HITACHI
Inspire the Next

GRID AUTOMATION PRODUCTS

MicroSCADA X SDM600

User Manual

Hitachi Energy

Document ID: 8DCB000001
Issued: February 2024
Revision: B
Product version: SDM600 1.3.4 and newer

Table of contents

Section 1 Copyrights

We reserve the right to make technical changes or modify the contents of this document without prior notice. With regard to purchase orders, the agreed particulars shall prevail. Hitachi Energy does not accept any responsibility whatsoever for potential errors or possible lack of information in this document.

We reserve all rights in this document and in the subject matter and illustrations contained therein. Any reproduction, disclosure to third parties or utilization of its contents – in whole or in parts – is forbidden without prior written consent of Hitachi Energy.

The information in this document is subject to change without notice and should not be construed as a commitment by Hitachi Energy. Hitachi Energy assumes no responsibility for any errors that may appear in this document.

In no event shall Hitachi Energy be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, nor shall Hitachi Energy be liable for incidental or consequential damages arising from the use of any software or hardware described in this document.

This document and parts thereof must not be reproduced or copied without written permission from Hitachi Energy, and the contents thereof must not be imparted to a third party nor used for any unauthorized purpose.

The software or hardware described in this document is furnished under a license and may be used, copied, or disclosed only in accordance with the terms of such license.

Trademarks

ABB is a registered trademark of ABB Asea Brown Boveri Ltd. Manufactured by/for a Hitachi Energy company. All other brand or product names mentioned in this document may be trademarks or registered trademarks of their respective holders.

Guarantee

Please inquire about the terms of guarantee from your nearest Hitachi Energy representative.

Third Party Copyright Notices

List of Third Party Copyrights notices are documented in "*OS Licenses Overview*" under the installation directory.

Additional details could be found in the *OS License* folder under the installation directory.

Section 2 Introduction

2.1 Scope of the document

This document is the User manual for Hitachi Energy's MicroSCADA X SDM600 product. It provides information about the available features and how to configure SDM600.

Depending on the purchased SDM600 license, some instructions in this document may not be relevant or available.

2.2 Abbreviations and definitions

AAT	Application Administration Tool
CA	Certificate Authority or Certification Authority
CAM	Central Account Management
DR	Disturbance Record
FTP	File Transfer Protocol
FQDN	Fully Qualified Domain Name
GB	Gigabyte
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IP	Internet Protocol
kV	kilo Volt
LAN	Local Area Network
LN	Logical Node
PC	Personal Computer
RAM	Random Access Memory
RBAC	Role Based Access Control
RDRE	Logical node name for Disturbance Record
SA	Substation Automation
SCD	Substation Configuration Description
SDM	System Data Manager
SFTP	Secure File Transfer Protocol
SQL	Structured Query Language
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UI	User Interface
UNC	Universal Naming Convention
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VSA	Vendor Specific Attribute
XML	Extended Markup Language

2.3 Use of symbols

This document includes warning, caution and information symbols where appropriate to point out safety-related or other important information. It also includes tips to point out useful hints to the reader. The corresponding symbols should be interpreted as follows:

Warning icon indicates the presence of a hazard which could result in personal injury.

Caution icon indicates important information or a warning related to the concept discussed in the text. It might indicate the presence of a hazard, which could result in corruption of software or damage to equipment/property.

Information icon alerts the reader to relevant factors and conditions.

Tip icon indicates advice on, for example, how to design a project or how to use a certain function.

Although warning hazards are related to personal injury, and caution hazards are associated with equipment or property damage, it should be understood that operation of damaged equipment could, under certain operational conditions, result in degraded process performance leading to personal injury or death. Therefore, comply fully with all warnings and caution notices.

2.4 Document revisions

Revision	Version number	Date	History
B	1.3.4	12.02.2024	• Updated the Supervision section, describing the new functionality. • Updated the Troubleshooting section, providing additional support. • Updated several outdated screenshots to reflect the actual UI of the product.

Section 3 Product overview

SDM600 is a comprehensive software solution for automatic management of service and cybersecurity relevant data across multiple sites.

Under the SDM600's installation directory, in the *UserManuals* folder, it is possible to find the following documents:

- SDM600 User Manual (this document)
- SDM600 Installation Guide
- SDM600 Cybersecurity Guideline
- MS SQL 2019 Migration Workflow
- Active Directory Integration Workflow

3.1 Main functionality

SDM600 functionality can be grouped into three major areas:

1. Disturbance Recorder data management
2. Management of Cybersecurity related tasks
3. Service and Maintenance relevant data management and tasks

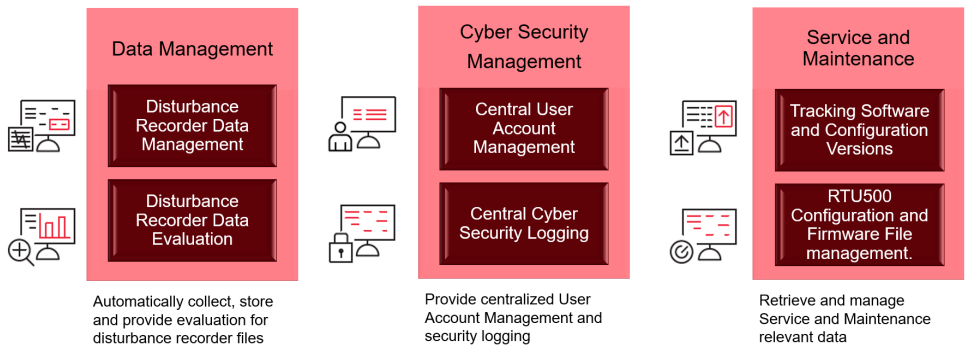


Figure 1: SDM600 High Level Functionality

SDM600 main functionality

SDM600 functions are licensed individually. This user manual describes the full product; therefore, certain features might not be available in particular installations due to the available license.

3.1.1 Disturbance Recorder data management

SDM600 collects Disturbance Recorder files from protection, control, or dedicated fault recorder devices supporting the COMTRADE format via standard file transfer interfaces. To retrieve the DR files, protocols like IEC 61850 (MMS), FTP, and secure FTP are supported.

Since SDM600 is based on open standards, many different device brands are supported. Both from Hitachi Energy and also a 3rd party.

The DR Files are collected automatically using a polling mechanism with a configurable polling time, which allows seamless integration into existing SA Systems.

3.1.2 Management of Cybersecurity related tasks

SDM600 provides a Central User Account management System based on IEC 62351-8. It supports a Role Based Access Control system for entire SA systems. This allows the definition of personalized users to access the components of an SA system based on predefined Roles.

CAM must be supported in connected devices via IEC 62351-8 (LDAP) or RADIUS protocol and requires specific configuration also in the device (for example, the definition of SDM600 as Authentication Server).

The second major functionality is the collection of Cybersecurity related events via the Syslog protocol. Devices must be configured to send the Syslog information to the SDM600 Server.

3.1.3 Service and Maintenance relevant data management and tasks

SDM600 can be used to collect Service and Maintenance relevant information from configured devices via IEC 61850, SNMP or a dedicated agent running on Windows computers.

Information such as installed firmware or configuration versions will be automatically and periodically read from the configured devices. This will provide an up-to-date inventory of deployed devices.

Moreover, for the Hitachi Energy RTU500 product family, SDM600 can be used to read and write configuration and firmware files from the configured devices.

3.2 Deployment variant

SDM600 can be deployed as a standalone, redundant, or hierarchical installation.

- It is recommended to plan the SDM600 installation carefully before doing any installation activities.
- When adding a redundant or hierarchical installation, certificates must be re-created, which could lead to the re-configuration of connected devices.

- To optimally operate SDM600, it is recommended to deploy the Microsoft SQL Server Standard Edition (an SQL Server Standard License is required). This ensures a larger amount of available permanent storage. Using a standard license is recommended for hierarchical systems.

- By default, SDM600 installation contains the free Microsoft SQL Server Express Edition, which has a limit of 10 GB per database. In larger installations, 10 GB may not be sufficient to store all the required data.
- In case of Microsoft SQL Server Standard Edition deployment is not an option, it is recommended to configure the Data Retention Feature in the Application Administration tool to delete older data from the database.

3.2.1 Standalone installation

In a standalone installation, SDM600 is installed on a single computer, accessing the configured devices directly via a LAN connection.

SDM600 can be installed together with other applications, however Hitachi Energy recommends using a dedicated computer to avoid any interference with existing applications. In addition, the user installing the system must ensure that the recommended performance criteria are met.

SDM600 is a server application and it may interfere with other server applications, such as SYS600. If possible, avoid installing SDM600 side-by-side with other server applications, see Figure 2. When this is not possible, be aware of the possible configuration clashes. For instance, if another web application is already installed on the same PC, the port for the SDM600 application can be changed using the IIS configuration tool on the PC.

Installing SDM600 side-by-side with other demanding applications (such as SYS600) may impact the user experience and/or overload the system. If possible, avoid installing SDM600 side-by-side with other demanding applications. If the situation cannot be avoided, make sure the HW performance criteria are met when installing SDM600 side-by-side with other applications.

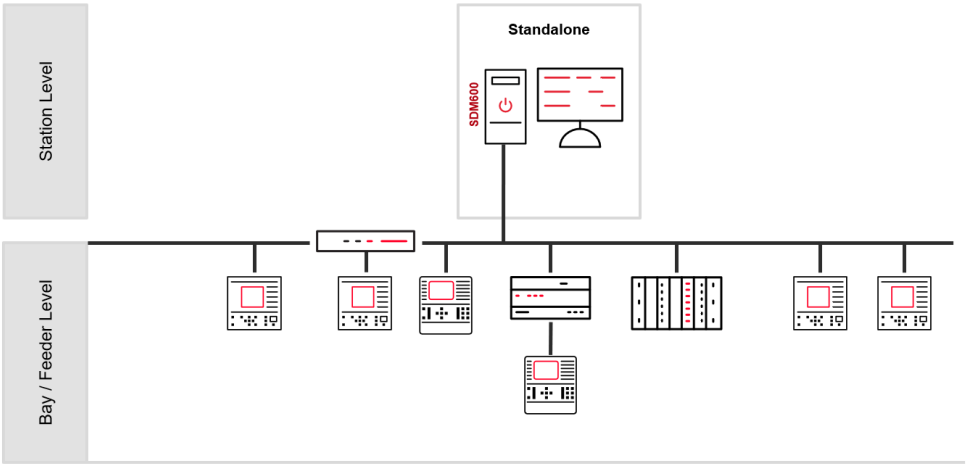


Figure 2: SDM600 Standalone Installation

3.2.2 Redundant installation

SDM600 supports redundant installation to increase the overall availability. Two independent SDM600 standalone installations will be paired to become one redundant system.

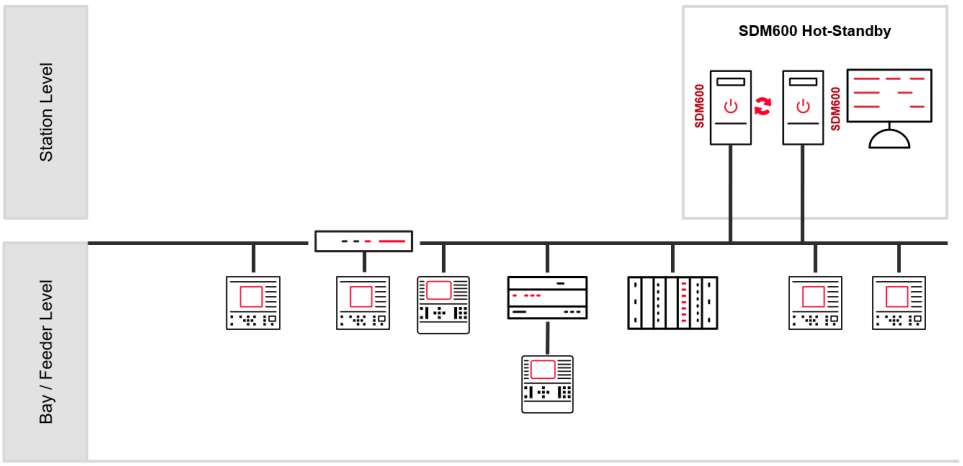


Figure 3: SDM600 Redundant Installation

3.2.3 Hierarchical installation

Using hierarchical installation, the overall capacity of SDM600 can be extended. Individual SDM600 installations, for example, per substation, can be connected to a higher-level system. The higher-level system will collect all the data from the underlying systems and provide an aggregated overview of the whole system.

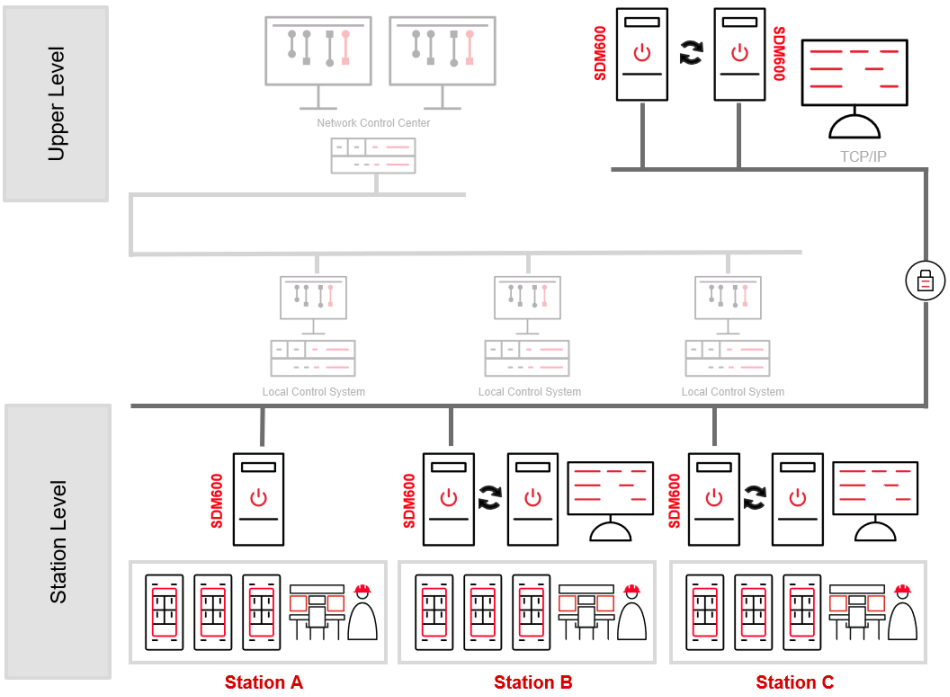


Figure 4: SDM600 Hierarchical Installation

Section 4 Accessing SDM600

SDM600 is a web application, therefore accessing the User Interface requires a web browser. Access can be done from the same computer where SDM600 is installed, or from a remote computer.

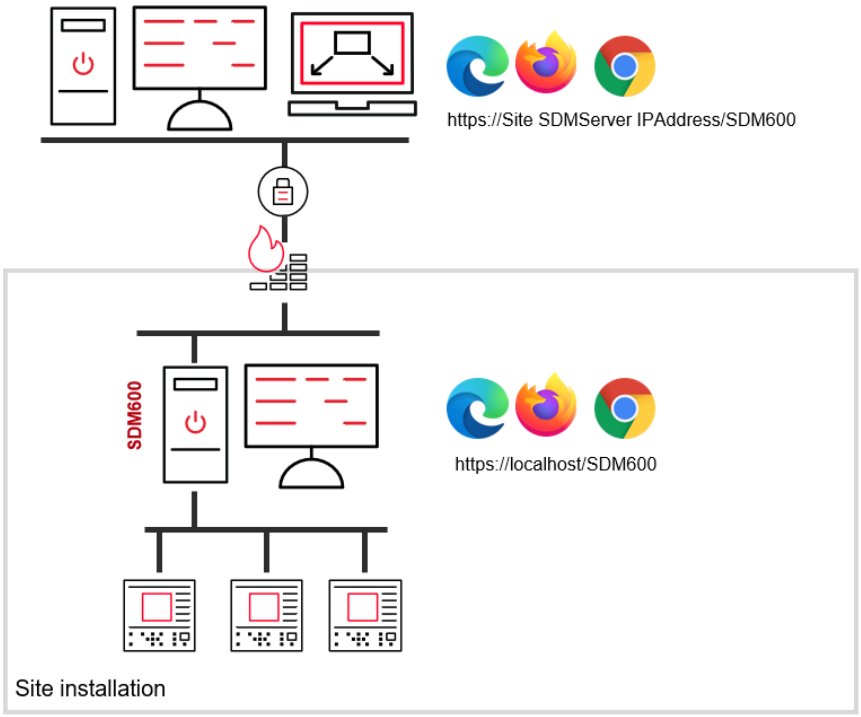


Figure 5: Browser Access to SDM600

- Accessing SDM600 over Remote Desktop Connectivity will increase the load on the server, impacting the overall performance of the server.
- Accessing SDM600 does not require Remote Desktop Connectivity. Only a web browser is required to use SDM600 from a remote server.

To open SDM600, type *https://IPaddress* (or *https://localhost* on the same PC) into the address bar of your browser. In case SDM600 is configured to be accessible via a different port, use *https://IPAddress:Port*, for example, *https://192.168.1.100:1010*.

4.1 Security settings

To establish a secure connection, on the first connection to the SDM600 server, your browser may issue a warning about the validity of the certificate that is used for encrypting the connection. The warning is issued because SDM600 uses a self-signed certificate. A self-signed certificate is an identity certificate that is signed by the same entity that issues the certificate. In this case, during the installation, SDM600 issues a self-signed certificate to establish TLS communication between the client and the server.

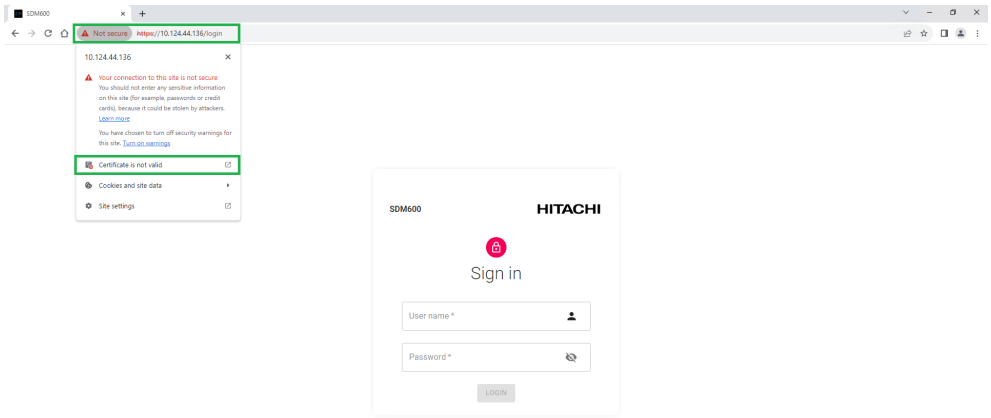


Figure 6: Certificate Warning

To trust the certificate on different computers, the certificate has to be imported. To do this, download the SDM600 certificates from the **Download** section of the **System Configuration** and run the import tool on the specific computer.

4.2 Login and Role Based Access Control

SDM600 supports RBAC and requires a user to login. When opening SDM600, a login page is shown. To get access, a user must enter valid credentials (username and password). Then, if the user is assigned more than one role, the user will be given the option to select the role to use to log into the SDM600.

Best practices in cybersecurity recommend the principle of least privilege. Therefore, if a user has more than one role, it is important to remember that the user should only login with a role that fits the tasks that are going to be done in that login session.

When only one role is assigned to the user, SDM600 will automatically select that role if the entered credentials are valid. Information regarding user management can be found in the section about Centralized Account Management.

4.3 Main navigation and filtering

The SDM600 application is divided into four major areas, which are selected by the navigation icons on the left side. Specific information is provided in the context area depending on the selected area.

Typically, all shown information is filtered by the selected structure and time axis.

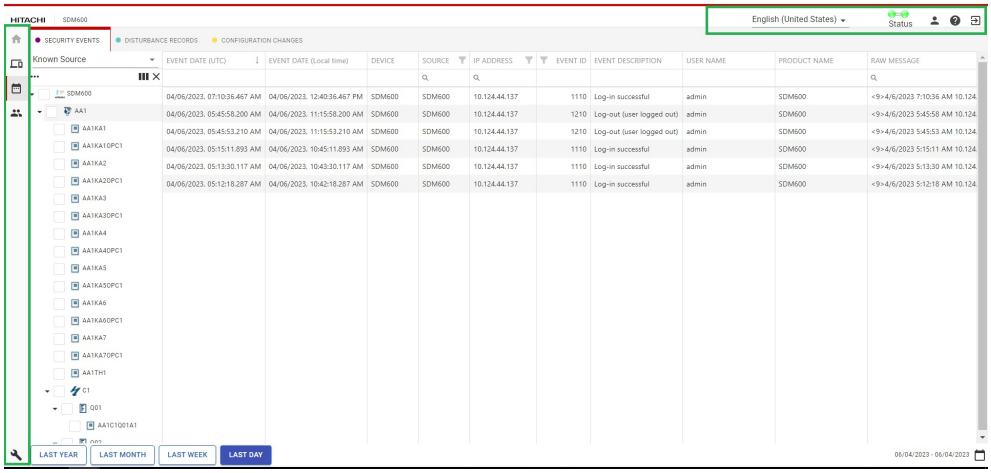


Figure 7: SDM600 main navigation

1. Main navigation / functionality
   - Dashboard: user can review the events dashboard, providing a comprehensive event-based timeline to track cybersecurity events, DR files, and configuration changes. The evens dashboard allows users to gain insights into what happened, when, and where in the system.
   - Devices : user can view and collect information related to the Devices.
   - Event Monitoring: user can download or view events.
   - Account Management: user can manage Users and permissions.
   - SDM600 Configuration: user can manage and configure the SDM600 Installation.

2. Tabs showing the different data for the selected main functionality.
3. Context specific data.
4. Header and status information.

There are context-specific actions throughout the application. These can be triggered by expanding the **Actions** button and clicking on a specific button.

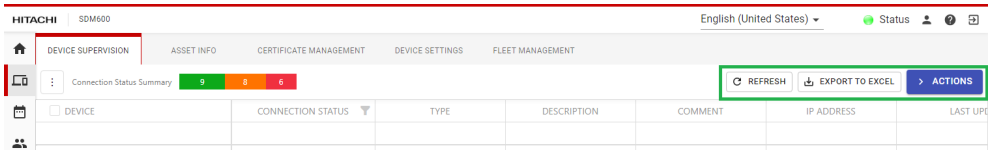


Figure 8: Actions button

Section 5 Features

The following sections describe the individual SDM600 features and their configuration.

When configuring SDM600, please perform the following steps in the provided order.

1. Configure Hierarchy, if required
2. Configure High Availability (Hot-Standby), if required
3. Configure Central Account Management
4. Continue with the remaining configuration

Adhering to the ordered steps ensure the maximum efficiency while configuring SDM600.

When enabling Hierarchy and/or Hot-Standby, configuration and/or live data will be replicated among the SDM600 instances. Configuring Hierarchy and/or Hot-Standby on a system with data already collected will lead to longer replication time: all the data already collected in the system must be replicated on other instances. To avoid long waiting time due to replication, it is recommended to setup Hierarchy and/or Hot-Standby at the very beginning, before configuring SDM600 for data collection.

5.1 Hierarchical systems

Individual SDM600 installations, for example, per substation can be connected to a higher level system. The higher level system will collect all the data from the underlaying systems and provide an overview of the whole system.

It is important that the Windows Operating System time between an SDM600 parent and an SDM600 child is synchronized. For instructions, see the Windows Operating System user manual.

For Hierarchical functionality, both SDM600 system must communicate using various TCP/IP based protocols and ports. Ensure that Firewalls are configured accordingly.

Recommended installation sequence

Creating a Hierarchical setup should be planned carefully to avoid additional rework afterwards. Specifically, when Central Account Management for Devices is enabled, converting an existing SDM600 to a child system might result in re-configuration of the connected IEDs.

Before attempting to configure a Hierachical system, ensure the SQL Database Password of the two SDM600 instances are identical. You can use the Application Administration Tool to check the current password and change it if required.

It is recommended to back up the SDM600 child before establishing the hierarchical structure. In case of an unexpected result, it is easier to restore the configuration.

Child system configuration

The SDM600 structure has to be defined in each SDM600 system individually. For example, each child system's structure must be configured in the respective child.

Pushing a configuration from a Parent system to a Child is not supported.

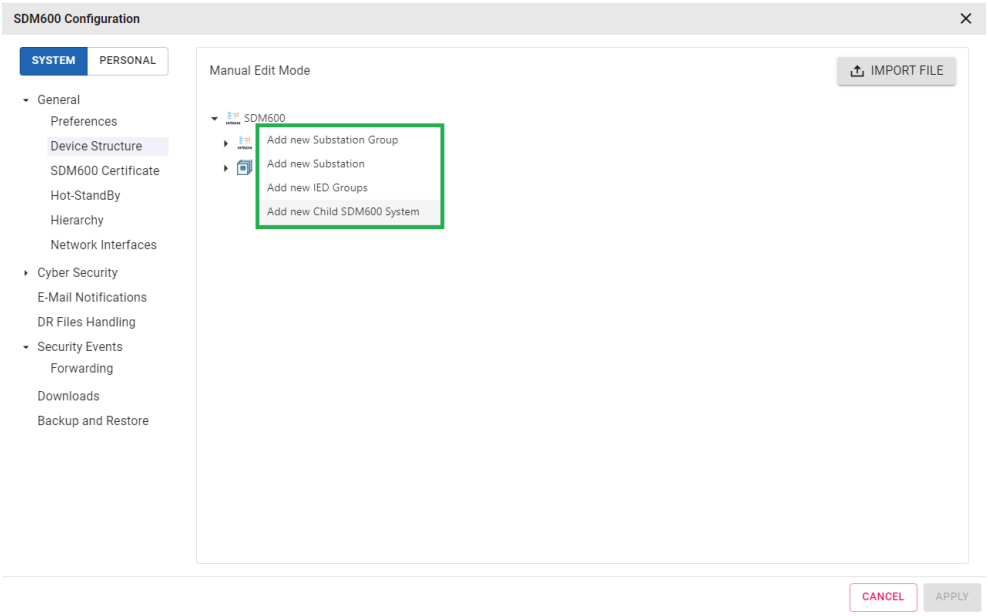


Figure 9: Child System
Manually adding devices on the child system.

Integration of an SDM600 child system to a parent

1. Select Hierarchy Configuration in the System Configuration of the Child.
2. Enter a Shared Secret that will be used later on the Parent System.
3. Initiate the Communication.
4. On the Parent System, open the **Device Structure** in the **System Configuration** tab.
5. Right Click on the **SDM600 Node** and select **Add new child SDM600**.
6. Enter a **Name** and a **Description** (optional) for the Child system.
7. Enter the Required Addressing Information (IP Address, Custom Port is only required if the default port was changed).
8. To connect both systems, enter the current Administrator User and Password of the Child System.
9. Enter the same Shared Secret as used in the Child system.
10. Click **Add**.

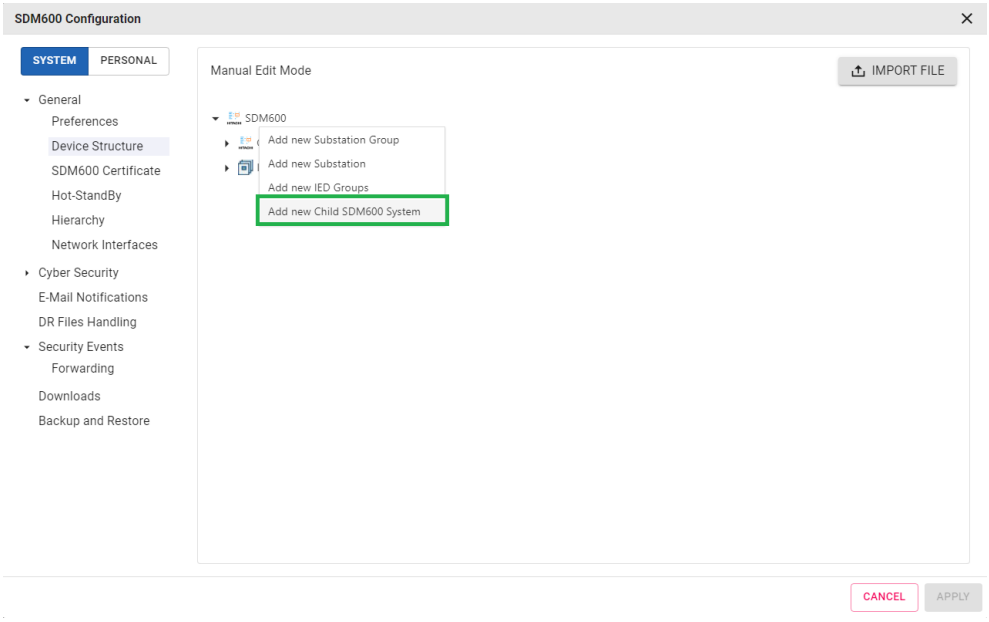


Figure 10: Parent System

When setting up the SDM600 hierarchy, it is important that the network connection between the SDM600 parent and child is not disturbed. If there is a disturbance, transporting the SDM600 child package may fail, or the SDM600 parent may not receive feedback from the SDM600 child. In this case, it can be seen on the SDM600 parent that the establishment of the hierarchy fails.
In addition, as the configuration file changes the behavior of the SDM600 child, all related SDM600 services on the SDM600 child are restarted. In general, restarting of the services should work fine. If it fails, the SDM600 parent receives a notification that the establishment of the hierarchy has failed.

If the establishment of the hierarchy has started and failed, it is also possible that the SDM600 child can no longer be accessed using the original user accounts. This is because the user management part of the SDM600 child has been successfully integrated into the SDM600 parent's centralized account management. Therefore, the user can try to log in with a user from the SDM600 parent.
When the establishment of the hierarchy fails, it is not possible to directly add the same SDM600 as a child. At this stage, it is important to revert the SDM600 child to a standalone SDM600, log out from parent and child, and log in again before trying to establish the hierarchy again.
Notice that replication between parent and child may take time. It is strongly recommended to wait about 5 minutes before logging into SDM600 after hierarchy relation is established.

After establishing a hierarchy relationship between the SDM600 parent and child, the following behavior is expected of the SDM600 child. As the account management functionality at the SDM600 child is now integrated to the SDM600 parent, it is no longer possible to manage users on the SDM600 child. Also, any user changes that are made at the SDM600 parent are reflected directly on the SDM600 child.

When the hierarchy structure is established between the SDM600 parent and child, the centralized account management of the SDM600 child is integrated to the SDM600 parent. This implies that any user account previously created on the SDM600 child is no longer available. The user accounts on the SDM600 child will be the same as on the SDM600 parent. Any account changes made on the SDM600 parent will automatically be reflected on any SDM600 child. In addition to that, all centralized account management certificates created on child must be regenerated and uploaded to devices.

The parent synchronise data by sequentially polling data from the child systems: periodically the parent queries each child system for new available data, one-by-one.
The polling cycle time (in minutes) is configurable on the parent system, under the Hierarchical tab in the System Configuration. The smaller the value, the more often the parent system will poll the child systems for new data. The minumum allowed value is 1 minute.
When configuring the polling cycle time, consider that there is trade off between cpu/memory/network footprint and update rate. Configuring a smaller polling cycle time will upload data from the child to the parent more frequently and quicker, but it will increase the cpu, memory and network consumption due to increased processing power and communication. Configuring a larger polling cycle time will increase the amount of time required for the events to be available on the parent once they're available on the child system, but it will reduce the footprint on memory, cpu and network.

Removing a child SDM600 from the parent

If a user would like to remove the hierarchical relationship between the SDM600 Parent and one SDM600 child system, the user should remove the child instance entry from the SDM600 Parent. This can be done by following the below steps:

1. Navigate to the **Parent System/SDM600 Configuration/Device Structure**.
2. Navigate to the **Navigation Reference Area** and click the SDM600 child unit that is to be deleted.
3. Right-click on the child unit and select **Delete**.
4. The child system will be successfully deleted from the parent system.

Depending on the size of the database, this operation might take several minutes.

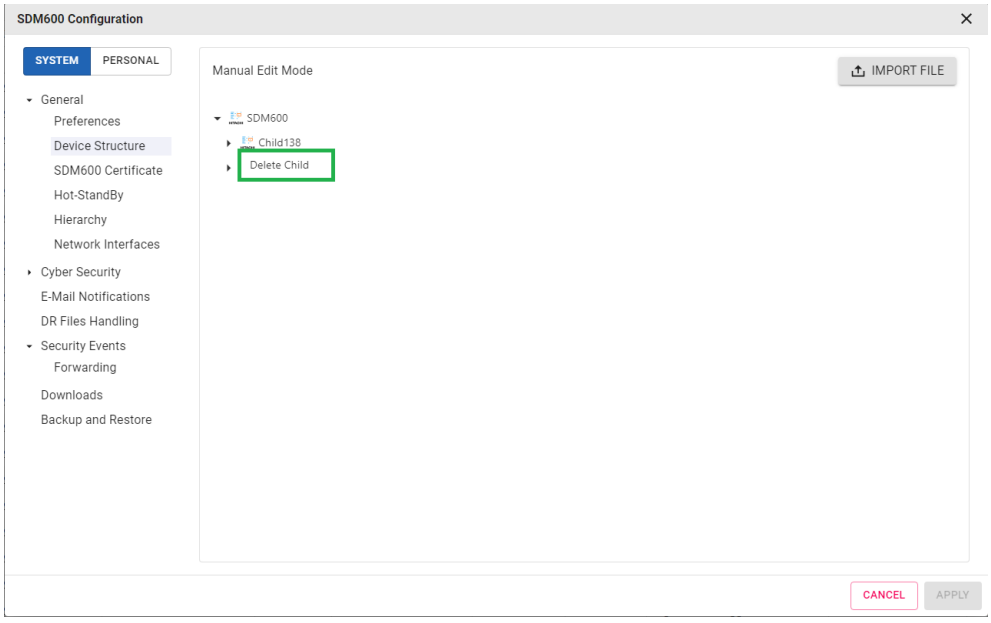


Figure 11: Parent Child Disconnection

Reverting the child system to standalone

The Revert to Standalone Configuration functionality is not the indended and suggested workflow to break the hierarchical communication between the parent and the child system.

The Revert to Standalone Configuration functionality is intended to be used only when, regardless of the cause, the Parent system is not available.

If the parent system is available, the recommeded workflow to remove the hierarchical connection is to remove the child from the parent system, as documented in the section above.

It is possible to remove the hierarchical connection from the child system, if the parent is not available.

1. Select **Hierarchy Configuration** in the **System Configuration** of the Child.
2. To revert the state of an SDM600, click **REVERT TO STANDALONE CONFIGURATION** button. Enter the SDM600 administrator username and password. After this, restart the PC.

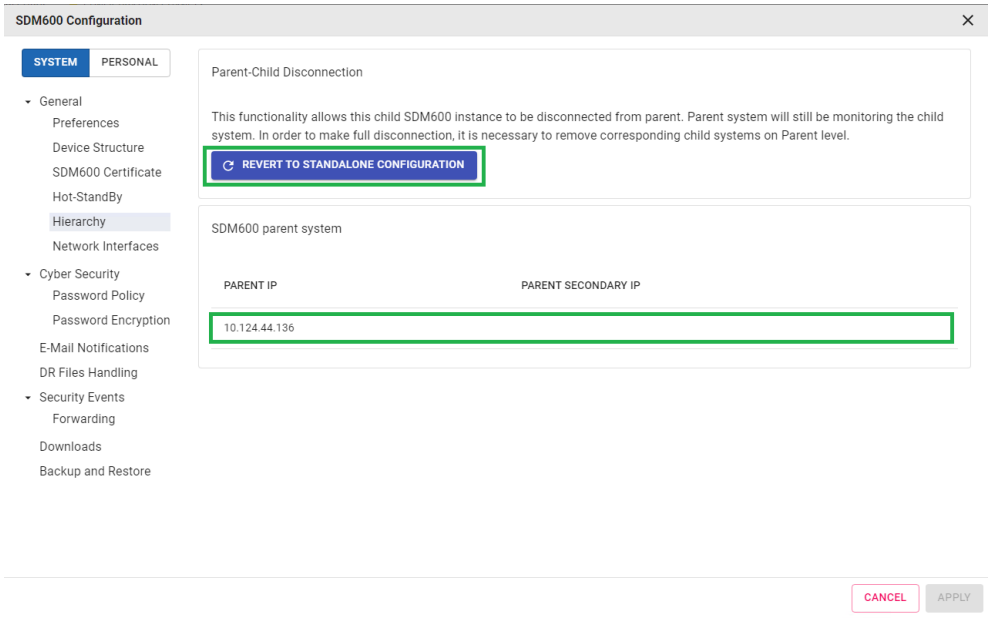


Figure 12: Parent System Disconnection from the Child

If a child has been successfully removed from the parent, the Revert to Standalone Configuration functionality will not be available.

After the reversion, the SDM600 parent will no longer be able to connect to the SDM600 child. Furthermore, the user account management on the SDM600 child is no longer synchronized with the SDM600 parent.

If Revert to Standalone Configuration was triggered, the child system will not be automatically removed from the Parent. From the Parent perspective, the child will simply appear as not reachable. To perform a clean termination, the child system must be removed from the parent system.

The Revert to Standalone Configuration functionality is a critical function and should be executed with extra care. Therefore, only an SDM600 administrator can perform such a function by means of extra authentication. This implies that, even if users are granted access to the SDM600 configuration, they do not necessarily have the right to execute this function. When clicking the button, an additional user verification dialog is shown. The user must enter the SDM600 administrator credentials. Only if the authentication is successful, the revert function is executed.

5.2 High availability

SDM600 offers hot standby functionality to increase the overall availability of the SDM600 system through a failover mechanism. Both SDM600 systems in a Hot-Standby Configuration operate actively. If any key component in one system fails, the other SDM will continue the operation seamlessly. High availability supports:

- Fully automated synchronization of all relevant data between both units.
- Integrated self-tests for checking system status.
- Automatic failover if internal errors are detected.

User Login is limited to one SDM600 system in a Hot-Standby system at any time. Users can logout from one SDM600 system and login on the other SDM600 System.

After configuring hot standby functionality, all data from the hot unit will be replicated to the standby unit. It means that all the existing data on standby unit will be replaced by data from the hot unit.

For Hot-Standby functionality, both SDM600 systems must communicate using various TCP/IP based protocols and ports. Ensure that firewalls are configured accordingly.

It is important to back up the SDM600 before establishing the hot standby relationship. In the event of an unexpected result, it is easier to restore the configuration.

Hot-Standby functionality is configured in the System Configuration. Both SDM600 must be available to connect them.

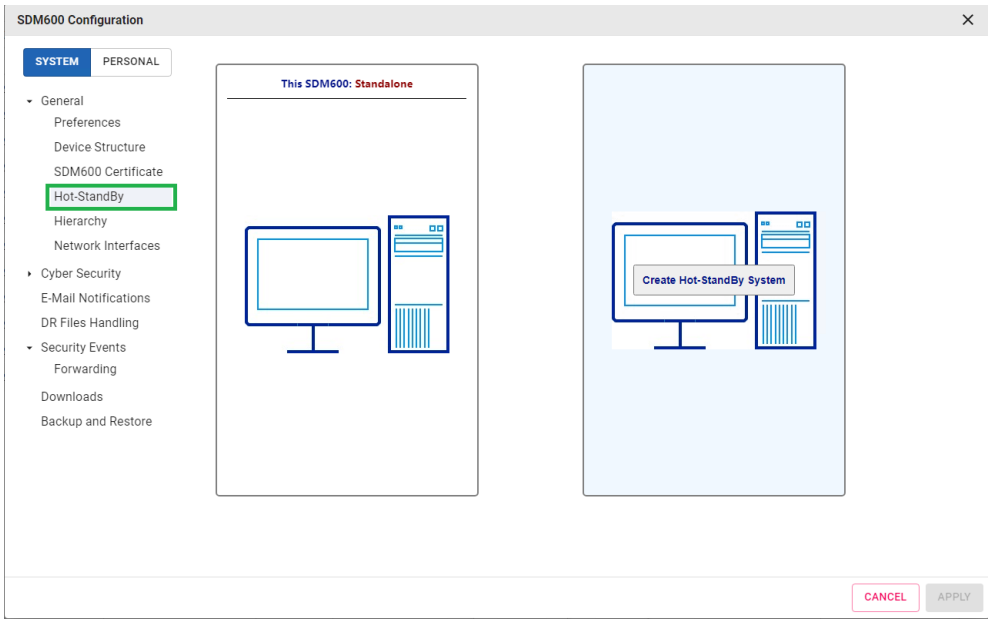


Figure 13: HSB Configuration

Before attempting to configure Hot-Standby, ensure the SQL Database Password of the two SDM600 instances are identical. You can use the Application Administration Tool to check the current password and change it if required.

To setup HSB, follow the steps below:

1. Open the Hot-Standby Configuration on both computers.
2. Select the existing configured System to become initially HOT.
3. Select the 2nd system to become Standby.
4. Enter the shared Secret on the HOT System.
5. Select the Validity Period for the connection.
6. Enter the Shared Secret on the Standby System and Connect the systems.

Right after enabling Hot-Standby configuration, the whole database (configuration and live files) of the hot system will be replicated on the standby system. Depending on the size of the database files, the replication process may take some time. Until the replication is finalised, the Hot-Standby is not fully operable.
To avoid long waiting time due to replication, it is recommended to setup Hot-Standby before configuring SDM600 for data collection.

Once the Hot-Standby setup has been established, it is possible to monitor the status of systems at any time on the SDM600 banner.

The STATUS icon signals the overall status of the Hot-Standby system:

- Red Light - Green Light: The partner system is reporting an issue, therefore is displayed as red. This situation must be addressed, as the High Availability of the system might be compromised. Please, continue reading through this user manual, as there are common transient situation leading to the partner system to be detected as red. If the problem persists, please contact the Support Team.
- Green Light - Green Light: Both the hot and the standby system are healthy, up and running. If any system was to face issues, the other one will be still available to collect and visualise data. This is the expected operative scenario: both systems operational.

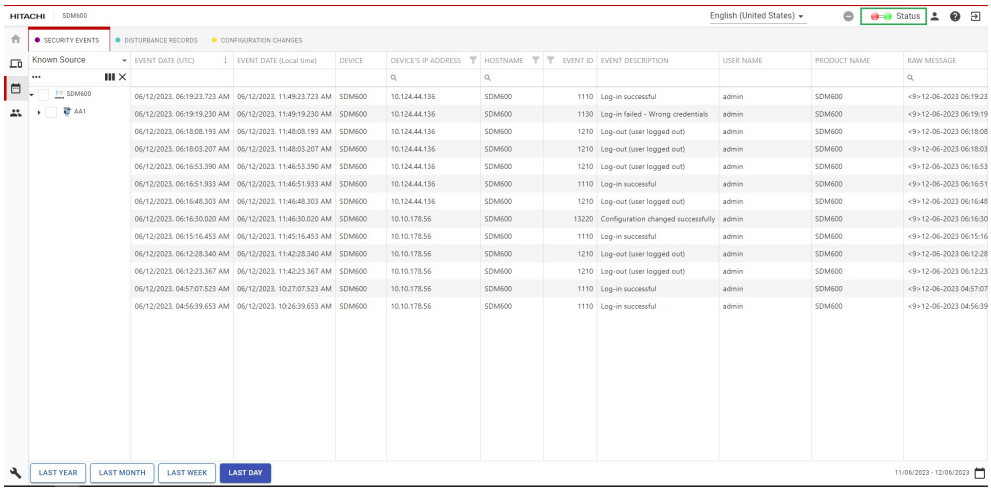


Figure 14: SDM600 HSB Status indicator

Red Light - Green Light Indicator signals an issue in the Hot/Standby System

Additionally, SDM600 provides information regarding the status of the data synchronization between the hot and the standby system. Data synchronization is the operation of replicating data among the Hot-Standby systems, to prevent data loss.

Synchronization Status Unknown: this is the initial state shown before SDM600 starts performing the first synchronization. After the synchronization has been performed, the status will be updated to either to **Synchronization Finished** or **Synchronization Failed**. This is a normal status.

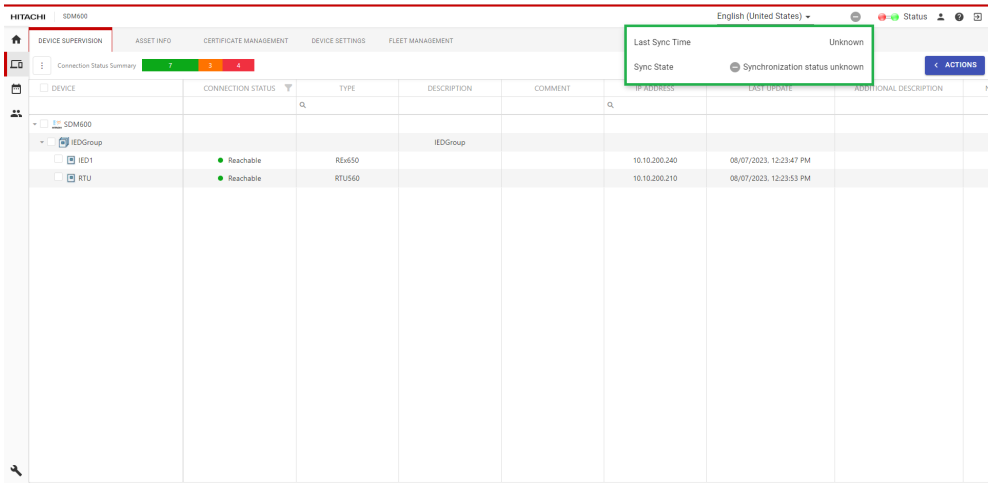


Figure 15: HSB Synchronization Status

Synchronization status is not known

- **Synchronization in Progress:** SDM600 is synchronizing data between the two instances. While data are being synchronized, mismatch must be expected in the data visualised on the two systems, because the replication is not over yet. This is a normal status.

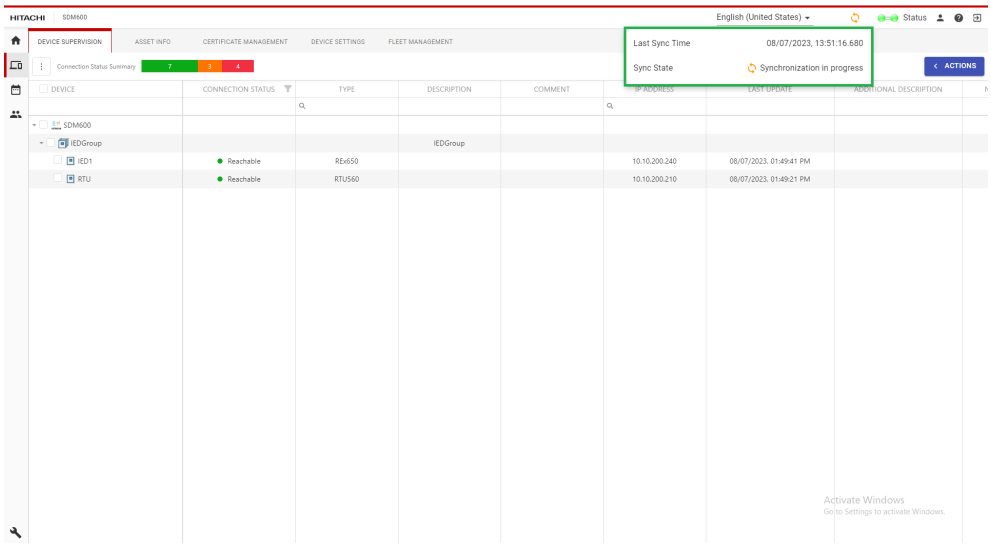


Figure 16: HSB Synchronization Status
Synchronization is currently in progress

- **Synchronization Finished:** all the data available on the hot system have been synchronized to the standby system. This is a normal status.

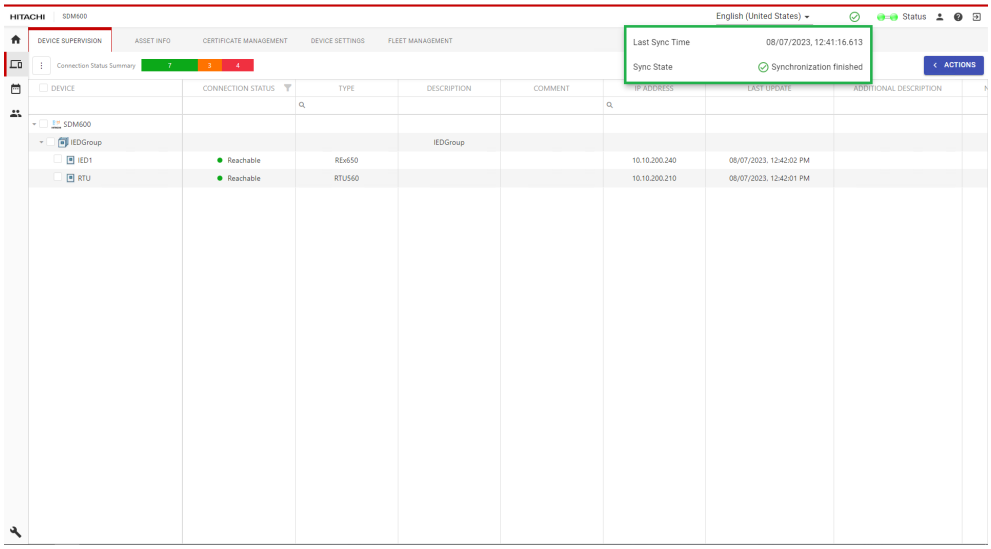


Figure 17: HSB Synchronization Status
Synchronization has finished

- **Synchronization Failed:** SDM600 reports an error in the synchronization. This is an error status. If the problem persists, please contact the Support Team.

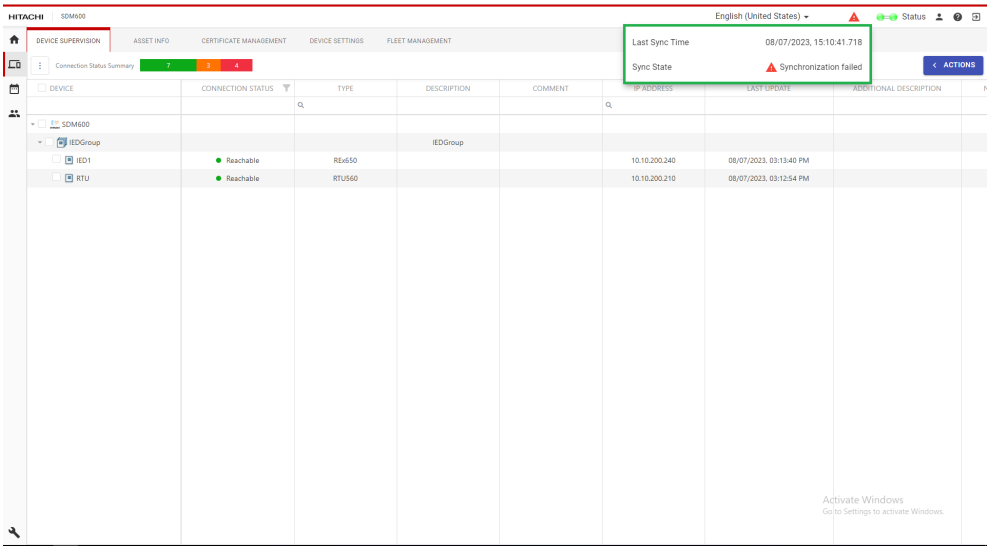


Figure 18: HSB Synchronization Status
Synchronization has failed

It is important to highlight that Hot-Standby synchronization is a periodical operation, therefore the status is expected to fluctuate between **Synchronization in Progress** and **Synchronization Finished**.

The **HSB Synch Status** indication is important after establishing Hot-Standby or updating to a new SDM600 version, to keep track of the status of the data replication. Until the data replication has been finalised, the Hot-Standby is not fully operative.

To revert the system to standalone, follow the steps below:

1. Login into the Hot System.
2. Navigate to **SDM600 Configuration/ Hot-StandBy**.
3. Click the **Revert to Standalone SDM600** button.

Depending on the size of the database files, deletion may take some time.

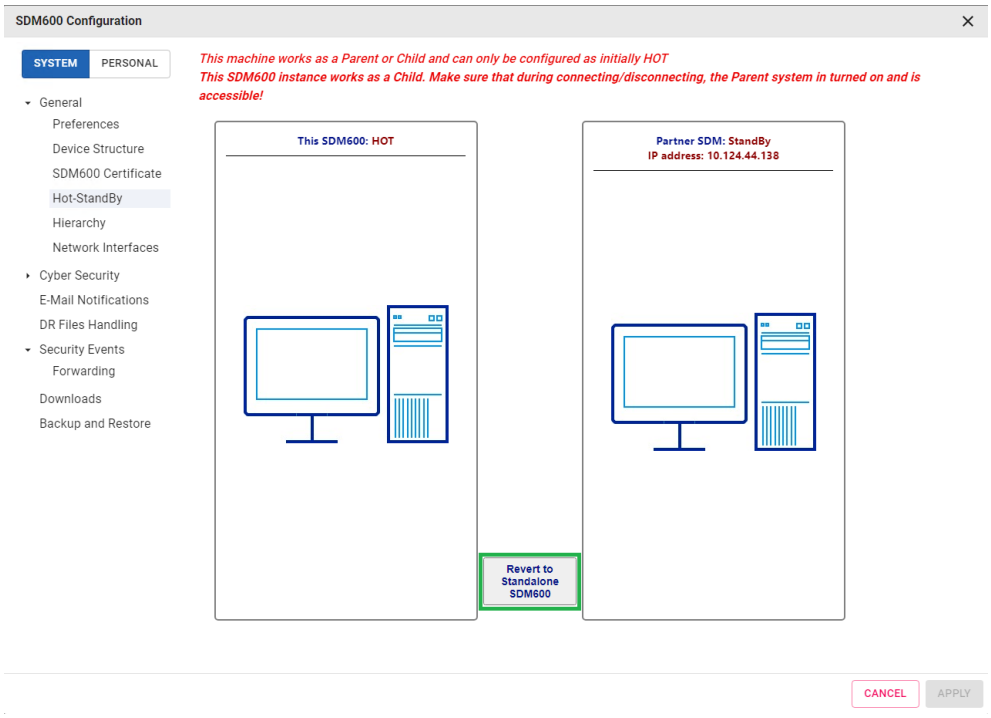


Figure 19: Hot-Standby disconnection

After disconnection, restart the partner machine (formerly standby).

Removing the Hot-Standby configuration must be done with extra caution. Disabling this feature means the SDM600 returns to a standalone mode, and thus, there is no backup when the installed SDM600 is encountering problems. It is recommended to create a backup after a successful Hot-Standby disconnection.

5.3 Central Account Management

SDM600 can be configured to either act as Authentication and Authorization Server, or to integrate against existing Active Directory servers. One configuration excludes the other: SDM600 is either completely managing the users and acting as an authentication and authorization server, or it is performing authentication and authorization against Active Directory.

When configured to act as Authentication and Authorization Server, SDM600 provides Central Account Management (CAM) functionality to manage users for the entire SA system and therefore defines the access to different devices and applications. Users are defined and managed from SDM600, allowing system-wide authentication. The definition of the access level follows a Role Based Access Control concept, where individual users get at least one role assigned. The role will then be interpreted in the individual device or application during the authorization process and translated into specific user rights. Since in this configuration SDM600 is the official authentication and authorization server for the system, it must be ensured that the devices can communicate with the SDM600 computer using various TCP/IP based protocols such as LDAP or RADIUS. Ensure that firewalls are configured accordingly.

To enable SDM600 CAM for devices or applications, configuration changes in the devices are required. This user manual does not describe the settings for individual devices, but gives a general overview of the functionality. The product specific settings are described in the respective product manuals.

Alternatively, when SDM600 is configured to authenticate and authorize users against Active Directory, SDM600 will act as any regular device and authenticate the users against the Active Directory accounts. Multiple Domain Controllers can be configured to increase the availability. Local Users, also known as Emergency Users, are also available in SDM600 to ensure access to the system in the event that the configured Domain Controllers are not available/reachable. Central Account Management for devices is not supported when SDM600 is configured to authenticate against Active Directory: SDM600 is not acting as a proxy for Active Directory. SDM600 does not provide any functionality to create, delete or edit Active Directory accounts or groups. The definition of the access level follows a Role Based Access Control concept, where an individual Active Directory group is mapped to at least one role.

When configured to integrate with Active Directory, SDM600 does not act as proxy for other devices to authenticate against Active Directory.
SDM600 will not forward authentication requests from other devices to Active Directory.

Once SDM600 is configured to use Active Directory, Local Users (also known as Emergency Users) will be only used if the configured Domain Controllers are not reachable.
SDM600 will not fallback to Local Users if invalid Active Directory credentials are provided during login.

5.3.1 General settings

In general, all configuration and user data will be synchronized between hierarchical and redundant SDM600 installations. Differences apply based on whether SDM600 is configured to integrate with Active Directory or not.

In order to modify the Active Directory configuration, users must have SDM600 Configuration modify rights.

SDM600 can either be configured to be integrated with Active Directory or to act as Authentication and Authorization Server - not both at the same time.

SDM600 integrated with Active Directory

Active Directory integration is by default not enabled: this means that by default, SDM600 will use Local Users.

Due to technical limitations, Hierarchical and Hot/Stanby must be configured before enabling Active Directory.
Finalise the Hierarchical and Hot/Stanby before configuring the Active Directory.

To configure Active Directory integration, navigate to the Account Management section and open the Active Directory Configuration tab.

To facilitate the configuration of Active Directory in SDM600, a dedicated workflow document can be downloaded directly from the SDM600 user interface, by clicking on the information icon. The *Active Directory Configuration Workflow* document will provide the user a step-by-step guideline on how to efficiently and effectively configure Active Directory.

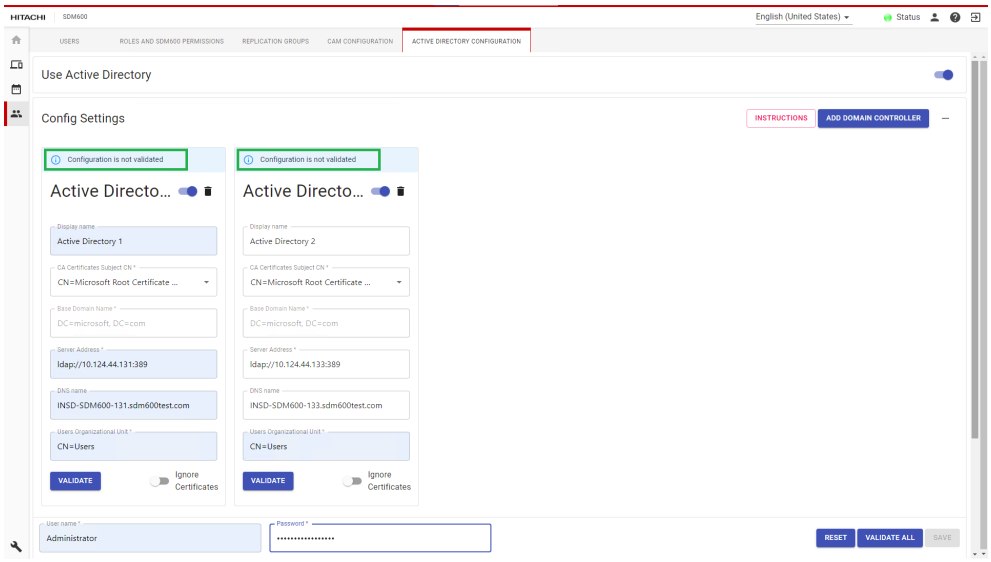


Figure 20: Active Directory Configuration tab

The following section provides a brief highlight on the Active Directory aspects that can be configured in the SDM600 user interface.

For a step-by-step guideline on how to configure Active Directory, please refer to the *Active Directory Configuration Workflow*.

- **Use Active Directory**: this slider works as a global switch to enable or disable the usage of Active Directory. In order to start configuring and using Active Directory, the slider must be enabled. To turn off the usage of Active Directory, simply disable the slider. Turning off the usage of Active Directory using the slider will preserve already configured settings for future use.

- **Domain Controller Configuration**: this section allows the user to configure the Domain Controllers. For each Domain Controller the user can enter an arbitrary Display Name, select the matching certificate, and configure the Server Address, DNS Name the Users Organizational Unit.
  - ServerAddress - SDM600 supports configurations in the following format: 'ldap(s)://[ip or hostname]:[port]'.
  - Users Organizational Unit - it is an LDAP container where to search for users, by default it is 'CN=Users' (meaning container with Common Name 'Users'). Alternatively, a custom Organization Unit could be configured, e.g. 'OU=MyUsers'. Only one value is allowed.

  A domain controller can be permanently removed by clicking on the trash bin icon.
  Alternatively, if you want to keep the configuration but disable the usage of a given domain controller, it is possible to disable it by using the corresponding slider. A disabled Domain Controller is still visible in the user interface, but SDM600 will not use it.

- **Role Mappings**: this section allows the user to configure roles assigned to a specific Active Directory group. When SDM600 is configured to use Active Directory, the role assignment is specified at Active

Directory group level: all users belonging to an Active Directory group will be mapped to the user configured roles.

Users belonging to Active Directory groups, for which no role mapping has been configured, will not be able to login to SDM600.
This functionality is driven by cybersecurity principles, ensuring that access to the SDM600 system is allowed only to users belonging to explicitly configured Active Directory groups.

In order to save the existing configuration, at least one role mapping must be specified. When editing the Role Mappings, beware of typos when entering the Active Directory group name.

- The **Validate** button allows the user to verify the current configuration by trying to login. The test will check whether each of the configured Domain Controllers can be reached and the authentication/ authorization can be performed with the provided username/password and the configured role mapping. The test result is displayed on each Domain Controller, to provide clear guidance to the user. The **Test** button is disabled as long as all the required settings to perform the test has been entered by the user. When testing whether a connection can be established with the Domain Controller, it is possible to Ignore Certificates.

Ignore Certificates can only be used for testing purposes, to help troubleshoot network or certificate issues. SDM600 will only use secure communication.

- The **Save** button allows the user to commit the changes. In order to be able to save the changes, a test must be performed and successufully passed: the **Save** button will be enabled only after a configuration has been succesfully tested. After a test has been successfully passed, any further

change will invalidate the testresult, preventing the user from saving the changes. Upon changing the configuration, all logged in users will be logged out, because the sessions will be invalidated.

- The **Reset** button allows the user to discard any unsaved change and revert back to the last saved configuration.

Due to the far reaching consequences of improper configuration of Active Directory, auto save functionality is not available for this page. Changes must be manually saved for them to be persisted.

For hierarchical installations, Active Directory must be configured on each instance independently.
For hot/standby installations, Active Directory must be configured on the hot instance; the configuration will then be fully replicated to the standby instance.

For hierarchical installations, the Domain Controllers configured in the parent system will not be synchronizated to the child instances. Rationale: hierarchical instances are likely to belong to different network segments, making it not realistic for all the instances to access the same domain controllers.
For hot/standby installations, the Domain Controllers configured in the hot system will be synchronized to the standby instance.

Local Users (or Emergency Users) will be synchronized between hierarchical and redundant SDM600 installations. In case of hierarchical setup, as usual, user creation is only enabled on the parent system.
Once Active Directory is enabled, users must use an Active Directory account to log into SDM600. The editing (creation, modification, deletion) of Local Users (or Emergency Users) will be disabled for users authenticated against Active Directory. Before enabling/configuring Active Directory, it is highly recommended to finalise the creation of all the envisioned Local Users.

Groups to Role Mapping will be synchronized for hot/standby installations, whereas it needs to be manually configured on all the hierarchical instances.

On an instance where SDM600 is configured to act as Authentication and Authorization Server for devices and applications, enabling Active Directory integration will cause the CAM for devices functionality to stop working. Users might not be able to log into existing devices, because the functionality has been disabled.

SDM600 acting as Authentication and Authorization Server

The CAM functionality must be enabled for the different network interfaces on the SDM600 computer. A refresh is required in the case where not all network interfaces are listed. Enable the CAM functionality on all network interfaces that are connected to devices. Hierarchical and redundant SDM600 installations require CAM to synchronize user accounts to ensure that the corresponding network interface is enabled and configured as the default.

It is recommended to plan the SDM600 installation carefully before doing any installation activities. Specifically, when adding a redundant or hierarchical installation, certificates have to be re-created, which could lead to re-configuration of devices.

5.3.2 Manage Users and Roles

In general, users and roles are managed in the **Account Management** section of SDM600. Adding, editing, and deleting users is intuitive and does not require additional description. Additionally, a user

with the **Administrator** role can reset the password of other users. Differences apply based on whether SDM600 is configured to integrate with Active Directory or not.

The editing (creation, modification, deletion) of Local Users (aka Emergency Users) will be disabled for users logged into SDM600 using Active Directory accounts.
In order to edit Local Users, the user must be logged in using a local user account.

Setting up user accounts in SDM600 is a very important step. Best practices in cybersecurity recommend the principle of least privilege. The principle is based on providing a user account with only the privileges that are essential to the user's work. Thus, it is recommended to first set up proper user accounts with roles before starting to engineer SDM600.

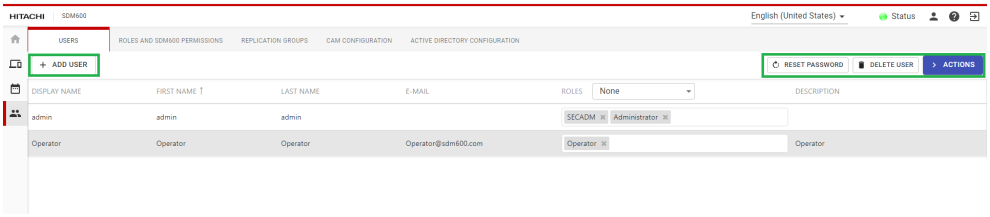


Figure 21: User Management

When using local users, during the first login, a user must change the initial password. It is recommended that a new user logs in to SDM600 to change the password immediately. However, the password change can also be done on connected systems.

The SDM600 supports e-mail notification. While creating new local users, in order to avoid copying and pasting a user's password and manually notifying the user, the e-mail notification should be configured first.

The **Roles and SDM600 Permissions** tab allows to manage the roles and configure the matching SDM600 permissions.

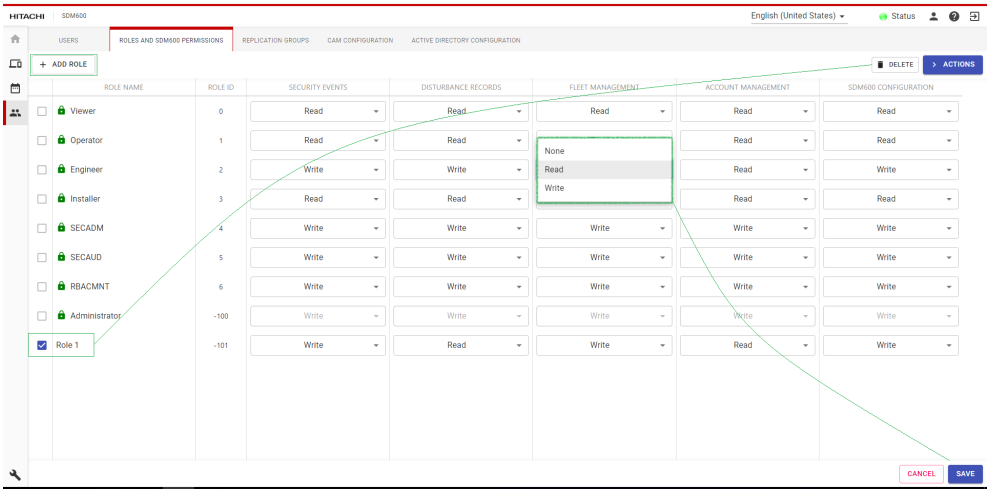


Figure 22: Role and SDM600 Permissions Management

SDM600 provides the possibility to manage the existing roles. As default, standard roles described in IEC 62351 are configured. These roles cannot be removed. In addition to the IEC 62351 roles, there is a possibility to create custom roles.

Every role needs a unique ID. According to IEC 62351, custom roles must have negative IDs.

Each role can be tailored to be allowed to view and/or modify specific data in SDM600.

For each Role, the following SDM600 permissions can be configured:

- **Security Events**, controls the visibility of the security events data, e.g. whether it is allowed to view the collected security events.
- **Disturbance Records**, controls the visibility of the DR files, e.g. whether it is allowed to view the collected DR files,
- **Fleet Management**, controls the fleet management functionality, e.g. whether it is allowed to view the collected files, whether it is allowed to modify the configuration of a device by writing a new configuration file.
- **Account Management**, controls the management of the accounts, e.g. whether it is allowed to view/add/remove/edit users, roles, mapping, replication groups.
- **SDM600 Configuration**, controls the configuration of the whole SDM600 as a system, e.g. whether it is allowed to add/remove IEDs, configure hierarchy or hot/standby, enable usage of Active Directory.

For each SDM600 Permission, three different access levels can be defined:

- **None**: no access to the content - the content will not be visible.
- **Read**: read-only access to the content - the content will be visible, but no changes could be made.
- **Modify**: read and write access to the content - the content will be visible and changes will be allowed.

The definition of user permissions in SDM600 only affects the SDM600 application. When CAM for devices is used, user permissions of individual devices or application must be defined within the respective device.

5.3.3 Password Policy

For local users, it is possible to enable the password policy, which enforces that configured criteria are met while entering the password.

SDM600 accepts only ASCII password.

When enabled, Password Policy will only enforce the selected criteria on the passwords created for local users. This setting will not have any impact on the password of the Active Directory users.

The following options can be configured for the password:

- Enable or disable password policy
- Minimum password length
- Maximum password age

- Expire warning
- Password history enforcement
- Number of maximum failed login attempts
- Lockout duration
- Password Complexity Settings:
  - Lowercase characters (a - z)
  - Uppercase characters (A - Z)
  - Base digits (0 - 9)
  - Non-Alphanumeric

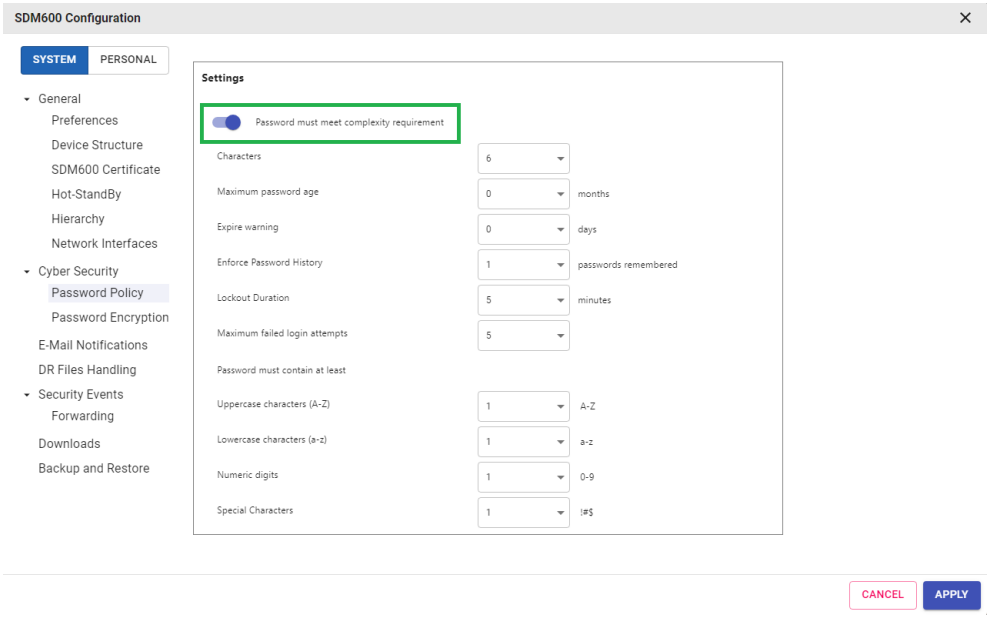


Figure 23: Password policy

When **Maximum Password Age** is configured, the password will no longer be valid once it expires, that is once it has been used for more than its valid age. Before the password expires, as configured in the **Expire Warning**, SDM600 will prompt a pop-up message warning the user that the password is about to expire: the user can change the password, refreshing the password age.

If user did not change the password before its expiration, then a new password will be requested during the next login.

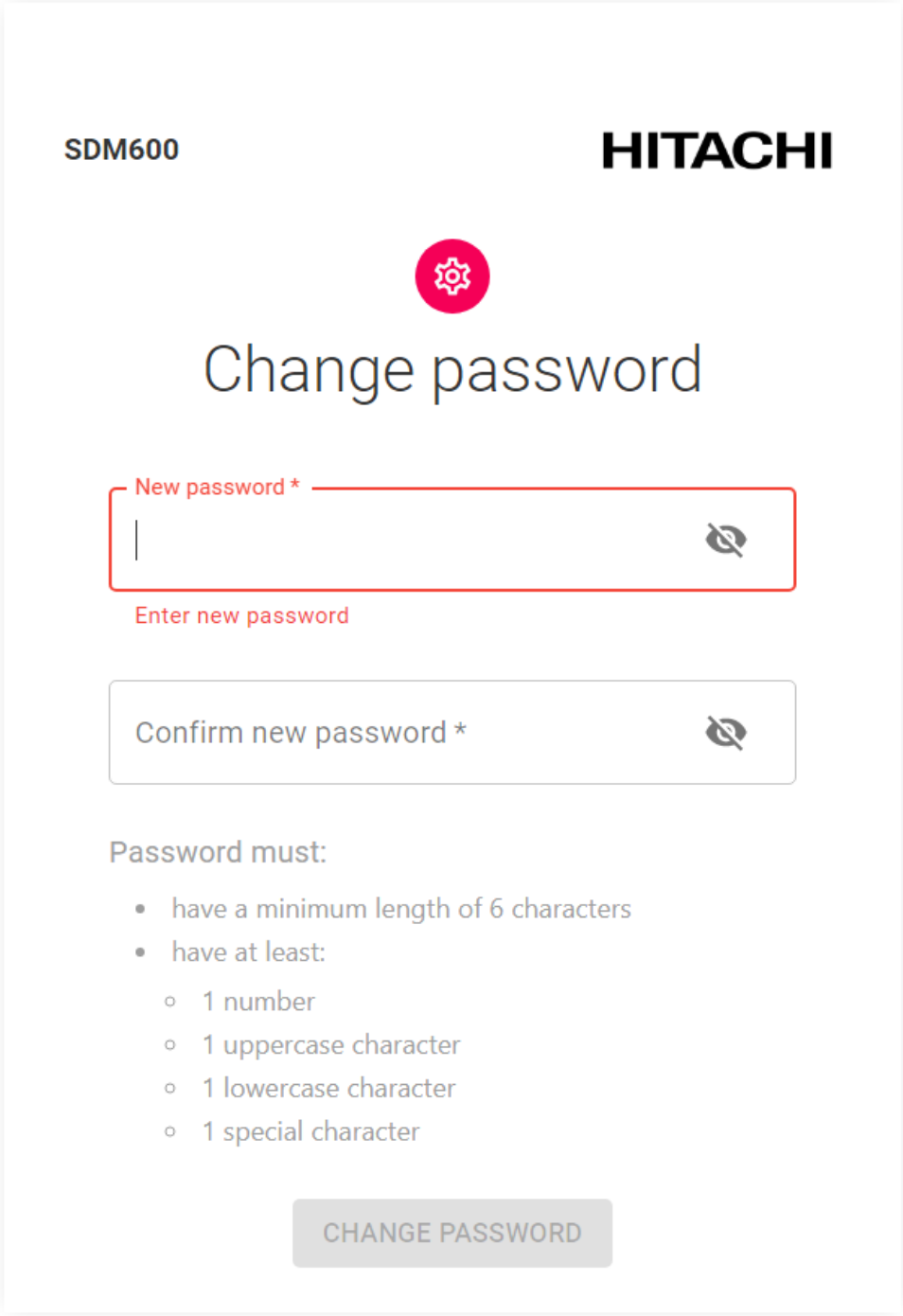


Figure 24: New Password after Expiration

5.3.4 Password Encryption

Starting with version 1.3.2, SDM600 will support cryptographic security mechanisms according to internationally recognized, proven security practices and recommendations. Passwords in the LDAP database are hashed using the selected algorithm.

By default, during a fresh installation SDM600 uses the SSHA256 password encryption. If you upgrade your SDM600 from a previous version and devices were configured to use IEC 62351-8 integration, by default the password encryption will be set to SSHA.

The passwords that were created before the SSH256 encryption support was available are encrypted with the SSHA algorithm and will keep working properly without the need for any manual intervention.

The password hashing is changed when users will change their password. It is advised that, after the password encryption was changed, that all users will change their passwords.

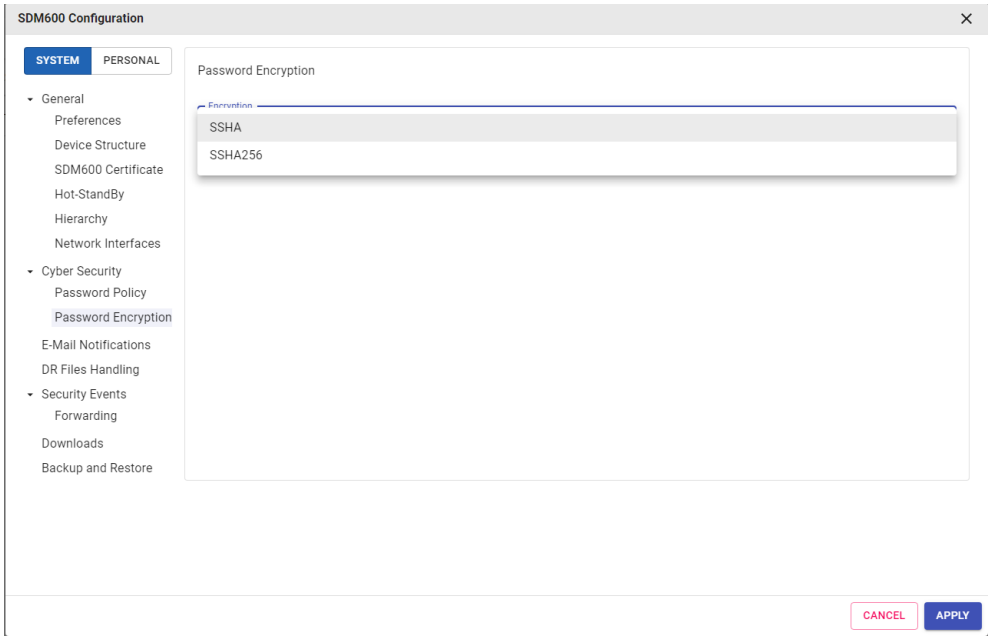


Figure 25: Password Encryption

5.3.5 CAM for devices: device integration

RESTRICTION

CAM for Devices is not available when SDM600 is configured to use Active Directory.

SDM600 provides CAM functionality with Role Based Access Control (RBAC) for devices or applications. The following protocols must be supported:

- IEC 62351-8 (Pull Model, Profile A)
- RADIUS (RFC 2865) devices
- MicroSCADA X specific CAM interface

Depending on the device / application and protocol, the integration varies. As a general rule, the SDM600 address must be configured as an authentication/authorization provider and certificates or shared secrets have to be imported to enable a secure connection between both endpoints.

The certificates and configuration can be retrieved from SDM600 and individually imported to the devices. For Hitachi Energy products, device specific packages are provided, which makes the integration more efficient.

Device specific configuration is done in the **CAM Configuration** tab within **Account Management** and is protocol specific. In order to configure devices for specific protocols, the device has to be licensed first.

To generate the CAM package configuration from the child system, a communication towards the parent system is required. Thus you must specify the user password during the CAM package generation.

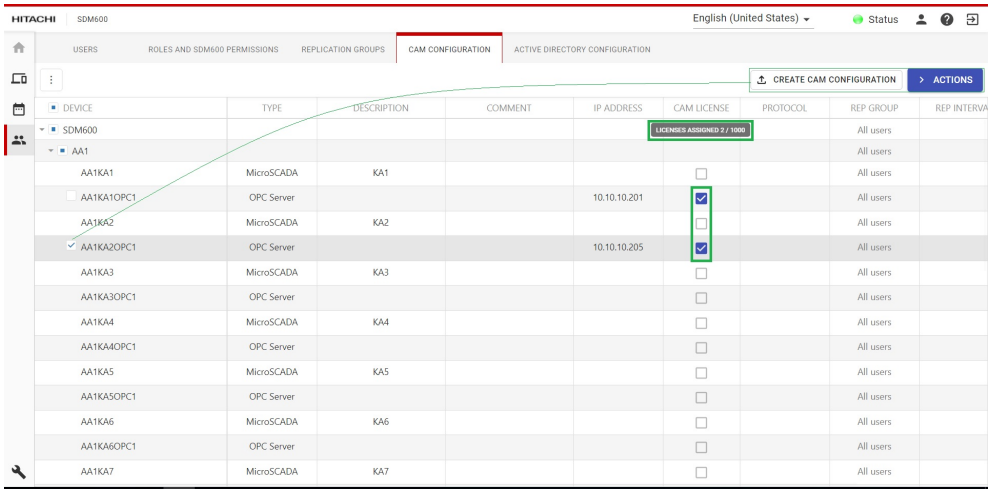


Figure 26: CAM licensing

RESTRICTION

LIMITATIONS APPLY!
Devices must be licensed to be configured.
Devices must have an IP Address to be configurable.

To configure devices, select the device (or multiple devices) and choose **Add CAM Configuration** from the **Actions** menu.

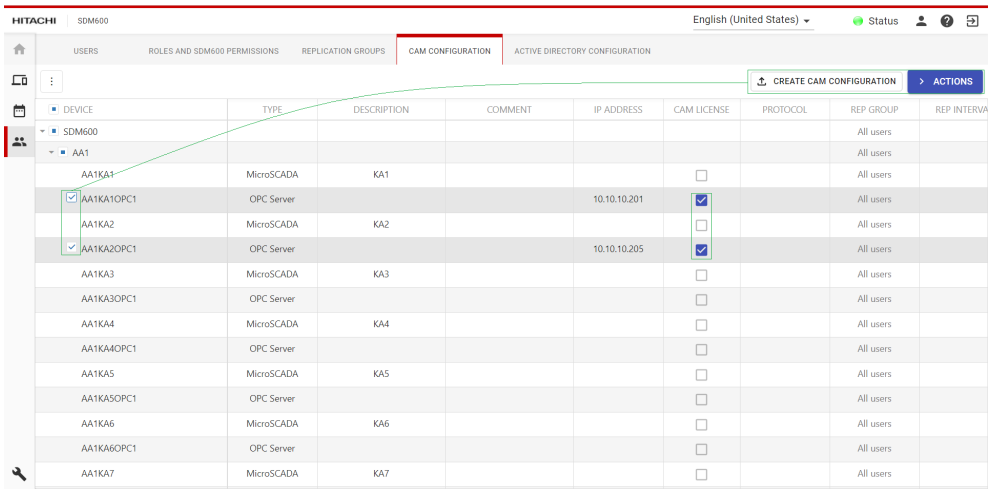


Figure 27: CAM multi-selecting

If IEC62351 is selected, then a CAM configuration and certificate for the target device must be created, to ensure a secure communication between SDM600 and the device. For this configuration, the user can edit the following settings:

- **Replication Group**: the user replication functionality is explained in the "IEC 62351-8 (LDAP) settings" section below. The user can select:
  - a specific replication group (listed by the name used when the group was created)
  - all the available users (All)
  - no replication at all (None)

- Replication Interval: if user replication is enabled (a replication group has been selected), the user can select how often the device will perform the replication. The value is expressed in [minutes] - 1440 minutes = 24 hours = once a day.
- **Password**: this field allows the user to configure the password used in the certificate
- **Key Length**: this field allows the user to configure the length of the RSA key of the certificate. Increase the value for improved cybersecurity, but higher CPU usage.
- **Valid from** and **Valid to**: these fields allows the user to configure the validity range for the certificate, specifying a starting and an ending date.
- **Subject Alternative Name**: this read-only field shows the currently configured subject alternative name that will be used when the certificate is created. The user can edit the subject alternative name by clicking on the pencil button: a modal dialog will be displayed allowing to add and remove IP addresses or DNS names.
  - For each device, the value of the last configured subject alternative name is remembered and provided as default value the next time we want to create a certificate. You can inspect the value in the read-only field and edit it via the pencil button.
  - SDM600 will prevent the user from removing the IP address of the device and the name of the device from the subject alternative name. This is done to ensure that all functionality could work properly.
  - RESTRICTION

    RESTRICTIONS APPLY!
    Editing the certificate's subject alternative name is disabled for bulk CAM Package creation. During bulk CAM Package creation, if IEC62351 is selected, each device's certificate will be generated with the subject alternative name set to the default subject alternative name value configured for that device.

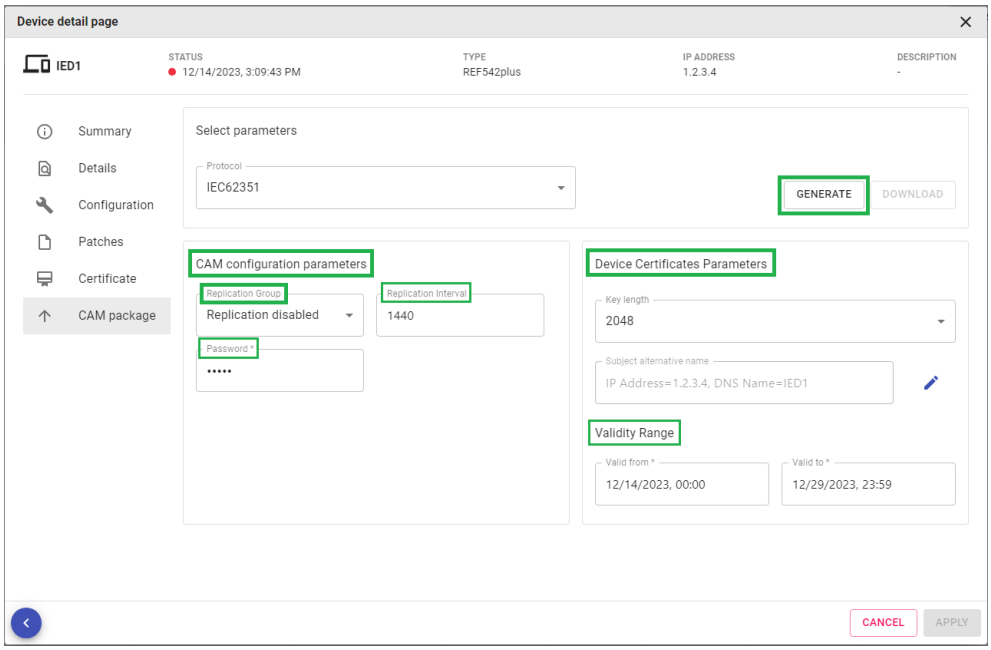


Figure 28: CAM package generation

5.3.5.1 IEC 62351-8 (LDAP) settings

In order to activate CAM for the IEDs managed in PCM600, the IED name in SDM600 must correspond to the PCM600 Technical Key. The CAM package for the IEDs can be downloaded and directly imported into PCM600.

Certain Hitachi Energy products support user replication from SDM600. If this feature is used, it allows the CAM users to use the CAM even in the case where SDM600 is not reachable from the devices as a fallback scenario.

To minimize those users, replication groups can be defined in SDM600.

User replication is only supported by certain Hitachi Energy products. Full user credentials are replicated to the devices to support offline login.

Starting with 1.3.2, SDM600 by default uses SSHA256 password encryption. Please verify if all your devices support this encryption or reconfigure the password encryption to use SSHA.

5.3.5.2 RADIUS settings

RADIUS requires a shared secret which must be configured in the device and SDM600. In case the shared secret is not equal on both ends, the connection cannot be established and the authentication will fail.

For authorization, RADIUS uses so-called Service-Type attributes. Those attributes can be device or vendor specific. In case authorization does not work out of the box, make sure that the attributes are configured correctly.

SDM600 has a predefined mapping of roles to the RADIUS Attributes Service-Type. This means that the RADIUS device can determine the user's authorization (rights) according to the user's role. Each RADIUS device vendor may have a different definition of what does a specific Attribute Service-Type mean in its device.

The default mapping between SDM600 Roles and the RADIUS Attributes Service-Types is shown in the Table 1.

Table 1: Default mapping of SDM600 Roles to the RADIUS Attributes Service-Type

SDM600 Roles	RADIUS Attribute Service-Type
Viewer	Service-Type [7]
Operator	Service-Type [1]
Engineer	Service-Type [6]
Installer	Service-Type [6]
SECADM	Service-Type [6]
SECAUD	Service-Type [6]
RBACMNT	Service-Type [7]
Administrator	Service-Type [6]

In SDM600, a user may be assigned multiple roles. In this case, when the user accesses a RADIUS device, the user will be assigned a corresponding RADIUS Attribute Service-Type that belongs to the most priority role. For instance, if the user has Administrator and Operator roles, the user gets the RADIUS Attribute Service-Type that correlates with the role Administrator since this is the most priority role, which in the default mapping is Service-Type [6].

The users have the possibility to customize the mapping to the users' needs. In order to adapt the mapping, execute the following steps:

1. Open the file **CAMRoleToRadiusRights.xml** where the original SDM600 mapping is stored. By default, it is located in the UserAuthentication Service directory (in the 64-bit Operating System, it is under **C:/Program Files (x86)/ABB/SDM600/UserAuthService**).

2. There are two major sections that are related to mapping. These two major sections are *RoleDefinitionRadiusRight specific for IEC 62351* section and *RoleDefinitionRadiusRight specific for ABB* section. The users can navigate to the section where the role mapping adaption is to be done.

- *RoleDefinitionRadiusRight specific for IEC 62351* section defines the mapping from the standard IEC 62351 roles to RADIUS Attributes Service-Type.
- *RoleDefinitionRadiusRight specific for ABB* section defines the mapping from the ABB specific role (that is, Administrator role) to RADIUS Attributes Service-Type.

3. Inside each *RoleDefinitionRadiusRight* section, there is one *RoleToRight* section, and inside the *RoleToRight* section, there are multiple *RoleToRadiusRight* sections. Each *RoleToRadiusRight* section represents a mapping between a known SDM600 role to a RADIUS Attributes Service-Type. The *RoleToRadiusRight* section is composed out of two sections, namely *Role* section and *Rights* section. In order to modify the role to right mapping, the users can add or delete the respective RADIUS Attributes Service-Type (or also the Vendor Specific Attribute).

See the following examples. If a user would like to assign a RADIUS Attributes Service-Type *Service-Type[6]* from IEC 62351 role Engineer to IEC 62351 role Operator, the user can edit the respective part in the **CAMRoleToRadiusRights.xml** file. Table 2 shows the before and after adaptation of the mapping. Note that the table only shows a snapshot of the file's content.

Table 2: How to Customize the Mapping Between SDM600 Roles and RADIUS Attributes Service-Type

Default mapping from SDM600	Customized mapping by user
<RoleDefinitionRadiusRight> <RoleDefinition> <Revision xsi:nil="true" /> <Definition>IEC62351-8</Definition> <Roles /> </RoleDefinition> <RoleToRight> <RoleToRadiusRight> <Role> <Name>Viewer</Name> <RoleId>0</RoleId> </Role> <Rights> <string>Service-Type[7]</string> <string>RuggedCom-Privilege-level[guest]</string> </Rights> </RoleToRadiusRight> <RoleToRadiusRight> <Role> <Name>Operator</Name> <RoleId>1</RoleId> </Role> <Rights> <string>Service-Type[1]</string> <string>RuggedCom-Privilege-level[operator]</string> </Rights> </RoleToRadiusRight> <RoleToRadiusRight> <Role> <Name>Engineer</Name> <RoleId>2</RoleId> </Role> <Rights> <string>Service-Type[6]</string> <string>RuggedCom-Privilege-level[admin]</string> </Rights> </RoleToRadiusRight> . . . </RoleDefinitionRadiusRight>	<RoleDefinitionRadiusRight> <RoleDefinition> <Revision xsi:nil="true" /> <Definition>IEC62351-8</Definition> <Roles /> </RoleDefinition> <RoleToRight> <RoleToRadiusRight> <Role> <Name>Viewer</Name> <RoleId>0</RoleId> </Role> <Rights> <string>Service-Type[7]</string> <string>RuggedCom-Privilege-level[guest]</string> </Rights> </RoleToRadiusRight> <RoleToRadiusRight> <Role> <Name>Operator</Name> <RoleId>1</RoleId> </Role> <Rights> <string>Service-Type[1]</string> <string>Service-Type[6]</string> <string>RuggedCom-Privilege-level[operator]</string> </Rights> </RoleToRadiusRight> <RoleToRadiusRight> <Role> <Name>Engineer</Name> <RoleId>2</RoleId> </Role> <Rights> <string>RuggedCom-Privilege-level[admin]</string> </Rights> </RoleToRadiusRight> . . . </RoleDefinitionRadiusRight>

It is required to restart the SDM600 services after the re-mapping action between SDM600 Roles and RADIUS Attributes Service-Type is done.

5.4 Structure definition

SDM600 collects data from many devices. For a better overview, those devices are represented in a structure. The structure is fully configurable and can consist of grouping elements such as Substations, Voltage Levels or Simple Device Groups.

The structure is represented in a tree view and is visible in different SDM600 areas.

- PCM600 will not activate CAM functionality for an IED, unless the IED name in SDM600 matches the PCM600 Technical Key.
- Pay attention when editing the name of an IED. The IED name in SDM600 must match the Technical Key in PCM600.

5.4.1 File import

The SDM600 structure can be imported via two file types:

1. IEC 61850 .scd file
   When importing .scd files, the Substation Section and IED information are automatically imported. IEDs which cannot be allocated to a specific part of the Substation, will be added to a grouping node.

   - When importing an .scd file, SDM600 will not merge its content with an existing substation structure, but always add a new Substation.
   - After importing an .scd file, it's possible to move nodes between different substations by using drag/drop functionality in the tree view.

2. SDM600 specific csv file format
   IEDs and configuration provided via csv format will be imported.

   A template for the csv file format is available from the SDM600 downloads.

   Devices require a unique IP address in SDM600. In case devices with duplicated IP addresses are imported, the IP address of subsequent devices will be empty.

After importing a structure, it can be changed manually.

5.4.2 Manual structure definition

The SDM600 structure can be imported, built manually, or a combination of both workflows. To manually edit the SDM600 structure, open the **System Configuration/General/Device Structure** configuration menu.

Existing nodes can be renamed or deleted by right-clicking. To add additional nodes, right click on a structure node and choose the appropriate type.

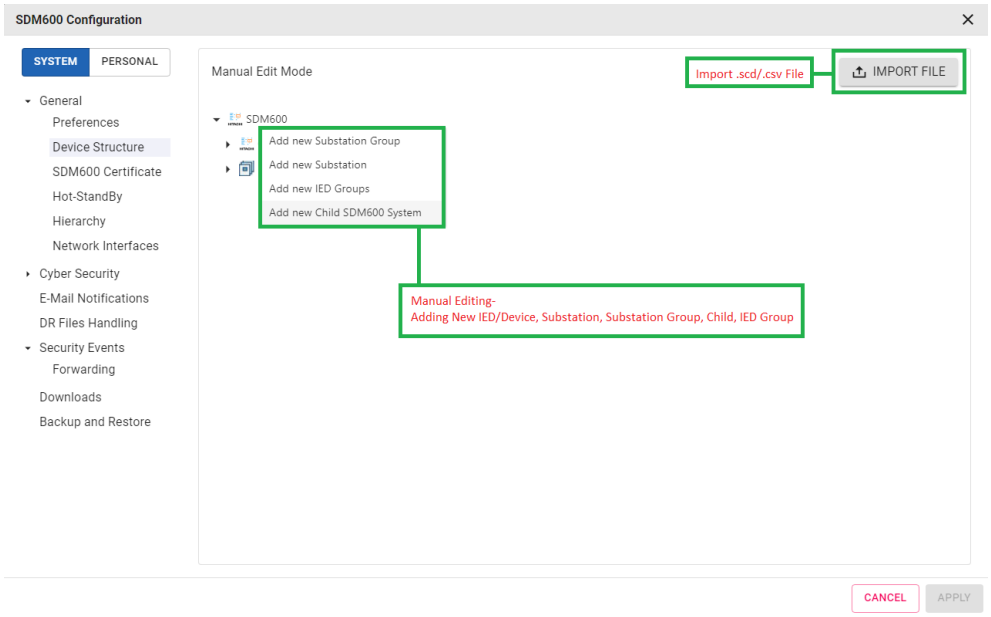


Figure 29: Manual tree structure

5.4.2.1 SDM600 structure node types

SDM600 supports the following node types, which will be displayed by a different icon:

- *Substation Group*: is a virtual group of two or more substations. For example, it is possible to create a substation group for Region A that consists of Substation A1, Substation A2, and so on. It is only possible to create substation entries directly under a substation group.
- *Substation*: is a container for a substation. For example, to accommodate Substation A1, a substation entry called "Substation A1" can be created. It is possible to create Voltage Level and IED entries directly under a substation.
- *Voltage Level*: is a container for different voltage levels under a substation. For example, under Substation A1, there can be two voltage levels: 110 kV and 220 kV. It is possible to create Bay and IED entries directly under the Voltage Level.
- *Bay*: It is possible to create IED entries directly under a bay.
- *IED/device*: is a device in a substation.
- *SDM600* Child: is a connected SDM600 instance.

5.4.2.2 SDM600 device types

Each device in SDM600 has an assigned Device Type.

To provide a certain default configuration per device type, SDM600 supports IED templates, which can be extended on demand.

An IED template is an XML-based file that describes the IED type:

- IED type name (for example, RE.670, REL650)
- Manufacturer of the IED (for example, Hitachi Energy)
- Supported protocols - IEC 61850 MMS
- Information whether the IED can have a disturbance record or not
- Information on the directory location of the disturbance record

It is not mandatory to have device templates for all devices used in an SDM600 deployment. Device Templates contain predefined configurations that can be changed manually in the Device Configuration.

By default, the IED templates are in the IED Template folder in the SDM600 installation folder. For example, in the Microsoft Windows 7 x64 operating system, the IED template files can be found under **C:/Program Files (x86)/ABB/SDM600/IEDTemplates**.

To create a new template for a specific IED that is not currently listed, do the following:

1. Copy one of the IED Template files. The new file should be in the same location as the default IED Template files. Rename it accordingly. By default, it is named based on its type name/type family name.
2. Open the template file in an XML editor.
3. Fill in the mandatory *Type* attribute information. For example, *Type* = *"IED_NewType"*. It is highly recommended to fill in the *Manufacturer* attribute information, as well. For example, *Manufacturer* = *"Hitachi Energy"*. The strings defined for attributes *Type* and *Manufacturer* must match the strings defined in the *SCD* files that were originally delivered in the manufacturer's *ICD* or files. This is to

ensure that when importing the IEC 61850 SCD file into SDM600, it matches the corresponding template files and the correct information of the IED can be shown and further used.

4. Fill in other attribute information such as *ShownType*, *Description*, *ShownManufacturer*, *CommProtocol*, *HasDR*, and the *DRPath*. The *HasDR* attribute indicates that the IED has DR Functionality. The *DRPath* attribute indicates the path to the DR files on the device.
5. To see the newly created IED template, SDM600 log-out and log-in are required.

5.5 Manually triggering data collection

SDM600 offers an option for the user to right click on any IED/Device and manually collect the DR and also Service Data.

For example, if the polling cycle for a IED/Device is set to 3600 Sec (60 Mins) and if the user wants to collect the data manually without waiting for the polling time, the user can right-click on any IED/Device and select **Collect Data Now**.

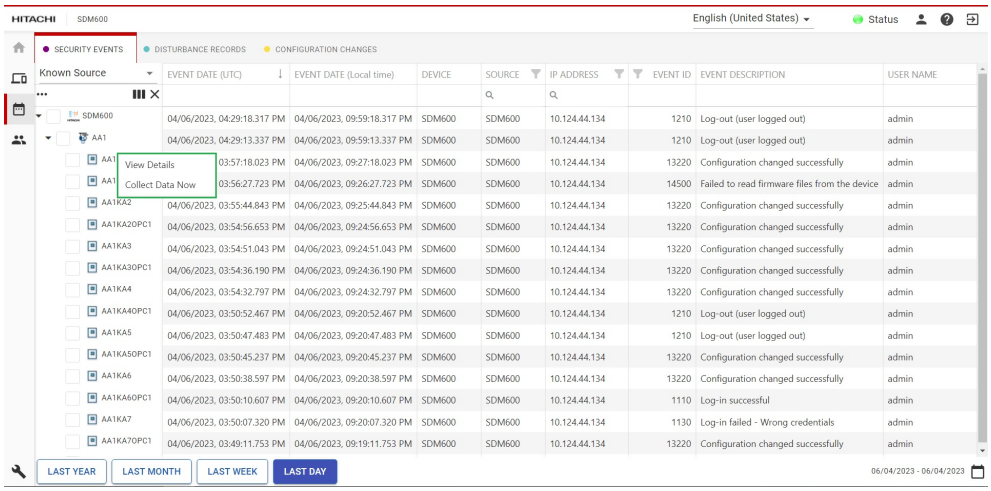


Figure 30: Collect Data Now

5.6 Efficient configuration of devices

When configuring SDM600 to collect data from a large system, one of the biggest challenges is to configure each device individually. Whereas it is a comparably simple operation to setup SDM600 to collect data from a device, it can take a considerable amount of time when this configuration must be repeated on a large number of devices.

To increase the configuration efficiency, SDM600 introduced the possibility to clone the existing configuration from one source device to several target devices. This functionality enables the user to edit the required configuration parameters on a single device and then replicate the configuration on

other target devices. To maximise the flexibility, the user can decide which configuration parameters to clone from the source to the target devices.

To save time and effort, it is recommended to configure one device in SDM600 to reflect the desired settings, and then utilize the "Clone Configuration" feature to replicate the configuration across several similar devices. By configuring only one device and propagating the changes to other target devices, users can efficiently ensure that required devices have the same desired settings. This workflow can be repeated as needed, allowing users to easily apply configuration changes across multiple devices without having to manually configure each device individually.
For instance, configure one RTU device as required and then clone the configuration other RTU devices.

To quickly replicate the configuration of one device across multiple devices, simply follow these steps:

1. In the tree view, select all the devices you want to update with the new configuration by multi-selecting them.
2. In the tree view, right-click on the source device whose configuration you want to clone, and select "Clone Configuration" from the context menu.
3. In the "Clone Configuration" modal dialog, review the current values for each configuration parameter of the source device and select which parameters to clone.
4. Press "Clone" to start the cloning procedure. A confirmation message will be displayed before propagating the changes.

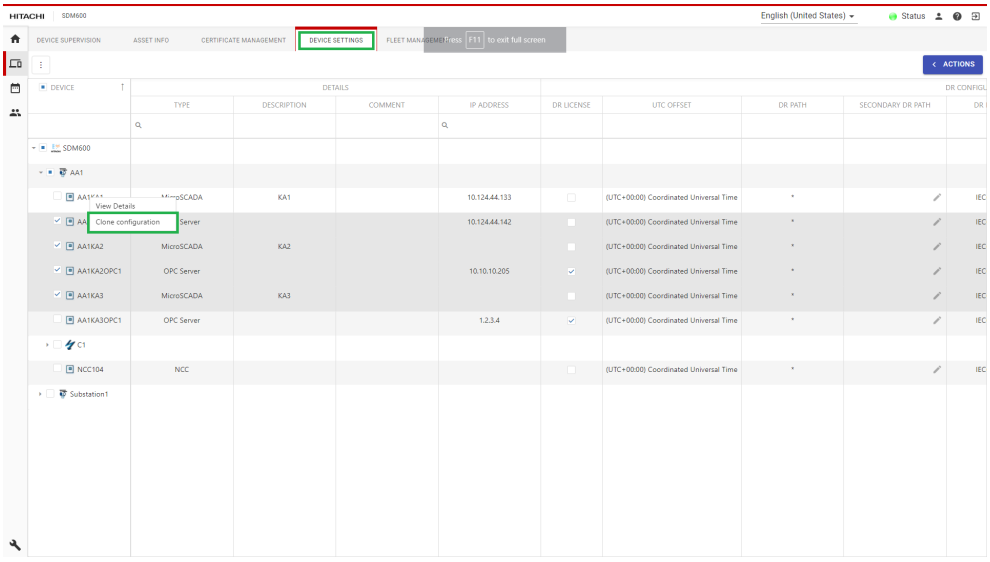


Figure 31: Multi-Select Devices & Clone Configuration

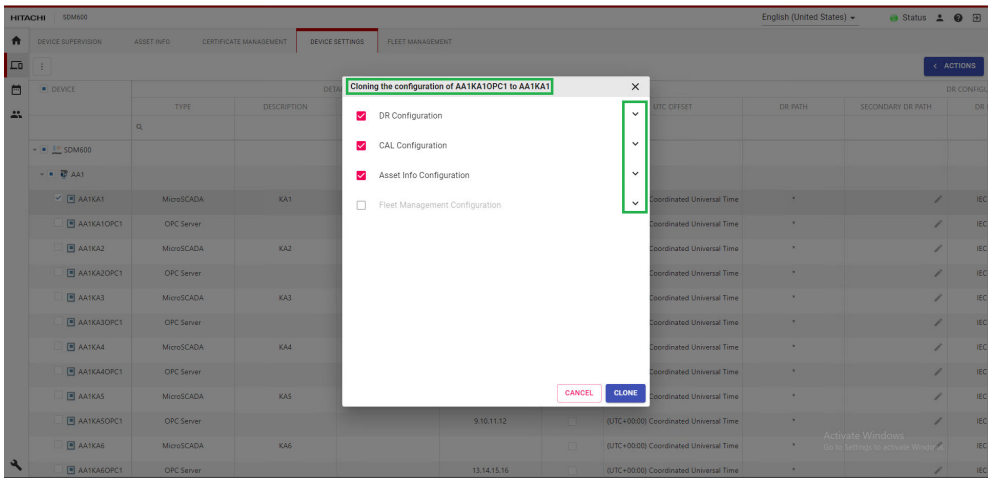


Figure 32: Clone Configuration Dialog

To enhance the usability, efficiency, and safety of the cloning process, SDM600 will automatically load the "Clone Configuration" modal dialog with default settings that suggest which configuration parameters should be cloned. The user should review these suggestions and make necessary adjustments to fine-tune which parameters to clone.
Configuration parameters that are likely to be cloned will be enabled and checked by default, while those that are unlikely to be cloned will be enabled but unchecked. For example, the "DR Protocol" configuration parameter will be enabled and checked by default as it is commonly needed to be cloned across multiple devices. On the other hand, the "DR Path" configuration parameter will be enabled but unchecked by default as it is device-specific and typically not necessary to be cloned across different devices. However, the user can still quickly select the parameter to clone if needed.
Lastly, configuration parameters that cannot be cloned will appear as disabled and unchecked. This may be due to various reasons, e.g. if the number of devices allowed by the DR License has been reached, the "DR License" parameter will appear as disabled and unchecked.

Make sure to review the changes before the propagation, as the clone configuration operation could not be undone.

If SDM600 is configured as a hierarchical system, the usual limitations apply when editing the configuration of the devices. As it should be expected, when editing the configuration of the devices from the parent system, clone configuration is disabled when targeting devices belonging to the child system.

5.7 Filtering Events using the Time Window

When applying time filtering on events displayed in the "Events Monitoring" tabs, the Time Window component is designed to help the operators by providing additional context and guidance.

The Time Window component displays a chart showing how many events of each kind happened in the system over the selected time horizon. DR files are displayed in blue, security events in magenta and configuration changes in yellow.

Filtering by source (selecting one or more devices in the device structure) will not have any effect on the Time Window. At any moment in time, the Time Window component displays all the events collected by SDM600 over the selected time horizon.

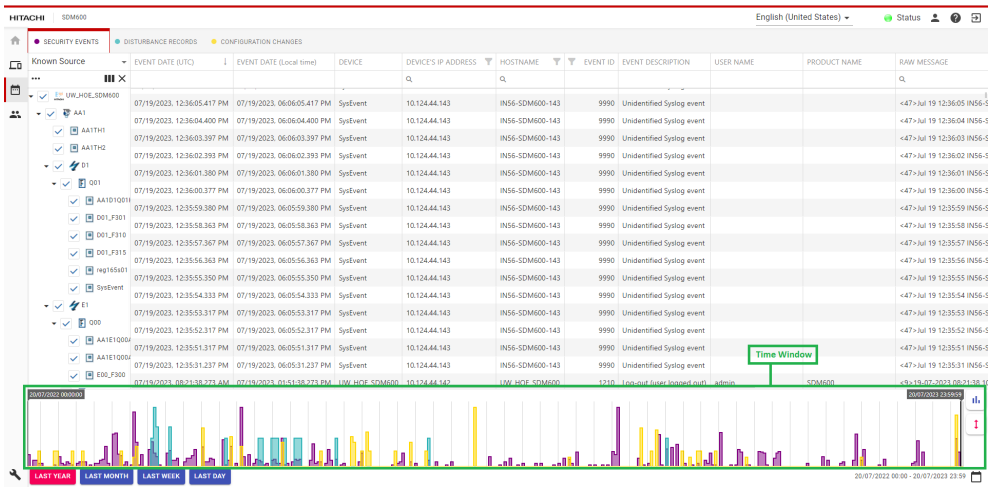


Figure 33: Time Window

To change the time horizon

The time horizon can be changed:

- by clicking on the "Last Year", "Last Month", "Last Day" buttons
- by selecting any desired dates directly in the calendar.

Loading data over large time horizon might take some time.

When changing the time horizon:

- The Time Window will refresh and display a graph of the events which happened in the system over the newly selected time horizon
- The data shown in the endless scrolling grid will be filtered according to newly selected time horizon, e.g. "Last Month".

To further refine the time filtering users can move the range selector, which is designed to allow to select the exact moment in time to filter. Editing the range selector will apply a new time filtering, loading the events that occurred in the selected range in the endless scrolling grid.

On the right side of the Time Window component, three buttons allows to customize and interact with the charts:

- Chart Settings
- Data Normalization
- Zoom

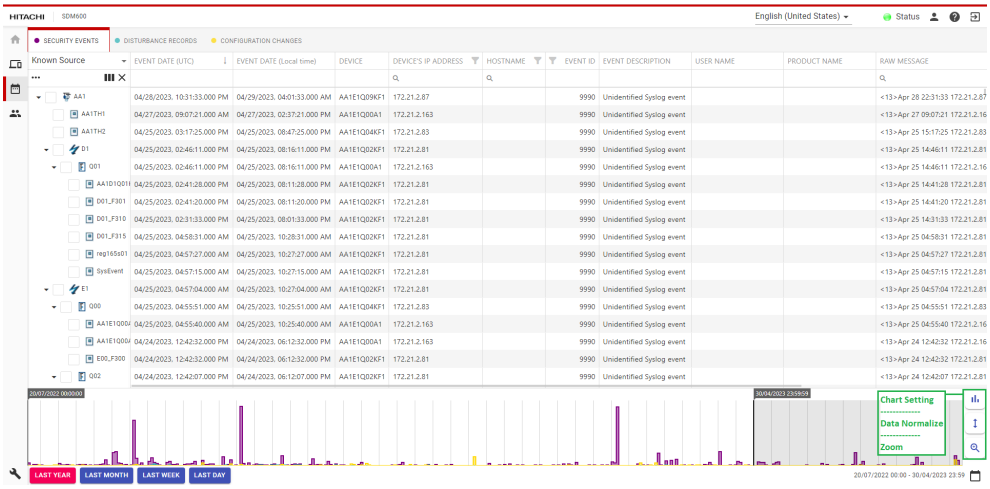


Figure 34: Time Window Options

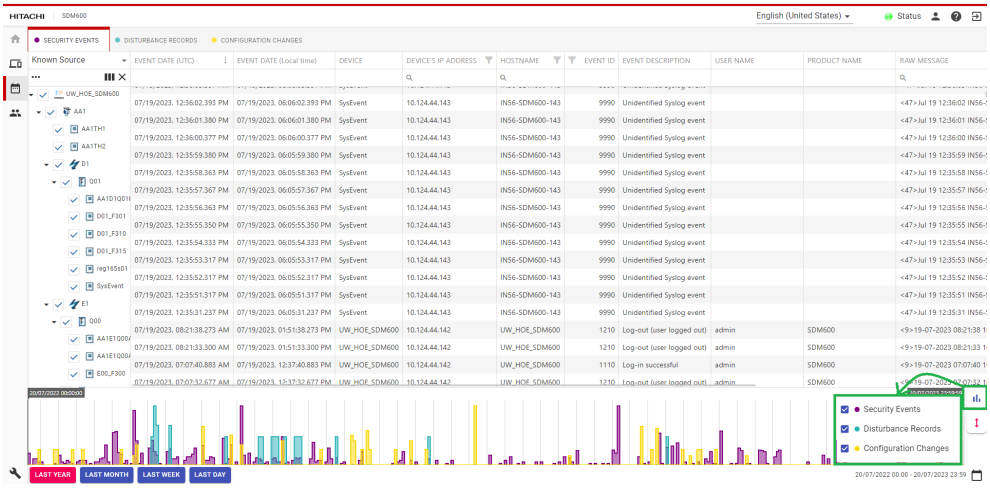


Figure 35: Time Window Chart Settings Options

By clicking on the "*Chart Settings*", a menu will be shown allowing to select / deselect which kind of event to visualise in the Time Window; this functionality allows the user to focus on specific data kind, while temporarely hiding the chart that are not required. For instance, it is possible to uncheck "Security Events" and the matching yellow chart will not displayed in the Time Window component.

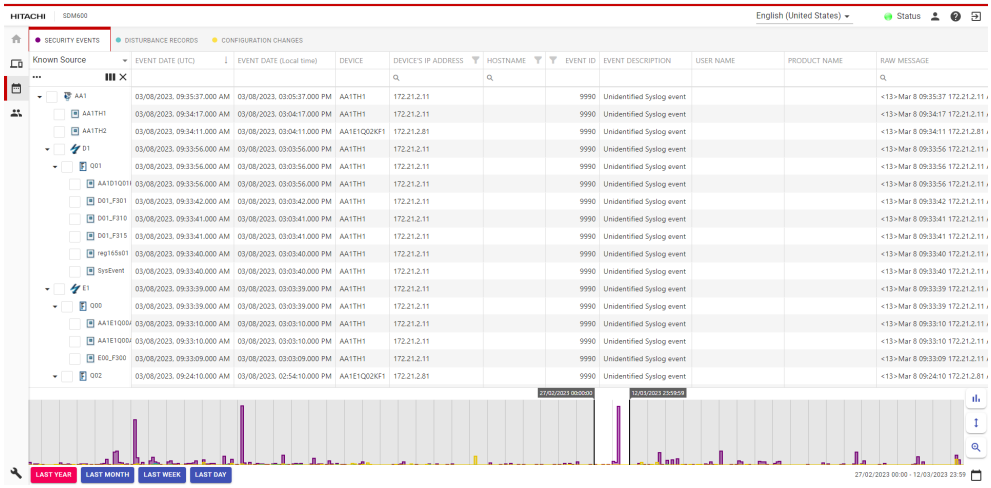


Figure 36: Time Window Range Selection

Based on the events available in the system, the graph's presentation might suffer from an inadequate scaling, leading to the diminished visibility of events with smaller magnitudes compared to events with larger magnitudes. To address this problem, data normalization is employed. By adjusting the scale of the graph, the data with smaller magnitudes can be visually emphasized, ensuring their visibility and maintaining a balanced representation across the entire range of values. "*Data Normalization*" can be enabled or disabled by clicking on the matching button. At any moment in time, the status of the button will tell whether normalization is applied to the data shown in the charts.

When enabling or disabling the normalization, the range selector will be reset to its default position as the charts are plotted again.

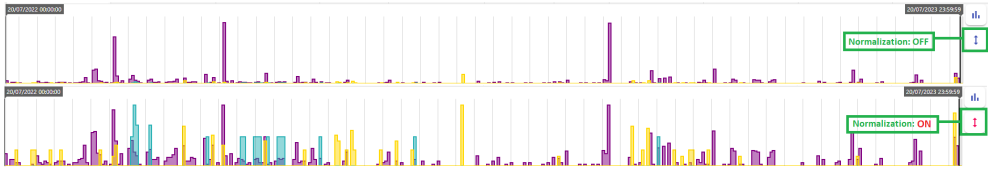


Figure 37: Time Window - Data Normalization

If more details are required while inspecting a manually configured time range, the "*Zoom*" functionality allows to delve into it: this functionality will expand the currently selected time range over the whole time horizon, providing more granularity and details for the analyzed time.

The smallest granularity supported by Time Window is 1 hour. For this reason, the zoom functionality is not available when the smallest granularity has been reached.

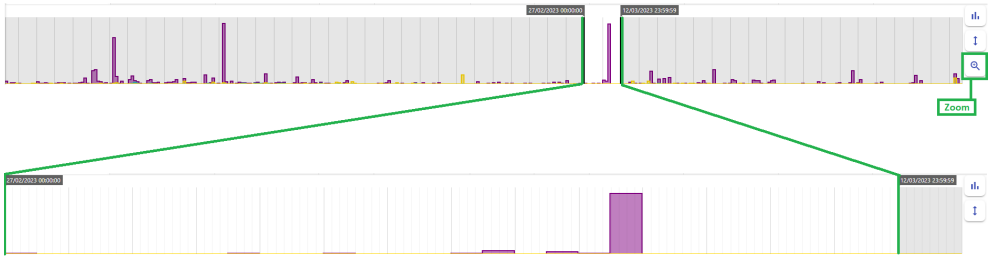


Figure 38: Time Window - Zoom in the selected Time Range

5.8 Disturbance Recorder data management

SDM600 periodically collects DR data from licensed devices. SDM600 automatically detects, transfers, and stores DR files in a designated database aligned with the configured SDM600 structure.

SDM600 only supports DR Files based on the COMTRADE format.

5.8.1 Operations

DR files are available in the **Events Monitoring** section under the **All Events** tab and the dedicated **Disturbance Records** tab.

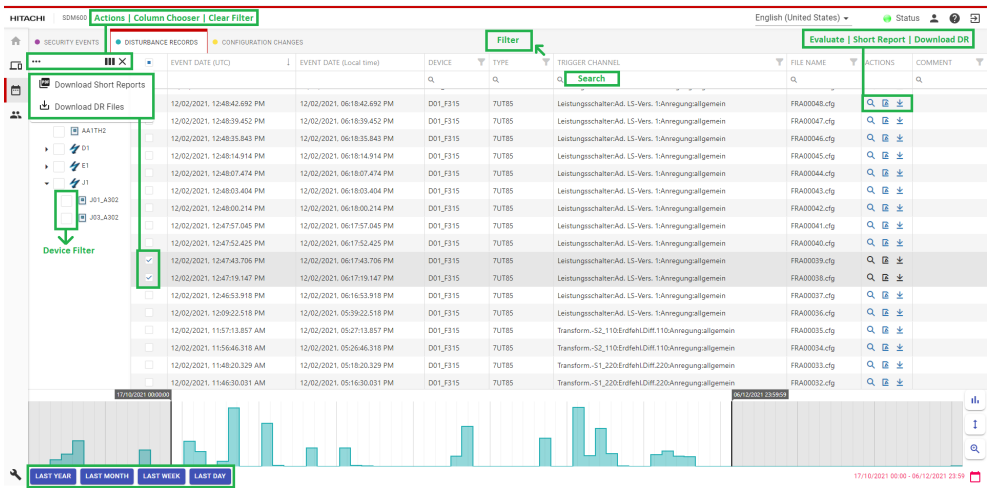


Figure 39: Disturbance Records

The Disturbance Record functionalities are described below:

1. Actions: This option allows the user to download and generate the short reports for multi selected Disturbance Records.
2. Column Chooser: This option allows the user to select the columns of the grid that are displayed, see Figure 39.
3. Clear Filter: This option allows the user to clear any filter applied to the columns of the grid.
4. Sorting/Filtering: This option allows the user to sort the data in the grid and to edit the filtering criteria to apply to the shown data.
5. Action(Single DR): The option allows the user to evaluate DR, download DR and generate short report.

The displayed DR data is filtered by the selected node and time period. The DR files can be evaluated by clicking on the search icon. DR Files can be downloaded from the SDM600 server to the client PC by clicking on the download icon. Clicking on the PDF icon will open the respective short report in a new tab within the web browser.

The Evaluate option is configured using DR Selector Tool and is a one-time activity to select the desired application to evaluate the DR file. Please refer installation guide how to install the DR Selector Tool.

When selecting multiple events, download of DR files and short report are available from the **Action** menu.

5.8.1.1 DR file analysis

DR files can be downloaded to the PC to be analyzed using a dedicated SW application.

SDM600 includes the WaveWin Application that can be downloaded from the SDM600 server installed on the client PC.

5.8.2 Device integration

SDM600 supports different communication protocols to read DR files from devices. Some configuration parameters are protocol specific.

SDM600 uses a vendor-neutral implementation for DR file retrieval. However, some product specific settings might be required. Vendor or device type specific information can be obtained from the respective manufacturer.

The device specific configuration is done in the **Device Settings** tab under the **Devices** section.

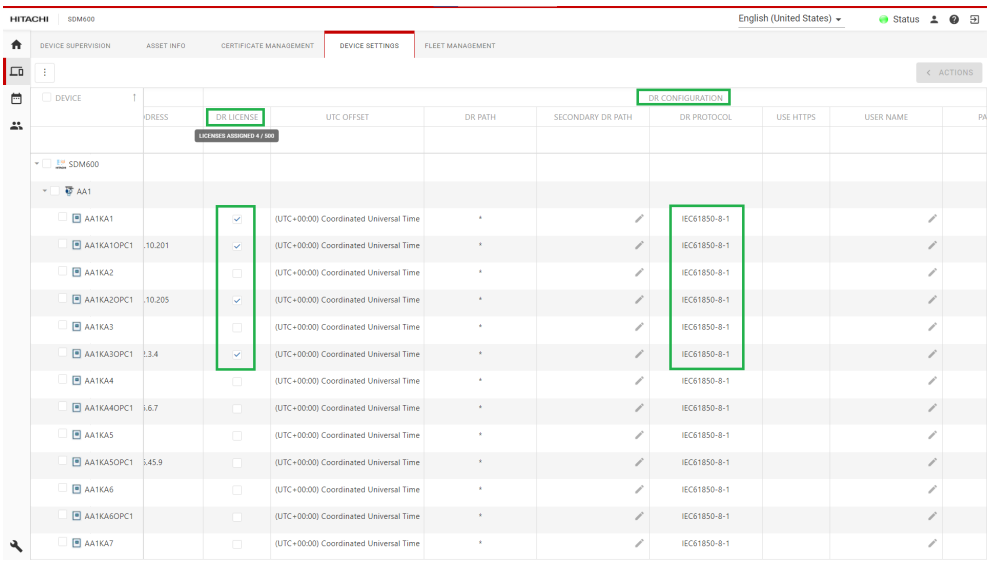


Figure 40: Device Settings

5.8.2.1 General

The DR file collection is based on a cyclic polling mechanism for different communication protocols. This allows integration of SDM600 into existing systems without re-configuration of the IEDs. The polling interval is flexible and has to be configured.

Selecting a short poll cycle time will impact the SDM600 computer and IED CPU load. It is recommended to start with a high poll cycle (for example, 30 minutes).

In order to retrieve DR files from a device, each device has to be licensed. DR Licenses are available for different batch sizes. If the license for a device is disabled, all related DR files are deleted.

SDM600 Displays the Trigger Time of Disturbance records. This time is directly read from the COMTRADE .cfg file and is treated as UTC time. An offset can be defined for each device, to have the same time source in SDM600.

In case if an IED is not using UTC time as the trigger time in the .cfg file, an offset can be configured. It is important to configure the offset before the device is licensed and the DR file collection starts.

Well known configuration parameters are pre-defined in the device templates.

The file location where DR files reside within the device must be configured. An alternative location can be defined. This will be used if the first one is not accessible.

SDM600 will not merge the content of the two directories; only one of the two directories is used at any time.

5.8.2.2 IEC 61850 devices

Most IEC 61850 IEDs support direct IEC 61850-8-1 MMS file transfer. To support device specific implementation flavours, two different implementations are supported:

- **IEC 61850-8-1:** DR files are collected by SDM600 over the IEC 61850-8-1 MMS protocol. Designed to minimize CPU usage and network footprint, the algorithm relies on the filename and the creation date of each DR file to detect whether the file has already been collected. For devices unable to provide a reliable and trustworthy creation date for the DR file, it is suggested to use the IEC 61850-8-1 (safe mode) described below.
- **IEC 61850-8-1 (safe mode)**: DR files are collected by SDM600 over the IEC 61850-8-1 MMS protocol. This algorithm is suggested for devices unable to provide a reliable and trustworthy creation date for the DR files. Compared to the aforementioned IEC 61850-8-1 algorithm, this implementation allows to cope with suboptimal data quality (for example, creation date of the DR file is always set to 1.1.1970), whereas delivering inferior performance regarding CPU usage and network footprint.

The DR path is typically "*", "\COMTRADE" or can be left empty. This depends on the IED and is embedded in the device templates for well-known devices.

5.8.2.3 FTP devices

The following FTP variants are supported:

- **FTP:** DR files are collected by SDM600 by using the standard File Transfer Protocol
- **SFTP:** DR files are collected by SDM600 by using the SSH File Transfer Protocol. The SDM600 currently supports the following key exchange algorithms:
  1. diffie-hellman-group-exchange-sha256
  2. diffie-hellman-group-exchange-sha1
  3. diffie-hellman-group14-sha1
  4. diffie-hellman-group1-sha1

  When selecting SFTP as the DR Protocol, make sure the SFTP server supports at least one of the key exchange algorithms supported by SDM600.
- **FTPS (Implicit):** DR files are collected by SDM600 by using File Transfer Protocol Secure.

Accessing files via FTP requires a username and password. Those credentials can be device or device type specific and must be provided when configuring the device.

5.8.2.4 Windows folder

This method is used when DR files are collected manually by a user and placed into a folder in a computer where SDM600 is installed or into a folder in another computer which is accessible by SDM600. In this case, SDM600 reads the specified folder and imports the DR files into SDM600.

Windows Folder integration is particularly useful for devices using a proprietary communication protocol. Usually, the vendor provides a tool to collect the DR files from the device and save them to a folder on the SDM600 PC. The integration of 3rd party tools is not described in this manual.

Local Folders

If the directory is located on the same computer as the SDM600, use the following notation: \ *localhost*\c$*Directory*.

For example, if the DR files are located under **C:/Substation_A/Bay1/IED1**, then type in *localhost*\c$ *Substation_A**Bay1**IED1*\ into DR Path column of the respective IED.

Folders on another computer

If the directory is located on a different computer, it is important to make sure that the directory is accessible from SDM600, that is, by sharing the folder. While sharing the folder, it is important to ensure that the *SDM600 IED Communication Service* is running under an account that has enough privileges to access the network path or the remote shared folder, that is, same credentials and same rights as used on the other computer that stores the DR files.

Next, fill in the DR Path with the full UNC path (**\\computername/sharedfolder**). For example, if the DR files are located in a computer with an IP address *192.168.1.33* at **C:/Substation Baden/Baden/ IED2** drive, and **C:/Substation Baden** is a shared folder, the correct way to write the full UNC path is *192.168.1.33**Substation Baden**Baden**IED2*\.

In general, when accessing files that are located on another computer, it is common to map the network drive to the local drive. In SDM600 DR collection mechanism, this will not work. It is important that the full UNC path to the folder on another machine is given to SDM600.

The SDM600 *IED Communication Service* must have access right to the folder. In case the service has no access, it can be configured to run as a specific user account. Refer to Windows documentation on how to run a Service using a specific user account.

To support integration of DR files from redundant setups (for example, accessing DR files from a MicroSCADA HSB System), two DR paths can be configured per device. SDM600 will not store duplicated entries in this case.

5.8.2.5 RTU500

For a Hitachi Energy RTU500, a specific method is used to collect DR files; from the list of available protocols, select "RTU Web API". The DR file format will be recognized automatically, and a suitable converter used if needed.

To access the RTU500, it is important to enter the name of the role with defined privileges to read disturbance record files from the RTU device.

It is possible to configure the "Use HTTPs". This is an important cybersecurity setting: please refer to the *Hitachi Energy RTU500 "Use HTTPs"* section.

5.8.3 DR file export

All DR files can be exported from SDM600 to make them accessible for other applications or to backup/store them on a different system.

Additionally, the filename for the exported DR file can be configured in a flexible manner according to the COMNAME standard.

Depending on the number of DR files, an export can be time-consuming and produce additional CPU load on the SDM600 computer.

5.8.3.1 Export file name definition

Usually, the DR File names from devices contains a standard name (for example, "drec_") and an incremental number.

The export file name can be defined very flexibly to match different requirements. The main objective is to add information related to the device and location from which the specific DR was generated.

The export file name can be composed of the following elements:

Tag name	Description
<STRUCTURE>	Structure
<STRUCTURE_DESC>	Custom name for a structure level.
<IEDG>	IED Group
<IEDG_DESC>	Custom name for an IED Group
<SUBG>	Substation Group
<SUBG_DESC>	Custom name for a Substation Group
<SUBSTATION>	Substation
<SUBSTATION_DESC>	Custom name for a Substation
<VL>	Voltage Level
<VL_DESC>	Custom name for a Voltage Level
<BAY>	Bay
<BAY_DESC>	Custom name for a Bay
<DEVICE>	Device
<DEVICE_DESC>	Custom name for a Device
<ORIGINAL_NAME>	Original File Name (from an IED device)
<COMPANY>	Company Name
<DATE>	UTC Date
<TIME>	UTC Time
<DATE_SRV>	Server Local Date
<TIME_SRV>	Server Local Time
<TIMEZONE>	Server Time Zone

In addition to the tags above, it is possible to define a custom date or time format. In this case <DATE> or <DATE_SRV> tag must be extended with a date and time format definition. For example: <DATE_SRV_dd:MMMMM:yyyy:HH.mm.ss.ff>, all possible options are listed in: *https://learn.microsoft.com/en-us/dotnet/standard/base-types/custom-date-and-time-format-strings*.

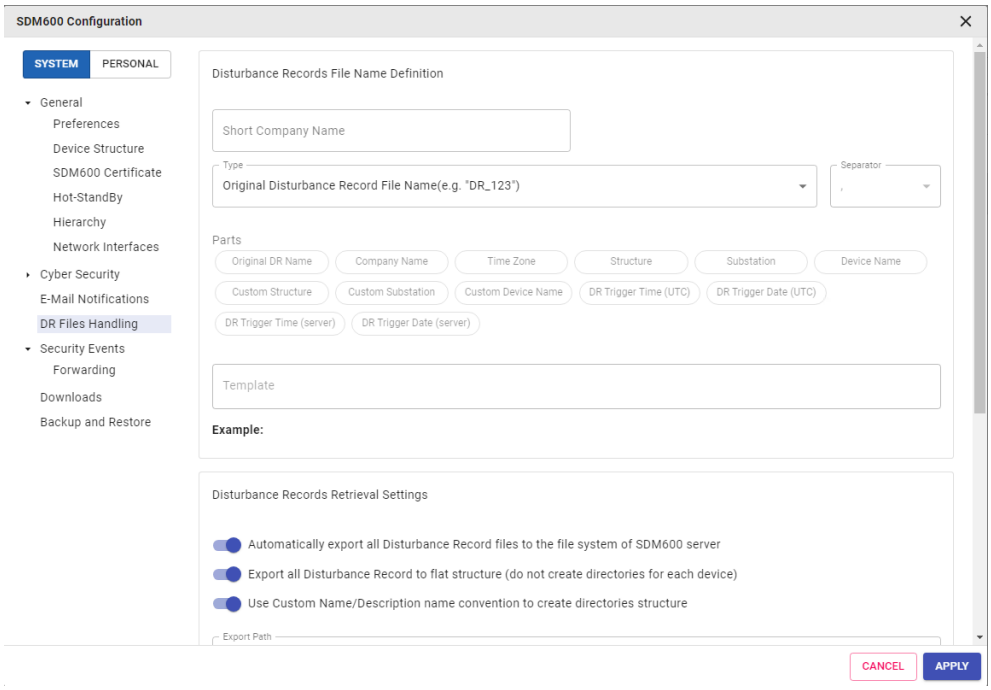


Figure 41: DR file handling

5.8.3.2 Manual export

It manually exports the collected disturbance records to the SDM600 computer. It is possible to export disturbance records files only from a given date range or from a selected level. To execute this function, provide the directory to store the exported DR files or pick direct download as a .zip file, then click the Export all DR Files button.

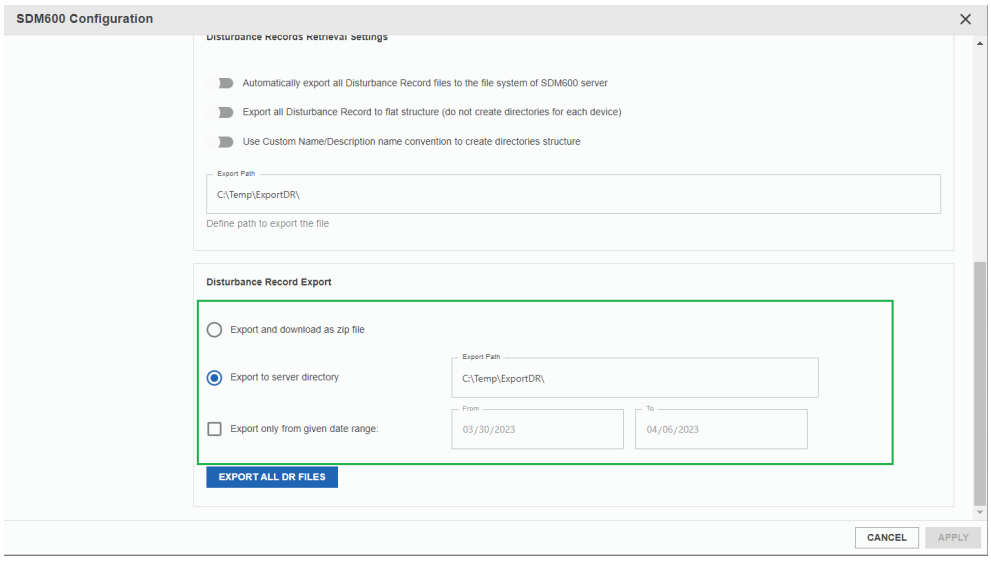


Figure 42: Manual Export of DR

5.8.3.3 Automatic export

It automatically saves the disturbance record files to the SDM600 server folder structure when a disturbance record arrives at SDM600. To enable this function, check the automatically export all DR files to the system option.

By default, SDM600 exports disturbance records files to the folder structure corresponding to the substation structure. It is possible to export all the disturbance records to the single folder. To enable this function, check the export disturbance records to flat structure (don't create directories for each device) option.

The automatic DR file export will save the files on the SDM600 computer. Files will only be appended, available hard disk space is not monitored. It is up to the SDM600 user to ensure the disk space is managed.

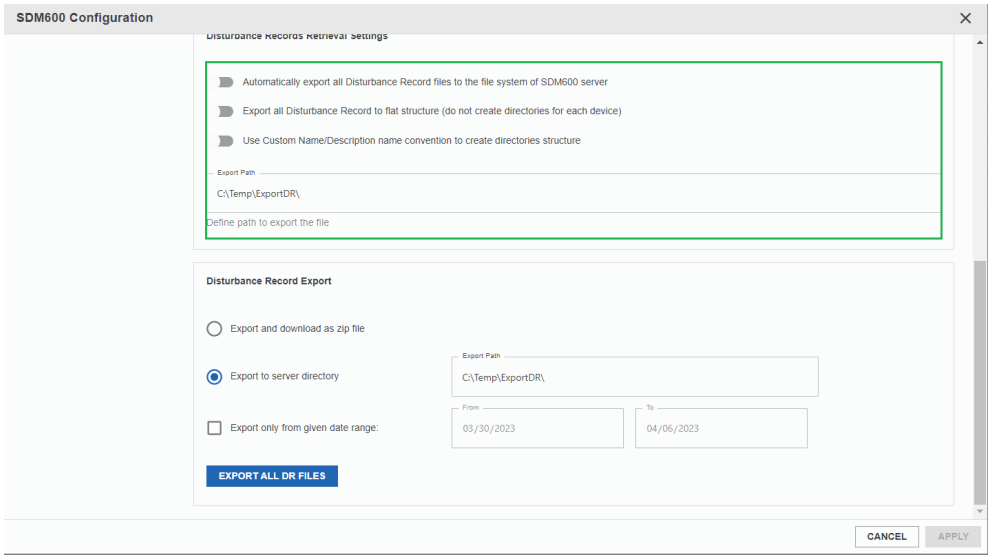


Figure 43: Automatic Export of DR

5.9 Cybersecurity event logging

SDM600 offers the possibility to collect security events or logs that are sent in the format of Syslog from devices and applications.

5.9.1 Operations

Cybersecurity events are collected automatically by SDM600 and are shown to the user in the **Security Events** tab in the **Events Monitoring** Area.

All events are displayed as received from the devices in the raw message format.

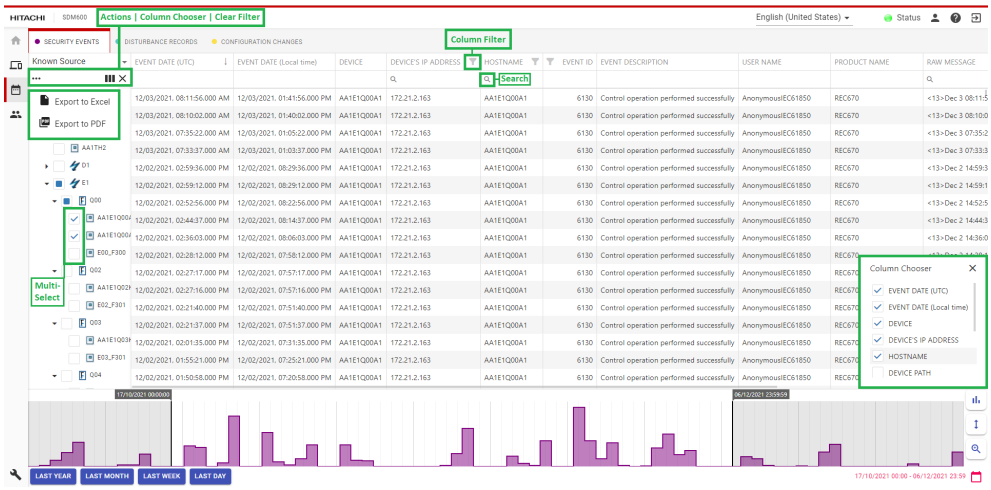


Figure 44: Cybersecurity Events

The Security Event functionalities are described below:

1. Actions: This option allows the user to export the security events in both PDF and Excel format.
2. Column Chooser: This option allows the user to select the columns of the grid that are displayed, see Figure 44.
3. Clear Filter: This option allows the user to clear any filter applied to the columns.
4. Sorting/Filtering: This option allows the user to sort the data in the grid and to edit the filtering criteria to apply to the shown data.

For each security event, SDM600 provides the following information:

1. Event Date (UTC): the moment in time when the event was generated in UTC time.
2. Event Date (Local Time): the moment in time when the event was generated in the user local time.
3. Device: the name of the device from which SDM600 received the security event. This field is resolved based on the Device's IP Address.
4. Device's IP Address: the IP address of the device from which SDM600 received the security event.
5. Hostname: the hostname parsed from the security event, as defined in RFC 5424, RFC 5426.
6. Event ID: the identifier of an event. As defined in "List of Hitachi Energy Security Events"
7. Event Description: a localized description of the event, based on the Event ID.
8. Username: when feasible, SDM600 will try and parse from the security event the username of the user who performed a given operation.
9. Product Name:when feasible, SDM600 will try and parse from the security event the product name used to perform a given operation.

5.9.2 Device integration

Syslog events are actively sent from devices to a Syslog Aggregator, which is SDM600.

SDM600 has to be configured in each device as a Syslog receiver. The configuration is device specific but can usually be done with a local user interface, where the IP address of the SDM600 computer has to be defined.

Syslog can be sent as UDP or TCP. Both are supported in SDM600. However, sending events using both protocols will lead to duplicated entries in SDM600.

If a security event is received that cannot be parsed (for example, due to a missing or wrong timestamp), the raw message will be shown in the *Unparsed* table.

5.9.2.1 General

Syslog events are received as soon as a device is licensed.

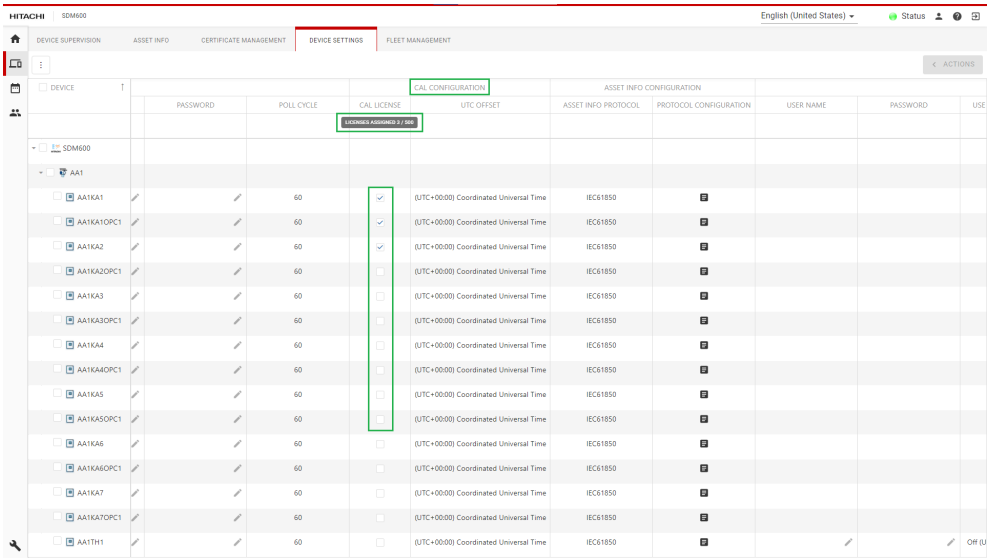


Figure 45: CAL License

In order to retrieve Syslog events from a device, each device has to be licensed. Security Logging Licenses are available for different batch sizes. If the license for a device is disabled, all related Syslog events are deleted.

SDM600 shows Syslog events from unknown or unlicensed devices in the Unknown Source Table. Those events will not be stored to the database.

Syslog messages should be sent using UTC timestamp. However this is not the case for all devices. To correct the timestamp for such devices a UTC offset can be configured.

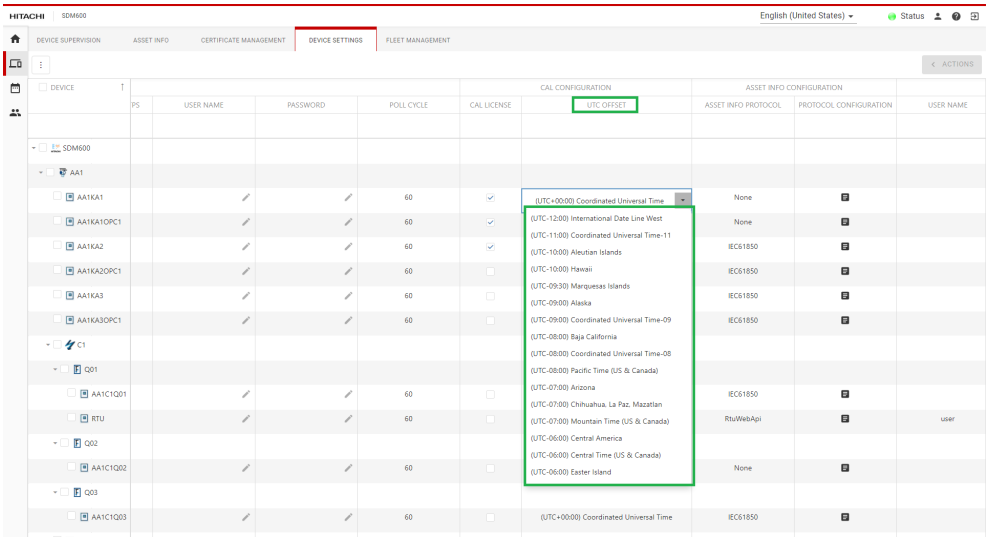


Figure 46: UTC offset Selection

A UTC offset is only required if the Syslog events are not sent with a UTC based timestamp.

Depending on the device configuration, different severity events will be sent to SDM600. It has been observed that the number of Syslog messages can be huge. This will have an impact on the overall performance and CPU load of the computer and might affect other applications installed on the same computer. It is recommended to restrict the severity to Error (3) or higher (Critical, Alert, Emergency).

5.9.2.2 Syslog devices

There is no specific configuration required in SDM600 for Syslog Devices.

To retrieve Syslog messages from a device, it must be licensed for SDM600. Syslog data received from unlicensed devices will not be stored.

In case devices are not licensed, but still send Syslog messages to SDM600, the data will be shown in the **Unknown Source** section of the **Security Event** tab.

Those messages will not be stored in SDM600.

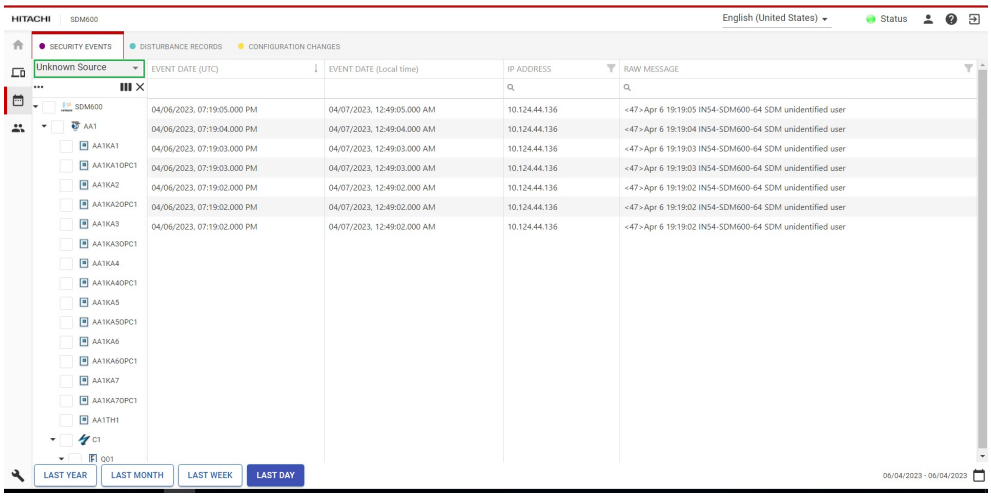


Figure 47: Unknown Source

If the processing of the Syslog message fails, for example, when extracting the timestamp, those messages will be shown in the **Unparsed** section of the **Security Event** tab.

5.9.2.3 Windows computer

SDM600 provides possibility to convert Windows Eventlog entries from Windows PCs to security events. In order to enable the SDM600 Windows Event Log Forwarder, follow steps below:

1. Add the Windows PC as a device in SDM600 (if not yet available).
2. Select the IP address, Device name and provide password for which the SDM600 Windows Event Log Forwarder installer will be generated.
3. Download the installer from the SDM600 System Configuration "Download" section and copy the file to the target computer.
4. Unzip the installer into a directory.
5. Run the installer.

The Windows Event Forwarder installer is tailored to a specific Windows PC. If you need to install the Windows Event Log Forwarder SW on a different computer, you have to create a new installer in SDM600 for the target computer.

Configure Hot-Standby mode before creating the Windows Event Log Forwarder to ensure events are sent to both SDM600 systems.

For Windows Domain joined PC's, the Authentication of SDM600 Services can be changed in the Application Administration Tool to minimize Login/Logout events.

5.9.3 Forwarding the security events to an external system

It is also possible to forward incoming security events to another Syslog server or aggregator.

The External Syslog Aggregator must be configured and running. It must be ensured that Syslog messages are not blocked by a firewall between the SDM600 and external system.

Up to 4 Syslog receivers can be configured in the System Configuration "Security Events - Forwarding" section.

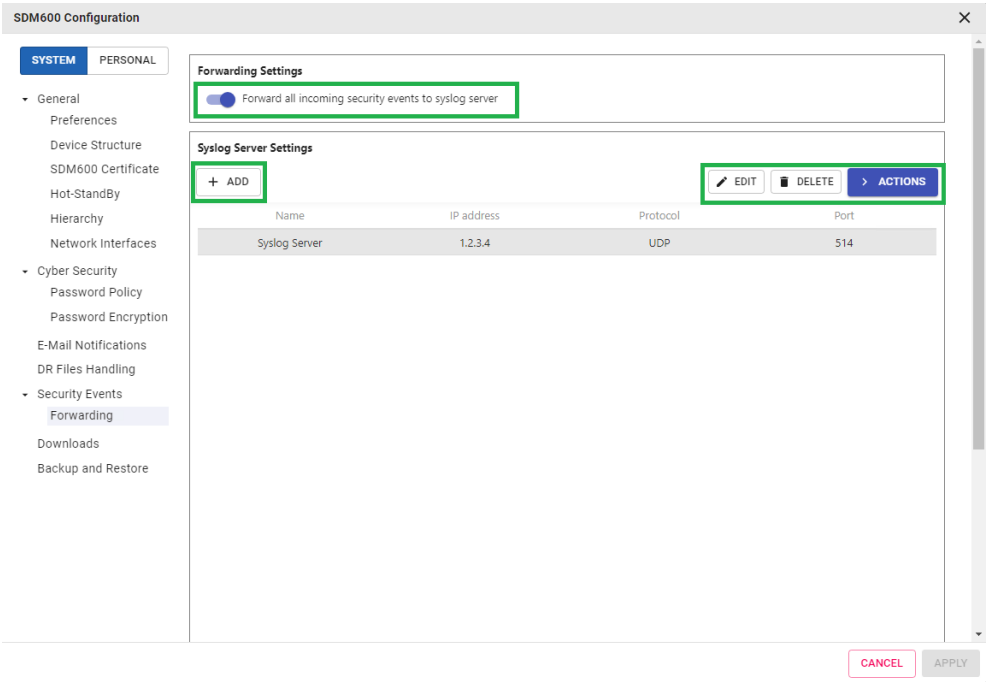


Figure 48: Syslog Forwarding

5.9.3.1 Syslog message format

The following section provides detailed information on the SYSLOG message structure forwarded by SDM600 to a target endpoint.

The following is an example of SYSLOG message forwarded by SDM600:

/IpAddress=192.168.1.55/<9>22-07-2020 10:29:28 10.10.10.254 ABB-UAL:01:Configuration changed successfully modified: AA1KA7OPC1|13220|88|SDM600|SDM600|admin

The SYSLOG structure format in SDM600 can be detailed as follows:

/OriginalSourceIP/<PRI>DD-MM-YYYY HH:MM:SS HOST LogFormatType:LogFormatVersion:EventDescription| AdditionalInformation|InternalEventID| SequenceNumber|SourceDevice|ProductName|UserName

- The OriginalSourceIP shows the original host IP address where the SYSLOG message was generated. SDM600 collects SYSLOG and other messages from different connected industrial specific supported devices (for example, RTU500 series) in an isolated secure network environment and forwards them together to dedicated multiple analysis tools or long-term storage places. In some cases, the original SYSLOG message does not contain the sender's IP address. For accurate identification of the real source of the messages, SDM600 always puts the original host IP address at the beginning of the forwarded message.
- The PRI part, or "*priority*", is calculated from the facility and severity codes. The facility code indicates the type of program that generated the message, and the severity code indicates the severity of the message. The priority code is calculated by multiplying the facility code by eight and then adding the severity code.

The PRI part is not written to file by many Syslog loggers. In that case, each log entry begins with the HEADER.

- The HEADER part contains two fields: TIMESTAMP and HOSTNAME.
  - The TIMESTAMP provides the local time when the message was generated in MM-DD-YYYY hh:mm:ss format.
  - The HOST is the IP address of the SDM600 device where the message was generated.

- The MSG part contains two fields: TAG and CONTENT.
  - The TAG contains 2 fields: LogFormatType and LogFormatVersion.
    - LogFormatType represents the format of the Syslog messages. In case of Hitachi Energy devices, it has its own UAL format.
    - LogFormatVersion shows the version number of the LogFormatType.

  - The CONTENT contains two fields EventDescription and AdditionalInformation which contain only ASCII printable characters (32-126).
    - EventDescription shows the event description in human readable way.
    - AdditionalInformation shows more detailed information in human readable way, not always filled. Very detailed instruction behind the content can be seen in the manual which helps to keep shorten SYSLOG message.

- The FOOTER part contains 5 fields: EventID, SequenceNumber, SourceDevice, ProductName, UserName.
  - EventID shows the ID of the generated security events. Very detailed instruction behind the EventID can be seen in the manual, which helps to keep short SYSLOG messages.
  - SequenceNumber displays messages with sequence numbers because there is a chance that more than one log message can have the same timestamp.
  - SourceDevice represents the original device where the syslog message is generated.
  - ProductName displays the original product where the syslog message is generated.
  - UserName provides information about the actual logged in user (or service user) who generated the event.

5.9.4 Event mapping

Cybersecurity Events are currently only displayed as raw syslog messages. Event mapping to a common Hitachi Energy specific format as it was available in previous versions is not supported.

5.10 The Events Dashboard

The Events Dashboard is a comprehensive tool designed to provide operators with a versatile platform for analyzing events within a power distribution network. This feature offers a range of functionalities to aid operators in inspecting and navigating events across various levels of detail. Operators can choose and adjust a time horizon, allowing for event analysis within specific time periods, providing valuable insights into event patterns over time. The dashboard features a hierarchical representation of the network, encompassing substations, voltage levels, bays, and individual devices. Operators can navigate through this hierarchy to explore events at different network levels.

The main objective of the dashboard is to provide an overview on the system, answering the following questions: what happened, when and where.

- what: refers to what kind of event happened (e.g. Security event, DR file, or configuration change)
- when: refers to the moment in time when the event occurred
- where: refers to which device generated the events

For this reason, the dashboard is the product landing page, that is, the first page users will see after successfully logging in.

Figure 49: The Events Dashboard Page

The dashboard is designed as a scatter plot:

- On the X-axis, the timeline is displayed.
- On the Y-axis, the source of the events is displayed (substations, voltage levels, bays, or devices)
- Each dot represents one or more events of a given kind: the event kind is color coded: DR files are displayed in blue, security events in magenta and configuration changes in yellow.
- Several options are available to fine tune the navigation and the visualization of data, to support the user while navigating the events.

The following sections provide guidance on the options and settings available for the dashboard.

Filtering

The content displayed on the dashboard can be filtered by source and/or by time.

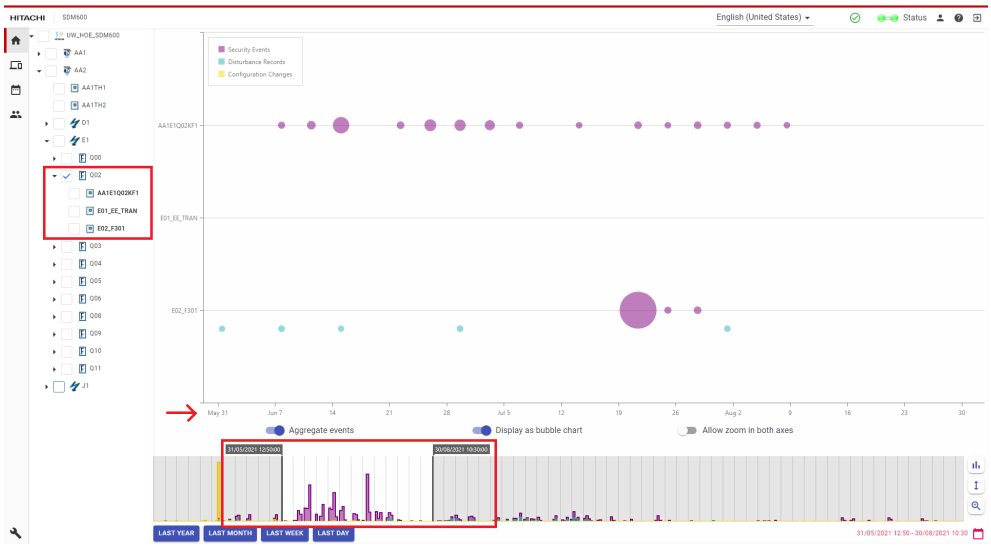


Figure 50: Filtering the dashboard by source and time

Filtering by source means selecting ***where*** the events to display in the dashboard have originated from. For instance, inspecting how the different substations have generated events. Filtering by source is performed by selecting a node in the tree view. The user-friendly tree view interface enables users to expand or collapse nodes within a hierarchy. When a user selects a specific node, the immediate child items at the first level are displayed in the dashboard, enhancing the navigation and exploration of hierarchical data.

Filtering by time means selecting ***when*** the events to display in the dashboard have originated. For instance, inspecting events generated during the last three weeks. Filtering by time is performed by interacting with Time Window component. For more information, please refer to "Filtering Events using the Time Window".

Inspecting the Events

Each data point on the visual representation signifies one or more occurrences of a specific event category, with distinct color coding denoting the respective event category: DR files are displayed in blue, security events in magenta and configuration changes in yellow. When a user hovers the mouse cursor over a data point, supplementary information will be presented in a callout.

Figure 51: Events details in the Callout

To access additional details related to the displayed event, users can interact with the dashboard. Clicking on a data point initiates a drill-down operation, providing more in-depth information. Alternatively, hovering the mouse cursor over a data point triggers a callout, which contains a button for viewing comprehensive event details within the 'Events Monitoring' tab.

- The ***drill-down*** functionality provides a more in-depth exploration of the associated events. The *drill-down* functionality facilitates a hierarchical exploration, automatically selecting the corresponding item in the tree view and adjusting the temporal focus to reveal more precise data. This operation is particularly advantageous when it is necessary to conduct a thorough investigation into a substantial volume of events within the dashboard.

Figure 52: Dashboard - before the drill-down

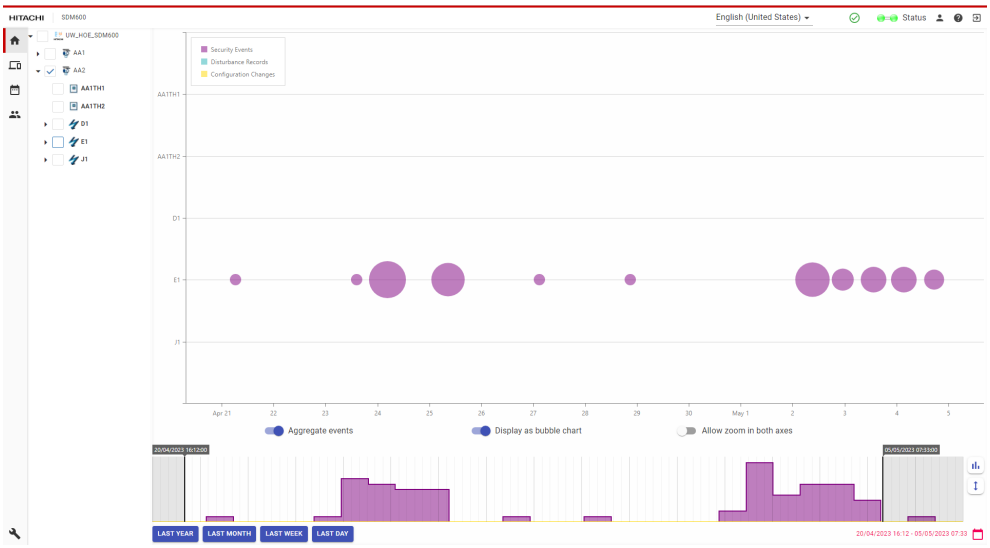


Figure 53: Dashboard - after the drill-down

- For a more comprehensive understanding, the ***view event details*** functionality empowers the operator to visually access the events represented by a highlighted data point of the dashboard within the 'Events Monitoring' grid. This functionality establishes a connection between the dashboard visualization and the grid, showcasing the highlighted events in a tabular format.

The dashboard could be used as a navigational tool for accessing the available data, enabling users to seamlessly transition to a grid representation for a more comprehensive inspection of specific details.

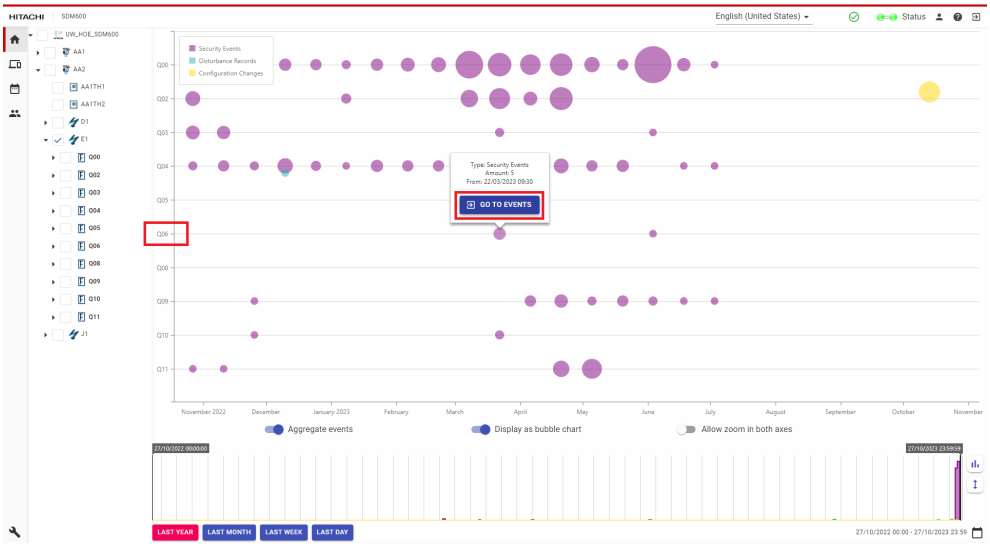


Figure 54: Dashboard - Go to Events is available in the Callout

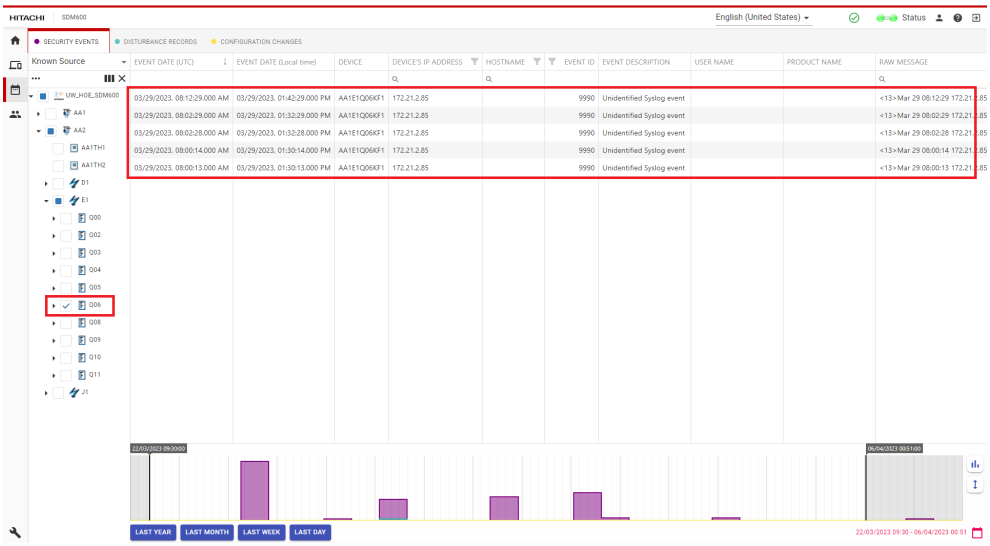


Figure 55: Dashboard - Redirecting to Events Monitoring Section

Visualization Options

The following options are available to fine tune navigation and visualization of the data:

- ***Aggregate Events*** functionality empowers the operator to effectively streamline the visualization of data by consolidating multiple individual events into a single representation. This capability proves particularly valuable in managing densely populated data, as it significantly reduces the number of discrete data points, resulting in a more efficient and comprehensible representation of events on the dashboard. This enhancement in visibility not only facilitates improved navigation but also enables the selection of individual events that might have otherwise been obscured or challenging to discern.

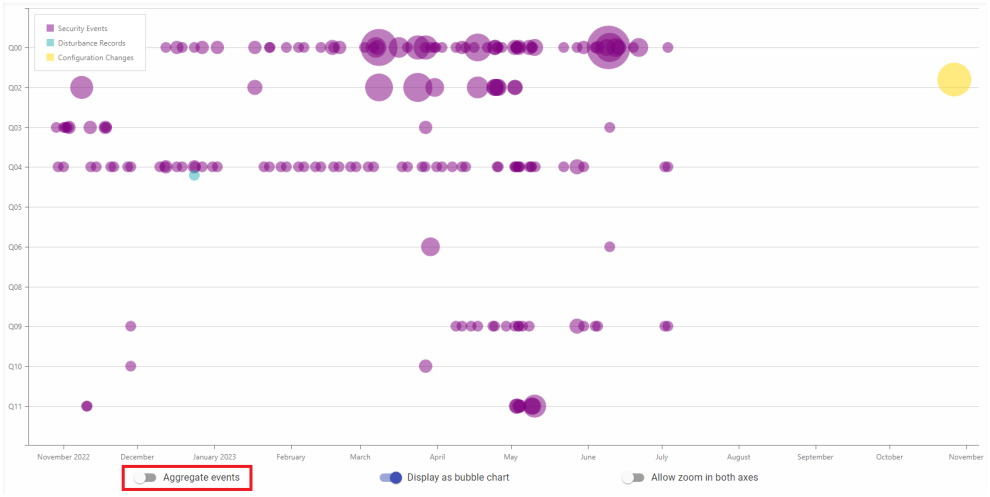


Figure 56: Dashboard - Data aggregation is disabled

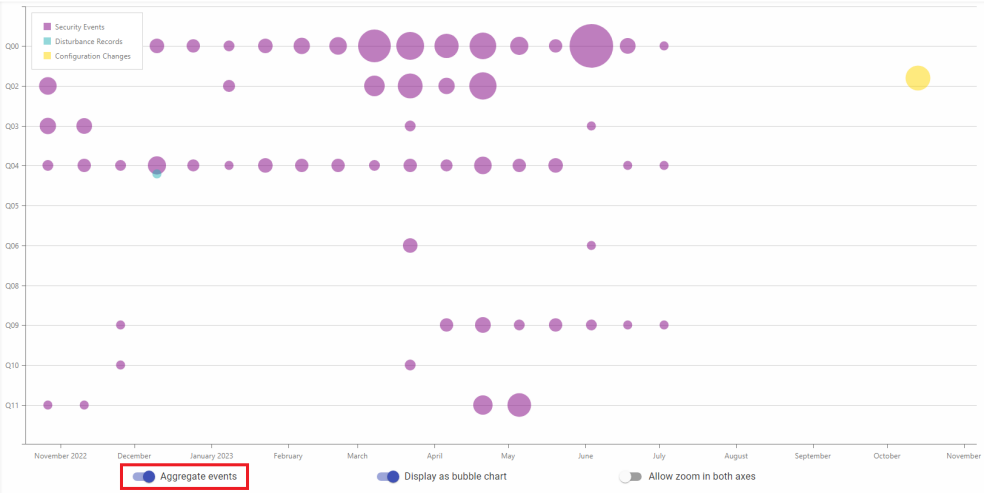


Figure 57: Dashboard - Data aggregation is enabled

- ***Display as Bubble Chart*** allows to display the data as a bubble chart. A bubble chart offers the added dimension of displaying data values using bubble sizes, highlighting their relative significance, whereas a scatter plot shows individual data points without this feature. Activating this feature facilitates the visualization of event quantities represented by each bubble in relation to others. While employing a bubble chart may lead to a denser display, it offers the advantage of promptly conveying information about event peaks.

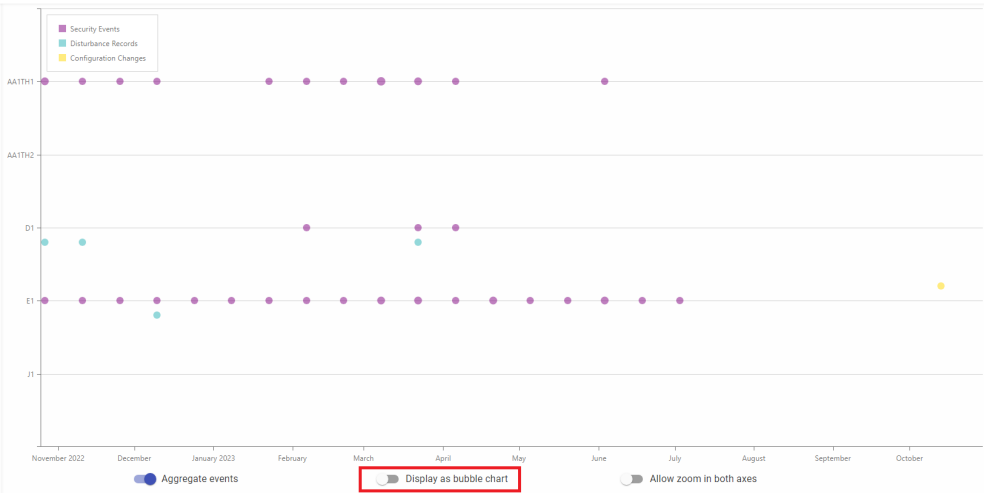


Figure 58: Dashboard - Events are displayed as scatter plot chart

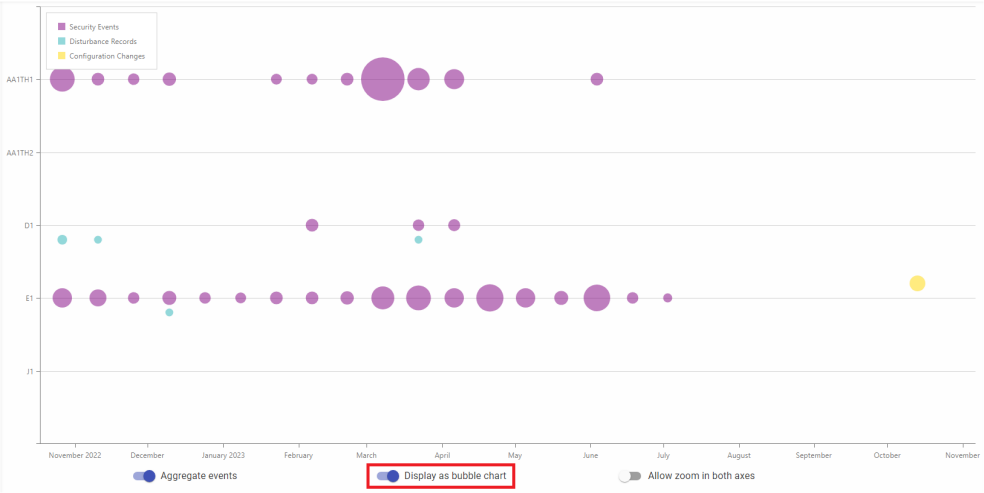


Figure 59: Dashboard - Events are displayed as bubble chart

- The ***Allow zoom on both axes*** feature empowers operators to tailor the behavior of the zoom functionality. To zoom in, simply scroll the mouse wheel forward (zoom in), or backward (zoom out). This capability is particularly valuable for enhancing data visibility in scenarios involving a substantial number of devices or data points. When ***Allow zoom on both axes*** is enabled, any zoom operation will simultaneously affect both the X and Y axes of the chart. Conversely, when ***Allow zoom on both axes*** is disabled, zoom operations will exclusively impact the Y-axis.

Any zoom operation performed on the time axis will not have any implication / effect on the Time Window component.

5.11 Device detail page

SDM600 offers an option for users to right click on any IED/Device and view the details of the selected device.

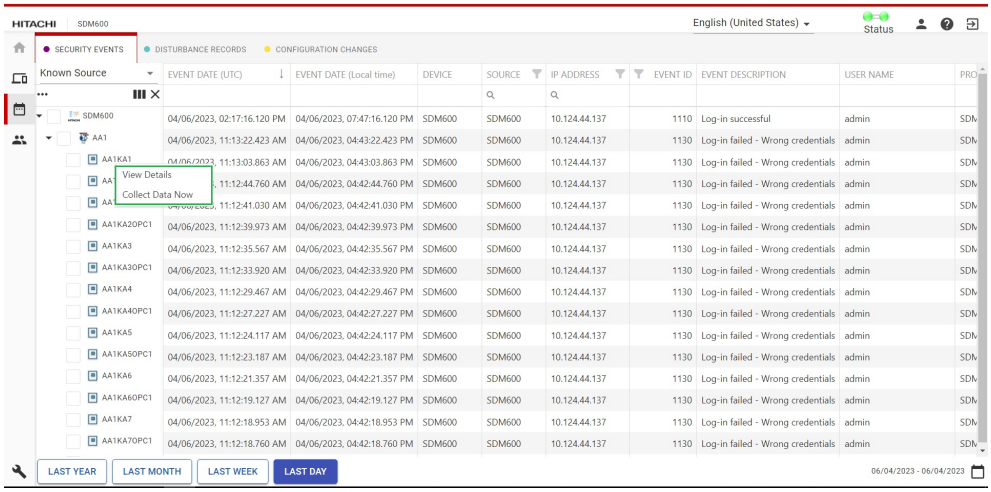


Figure 60: View Details

The Device Detail Page provides quick access to several functionalities, which are described in the following section.

In the *Summary* section, the user can have an overview of the events collected/received from the selected device. The Time Window component allows the user to select the time horizon to be used for time filtering, while displaying all the data available in the system. For more info about the Time Window functionality, please review the dedicated section: "Filtering Events using the Time Window".

The Time Window component displayed in the Summary tab does not filter the events based on the selected device. At any moment in time, the Time Window component displays all the events collected by SDM600 over the selected time horizon.

The following charts are available:

- the pie chart highlights how many events of each kind have been collected/received from the select device
- the stacked-bar char shows how many events of each kind were collected/received from the selected device over the selected time horizon, highlighting spikes of a given event kind.
- the spiderweb chart displays how many events belonging to each security event category have been received from the selected device.

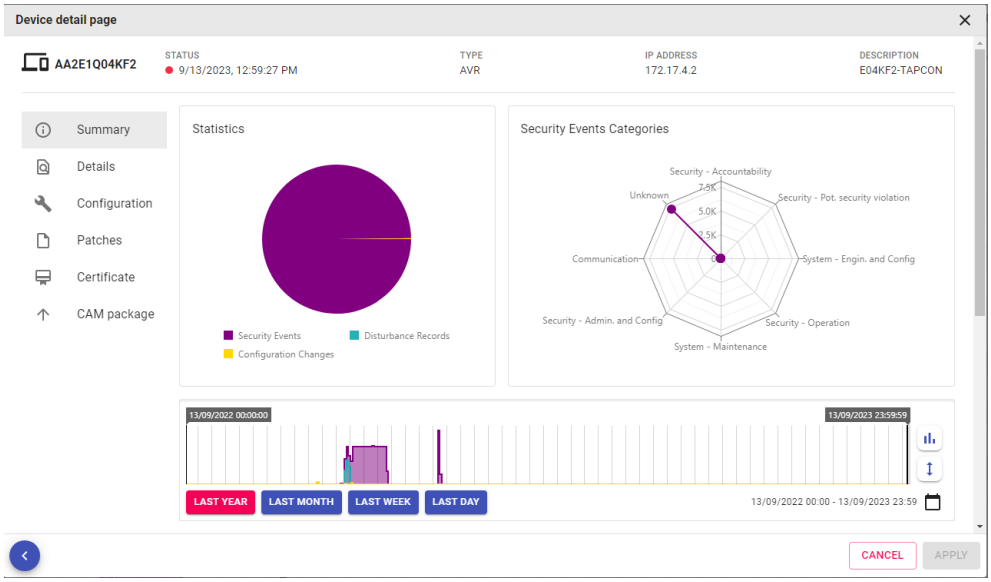


Figure 61: Summary Tab in Device Detail page

The Summary section helps the user understanding what happened in details for the selected device while reviewing what happened in the whole system.
The Time Window component is always visible to provide an overview of all the events collected in SDM600 over the selected time horizon, whereas the other charts show data related to the selected device, supporting the user in understanding how the selected device contributed to the overall big picture.

In the *Service Data* section, the user can view:

- the details of the collected Service Data
- the Windows Patches, in case of a Windows PC
- Configure the protocol to be used to collect the Service Data for the selected device.

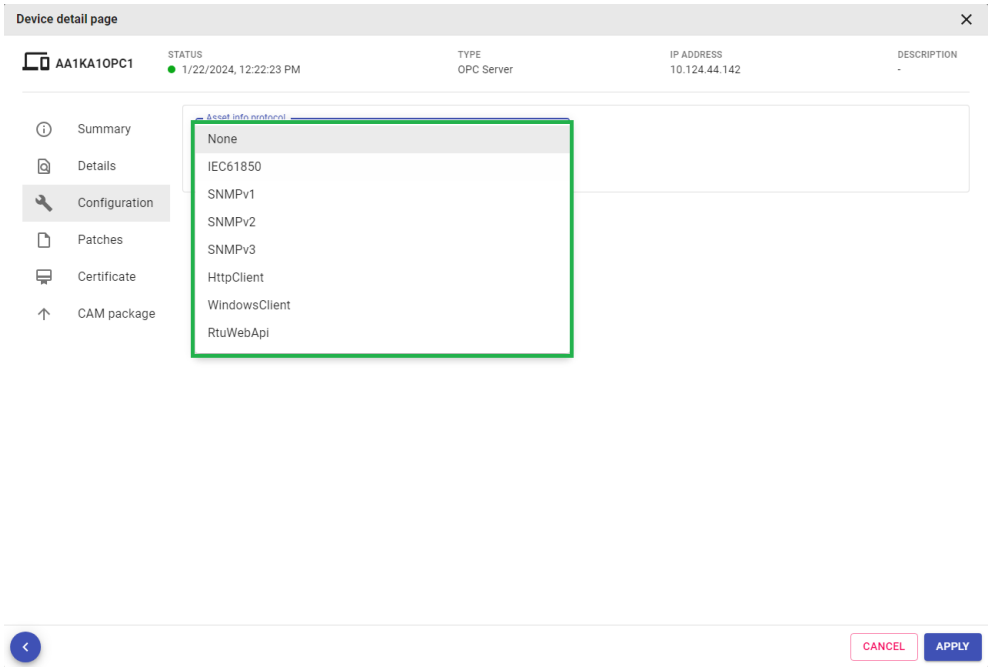


Figure 62: Configure the Service Data Protocol in the Device Detail Page

In the **Certificate** section, the user can generate a new certificate for the selected device, visualise and download the existing certificates.

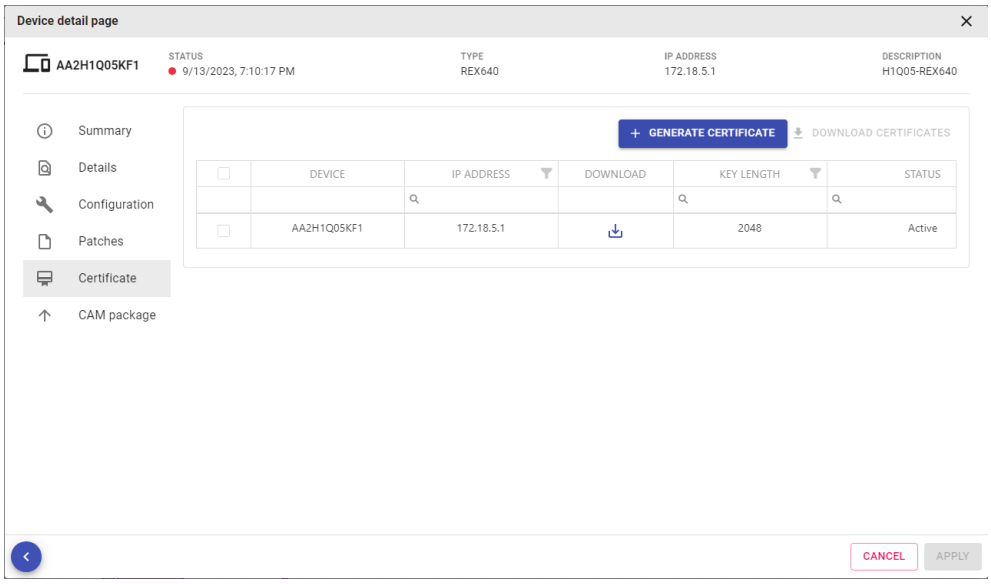


Figure 63: Certificate Management in Device Detail page

In the **CAM Package** section, the user can generate a new CAM Package for the selected device, or download an existing one.

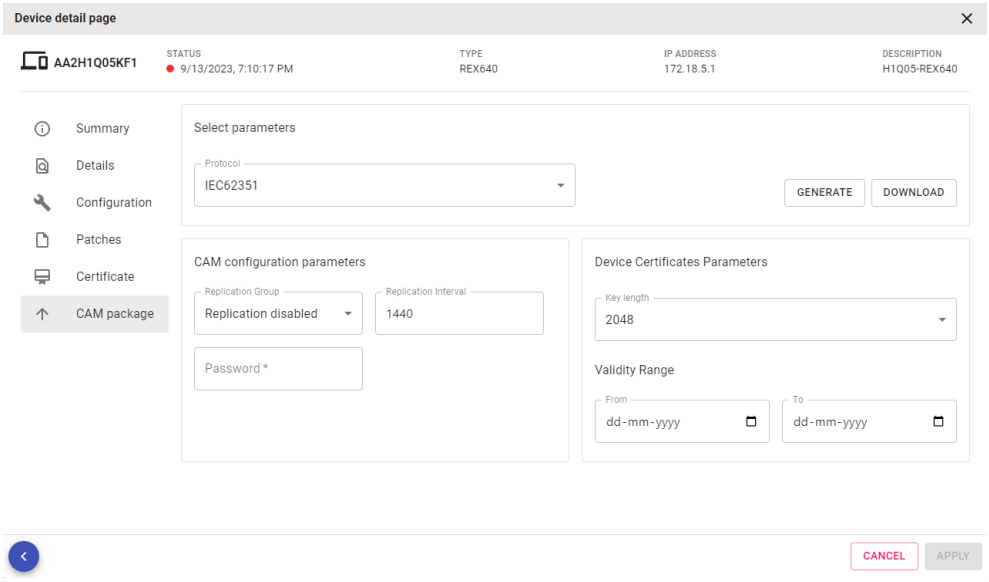


Figure 64: CAM Package in View Details page

5.12 Service data management

SDM600 offers the possibility to collect service relevant data from devices via IEC 61850 or SNMP protocols.

5.12.1 Operations

Service data is shown in two specific areas in SDM600. As a **Configuration Change** event in the Events Monitoring Area and as a **Service Data** displaying the most recent information in the Devices Area.

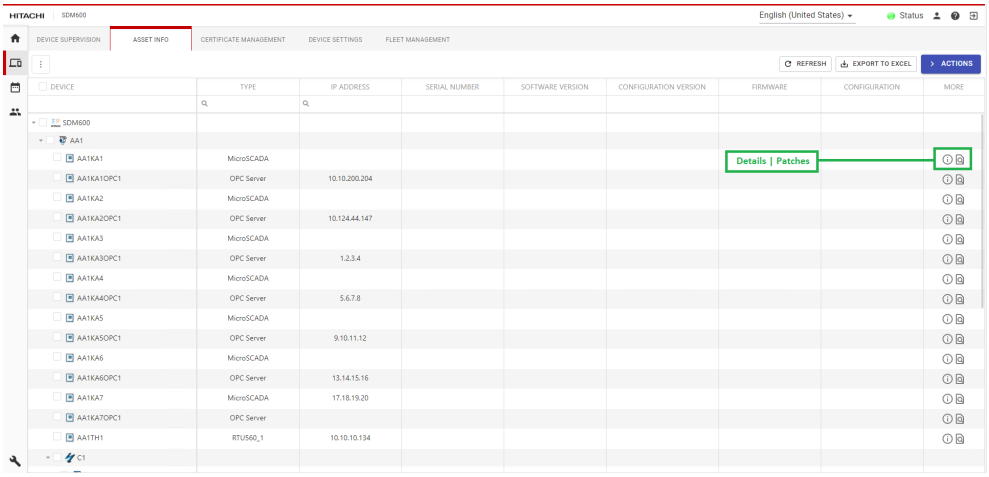


Figure 65: Service Data

It is possible to inspect additional Service data details by clicking on the dedicated icons.

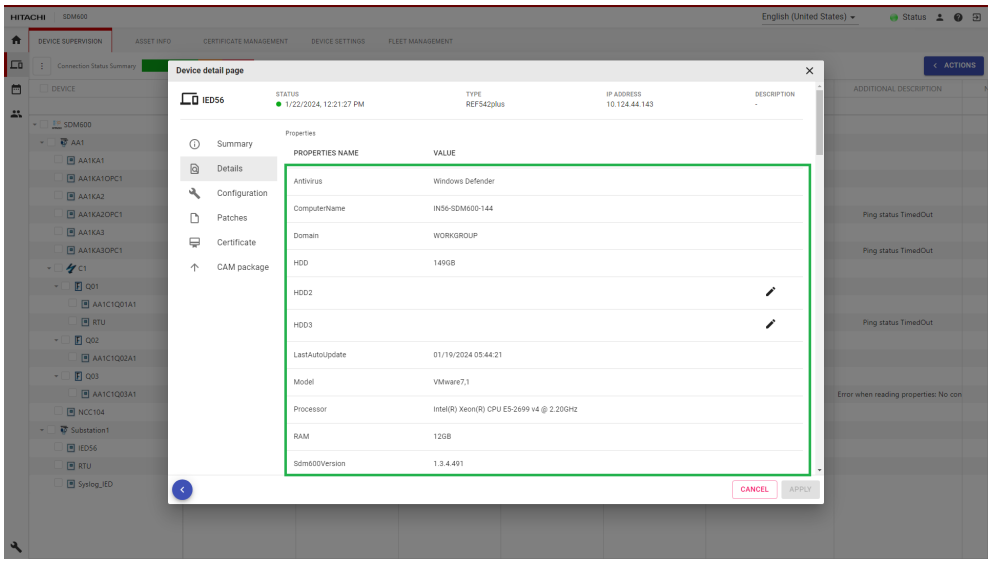


Figure 66: Service Data Details

The Service data can be exported to an Excel sheet on demand.

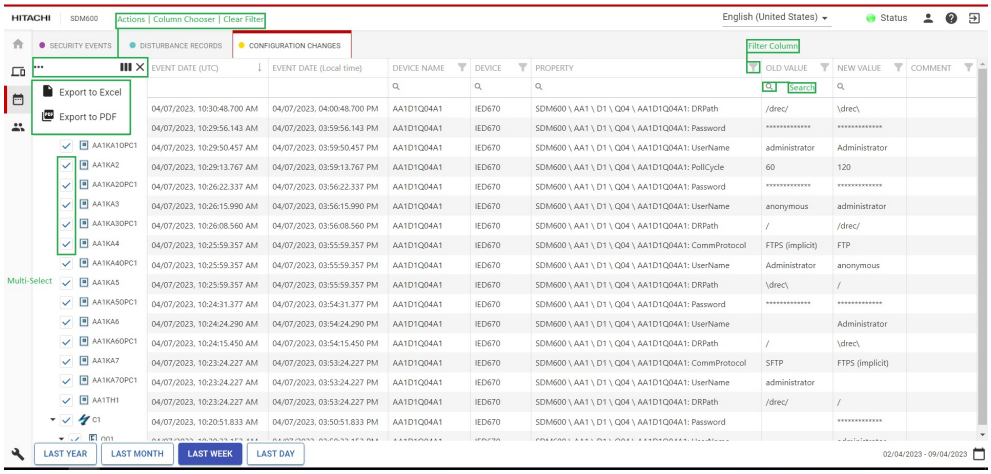


Figure 67: Configuration Changes

The Configuration Changes functionalities are described below:

1. Actions: This option allows the user to export the security events in both PDF and Excel format.
2. Column Chooser: This option allows the user to select the columns of the grid that are displayed, see Figure 67.
3. Clear Filter: This option allows the user to clear any filter applied to the columns.
4. Sorting/Filtering: This option allows the user to sort the data in the grid and to edit the filtering criteria to apply to the shown data.

5.12.2 Device integration

Service data is actively polled from the configured devices via the selected protocols.

5.12.2.1 General

The configuration is protocol specific and has to be performed in the **Device Settings** tab in the **Devices** area.

For aHitachi Energy RTU500, a specific method is used to collect Service Data; from the list of available protocols, select **RTU Web API**. The matching username and password must be entered.

It is possible to configure the Use HTTPs. This is an important cybersecurity setting: please refer to the *Hitachi Energy RTU500 Use HTTPs* section.

5.12.2.2 IEC 61850

IEC 61850 does not need any specific configuration.

SDM600 is reading information from LLN0 and LPHD logical nodes from Ed.1 and Ed.2 devices. Since a lot of information in the specific LNs is optional, SDM600 cannot guarantee to retrieve the same level of information for different devices. It will read all information (mandatory and optional), if available in the IEDs, it will be stored in SDM600.

Service data is optional. SDM600 cannot guarantee to retrieve the same level of information for different devices.

5.12.2.3 SNMP

All 3 versions of SNMP are supported and depending on the selected version, the specific configuration is required.

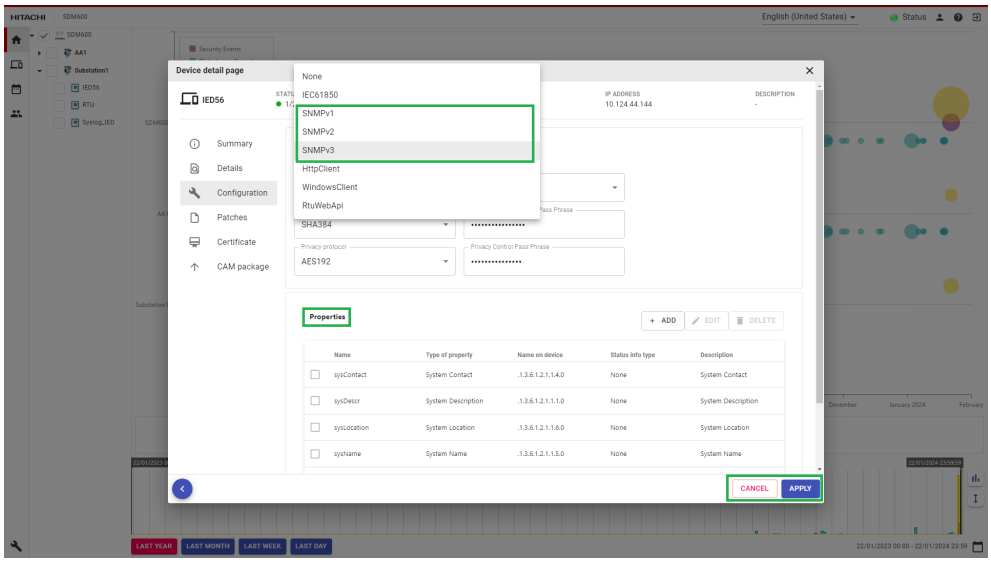


Figure 68: SNMP Configuration

For SNMP version 3, SDM600 supports the following protocols:

- authentication: MD5 (obsolete), SHA1 (obsolete), SHA256, SHA384, SHA512.
- privacy: DES (obsolete), AES, AES192, AES256.

To improve the cybersecurity posture, whenever possible, avoid using obsolete/deprecated protocols.

SNMP provides standardized and device specific information via OIDs. Those OIDs can be mapped in SDM600 to read specific information about selected devices.

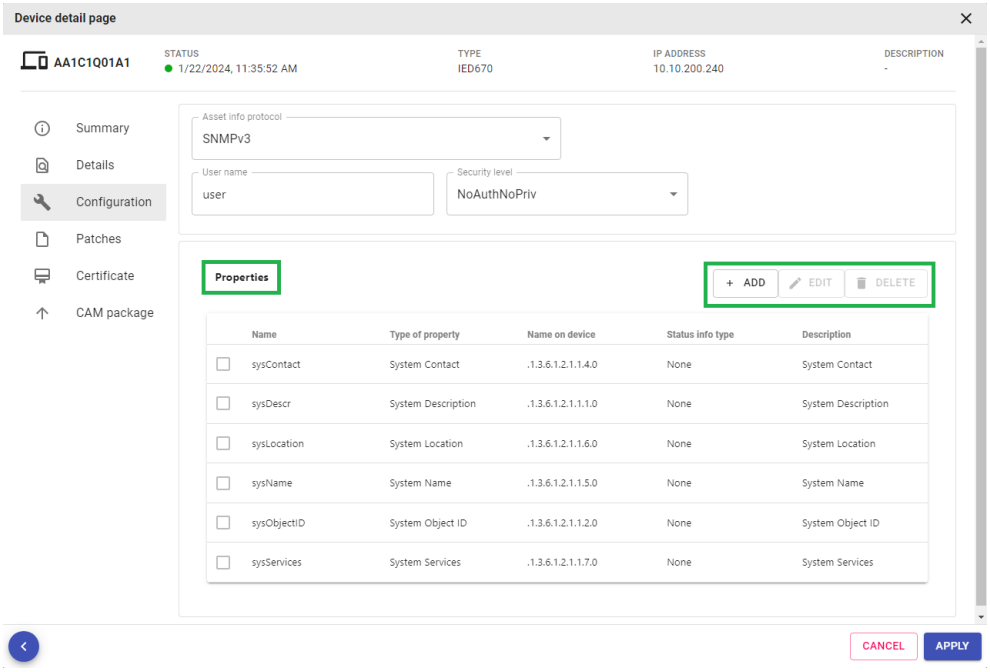


Figure 69: SNMP Properties

5.12.2.4 Windows computer

The SDM600 provides the possibility to read information, such as installed application and patches, from Windows PCs. To enable this functionality, the Windows Agent component must be installed on the PC.

Before installing the Windows Agent, please ensure Microsoft .Net 6 Runtime package is installed on the target Windows PC.

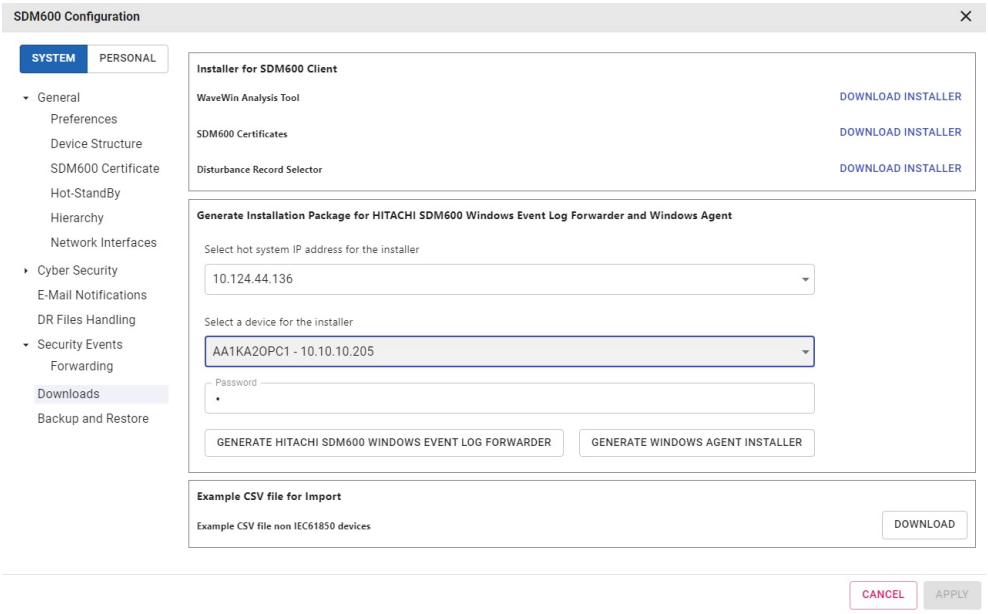


Figure 70: Windows Agent Install creation

1. Add the Windows PC as a device in SDM600 (if not yet available).
2. Select **Windows Client** as the Service Data Protocol.
3. Navigate to SDM600 Configuration-> Downloads Section.
4. Select the SDM600 Default IP, Device and provide a password for which the Windows Agent installer will be generated.
5. Download the installer and copy the file to the target computer.
6. Run the installer on the target system.
7. During the installation provide the password which was given during the creation of Windows Agent Installer.

RESTRICTION

The Windows Agent component is device-specific: the installer generated by SDM600 is valid only for the device for what it was created. Installing the Windows Agent on a different Windows PC than the one for what it was generated will lead to communication issues, ultimately preventing data to be sent to SDM600.

Install the Windows Agent only on the Windows PC for which it was generated.

5.13 Device configuration and firmware management

SDM600 allows to store and manage the firmware and configuration files specific to the Hitachi Energy RTU500 device. For each device, SDM600 stores the last five versions of both firmware and configuration files.

Device Configuration and Firmware Management is only available for Hitachi Energy RTU500 products.

5.13.1 Operations

Device Configuration and Firmware Management functionality is available from the **Fleet Management** tab in the **Devices** area.

The current status is shown in the grid.

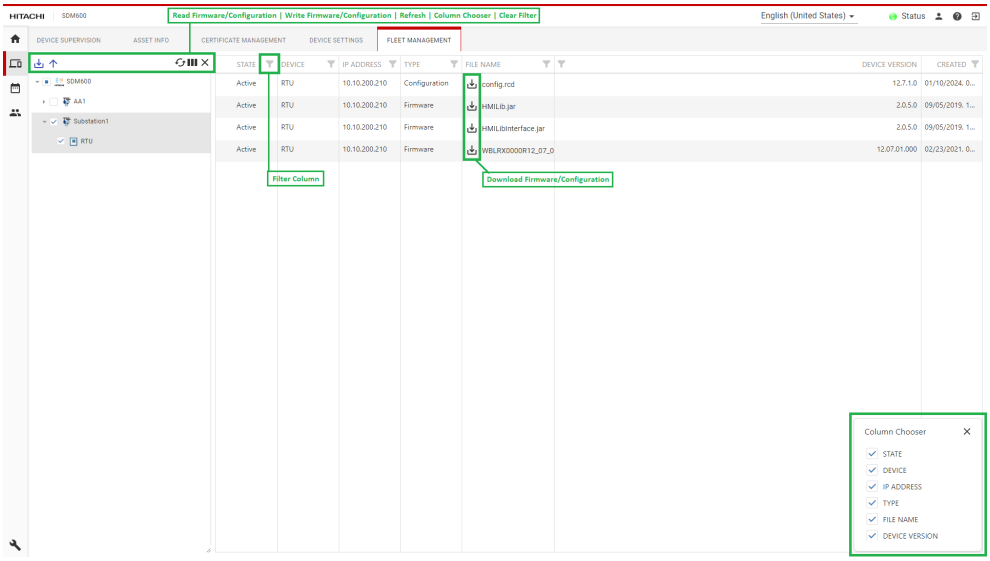


Figure 71: Fleet Management

The Fleet Management functionalities are described below:

1. Read Firmware/Configuration - This option allows the user to read the Firmware/Configuration file from the RTU. Clicking on the button will allow the SDM600 to start the read operation. Once the operation is successful, the data is loaded into the grid.
   A user can select multiple RTU devices and perform the Read Firmware/Configuration for all the selected devices.
2. Write Firmware/Configuration - This option allows the user to write the Firmware/Configuration file to the RTU.

   A user can select multiple RTU devices and perform the Write Firmware on all the selected devices. Writing configuration on multiple devices is not supported.
3. Refresh - This option reloads the grid, allowing the user to show actual data.
4. Column Chooser - This option allows the user to select the columns of the grid that are displayed, see Figure 71.
5. Clear Filter - This option allows the user to clear any filter applied to the columns.
6. Sorting/Filter - This option allows the user to sort the data in the grid and to edit the filtering criteria to apply to the shown data.

5.13.2 Device integration

The RTU specific configuration is done in the **Device Settings** tab under the **Devices** section.

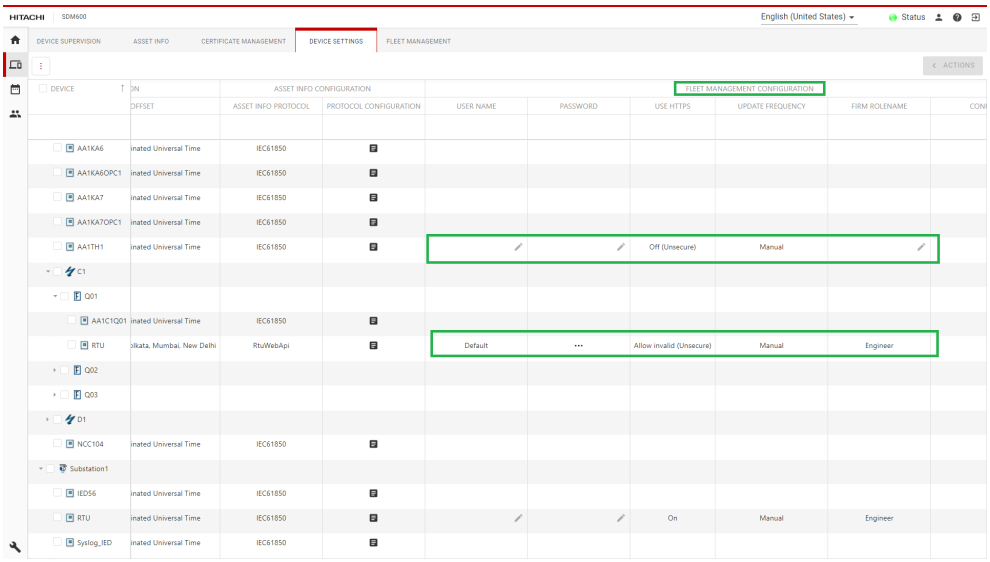


Figure 72: Fleet Management Configuration

The following parameters must be configured:

- Username and Password: configure the username and the password of the RTU user that SDM600 will use to read/write firmware/configuration files. Configuration and Firmware File Management require specific user roles. To be able to read/write files on the RTU500, the selected user must have the correct role assigned.
- Update Frequency: SDM600 can be configured to automatically read firmware/configuration files from the RTU device. Users can configure the polling cycle (Daily, Weekly, Monthly). The default value is Manual. When Manual is configure, SDM600 will not read automatically files from the device: the user can trigger the read operation at any time from the Fleet Management tab.
- Firm Rolename and Config Rolename: Configuration and Firmware File Management require specific user roles. Specify which role to use to perform the firmware and/or configuration files operation.

Fleet Management functionality is only available for RTU devices. Therefore, the user can configure the Fleet Management parameters only for devices having RTU as Device Type.

It is recommended to define a specific user for Firmware and Configuration file Management in the device.

This functionality is only available for Hitachi Energy RTU500 family devices with a Firmware Version >= 12.

It is possible to configure the Use HTTPs. This is an important cybersecurity setting: please refer to the *Hitachi Energy RTU500 Use HTTPs* section.

5.14 Certificate management

SDM600 uses Digital Certificates (X.509) for internal communication encryption and for device-to-SDM600 communication (for example, CAM).

In SDM600, it is possible:

- to manage the root certificate used in SDM600 itself.
- to create and manage the certificates used for the devices.

The following sections provide in-depth guidance on the certificate management functionality in SDM600.

5.14.1 Handling the SDM600 Root Certificate

To review and manage the root certificate used in SDM600:

1. Open the SDM600 Configuration dialog (wrench icon)
2. Select **System** configuration
3. Navigate to the **SDM600 Certificate** tab

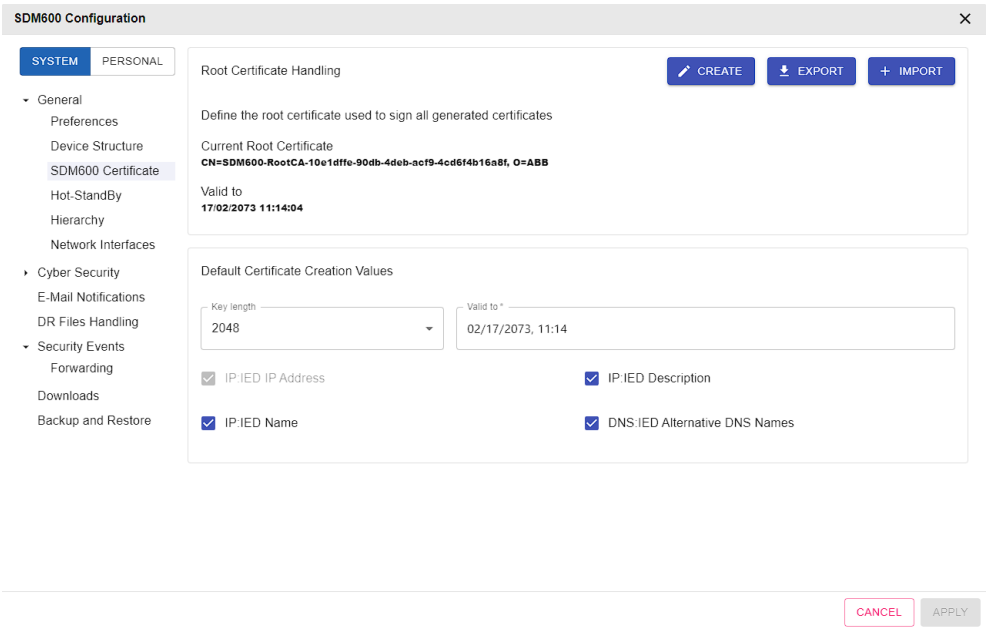


Figure 73: SDM600 Certificate Settings

In the Certificate Management Settings different properties of the certificates such as key length, validtiy and certain certificate entries are configured.

The settings in the Certificate Management affects all the certificates generated by SDM600 (including CAM certificates). Increasing the default certificate key length may negatively impact device performance. Misconfiguration of the certificate properties may cause SDM600 to stop working.

Additionally, it is used to manage root certificates and generate device certificates for general purposes. You can create a new root certificate via the *Create* option. Alternatively, you can import one from a file. Lastly, you can also export your Root certificate.

Keep the CA private key file in a safe place. Unauthorized use of a private key can compromise SDM600 security.

5.14.2 Device Certificate Management

In SDM600 the **Certificate Management** tab in the **Devices** area, certificates are visualized and can be created for every device. Based on your selection in the device tree, you can see certificates for all devices or just a specific one.

The view shows the following attributes of a certificate:

- **Devices/IP address:** This column shows the Name/IP of the device to which the certificate belongs.
- **Origin:** The origin field provides information on why the certificate has been created. The possible values of the origin field are:
  - **General Purpose Certificate**: this certificate has been manually generated by a user in SDM600.
  - **SDM600 Certificate**: this certificate is automatically generated and it is required by SDM600 functionality. E.g. Root CA Certificate, certificates used to ensure secure communication among different SDM600 instances.
  - **CAM Certificate**: this certificate is generated when configuring CAM functionality and it is required by CAM functionality.
  - **Windows Agent Certificate**: this certificate is automatically generated when creating the Windows Agent installer package for a device. This certificate is used to ensure the secure communication between SDM600 and the Windows Agent deployed on a target device.
  - **Windows Event Log Forwarder Certificate**: this certificate is automatically generated when creating the Windows Event Log Forwarder installer package for a device. This certificate is used to ensure the secure communication between SDM600 and the Windows Event Log Forwarder deployed on a target device.
  - **SDM600 HTTPs Certificate**: the automatically generated SSL Certificate used in IIS to host the SDM600 web site.
- **Status:** The status of the certificate displays one of the following values:
  - **Active**: the certificate is valid and in use
  - **About to expire**: the certificate will expire in 3 months or less
  - **Expired**: the certificate has passed its expiration date
  - **Obsolete**: the certificate is not in use anymore
- **Valid From/To-** Validity period of the Certificate.
- **Download-** This allows the user to download the latest generated certificate for the device.

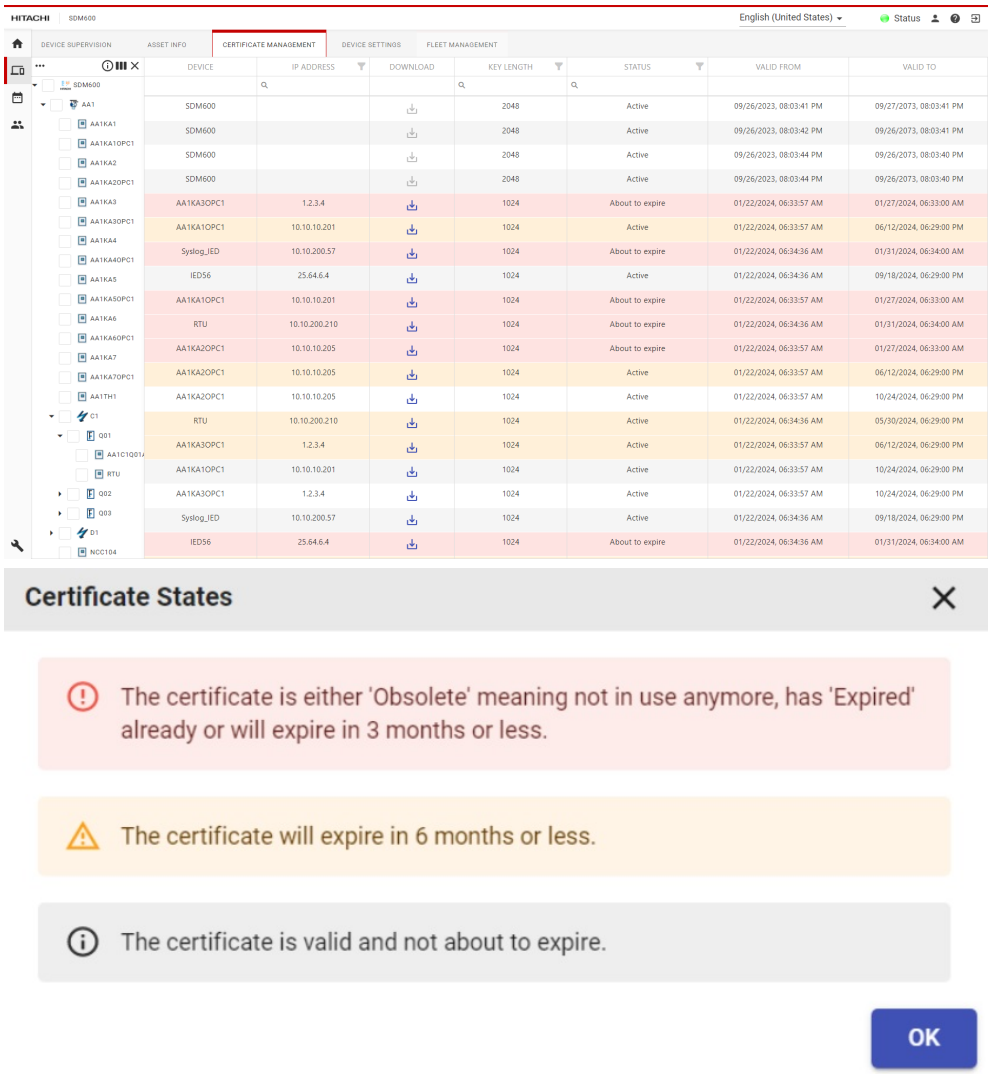


Figure 74: Status- Certificate Management

SDM600 can only track and visualise certificates created while using SDM600 1.3.2 or newer.
In general, certificates created while using older SDM600 versions will not be displayed in the Certificate Management tab, as SDM600 was not tracking certificates in the older versions.
When updating to SDM600 1.3.2 or newer from and older version, only certificates having General Purpose Certificate as Origin will be visualised in the Certificate Management tab.

The certificates available for a device can be visualised by opening the Device Detail Page for that device:

- existing certificates can be reviewed and downloaded
- new certificates can be created for the current device

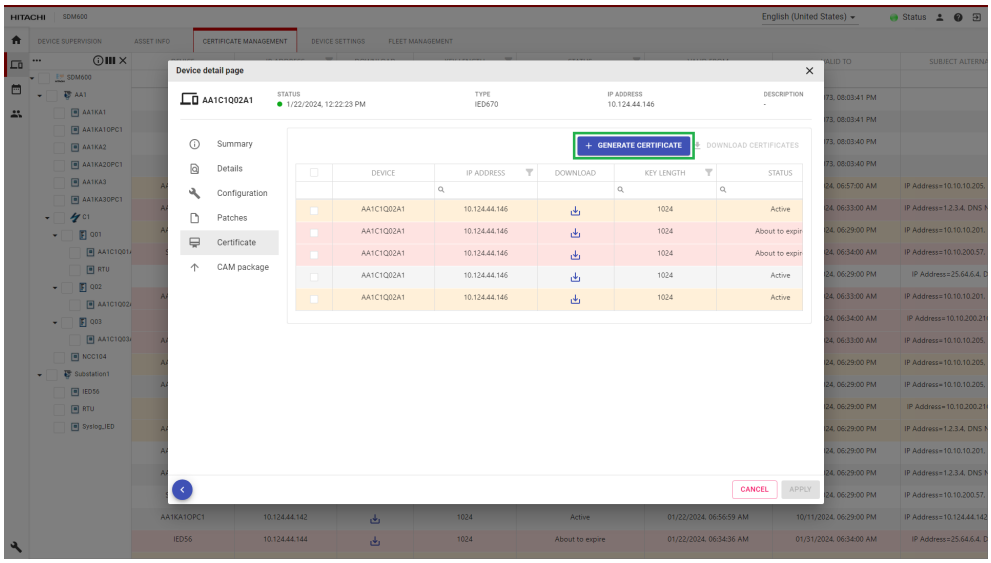


Figure 75: Device Detail Page
Certificates available for the selected device

SDM600 allows the creation of general purpose certificates for every configured device. These certificates can, for example, be used for securing web connection or file transfer (provided that the device offers this function). While creating a new certificate, the user can configure:

- **Password**: this field allows the user to configure the password used in the certificate
- **Key Length**: this field allows the user to configure the length of the RSA key of the certificate. Increase the value for improved cybersecurity, but higher CPU usage.
- **Valid from** and **Valid to**: these fields allows the user to configure the validity range for the certificate, specifying a starting and an ending date.
- **Subject Alternative Name**: this *read-only* field shows the currently configured subject alternative name that will be used when the certificate is created. The user can edit the subject alternative name by clicking on the pencil button: a modal dialog will be displayed allowing to add and remove IP addresses or DNS names.
  - For each device, the value of the last configured subject alternative name is *remembered* and *provided* as default value the next time we want to create a certificate. You can inspect the value in the *read-only* field and edit it via the pencil button.
  - SDM600 will prevent the user from removing the IP address of the device and the name of the device from the subject alternative name. This is done to ensure that all functionality could work properly.

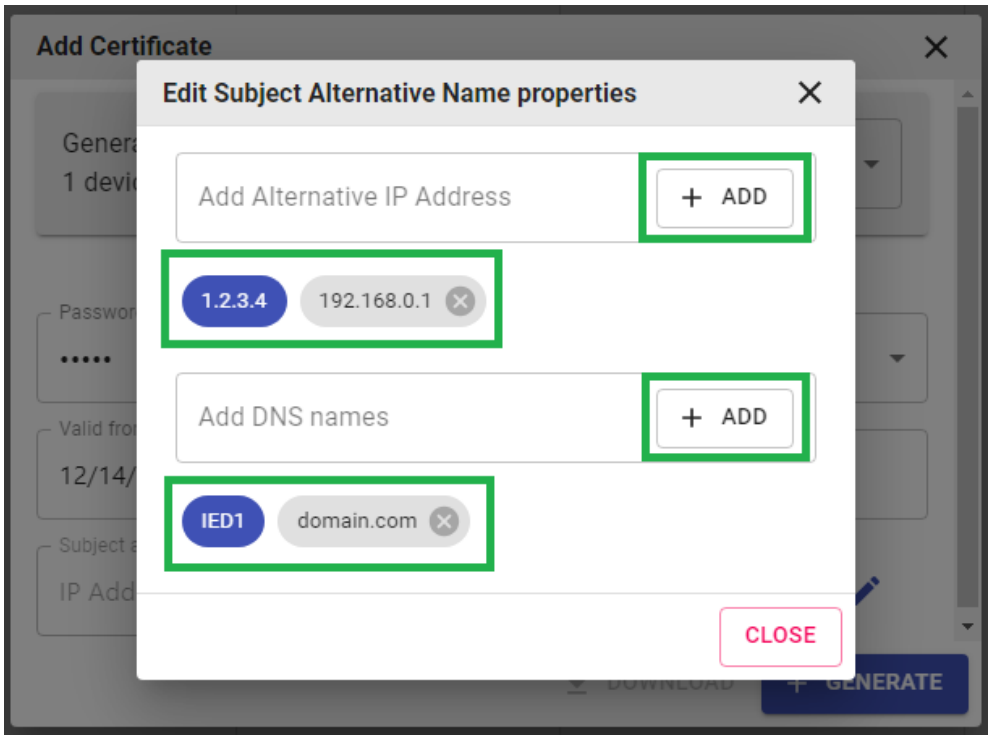


Figure 76: Custom SAN Properties

To increase efficiency, bulk certificate generation is available, allowing the creation of a new certificate of each selected device. To perform a bulk certificate generation, follow the next steps:

1. Select multiple devices in the device tree
2. Navigate to the actions (three dots) and expand the menu
3. Click on **New Certificate**
4. A modal dialog is visualised allowing the configuration of the required parameters for the new certificate
5. Click **Generate** to create a new certificate for all the selected devices.

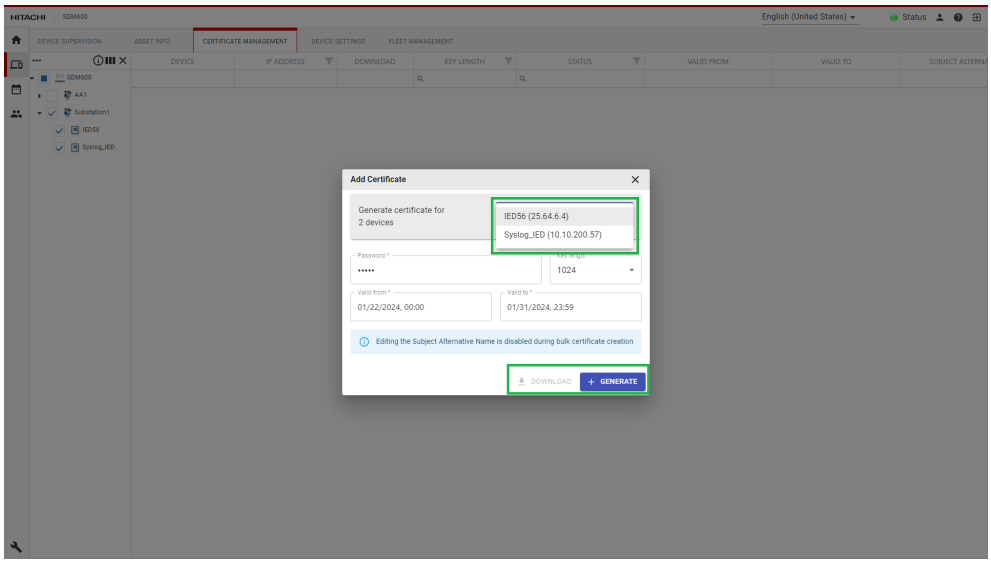


Figure 77: Bulk Certificate Generation

RESTRICTION

LIMITATIONS APPLY!
Editing the certificate's subject alternative name is disabled for bulk certificate creation. During bulk certificate creation, each device's certificate will be generated with the subject alternative name set to the default subject alternative name value configured for that device.

Once downloaded, the certificates generated with SDM600 must be manually transferred to the device. This is typically done using the device configuration tool or web interface.

System Certificates cannot be downloaded. Only certificates belonging to devices can be downloaded.

Certificates have an expiration date. Ensure that certificates will be replaced before they expire. SDM600 provides the possibility to configure e-mail notification, to ensure that the relevant people are notified about the imminent certificate expiration.

5.15 Email Notification

SDM600 supports e-mail notification for specific functionality or events. The notification is user specific and can be modified by clicking on the individual notification.

To enable e-mail notification, an external e-mail server is required. Ensure that required ports between the SDM600 computer and the email server are not blocked by a firewall.

E-mail notification is configured in the System Configuration. The following information is required for a successful e-mail notification setup:

- The address of a separate and running e-mail (SMTP) server, for example, *smtp.yourdomain.com*
- A valid SMTP username and password
- The SMTP port number, normally port 25, 465 or 587 is used
- How to access the SMTP server: secure (via SSL/TLS) or non-secure
- A valid e-mail address that will be used as sender address (for example, *sdm600@yourdomain.com*)

After configuration parameters have been entered, a test email can be sent.

The SDM600 does not come with its own SMTP server. In general, a user can set up their own SMTP server or one that is provided by the internet service provider. For information on an SMTP server that you can use and the relevant information (such as address and port numbers), consult your IT department.

It is mandatory to fill in all the required fields in this configuration setting.

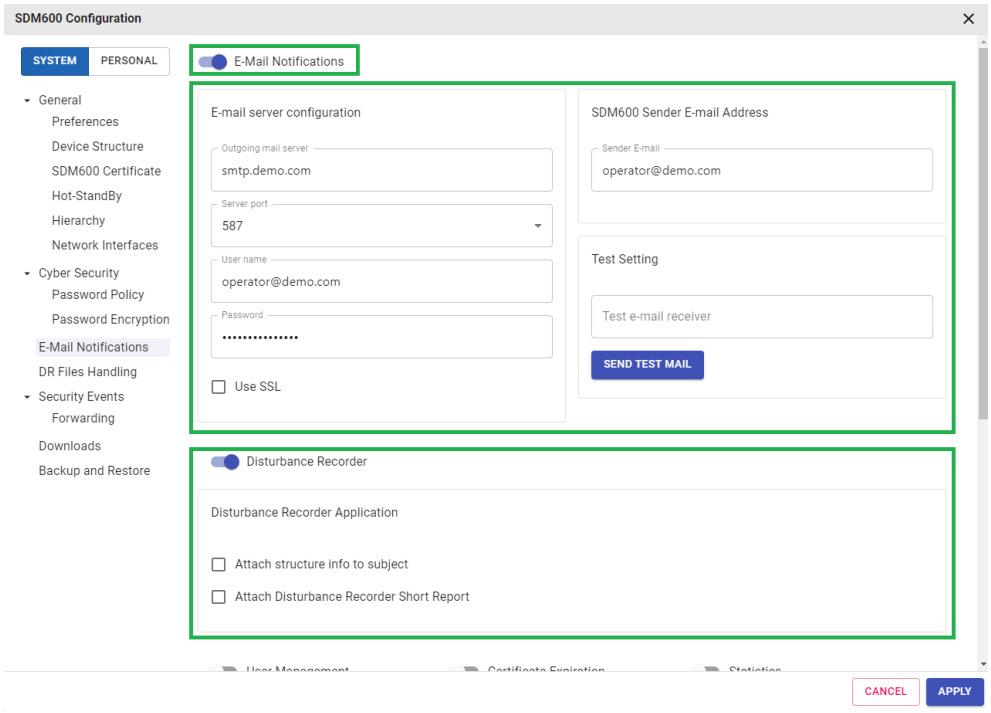


Figure 78: Configuring Email Notification Server

Email notification can be activated for existing local users or for user configured email address. It is possible to add a new entry to the distribution list but simply clicking on the + button: enter a display name and the matching email. For both local users and manually entered email addresses, to configure the email notifications, simply select the matching check boxes.

If a manually entered email address is no longer required, it's possible to remove it from the list by clicking on the trash bin. It is not possible to remove the entries for the local users.

Press **Apply** to save the changes.

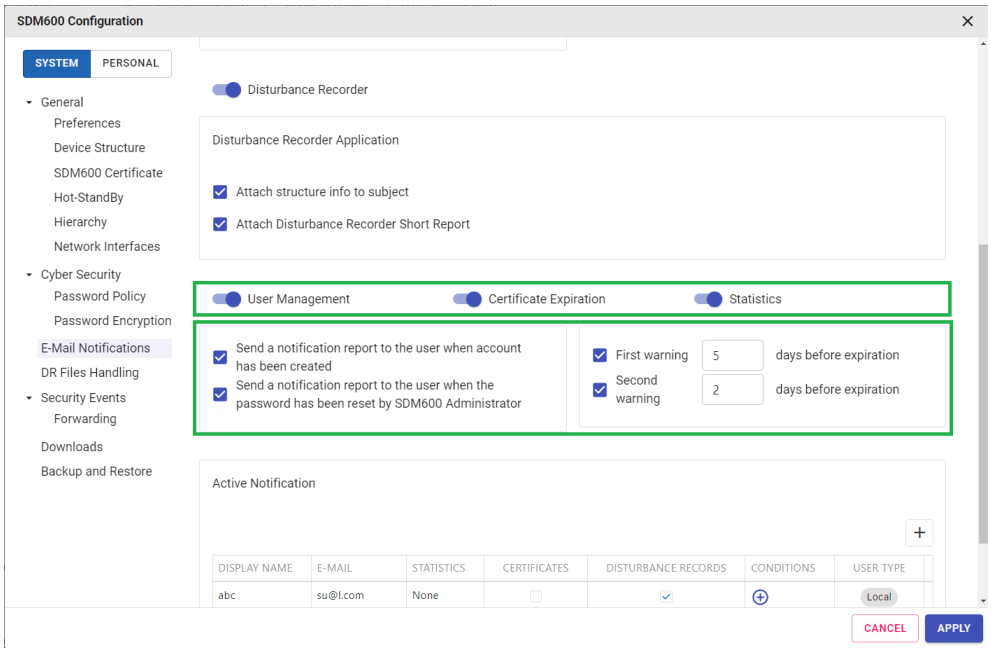


Figure 79: Editing the Email Notification distribution list

5.15.1 DR data management notifications

SDM600 offers user to configure DR Email Notifications for specific users. A user can toggle ON the **Disturbance recorder** option and enable the sub-options as per the user requirement.

- Attach structure info to the subject
- Attach Disturbance recorder short report

Before enabling the Attach Disturbance recorder short report, make sure the Automatic Short Report Generation is enabled in the **DR File Handling** tab.

A user should enable the Disturbance Record in the Active Notification column for specific users in order to receive e-mails. Also, the user has the possibility to customize condition of the e-mail notification for disturbance record.

For example, a user can configure conditions like Trigger Channel or Device Name.

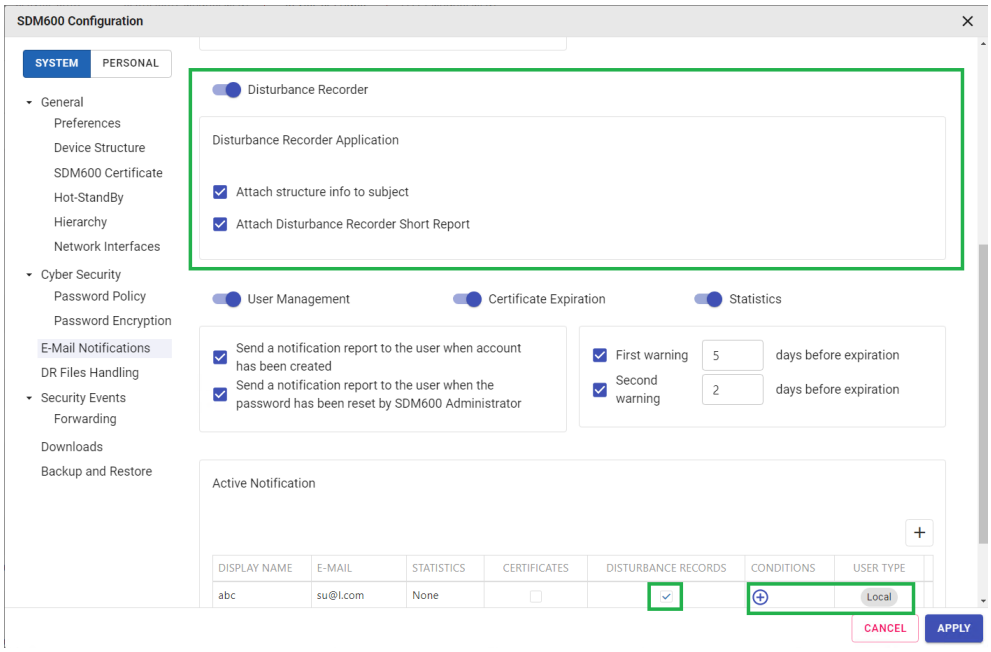


Figure 80: Email Notification DR

Email notification can be changed, by clicking on the **DR** Notification for a specific User.

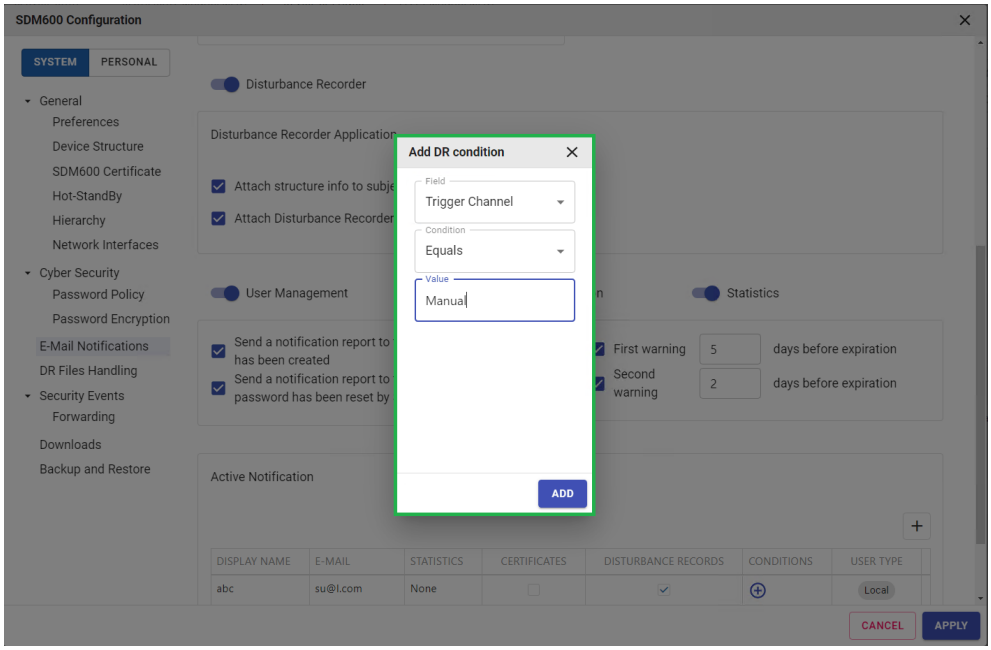


Figure 81: Change DR Email Notification

5.15.2 User Management Notifications

After enabling the User Management Notification, e-mails will be sent to the specific user (specified e-mail address of the user) for the following conditions:

- When a new User is created, the email will contain the initial password (which must be changed at first login).
- The User Password has been reset by a SDM600 Administrator User.
- The administrator changes the user's password. When this option is activated, whenever the administrator of the SDM600 changes a user's password, an e-mail is sent to the user's e-mail address, informing the user of the new password.

The User Management Notification will contain the initial password, which must be changed at first login.

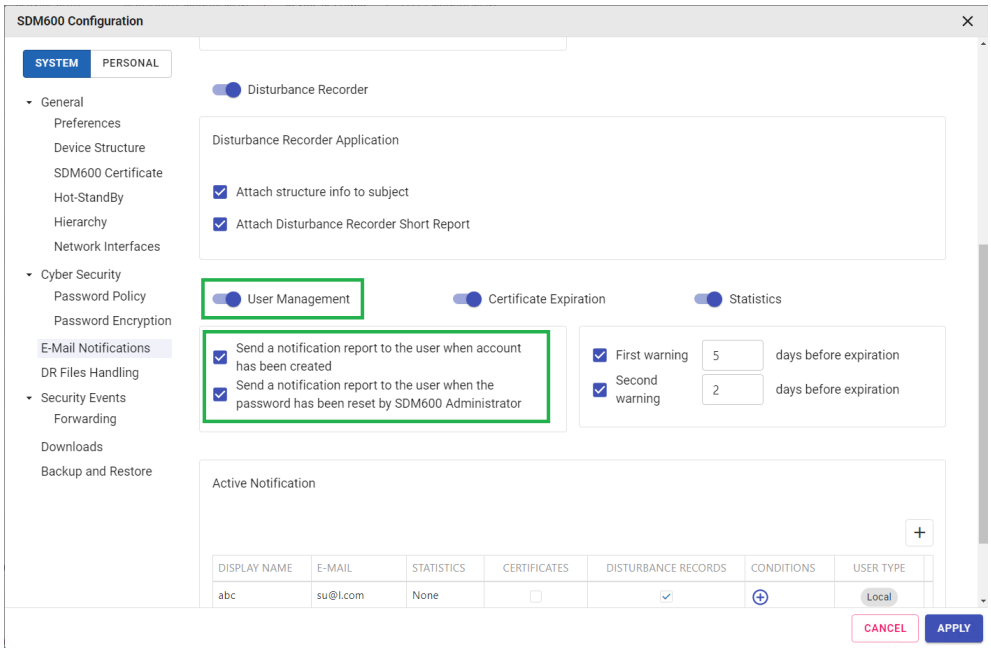


Figure 82: Email Notification User management

5.15.3 Certificate Expiration Notifications

After enabling the Certificate Expiration Notification, e-mails will be sent to the Enabled users in the Active Notification before the X.509 Certificates expire.

Since replacement of certificates must be done before expiration, two warnings can be configured.

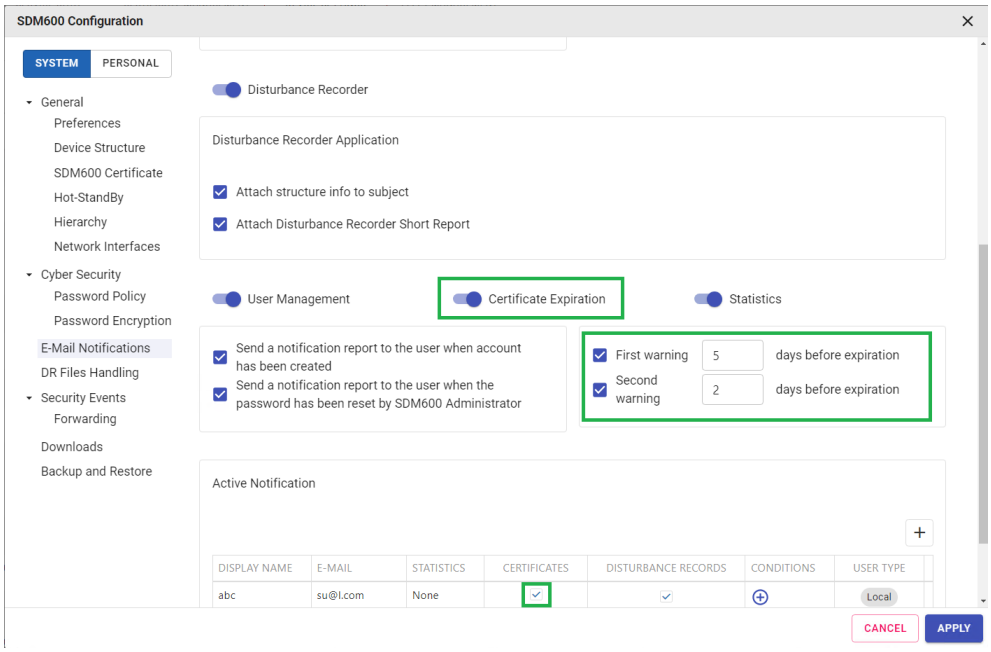


Figure 83: Certificate Expiration Notification

5.15.4 SDM600 Statistics Notification

After enabling the Statistics Notification, e-mails will be sent to the configured users with daily/weekly/monthly statistics about SDM600.

Statistics consist of number of Disturbance Records, Security Events, Configuration Changes and User Account changes registered in SDM600.

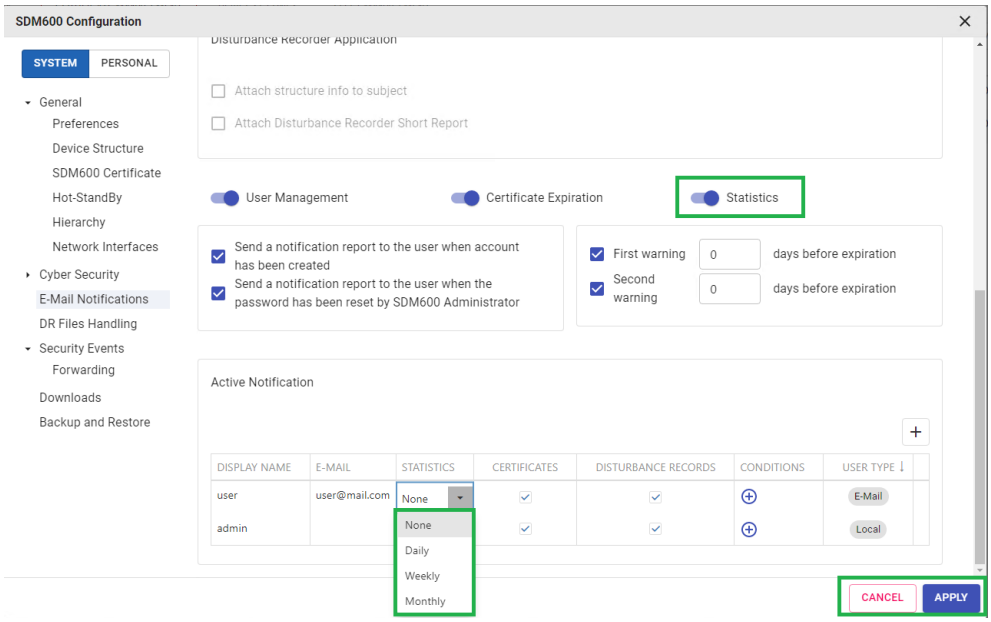


Figure 84: Statistics Notification

5.16 System Configuration

General SDM600 settings can be changed in the **System** section of the System Configuration.

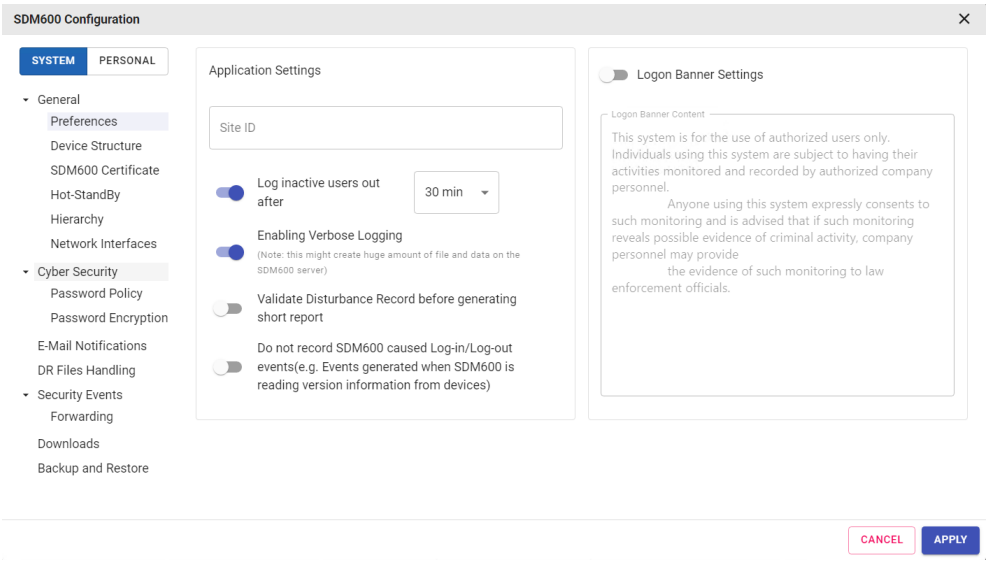


Figure 85: System Configuration

SDM600 provides additional software that can be downloaded from the SDM600 Server to a Client Computer. All software downloads are accessible from the **Downloads** section of the System Configuration.

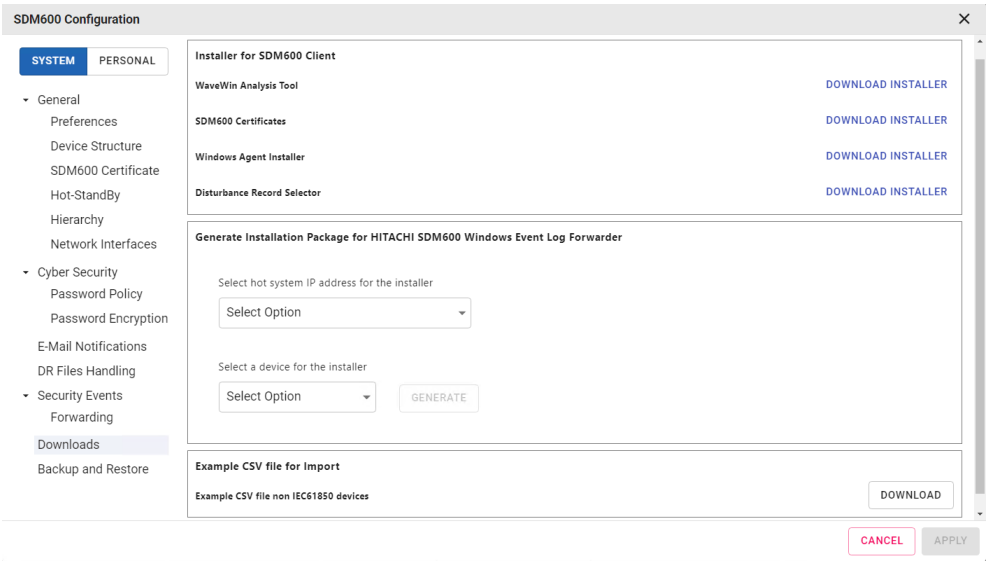


Figure 86: Downloads

The following items are available from the downloads:

1. Wavewin Analysis Tool-DR Analysis Tool.
2. SDM600 Certificates: User can download the SDM600 Certificates and run the SDM600 application in their browser with Secure Connection. Refer to **Access SDM600/Security Settings** (see Section 4) for more details.
3. Windows Agent Installer: Refer to **Service Data Management/Windows Computer** (see Section 5.12.2.4) for more details.
4. Disturbance Record Selector: Refer to Section 5.8.1 for more details
5. Windows Event Forwarder: Refer to **Cybersecurity Event Logging/Windows Computer** (see Section 5.9.2.3) for more details.
6. An example of a CSV file for importing non IEC 61850 devices.

To download the SDM600 Windows Event Forwarder the user needs to specify on which target device the application will be installed. Furthermore, the user needs to choose the IP address used for the communication: in case of Hot/Standby, it is required to configure the IP addresses for both the hot and the standby system. Make sure that the selected IP address is reachable from the target device. To receive communication, if there is no required IP address, go to **Configuration/Centralized Account Mgmt./Refresh network interface list**. When all the necessary information is selected, SDM600 generates the installer package. The user can then extract the installer package into a directory and run the installer.

5.17 Supervision

SDM600 supervises:

- the connection to the managed devices
- the status of all the SDM600 Windows services.

The Status icon in the header gives an overview of the status of the SDM600 Windows Services.

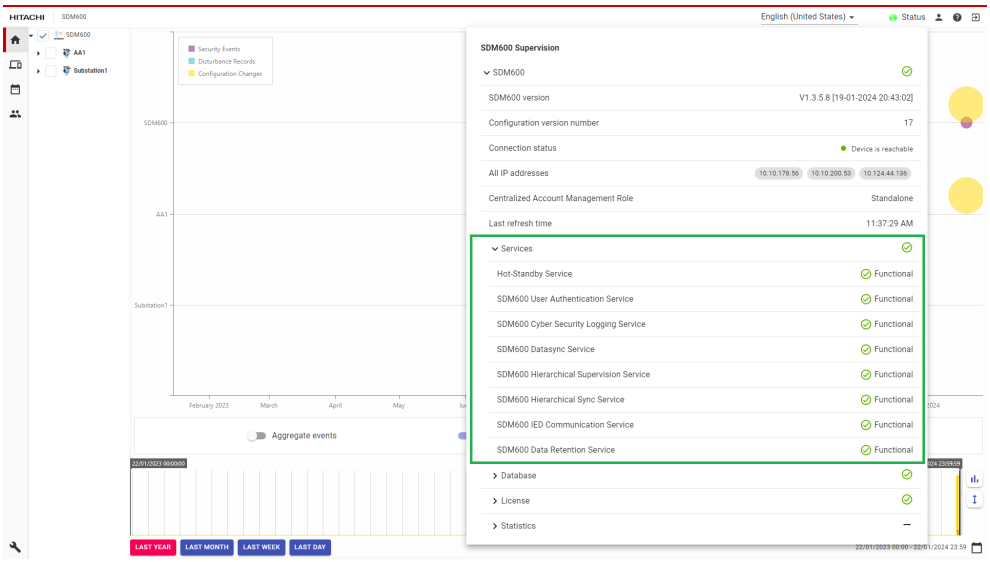


Figure 87: SDM600 Windows Services Status

The **Device Supervision** tab in the Devices area monitors the status of the managed devices.

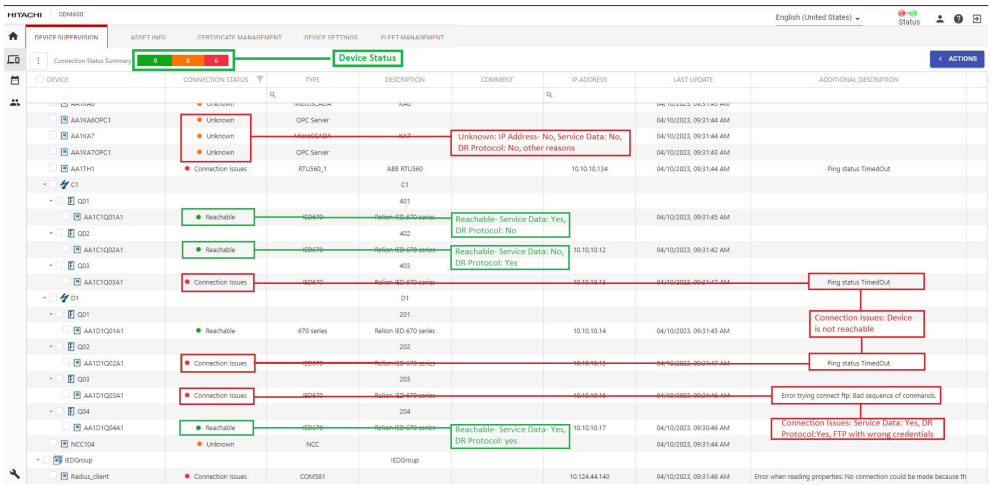


Figure 88: Device Supervision

The main objective of the **Device Supervision** tab is to help the user identify connectivity issue and troubleshoot configuration mistakes; a three-color visual indicator is located at the top of the page to offer a summary of the connection status of all managed devices.

To maximise engineering efficiency, the suggested workflow is the following:

1. Import the managed devices into SDM600.
2. In the **Device Settings** tab, configure as required the communication settings (IP address, DR protocol, Service Data protocol).
3. Navigate to **Device Supervision** and inspect the **Connection Status** to ensure that SDM600 is able to successfully connect to the devices as specified previously (point 2).
4. If SDM600 is facing any issue while connecting to a device, the **Connection Status** will be set to **Connection Issues**. Inspect the **Additional Description** for supplementary information.

To focus on troubleshooting, click on the funnel icon in the Connection Status and select **Connection Issues**. Inspect the Additional Description to collect hints on why SDM600 could not successfully connect to a given device.

SDM600 provides three possible values for the Connection Status:

- Reachable (green dot): A device is marked as Reachable when SDM600 can successfully connect to the target device based on every protocol configured by the user. Example: SDM600 successfully manages to ping the device, to connect over SFTP to collect DR files and to connect over SNMPv3 to collect Service Data.
- Connection Issues (red dot): A device is marked as Connection Issues when SDM600 fails to connect to the target device for at least one of the selected protocols. Any hint is visualised in the Additional Description. Example: SDM600 successfully manages to ping the device and to connect over SNMPv3 to collect Service Data, but no connection can be established over SFTP due to wrong credentials.
- Unknown (orange dot): A device is marked as Unknown when SDM600 does not have enough information to attempt any connection. Example: IP is not configured and DR protocol is not configured.

5.18 Cybersecurity: secure communication towards devices

This section will review important cybersecurity information and settings, to guide the user in configuring SDM600 to provide a secure communication with the devices.

5.18.1 Minimum TLS version for 62351-8 (LDAP)

The TLS version is selected through a negotiation process called the TLS handshake, where the client and server exchange supported versions and agree on the highest mutually supported version. The negotiation involves the client sending its preferred version in the ClientHello message and the server responding with the highest version it supports that is not greater than the client's preference.

If the handshake fails, it means that the client and server were unable to agree on a mutually supported TLS version. This can occur if the client's preferred version is not supported by the server or if there are compatibility issues between the versions. In such cases, the connection cannot be established, and the client and server may need to fallback to a lower TLS version or terminate the connection.

In SDM600 it is possible to configure the minimum TLS version to be used in scope of 62351-8 (LDAP) communication. During the TLS handshake, SDM600 will not fallback to a version older than the specified one. SDM600 can be configured to use TLS 1.0, TLS 1.1 and TLS 1.2. Example, when SDM600 is configured to use TLS 1.1 as minimum TLS version during the handshake, it will only accept commections over TLS 1.2 and TLS 1.1: connections required TLS 1.0 will be terminated.

TLS 1.0 and TLS 1.1 are no longer considered secure due to several vulnerabilities and weaknesses that have been discovered in these versions. Generally, it is recommended to disable both TLS 1.0 and TLS 1.1, and upgraded to more secure versions, such as TLS 1.2. It is important to keep the TLS implementation up-to-date to ensure the security and integrity of data transmitted over the network.

When installing SDM600 for the first time on a new system, the minumum TLS version is 1.2 by default.
When updating an existing SDM600 installation, to ensure backward compatibility, the already configured minimum TLS version is kept.

To review or change the minimum TLS version to be used for 62351-8 (LDAP) communication, follow these steps:

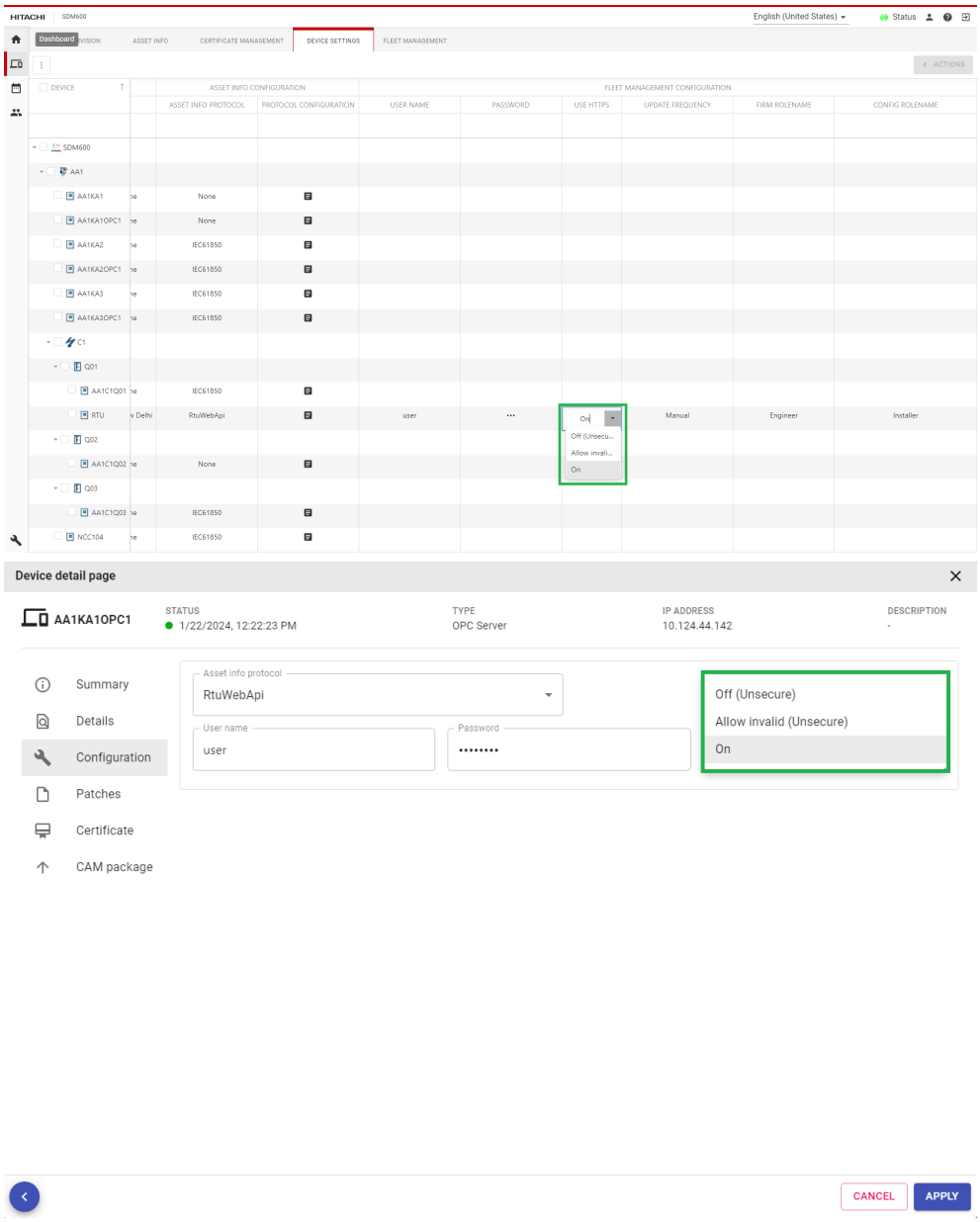
1. Stop the HE Authentication Service
2. Navigate to the SDM600 installation folder
3. Nagivate to the OpenLDAP folder
4. Open the slapd.conf file
5. Locate the entry: **TLSProtocolMin**
6. Review the value:
   6.1. **3.1** stands for TLS 1.0
   6.2. **3.2** stands for TLS 1.1
   6.3. **3.3** stands for TLS 1.2
7. If needed, enter a new value. The only possible values are: **3.1**, **3.2**, **3.3**. Not other values are allowed to be entered.
8. Save the file.
9. Restart the HE Authentication Service

TLS 1.0 and TLS 1.1 are no longer considered secure.
It is not recommended to configure SDM600 to use TLS 1.0 and TLS 1.1.

5.18.2 Hitachi Energy RTU500 - HTTPs

For Hitachi Energy RTU500 devices, SDM600 can be configured to use RtuWebApi as communication protocol for collecting DR files and Service Data. The RTU fleet management functionality always uses the RtuWebApi; the user cannot select a different protocol.

In general, when SDM600 communicates with a Hitachi Energy RTU500 device, it is possible to configure HTTPS using the Use HTTPs setting. This setting allows the user to define if secure HTTP is used and how strictly the certificate validation is performed.



Use HTTPs Option in Device settings and View Detail Page

Three possible values can be configured.

- Off (Unsecure): HTTPs is completely disabled, and HTTP is used instead. This setting is not recommended.
- Allow invalid (Unsecure): HTTPs is enabled, but the certificate presented by the RTU device is not validated, and any untrusted certificate will be accepted by SDM600. This setting is not recommended.
- On: HTTPs is enabled, and the certificate presented by the RTU device will be strictly validated by SDM600. User must import the CA (or intermediate CA) certificate used to sign the RTU certificate on the SDM600 Windows Machine. If no CA is used, then each RTU certificate has to be added as trusted.

When Use HTTPs is configured as On, SDM600 will strictly validate the certificate provided by RTU, and the communication will be rejected if the provided certificate is not trusted by SDM600.

The following list highlights the possible scenarios, and the actions required from the user to ensure that the communication between SDM600 and the target RTU device can be established successfully.

- **The RTU certificate was created via SDM:** the secure communication between SDM600 and the target RTU device will be established without any further action from the user. The RTU certificate has been generated by SDM600, and the SDM root CA is already trusted.
- **The RTU certificate was created by an external CA:** the CA must be manually added to the Trusted Root Certification Authorities store. Follow the next steps to perform this operation:
  1. Open Run box, type *mmc,* and hit Enter to open the Microsoft Management Control (MMC).
  2. Press the **File** menu link and select **Add/Remove Snap-in**.
  3. Under **Available snap-ins***:*, select **Certificates**, and then click **Add >**.
  4. Click **OK**. In the next dialog box, select **Computer account** and then on **Next**.
  5. Select **Local compute**r and click on **Finish**.
  6. Now, back in MMC, in the console tree, double-click on **Certificates** and then right-click on **Trusted Root Certification Authorities Store**. Under **All tasks**, select **Import**.
  7. The Certificate Import Wizard will open.
  8. Follow the instructions in the wizard to complete the process.
  9. Once the procedure is completed successfully, the manually imported CA entry is available under the **Certificates - Local Computer/Trusted Root Certification Authorities** of the computer cert store.

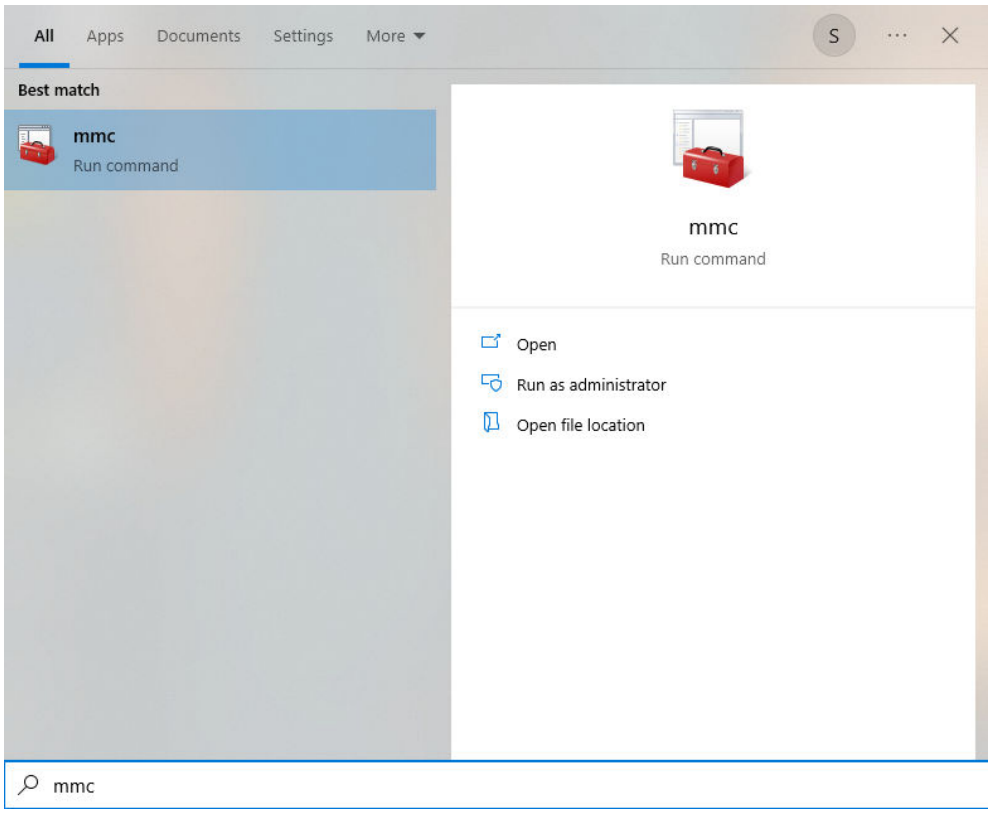


Figure 89: Microsoft Management Control

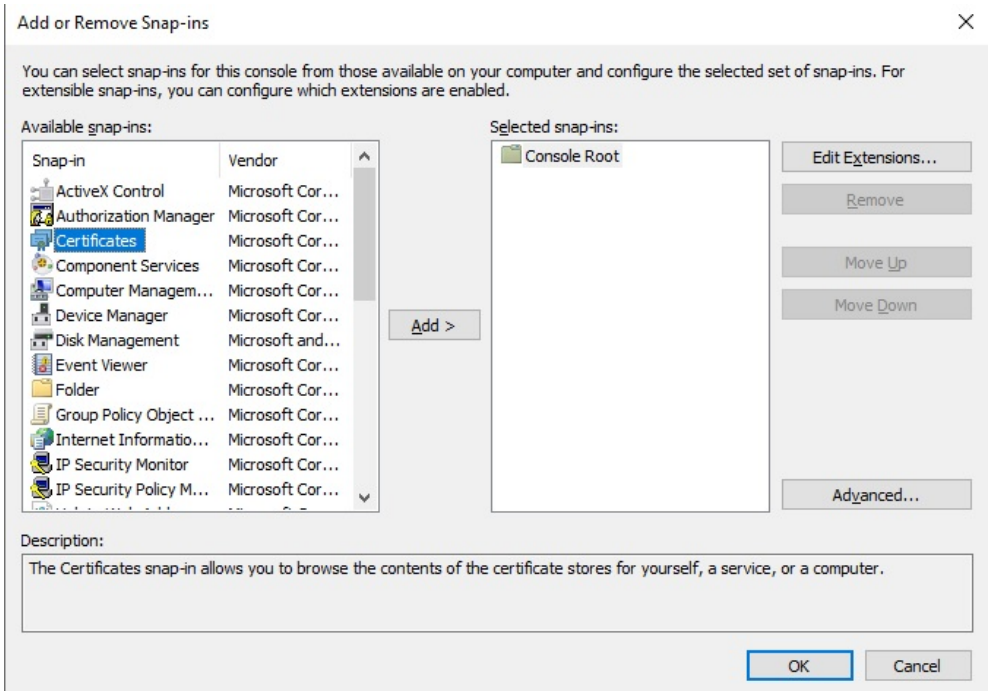


Figure 90: Add or Remove Snap-ins

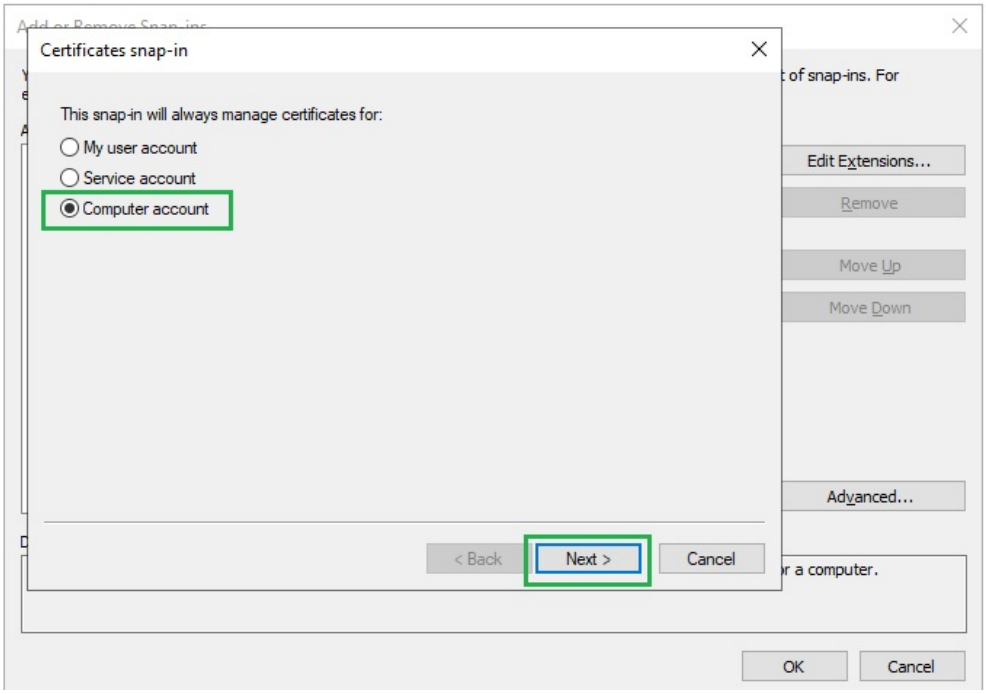


Figure 91: Select-> Computer Account

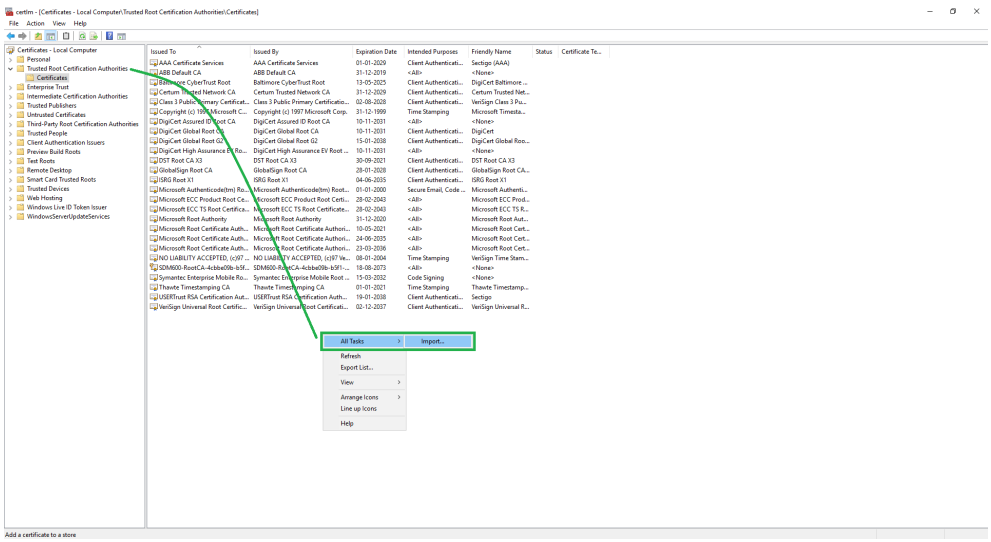
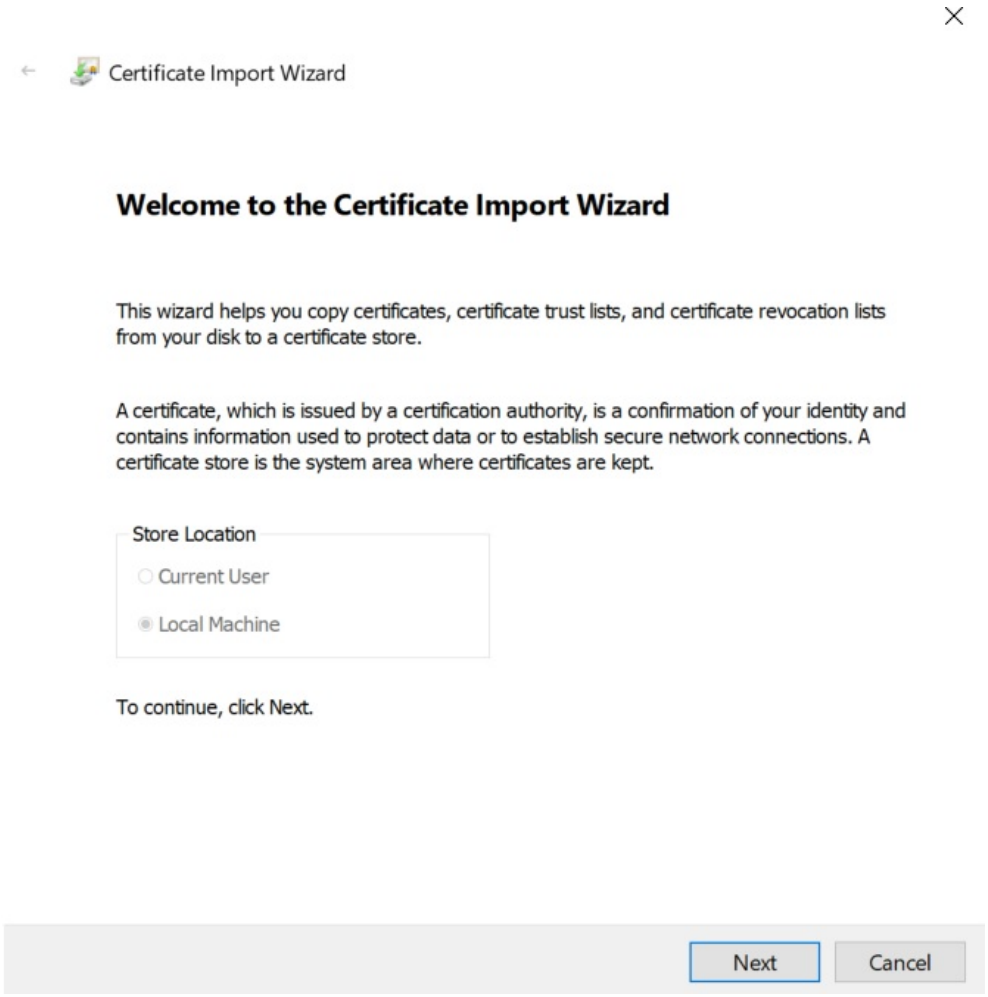
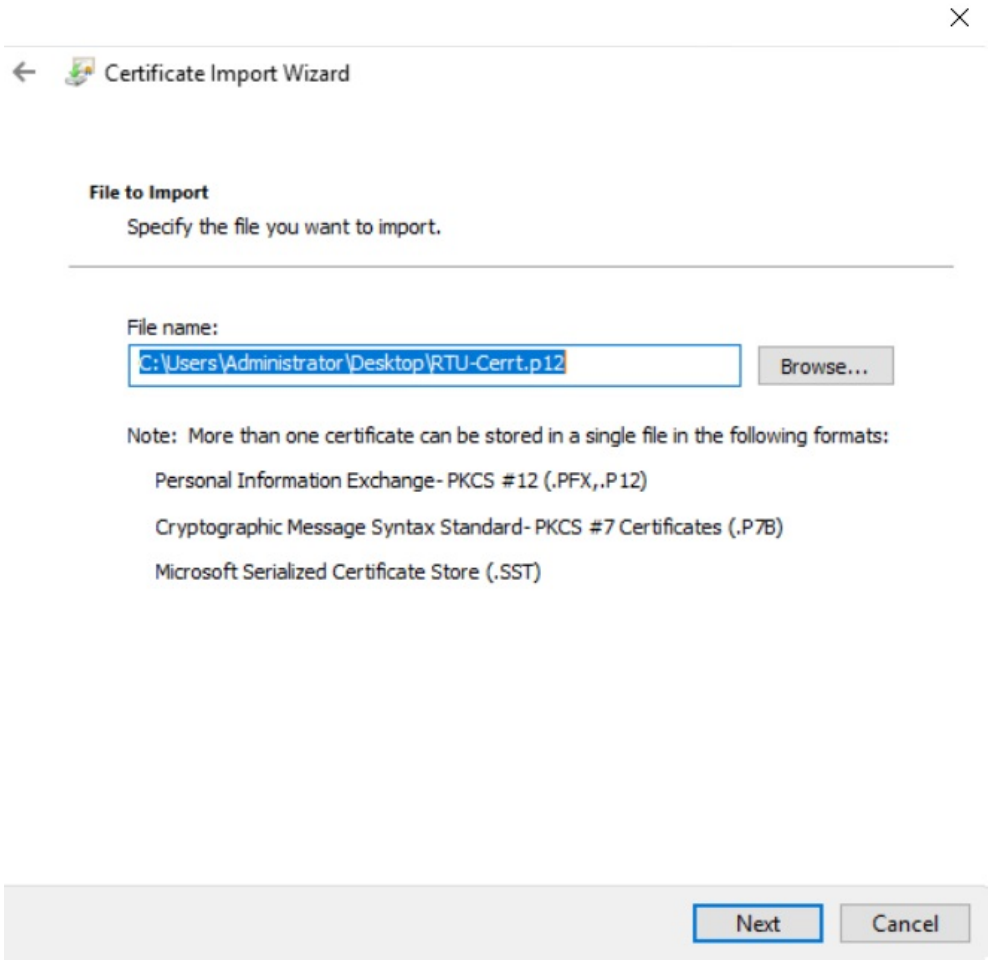
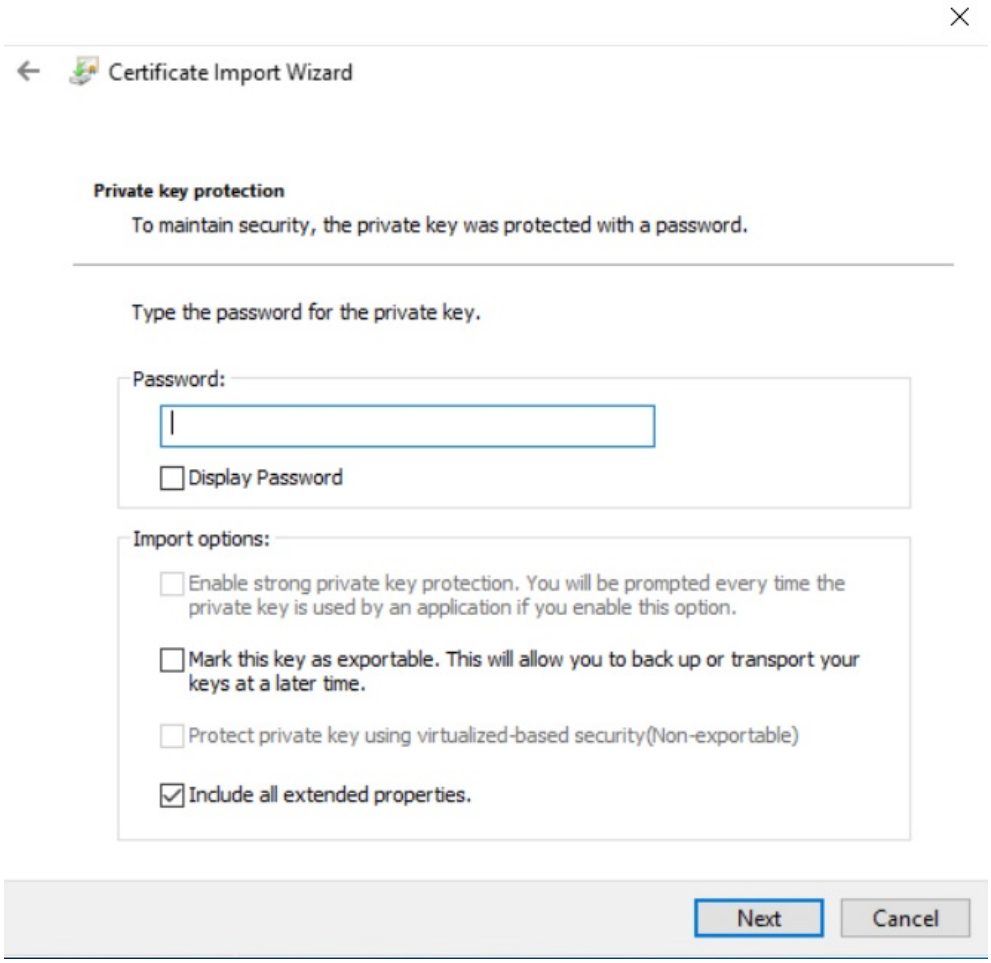
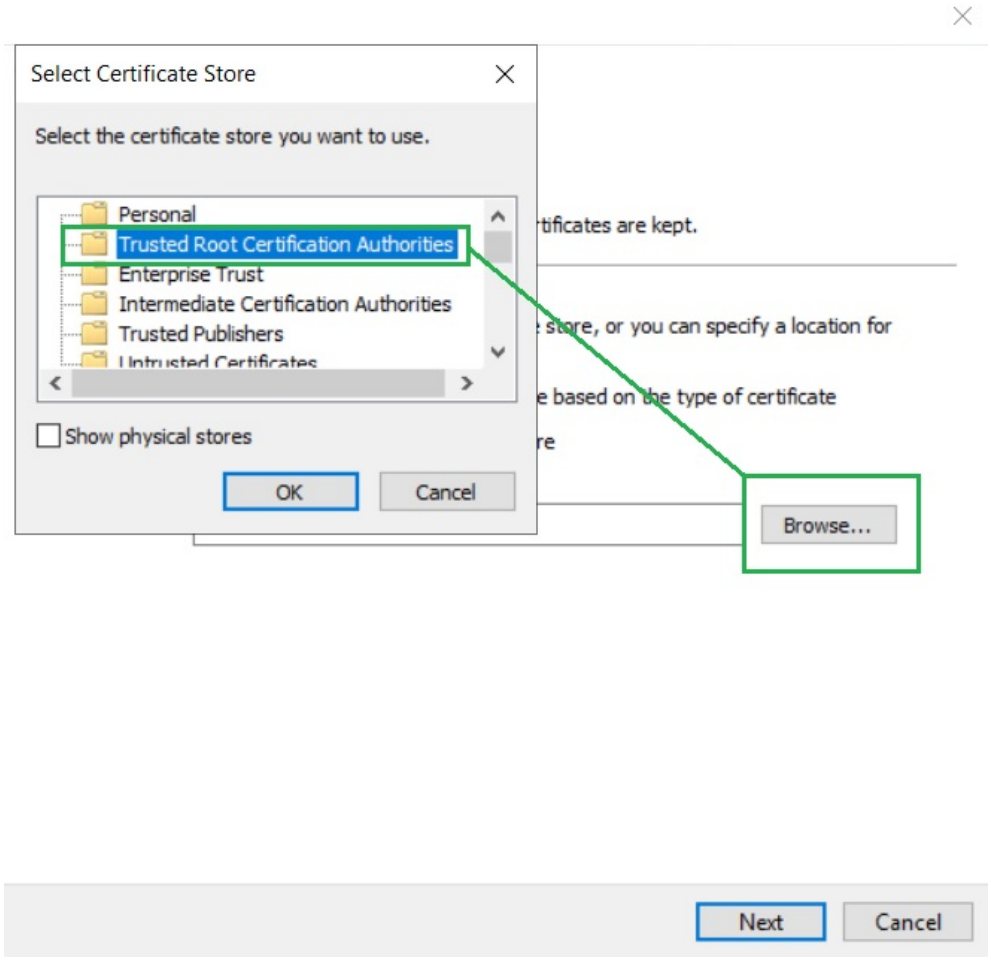


Figure 92: Import Certificate









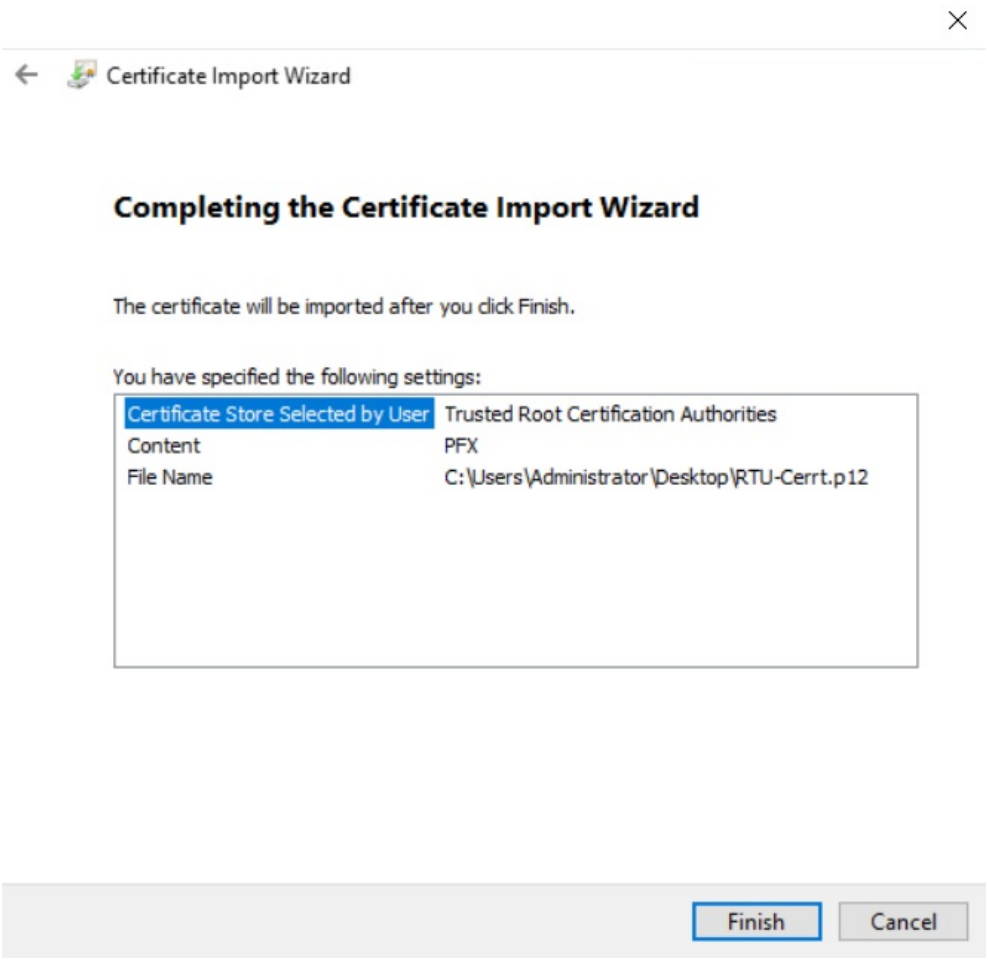


Figure 93: Certificate Import Wizard

- **The RTU certificate is self-signed:** the RTU certificate must be imported manually. This operation must be performed for each and every self-signed RTU certificate.

In SDM600 1.3.1 and older, Use HTTPs could be configured as *Enabled* or *Disabled*. When updating to SDM600 1.3.2 or newer, to ensure that existing connections towards RTU500 devices are still working, the Use HTTPs values will be migrated as follow:

- *Disable* will be migrated to *Off (Unsecure)*
- *Enabled* will be migrated to *Allow invalid (Unsecure)*

This migration strategy will ensure that SDM600 will still communicate with the existing RTU devices, without additional user action.
User must manually update existing installation to enforce stricter secure settings.

For newly created RTU500 devices, Use HTTPs is by default configured to *On*.

As usual, the *Device Supervision* tab is the starting point to troubleshoot any connection issue affecting the devices: detailed information could be collected by hovering on the Additional Description column.

If further details are required use a web-browser (chrome/...) to access the RTU Web Interface directly from the machine where SDM is installed.

Section 6 User Preferences

Each user can define certain preferences when accessing SDM600.

Preferences can be defined in the **Personal** tab in the SDM600 Configuration.

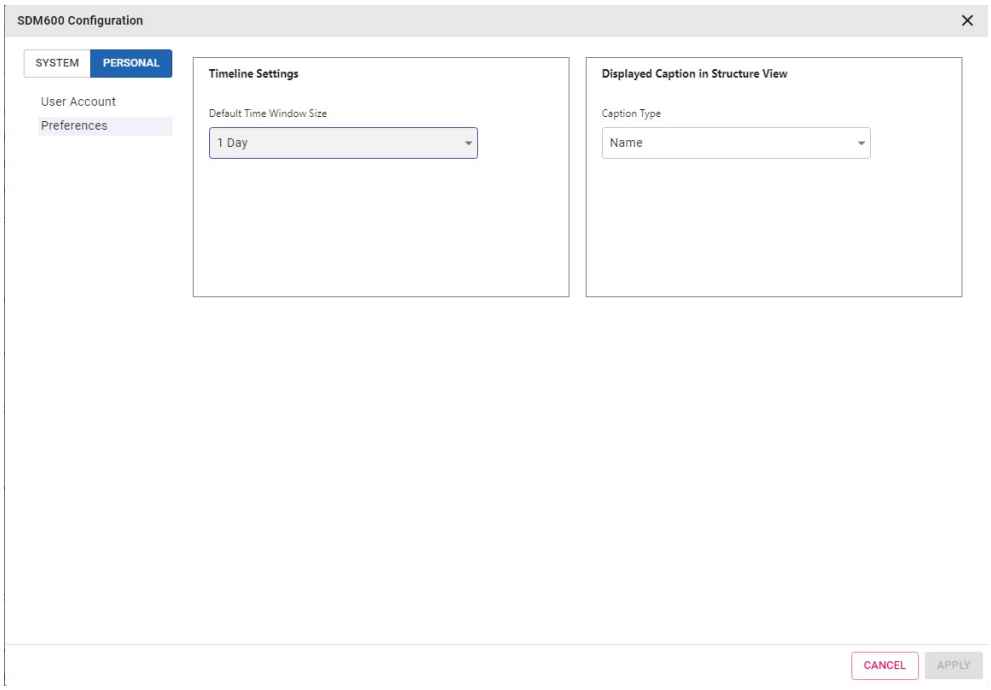


Figure 94: Preference under Personal Tab

Language selection for the user interface

It is possible to change the language used to display the user interface. Users can select the preferred language among the supported language packs. The language selection is always available in the top-right corner of the user interface. The language will be changed immediately, without requiring the user to re-login.

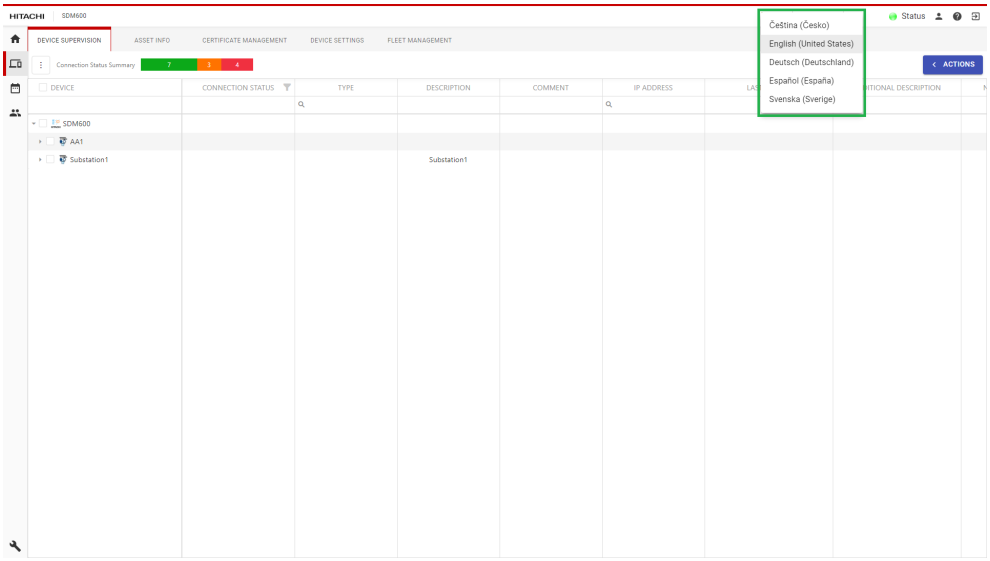


Figure 95: Change the Language of the UI

During the user creation, the administrator configures the default language for the created user. By default, the selected language will be used to display the user interface for the user, each time he/she logs into SDM600. This functionality can be used to configure the envisioned language for the newly created user. As mentioned above, at any time, the user can change the language by selecting a new one on the top-right corner of the application.

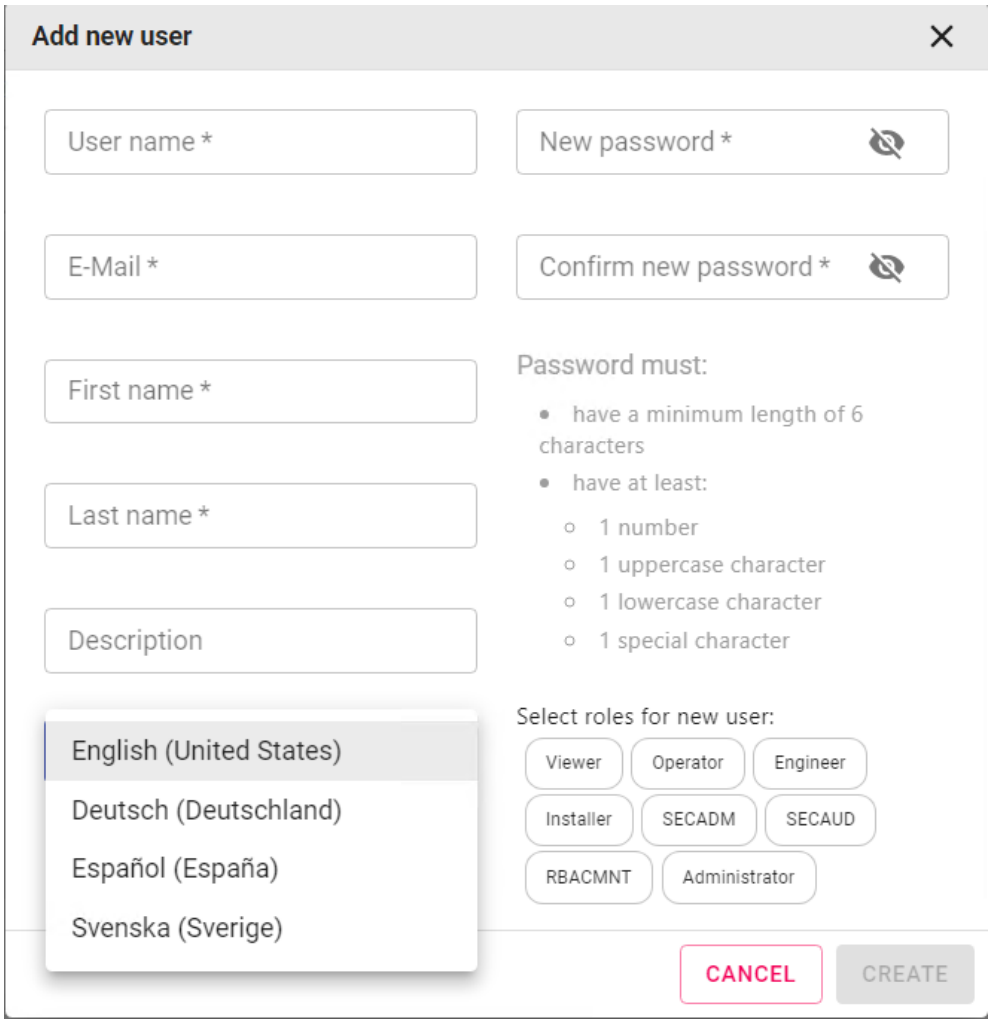


Figure 96: Default Language selection during user creation.

Whenever a user logs into SDM600, the user interface is displayed in the default language for that user, which the administrator selected upon creation. User can select a different language in the top-right corner, but, on the next login, the user interface will be displayed again the default language. The user can change the default language in the *Personal Settings* tab, under the *User Account* menu.

When Active Directory is enabled, the User Account menu (in the Personal Settings tab) is disabled, because all the user related info are managed by Active Directory. When Active Directory is enabled, it is not possible to configure a Default Language for a user. Still, users can change the language of the user interface by using the language menu in the top-right corner.

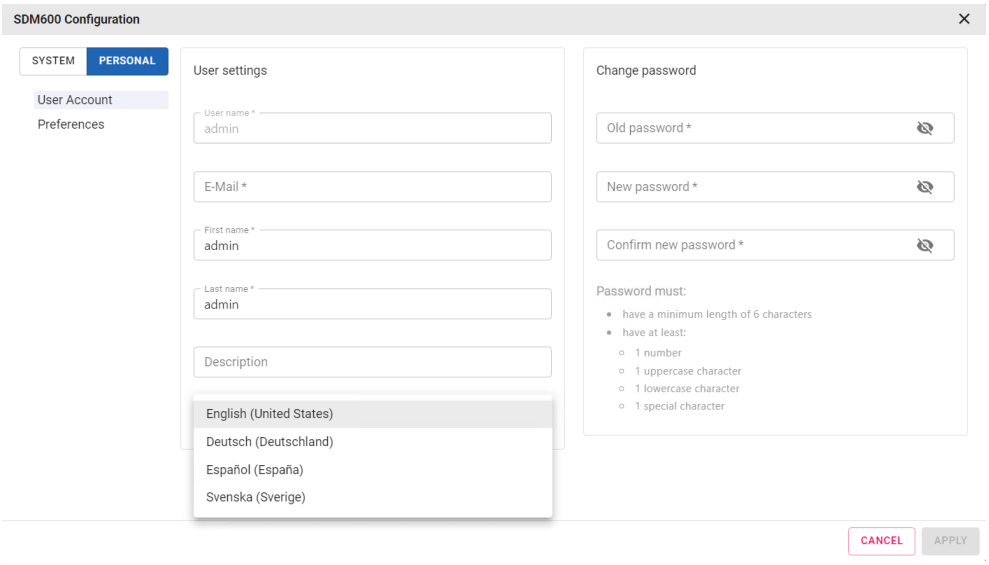


Figure 97: Changing Default Language in the personal settings

Section 7 SDM600 Application Administration Tool

The SDM600 Application Administration Tool provides a set of functionalities to manage and configure the SDM600 server application, including its database and the way it communicates.

Please note that the SDM600 Application Administration Tool is only available on the PC where SDM600 is installed, thus it's not accessible via a web browser from remote.

The SDM600 Application Administration Tool can be launched in two ways:

- Launch it from the Start Menu by navigating to the SDM600 Application Administration Tool.

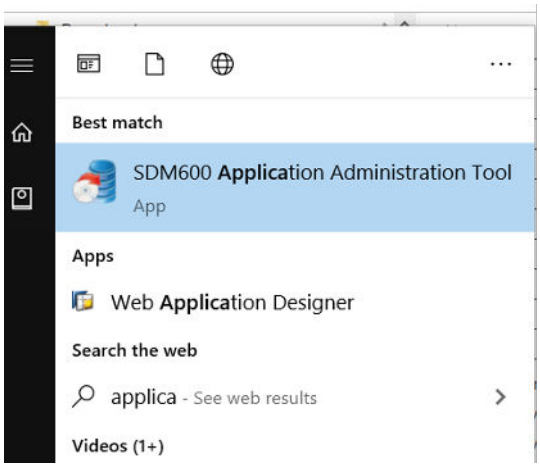


Figure 98: SDM600 Application Administration Tool - Access from Windows Start Menu

- Launch it from the File System by navigating to the SDM600 installation folder (by default, it is under C:\Program Files (x86)\ABB\SDM600). Open the ApplicationAdministrationTool folder and execute SDM600ApplicationAdministrationTool.exe.

7.1 Backup

The SDM600 Application Administration Tool provides a function to back up the database, including both the configuration and live data. To protect confidential information within the backup file, every backup must be password protected.

When creating a new backup, the user must enter password. It is suggested to use a strong password.

Be aware that in order to restore a password protected backup, the matching password must be entered – a lost password cannot be recovered, making it impossible to restore the backup.

To create a backup in AAT, select the **Backup** tab.

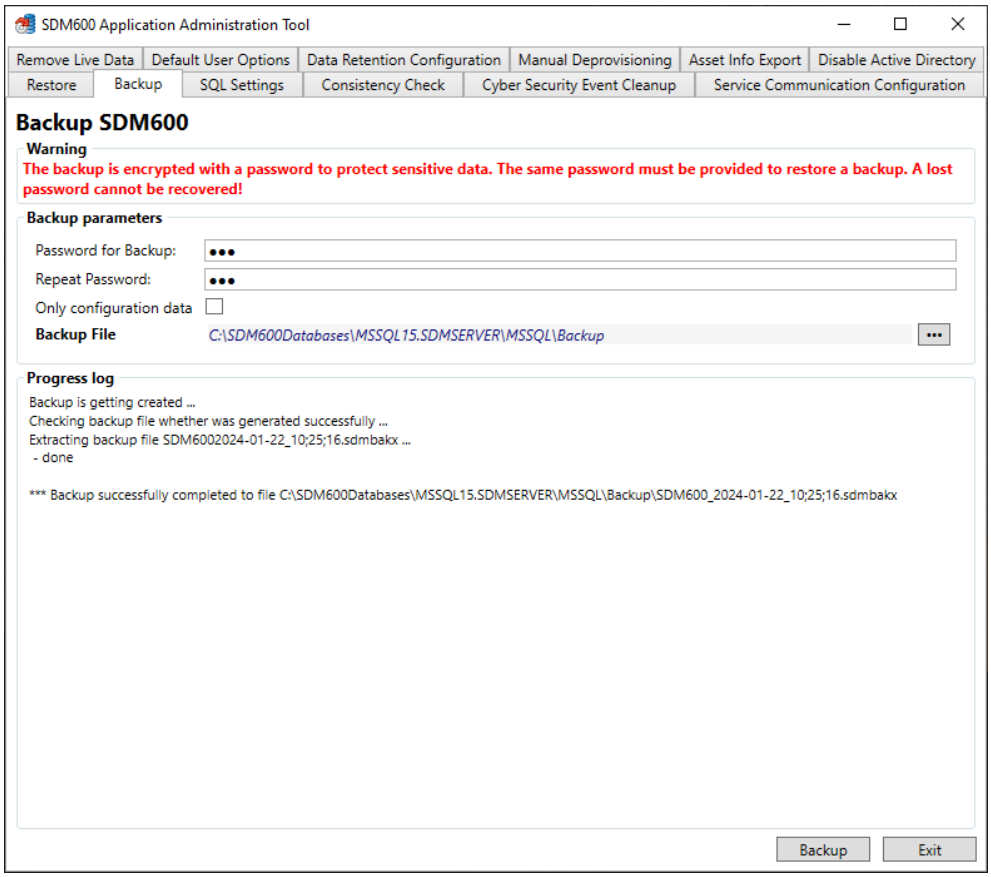


Figure 99: AAT Backup functionality

The backup created on a system running on SQL2019 cannot be restored on a system running on SQL2012.

There is an option to backup configuration data only. If the option is selected, then disturbance records data, configuration changes, and security events data are not backed up.

7.2 Restore

SDM600 Application Administration Tool must be used to restore the configuration and all the data from a backup file. Restore operation will overwrite any existing data and any changes made since the last backup.

The backup created on a system running on SQL2019 cannot be restored on a system running on SQL2012.

In order to restore a password protected backup file, the correct password must be provided.

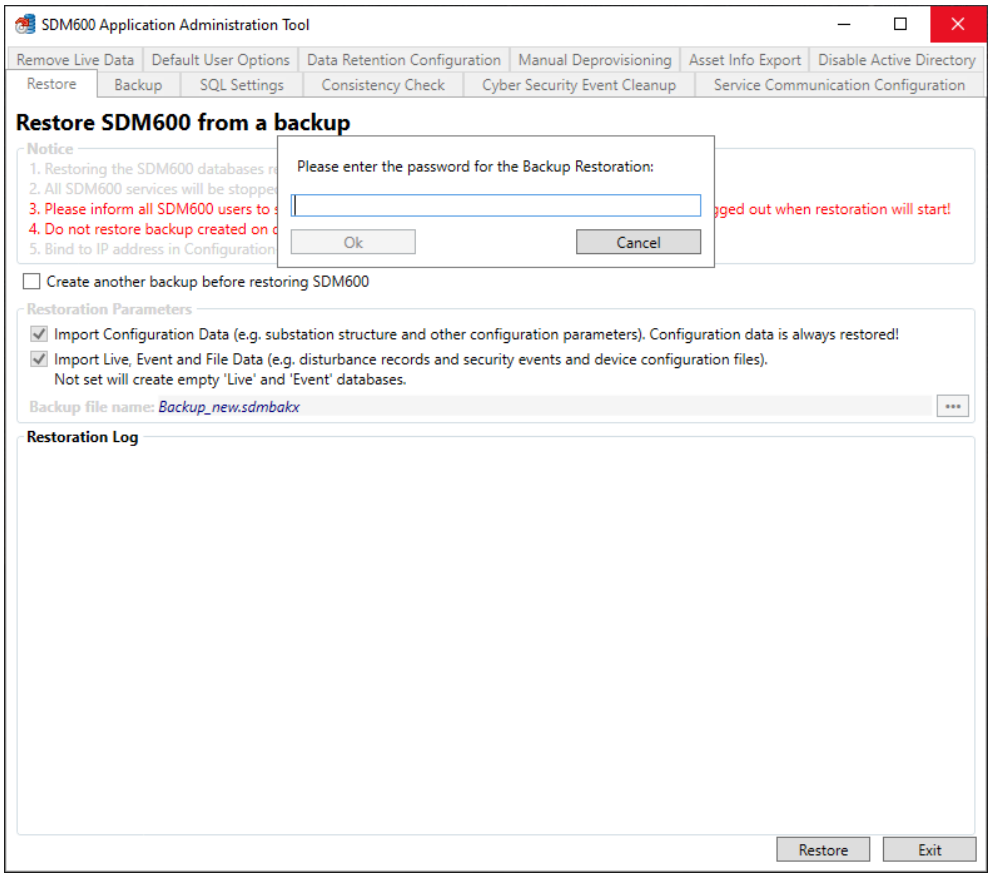


Figure 100: Restore SDM600 Backup

When restoring a previously created back up, additional options are provided:

- To create a backup of the current database before restoring a backup database:
  If this option is selected, user is requested to provide the password for the backup.
- To import SDM600 live data (configuration will always be imported):
  User can decide whether live data should be imported as well. When this option is not selected, only SDM600 configuration will be restored and disturbance records data, configuration changes and security events data are not imported.

After defining the options, select the backup file that should be restored.

The SDM600 restore functionality requires that all the services are stopped before the restoration can be done. After the restoration is completed, all the services are automatically started. Therefore, it is important to make sure that during the restoration period, no user is connected to SDM600.

Restoring a backup in an SDM600 parent-child setup must be done with extra care, particularly on SDM600 Centralized Account Management feature. SDM600 Centralized Account Management requires the centralized account management database at the parent to always be in the most updated state than the one in the SDM600 children. In the case where a backup file that contains older centralized account management database needs to be restored at the SDM600 parent, there is a chance that centralized account management at SDM600 children will not receive any update from SDM600 parent. This is because the centralized account management at the SDM600 child has a newer data than the one in the centralized account management at the SDM600 parent. To overcome this situation, it is important to first stop the Authentication Service. Next, delete the content of the SDM600 centralized account management Data folder from SDM600 children. By default, the Data folder can be found under C:\Program Files (x86)\ABB\SDM600\OpenLDAP\data. Next, restart the Authentication Service, or simply conduct a full restart of the computer where SDM600 children is installed.

The SDM600 restore functionality requires that all the services are stopped before the restoration can be done. If the services cannot be stopped, the restoration process will be canceled. If this happens, try again or restart the PC where SDM600 is installed.

After restoring a backup, the SDM600 restore functionality restarts the services. If any of the services does not start properly, try to restart the computer. To check whether all services have been started, go to **Task Manager**, open the **Services** tab, and click **Services**. In a fully operational condition, all SDM600 services should be in the Started state. If a service is not up and running, the cause for this can be checked by navigating to **Windows Event Viewer > Windows Log > Application**. If this happens, please contact your SDM600 Support line.

7.3 Database Consistency Check

The SDM600 Application Administration Tool provides the possibility to check databases consistency and fix the most common issues. Click on *Check* button to execute the Consistency Check and wait for the result to be shown in the *Output Window*.

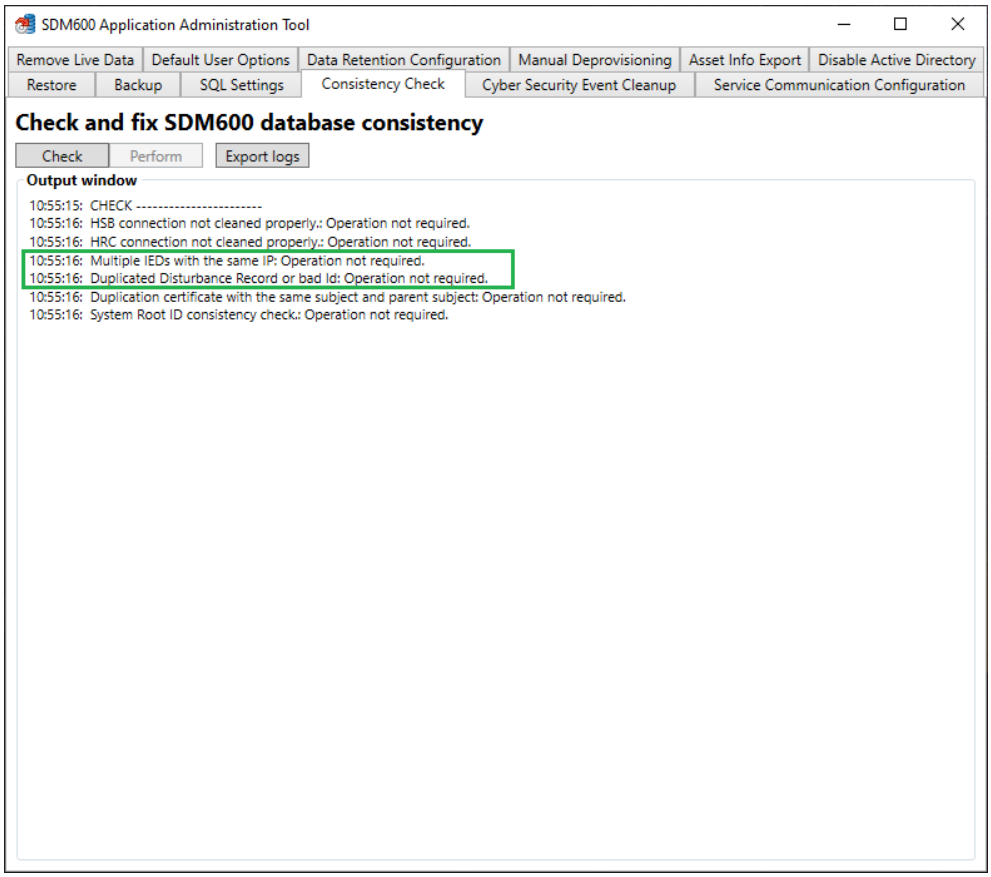


Figure 101: Check Database Consistency

AAT will delete duplicated IP addresses from all devices and also will delete if any duplicated DR records are available in the SDM600 Database. It is recommended to save logs, using the *Export logs* button, in order to manually assign correct IP addresses.

7.4 Cybersecurity Event Cleanup

The SDM600 Application Administration Tool provides the possibility to clean up Cybersecurity Events generated by SDM600 itself.

Click **Cleanup ignored events** to perform the cleanup operation. The outcome is visible in the **Output window**.

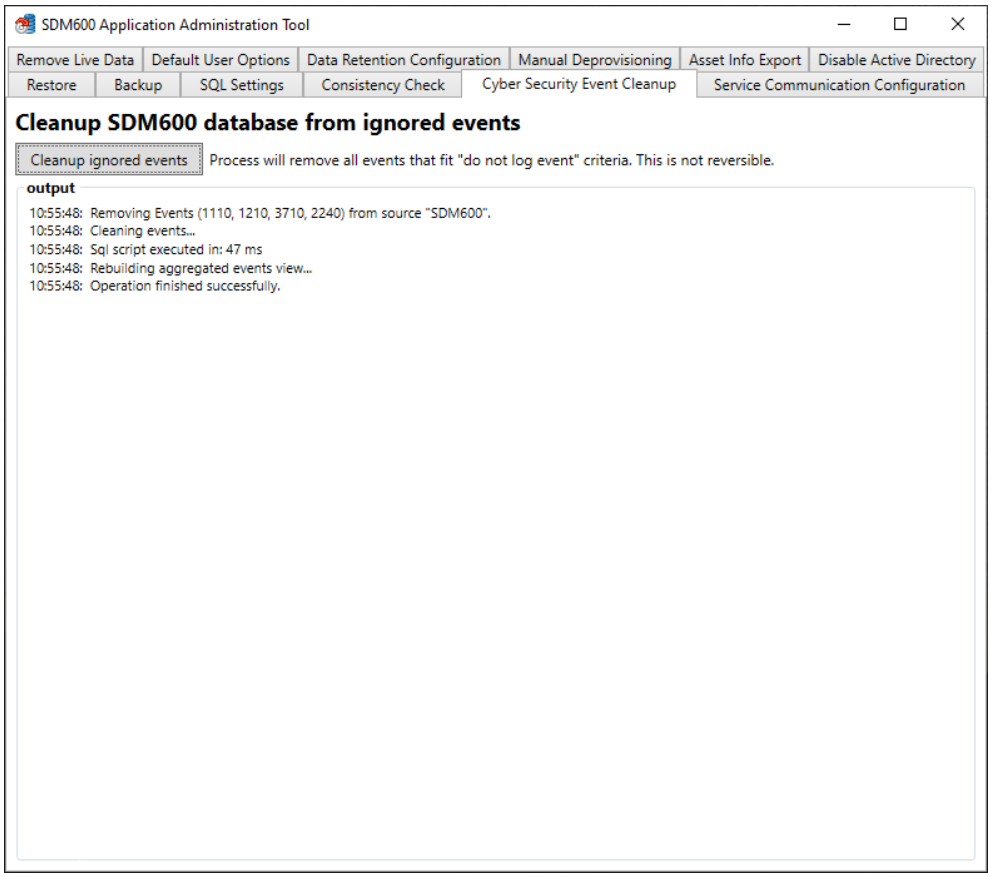


Figure 102: Cleanup Cybersecurity Events

7.5 Service Communication Authentication

The SDM600 Service Communication Configuration allows to configure the way SDM600 authenticates the communication with another SDM600, for example, in Hot-Standby mode.

Default setting is Certificate authentication method. If SDM600 is running in domain joined environment, then it is suggested to use dedicated user to authenticate external communication between systems to avoid “Audit failure” events in Windows Event Log.

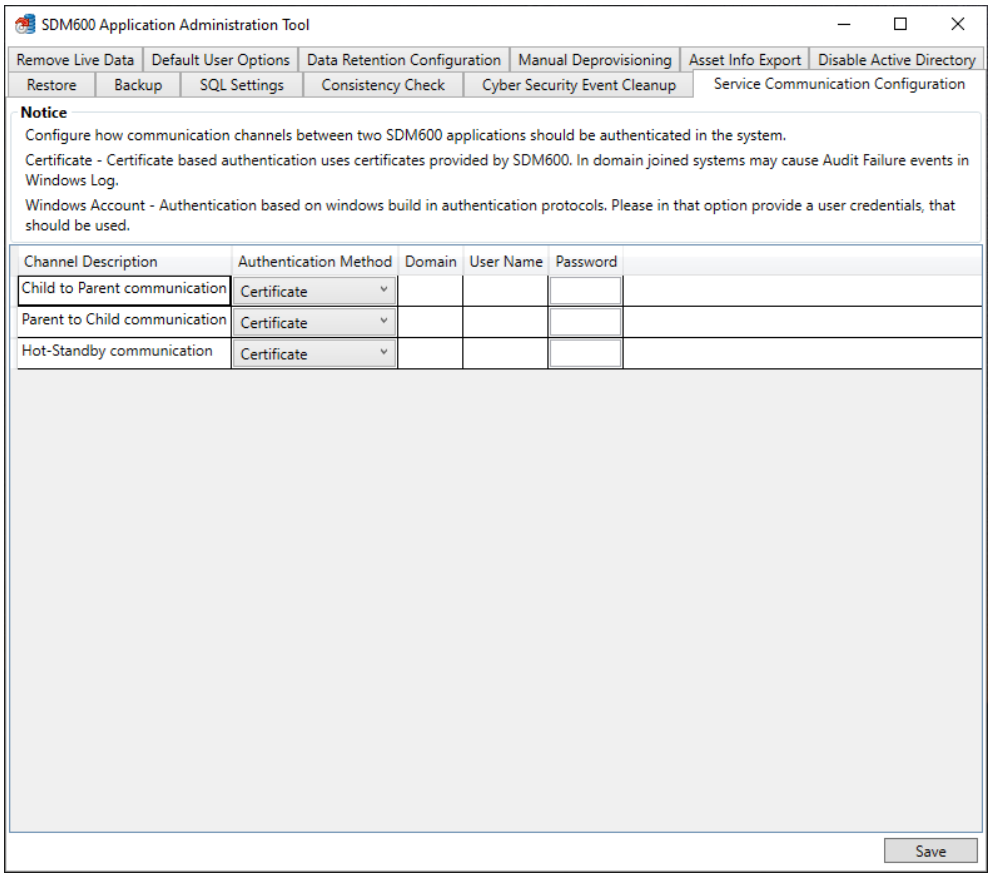


Figure 103: SDM600 Service Authentication

7.6 Remove Live Data

The SDM600 Application Administration Tool provides the possibility to clean up data collected in the database, without uninstalling the whole application.

It’s possible to select which live data will be removed by means of the checkbox: Disturbance Records, Cybersecurity Events, Service and Maintenance data (for example, IED status change, Windows Application Information and Patches).

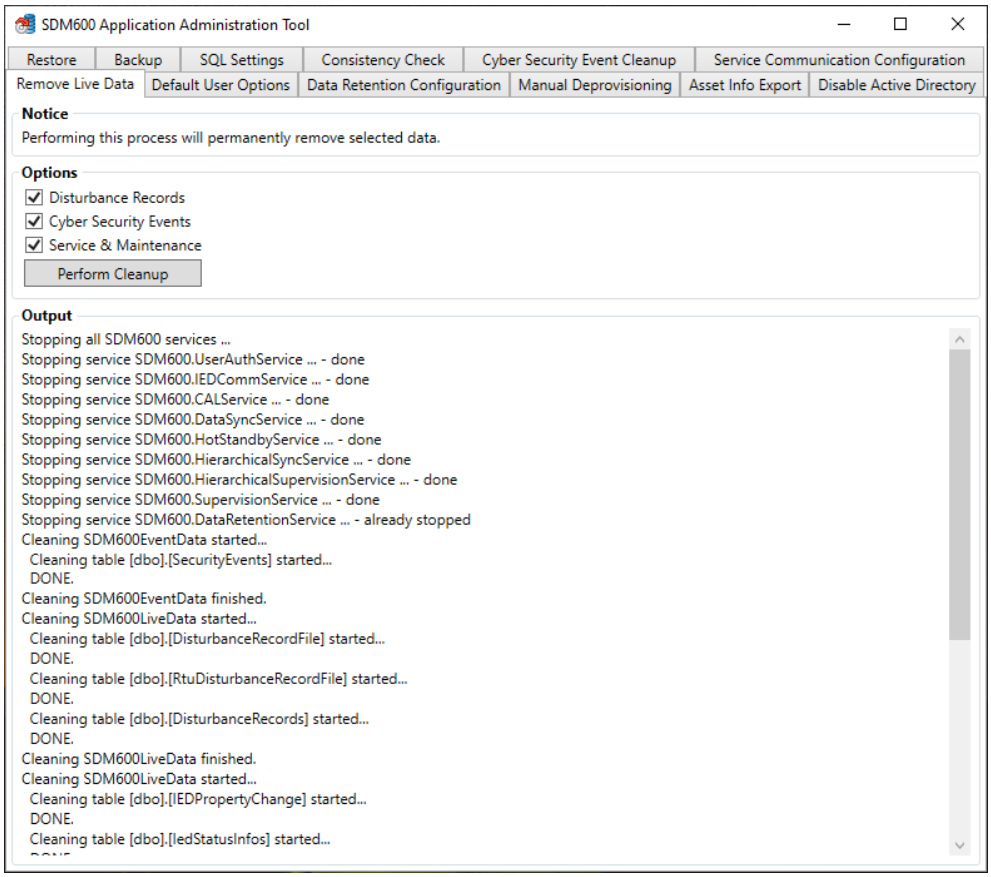


Figure 104: Removing Live Data from SDM600

This operation cannot be undone. Depending on the database size, it could take several minutes. The user will be asked for confirmation before starting the operation.

- It is recommended to take a backup before removing live data.

In case live data that is older than a specified date should be removed, use the Data Retention functionality.

7.7 Default User Options

The SDM600 Application Administration Tool provides the possibility to configure the default options applied to newly created users.

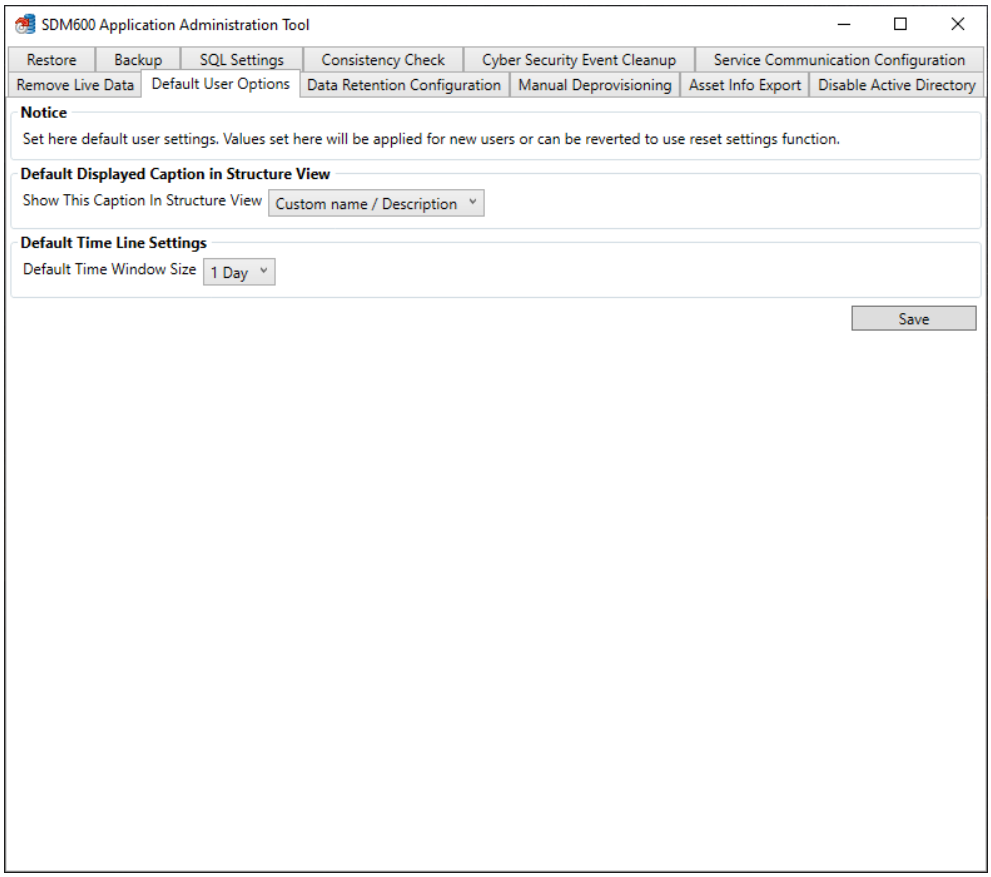


Figure 105: Default user options when creating users.

- *Timeline Settings* is used to define the width of the dashboard time navigator. Available time ranges span from a minimum of 1Dday to a maximum of 1 Year.
- *Displayed Caption in Structure View* allows to choose which text will be displayed for the items in the structure view. A user can choose between two options: the name or the description.

7.8 Data Retention Configuration

The Data Retention Service manages how long data will be stored in the SQL D\database. Data older than the specified number of days is permanently removed from the database, allowing the database size to be within certain limits.

For both DRs and Security Events, it is possible to enable the data retention policy and to configure the number of days. Data older than *the configured number of days* will be deleted.

Moreover, for Security Event, it is possible to enable backup functionality. Before deleting an older event, a .csv file backup will be generated in the configured backup location.

To backup DR files, configure the DR Export functionality.

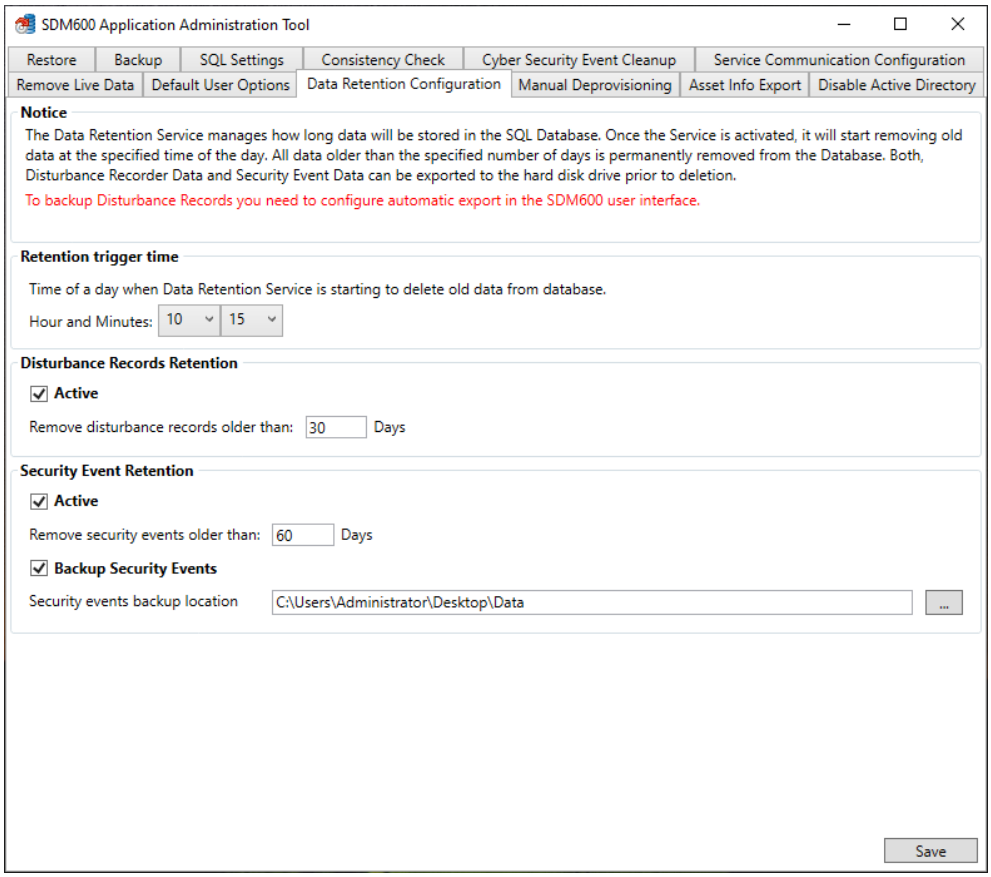


Figure 106: Data Retention Service Configuration

7.9 Manual Deprovisioning

Application Administration Tool provides a procedure to clean up corrupted provisioning data, causing parent-child and/or hot-standby synchronization issues.

To perform proper deprovisioning follow these steps:

1. On each SDM600 PC (parent, hot child, standby child) stop all the SDM600 services, except for the *SQL Server (SDMSERVER)*.

   It is important that the “SQL Server (SDMSERVER)” service is running on all SDM600 PCs. Make sure to perform Manual Deprovisioning on all the affected system at the same time.

2. Using the Application Administration Tool, perform *Manual Deprovisioning* on each system.
3. Restart SDM600 services on all the affected systems.

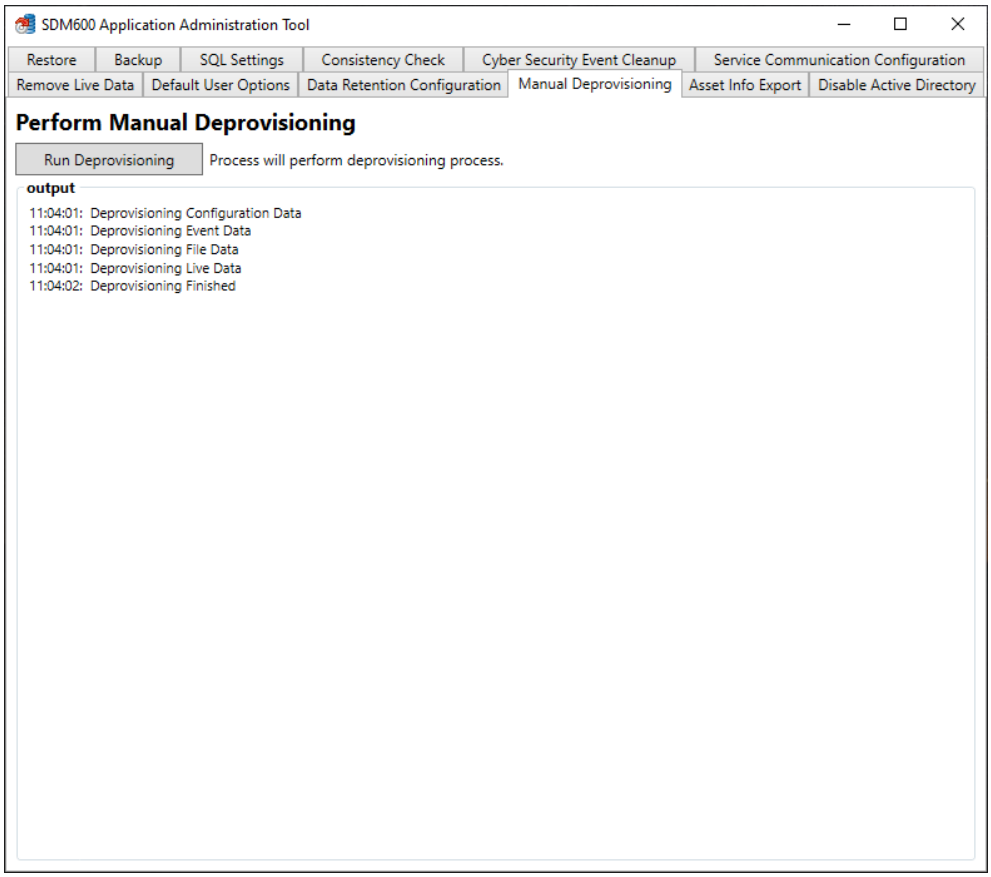


Figure 107: Manual Deprovisioning

- Follow the procedure as described. Otherwise, it could lead to no-functional SDM600.
- Create backup copies of all systems before this step.

7.10 Service Data Export

The **Service Data Export** tab in the Application Administration Tool provides the possibility to configure an automatic Excel export of the Service Data information that is happening periodically.

The automatic export can be enabled by ticking the checkbox.

Configure the target location for the exported files by using the “Browse folder” option and select a location on the system. You also must specify the frequency in days. Once configured, the automatic export will happen at midnight, with the configured frequency.

The automatic export will save the data only on the PC where SDM600 is installed.

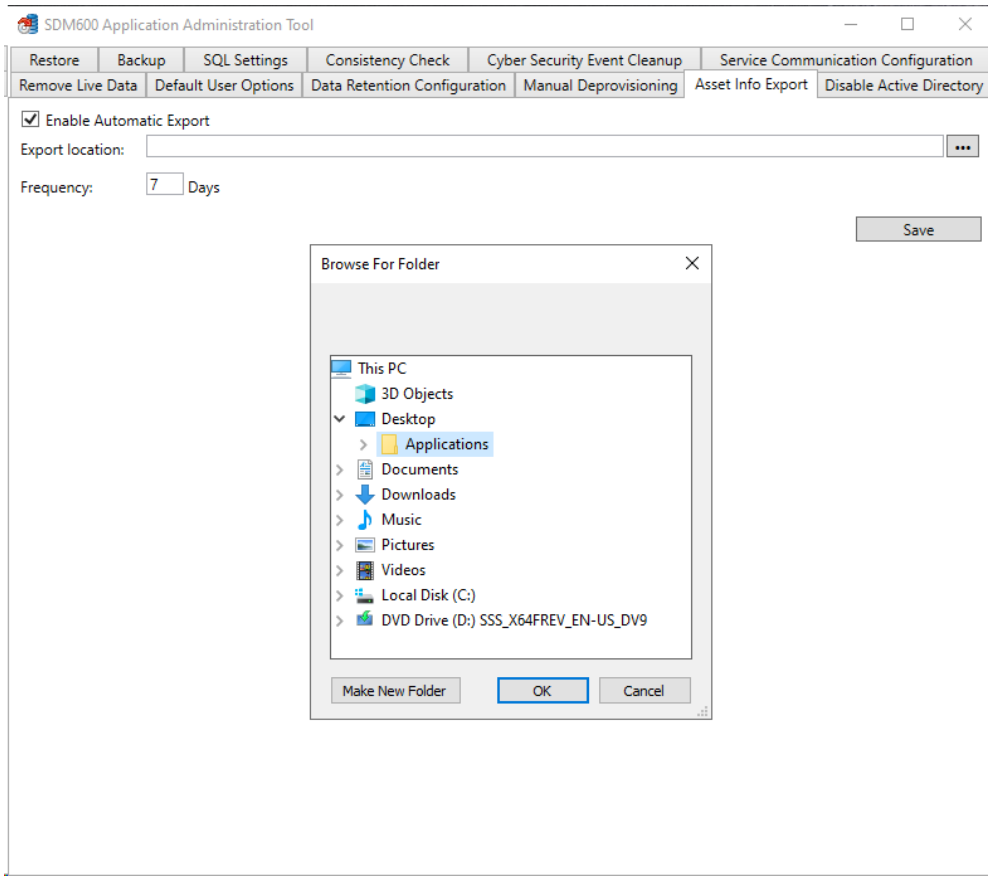


Figure 108: Automatic Service Data Export

7.11 SQL Settings

The **SQL Settings** tab in the Application Administration Tool provides the possibility to adjust the settings related to the SQL Server.

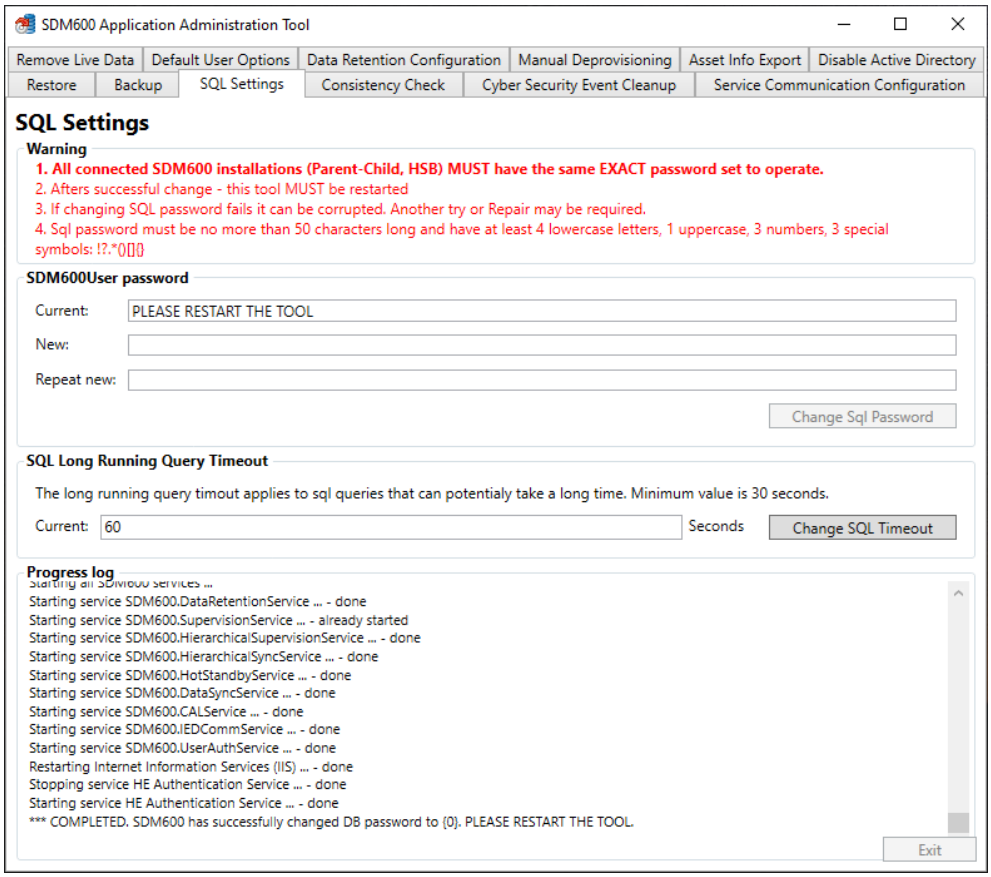


Figure 109: SQL Settings

7.11.1 SQL password

You can change the password that will be used as connection string by SDM600 towards the SQL Server database

In order to change the password, enter the new password meeting the expected complexity criteria and then press Change SQL Password.

The status of the operation can be inspected in the Progress log. During the procedure, the SDM600 services will be restarted. Once the operation is successfully completed, it is required to restart the Application Administration Tool.

RESTRICTION

LIMITATIONS APPLY!
When configuring the SQL Server database passwords for SDM600 instances belonging to a hierarchical and/or hot/standby system, the configured passwords must match.
When SDM600 instances are configured as hierarchical and/or hot/standby, failing to configure the same SQL Server database password in each SDM600 instance will cause the data synchronization to not work.

7.11.2 SQL Long Running Query Timeout

This setting allows to set a custom timeout for SQL operations in cases where you have a lot of data and the default timeout is not enough for certain long running operations. The default timeout is 60 seconds.

It cannot be decreased below 30 seconds. In certain cases it's necessary to increase it as otherwise SDM600 will show an error.

An example of this is when the Supervision Service fails to start after an upgrade of an existing SDM600 installation. Other cases where the timeout increase might help is if the removal of Live Data fails, or if there is a problem with the data retention.

Having a longer timeout might lead to you waiting long time before you get an error that is not related to the timeout itself. If you are in doubt, please consult with the SDM600 support.

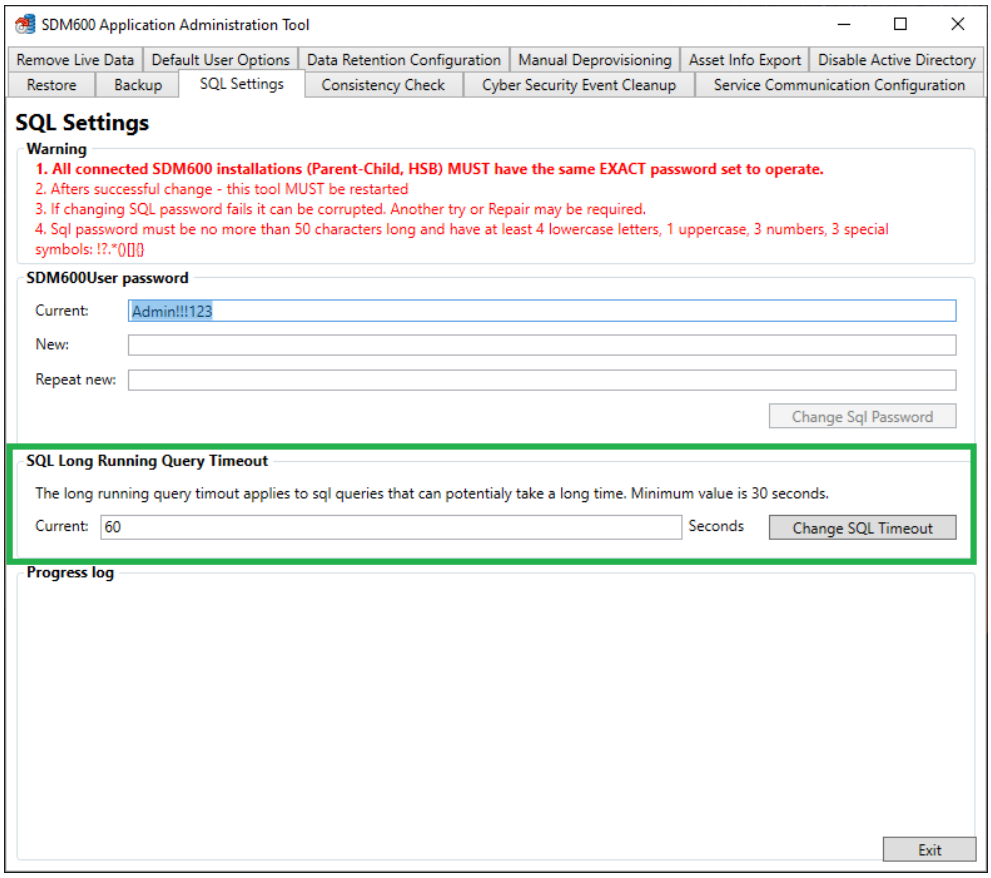


Figure 110: SQL Long Running Query Timeout

7.12 Disable Active Directory

When SDM600 is configured to authenticate against Active Directory, any change to the Domain Controller must be carefully planned and considered as it could have consequences on SDM600.

Ensure that any change to the Domain Controller is discussed with the SDM600 administrator as the configuration might require to be updated in order to ensure continuity. For example, removing or renaming Active Directory groups might cause one or more user to not be able to log into SDM600 any longer.

In the remote event that changes performed on the Domain Controller prevents the users to log into SDM600, you can disable Active Directory integration by using the Application Administration Tool from the SDM600 server.

It is only possible to disable Active Directory from the Application Administration Tool. Enabling Active Directory is not supported from the Application Administration Tool, because extensive validation must be performed: this activity must be perform form the SDM600 user interface.

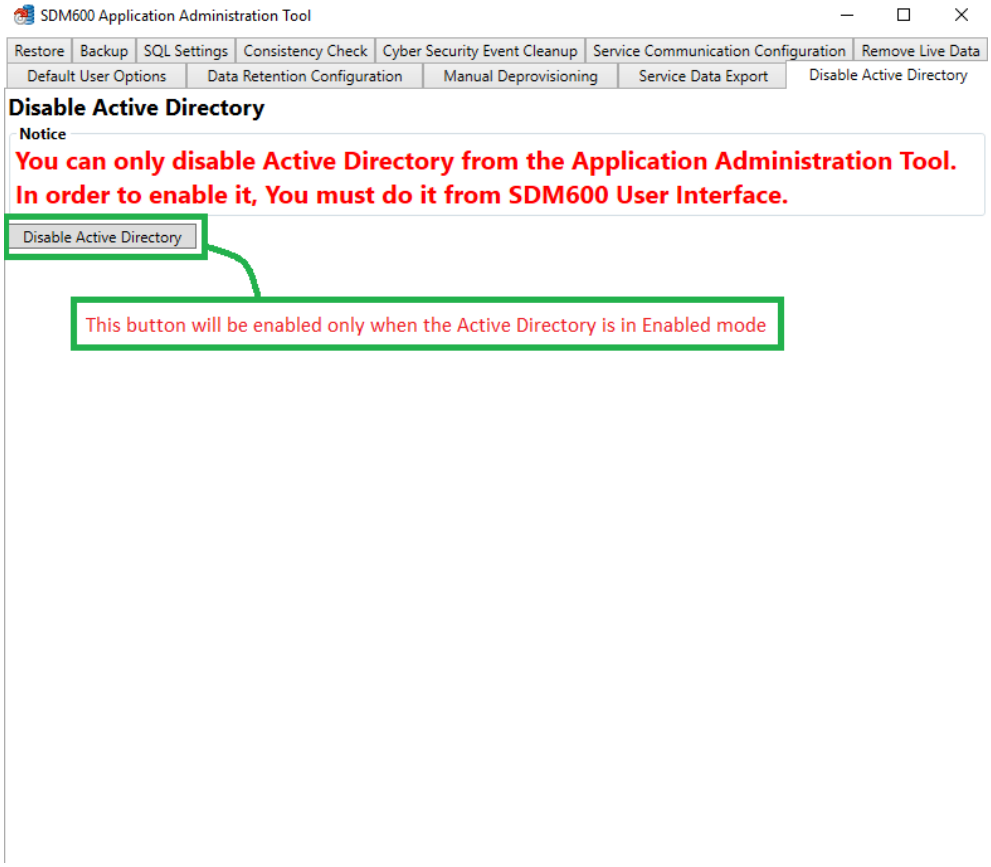


Figure 111: Disable Active Directory

Section 8 Troubleshooting

This chapter contains known problems when operating or configuring SDM600 and potential solutions. It is important to isolate the root cause of the problem, for example, whether it is a device or a SDM600 related problem.

SDM600 creates log files in the <Installation Folder>\log Folder. The log files are separated by service and provide useful information in case of problems.

Additional tools used during that phase are Network Analyzers to show the communication between devices and SDM600.

For additional information and support, contact your product provider or Hitachi Energy service organization. To contact Hitachi Energy centers, see *https://www.hitachienergy.com/contact-us/*.

When contacting Hitachi Energy support, provide as much information as possible so the problem can be reproduced, including:

- The log files (zipped folder)
- Device Type, Firmware Version
- Network Analyzer log
- SDM600 Backup

The following tips might help to resolve problems quickly.

- Cannot log into the SDM600 web UI
- Ensure all the required ports are open.

- One or more SDM600 Windows Services fail to start

- As part of the brand migration, the SDM600 Windows Services have been renamed. If one or more SDM600 Windows services fail to start, make sure the service is properly whitelisted within any antivirus products and/or security policies: the name change might be causing the issue.

- Security Events or Disturbance Recorder Data is not shown in SDM600

- SDM600 shows data for a specific Element and all its Children for a specific time span. Make sure that the data that is missing is received from one of the selected devices and that it matches the selected Time Window. It might happen that devices are not time-synchronized and send data "in the future" in this case the data cannot be shown.

- High Availability or Hierarchical setup cannot be configured

- To establish High Availability or Hierarchical setup, various communication via different ports have to be established. Make sure that the communication is not blocked by a firewall.

- COMTRADE files cannot be retrieved

- The DR files are stored on a specific folder on the devices. Make sure that the source directory is configured correctly.

- Disturbance Records are shown with a time offset

- SDM600 shows the trigger time of the Disturbance Record from the .cfg file. The timestamp should be in UTC, however it has been observed that some devices are using local times. To correct the offset, adjust the UTC Offset in SDM600.

- Security Events are shown with a time offset

- SDM600 shows the event time based on the content of the Syslog message. The timestamp should be in UTC, however it has been observed that some devices are using local times. To correct the offset, adjust the UTC Offset in SDM600.

- High Availability (HSB) or Hierarchical System cannot be established
- Ensure the SQL Database Password matches in all the SDM600 instances. You can use the Application Administration Tool to inspect and change the SQL Database Password.
- Ensure all the required ports are whitelisted in the firewall.

- SDM600 relies on digital certificates to establish secure communication between SDM600 systems. In case multiple SDM600 root certificates are found on the same PC, communication between the two systems will not work. In case the PC was cloned or a previous SDM600 backup was restored, unused root certificates must be manually deleted using the mmc tool on the Windows computer. Do not delete any certificates unless you are 100% sure of what you're doing.

- Data synchronization not working for High Availability (*HSB Synch Status* reports *Synchronization Failed*) or Hierarchical System

- SDM600 data synchronization in HSB and Hierarchical systems relies on SQL Server database synchronization. Ensure that the SQL Server database passwords configured for each SDM600 instance are identical and that the required ports for communication are open. Review and perform Manual Deprovisioning in the Application Administration Tool. If the problem persists, contact the Hitachi Energy support.

- Supervision Service fails to start after an update of an existing SDM600 installation.
- Review and increase the SQL Long Running Query Timeout in the Application Administration Tool.

- CAM Authentication is not working from an Hitachi Energy IED configured to use IEC 62351-8 (LDAP)
- Review the Minimum TLS version for 62351-8 (LDAP)

- In a Hierarchical system, the synchronization of users between the parent and the child is not working (e.g. a user is created on the parent system, but it is not available on the child system).
- The synchronization issue might be caused by network issues or instability, leading to invalid TLS session between the parent LDAP and child LDAP. Configuring thekeepalive parameters in *sldap.conf* file of all child systems will enable TCP keep-alive messages every 30 seconds, allowing to cope with network instability or issues.
  Perform the following steps *on each child system*:

1. Navigate to the SDM600 installation folder, e.g. C:\Program Files (x86)\ABB\SDM600\
2. Navigate to the OpenLDAP folder, e.g. C:\Program Files (x86)\ABB\SDM600\OpenLDAP
3. Open for edit the *slapd.conf* file
4. Locate the # syncrepl overlay entry
5. Locate the retry="60 +" entry
6. Add a new line
7. Enter a new entry: keepalive="30000:0:0"
8. Save the file
9. Restart the Hitachi Energy Authentication Service

- Windows Agent is configured for a target pc, but no data are available in SDM600.

- Occasionally, changes (including cybersecurity improvements) causes existing Windows Agent versions to no longer be compatible with a newer SDM600 version. It might be required to regenerate and redeploy the Windows Agent instances to all the target PCs. Review the Release Notes to gather more info.

- In a Hierarchical system, after restoring a backup, it is no longer possible to log into SDM600 child system.

- Issue might be caused by a type overflow bug in OpenLDAP (contextCSN or entryCSN having a negative value). Contact the Hitachi Energy support.

- In a Hierarchical system, users are not synchronized between the parent system and the child system.
- Issue might be caused by network instability. Contact the Hitachi Energy support.

- Inspecting DR files with the configured tool does not work.
- Issue might be caused by the wrong path being configured in the DRSelector. Review the Installation Guideline for more details on how to edit the DRSelector configuration.

- In a Hierarchical system, attempting to change a user's password directly from a device configured with CAM proves unsuccessful.
- Owing to technical constraints, within Hierarchical systems, this feature is exclusively operational for devices directly connected to the parent system. For this reason, it is always recommended to change passwords from the SDM600 parent system user interface.

- When using SDM600 1.3.4 or older, the installer of the *CAM for MicroSCADA* package fails for SYS600 v10.6 or newer.
- In the Windows registry, navigate to *Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services* and rename "*HE Authentication Service*" to "*ABB Authentication Service*" in registry. Restart the system to ensure the change is applied.

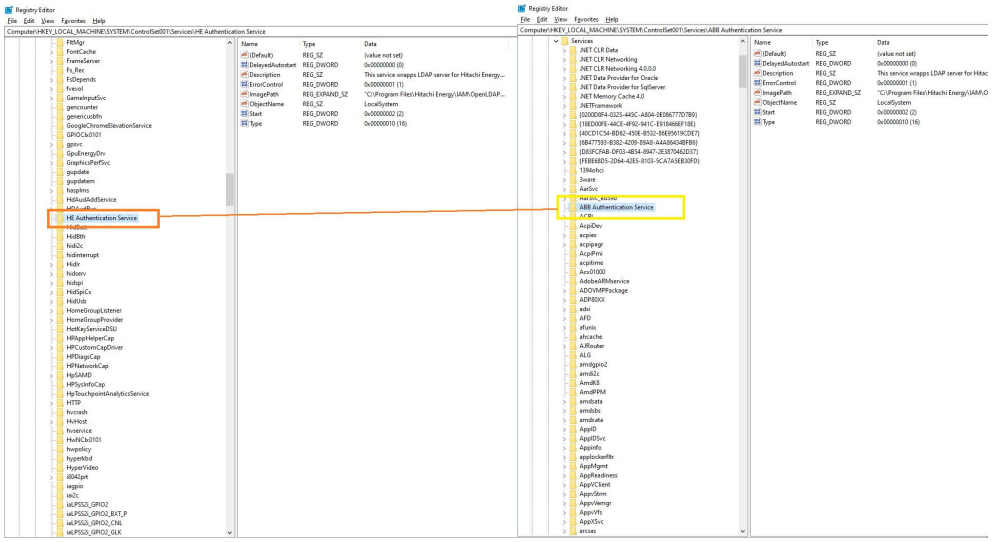


Figure 112: Rename HE Authentication Service To ABB Authentication Service

Section 9 Safety information

9.1 Backup copies

It is recommended to create a backup before making major modifications.

- Create a backup regularly to minimize the potential amount of data lost.
- Store backups on a different system, to minimize the chance of the backup being destroyed in case of the SDM600.

Backup files are encrypted and must be protected as they contain sensitive information that can be exploited by an attacker in similar ways as a live database. Therefore it is strongly recommended to protect backup files with appropriate access control.

Backup and Restore functions are provided with the SDM600 Application Administration tool.

9.2 Error reporting

In case of an error in SDM600 follow these steps:

1. Write down the possible error messages.
2. Copy the **Log** folder under SDM600 installation directory.
3. Open **Event Viewer** and look for SDM600 errors under WindowsLogs Application folder.
4. Restart the PC where SDM600 is installed.

In case the error persist, contact your SDM600 representative.

Appendix A List of Hitachi Energy Security Events

Hitachi Energy products include predefined Cybersecurity events that follow a specific definition to harmonize such events among different products. The events are sent via syslog.

Table 3:

Event ID	Type	Event Description	SDM600 Event Category
1110	Event	Login successful	Security Accountability
1115	Event	Password expired; Login successful	Security Accountability
1120	Alarm	Login failed - Unknown user	Potential Security Violation
1130	Event	Login failed - Wrong credentials	Potential Security Violation
1140	Event	Login failed - Wrong password	Potential Security Violation
1150	Alarm	Login failed - Password expired	Security Accountability
1170	Alarm	Login failed too many times	Potential Security Violation
1180	Alarm	Login failed too many user sessions	Potential Security Violation
1190	Alarm	User locked - Wrong credentials	Security Accountability
1210	Event	Logout (user logged out)	Security Accountability
1220	Event	Logout due to user inactivity (timeout)	Security Accountability
1310	Event	Connection with configuration tool successful	System Engineering and Configuration
1320	Event	Downloaded/wrote configuration successfully	System Engineering and Configuration
1321	Event	Configuration download started	System Engineering and Configuration
1322	Event	Configuration stored in the device successfully	System Engineering and Configuration
1330	Event	Uploaded/read configuration successfully	System Engineering and Configuration
1331	Event	Configuration upload started	System Engineering and Configuration
1340	Event	Downloaded/wrote firmware successfully	System Maintenance
1350	Event	Uploaded/read firmware successfully	System Maintenance
1352	Alarm	Stored certificates in the device successfully	System Operation
1356	Event	Extracted/exported archive file from device successfully	System Operation
1357	Event	Extracted/exported diagnosis file from device successfully	System Operation
1358	Event	Extracted/exported certificates from device successfully	System Operation
1360	Event	Viewed parameter value(s) successfully	System Operation
1370	Event	Viewed Security Event logs successfully	Security Operation

Table continues on next page

Event ID	Type	Event Description	SDM600 Event Category
1375	Event	Viewed disturbance records successfully	System Operation
1380	Event	Parameter changed successfully	System Engineering and Configuration
1390	Event	Downloaded Security Event list successfully	Security Operation
1400	Event	Configuration deleted successfully	System Engineering and Configuration
1410	Alarm	Connection with configuration tool failed	System Engineering and Configuration
1420	Event	Download/writing configuration failed	System Engineering and Configuration
1422	Event	Device configuration update failed	System Engineering and Configuration
1425	Alarm	File hash check failed	System Engineering and Configuration
1427	Alarm	File digital signature check failed	System Engineering and Configuration
1430	Event	Upload/read configuration failed	System Engineering and Configuration
1440	Event	Download/writing firmware failed	System Maintenance
1450	Event	Upload/read firmware failed	System Maintenance
1452	Event	Storing/writing certificates in the device failed	System Operation
1456	Event	Extracting/exporting archive file from the device failed	System Operation
1457	Event	Extracting/exporting diagnosis file from the device failed	System Operation
1458	Event	Extracting/exporting certificates from the device failed	System Operation
1460	Alarm	Parameter change failed - no rights	System Engineering and Configuration
1470	Event	Parameter change failed - out of range	System Engineering and Configuration
1480	Event	Parameter change failed - wrong type	System Engineering and Configuration
1490	Event	Download of Security Event list failed	Security Operation
1500	Alarm	Deletion of configuration failed	System Engineering and Configuration
1510	Event	Software update initiated successfully	System Maintenance
1520	Event	Software updated successfully	System Maintenance
1530	Event	License updated successfully	System Maintenance
1550	Event	Device connected to switch successfully	System Maintenance
1610	Alarm	Device software update failed	System Maintenance
1630	Alarm	License update failed	System Maintenance
1650	Event	Device disconnected from switch successfully	System Maintenacne

Table continues on next page

Event ID	Type	Event Description	SDM600 Event Category
1660	Event	View of parameter failed	System Operation
1670	Event	View of Security Event list failed	Security Operation
1675	Event	View disturbance records failed	System Operation
1680	Event	Disturbance records deleted successfully	System Operation
1682	Event	Deleted disturbance records failed	System Operation
1684	Event	Programmable LEDs cleared successfully	System Operation
1685	Event	Metering Records cleared successfully	System Operation
1686	Event	Power quality data cleared successfully	System Operation
1687	Event	Fault records cleared successfully	System Operation
1688	Event	Load Profile records cleared successfully	System Operation
1689	Event	Application function counters cleared successfully	System Operation
1710	Alarm	Device reset to factory default	System Engineering and Configuration
1720	Alarm	User accounts reset to factory default	Security Administration and Configuration
1730	Alarm	Admin password reset to factory default	Security Administration and Configuration
1783	Event	Reset indication LEDs failed	Security Administration and Configuration
1784	Event	Clear programmable LEDs failed	Security Administration and Configuration
1785	Event	Clear metering Records failed	Security Administration and Configuration
1786	Event	Clear power quality data failed	Security Administration and Configuration
1787	Event	Clear fault records failed	Security Administration and Configuration
1788	Event	Clear load Profile records failed	Security Administration and Configuration
1789	Event	Clear Application function counters failed	Security Administration and Configuration
1790	Event	Clear Security events failed	Security Administration and Configuration
2110	Event	User account created successfully	Security Administration and Configuration
2112	Event	User account added to replication group successfully	Security Administration and Configuration
2113	Event	User account removed from replication group successfully	Security Administration and Configuration
2115	Event	User account enabled successfully	Security Administration and Configuration
2117	Event	User account disabled successfully	Security Administration and Configuration

Table continues on next page

Event ID	Type	Event Description	SDM600 Event Category
2120	Event	User account deleted successfully	Security Administration and Configuration
2130	Event	User account creation failed	Security Administration and Configuration
2132	Event	Addition of user account to replication group failed	Security Administration and Configuration
2133	Event	Removal of user account from replication group failed	Security Administration and Configuration
2135	Event	User account enabling failed	Security Administration and Configuration
2137	Event	User account disabling failed	Security Administration and Configuration
2140	Event	User account deletion failed	Security Administration and Configuration
2160	Event	New role assigned to user successfully	Security Administration and Configuration
2161	Event	Permission changed successfully	Security Administration and Configuration
2162	Event	Permission added successfully	Security Administration and Configuration
2170	Event	User role assignment removed successfully	Security Administration and Configuration
2172	Event	User permission removed successfully	Security Administration and Configuration
2180	Event	New role created successfully	Security Administration and Configuration
2190	Event	Role deleted successfully	Security Administration and Configuration
2210	Event	User password changed successfully	Security Administration and Configuration
2220	Event	Change of user password failed	Security Administration and Configuration
2225	Event	User data changed successfully (for example, username, etc.)	Security Administration and Configuration
2226	Event	Change of user data failed	Security Administration and Configuration
2230	Event	New user role assignment failed	Security Administration and Configuration
2231	Event	Permission change failed	Security Administration and Configuration
2232	Event	Addition of permission failed	Security Administration and Configuration
2233	Event	User password change failed - too short	Security Administration and Configuration
2235	Event	User password change failed - policy check failed	Security Administration and Configuration
2240	Event	User session role changed successfully	Security Administration and Configuration
2245	Event	User session role change failed	Security Administration and Configuration
2270	Event	Role assignment removal failed	Security Administration and Configuration
2272	Event	User permission removed failed	Security Administration and Configuration

Table continues on next page

Event ID	Type	Event Description	SDM600 Event Category
2280	Event	New role creation failed	Security Administration and Configuration
2290	Event	Role deletion failed	Security Administration and Configuration
2310	Event	Password file downloaded successful	Security Operation
2320	Event	Password file uploaded successful	Security Operation
2350	Event	Download of password file failed	Security Operation
2360	Event	Upload of password file failed	Security Operation
2410	Event	Areas of Responsibility enabled successfully	Security Operation
2411	Event	Areas of Responsibility disabled successfully	Security Operation
2413	Event	Area of Responsibility created successfully	Security Operation
2414	Event	Area of Responsibility removed successfully	Security Operation
2416	Event	User assigned to Area of Responsibility successfully	Security Operation
2417	Event	User's Area of Responsibility assignment removed successfully	Security Operation
2420	Event	Role added to user's Area of Responsibility successfully	Security Operation
2421	Event	Role removed to user's Area of Responsibility successfully	Security Operation
2423	Event	User's Area of Responsibility role changed successfully	Security Operation
2425	Event	Area of Responsibility controlled - operator present	Security Operation
2426	Alarm	Area of Responsibility left uncontrolled - no operator	Security Operation
2430	Event	Exclusive Access Rights enabled successfully	Security Operation
2431	Event	Exclusive Access Rights disabled successfully	Security Operation
2435	Event	Exclusive access rights reassigned successfully	Security Operation
2436	Event	Exclusive Access Rights unassigned successfully	Security Operation
2437	Event	Exclusive Access Rights auto-assigned successfully	Security Operation
2440	Event	Exclusive Access Rights added to user's AoR successfully	Security Operation
2441	Event	Exclusive Access Rights removed from user's AoR successfully	Security Operation
2442	Event	User's Exclusive Access Rights role changed successfully	Security Operation
2460	Event	Failed to enable Areas of Responsibility	Security Operation

Table continues on next page

Event ID	Type	Event Description	SDM600 Event Category
2461	Event	Failed to disable Areas of Responsibility	Security Operation
2463	Event	Failed to create Area of Responsibility	Security Operation
2464	Event	Failed to remove Area of Responsibility	Security Operation
2466	Event	Failed to assign Area of Responsibility to user	Security Operation
2467	Event	Failed to remove AoR assignment from user	Security Operation
2470	Event	Failed to add Role to user's Area of Responsibility	Security Operation
2471	Event	Failed to remove Role to user's Area of Responsibility	Security Operation
2473	Event	Failed to change Role in User's Area of Responsibility	Security Operation
2480	Alarm	Failed to enable Exclusive Access Rights	Security Operation
2481	Event	Failed to disable Exclusive Access Rights	Security Operation
2485	Event	Failed to reassign Exclusive Access Rights	Security Operation
2486	Event	Failed to unassign Exclusive Access Rights	Security Operation
2487	Event	Failed to auto-assign Exclusive Access Rights	Security Operation
2490	Event	Failed to add Exclusive Access Rights to user's AoR	Security Operation
2491	Event	Failed to remove Exclusive Access Rights from user's AoR	Security Operation
2492	Event	Failed to change user's Exclusive Access Rights role	Security Operation
2510	Alarm	Password file on CF card corrupted	Security Operation
2520	Alarm	Password file corrupted	Security Operation
3110	Event	TCP communication with security log subscriber successful	Communication
3120	Event	TCP communication with security log publisher successful	Communication
3150	Event	TCP communication with security log server successful	Communication
3190	Event	Ethernet reconnection	Communication
3210	Alarm	TCP communication with security log subscriber failed	Communication
3220	Alarm	Log data hash check failed (Log data altered)	Communication
3230	Alarm	TCP communication with security log publisher failed	Communication
3250	Alarm	TCP communication with security log server failed - Event not sent	Communication
3290	Alarm	Ethernet connection failure	Communication

Table continues on next page

Event ID	Type	Event Description	SDM600 Event Category
3292	Alarm	Communication failure - Negotiation failed	Communication
3293	Alarm	Communication failure - Cipher suite negotiation failed	Communication
3294	Alarm	Communication failure - Key negotiation failed	Communication
3296	Alarm	Communication failure - Peer authentication failed	Communication
3298	Alarm	Communication failure - Packet authentication failed	Communication
3420	Alarm	Security log file deleted by user	Potential Security Violation
3430	Event	SEC_Security log file deleted by system	System Engineering and Configuration
3440	Alarm	Security logs edited by user	Potential Security Violation
3710	Event	CAM server communication successful	Security Operation
3810	Alarm	CAM server communication failed	Security Operation
3820	Alarm	Replication performed. No users replicated!	Security Operation
3830	Alarm	Replication attempted but failed. No capacity	Security Operation
4110	Event	SSL connection successful	Security Operation
4120	Alarm	SSL connection/certificate accepted	Security Operation
4130	Alarm	TLS certificate validation check disabled successfully	Security Operation
4210	Alarm	SSL connection failed - Certificate validation failed	Potential Security Violation
4220	Alarm	SSL connection failed - IKE failed	Potential Security Violation
4310	Event	VPN connection successful	Security Operation
4350	Alarm	VPN connection failed - Negotiation failed	Potential Security Violation
4360	Alarm	VPN connection failed - IKE failed	Potential Security Violation
5110	Event	Manual reset	System Operation
5120	Event	Reset trips	System Operation
5130	Event	Reset LEDs	System Operation
5140	Event	Protection system restarted	System Operation
5150	Alarm	Control system restarted	System Operation
5152	Alarm	Control system restarted	System Operation
5160	Event	Gateway/RTU restarted	System Operation
5270	Alarm	System startup	System Operation
5272	Alarm	System startup failed	System Operation
5280	Event	System shutting down	System Operation
6110	Event	Test Mode started	System Operation
6112	Event	Starting of Test Mode failed	System Operation
6120	Event	Test Mode ended	System Operation
6130	Event	Control operation performed successfully	System Operation

Table continues on next page

Event ID	Type	Event Description	SDM600 Event Category
6132	Event	Failed to perform a control operation	System Operation
6140	Event	Signal forced - value changed	System Operation
6150	Event	Test Event - to test routing configuration	System Operation
6160	Event	General command performed successfully	System Operation
6162	Event	Failed to perform a general command	System Operation
6170	Event	Simulation Mode started	System Operation
6172	Event	Starting of Simulation Mode failed	System Operation
6175	Event	Simulation Mode ended	System Operation
6180	Event	Blocked Mode started	System Operation
6182	Event	Blocked of Simulation Mode failed	System Operation
6185	Event	Blocked Mode ended	System Operation
6180	Event	Blocked Mode started successfully	System Operation
6182	Event	Blocked of Simulation Mode failed	System Operation
6185	Event	Blocked Mode ended successfully	System Operation
6190	Event	Added graphical object successfully	System Operation
6192	Event	Failed to add graphical object	System Operation
6194	Event	Modified graphical object successfully	System Operation
6196	Event	Failed to modify graphical object	System Operation
6210	Event	System time set manually successfully	System Engineering and Configuration
6220	Event	Source time sync operation successful	System Engineering and Configuration
6310	Event	System time set manually failed	System Engineering and Configuration
6320	Event	Source time sync operation failed	System Engineering and Configuration
6410	Alarm	Antivirus found a virus	System Operation
6412	Alarm	Antivirus failed to gain scanning access to file or directory	System Operation
6414	Alarm	Antivirus detected checksum (digital signature) failure	System Operation
6416	Alarm	Antivirus not fully operational	System Operation
6418	Alarm	Antivirus shutdown	System Operation
6420	Event	Antivirus started	System Operation
6422	Alarm	Antivirus scan stopped	System Operation
6424	Event	Antivirus scan delayed	System Operation
6426	Event	Antivirus scan restarted	System Operation
6428	Alarm	Antivirus log forwarding error	System Operation

Table continues on next page

Event ID	Type	Event Description	SDM600 Event Category
6432	Event	Antivirus performed a repair successfully	System Operation
6434	Alarm	Antivirus engine or signature update failed	System Operation
6497	Alarm	Antivirus general info event, see antivirus logs for details	Security Operation
6498	Alarm	Antivirus general warning event, see antivirus logs for details	Security Operation
6499	Alarm	Antivirus general error event, see antivirus logs for details	Security Operation
6510	Alarm	Debug mode started successfully	System Maintenance
6515	Alarm	Starting Debug Mode failed	System Maintenance
6520	Event	Debug Mode ended	System Maintenance
6550	Event	Protocol logging mode started	System Maintenance
6560	Event	Protocol logging mode ended	System Maintenance
6570	Event	Service started successfully	System Operation
6571	Event	Service enabled successfully	System Operation
6572	Alarm	Failed to start service	System Operation
6573	Alarm	Failed to enable service	System Operation
6575	Alarm	Service stopped successfully	System Operation
6577	Alarm	Stopping of service failed	System Operation
6578	Event	Task started successfully	System Operation
6579	Alarm	Failed to start task	System Operation
6580	Event	Data capturing started successfully	System Operation
6582	Event	Start of data capturing failed	System Operation
6585	Event	Data capturing stopped successfully	System Operation
6587	Event	Stopping of data capturing failed	System Operation
6590	Alarm	MCM configuration changed successfully	System Operation
6592	Alarm	Change of MCM configuration failed	System Operation
6595	Alarm	MCM configuration reset successfully	System Operation
6597	Alarm	Resetting of MCM configuration failed	System Operation
6610	Event	Flagged object for history storage successfully	System Operation
6612	Event	Failed to flag object for history storage	System Operation
6613	Event	Unflagged object for history storage successfully	System Operation
6615	Event	Failed to unflag object for history storage	System Operation
6620	Alarm	802.1X state changed to locked unauthenticated	System Operation
6621	Event	802.1X state changed to authenticated	System Operation

Table continues on next page

Event ID	Type	Event Description	SDM600 Event Category
6622	Event	802.1X state changed to unauthenticated	System Operation
6623	Event	Interface changed state to up	System Operation
6624	Event	Interface changed state to down	System Operation
6625	Event	SFP inserted	System Operation
6626	Event	SFP removed	System Operation
6627	Alarm	No more SSH sessions possible	System Operation
6628	Alarm	Fallback password authentication activated	System Operation
6629	Alarm	Session ID spoof detected	System Operation
6630	Alarm	Timeout occurred when contacting the RADIUS server	System Operation
6631	Event	Activating alternative RADIUS server due to primary unreachable	System Operation
6632	Alarm	Timeout occurred when contacting the SNTP server	System Operation
6633	Event	Activating alternative SNTP server due to primary unreachable	System Operation
6634	Alarm	X.509 certificate pub key does not match private key	System Operation
7110	Event	Switching device open	System Operation
7120	Event	Switching device close	System Operation
7310	Alarm	Hardware change detected	System Engineering and Configuration
8010	Alarm	Recovery of previous configuration successful	System Engineering and Configuration
8020	Event	Date and time set successfully	System Engineering and Configuration
8030	Event	New certificate generated successfully	System Engineering and Configuration
8040	Event	Communication system startup successful	System Operation
8050	Event	System backup performed successfully	System Operation
8060	Event	System backup started successfully	System Operation
8070	Event	System restore performed successfully	System Operation
8080	Event	System restore started successfully	System Operation
8090	Event	Baseline checked : OK	System Operation
8210	Alarm	Recovery of previous configuration failed	System Engineering and Configuration
8220	Event	Date and time setting failed	System Engineering and Configuration
8230	Event	New certificate generation failed	System Operation
8240	Event	Communication system startup failed	System Operation

Table continues on next page

Event ID	Type	Event Description	SDM600 Event Category
8250	Event	System backup failed	System Operation
8260	Event	Failed to start system backup	System Operation
8270	Event	Failed to restore the system	System Operation
8280	Event	Failed to start system restore	System Operation
8290	Event	Unexpected baseline	System Operation
9010	Alarm	Flooding attack detected	Potential Security Violation
9020	Alarm	Malformed packets attack detected	Potential Security Violation
9025	Alarm	Replayed packets detected	Potential Security Violation
9030	Alarm	Intrusion detected or Application blocked	Potential Security Violation
9040	Alarm	Intrusion detected	Potential Security Violation
9050	Alarm	Intrusion detected or Application blocked	Potential Security Violation
9060	Alarm	IDS detected unknown traffic	Potential Security Violation
9070	Alarm	IDS detected illegal traffic	Potential Security Violation
9080	Alarm	IDS detected missing traffic	Potential Security Violation
9110	Alarm	Firewall blocked incoming connection	Potential Security Violation
9120	Alarm	Firewall blocked outgoing connection	Potential Security Violation
9130	Alarm	Firewall stopped/disabled	Security Operation
9140	Alarm	Firewall started/enabled	Security Operation
9150	Alarm	Firewall settings/rules changed successfully	Security Administration and Configuration
9260	Alarm	IPS event log full	Security Administration and Configuration
9310	Alarm	File access blocked by protection software	Security Administration and Configuration
9320	Alarm	File access would've been blocked if policy enforced	Security Administration and Configuration
9330	Alarm	File access whitelisted	Security Operation
9340	Alarm	File access blacklisted	Security Operation
9350	Alarm	Process terminated due to unauthorized call	Security Administration and Configuration
9352	Alarm	System configuration change blocked by protection software	Security Administration and Configuration
9210	Alarm	IPS blocked incoming packet	Potential Security Violation
9220	Alarm	IPS blocked incoming packet	Potential Security Violation
9230	Alarm	IPS stopped/disabled	Security Operation
9240	Alarm	IPS started/enabled	Security Operation
9250	Alarm	IPS settings/rules changed successfully	Security Administration and Configuration
9510	Alarm	CSR approved and certificate issued successfully	Security Administration and Configuration
9511	Event	CSR is pending for approval	Security Administration and Configuration
9520	Alarm	Certificate signing request failed	Security Administration and Configuration

Table continues on next page

Event ID	Type	Event Description	SDM600 Event Category
9530	Alarm	Certificate about to expire	Security Administration and Configuration
9540	Alarm	Communication with CA/RA failed	Security Administration and Configuration
9610	Alarm	Certificate validation succeeded	Security Administration and Configuration
9615	Alarm	Certificate validation failed	Security Administration and Configuration
9620	Alarm	Certificate validation failed - Certificate expired	Security Administration and Configuration
9630	Alarm	Certificate validation failed - Certificate revoked	Security Administration and Configuration
9640	Alarm	Certificate validation failed - Certificate signature check failed	Security Administration and Configuration
9710	Event	Transfer CRL into the entity successfully	Security Administration and Configuration
9810	Alarm	Failed to transfer the CRL into the device	Security Administration and Configuration
9820	Alarm	Unknown certificate revocation status. CRL not available.	Security Administration and Configuration
9830	Alarm	CRL expired	Security Administration and Configuration
9860	Event	OCSP communication failure	Security Administration and Configuration
9870	Event	OCSP: Unknown certificate revocation status	Security Administration and Configuration
9990	Event	Unidentified Syslog event	Unknown
9991	Event	Unidentified IEC 61850 event	Unknown
9995	Alarm	UAL Syslog FIFO receiver overflow, message overwritten	Security Operation
9996	Alarm	UAL Syslog FIFO sender overflow, message overwritten	Security Operation
10010	Event	Device successfully entered maintenance menu due to a user action	System Maintenance
10012	Event	Device failed to enter maintenance menu due to a user action	System Maintenance
10020	Event	Device successfully forced into maintenance menu due to new state	System Maintenance
10022	Event	Device failed to force maintenance menu after a new state	System Maintenance
10030	Event	FTP server successfully activated from maintenance menu	System Maintenance
10032	Event	Activation of FTP server from maintenance menu failed	System Maintenance
10040	Event	Firmware update procedure aborted successfully	System Maintenance

Table continues on next page

Event ID	Type	Event Description	SDM600 Event Category
10042	Event	Failed to abort firmware update procedure	System Maintenance
10050	Event	Recovery menu entered successfully	System Maintenance
10052	Event	Failed to enter Recovery menu	System Maintenance
10060	Event	Authentication disabled from Maintenance menu successfully	System Maintenance
10062	Event	Failed to disable authentication from Maintenance menu	System Maintenance
10070	Event	Change lock disabled successfully from Maintenance menu	System Maintenance
10072	Event	Failed to disable change lock from Maintenance menu	System Maintenance
10080	Event	IEC 61850 disabled successfully from Maintenance menu	System Maintenance
10082	Event	Failed to disable IEC 61850 from Maintenance menu	System Maintenance
10090	Event	Flagged object for Maintenance successfully	System Maintenance
10092	Event	Failed to flag object for maintenance	System Maintenance
10093	Event	Unflagged object for Maintenance successfully	System Maintenance
10095	Event	Failed to unflag object for maintenance	System Maintenance
13200	Event	Configuration transferred to the device successfully	System Engineering and Configuration
13210	Event	Configuration transfer to the device started	System Engineering and Configuration
13220	Event	Configuration changed successfully	System Engineering and Configuration
13250	Event	Entered configuration mode successfully	System Engineering and Configuration
13260	Event	Exited configuration mode successfully	System Engineering and Configuration
13300	Event	Configuration files read/ exported from the device successfully	System Engineering and Configuration
13310	Event	Configuration exporting from the device started successfully	System Engineering and Configuration
13400	Event	Firmware transferred to the device successfully	System Engineering and Configuration
13500	Event	Firmware files read/exported from the device successfully	System Engineering and Configuration
13520	Event	Certificates transferred to the device successfully	System Engineering and Configuration
13560	Event	Exported/read archive file from the device successfully	System Engineering and Configuration
13570	Event	Exported/read diagnosis file from the device successfully	System Engineering and Configuration

Table continues on next page

Event ID	Type	Event Description	SDM600 Event Category
13580	Event	Exported/read certificates from device successfully	System Engineering and Configuration
13610	Alarm	Installed entity certificate successfully	System Operation
13620	Alarm	Removed entity certificate successfully	System Operation
13630	Alarm	Installed trust anchor certificate successfully	System Operation
13640	Alarm	Removed trust anchor certificate successfully	System Operation
13710	Alarm	Failed to install entity certificate	System Operation
13720	Alarm	Failed to remove entity certificate	System Operation
13730	Alarm	Failed to install trust anchor certificate	System Operation
13740	Alarm	Failed to remove trust anchor certificate	System Operation
13900	Alarm	Security logs read/exported from the device successfully	Security Administration and Configuration
13910	Alarm	Security logs report generated successfully	Security Administration and Configuration
14200	Event	Failed to transfer configuration to the device	System Engineering and Configuration
14210	Event	Failed to start transfer of configuration to the device	System Engineering and Configuration
14220	Event	Failed to change the configuration	System Engineering and Configuration
14250	Event	Failed to enter configuration mode	System Engineering and Configuration
14260	Event	Failed to exit configuration mode	System Engineering and Configuration
14300	Event	Failed to read configuration files from the device	System Engineering and Configuration
14310	Event	Failed to start export of configuration from the device	System Engineering and Configuration
14400	Event	Failed to transfer firmware to the device	System Engineering and Configuration
14500	Event	Failed to read firmware files from the device	System Engineering and Configuration
14520	Event	Failed to transfer certificates to the device	System Engineering and Configuration
14560	Event	Failed to read archive file from the device	System Engineering and Configuration
14570	Event	Failed to read diagnosis file from the device	System Engineering and Configuration
14580	Event	Failed to read certificates from the device	System Engineering and Configuration
14900	Event	Failed to read security logs from the device	Security Administration and Configuration
14910	Alarm	Failed to generate security logs report	Security Administration and Configuration
23100	Event	Password file transferred and stored in the device successfully	Security Operation

Table continues on next page

Event ID	Type	Event Description	SDM600 Event Category
23200	Event	Password file read/exported from the device successfully	Security Operation
23500	Event	Failed to transfer password file to the device	Security Operation
23600	Event	Failed to read password file from the device	Security Operation
15010	Event	Controller mode changed to configuration mode successfully	System Engineering and Configuration
15020	Event	Controller mode changed to execute mode successfully	System Engineering and Configuration
15110	Alarm	Controller mode change to configuration mode failed	System Engineering and Configuration
15120	Alarm	Controller mode change to execute mode failed	System Engineering and Configuration
15200	Event	Bus IF mounted successfully	System Engineering and Configuration
15210	Event	Bus IF unmounted successfully	System Engineering and Configuration
15220	Event	Global device configuration updated successfully	System Engineering and Configuration
15230	Event	Configuration data initialized successfully	System Engineering and Configuration
15240	Event	Complete configuration data reloaded successfully	System Engineering and Configuration
15250	Event	CCO converted module process variables removed successfully	System Engineering and Configuration
15260	Event	Function diagrams commissioned successfully	System Engineering and Configuration
15270	Event	CCO process variable parameterized successfully	System Engineering and Configuration
15280	Event	Single parameter parameterized successfully	System Engineering and Configuration
15290	Event	Single parameter simulated successfully	System Engineering and Configuration
15300	Event	Bus IF mounting failed	System Engineering and Configuration
15310	Event	Bus IF unmounting failed	System Engineering and Configuration
15320	Alarm	Global device configuration update failed	System Engineering and Configuration
15330	Event	Configuration data initialization failed	System Engineering and Configuration
15340	Event	Complete configuration data reload failed	System Engineering and Configuration
15350	Event	CCO converted module process variables removal failed	System Engineering and Configuration
15360	Event	Function diagrams commissioning failed	System Engineering and Configuration
15370	Event	CCO process variable parametrization failed	System Engineering and Configuration
15380	Event	Single parameter parametrization failed	System Engineering and Configuration
15390	Event	Single parameter simulation failed	System Engineering and Configuration

Table continues on next page

Event ID	Type	Event Description	SDM600 Event Category
15410	Event	Profibus master/slave configured successfully	System Engineering and Configuration
15420	Event	Profibus channel configured successfully	System Engineering and Configuration
15430	Event	Profibus parameterized channel configured successfully	System Engineering and Configuration
15440	Event	Profibus master/slave configuration reloaded successfully	System Engineering and Configuration
15450	Event	Profibus channel configuration reloaded successfully	System Engineering and Configuration
15510	Alarm	Profibus master/slave configuration failed	System Engineering and Configuration
15520	Alarm	Profibus channel configuration failed	System Engineering and Configuration
15530	Alarm	Profibus parameterized channel configuration failed	System Engineering and Configuration
15540	Event	Profibus master/slave configuration reload failed	System Engineering and Configuration
15550	Event	Profibus channel configuration reload failed	System Engineering and Configuration
15610	Event	IEC 61850 stack initialized successfully	System Operation
15620	Event	IEC 61850 stack configured successfully	System Engineering and Configuration
15630	Event	IEC 61850 stack configuration reloaded successfully	System Engineering and Configuration
15710	Event	IEC 61850 stack initialization failed	System Operation
15720	Alarm	IEC 61850 stack configuration failed	System Engineering and Configuration
15730	Event	IEC 61850 stack configuration reload failed	System Engineering and Configuration
15740	Event	IEC 60870-5-104 connection opened (Interface 1)	System Operation
15741	Event	IEC 60870-5-104 connection closed (Interface 1)	System Operation
15742	Event	IEC 60870-5-101 connection opened (Interface 1)	System Operation
15743	Event	IEC 60870-5-101 connection closed (Interface 1)	System Operation
15744	Event	IEC 60870-5-104 connection opened (Interface 2)	System Operation
15745	Event	IEC 60870-5-104 connection closed (Interface 2)	System Operation
15746	Event	IEC 60870-5-101 connection opened (Interface 2)	System Operation
15747	Event	IEC 60870-5-101 connection closed (Interface 2)	System Operation
15770	Event	RS-232/-485 tunnel connected (Console0)	System Operation
15771	Event	RS-232/-485 tunnel disconnected (Console0)	System Operation

Table continues on next page

Event ID	Type	Event Description	SDM600 Event Category
15772	Event	RS-232/-485 tunnel connected (Console1)	System Operation
15773	Event	RS-232/-485 tunnel disconnected (Console1)	System Operation
15810	Event	Control parameter read and view from device successfully	System Operation
15850	Event	Operable parameters read from device into project data base successfully	System Operation
15860	Event	Operable parameters transferred and stored into the device successfully	System Operation
15890	Event	Generic DTM event	System Operation
15910	Event	Failed to read control value parameter from device	System Operation
15950	Event	Failed to read operable parameters from device into project data base	System Operation
15960	Event	Failed to transfer and store operable parameters into the device	System Operation

Appendix B Mapping Windows Events to Hitachi Energy Security Events

The SDM600 Windows Event forwarder converts Windows Events to The Hitachi Energy specific Format defined in the previous chapter. The Windows Event IDs are mapped to the Hitachi Energy format to achieve consistency.

EventID	Successful Windows Event result	Fail Windows Event Result	Event Description
1102	3420		Security log file deleted by user
4608	5270	5272	System startup
4609	5280		System shutting down
4616	8020	8220	Date and time set
4624	1110		Login successful
4625		1130	Login failed
4634	1210		Logout (user logged out)
4647	1210		Logout (user logged out)
4649	9020		Flooding attack detected
4650, 4651	4310	4350	VPN connection
4652, 4653, 4654	4350	4350	VPN connection failed - Negotiation failed
4704	2162	2232	Permission added
4705	2172	2272	User permission removed
4720	2110	2130	User account created
4722	2115	2135	User account enabled
4723	2220	2220	Change of user password failed
4724	2220	2220	Change of user password failed
4725	2117	2137	User account disabled
4726	2120	2140	User account deleted
4774	1110	1130	Login
4775	1130	1130	Login failed - Wrong credentials
4887	9510	9520	CSR approved and certificate issued successfully
4888	9520	9520	Certificate signing request failed
4946, 4947, 4948, 4950	9150		Firewall settings/rules changed
4976, 4977, 4978	4350	4350	VPN connection failed - Negotiation failed
4979, 4980, 4981, 4982	4310	4350	VPN connection successful
4983, 4984	4350	4350	VPN connection failed - Negotiation failed
5031	9110		Firewall blocked incoming connection
5148	9010		Flooding attack detected
5152	9210	9210	IPS blocked incoming packet

Table continues on next page

EventID	Successful Windows Event result	Fail Windows Event Result	Event Description
5155	9110	9110	Firewall blocked incoming connection
5451	4310	4360	VPN connection successful
5453	4360	4360	VPN connection failed - IKE failed

Appendix C Security Events generated by SDM600

SDM600 is creating security Events for specific user interaction.

EventID	Event Description	Cause of Event in SDM600
1110	Login successful	When a user successfully logged into SDM600
1115	Password expired; login successful	When a user manages to log in even if the user's password has expired
1130	Login failed - Wrong credentials	When a user enters a wrong combination of username and password
1210	Logout (user logged out)	When a user logged out from SDM600
2110	User account created successfully	When a new user account is successfully created
2120	User account deleted successfully	When a user account is successfully deleted
2160	New role assigned to user successfully	When a new role is successfully assigned to a user
2161	Permission changed successfully	When a user adjusts the SDM600 role to right mapping
2170	User role assignment removed successfully	When a user role is successfully removed from a user's role assignment
2210	User password changed successfully	When a user changes their password by entering correct required credentials
2220	Change of user password failed	When a user changes their password by entering a wrong combination of the required credentials
2225	User data changed successfully (for example, username, etc.)	When a user changes their data
8030	New certificate generated successfully	When a user requests SDM600 to generate a certificate and the certificate is successfully generated
8050	System backup performed successfully	When a user requests SDM600 to perform a system backup and the request is executed successfully
8230	New certificate generation failed	When a user requests SDM600 to generate a certificate and the certificate is not successfully generated
8250	System backup failed	When a user requests SDM600 to perform a system backup and the request is not executed successfully
13200	Configuration transferred to the device successfully	When a user requests SDM600 to generate configuration files for another application or device to integrate it into SDM600 Centralized Account Management and Centralized Activity Logging and the configuration files successfully generated and saved to user preferred location
13220	Configuration changed successfully	When a user conducts any configuration changes in SDM600, and the configuration is successfully applied
13520	Certificates transferred to the device successfully	When a user manages to export the credential that is used to sign certificates for all devices

Table continues on next page

EventID	Event Description	Cause of Event in SDM600
14200	Failed to transfer configuration to the device	When a user requests SDM600 to generate configuration files for another application or device to integrate it into SDM600 Centralized Account Management and Centralized Activity Logging and the configuration file fails to generate, or configuration files are not saved properly to user preferred location
14220	Failed to change the configuration	When a user conducts any configuration changes in SDM600, and the configuration is not successfully applied
14520	Failed to transfer certificates to the device	When a user fails to export the credential that is used to sign certificates for all devices

Appendix D Activities in SDM600 that generate Configuration Changed Security Events

The following activities in SDM600 will generate a “Configuration Changed” Security Event in the SDM600 Security Event List:

- SDM600 - new root certificate created and applied.
- SDM600 - selection and application existing certificate from store.
- SDM600 - import and application existing certificate from file.
- SDM600 child modified.
- SDM600 child device added.
- Bay added.
- Bay deleted
- Bay modified
- Data Retention Export Configuration added
- Data Retention Export Configuration deleted
- Data Retention Export Configuration modified
- IED added
- IED deleted
- IED modified
- IED group added
- IED group deleted
- IED group modified
- Substation added
- Substation deleted
- Substation modified
- Substation group added
- Substation group deleted
- Substation group modified
- Syslog Publisher added
- Syslog Publisher deleted
- Syslog Publisher modified
- System Certificate config added
- Voltage level added
- Voltage level deleted
- Voltage level modified
- SDM600 child data polling interval changed
- Certificate Config deleted

- System Certificate config modified
- SDM600 switched back to standalone configuration
- Secure communication connection opened
- SDM600 Hot-Standby termination
- Import SCD
- Generated certificate for device
- Updated Hsb Sys Config
- Updated Hrc Sync Config
- Updated SDM600 device
- Updated CAM config
- Updated SDM600 configuration
- Updated Notification
- Updated Notification Recipient
- Updated Notification Condition
- Updated Notification Condition Value Pair
- Updated Property Configuration
- User Settings modified
- User Settings deleted

Appendix E Used communication ports and services

Hardware and software firewalls can block traffic from or to SDM600. To function properly, SDM600 requires the following default incoming ports to be opened:

Port No.	Description	Condition
ICMP echo request and ICMP echo reply	Ping to check if connection to the device is possible	Always
389 TCP, 636 TCP	Port for SDM600 Centralized Account Management (LDAP Authentication)	Always
443 TCP, 54687 TCP, 54688 TCP	Ports required for HTTPS web access.	Always
1433 TCP, 58900 TCP	Port for SQL Server data synchronization	Required between SDM600 nodes only if used in Hierarchical and/orHot-Standby Setup
1468 TCP	Port for SDM600 Centralized Activity Logging Service	Required only if receiving Syslog events over TPC
1812 UDP and TCP	Port for SDM600 Centralized Account Management Service	Required only if configured to provide CAM over RADIUS protocol
59100 - 59199 TCP	SDM600 internal service: Parent-Child Initialization	Required between SDM600 nodes only during Hierarchical configuration. Ports can be blocked after successful Hierarchical Setup
59200 TCP	SDM600 internal service: Centralized Activity Logging Service	Required between SDM600 and integrated Windows endpoints only if receiving events from *Windows Event Log Forwarder*
59960 TCP	SDM600 internal service: Hierarchical data synchronization	Required between SDM600 nodes only on the child system in Hierarchical configuration
59990 - 59999 TCP	SDM600 internal service: Hot-Standby Initialization	Required between SDM600 nodes only during Hot-Standby configuration. Ports can be blocked after successful Hot-Standby Setup
60000 - 60010 TCP	SDM600 internal service: Hot-Standby data synchronization	Required between SDM600 nodes only if used in Hot-Standby configuration
514 UDP	Port for SDM600 Centralized Activity Logging Service	Required only if receiving Syslog events over UDP
990 TCP and 989 TCP	Disturbance Records retrieval over FTPS.	Required only if configured to collect Disturbance Records files over FTPS.
22 TCP	Disturbance Records retrieval over SFTP.	Required only if configured to collect Disturbance Records files over SFTP.
21 TCP	Disturbance Records retrieval over FTP.	Required only if configured to collect Disturbance Records files over FTP.
389 TCP and 636 TCP	Active Directory	Required only if Active Directory feature is used
25 TCP, 465 TCP or 587 TCP	SMTP	Required only if Mail Notification feature is used.
102 TCP	MMS Device Connections	Rquired if any device is setup to use the MMS protocol
161 TCP	SNMP Device Connections	Rquired if any device is setup to use the SNMP protocol

Each hardware firewall device or software solution comes with an instruction manual on how to configure the firewall to allow certain traffic to pass.

HITACHI
Inspire the Next

Hitachi Energy Finland Oy
Grid Automation
PL 688
65101 Vaasa, Finland

https://hitachienergy.com/microscadax

Scan this QR code to visit our website

8DCB000001

Hitachi Energy