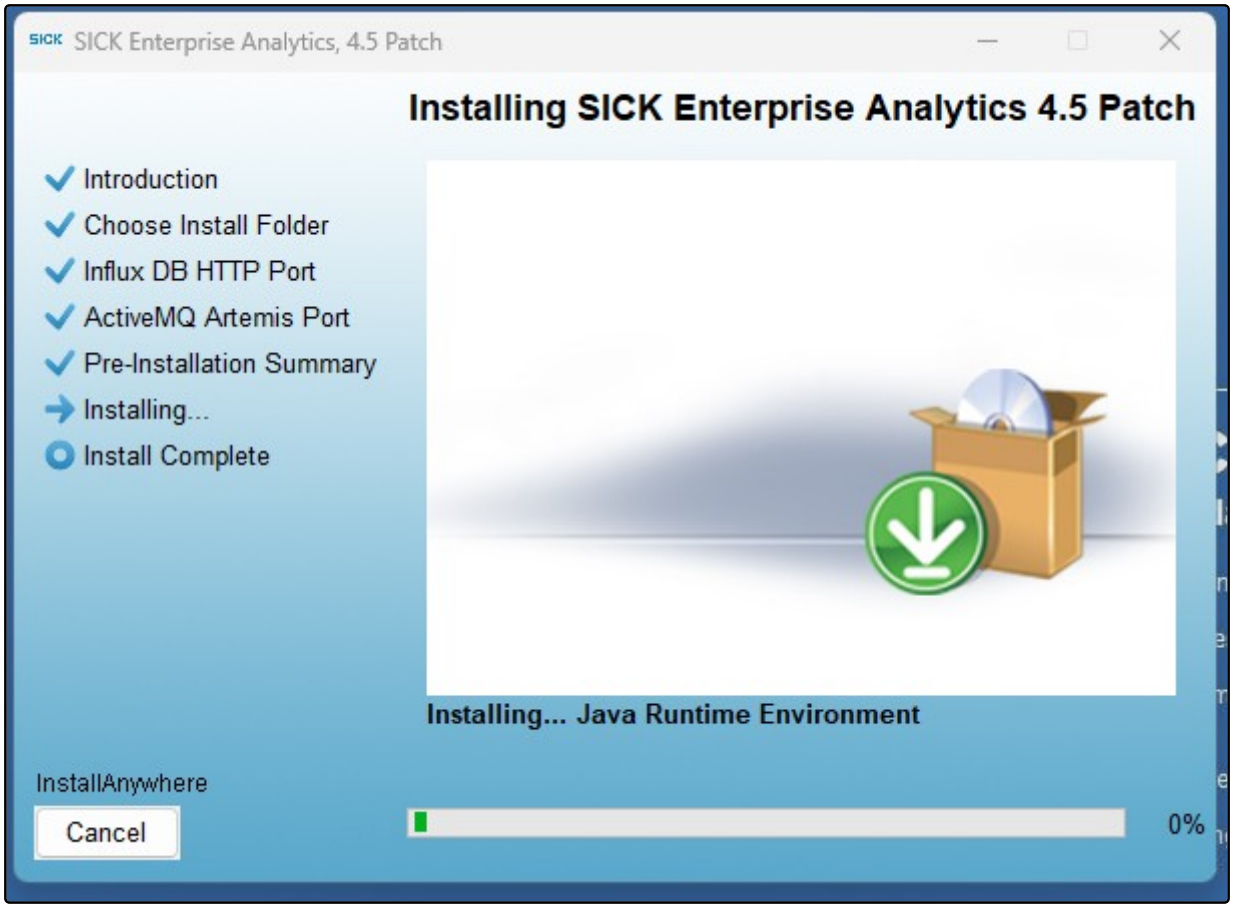


Figure 31

6. Once patch installation is complete, the **Install Complete** screen appears. The installation directory is displayed for reference. Click **Done** to exit the installer.

©SICK All rights reserved

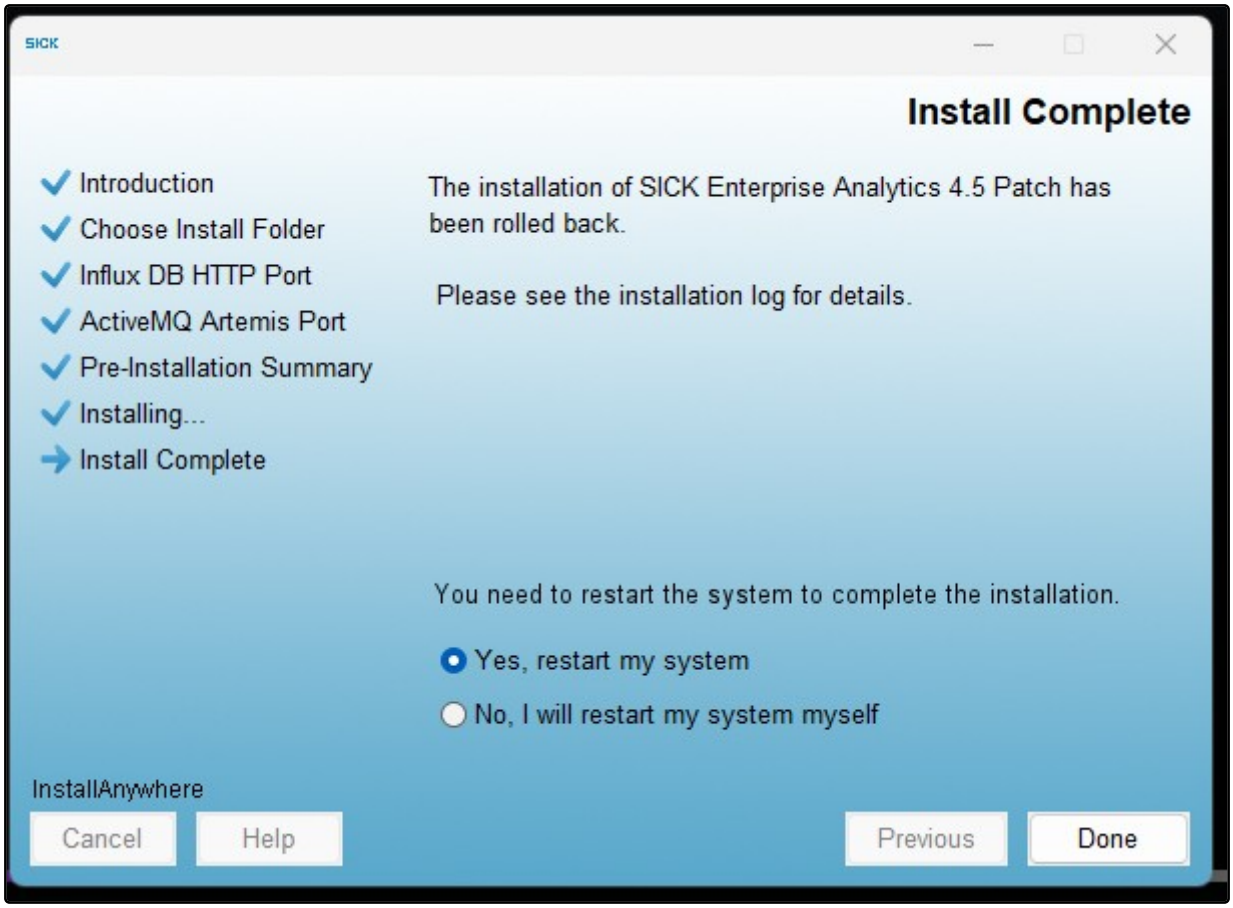


Figure 32

©SICK All rights reserved

6.4 To Uninstall on Windows

1. Open the **Control Panel**.

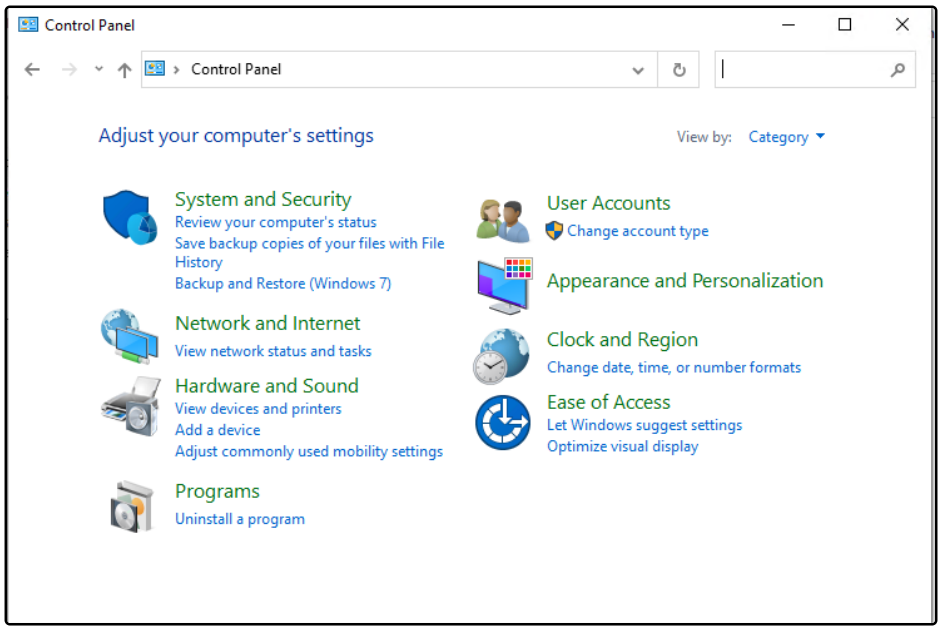


Figure 33

2. Click **Programs**.

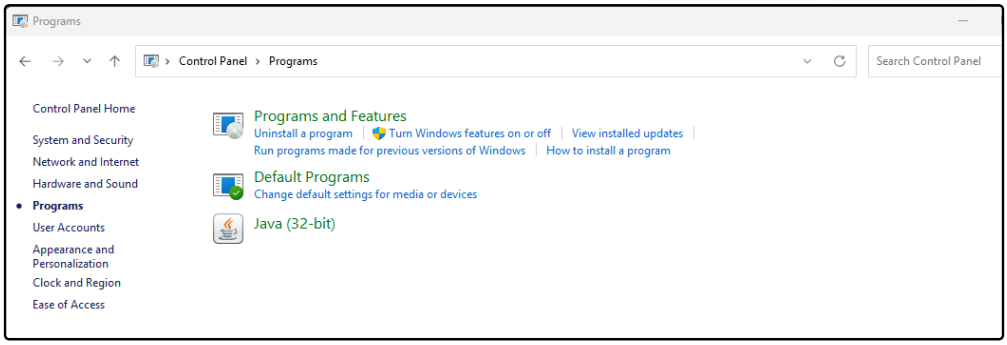


Figure 34

3. Click **Uninstall a Program** under Programs and Features.

©SICK All rights reserved

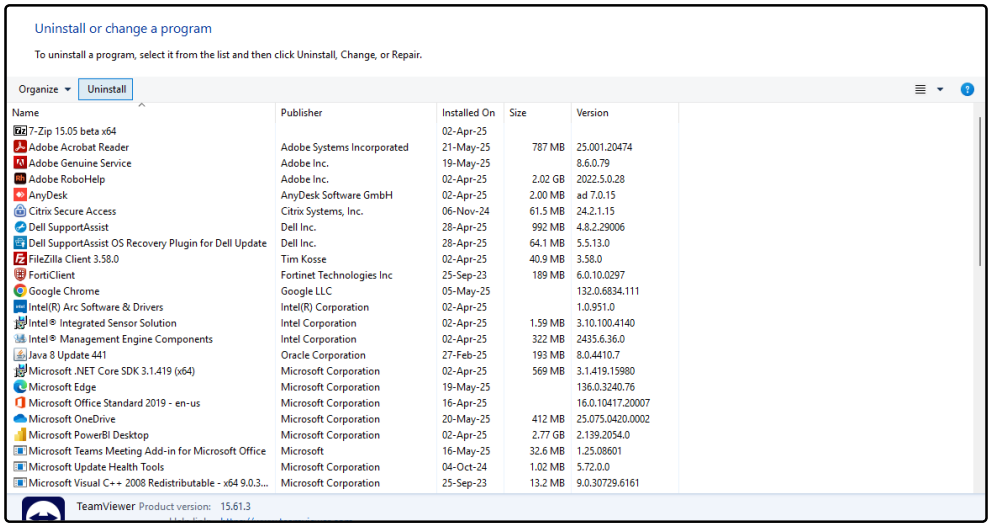


Figure 35

4. Select **SICK Enterprise Analytics** from the list. Click **Uninstall** to launch Maintenance Mode.

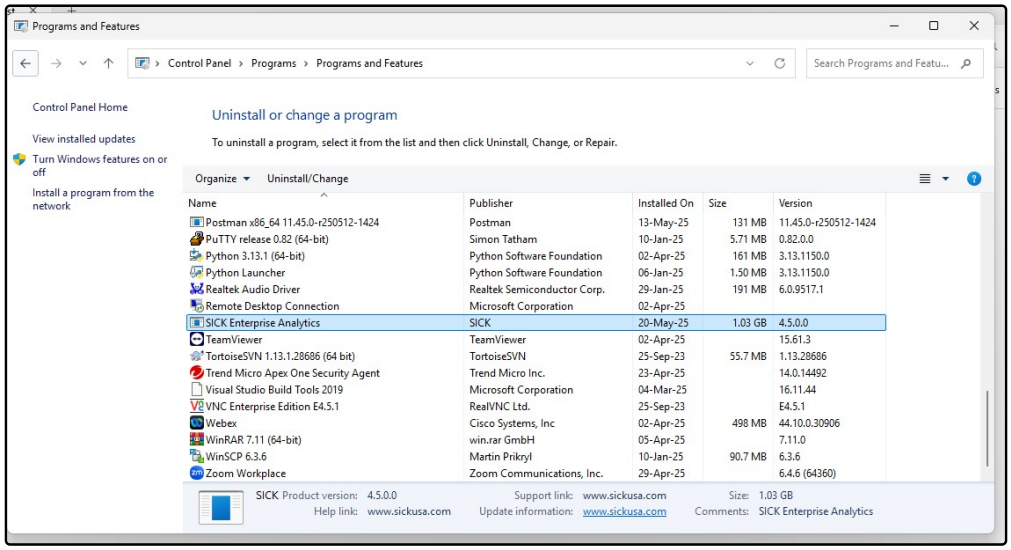


Figure 36

©SICK All rights reserved

5. On the **Maintenance Mode** screen, select **Uninstall Product** and click **Next**.

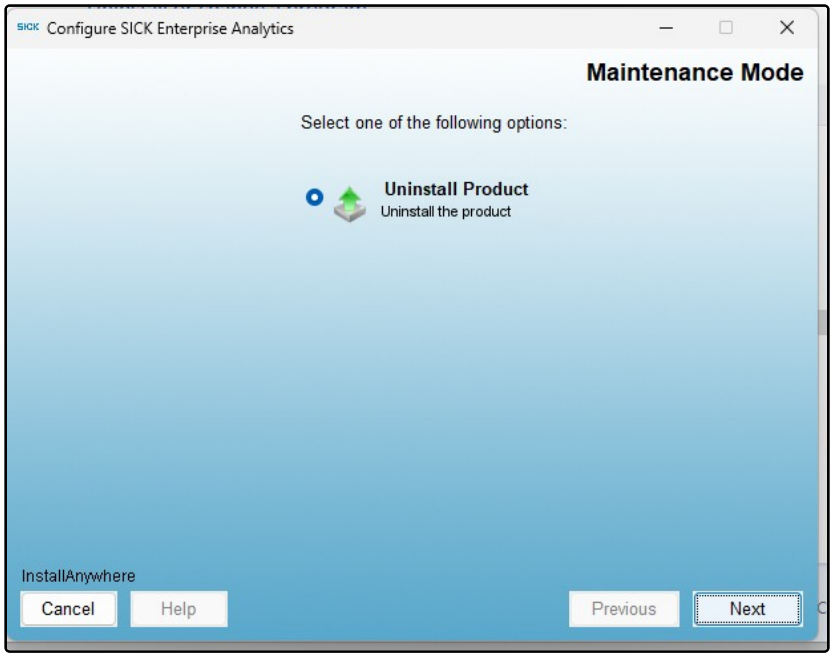


Figure 37

6. On the **Uninstall SICK Enterprise Analytics** screen, a warning will appear stating that the uninstaller will remove features installed by InstallAnywhere but will not remove files and folders created after the installation. Click **UNINSTALL** to proceed, or click **CANCEL** to stop.

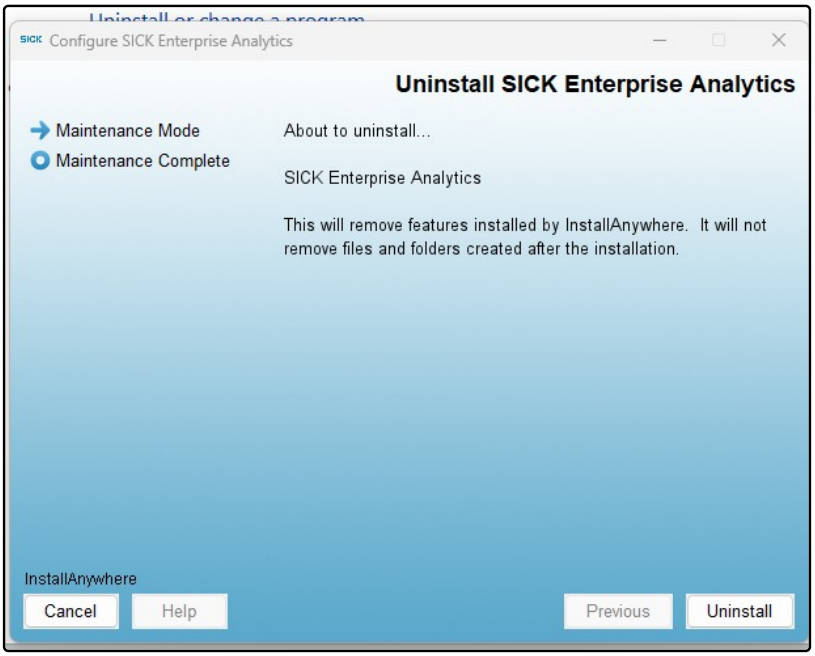


Figure 38

©SICK All rights reserved

7. A progress bar starts at 0%, removing Files, LaunchAnywheres, Shortcuts/Links/Aliases, Registry Entries, Folders, and Others Category. Wait until 100%. Click **Cancel** to stop if needed.

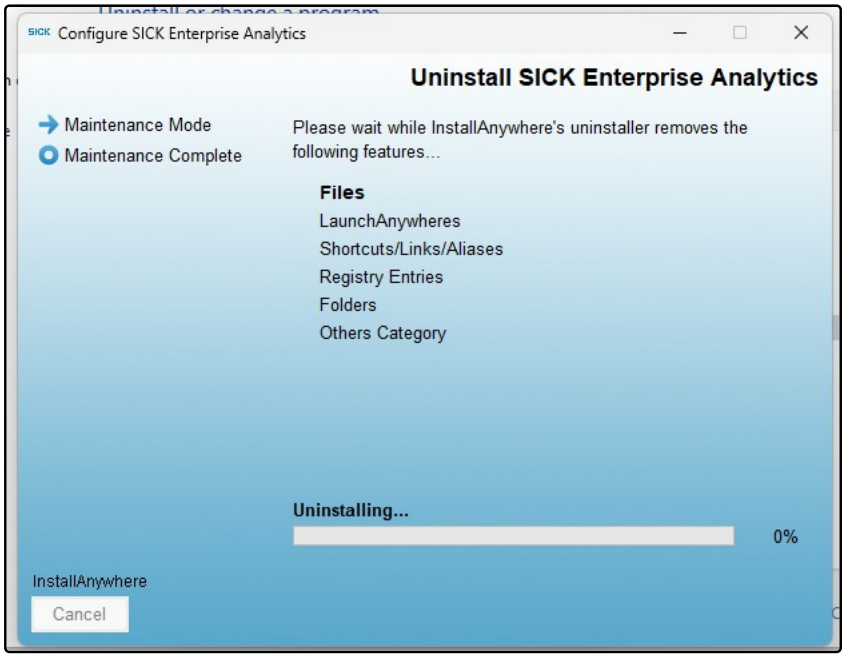


Figure 39

8. The **Uninstall Complete** screen confirms success. Click **Done** to exit.

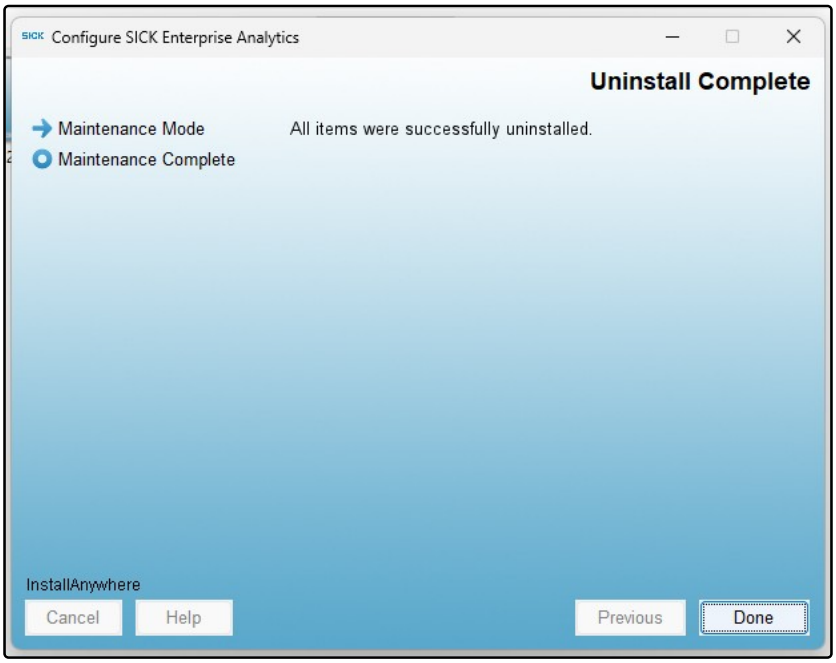


Figure 40

©SICK All rights reserved

7 User and Access Management

This section describes how to configure user accounts, groups, and roles to manage access to the SICK Enterprise Application (EA) Analytics. Authorized administrators can create and manage user accounts, define groups to assign roles, and configure roles with specific privileges to ensure secure access to Analytics data and system functionality. These tasks are performed through the **EA Dashboard**'s administrative interfaces, with actions restricted by role-based privileges.

7.1 Manage Users

The Manage Users interface lets authorized administrators view and manage user accounts. You can create, edit, delete, or reset passwords for user accounts.

Go to Manage Users

1. In the top-right corner of the **EA Dashboard**, select your profile icon SS.

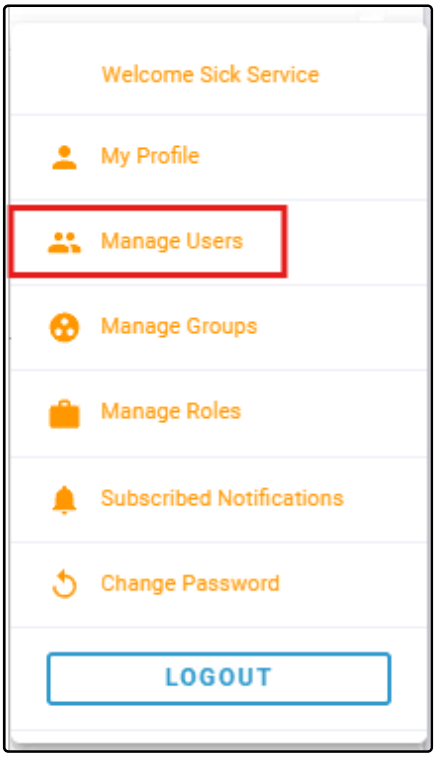


Figure 41

2. From the dropdown menu, select **Manage Users**.

The Manage Users interface opens, showing:

- **User Table** (left panel): A table listing all user accounts.
- **User Details Panel** (right panel): Details and privileges for a selected user.

©SICK All rights reserved

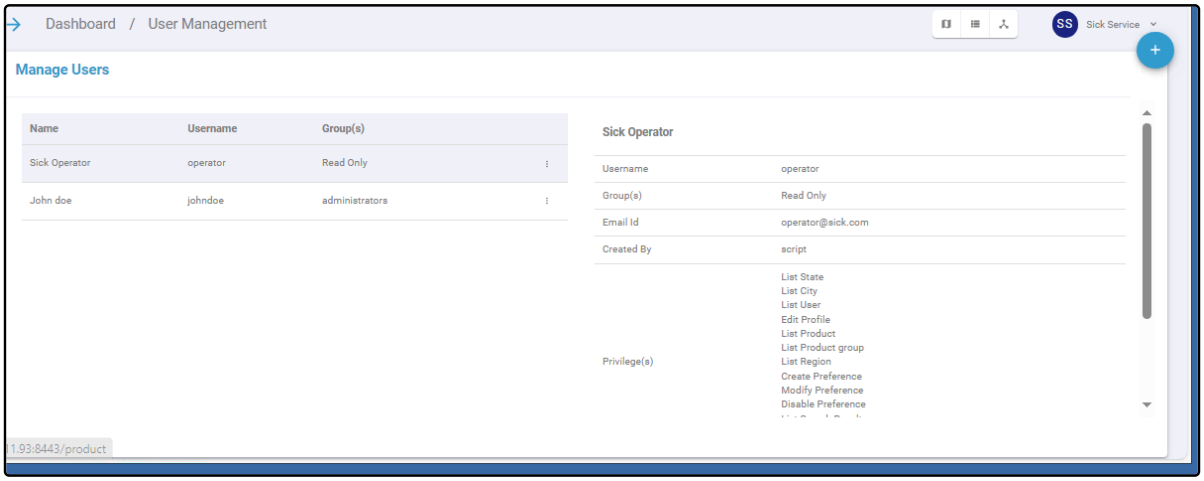


Figure 42

User Table

The table includes these columns:

Column	Description
Name	The user's full name, like John Doe or Sick Operator.
Username	The unique login ID, like johndoe or operator.
Group(s)	The user's assigned role or group, like Administrators or Read Only.
Actions	A menu (⋮) with options to edit, delete, or reset the user's password.

To view a user's details, select their row in the table.

User Details Panel

When you select a user, the right panel shows:

The **Profile Information** section displays key details about the selected user in a table.

©SICK All rights reserved

Field	Description	Example
User-name	The unique identifier the user enters to log in.	johndoe
Group(s)	The role or group assigned to the user, defining their permissions.	Administrators
Email	The email address associated with the user's account.	johndoe@example.com
Created By	The account or service that created the user's profile.	sickservice
Privi-leges	The actions the user is authorized to perform, based on their group. For example, an Administrator might be able to update search queries, create users, reset passwords, etc.	

7.1.1 Add a New User

To add a new user:

1. In the **Manage Users** interface, select the **Add** icon in the upper-right corner of the user table. The **Create User** dialog opens.

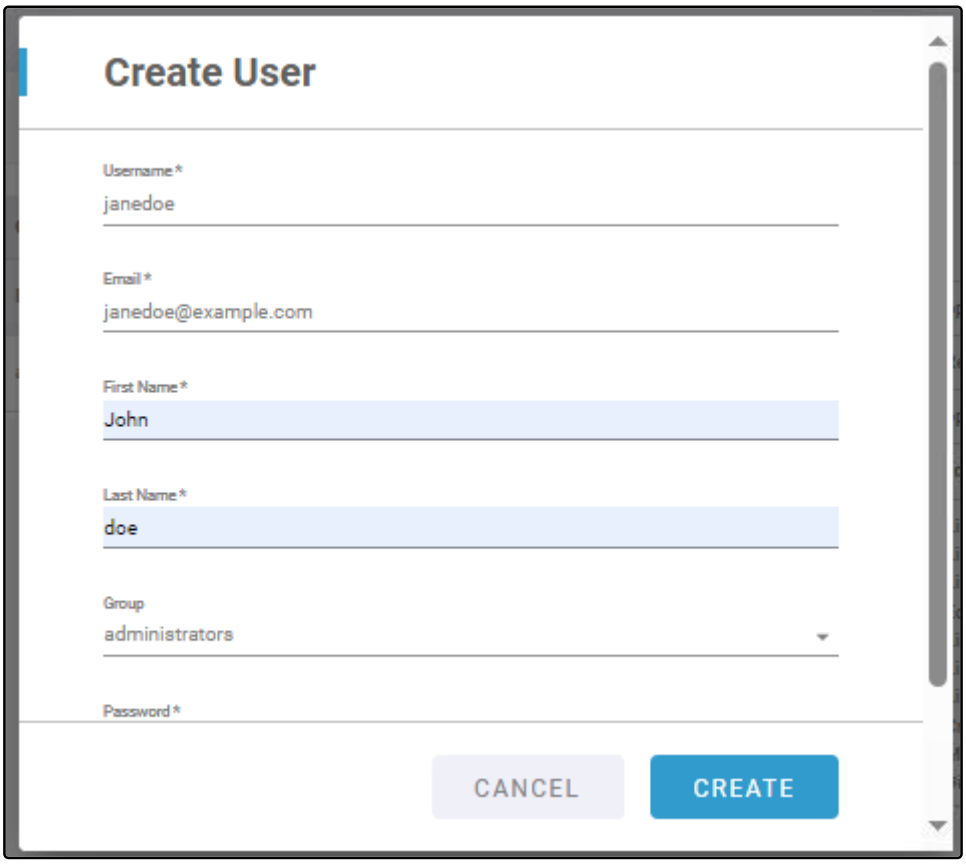


Figure 43

2. In the **Create User** dialog, enter the following details:

©SICK All rights reserved

Field	Example Input
Username	janedoe
Email	janedoe@example.com
First Name	Jane
Last Name	Doe
Password	JaneDoe123
Group	administrators

3. Select **Create** to add the user, or select **Cancel** to discard changes.

4. A snackbar message appears confirming the action—for example:
   "User created successfully."

5. The new user is added to the **User Table**.

7.1.2 Edit a User

To edit an existing user:

1. In the **Manage Users** interface, locate the user you want to update.

2. In the **Actions** column, select the **More options** icon (⋮) for that user.

3. Select the **Edit** option. The **Edit User** dialog opens.

©SICK All rights reserved

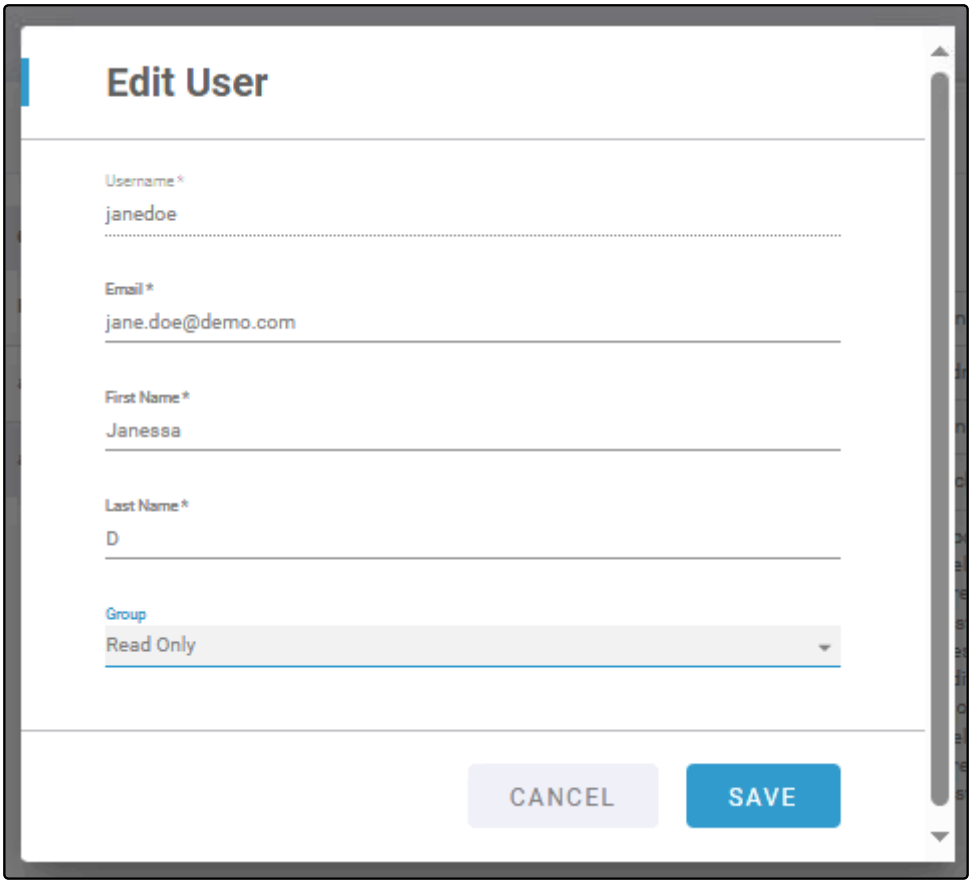


Figure 44

4. Update the **Email**, **First Name**, **Last Name**, and **Group** fields with the new values as required.

> **Note:**
> **Note:** The **Username** field is not editable.

5. Select **Save** to apply changes, or select **Cancel** to discard.

6. A snackbar message appears confirming the update—for example:
   "User updated successfully."

7.1.3 Delete a User

To delete an existing user:

1. In the **Manage Users** interface, locate the user you want to remove—for example, janedoe.

2. In the **Actions** column, select the **More options** icon (⋮) for that user.

3. Select **Delete** from the dropdown menu.
   A confirmation dialog appears.

©SICK All rights reserved

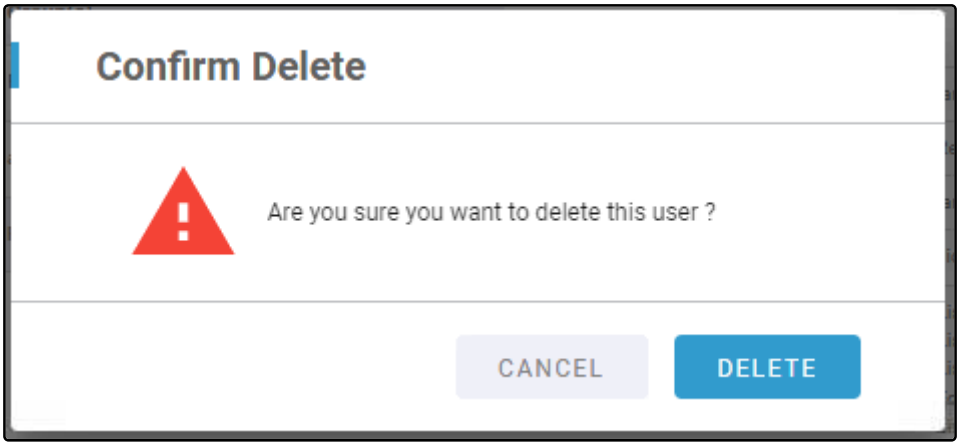


Figure 45

4. In the confirmation dialog, select **Delete** to permanently remove the user, or select **Cancel** to return without deleting.

5. A snackbar message appears confirming the action—for example:
   "User deleted successfully."
   An **Undo** option may also be available to restore the user.

7.1.4 Reset a User's Password

To reset the password for an existing user:

1. In the **Manage Users** interface, locate the user whose password you want to reset—for example, janedoe.

2. In the **Actions** column, select the **More options icon (⋮)**.

3. Select **Reset Password** from the dropdown menu. The **Reset Password** dialog opens.

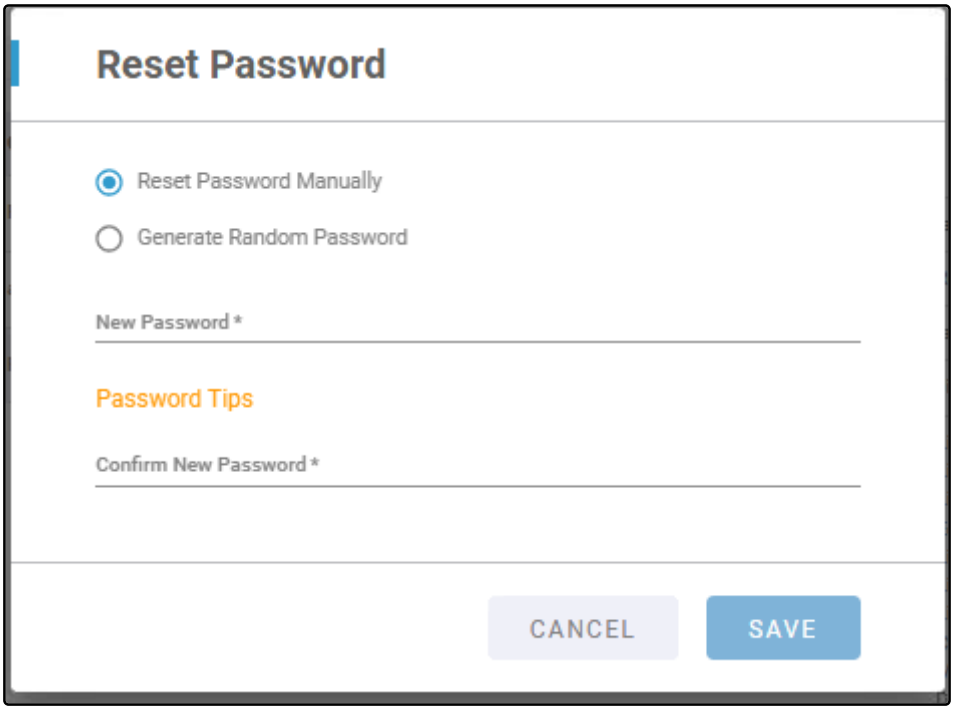


Figure 46

©SICK All rights reserved

4. Choose one of the following options:

- **Reset Password Manually:** Enter a new password and confirm it.
- **Generate Random Password:** The system creates a secure password automatically.

7.2 Manage Groups

The Manage Groups interface lets administrators view and manage user groups. Groups define access by assigning roles and privileges to users. Each user must belong to one group.

Go to Manage Groups

1. In the top-right corner of the EA Dashboard, click your profile icon SS.

2. From the dropdown menu, select **Manage Groups**.

The Manage Groups interface opens, showing:

- **Group Table** (left panel): A table listing all user groups.
- **Group Details Panel** (right panel): Detailed information and privileges for the selected group.

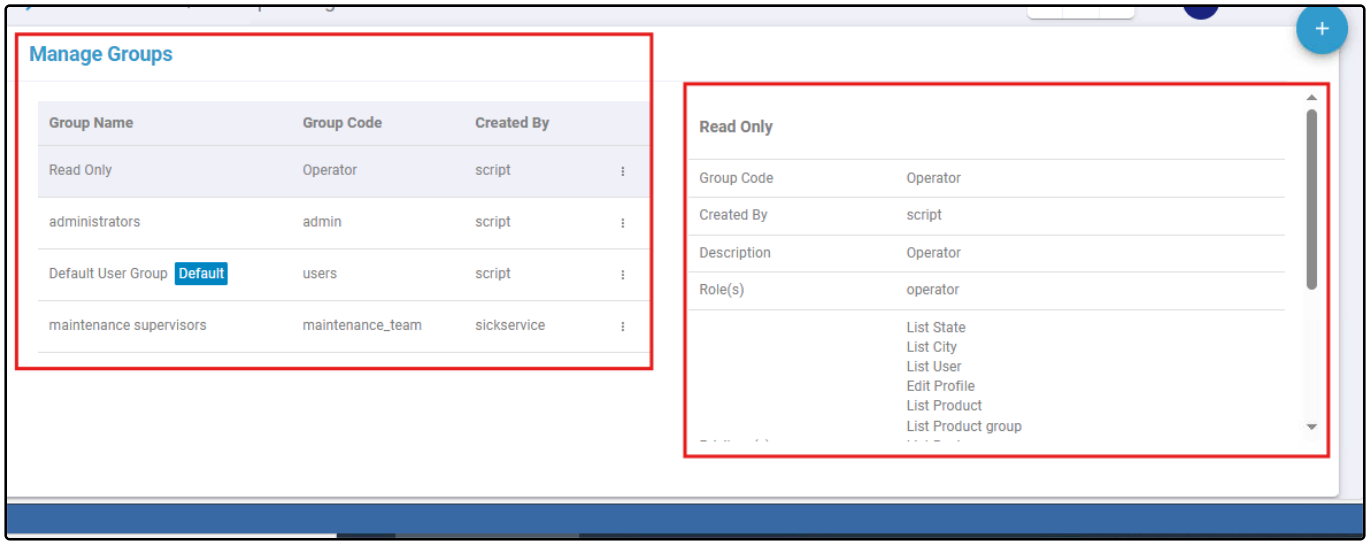


Figure 47

Group Table

The table includes these columns:

Column	Description
Group Name	The name of the group, such as **Read Only** or **Administrators**.
Group Code	A unique identifier for the group, such as **Operator** or **admin**.
Created By	The user or service that created the group, such as **script**.
Actions	A menu (⋮) with options to **Edit**, **Delete**, or **Set Default**.

To view a group's details, select its row in the table.

Group Details Panel

©SICK All rights reserved

When you select a group, the right panel displays key information and associated privileges for that group.

Field	Description	Example
Group Code	The unique identifier used internally for the group.	**Operator**
Created By	The account or service that created the group.	**script**
Description	A brief summary of the group's purpose or function.	**Operator**
Role(s)	The role assigned to the group, which determines user access.	**operator**
Privileges	The actions users in the group are authorized to perform, based on their role. For example, the **Operator** group may have the following privileges: List State, List City, List User, Edit Profile, List Product, List Product Group, List Region, Create Preference, Modify Preference, Disable Preference	

7.2.1 Add a New Group

Use the **Create Group** dialog to define a new user group. Groups control which users have access to specific roles and privileges, such as equipment monitoring, maintenance management, or production reporting.

1. In the **Manage Groups** interface, select the **Add** icon  in the top-right corner.
   The **Create Group** dialog appears.

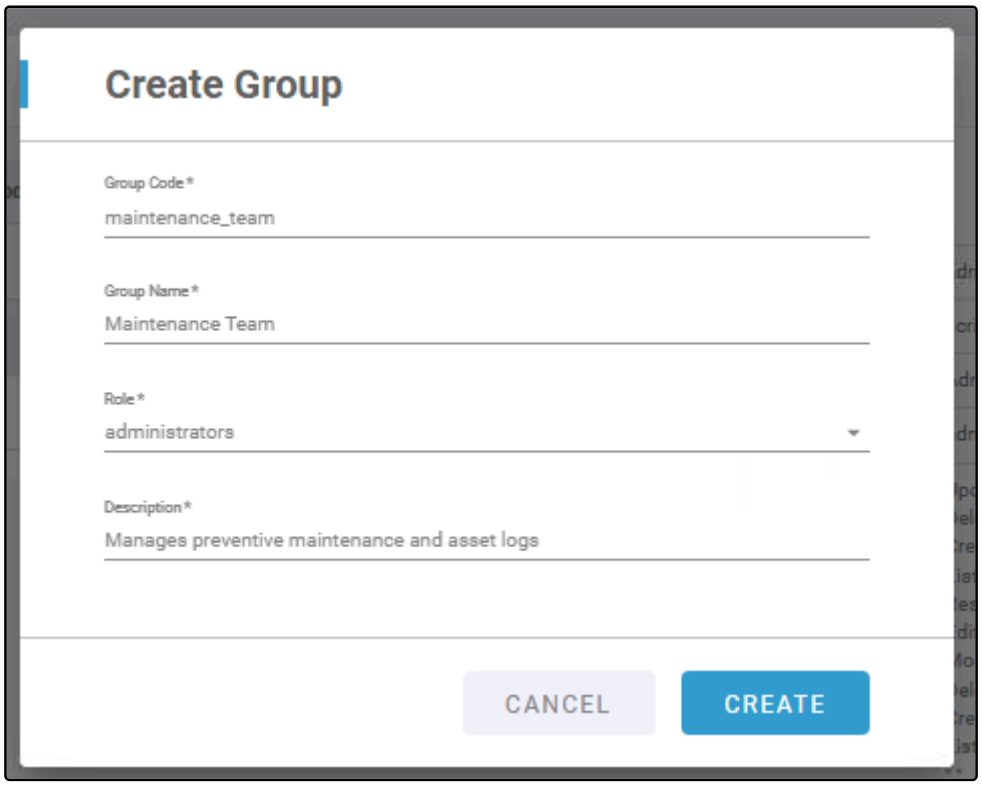


Figure 48

2. Fill in the required fields:

©SICK All rights reserved

Field	Description	Example Input
Group Code	Unique system-friendly identifier (use lowercase and underscores).	maintenance_team
Group Name	Display name that users will see.	Maintenance Team
Role	The role to assign to the group (choose from the existing list).	administrators
Description	A short explanation of the group's responsibilities.	Manages preventive maintenance and asset logs

1. Select **Create** to add the group or **Cancel** to close the dialog without saving.

2. A snackbar message confirms the result:
   "Group created successfully."

3. The new group now appears in the **Group Table**, and its details are available in the **Group Details Panel**.

7.2.2 Edit a Group

You can edit the name, role, and description of an existing group. The group code is fixed and cannot be changed.

1. In the **Manage Groups** interface, locate the group you want to update—for example, maintenance team.

2. In the **Actions** column, select the **More options** icon (⋮) next to the group.

3. Select the **Edit** option. The **Edit Group** dialog opens.

©SICK All rights reserved

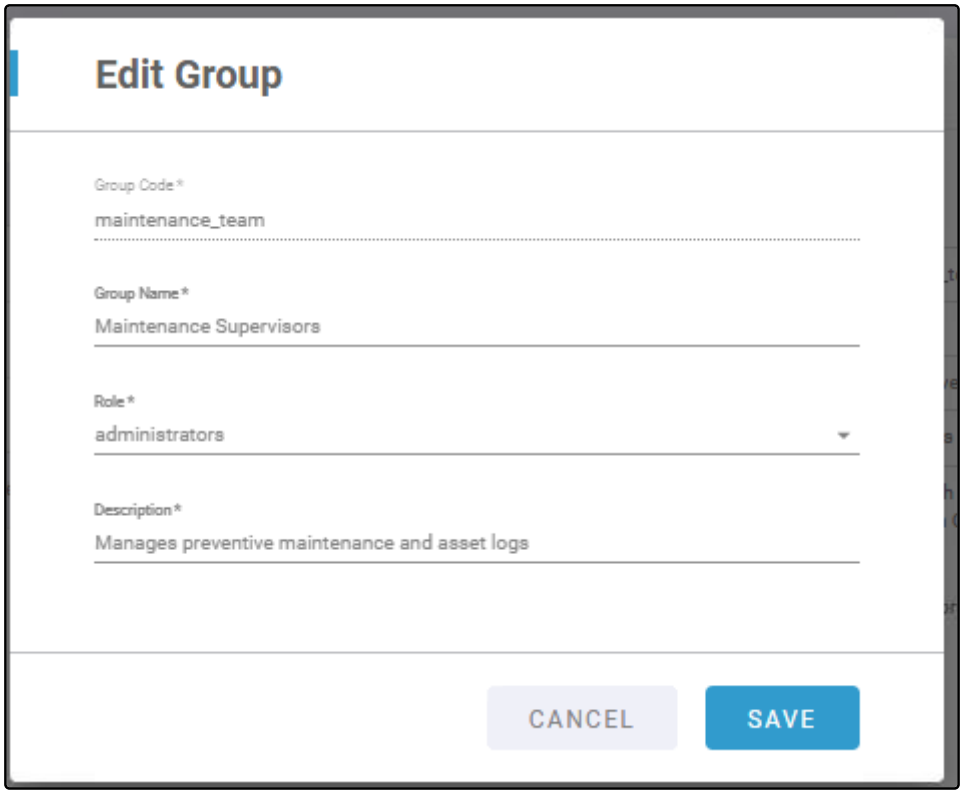


Figure 49

4. Update the **Group Name**, **Role**, and **Description** fields with the new values as required.

> **Note:**
> **Note:** The **Group Code** field is not editable.

5. Select **Save** to apply the changes or **Cancel** to discard them.

6. A snackbar message appears confirming the update:
   “Group updated successfully.” An **Undo** link may be shown to revert the changes.

7.2.3 Delete a Group

You can delete a group if it is not set as the default and is not assigned to any active users.

1. In the **Manage Groups** interface, locate the group you want to delete—for example, maintenance team.

2. In the **Actions** column, select the **More options** icon (⋮) next to the group.

3. Select **Delete** from the menu.
   A confirmation dialog appears.

©SICK All rights reserved

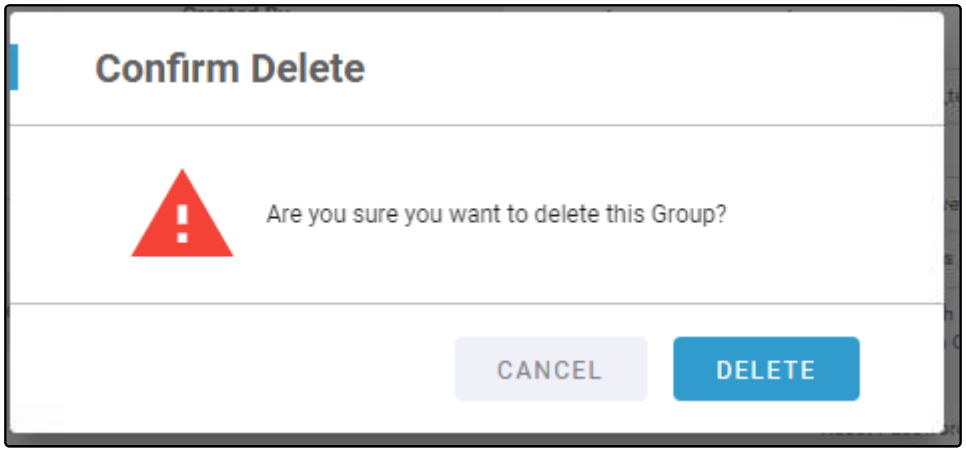


Figure 50

4. Select **Delete** to confirm the deletion, or **Cancel** to abort.

7.2.4 Set a Group as Default

You can set a group as the default to automatically assign it to new LDAP users or system-created accounts. Only one group can be the default at a time.

1. In the **Manage Groups** interface, locate the group you want to set as default—for example, maintenance team.

2. In the **Actions** column, select the **More options** icon (⋮) next to the group.

3. Select **Set Default** from the menu. The group is now marked as the default.

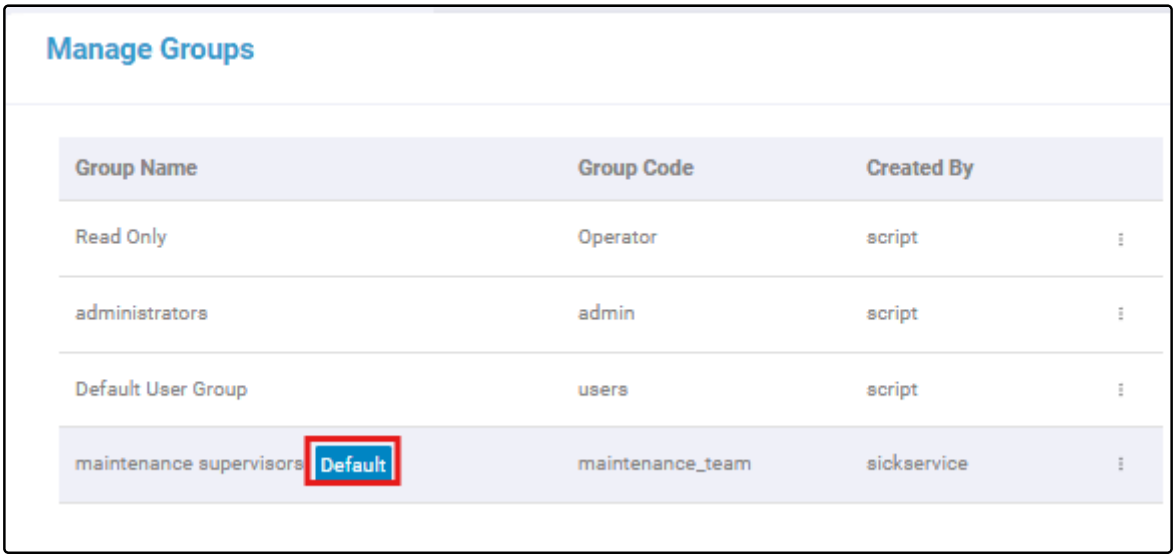


Figure 51

7.3 Manage Roles

Roles define collections of privileges that are assigned to groups. These privileges control what actions users within a group can perform. Common system roles include operator, users, and administrators.

Go to Manage Roles

©SICK All rights reserved

1. In the top-right corner of the **EA Dashboard**, click your profile icon 

.

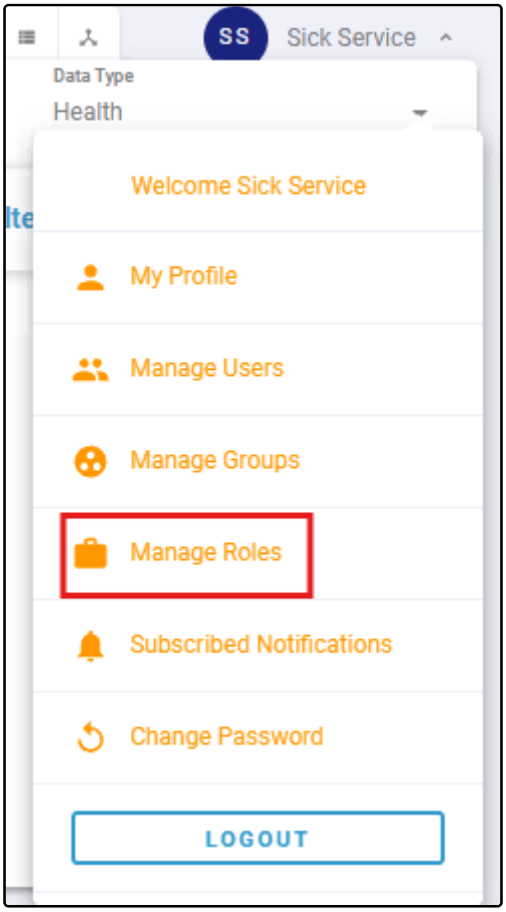


Figure 52

2. From the dropdown menu. Select **Manage Roles**.

The **Manage Roles** interface opens, displaying:

- **Role Table** (left panel): A list of existing roles.
- **Role Details Panel** (right panel): Details and privileges for a selected role.

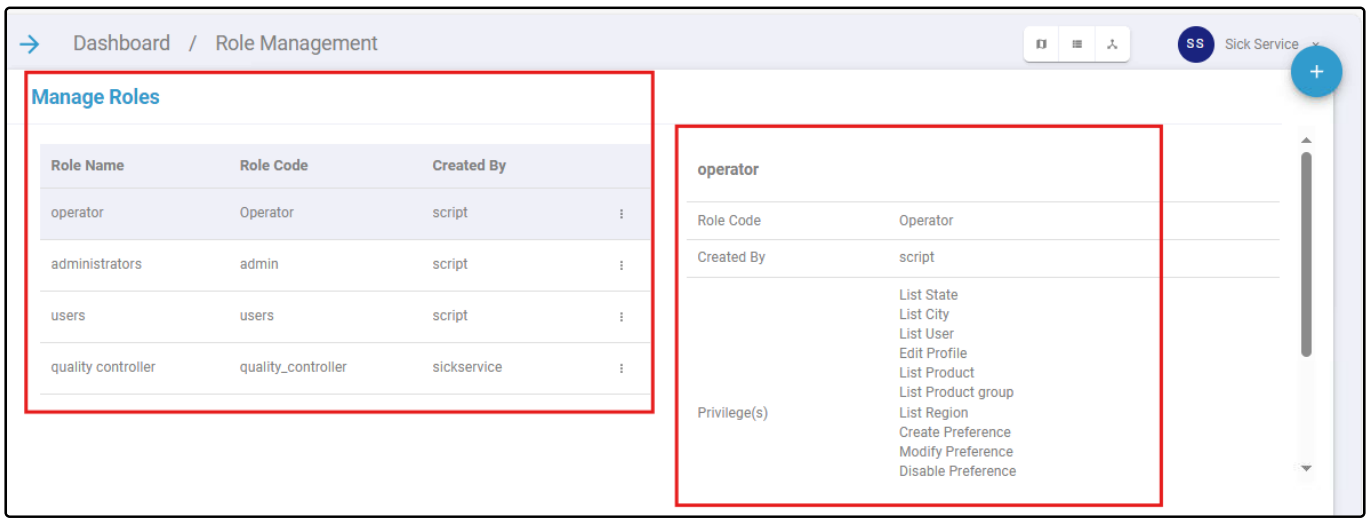


Figure 53

Role Table

©SICK All rights reserved

Column	Description
Role Name	Display name of the role (e.g., operator, users).
Role Code	Unique internal code used to reference the role.
Created By	The account or system process that created the role.
Actions	A menu (⋮) to edit or delete the role.

Role Details Panel

When a role is selected from the table, its details are displayed on the right.

Field	Description	Example
Role Code	Unique system identifier for the role.	Operator
Created By	The account that created the role.	script
Privilege(s)	List of actions users with this role can perform.	List State, List City, List User, Edit Profile, List Product, List Product Group, List Region, Create Preference, Modify Preference, Disable Preference, List Search Result, Download Search Result, List Country

7.3.1 Add a New Role

Use the **Create Role** dialog to define a custom role and assign specific privileges. Roles control what actions users in corresponding groups can perform.

1. In the **Manage Roles** interface, select the **Add** icon: 
   The **Create Role** dialog opens.

©SICK All rights reserved

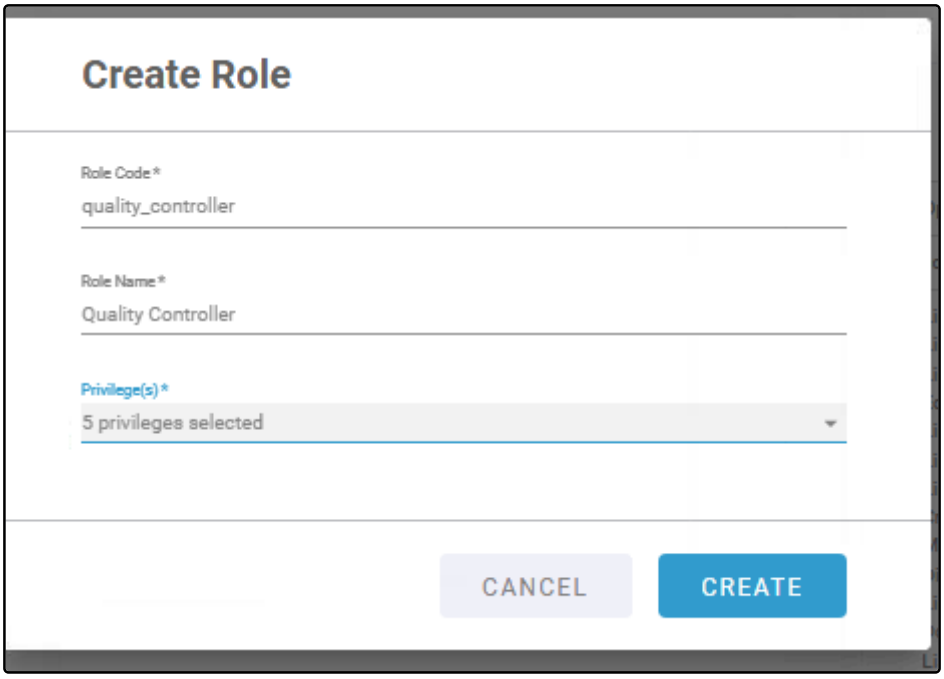


Figure 54

2. In the **Create Role** dialog, enter the following details:

Field	Description	Example Input
Role Code	A unique identifier used internally by the system (no spaces or capitals).	quality_controller
Role Name	The display name of the role shown in the UI.	Quality Controller
Privilege(s)	Select from the available privileges list.	5 privileges selected: • Delete Global Preference • Create Global Preference • List State • Download log files • Delete Role

3. Select **Create** to save the role, or **Cancel** to discard the changes.

4. A snackbar message appears:
   "Role created successfully."

5. The new role appears in the **Roles Table**, and its full set of privileges is shown in the **Role Details Panel** when selected.

7.3.2 Edit a Role

You can update the name and privileges of an existing role. The Role Code is fixed and cannot be changed.

©SICK All rights reserved

1. In the **Manage Roles** interface, locate the role you want to update—for example, **quality_controller**.
2. In the **Actions** column, select the **More options** icon (⋮) next to the role.
3. Select the **Edit** option. The **Edit Role** dialog opens.

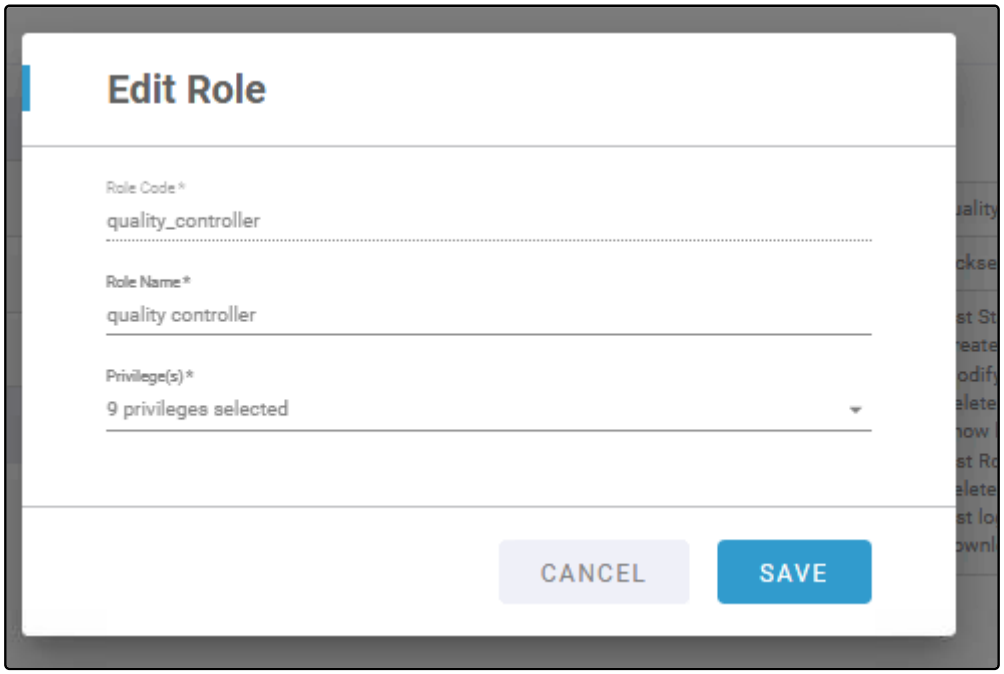


Figure 55

4. Update the **Role Name** and **Privileges** fields with the new values as required.

> Note:
> The **Role Code** field is not editable.

5. Select **Save** to apply changes, or **Cancel** to discard.
6. A snackbar message appears confirming the update:
   “Role updated successfully.” An **Undo** link may also be available.

7.3.3 Delete a Role

You can delete a role if it is not assigned to any group. Deleting a role removes its associated privileges from the system.

1. In the **Manage Roles** interface, locate the role you want to delete—for example, **quality_controller**.
2. In the **Actions** column, select the **More options** icon (⋮) next to the role.
3. Select **Delete** from the dropdown menu.
   A confirmation dialog appears.

©SICK All rights reserved

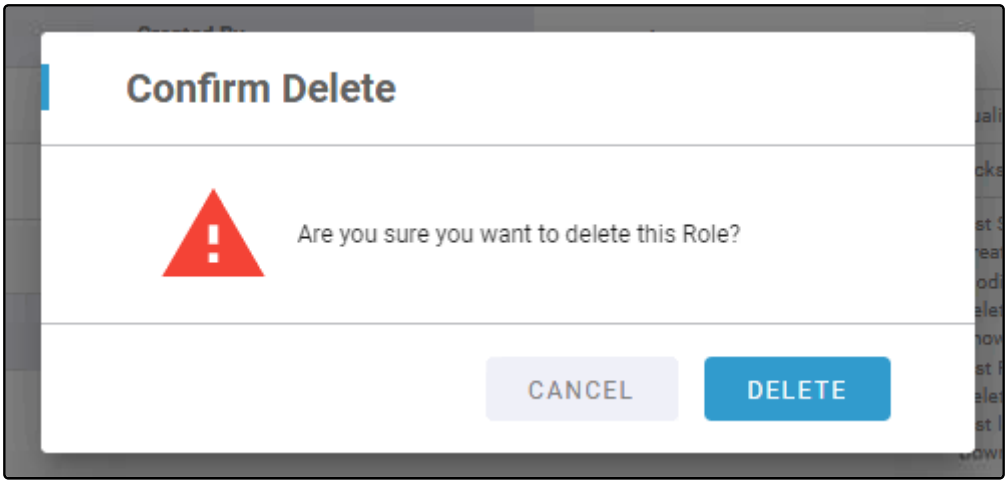


Figure 56

4. Select **Delete** to confirm the deletion, or **Cancel** to abort.

©SICK All rights reserved

8 Configuration Overview

The **Configuration** tab enables administrators to manage software settings, update or upload the enterprise license, and configure application settings such as adding/editing products, product groups, regions, and authentication methods.

8.1 Accessing the Configuration Tab

1. In the left navigation menu, locate the **Configuration** icon.
2. Click the **Configuration** icon to open the Configuration tab.

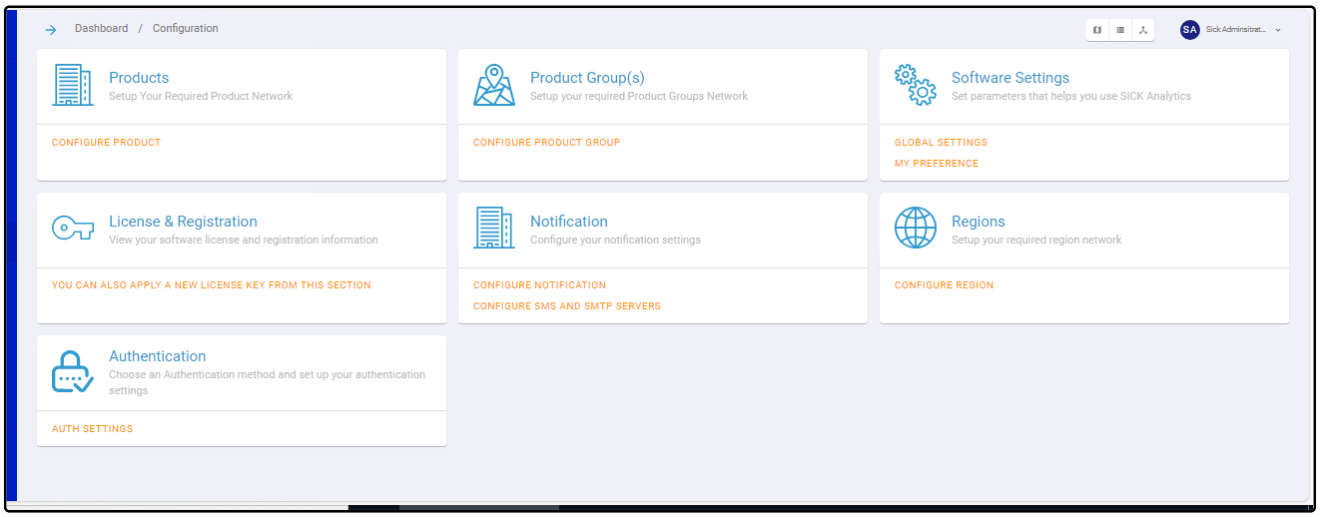


Figure 57

The Configuration tab includes the following sections, each dedicated to specific setup tasks for EA Analytics:

©SICK All rights reserved

Configuration Section	Purpose	Key Configuration Tasks
Products	Manage SICK products (e.g., Package Analytics, Field Analytics) for Analytics data collection.	• Add products (single or bulk with IP-address lists). • Configure MQTT connections (URLs, HTTP/HTTPS ports). • Edit product details (inline edits). • Delete products.
Product Groups	Organize products into groups for streamlined Analytics reporting and management.	• Create product groups. • Add/remove products from groups. • Edit group details. • Delete groups.
Software Settings	Configure global and user-specific settings to customize EA behavior and data handling.	• Set global settings (date/time format, locale, unit system, log retention up to 30 days). • Configure user preferences (personalized date format, locale, units).
License & Registration	Apply and manage the EA enterprise license to enable full functionality.	• Upload the enterprise license. • Verify license status.
Notification	Set up alerts for product status and system events to support Analytics monitoring.	• Configure email/SMS servers (host, port, credentials). • Create notification rules (up to one-hour frequency).
Regions	Define geographic regions for product organization and map-based Analytics.	• Add regions with autocomplete for countries. • Edit region details (name, associated countries). • Delete regions.
Authentication	Configure secure access methods for EA users.	• Set up LDAP authentication (URL, Distinguished Name). • Configure OpenID authentication (Client Secret, JWT Assertion). • Configure database authentication (host, port).

©SICK All rights reserved

9 License/Registration

When logged into Enterprise application, select, **"Apply License"** on the license configuration page and upload the enterprise license.

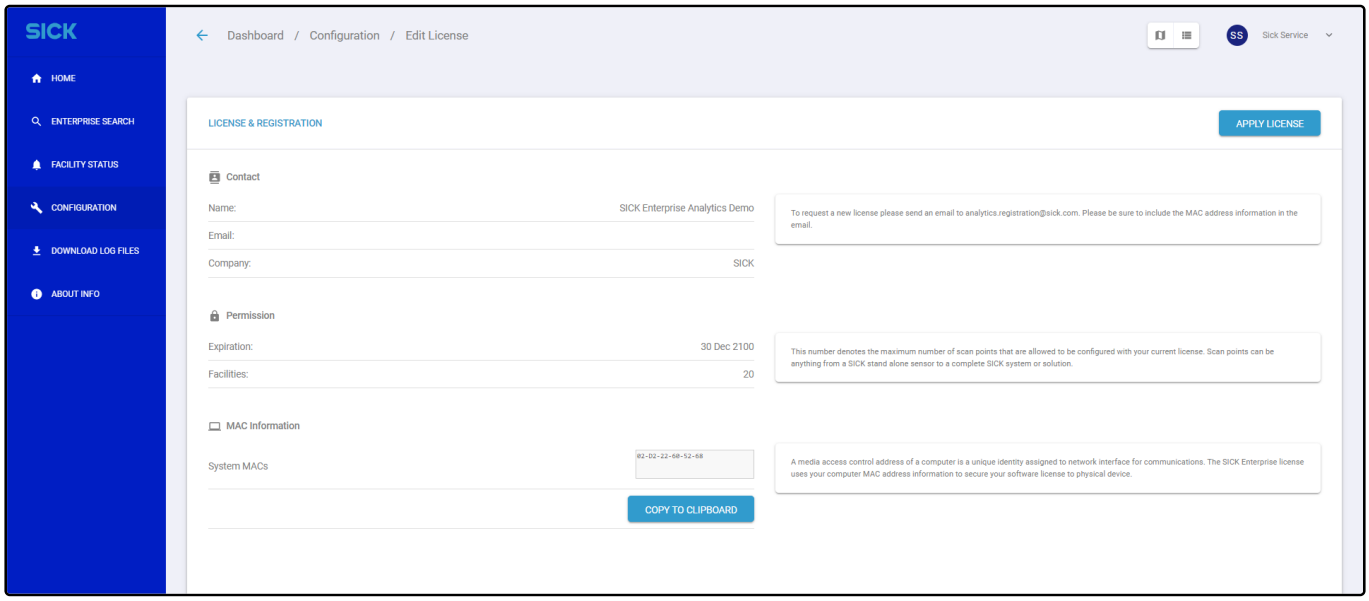


Figure 58

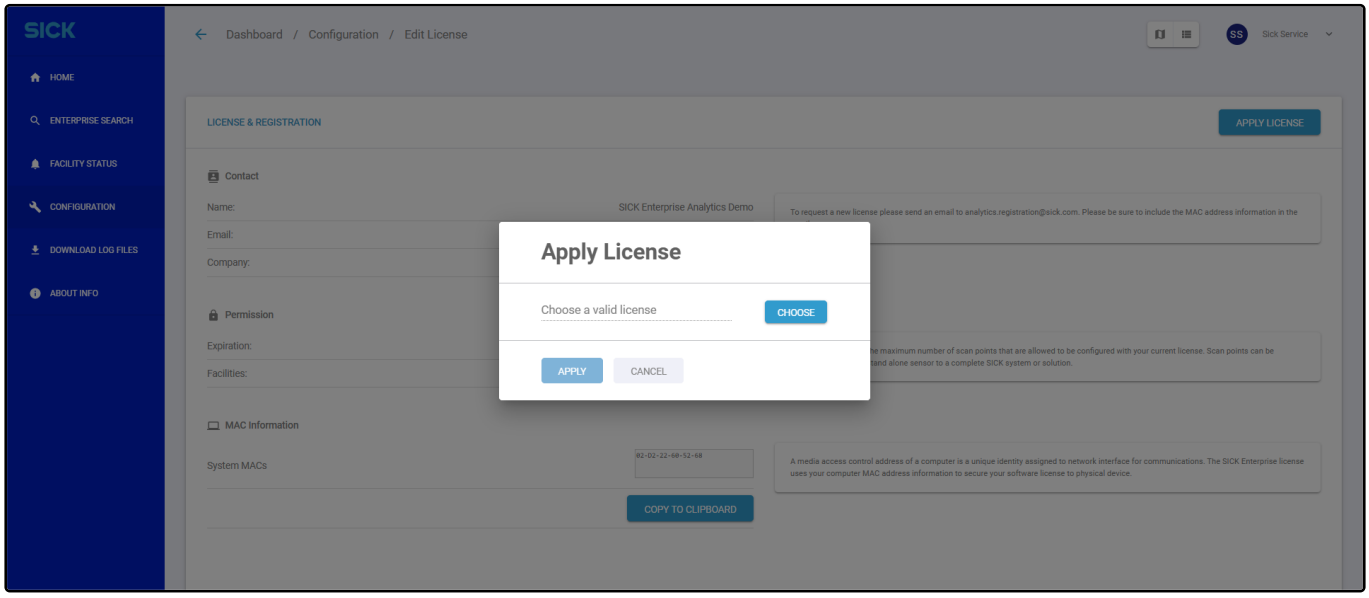


Figure 59

Enterprise application allows users to personalize their experience with a few parameters and settings according to their geographical location and personal needs.

©SICK All rights reserved

10 Product Management

10.1 Configure Products

You can add, edit, and delete products from the **Configure Product** page under the **Configuration** tab.

10.1.1 Navigate to the Configure Product Page

1. In the left navigation pane, select **Configuration**.

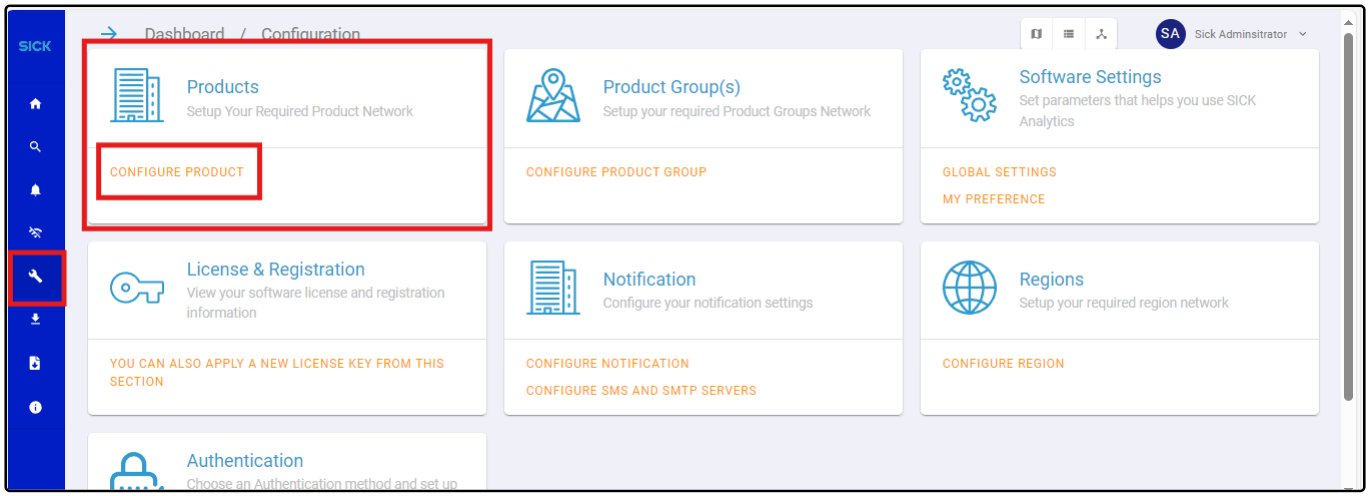
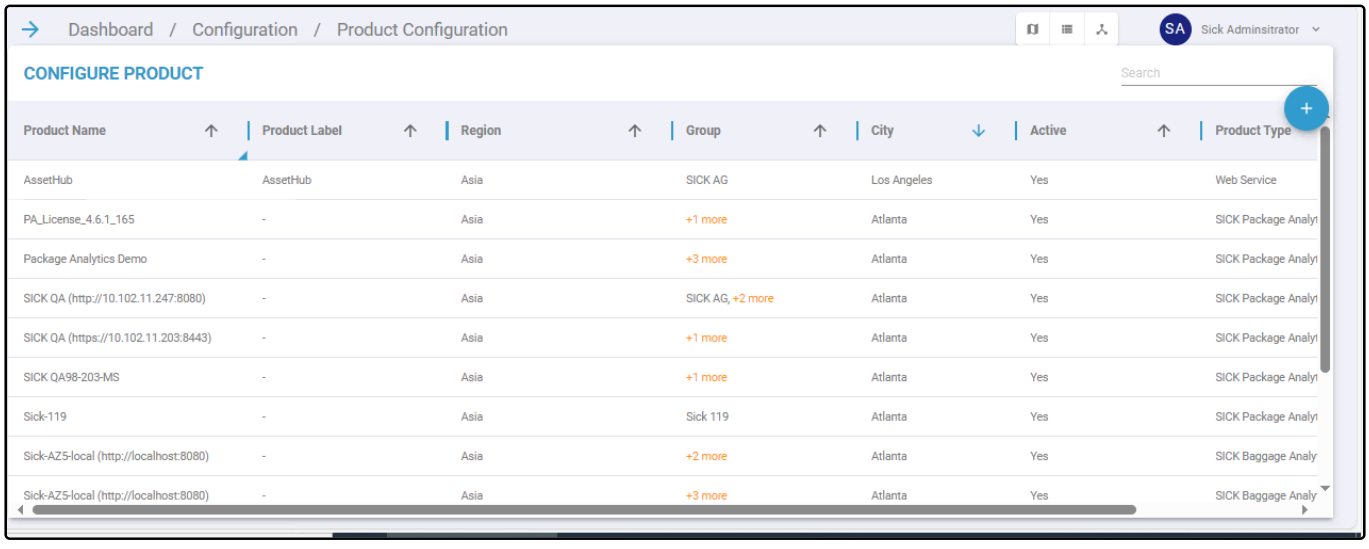


Figure 60

1. On the **Configuration** page, locate the Products section.

2. Select **Configure Product** to open the product management interface.

- The **Configure Product** page displays a table listing all configured products with columns for Product Label, Region, Group, City, Active, Product Type, and Actions (**Edit**/**Delete** icons).
- You can sort the table by selecting any column header arrow .



©SICK All rights reserved

3. To filter the list of products, enter a keyword in the **Search** field at the top-right corner of the page and press Enter.

The table updates to show only the products that match the search keyword.

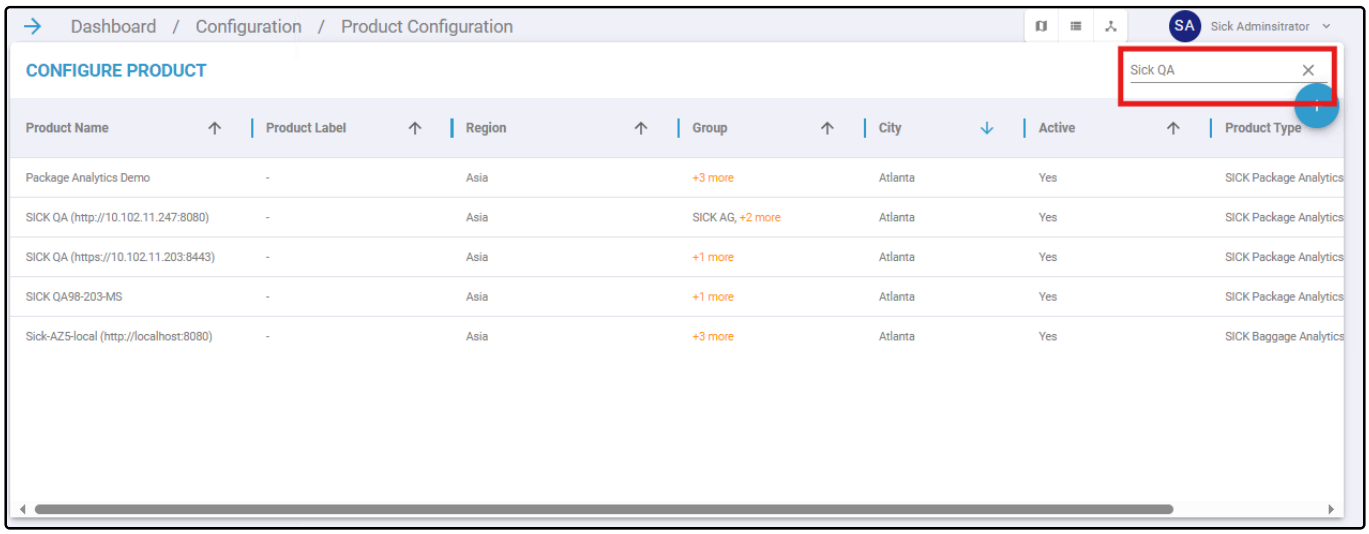


Figure 62

10.1.2 Add a New Product

To add a new product:

1. On the **Configure Product** page, select the  icon in the top-right corner.

2. In the Enable MQTT Connection for Products form, complete the following steps:

Step 1: Add URL Info

1. In the **Add URL Info** tab, enter the following:
   - Facility Section:
     - **Facility URL(s):** Enter the URL where the product is installed. You can include or omit the protocol. To add multiple URLs, separate them with commas.
     - **Default Protocol:** Select HTTP or HTTPS.
     - **Default HTTP Port:** Pre-filled with the default HTTP port. You can edit this.
     - **Default HTTPS Port:** Pre-filled with the default HTTPS port. You can edit this.
   - Enterprise Section:
     - **Enterprise Address:** Displays the address of the EA application (pre-filled).

2. Select **Cancel** to abort, or **Next** to proceed.

©SICK All rights reserved

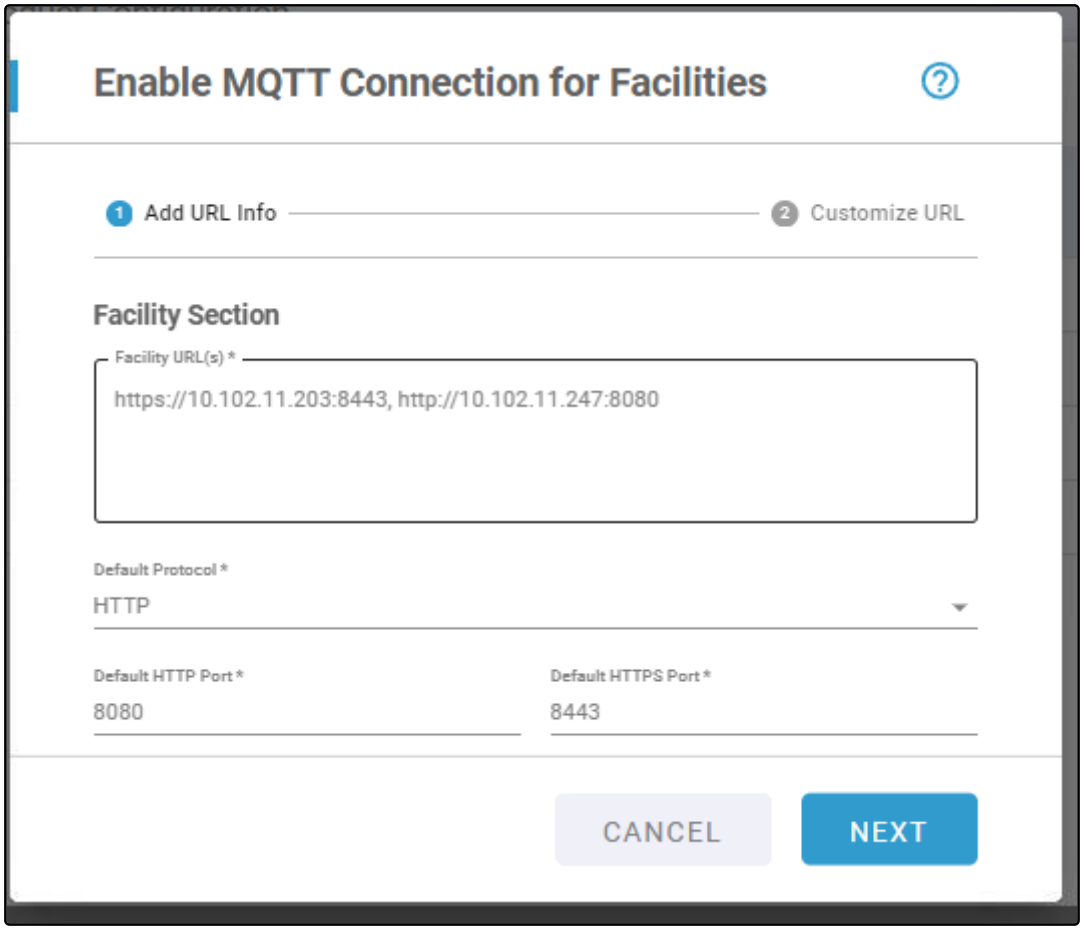


Figure 63

Step 2: Customize URL

1. In the **Customize URL** tab, review the entered URL(s). A message indicates the number of valid URLs.

2. Select **Back** to modify the URL or settings, or **Save** to proceed.

©SICK All rights reserved

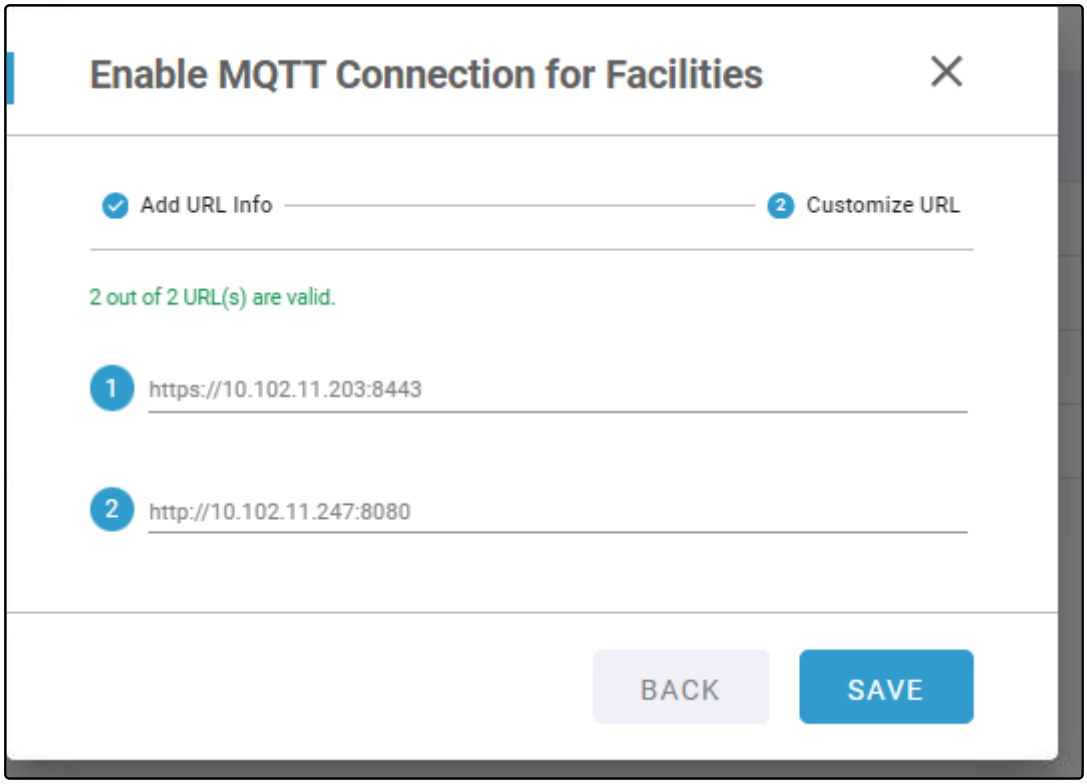


Figure 64

Step 3: Confirm MQTT Connection Settings

1. A confirmation pop-up titled "Products Configuration Summary" appears, listing the saved URL(s).
2. A message confirms: "Enterprise connection settings saved successfully."
3. Select **Close** to proceed.

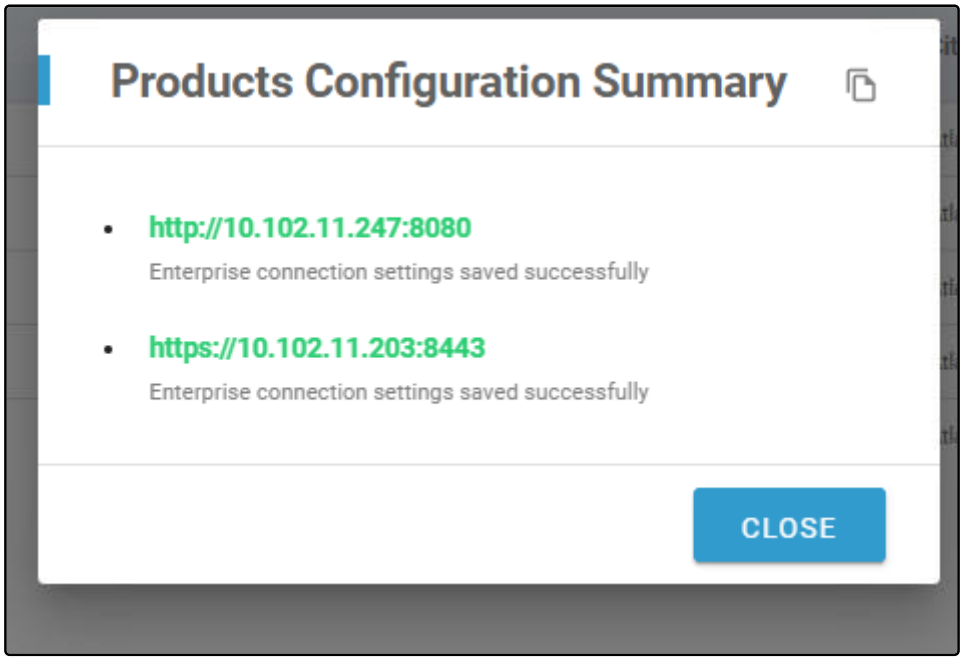


Figure 65

Step 4: View the Updated Product List

©SICK All rights reserved

1. The **Configure Product** page refreshes, and the new product appears in the product list.

2. Verify the new product in the table.

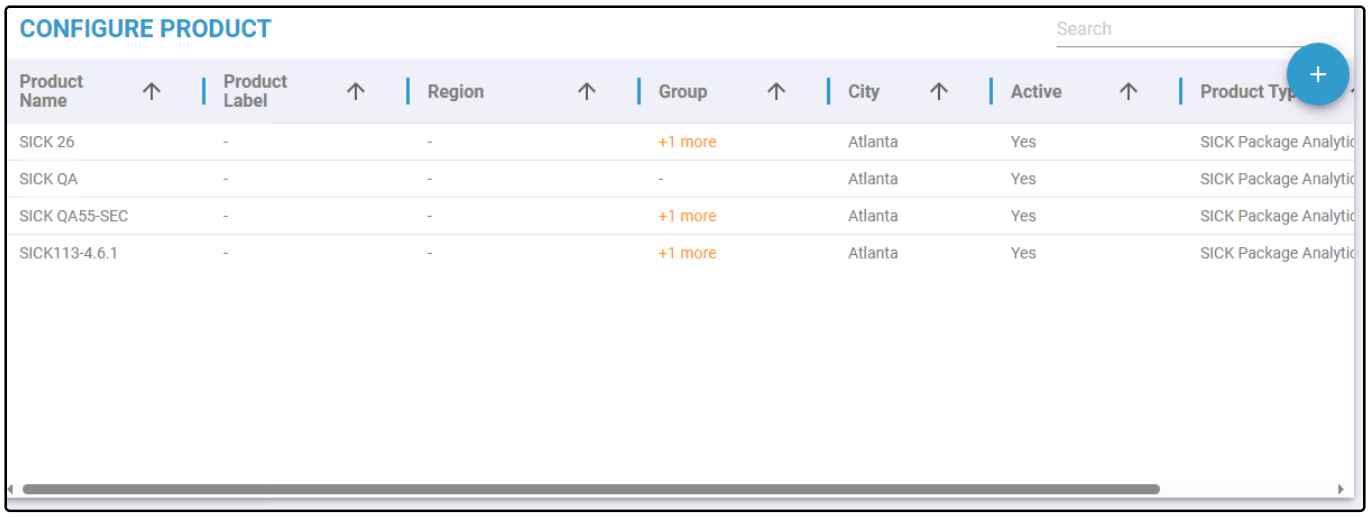


Figure 66

10.1.3 Edit a Product

To edit a product:

1. On the **Configure Product** page, locate the product in the table.

2. In the **Actions** column, select the **Edit** icon 

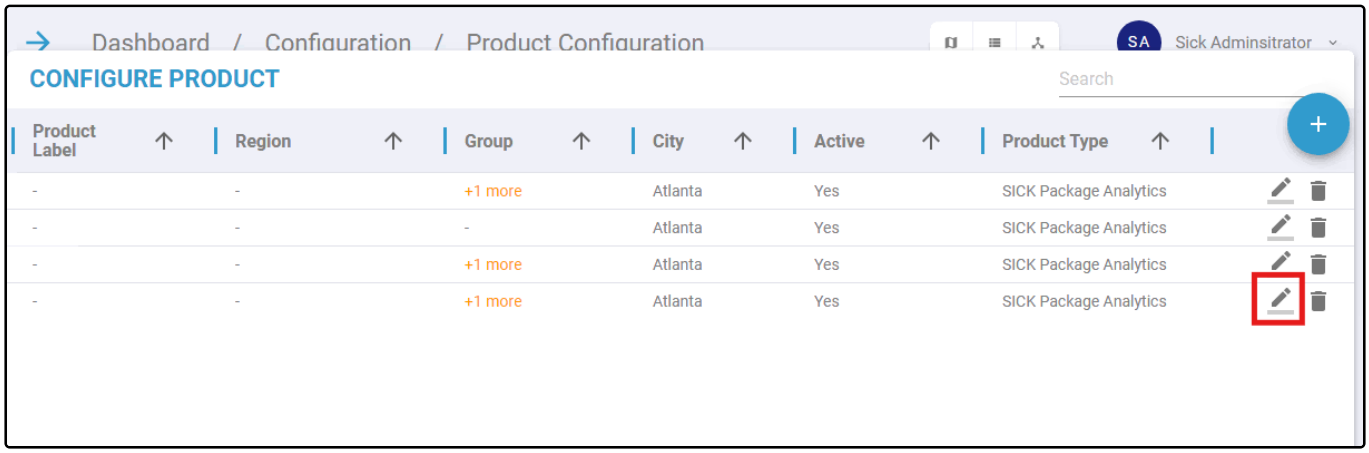


Figure 67

In the **Edit Product** form, update the following fields as needed:

©SICK All rights reserved

Field	Description
Product Type	Displays the type of SICK product.
Name	The product name.
URL	The URL where the product is installed. You can modify the protocol (HTTP/HTTPS) and port.
ID	The product ID.
Label	The product label.
Add Group	The linked product group.
Polling Frequency (mins)	The polling frequency in minutes.
Country	The country.
State	The state or province.
City	The city.
Active	A checkbox to set the product's visibility. When checked, the product is active and appears in the EA Dashboard views (e.g., Map View, Tree View, List View); when unchecked, the product is inactive and does not appear in these views.

©SICK All rights reserved

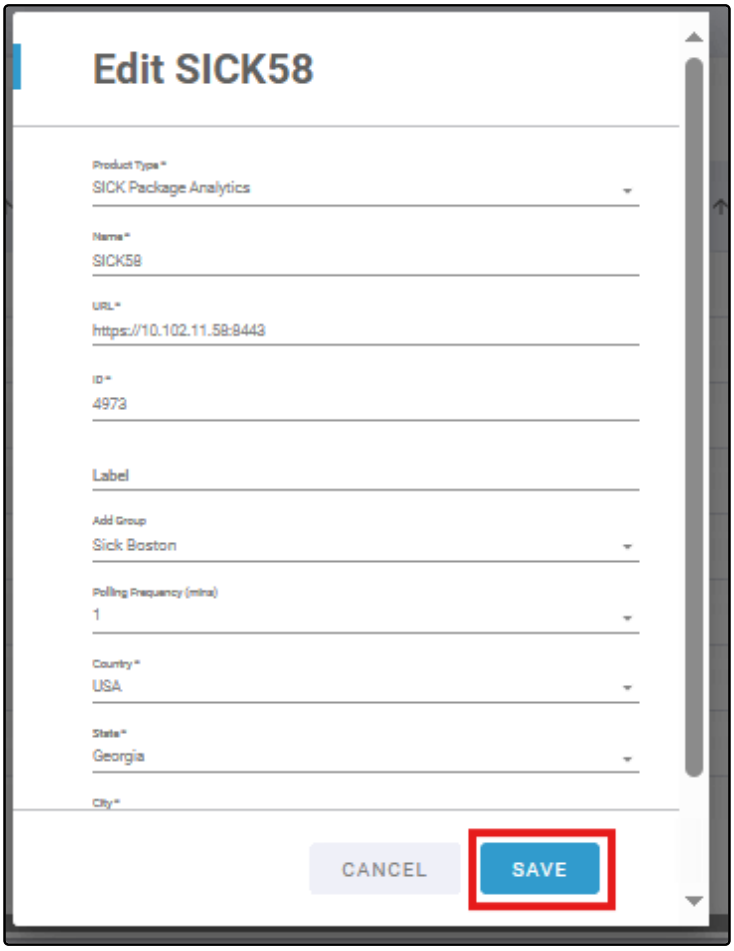


Figure 68

3. Select **Save** to apply changes, or **Cancel** to discard them.

4. The **Configure Product** page updates. A notification with an **UNDO** link appears, allowing you to revert the deletion if needed.

Figure 69

10.1.4 Delete a Product

To delete a product:

©SICK All rights reserved

1. On the **Configure Product** page, locate the product in the table.

2. In the "Actions" column, select the **Delete** icon

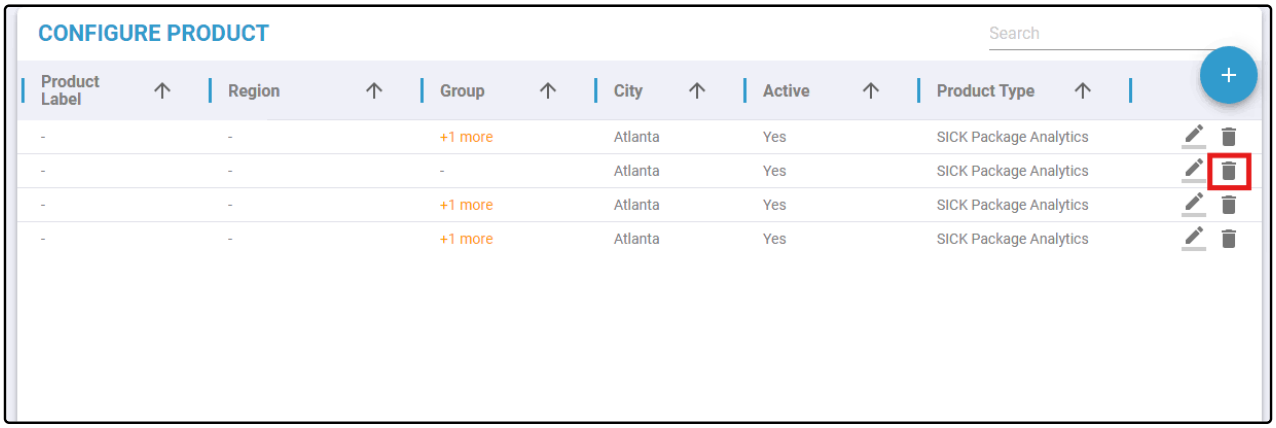


Figure 71

3. In the confirmation pop-up, select **Delete** to confirm, or **Cancel** to abort.

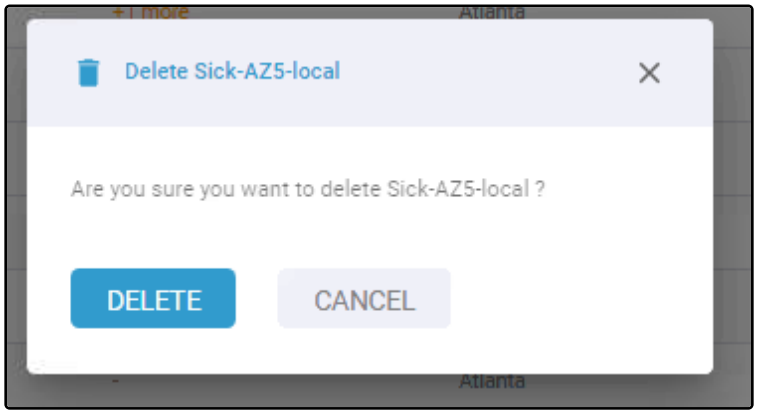


Figure 72

4. The **Configure Product** page updates, and the product is removed from the list. A notification with an **UNDO** link appears, allowing you to revert the deletion if needed.

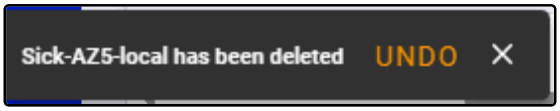


Figure 73

10.2 Configure Product Group

You can add, edit, and delete product groups from the **Configure Product Group** page under the **Configuration** tab.

©SICK All rights reserved

10.2.1 Navigate to the Configure Product Group Page

1. In the left navigation pane, select  **Configuration**.
2. On the **Configuration** page, locate the Product Groups section.
3. Select **Configure Product Group** to open the product-group management interface.

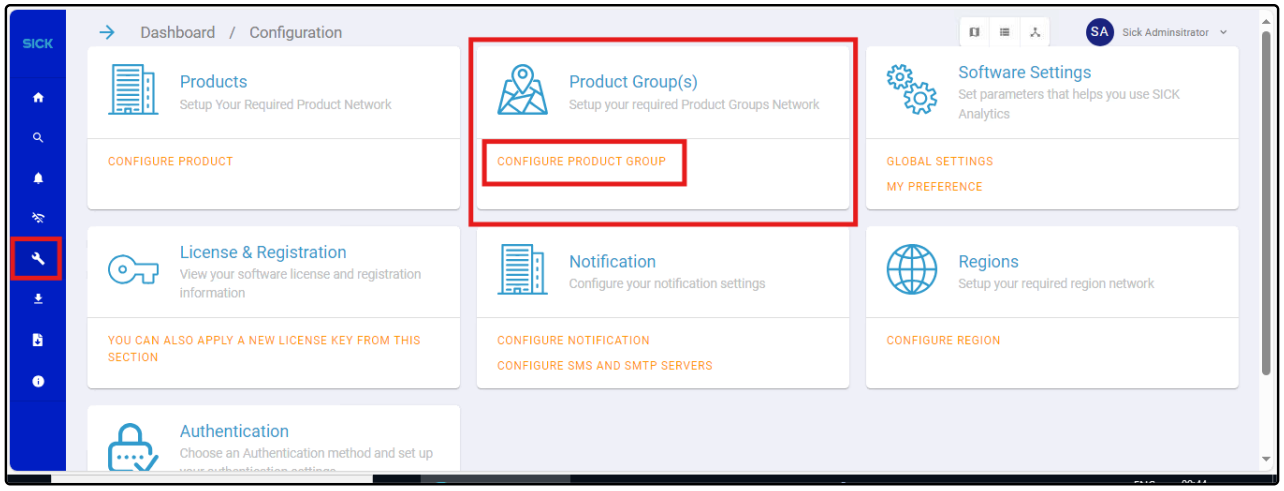


Figure 74

- The **Configure Product Group** page displays a table listing all configured product groups with columns for Product Group Name, Products, and Actions (Edit/Delete icons).
- You can sort the table by selecting any column header arrow  .
- If a product group has multiple products, the Products column shows a partial list with a **More** link to view the full list.

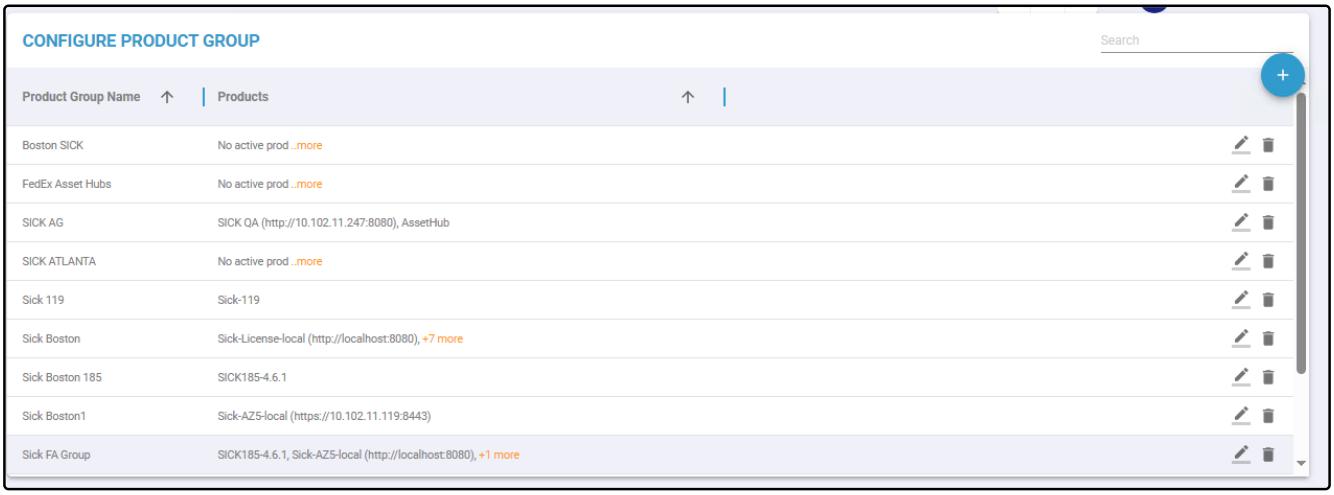
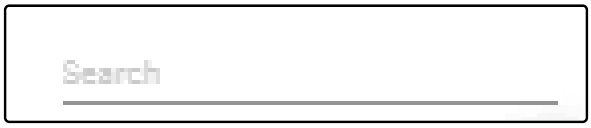


Figure 75

©SICK All rights reserved

4. To filter the list of product groups, enter a keyword in the **Search** field at the top-right corner of the page and press Enter.



   The table updates to show only the product groups that match the search keyword.

5. To view the full list of products in a group, select the **More** link in the Products column.

The row expands to display the complete list of products associated with the product group.

10.2.2 Add a New Product Group

To add a new product group:

©SICK All rights reserved

1. On the **Configure Product Group** page, select the **Add** icon in the top-right corner.

2. In the **Add Product Group** form, enter the following:
   - Product Group Name: Enter a unique name for the product group.
   - Add Product: Select the products to include in this group from a dropdown list of available products. You can add multiple products, and each selected product will appear with an "X" to remove it if needed.

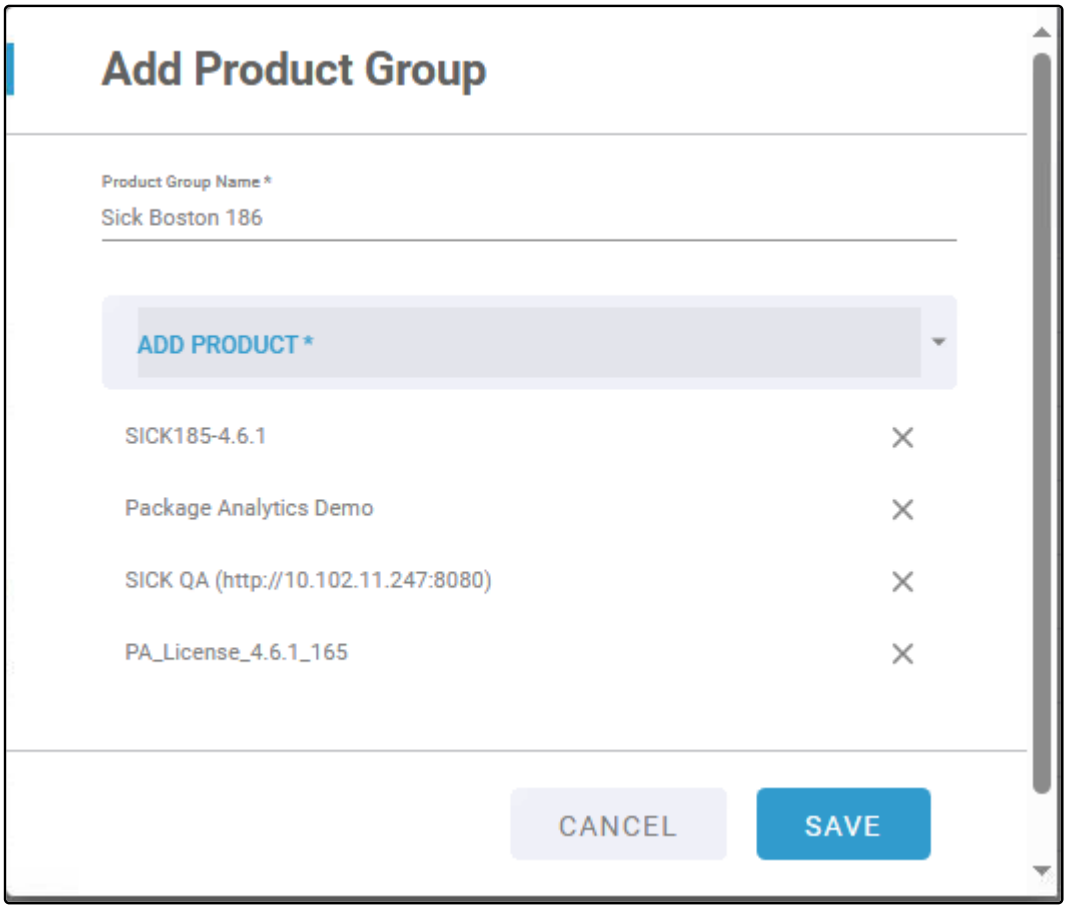


Figure 77

3. Select **Save** to add the product group, or **Cancel** to discard the changes.

4. The Configure Product page refreshes, and the product is removed from the list. A notification with an UNDO link appears, allowing you to revert the deletion if needed.

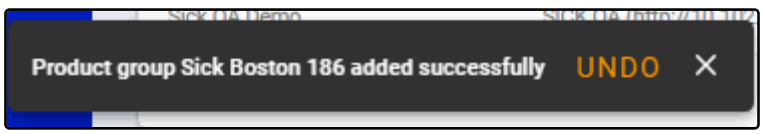


Figure 78

10.2.3 Edit a Product Group

To edit a product group:

©SICK All rights reserved

1. On the **Configure Product Group** page, locate the product group in the table.
2. In the "Actions" column, select the **Edit** icon.
3. In the **Edit Product Group** form, update the following fields as needed:
   - Product Group Name: The name of the product group.
   - Products: The products included in this group.
4. Select **Save** to apply changes, or **Cancel** to discard them.

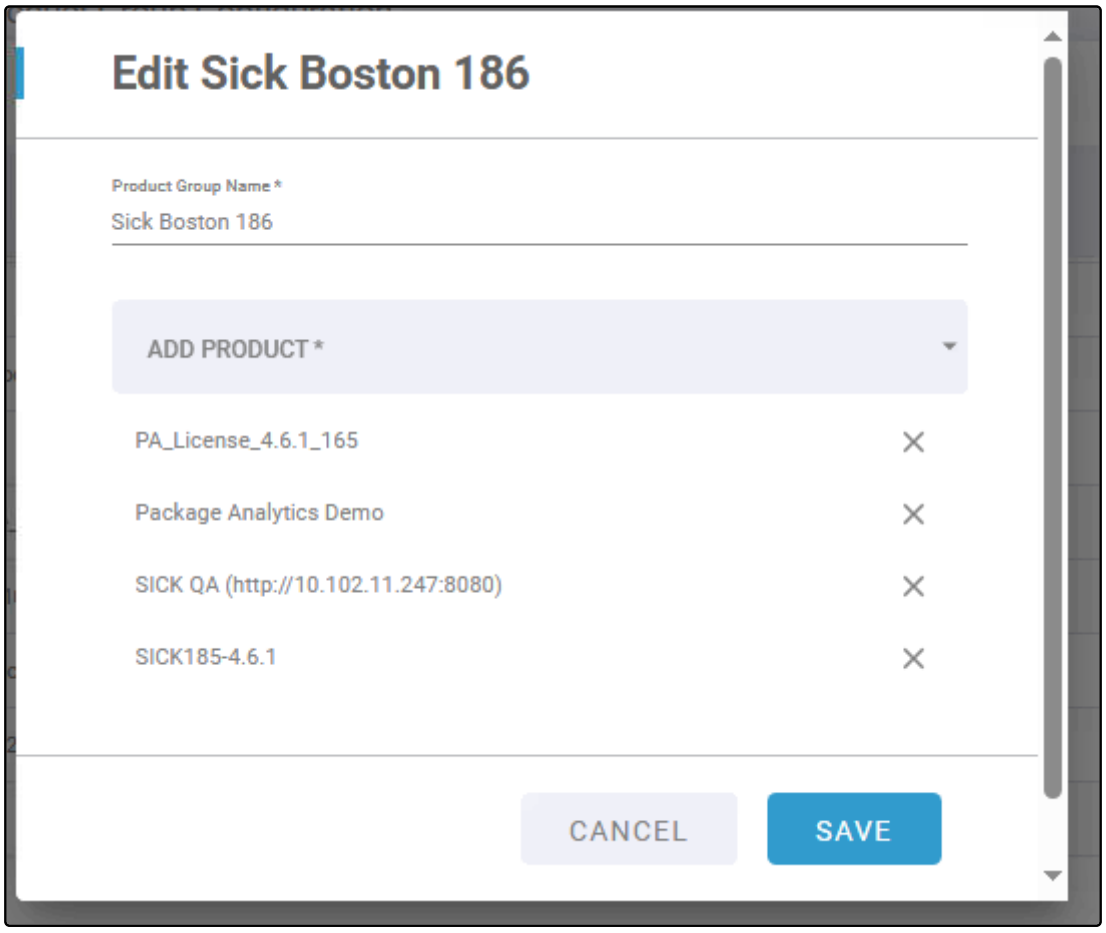


Figure 79

5. The **Configure Product Group** page refreshes, and the updated product group appears in the list with a notification confirming the edit (e.g., "Product group [Name] edited successfully") and an **UNDO** link to revert the action if needed. Verify the updated details in the product group list.

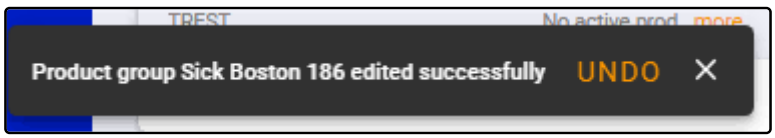


Figure 80

10.2.4 Delete a Product Group

To delete a product group:

©SICK All rights reserved

1. On the **Configure Product Group** page, locate the product group in the table.

2. In the "Actions" column, select the **Delete** icon .

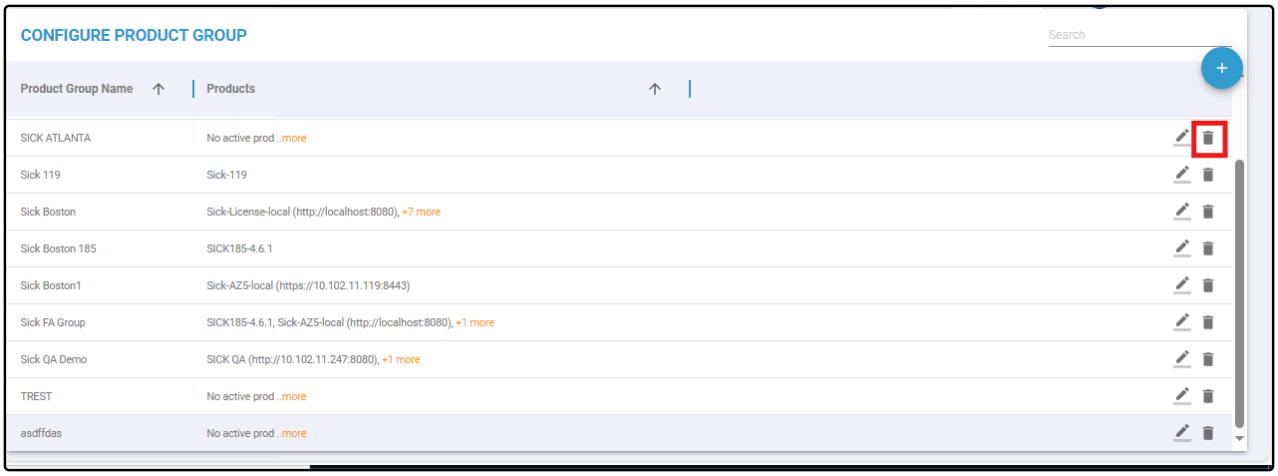


Figure 81

3. In the confirmation pop-up, select **Delete** to confirm, or **Cancel** to abort.

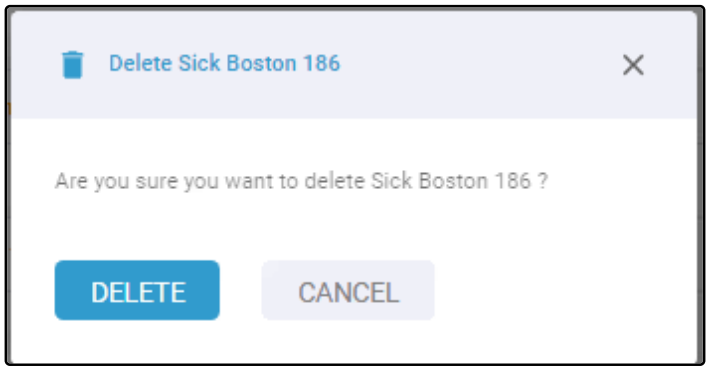


Figure 82

4. The **Configure Product Group** page refreshes, and the product group is removed from the list. A notification with an **UNDO** link appears, allowing you to revert the deletion if needed.

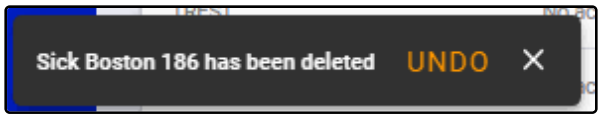


Figure 83

10.3 Configure Region

You can add, edit, and delete regions from the **Configure Region** page under the **Configuration** tab.

10.3.1 Navigate to the Configure Region Page

1. In the left navigation pane, select **Configuration**.

©SICK All rights reserved

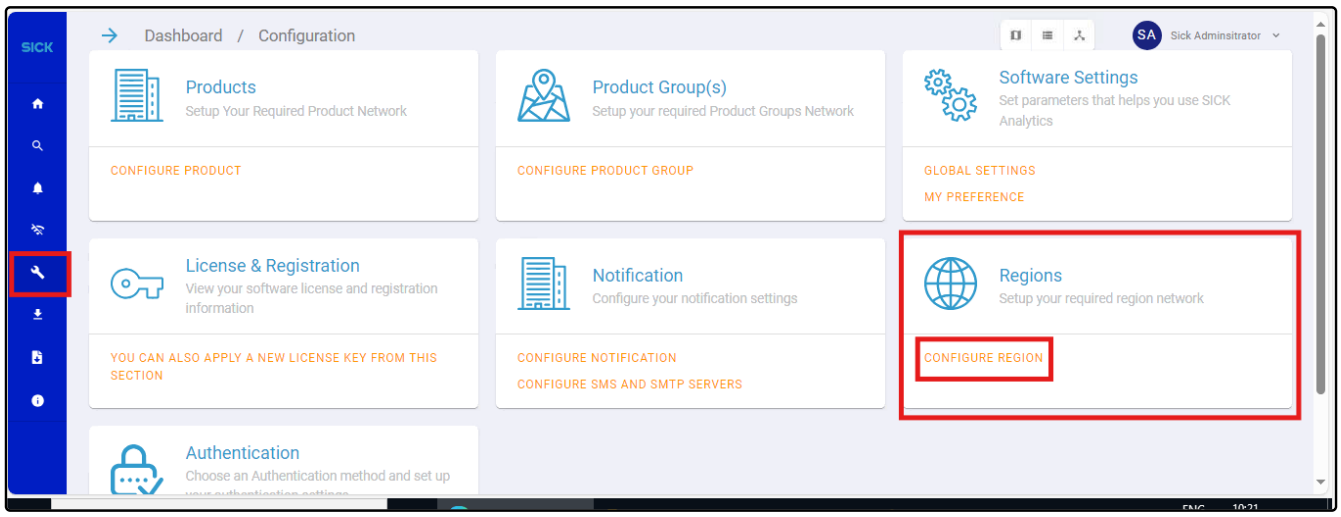


Figure 84

2. On the **Configuration** page, locate the Regions section.

3. Select **Configure Region** to open the region management interface.

4. The **Configure Region** page displays a table listing all configured regions with columns for Region Name, Countries, and Actions (Edit/Delete icons).

5. You can sort the table by selecting any column header .

6. To filter the list of regions, enter a keyword in the **Search** field at the top-right corner of the page and press Enter.

- The table updates to show only the regions that match the search keyword.

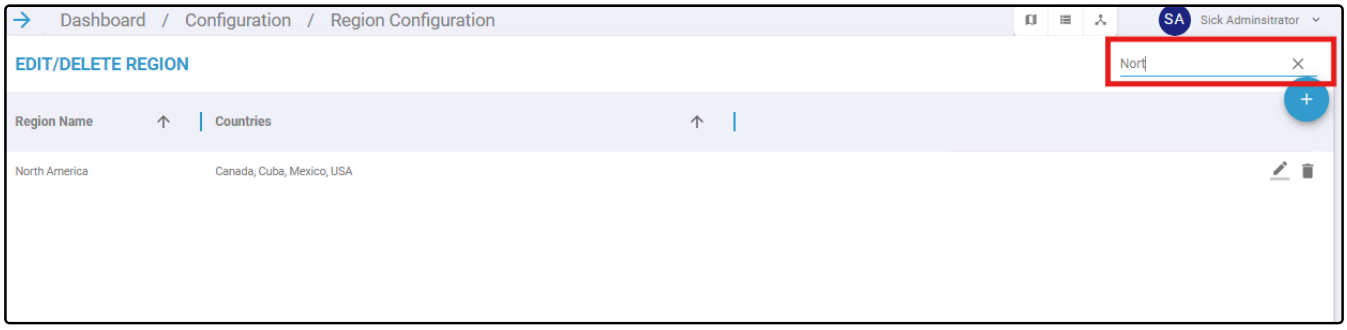


Figure 85

10.3.2 Add a New Region

To add a new region:

©SICK All rights reserved

1. On the **Configure Region** page, select the  icon in the top-right corner.

2. In the **Add Region** form, enter the following:
   - **Region Name:** Enter a unique name for the region.
   - **Add Country:** Select at least one Country to associate with the region. At least one location is required.

3. Select **Save** to add the region, or **Cancel** to discard the changes.

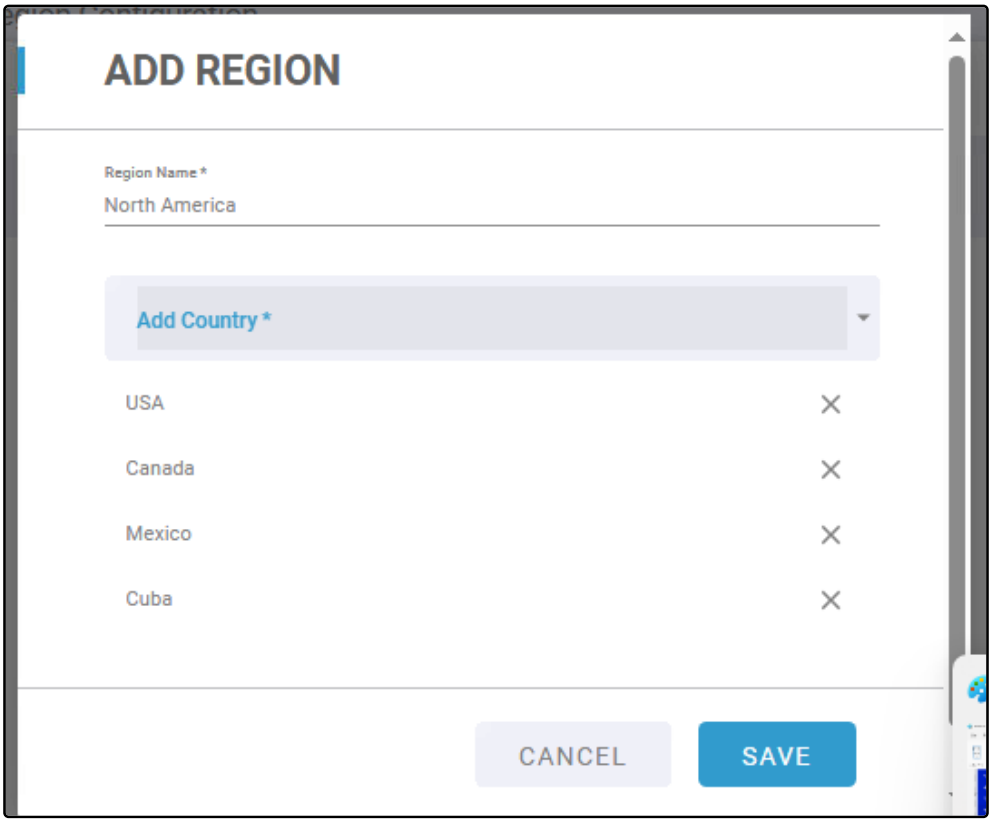


Figure 86

4. The **Configure Region** page refreshes, and the new region appears in the list with a notification confirming the addition (for example, "Region [Name] added successfully") and an **UNDO** link to revert the action if needed. Verify the new region in the table.

Figure 87

10.3.3 Edit a Region

To edit a region:

©SICK All rights reserved

1. On the **Configure Region** page, locate the region in the table.
2. In the "Actions" column, select the **Edit** icon.
3. In the **Edit Region** form, update the following fields as needed:
   - Region Name: The name of the region.
   - Add Location: The locations associated with this region. You can add new locations using the dropdown or remove existing ones by selecting the "X" next to each location.
4. Select **Save** to apply changes, or **Cancel** to discard them.

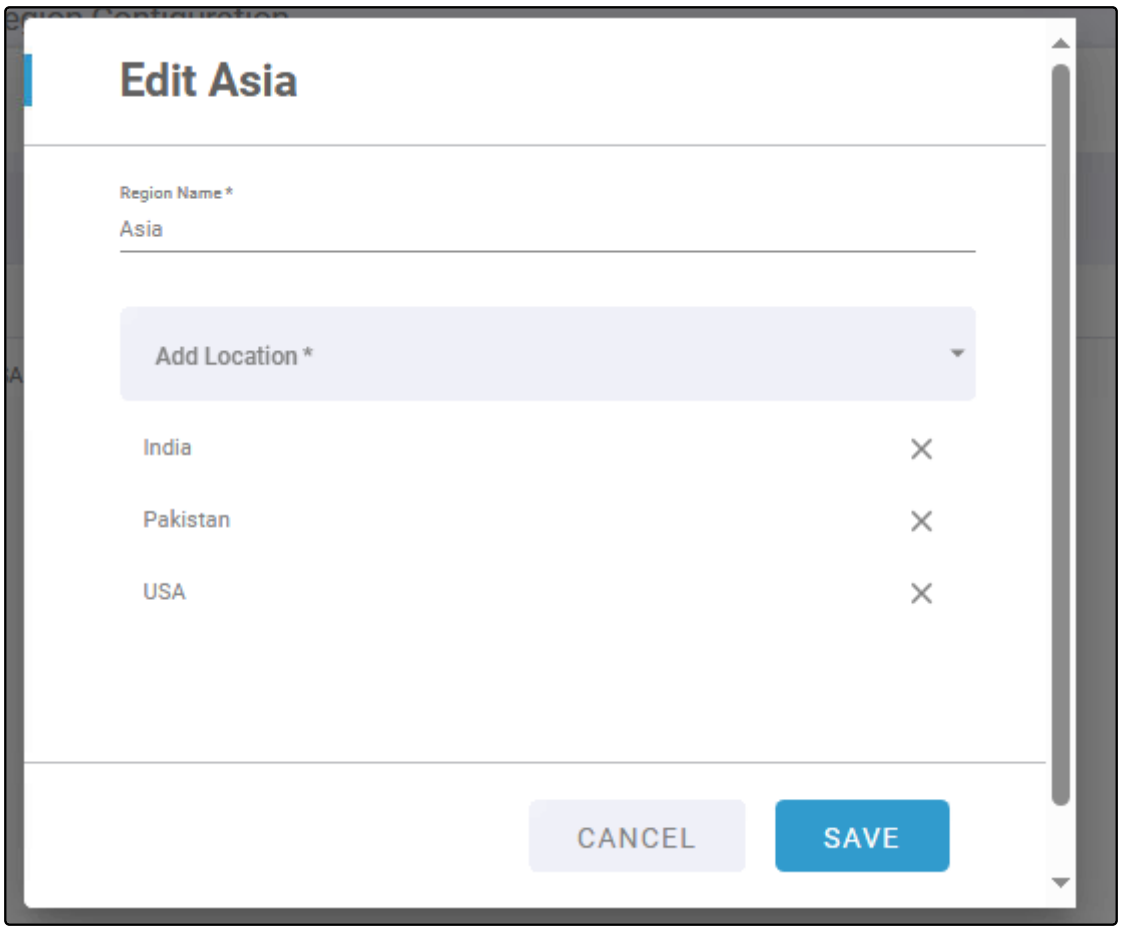


Figure 88

5. The **Configure Region** page refreshes, and the updated region appears in the list with a notification confirming the edit (e.g., "Region [Name] edited successfully") and an **UNDO** link to revert the action if needed. Verify the updated details in the region list.

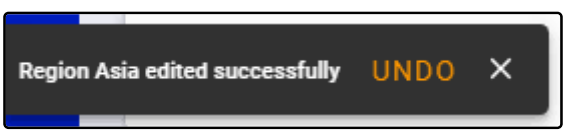


Figure 89

10.3.4 Delete a Region

To delete a region:

©SICK All rights reserved

1. On the **Configure Region** page, locate the region in the table.

2. In the "Actions" column, select the **Delete** icon

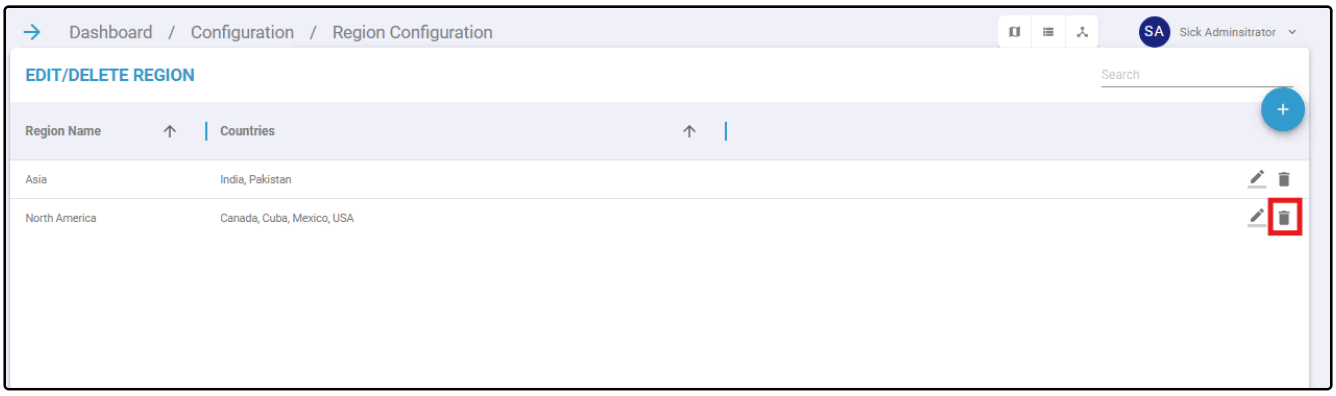


Figure 90

3. In the confirmation pop-up, select **Delete** to confirm, or **Cancel** to abort.

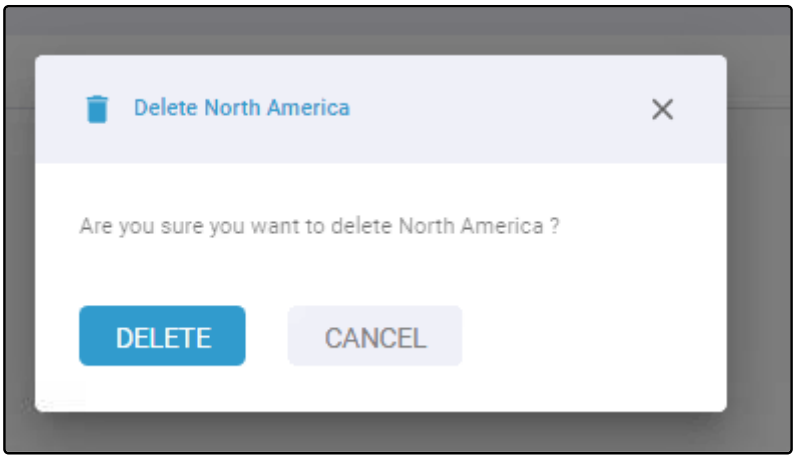


Figure 91

4. The **Configure Region** page refreshes, and the region is removed from the list. A notification with an **UNDO** link appears, allowing you to revert the deletion if needed.

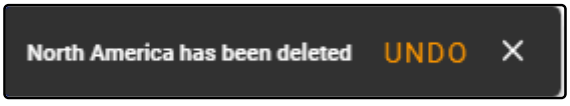


Figure 92

©SICK All rights reserved

11 Authentication Settings

To navigate to Authentication settings, select **"Auth settings"** under Authentication section on configuration screen.

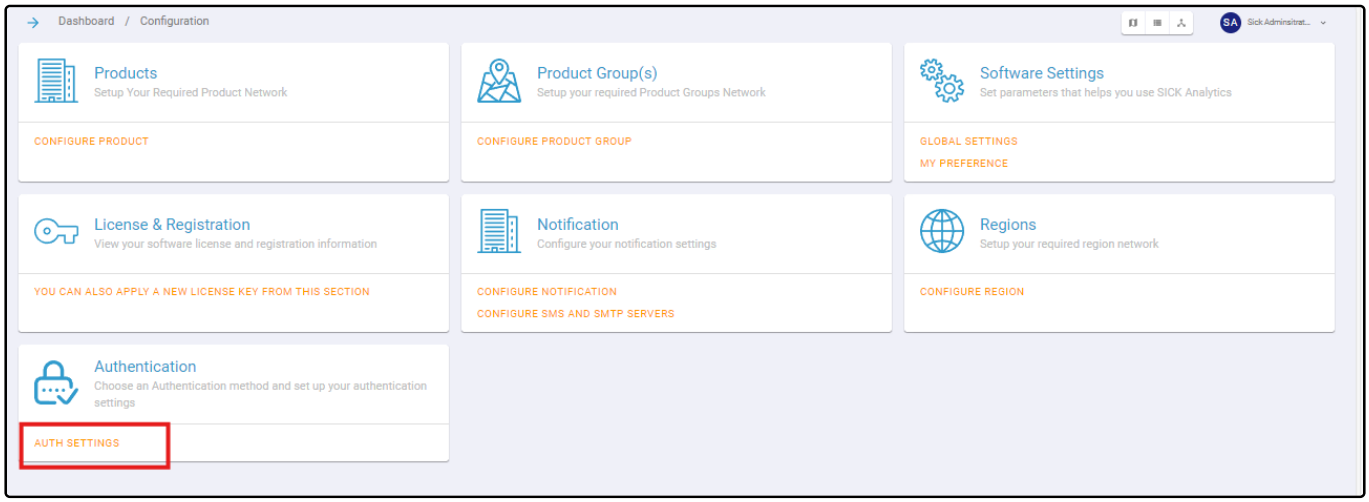


Figure 93

11.1 Configure LDAP Authentication

Auth Settings screen appears with two authentication options that are LDAP and Database.

When **LDAP** radio button is selected. Following fields appears:

- LDAP Type
- URL
- Distinguished Name
- Search Filter
- Username
- Password

Click on **Verify** button to verify the details then click on **Save** button to save the details.

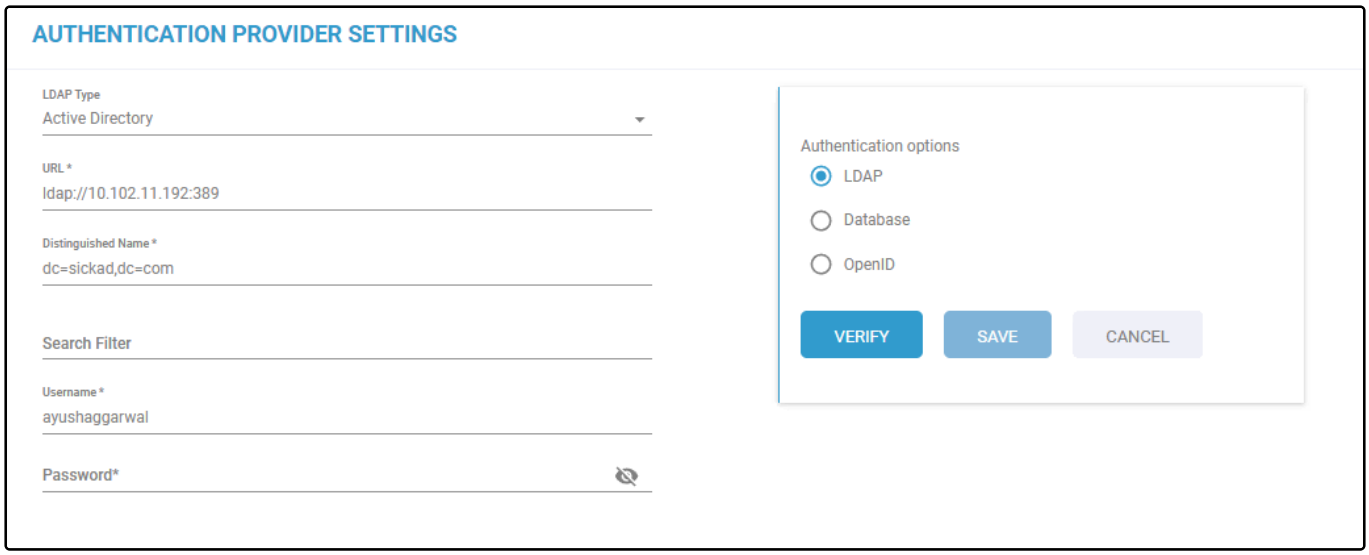


Figure 94

©SICK All rights reserved

11.2 Configure LDAP Authentication

Auth Settings screen appears with two authentication options that are LDAP and Database.

When **LDAP** radio button is selected. Following fields appears:

- LDAP Type
- URL
- Distinguished Name
- Search Filter
- Username
- Password

Click on **Verify** button to verify the details then click on **Save** button to save the details.

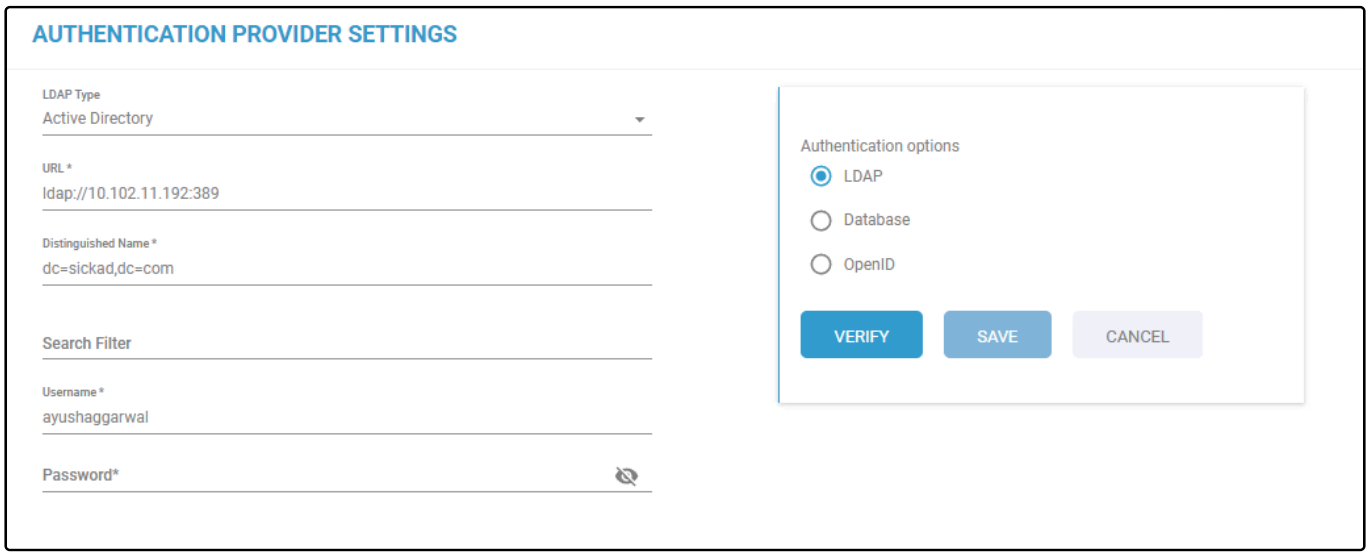


Figure 95

Figure 95

11.3 Configure OpenID Authentication

This section provides instructions on how to configure and switch to OpenID authentication, allowing users to log in using OpenID credentials. The OpenID authentication method supports two verification mechanisms: **Client Secret** and **JWT Assertion**.

©SICK All rights reserved

1. Select the **OpenID** radio button from the right-hand side under **Authentication Options**.

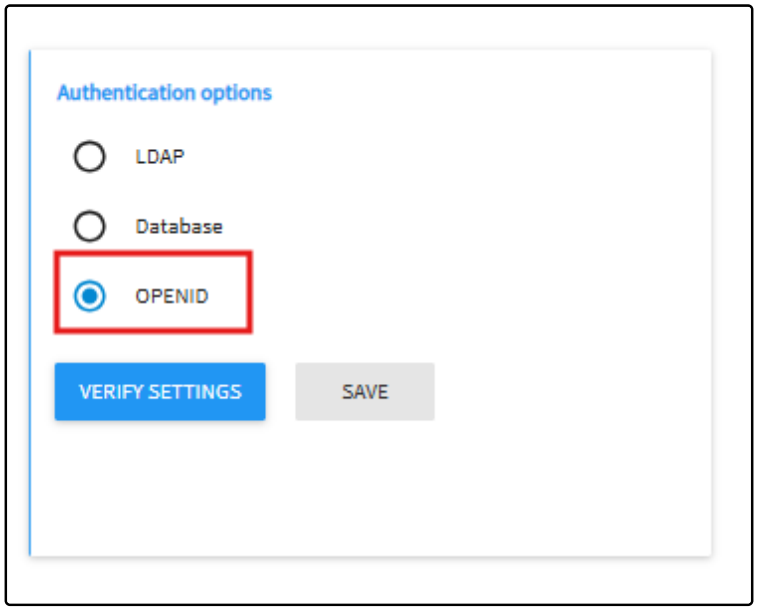


Figure 96

2. The **OpenID configuration fields** are displayed in the middle pane.

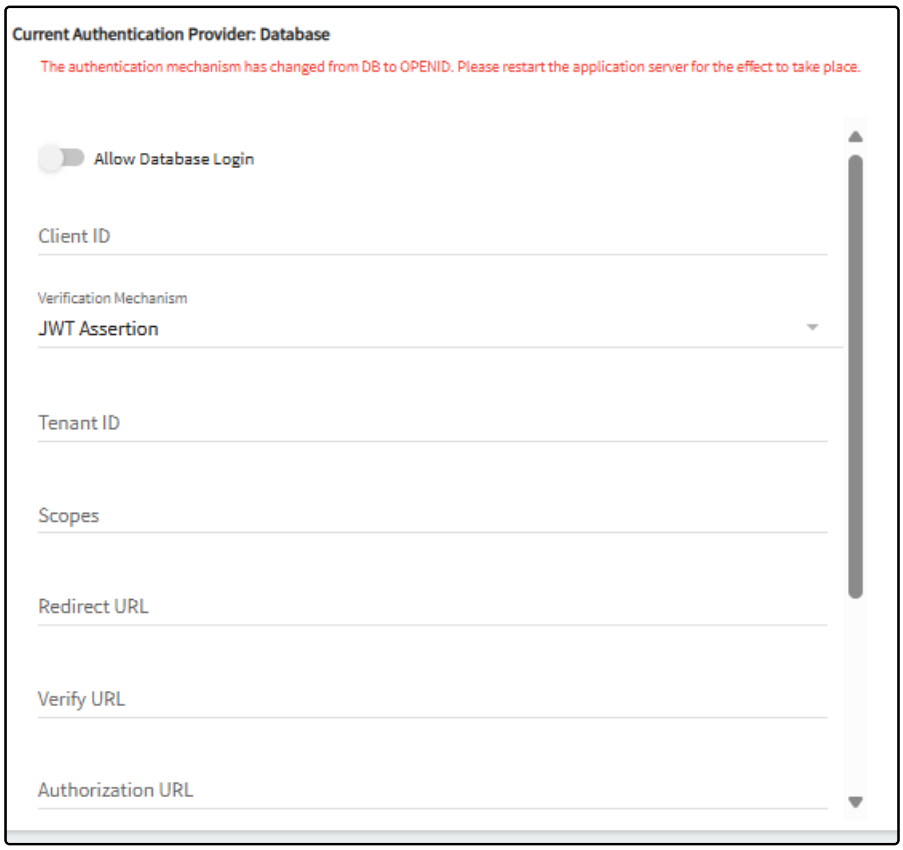


Figure 97

©SICK All rights reserved

3. Fill in the following fields):
   - **Allow Database Login** – Turn this on if users should also be allowed to log in using database credentials.
   - **Client ID** – Enter the client ID provided by your OpenID provider.
   - **Verification Mechanism** – Choose the appropriate verification method:
     - **Client Secret**: If selected, the **Client Secret** field appears. Enter the secret value provided by your OpenID provider.
     - **JWT Assertion**: If selected, the **Tenant ID** field appears. Enter the tenant or realm ID as required by your OpenID provider.
   - **Scope** – Specify the scope required for authentication.
   - **Redirect URL** – Enter the URL where the OpenID provider will redirect after authentication.
   - **Verify URL** – Enter the URL for the OpenID provider's configuration endpoint.
   - **Authorization URL** – Enter the URL for the OpenID provider's authorization endpoint.
   - **Token URL** – Enter the URL for the OpenID provider's token endpoint.
   - **JWK URL** – Enter the URL for the OpenID provider's JSON Web Key Set (JWKS) endpoint.
   - **Logout URL** – Enter the URL for the OpenID provider's logout endpoint.

4. Select **VERIFY SETTINGS**.

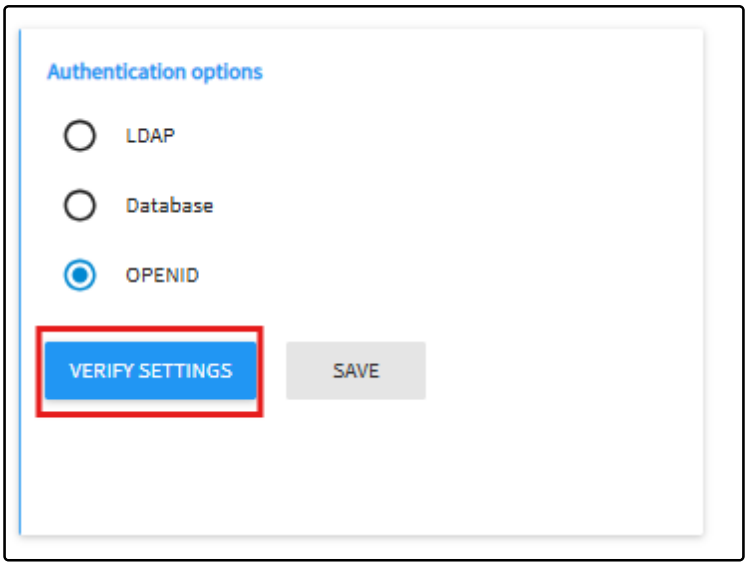
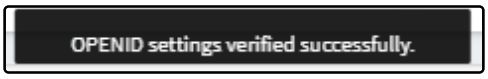


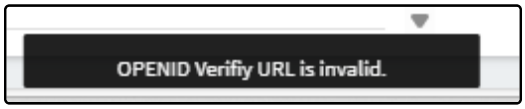
Figure 98

5. If the settings are valid, a snackbar message confirms that the connection is successful. The **SAVE** button becomes enabled.



©SICK All rights reserved

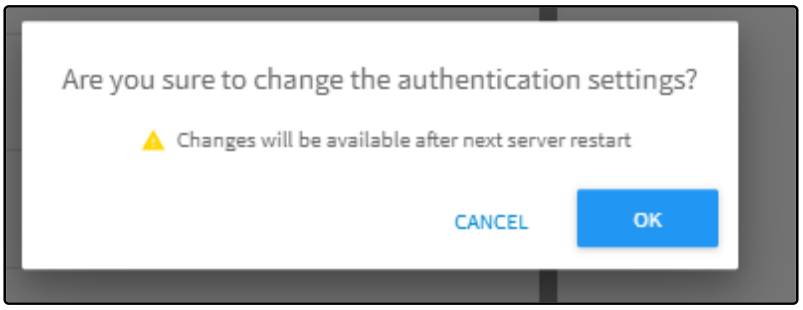
6. If any of the entered details are incorrect, a snackbar message is displayed indicating the error.



In this case, the SAVE button will remain disabled. Correct the input details and select VERIFY SETTINGS again.

7. Select **SAVE.**

8. A confirmation popup appears with the message:
Select **OK** to confirm or **CANCEL** to exit.



9. A red banner appears at the top of the page, prompting you to restart the services.

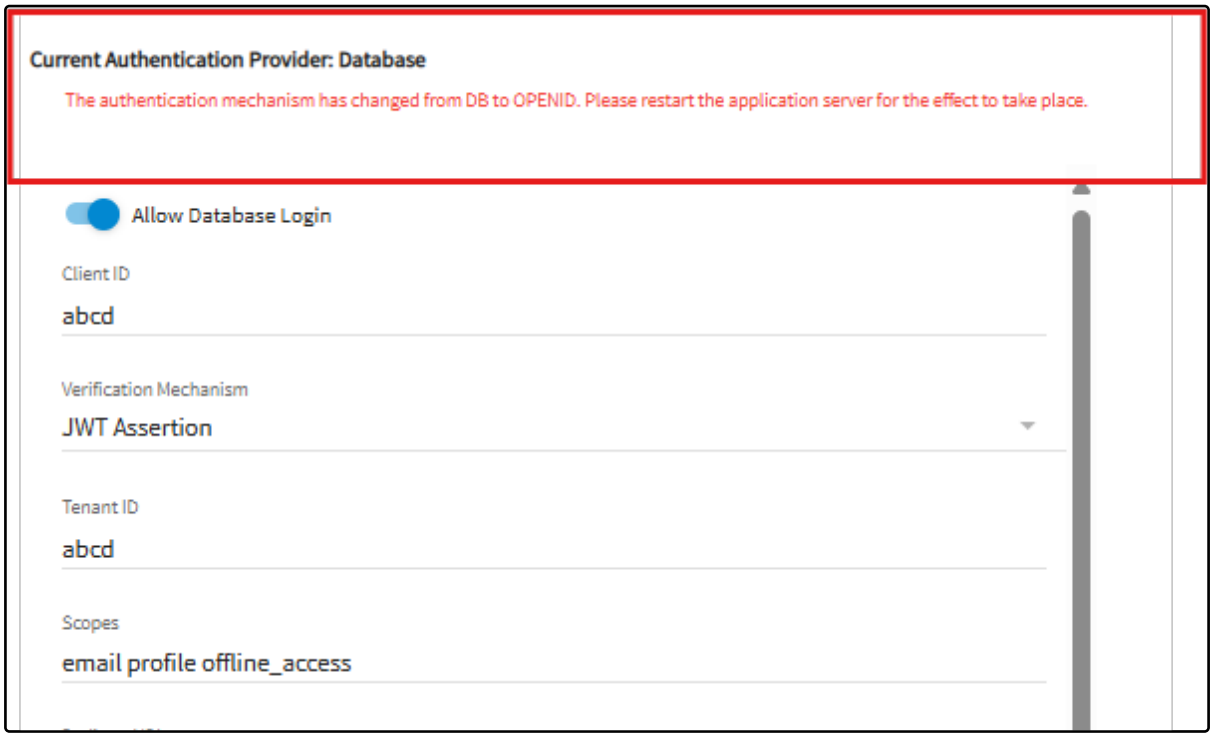
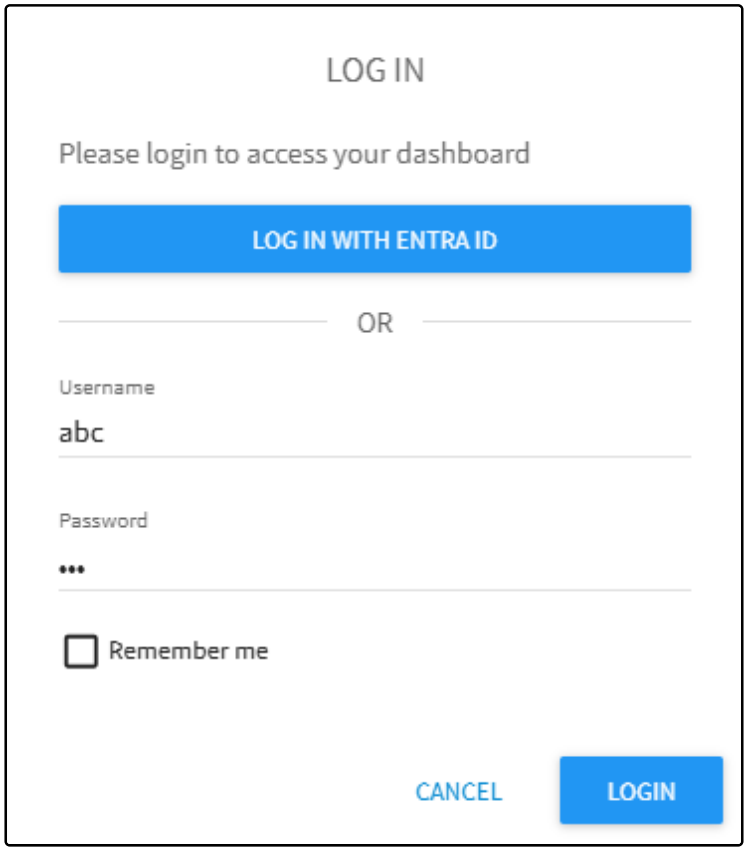


Figure 102

10. Restart the application services. For more information, refer to *How to Restart Services*.

11. After the restart:
    - Users can log in using their OpenID credentials.

©SICK All rights reserved



©SICK All rights reserved

12 Software Settings

This option allows the user to configure settings, related to **Locale**, **Date format**, and **Time format**

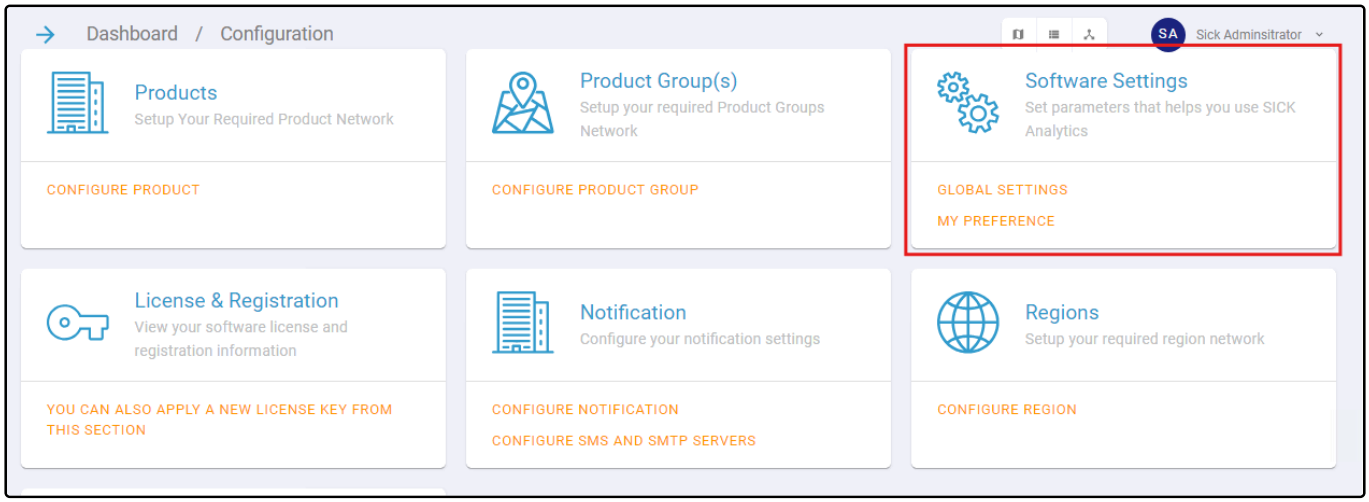


Figure 104

12.1 Global Settings

On the **Configuration** page, click on the **Global Settings** under the **Software Settings** section.

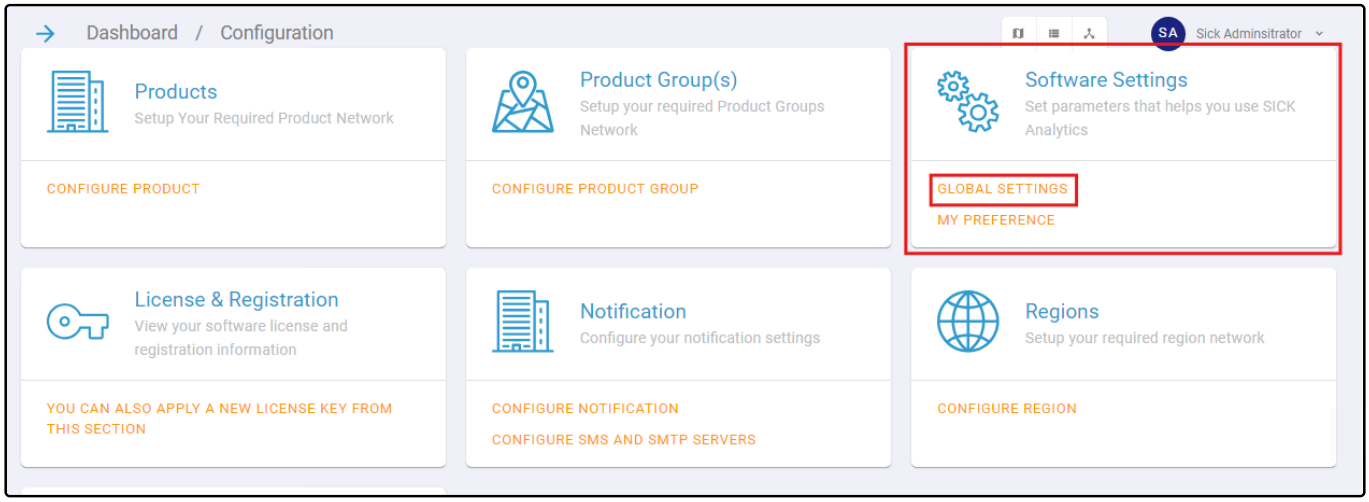


Figure 105

When user clicks on **Global Settings** under **Software Settings**, **Global settings** screen appears with following fields:

- **Date Format:** User can select the format of the date that user wish to appear from the drop-down
- **Time Format:** User can select the format of the date that user wish to appear from the drop-down
- **Week starts on:** Displays two options that are **Sunday** and **Monday**. Select any of the preferred option from the drop-down
- **Locale:** Select any of the locale language from the drop-down
- **Unit System:** Displays three options that are **Metric (mm)**, **Metric (cm)**, and **Imperial**. Select any of the preferred option from the drop-down

©SICK All rights reserved

- **Number of days to retain log files:** Select the number by clicking on arrows for retaining log files. Maximum number of days a user can retain log files is 30 days.

Click on **Save** button to save the settings.

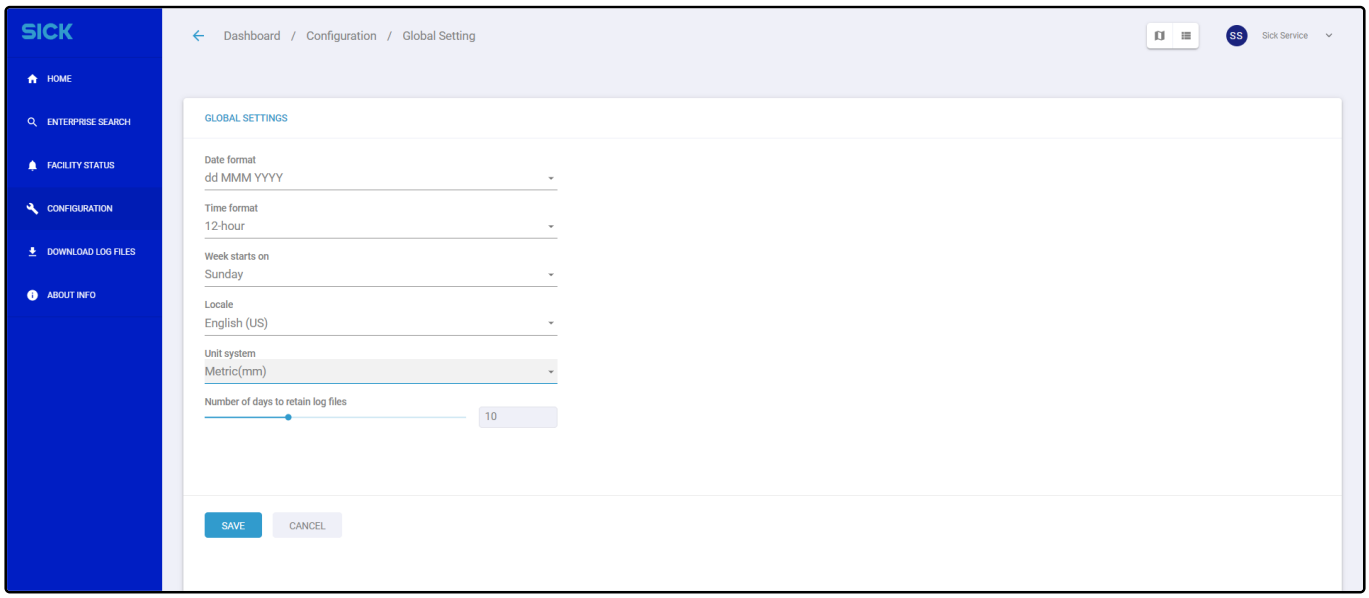


Figure 106

12.2 My Preference

User can select date and time formats, preferred language and unit from **My Preference** tab. On the **Configuration** page, click on the **My Preference** under the **Software Settings** section.

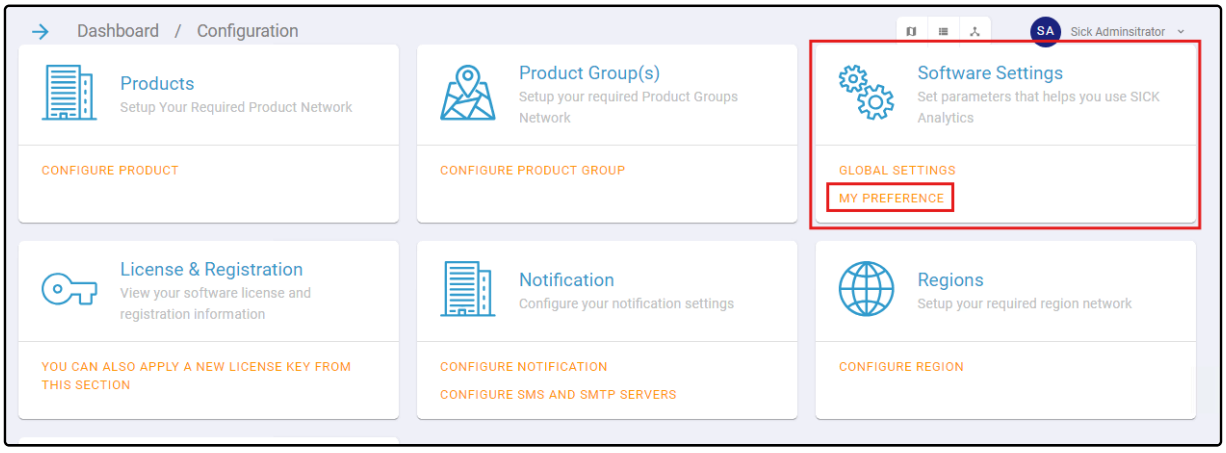


Figure 107

When user clicks on **My Preference** under **Software Settings**, **My Preference** screen appears with following fields:

- **Date Format:** User can select the format of the date that user wish to appear from the drop-down
- **Time Format:** User can select the format of the date that user wish to appear from the drop-down
- **Locale:** Select any of the locale language from the drop-down
- **Unit System:** Displays three options that are **Metric (mm)**, **Metric (cm)**, and **Imperial**. Select any of the preferred option from the drop-down

Click on **Save** to save the preferences.

©SICK All rights reserved

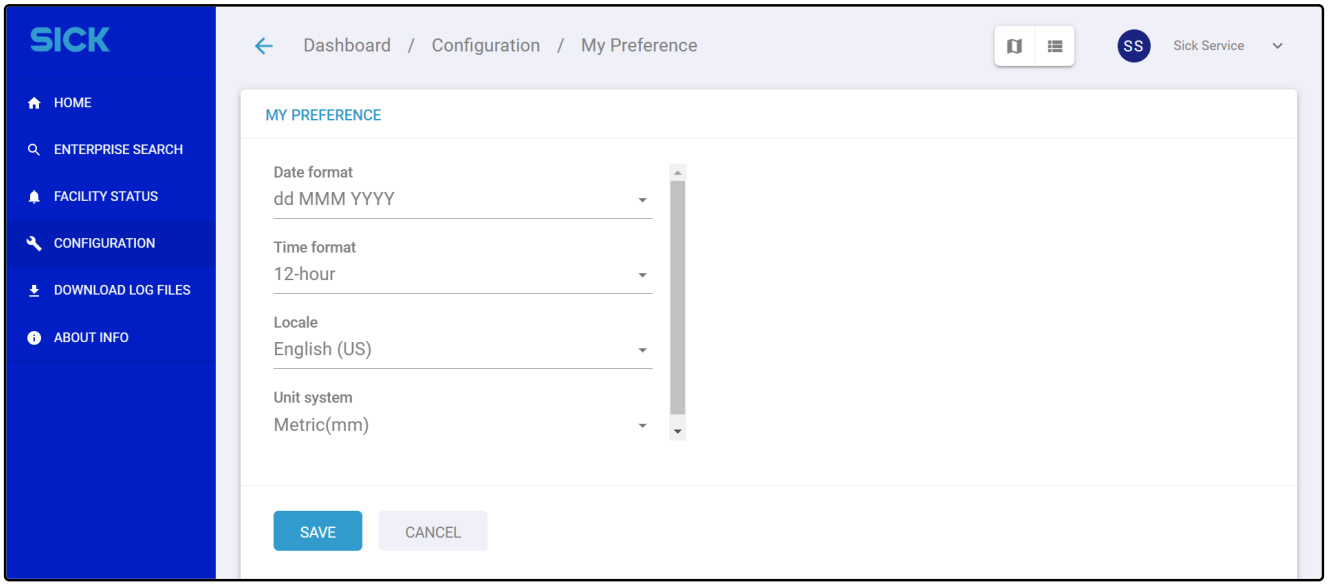


Figure 108

©SICK All rights reserved

13 Glossary

Code related condition	Evaluation Conditions which are code related monitor conditions for individual barcodes. For example, a code related condition may monitor if a barcode is a 2D barcode type. Because an object may have multiple barcodes, it is possible for a code related condition to have multiple outcomes for any one object. See also object related conditions
MQTT	Publish-subscribe-based messaging protocol which works on top of the TCP/IP protocol. This protocol is used to retrieve Facility data to EA.
Intelligent Sensor	Intelligent Sensors are devices which collect data and send to a central controller. These sensors include barcode scanners, dimensioners, and cameras, among others. Also referred to as devices
EA	Enterprise Application
auto ID system	All SICK systems which are part of the process of automatic data collection and identification for object processing, for example, camera tunnels and scan systems. Auto ID systems may consist of a network of data collection components, such as cameras, laser scanners, dimensioners, and scales, which work together to provide data on objects being processed through the system.
Device	A system component which collects analytical data which is transmitted to the Facility. Devices include CLVs, ICRs, MSC/SIMs Also referred to as Intelligent Sensor
device group	A logical grouping of devices, for example all CLVs or all ICRs. Devices may be grouped in order to enable collective reporting and analysis of the group.
Evaluation Condition	Evaluation Conditions are set in the SICK System Controller, which tags objects that meet criteria for a designated condition, for example, no read, or valid read. See also Performance Statistic.
Device [Group] Exclusive	Refers to exclusive reads; when only one device [group] has read a particular condition on an object
ICR	SICK's Image Code Reader, used for finding and detecting barcodes.
MAC	The system Media Access Controller (MAC) is a unique computer ID. It is used by PA to secure your software license to a physical computer.

Continued on page 89

©SICK All rights reserved

Continued from page 88

NORCA	No Read Code Analysis. A quality analysis for all readable and non-readable barcodes and 2D codes. This analysis is provided for the auto ID system's Lector cameras, and configured in the camera firmware. NORCA data is sent to Facility to allow filtering, evaluation and visualization of barcodes.
Object	Objects are items that are scanned by auto ID systems for data points, such as barcodes, weight, dimensions, and more.
object index	Identifier code for the current object sent from the system controller.
object related condition	Evaluation Conditions which are object related conditions evaluate conditions at the object level. For example, ValidDim or ValidWeight return a single outcome for any given object (e.g. ValidDim= yes or ValidDim= no). See also code related condition.
Performance Statistic	Performance Statistics are filters for pre-defined conditions or devices. Statistics represent a count of how many objects meet the requirements for a certain Evaluation Condition. See also Evaluation Condition.
read cycle	One read cycle is equivalent to the complete processing of an individual object, including the transmission of data from all system devices that recorded data for the object, to the SICK System Controller.
System	See auto ID system
Tunnel	An auto ID system which is configured as a tunnel system, with one or more reading devices mounted to a framework above, below, and to the side of tires, such as a camera tunnel. See also auto ID system.
web client	The client program which is used to launch EA. The web client opens the EA user interface using the Chrome browser by default.
Longterm Read Rate	Screens which provide a graphical analysis of your Facility's auto ID systems historical performance and operation.
moving average rate	The moving average rate is a succession of averages derived from the entered number of days. It helps smooth out fluctuations in the Primary Statistic read rate, and is an indicator of the current trend.
Current Results	Screens which provide a dynamic view of the real-time performance and heartbeat of an individual system. As objects move through the system and barcodes are read, an entry is added to the object data table on this screen, providing details.
Media Server	Images captured by the image capturing devices (ICR, Lector and IP cams) of the auto ID systems are stored in remote PC/server host where Media server is running.

Continued on page 90

©SICK All rights reserved

Continued from page 89

client computer	The client computer is any PC connected to the EA network. EA's client applications are Rich Internet Applications (RIA). The client applications connect to the EA Application Server to access rich data content and provide a powerful user experience.

©SICK All rights reserved

Enterprise Application