System Data Manager SDM600
User Manual
## Contents

1  **Copyrights**  

2  **Version Information**  

3  **Introductions**  
   3.1  Scope of the Document  
   3.2  Use of symbols  
   3.3  Abbreviations and Definitions  
   3.4  Related documents  

4  **Safety information**  
   4.1  Backup copies  
   4.2  Fatal errors  

5  **Product overview**  

6  **Accessing SDM600**  
   6.1  Secure Connections  
   6.2  Security certificate warnings  
   6.3  Network Configuration  
   6.3.1  IP Address  
   6.3.2  Virtual LAN (VLAN)  
   6.3.3  Firewall  
   6.3.4  Power Management  
   6.4  Login into SDM600  

7  **Navigation in SDM600**  
   7.1  Navigation reference area  
   7.2  Content Specific Area  
   7.2.1  Dashboard  
   7.2.2  Disturbance Records  
   7.2.3  Security Events  
   7.2.4  Service Data  
   7.2.5  Configuration Changes  
   7.2.6  Device Supervision  
   7.2.7  SDM600 Supervision  
   7.2.8  SDM600 Configuration  
   7.3  Toolbar Area  
   7.4  User Information and Application Settings Area  

8  **SDM600 Dashboard**  

5  

5  

6  

6  

7  

8  

9  

10  

10  

13  

13  

13  

14  

15  

15  

16  

17  

19  

19  

19  

19  

20  

21  

23  

24  

25  

25  

26  

26  

29
1 Copyrights

We reserve the right to make technical changes or modify the contents of this document without prior notice. Regarding purchase orders, the agreed particulars shall prevail. Hitachi ABB Power Grids 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 ABB Power Grids.

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

In no event shall Hitachi ABB Power Grids 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 ABB Power Grids 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 ABB Power Grids, 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.

Third Party Copyright Notices

List of 3rd Party Copyrights notices are documented in “OS Licenses Overview” file in the installation directory. Additional details could be found in the “OS License” folder under the installation directory.

2 Version Information

This User Manual is valid for: SDM600 1.2 FP2 HF8 and newer

Released November 2021
3 Introductions

3.1 Scope of the Document

This document is the user manual for the System Data Manager (SDM600) product. It provides information on SDM600, particularly on the available features and on how to engineer the system.

![Note icon]

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

NOTE

3.2 Use of symbols

This publication 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**

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

**CAUTION**

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.

**NOTE**

Information icon alerts the reader to relevant factors and conditions.

**TIP**

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, 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.
3.3 Abbreviations and Definitions

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DR</td>
<td>Disturbance Record</td>
</tr>
<tr>
<td>FQDN</td>
<td>Fully Qualified Domain Name</td>
</tr>
<tr>
<td>GB</td>
<td>Gigabyte</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Hypertext Transfer Protocol Secure</td>
</tr>
<tr>
<td>IEC</td>
<td>International Electrotechnical Commission</td>
</tr>
<tr>
<td>IED</td>
<td>Intelligent Electronic Device</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>kV</td>
<td>kilo Volt</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>LN</td>
<td>Logical Node</td>
</tr>
<tr>
<td>PC</td>
<td>Personal Computer</td>
</tr>
<tr>
<td>RAM</td>
<td>Random Access Memory</td>
</tr>
<tr>
<td>RDRE</td>
<td>Logical node name for Disturbance Record</td>
</tr>
<tr>
<td>SA</td>
<td>Substation Automation</td>
</tr>
<tr>
<td>SCD</td>
<td>Substation Configuration Description</td>
</tr>
<tr>
<td>SDM</td>
<td>System Data Manager</td>
</tr>
<tr>
<td>SQL</td>
<td>Structured Query Language</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Socket Layer</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>UI</td>
<td>User Interface</td>
</tr>
<tr>
<td>UNC</td>
<td>Universal Naming Convention</td>
</tr>
<tr>
<td>USB</td>
<td>Universal Serial Bus</td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual Local Area Network</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>VSA</td>
<td>Vendor Specific Attribute</td>
</tr>
<tr>
<td>XML</td>
<td>Extended Markup Language</td>
</tr>
</tbody>
</table>

3.4 Related documents

- 1MRS757749 - SDM600 Installation Guide
- 1MRS757880 - SDM600 Release Notes
4 Safety information

This section has information on the prevention of hazards and taking backups from the system.

4.1 Backup copies

Taking backup copies

We recommend creating a backup before making any changes, especially ones that might have side effects.

It is therefore recommended:

- to create a backup regularly, in order to minimize the potential amount of data lost.
- to store the backups on a different system, in order to minimize the chance of the backup being destroyed as well.

An important part of security is ensuring that complete and regular backups are kept enabling recovery after disaster. Backup files must be protected as they contain sensitive information that can be exploited by an attacker in similar ways as a live database. Because of this it is strongly recommended to protect backup files with appropriate access control.

Detailed information on how to make a backup is available in the user manual.

4.2 Fatal errors

A fatal error is an error that causes a breakdown or a locked situation in the SDM600 program execution.

Handling

In case of a fatal error:

1. Write down the possible error messages
2. Copy the folder Log 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

Avoid shutting down the PC by powering off the PC directly as this may cause damage on the base system file.

CAUTION

Report the program break-down together with the possible SDM600 error messages and the log files under the log directory to your SDM600 representative.
5 Product overview

SDM600 – see the unseen from a new perspective

The primary business of any utility is delivering services to their customers, and they have the tools and techniques to ensure contiguous delivery. But as those tools multiply the incoming data becomes unmanageable, while the complexity of tracking IED software versions and user accounts risks undermining the advantages that system automation brings. To manage the management network requires a new toolset, to see the unseen, protect the unguarded, and master the unwieldy.

SDM600 sees the unseen: with full support for IEC61850 interfaces, and the capability to talk to legacy equipment, it interrogates IEDs around the network. From those IEDs it gathers disturbance recorder files and collates them for centralized storage. SDM600 then analyzes the incoming data and produces concise reports so utilities can see patterns of activity, or identify correlations in performance, by seeing what had previously been hidden.

The centralized storage of disturbance files enables them to be extracted with ease, enabling the data to be shared with analysis software or aggregated with data from the rest of the grid to create a holistic view of operations.

SDM600 protects the unguarded, by creating a single point of management for user accounts and access control, and logging security events affecting the network. Cyber security is a vital component in modern networks, but access policies fragmented across network devices risk exposing critical vulnerabilities. The dispersed nature of automation networks has complicated tasks such as revoking staff credentials, or removing default passwords, but SDM600 brings back the simplicity by providing a single place in which accounts can be managed and access controlled: a gatekeeper to the automation network.

SDM600 masters the unwieldy, checking up on IEDs to ensure they are running the latest software, have the latest patches installed, and are properly configured for the tasks assigned to them. The complexity of modern software demands it become a changeable thing, constantly updated in response to new security concerns, or functionality fixes, or to add new features. IEDs are no exception to this and keeping track of software versions can become significantly onerous without a management system such as SDM600 to take care of it.

Information is only as good as the way in which it’s displayed, and with a web-based interface SDM600 creates a unique visualization of the automation network and the IEDs of which it is comprised. Security events, disturbance reports, and IED software versions are all collated into a single dashboard from which the user can share the insight of the SDM600 and see the unseen from a different perspective.
6 Accessing SDM600

SDM600 is a client server-based Rich Internet Application solution. To use SDM600, a web browser is needed.

A Rich Internet application (RIA) is a web application that has many of the characteristics of desktop application software. For more information on RIA, see http://en.wikipedia.org/wiki/Rich_Internet_application.

NOTE

6.1 Secure Connections

SDM600 can only be accessed by using an HTTPS connection (secure connection). A secure connection means a connection that is established by a combination of two protocols, namely HTTP and TLS. TLS are cryptographic protocols that provide security in network connections.

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.

6.2 Security certificate warnings

If a browser is not able to verify the certificate that is used to establish the secure connection to the SDM600 server, a warning is shown. This is because SDM600 comes with a self-signed certificate. To obtain a certificate that is signed by a well-known certification authority, such as VeriSign or Thawte, each organization that installs SDM600 must order this directly from the respected certification authority website as organization-specific information is needed to obtain the certificate. If there is a well-known certification authority signed TLS certificate available, install it on the server where SDM600 is installed. For more information, please consult your IT administrator.

In addition, if it is not possible to obtain a certificate from a proper or well-known certification authority, it is also possible to configure the PC that accesses SDM600 to trust SDM600. This can be done by installing ABB SDM600 certificates from User Application and Settings, Download tab.

Security certificate warning in Microsoft Internet Explorer
When this warning is shown, click **Continue to this website (not recommended)**. The SDM600 login page opens.

Protected Mode in Microsoft Internet Explorer

Microsoft Internet Explorer comes with an additional feature called Protected Mode. When this feature is activated, Microsoft Internet Explorer makes it more difficult to install malicious software on your computer. However, this also blocks several features that are introduced in SDM600. To overcome this and still protect your computer from malicious software, there are two ways: disabling the Protected Mode feature for the local intranet only or running the browser as administrator.

To disable the Protected Mode feature only for the local intranet, do the following:

1. Select **Control Panel > Internet Options**, and open the **Security** tab.
2. Click **Local Intranet**, then uncheck the **Enable Protected Mode** option.

3. To customize the list of your intranet site, in the same window, click **Sites**. A new window opens. Click **Advanced**.
4. In the following window, add the address of SDM600, then click **Add**. After that, click **Close**. To close all the remaining windows, click **OK** in each window.

5. Restart the Microsoft Internet Explorer browser.

**WARNING**

It is not recommended to disable the Protected Mode feature for Internet Explorer. This certainly increases the possibility that your PC will be infected by malicious software. If your SDM600 is designed to access through a wide internet connection, it is recommended to set up a VPN connection. Setting up a VPN connection is not in the scope of this guide.


To start your browser as an administrator, do the following:

1. Select **Microsoft Windows Start menu > Internet Explorer**.
2. Press the right button of the mouse, then select **Run as administrator**.
6.3 Network Configuration

SDM600 can be accessed remotely via a network or locally from the installed computer. To access SDM600 over the network, some specific network settings are required. Particularly when the computer that is used to access SDM600 is in the same subnet as the SDM600 server and firewall rules allow access to the SDM600 server. Nonetheless, the following settings are provided as a general guideline.

6.3.1 IP Address

SDM600 is a server product that comes with different features. It is important to assign a static IP address to the PC where SDM600 is installed.

The static IP address is used for accessing SDM600 as well as for user authentication, centralized activity logging and another core SDM600 functionality. Failing to assign a static IP address may result in a non-operational SDM600.

**WARNING**

Furthermore, as SDM600 is accessed by multiple systems, applications, and devices in the substation automation system, it is important to ensure that SDM600 can be reached from the systems, applications, and devices that need the SDM600 service. In the same way, it is important to ensure that SDM600 can reach the IEDs in the substation for disturbance records collecting purpose.

**NOTE**

For information on your system network design and on how to integrate SDM600 into the network infrastructure, please consult with your network administrator.

![Figure 5.5: An example of a network setting for the SDM600 system](image)

For information on your system network design and on how to integrate SDM600 into the network infrastructure, please consult with your network administrator.

**NOTE**

The SDM600 server in a substation should be in the same network as the IEDs in order to be able to connect them.

6.3.2 Virtual LAN (VLAN)

If the automation network is configured or segmented using Virtual LAN (VLAN), it needs to be ensured that the VLAN traffic that comes and goes out of SDM600 is properly configured.

**NOTE**

It is recommended that the respective network administrator is always involved while deploying SDM600 in your organization.
### 6.3.3 Firewall

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

<table>
<thead>
<tr>
<th>Port No.</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP echo request and ICMP echo reply</td>
<td>Ping to check if connection to the device is possible</td>
</tr>
<tr>
<td>389 TCP</td>
<td>Port for SDM600 Centralized Account Management (LDAP Authentication)</td>
</tr>
<tr>
<td>443 TCP</td>
<td>Port for HTTPS web access</td>
</tr>
<tr>
<td>636 TCP</td>
<td>Port for SDM600 Centralized Account Management secure connection (LDAP Authentication)</td>
</tr>
<tr>
<td>1433 TCP</td>
<td>Port for SQL Server</td>
</tr>
<tr>
<td>1468 TCP</td>
<td>Port for SDM600 Centralized Activity Logging Service (Syslog over TCP)</td>
</tr>
<tr>
<td>1812 UDP and TCP</td>
<td>Port for SDM600 Centralized Account Management Service (RADIUS communication)</td>
</tr>
<tr>
<td>58900 TCP</td>
<td>Port for SQL Server</td>
</tr>
<tr>
<td>59100 - 59199 TCP</td>
<td>SDM600 internal service (Parent-Child Initialization)</td>
</tr>
<tr>
<td>59200 TCP</td>
<td>SDM600 internal service (Centralized Activity Logging Service)</td>
</tr>
<tr>
<td>59960 TCP</td>
<td>SDM600 internal service (needed for Parent-Child synchronization, only required on child system)</td>
</tr>
<tr>
<td>59990 - 59999 TCP</td>
<td>SDM600 internal service (Parent-Child, Hot-Standby Initialization)</td>
</tr>
<tr>
<td>60000 - 60010 TCP</td>
<td>SDM600 internal service (Hot-Standby)</td>
</tr>
<tr>
<td>61743 TCP</td>
<td>SDM600 internal service - open only during migration from previous versions of SDM600</td>
</tr>
<tr>
<td>514 UDP</td>
<td>Port for SDM600 Centralized Activity Logging Service (Syslog over UDP)</td>
</tr>
<tr>
<td>990 TCP and 989 TCP</td>
<td>Port used only if FTPS file transfer option is used for Disturbance Records retrieval.</td>
</tr>
<tr>
<td>22 TCP</td>
<td>Port used only if SFTP file transfer option is used for Disturbance Records retrieval.</td>
</tr>
</tbody>
</table>

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

It is not recommended to disable any firewall without first informing the network administrator in your organization. The firewall should only be disabled during testing sessions.

**WARNING**

In general, while setting up the SDM600 Parent-Child relationship and if you have your operating system firewall enabled, it is important that all the listed ports are excluded from the firewall rules.

**CAUTION**
6.3.4 Power Management

To ensure that the operation of SDM600 is not interrupted by the power optimization behavior, the power management function can be modified so that the power profile is set to high performance.

While setting the computer power profile to high performance, it is important to set the computer to never go to sleep mode. Or you can also set the monitor to never turn off.

![Change settings for the plan: High performance](Image)

Figure 5.6: Power management settings in Windows 7 x64 Operating System

6.4 Login into SDM600

SDM600 provides a login page to get into SDM600. When a user loads the SDM600 on a browser or after logout from SDM600, a login page is shown. To login into SDM600, a user must enter a valid credentials (username and password). After entering the valid credentials, the user will be offered to select a single role (if the user is assigned to more than one role) which the user wants to use to login into the SDM600. Best practices in cyber security recommend the principle of least privilege. Therefore, if a user has more than one role, it is important to remember that the user should login only with role that fits to the tasks that are going to be done at that login session. When the user has only one role assigned, SDM600 will immediately log the user into SDM600 if the entered credentials are valid. Information regarding user management can be found in the Section about Centralized Account Management.
7 Navigation in SDM600

The SDM600 user interface (UI) is based on the Microsoft Silverlight technology. It is a web-based UI and designed to be easily used and navigated.

The SDM600 content is automatically updated when there is a new update available. Therefore, unlike a normal website where the content can be refreshed by pressing the F5 key, in SDM600, pressing the F5 key reloads the overall SDM600 application and subsequently a user will be reauthenticated.

The SDM600 UI is divided into four main areas:

- Navigation reference area (indicated with an orange box in the following figure)
- Content specific area (indicated with a red box in the following figure)
- User information and application settings area (indicated with a green box in the following figure)
- Toolbar area (indicated with a blue box in the following figure)
7.1 Navigation reference area

The left panel of the SDM600 UI is called the navigation reference area. This area helps the user to explore the system that is monitored or managed by SDM600. A selected entity in this panel automatically becomes a filter for the information shown in the right panel of the UI.

There are two tabs in the navigation reference area:

- The Structure tab shows the structure of the configured substation and the connected SDM600 devices.
- The Devices tab shows the available devices that are directly connected to the installed SDM600.
Figure 6.2: SDM600 Navigation Reference Area - Structure tab

Figure 6.3: SDM600 Navigation Reference Area - Devices tab
7.2 Content Specific Area

The right panel in the SDM600 UI is called the content Specific area.

7.2.1 Dashboard

The SDM600 Dashboard tab presents graphical information of the system under observation. The system can be a substation, a group of IEDs or substations, or another SDM600 device. The Dashboard tab contains three sub-tabs: the two-dimensional points-graph tab, a bar chart graph to show the statistics of the collected disturbance record entries, and a spider-web graph to show the statistics of the collected cyber security events in the system.

7.2.2 Disturbance Records

The Disturbance Records tab shows the collected disturbance records and presents them in a grid view.
7.2.3 Security Events

The Security Events tab shows the collected security events (in Syslog (RFC 5424) format) that are received by SDM600 from the connected systems, applications, or devices.
7.2.4 Service Data

The Service Data tab shows information useful for managing installed base. Please notice the following:

- **Device name** - shows name of the device. If native or web-based configuration tool is set, then Device name is a link, which is opening configured tool.

- **Details** - open another window with protocol specific details. For instance, for Windows devices, on top of several properties the window shows the installed applications.

- **Patches** - open another window with list of installed patches. This option is available for Windows Client only.

- **Configuration** - if configuration file for the device is stored in SDM600, then link to download of configuration to the disk is activated.

- **Firmware** - this checkbox is checked if there is firmware stored in SDM600 for the device.
By clicking the Export to Excel button in the tool bar, it is possible to export the content of the Service Data to Excel.

**NOTE**

Note the automatic export option from the Service Data Tab is no longer available via the Web Interface. Instead, it is now available on Application Administration Tool. Please refer to SDM600 Application Administration Tool section to enable the automatic export.
### 7.2.5 Configuration Changes

The Configuration Changes tab shows the collected changes in the device's configuration and presents them in a grid view.

**Figure 6.9: SDM600 Application Context Area – Security Events Tab**

<table>
<thead>
<tr>
<th>Event Date (Local time)</th>
<th>Device</th>
<th>Property</th>
<th>Old value</th>
<th>New value</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>6/9/2020 11:25:33 AM</td>
<td>AADIDQHF9F1</td>
<td>IPM (LUW)</td>
<td>14C 4650-7-4-2000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6/9/2020 11:25:33 AM</td>
<td>AADIDQHF9F1</td>
<td>model (LUW)</td>
<td>[AADIDQHF9F0AABB01] REB600Sry</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6/9/2020 11:25:33 AM</td>
<td>AADIDQHF9F1</td>
<td>vendor (LUW)</td>
<td>[AADIDQHF9F0AABB01] ABB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6/9/2020 11:25:33 AM</td>
<td>AADIDQHF9F1</td>
<td>(LUW)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6/9/2020 11:25:33 AM</td>
<td>AADIDQHF9F1</td>
<td>config (LUW)</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6/9/2020 11:25:33 AM</td>
<td>AADIDQHF9F1</td>
<td>swRev (LUW)</td>
<td>[AADIDQHF9F0AABB01] 7.50</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6/9/2020 11:25:33 AM</td>
<td>AADIDQHF9F1</td>
<td>version (LUW)</td>
<td>ABB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6/9/2020 11:25:33 AM</td>
<td>AADIDQHF9F1</td>
<td>swRev (LUW)</td>
<td>7.50</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
7.2.6 Device Supervision

The Device Supervision Tab shows a list of the devices that are managed by SDM600, for example, IEDs, computers, network devices and connected SDM600 devices.

Please notice the following:

- **Name**: the name of the device. If IP address or configuration tool of the device is set, (refer to the Setting Up the IEDs/Devices chapter) then Name is a link which is opening device's web page or configured tool.

- **Connection status**: the reachability status of the device (by means of the last access)
  - *Unknown*: IP address of the device is not configured; status has not been checked or device is unreachable for more than 30 minutes.
  - *Red*: the device is unreachable or sends no feedback.
  - *Yellow*: the device is reachable, but there are problems with communication.
  - *Green*: connection is working correctly
  - *No license*: Connection to the device is working, Disturbance records retrieval is configured, but SDM600 is not licensed to retrieve DRs from this device.

- **Time of last status change**: the time of the last status change.

- **Additional description**: a warning about a problem detected in connection status. The following warnings are available: Device address is incorrect, NMMS library can't connect with: <IP address>, Unable to Ping device, Invalid DR Path and Device is synchronizing.

*Device is synchronizing* means that SDM600 sent request to the device and still waiting for response or file transfer.

- **NERC-CIP Rating**: Possible values are: Not Applicable, Low Impact, Medium Impact, High Impact

![SDM600 Device Supervision Tab](image-url)
7.2.7 SDM600 Supervision

The SDM600 Supervision tab shows information and status of the SDM600. Tab is divided into five sections:

- **General** - shows general status of the SDM600, version number and all IP addresses recognized by SDM600.
- **Services** - shows status of SDM600 services.
- **Database** - shows path to Database folder and size of SDM600 databases.
  
  **WARNING**
  
  Microsoft SQL Express has limitation to 10Gb per database file. When your database size is reaching this limit, consider upgrading database engine to Microsoft SQL Server Standard.

- **License** - shows licensing information and number of used licenses vs. all licenses available for feature.

![SDM600 Supervision Tab](image)

Figure 6.11: SDM600 Supervision Tab

7.2.8 SDM600 Configuration

The Configuration tab contains several subtabs that are needed to configure SDM600:

- General Settings tab
- Tabs for configuring SDM600: Structure, Hierarchy, Device Settings
- Tabs for user management in SDM600: Centralized Account Management, User Management, SDM600 User Rights
- E-mail Notification tab
- Application-related configuration tabs: Disturbance Record Retrieval, Security Events, Event Mapping and File management
- SDM600 maintenance tab: Backup & Restore tab
7.2.8.1 Backup and Restore

The Backup and Restore functionality is available in the “Application Administration Tool” on the SDM600 Server. You can find additional information on how to use this feature.

At the top of the right panel of SDM600, there is a toolbar that provides several common functionalities, such as exporting a grid table into the Microsoft Excel format or saving the updated configuration. There are also some context-specific functionalities, for example, short report generation is only available when the Disturbance Records tab is highlighted.

In the right end of the toolbar, the number of entries in the highlighted tab is shown.

7.4 User Information and Application Settings Area

In the top right corner of the SDM600 UI, the following information is shown:

- **Reports**: Opens a window with reports generated on the server. Reports are stored in the servers for 1 hour.
• **Overall state:** the overall operational state of SDM600. State dot can be red or green. Whenever there is an issue with a core component of SDM600, this indicator turns red.

There are two indicator types:

- single dot for standalone configuration
- double dot for hot-standby configuration

When SDM600 is connected in hot-standby relation, then left dot is showing status of local system and right dot is showing status of remote partner.

**NOTE**

- **License:** the type of license used by SDM600. It can be a demo license or, if a proper license is used, the license information is shown as *Valid*.
- **User name:** the username that is used to log in to SDM600.
- **Current user role:** the role that is used to log in to SDM600.
- **Settings:** a link to the settings where users can modify their user information, modify application settings, or download some required software.
- **Logout:** this will log the current user out of SDM600.
- **Help:** a link to the help function and to *About SDM600*.

When clicking the help button, two options are shown:

- **Help option:** opens the SDM600 User Manual

  When the Help option is clicked, the SDM600 User Manual is opened in a new pop-up window. In some browsers, the pop-up blocker feature is enabled by default which causes the user manual window not to open. To open the user manual, first disable the pop-up blocker for your browser.

**NOTE**

The SDM600 User Manual can also be found under the *UserManuals* folder of the SDM600 installation folder, by default, this folder is under `C:\Program Files (x86)\ABB\SDM600\UserManuals`.

- **About option:** opens an SDM600 About box
Figure 6.14: SDM600 About box
8 SDM600 Dashboard

The SDM600 Dashboard has two parts:

- SDM600 Overall Status Dashboard
- SDM600 Application-Specific Dashboard

SDM600 Overall Status

The SDM600 Dashboard UI is a two-dimensional plot area. It shows three types of events from the system under observation, based on the entity that is selected on the SDM600 Navigation Reference Area. The event types are:

- Disturbance record events - represented by blue dots
- Device configuration change events - represented by green dots
- Security events - represented by orange dots

The X axis of the dashboard represents the time of an event and the Y axis represents the location where this event happens.

Figure 7.1: SDM600 Dashboard

The dashboard UI can show a wide range of data. It has a Zoom bar Time Navigator for navigating the dashboard. To zoom into a specific date range, click the Zoom bar control and move the mouse to the intended date limit, then release the mouse. Do this for both ends. To move to another date range, click the Zoom bar Time Navigator, then move and release the mouse.
Each dot in the dashboard can be clicked. When hovering over a point, a tooltip box shows information relevant for that point.

When clicking a disturbance record event (blue dot), a security event (orange dot) or a device configuration change events (green dots), SDM600 automatically navigates to the Disturbance Records tab, Security Events tab or Configuration Changes tab respectively. In addition, the record in focus is highlighted.
When right-clicking a Disturbance record event (blue dot), two context menus are shown:

- **Evaluate**: opens a tool to launch and analyze the disturbance record event
- **Short Report**: generates a short report of the disturbance record event

SDM600 allows to configure how many levels of the structure tree will be visible on the dashboard. Number of tree levels can be defined in the toolbar area in the dashboard.

Option **Rows with data only** is presenting rows from devices where Disturbance Records, Configuration Changes or Security events are stored in SDM600. This option is reducing number of displayed lines.

Option **Paths** is adding full path to the device name.

There is also possibility to filter information presented on the dashboard. By default, Disturbance Records, Configuration Changes and Security Events are selected. For large number of security events generated in the short amount of time there is possibility to aggregate security events entries. When this checkbox is selected then all security events form single day are represented by one dot on the dashboard.

Button with an arrow (indicated by red box on the following figure) is refreshing dashboard on demand.

If there is many information to display on the dashboard, then it's recommended to uncheck "Refresh every 1 minute" option and select aggregate security events.

This will prevent form automatic dashboard refreshing, decrease number of dots to render and increase performance.

**SDM600 Disturbance Record Statistics**

The Disturbance record statistics tab shows a bar chart of the disturbance record events in the entities that have been selected in the Navigation Reference Area.
Figure 7.8: SDM600 DR Specific Dashboard

SDM600 Security Event Statistics

The Security event statistics tab shows a radar chart of the recorded security events in SDM600 based on the selected entities in the Navigation Reference Area. The radar chart has security event categories as its axes. SDM600 provides the following security event categories:

- **Security – accountability**: any events from a user, which ensures unique traceability to that user. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.
- **Security – administration and configuration**: any events that come from administering or configuring cyber security measures in the system
- **Security – potential security violation**: any events that may come from potential security violation actions
- **Security – operation**: any operational events from cyber security measures
- **System – engineering and configuration**: any events that come from engineering and configuration of industrial control systems
- **System – operation**: any events that come from operational of industrial control systems
- **System – maintenance**: any events that come from maintenance activity on industrial control systems
- **System – monitoring**: any events that come from monitoring the operational of industrial control systems
- **Communication**: any events that relate with the establishment, operation, or de-establishment of communication-related functions or devices in industrial control systems
- **Unknown**: any uncategorized or unknown events or any events that cannot be interpreted by the existing interpreter engine.
Figure 7.9: SDM600 Security Event Statistics
9 Configuration of SDM600

9.1 General Settings

General Settings is the first subtab of the Configuration Tab in SDM600.

In General Settings, the following information can be configured:

- Enable automatic logout. It is possible to define that an SDM600 user is logged out after an inactivity of a pre-defined time period.
- Enable verbose logging. When there is a problem with SDM600, the verbose logging feature should be enabled. Enabling verbose logs might take up to 60 seconds. After this time, issue should be reproduced, and logs should be sent to the SDM600 support. By default, verbose logging is disabled.
- Enter SiteID information
- Enable and define logon banner. If this setting is active, text from logon banner content is displayed on the screen before SDM600 login window.
- Enable SDM600 caused Cyber Security events. Every time, when SDM600 is logging to the device to check Service Data, log-in and log-out event is recorded on the device. This option is hiding these events.

NOTE

SDM600 provides operational logging functionalities. Operational error messages and additional information are logged during operation. The log file is stored under the installation folder of SDM600, in other words, <Operating system default drive>:\Program Files (x86)\ABB\SDM600, if the default installation folder is selected. By default, it is located under C:\Program Files (x86)\ABB\SDM600\log.

9.2 Setting Up SDM600

The configuration of SDM600 follows the basic steps as reflected in the subtab sequence in the Configuration Tab.

- The structure of the system under observation
- Hierarchical system configuration
- Device settings

9.2.1 Setting Up the SDM600 Structure

There are three ways to set up the system structure in SDM600:
- Manual configuration
- Import the system configuration file (IEC 61850 SCD file)
- Import system configuration for non IEC61850 devices (CSV file)

This function can be found in the **General Settings > Structure** subtab of the **Configuration** tab.

**Figure 8.2:** Configuration Tab in the SDM600

Remember to save changes after manual structure editing

**Figure 8.3:** Save after manual structure editing

### 9.2.1.1 Manual Structure Configuration

To manually build the structure, do the following:

1. Open the **Go to the Manual Structure Editing** part in the **Configuration > Topology** subtab.
2. Click **Enter manual structure editing mode.**

When entering the manual structure editing mode, the related parts of the UI are surrounded by a red border.
Navigate to the Navigation Reference Area. Based on the selected entity, it is possible to create different types of sub-entities:

- **Substation Group**: 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**: 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**: 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**: a device in a substation. SDM600 prepares several commonly known IEDs in the default list. This list can be modified by adding or removing IED templates from the IEDTemplates folder of the SDM600 installation folder. To work on an IED template, see Step 4.

- **SDM600 Child**: an instance of SDM600 that this SDM600 is planning to connect to and retrieve necessary data from.

It is possible to rename each element that is added to the tree.

**NOTE**

In order to activate CAM for the IED in PCM600, the IED name in SDM600 must correspond the PCM600 Technical Key.

4. Add an IED or device. SDM600 comes with a pre-defined list of IED templates from multiple vendors. You can select from the list or, for an undefined IED, a custom type can be used.

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

- IED type name (for example, RE.670, RE.615, and so on)
- Manufacturer of the IED (for example, ABB)
- Supported protocols - IEC61850 MMS
- Information whether the IED can have a disturbance record or not
- Information on the directory location of the disturbance record
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`.

The SDM600 user can create a new IED Template for an IED that is not listed in the available list. The format of the XML schema is shown in the following figure. Only the part that is marked in yellow needs to be modified.

![XML schema for IED template](image)

**Figure 8.5: IED Template Format**

To create a new IED template for a specific IED type, do the following:

a. 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.

b. Open the template file in an XML editor.

c. 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="ABB"`. The strings defined for attributes `Type` and `Manufacturer` must match the strings defined in the SCD files that are 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.

d. Fill in other attribute information such as ShownType, Description, ShownManufacturer, CommProtocol, HasDR, and the DRPath. Filling in this information means more information regarding the IED type is provided at the UI level.

The HasDR attribute indicates that the IED in question can have a DR file. The DRPath attribute indicates the path to the DR files.

e. To see the newly created IED template, log out from SDM600 and log in again.

5. After the type of an IED or device is selected, a new node is added under the selected parent node.

6. If necessary, to change the name of an IED or device, double-click the name.
7. Repeat steps 4 – 6 to form a meaningful structure.

8. When the topology design activity is done, click **Save**.


### 9.2.1.2 Automatic Structure Creation

To automatically construct the SDM600 structure, from the SCL file, do the following:

1. In the **Configuration > Structure** tab, open the **Load Structure from IEC 61850 SCL file** part of the tab.

2. Click **Import**.

3. Load the SCL file by using the available dialog. First select an SCL file to be loaded, then click **Open** to load the SCL file to the SDM600 system.

   The state of the process can be seen in the import progress box.

4. Next, the SCL file is uploaded and processed by SDM600.

   When the loading is finished, the new substation is added to the tree. The user is informed based on the status message at the top of the progress bar.

   ![Image](image_url)

   **Figure 8.8: Configuration Tab - Topology Subtab - IEC61850 SCL file is loaded successfully**

   After the substation topology is imported from the IEC61850 SCL file, the tree view that represents the substation topology is automatically generated. To make the tree view easier to read, it is possible to edit the text that correlates to different parts of the tree. For example, instead of having “AA2” as a substation name, a user can edit the name and change it to “Substation Baden”. To edit texts in the tree, do the following:

   1. Click **Enter Manual structure editing mode**.

   ![Image](image_url)

   **Figure 8.7: SDM600 Manual Configuration - Edit IED's Name**
2. Navigate to the part of the tree where a text needs to be changed.
3. Double-click the node and enter the new text.

![Figure 8.9: How to Edit Text on the Treeview](image)

**NOTE**

Every IEC61850 SCD file that is imported by SDM600 is treated as a new substation. This also applies to an IEC61850 SCD file that has been imported before.

However, if IP address of imported device is already present in the SDM600 then this field will be empty after import. It's possible to change IP address of each device in **Configuration > General Settings > Device Settings.**

Another way to add devices to SDM600 structure is to upload CSV file. Template of the CSV file can be downloaded from **User and application settings > Downloads.**

### 9.2.2 Setting Up SDM600 Hierarchical Function

SDM600 offers a hierarchical functionality to integrate with other instances of SDM600 that are installed on another level of the organizational structure. For example, a standalone SDM600 that is installed at the network control center level can be integrated with one or multiple standalone SDM600 that are installed at the substation level. In this setup, the standalone SDM600 at the network control center level is further called as **SDM600 parent,** where the standalone SDM600 at the substation level is then called **SDM600 child.** With this integration, the SDM600 at the network control center level aggregates information from multiple substations and presents the information accordingly. The following figure shows a possible SDM600 hierarchical deployment scenario with an SDM600 parent at the network control center connected to the SDM600 children in the Substations A & B.
Figure 8.10: An Example of SDM600 Hierarchical Structure Deployment

To collect data from an SDM600 child device, the SDM600 parent requires the license for hierarchy mode. Without this license, it is not possible to add the SDM600 child.

**NOTE**

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

**NOTE**

After creation of parent - child relation, it is very important to reactivate again the Central Account Management. Consequently, all devices that need authentication to SDM600 needs to be re-configured.

**WARNING**

Before setting up the SDM600 hierarchy between an SDM600 parent and an SDM600 child, it is important that you ensure that the SDM600 servers have a dedicated IP address.

**CAUTION**

Make sure that "Default Interface" in Configuration > Centralized Account Mgmt. is selected for the interface used for communication between parent and child.
It is important to ensure that the time between an SDM600 parent and an SDM600 child is synchronized. For instructions, see the Windows Operating System user manual.

**CAUTION**

To create a parent/child relationship between this SDM600 (parent) and a standalone SDM600 (will be the new child to this parent), do the following:

1. To add an SDM600 hierarchy, it is important to execute the following steps on the SDM600 child in the presented order:
   a. Navigate to **Configuration Tab > General Settings > Hierarchy** on the SDM600 child.
   b. Focus on the **Initial communication encryption** part.
   c. Enter a shared secret that is used to secure the communication between the SDM600 child and the SDM600 parent.

**NOTE**

To enable secure communication between the SDM600 parent and child for the first time, the shared secret must be provided to both units. The shared secret is used to encrypt and decrypt the initial communication between the SDM600 parent and child. After the configuration is set up, the parent and child communicate by using transport layer security.

   d. Set the length the validity period of the temporary secure communication channel between the SDM600 child and parent. This secure channel is used to transport the SDM600 child configuration package from the SDM600 parent.

**CAUTION**

It is not recommended to permanently open this temporary secure communication channel (by selecting Always on Timeline Duration). In general, it is a cyber security principle to close any unnecessary communication channels. An exception can be accepted if the connection between the SDM600 child and parent is established by using a time-limited Virtual Private Network.

   e. Click **Initialize Communication**.

**Figure 8.11: Interface configuration for hierarchical relation**

**Figure 8.12: SDM600 Hierarchy Setup - Enter Initial Communication Encryption Details**
2. As of this step on, all actions are conducted **on the SDM600 parent.** Start by navigating to **Configuration > General Settings > Structure** on SDM600 parent and enable Manual Configuration by clicking on the button **Enter Manual structure editing mode.**

3. Navigate to the **Navigation Reference Area** and click the root SDM600 level.

4. Right-click with the mouse, and from the context menu, select **Add new Child SDM600 System.**

5. In the dialog box, fill in the relevant information, then click **Add.** Click **Save** to commit the changes.

6. When an SDM600 child is successfully added to the structure, it is shown in the tree structure and in the **Configuration Tab > Hierarchy** subtab.

**NOTE**

To integrate a child SDM600 successfully, the following information needs to be provided:

- The IP address of the child SDM600
- The port number if the child SDM600 is not using a default port number
- The user credentials of the child SDM600 that has administrator rights. If there is no access to the child SDM600, your user administrator needs to create a temporary administrator user for this integration.
- The shared secret. The shared secret must be the same as the one that is entered on the child SDM600.
NOTE

If connected child is working in Hot Standby relation, then IP address of the child's partner system (hot or standby) is presented in Partner System IP address column.

7. Log out from parent, after establishing parent child relation.

8. To add another SDM600 child, repeat steps 1-7.

If the integration of an SDM600 child into the SDM600 hierarchy fails, revert the SDM600 child to a standalone SDM600 before another integration attempt.

After establishing a hierarchy relationship between the SDM600 parent and child, the following behavior is expected on 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 accounts previously created on the SDM600 child are 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 children. In addition to that all centralized account management certificates created on child must be regenerated and uploaded to devices.

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 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 fails, 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 to SDM600 parent's centralized account management. Therefore, you 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's strongly recommended to wait about 5 minutes before logging in to SDM600 after hierarchy relation is established.

**WARNING**

If a user would like to cancel the hierarchical (parent - child) relationship between one SDM600 and another SDM600 completely, the user should first remove the SDM600 Child entry in the SDM600 Parent unit. This can be done by following the steps below:

1. Navigate to Configuration > General Settings > Structure, and enable Manual Configuration by clicking on the button Enter Manual structure editing mode.
2. Navigate to the Navigation Reference Area and click the SDM600 Child unit that is to be deleted.
3. Right-click with the mouse, and from the context menu, select Delete.
4. When it is done, remember to navigate out from the manual structure editing mode.
5. Click Save to commit the changes.

Secondly, SDM600 provides a reverse function to set the SDM600 Child status to become a standalone SDM600. This function can be used only when disconnecting on parent is done (see above) or parent system has been dismissed.

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.

To revert the state of an SDM600, navigate to Configuration > Centralized Account Management. Click Revert to standalone configuration button. Enter the SDM600 administrator username and password. After this, restart the PC.

**WARNING**

In order to have a clean termination between SDM600 Child unit and SDM600 Parent unit (when the disconnection was initiated on SDM600 Child), the steps on SDM600 Child unit and SDM600 Parent unit must be executed completely.

**WARNING**

The reverse function 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.

When configuring Hierarchical function in a Domain joined environment, please check the following paragraph 14.6

### 9.2.3 Setting Up the IEDs/Devices

In general, all the IED or device settings are available in the loaded SCD files. However, when some IED or device information needs to be edited, users can navigate to the Configuration tab > General Settings > Device settings subtab. In this subtab, it is possible to edit the following information:

- **Name**: the name of the IED or device
- **Description/ Customized name**: a description of the IED or device
- **Comment**: a placeholder for comments on a device
- **Type**: the type of the IED or device
- **IP Address**: the IP address that the IED or device is bound to
- **UTC offset (DR)**: the time zone setting, configured on the device, for Disturbance Records and Service data.
- **UTC offset (SysLog)**: the time zone setting, configured on the device, for Security Events (Syslog messages).
- **NERC-CIP Rating**: shows importance of the device in the substation.
- **Property protocol**: allows to configure protocol used for reading device’s configuration changes and service data. Possible values are:
  - IEC 61850-8 allows to read service data from devices using IEC 61850-8 protocol
  - SNMPv1 allows to read service data from devices using SNMPv1 protocol
  - SNMPv2 allows to read service data from devices using SNMPv2 protocol
  - SNMPv3 allows to read service data from devices using SNMPv3 protocol
  - HTTP Client allows SDM600 read client information based on http request header
  - Windows Client enables SDM600 to retrieve/receive information from a Microsoft Windows PC using the Microsoft Windows Agent

  **NOTE**

  The Windows Agent is an application for Microsoft Windows PCs.
  The Windows agent collects information from the target Microsoft Windows PC and sends it to SDM600. The information collected from the Microsoft Windows PC includes:
  - Windows Version
  - Hardware Information
  - Antivirus
  - Installed Windows updates

  Installed Application (application name, publisher and version)

  The Windows agent installation package can be downloaded from the Downloads tab in the SDM600 Options dialog:

  ![Downloads](image)

  The Windows agent must be installed on the target Windows PC

  - RTU Web API allows to read ABB RTU rel. 12 or newer
  - None

- **Service Data Protocol Configuration**: allows to set up protocol specific properties like login name, password or authentication method. This option appears only if chosen protocol requires additional properties and after saving changes.
- **Custom properties**: this option is available only for SNMP v1, v2 and v3 protocols. After clicking on Configure link the new window is opened.

  There are two tabs on newly opened window:

  - **Custom Properties for Device**: allows to map SNMP device properties with SDM600 device properties.
  - **System Properties for Protocol**: a list of predefined system properties.
Figure 8.16: SNMP Custom Properties for Device

- **Configuration Tool**: allows to set up configuration tool for the device. This value can be set to local path or http/https address. As default SDM600 is using https connection to the device IP address. After clicking on **Configure tool**, new window is opened.

![Configuration tool window](image)

In **Configuration tool** field is possible to enter http or https address or provide path to tool installed on the drive.

**CAUTION**

In order to be able to run configuration tool form local path, tool must be installed on the server and on all SDM600 clients in the same path on corresponding drives.

**CAUTION**

If configuration tool link will open Web based configuration tool, full URL must be provided (starting with http:// or https://)

**CAUTION**

- **Properties**: allows to manually overwrite service data information gathered form the device.
- **Contains DR Function**: to indicate whether the IED or device has the disturbance record functionality.
- **Manually Created**: indicates that device has been configured form structure import or manually
- **Poll cycle(sec)**: Defines minimum time when SDM600 can connect to the device in order to poll data.
To edit the information, double-click the cell where the information to be changed is. The changes take effect once they are saved.

The information mentioned in this section should be edited with care. Misconfiguration on the IED information properties may cause SDM600 to lose connectivity to the IEDs.

**WARNING**

IED / device information that is edited in this subtab is stored only in SDM600. Furthermore, IEC 61850 related information will be overwritten with the latest value from the device when SDM600 is connected to the device.

**NOTE**

### 9.2.4 Setting Up SDM600 Hot Standby Function

SDM600 offers a hot standby functionality to increase the availability of the overall SDM600.

A hot standby is a failover mechanism to provide maximum reliability with outstanding convenience at the same time in SDM600 system. The hot unit is the active unit and in the normal operation is considered as a working system. If any of the key component in the hot unit fails, the standby unit will immediately take over the operation.

In SDM600, the hot standby function enhances overall system functionality by providing the following attributes:

- Fully automated synchronization of all relevant data between hot and standby unit
- Integrated self-tests for checking system status
- Automatic failover if internal errors is detected
- Easy setup and configuration of the hot standby redundancy functionality
After configuring of hot standby functionality, all data from hot unit will be mirrored to standby unit. It means that all existing data on standby unit will be replaced by data from hot unit.

**NOTE**

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

To setup the hot standby function between two SDM600, do the following:

1. Configure an SDM600 (B) to become a standby unit. It is important to execute the following steps on the SDM600 standby unit in the presented order:
   a. Navigate to **Configuration Tab > General Settings > Hot Standby**
   b. Click on **Create Hot-Standby System**
   c. Enter a shared secret that is used to secure the communication between the SDM600 hot unit and the SDM600 standby unit

   **NOTE**
   To enable secure communication between the SDM600 hot unit and standby unit for the first time, the shared secret must be provided to both units. The shared secret is used to encrypt and decrypt the initial communication between the SDM600 hot and standby units. After the configuration is set up, the hot and standby units communicate by using transport layer security.

   d. Set the validity period of the temporary secure communication channel between the SDM600 hot unit (A) and standby unit (B). This secure channel is used to transport the SDM600 standby unit configuration package from the SDM600 hot unit.

   **CAUTION**
   It is not recommended to permanently open this temporary secure communication channel (by selecting Always on Timeline Duration). In general, it is a cyber security principle to close any unnecessary communication channels. An exception can be accepted if the connection between the SDM600 standby unit and hot unit is established by using a time-limited Virtual Private Network.

   e. Click **Initialize**.
2. On the SDM600 unit that is designated to become a hot unit (A), follow the next steps in the presented order:
   a. Navigate to **Configuration Tab > General Settings > Hot Standby**
   b. Click on **Create Hot-Standby System**. A small dialog window will be opened
   c. Select this SDM600 unit will be initially HOT
   d. Enter the shared secret that is also entered at the SDM600 standby unit
   e. Enter the IP address of the SDM600 standby unit
   f. Enter the port number of the SDM600 standby unit
   g. Click on **Initialize** to start the hot standby pairing process

*Figure 8.20: Set SDM600 as a standby unit.*
Figure 8.21: Set SDM600 as a hot unit.

Depending of the size of the database files, replication may take some time. Unless replication is done, Hot Standby is not fully operable. Make sure that the double dot status indicator stops blinking. Dots blinking may be not visible when remote desktop connection to SDM600 client is used.

NOTE

Figure 8.22: Double dot replication status indicator

To activate the Hot Standby feature, the assigned SDM600 peer must be in the same network as the installed SDM600 and time on both machines must be synchronized.

NOTE

In SDM600 Hot Standby function, there is no fix definition in defining that a unit is hot or standby. Initially, the user must define which unit is set to hot and standby.

WARNING

Figure 8.23: Hot and Standby Definition in SDM600 Hot Standby Redundancy functionality

After the definition is set, if both units are shut down, then unit, where first user will log in to SDM600 becomes the hot unit.
When configured in Hot Standby, both the SDM600 devices will be connected to the devices to collect data. In case MMS is used as communication protocol, two MMS Client Slots will be used.

**WARNING**

### 9.2.5 Revert to Standalone Systems from Hot Standby

In order to disconnect SDM600 systems from Hot-Standby relation follow below steps

1. Navigate to Configuration Tab > General Settings > Hot Standby
2. Click on **Revert to Standalone SDM600** button.

![Hot-Standby status](image)

**Figure 8.24: Hot Standby disconnection**

After disconnection, restart partner machine (former standby).

**WARNING**

Cancelling the Hot Standby function must be done with extra caution. Disabling this feature means the SDM600 returns to a stand-alone mode and thus, there is no backup when the installed SDM600 is encountering problems. It's recommended to create a backup after successful hot-standby disconnection.

**WARNING**

Notice that all information is deleted from disconnected standby unit.

**CAUTION**

When configuring HSB function in a Domain joined environment, please check the following paragraph 14.6

**WARNING**
9.2.6 Centralized Account Management

The SDM600 provides central user account management functionality with Role Based Access Control (RBAC) Management for devices supporting:

- IEC 62351-8 (Pull Model, Profile A)
- RADIUS (RFC 2865) devices
- Windows PC
- MicroSCADA

This feature enables SDM600 to centrally manage users on different devices, applications and systems. This feature benefits both the users and the administrator of the system that is managed by SDM600. For the administrator, the feature enables access control on every device without being exposed to the complexity of credential management on every device or application in the system. The users must remember only one credential when accessing devices or applications that authenticate the users against the SDM600 server. In addition, for both the administrator and users, changing of credentials can be done directly from SDM600 and the change becomes effective immediately on the connected devices and systems. Furthermore, the SDM600 centralized account management is more than just credential management. A user can be assigned one role or multiple roles. From SDM600, the administrator or an authorized user can assign IEC 62351 pre-defined or custom defined roles to users. RBAC allows a user to select the role that is appropriate for the current task/job, thus preventing the possibility of the user unwittingly making changes or performing unwanted operations. This also ensures that users can only perform the tasks they are authorized to perform. The design of the centralized account management in SDM600 is based on IEC 62351-8 on Role-based access control.

The Centralized Account Management functionality is configured as follows:

1. Activate Centralized Account Management in SDM600.
2. Assign a Role or Roles to each user.
3. Define the user role to rights mapping for SDM600 application.

9.2.6.1 Centralized Account Management Setting

The Centralized Account Management setting provides the following functions to the user:

- Enable network interface for SDM600 Centralized Account Management. This setting instructs SDM600 to set the centralized account management functionality on a defined IP address. SDM600 is automatically trying to distinguish correct network interface for every device. If this is not possible then interface marked as default is taken. In addition to that Default interface shall be selected for the interface used for parent-child or hot-standby connection.

Figure 8.25: SDM600 Configuration - Bind to Other IP Address
• Generate user authentication configuration file for devices. This function allows users to download the user authentication configuration file for a device or application that wants to benefit from using SDM600 centralized account management.

• Manage users accounts. This function allows to add and delete users accounts. Administrator can reset password for selected user.

• Manage replication groups. This function allows to replicate to the device only selected groups of users. This is decreasing replication time and saving device memory.

• Define password policy. This function allows to increase accounts security by enforcing password policies and rules.

• Set users rights. This function allows to define rights for selected roles.

9.2.6.2 Create CAM configuration package for device

In order to create CAM package for application or device to use SDM600 centralized account management, the user needs to:

1. Make sure that SDM600 is bound to correct IP address

   • Download the configuration to replicate complete SDM600 users
   
   !
   
   **NOTE**
   
   This is only possible for applications or devices from ABB.

3. Select device or devices for which CAM configuration will be generated.

4. Click on Add new CAM Configuration button.

   ![](image)

   **Figure 8.26: Add new CAM Configuration button**


   ![](image)

   **Figure 8.27: Add new CAM configuration protocols**

6. Define certificate key length, validity dates and certificate password.
If CAM package is generated for multiple devices in one step, then password for generated certificates will be the same.

CAUTION

Longer certificate key is increasing security, but too long key may impact device performance. Recommended value is 2048 bits.

CAUTION

7. Save newly created CAM package by hitting Save icon.
8. Copy CAM package for selected device or devices.

Figure 8.28: Copy CAM package button

9.2.6.3 Integrating RADIUS devices into SDM600 Centralized Account Management

As a centralized account management unit, SDM600 provides the functionality to integrate RADIUS devices into its account management functionality. This means that devices that use RADIUS authentication can be centrally authenticated to the SDM600 centralized account management.

Configuration of RADIUS device is very similar to configuration of IEC62351 device. To enable this, it is important to register the RADIUS device as a device in SDM600.

To register the devices, do the following:

2. Select device or devices which will use RADIUS for authorization.
3. Click on Add new CAM Configuration button.

Figure 8.29: Add new CAM Configuration button

4. Select RADIUS protocol.
5. Provide shared secret

It is important to specify the shared secret that is a text string that serves as a password between a RADIUS device and the SDM600 centralized account management.

NOTE

RADIUS shared secret is used to protect user passwords and the authentication of the SDM600 centralized account management replies. Therefore, if a user provides a shared secret that is not equal, the overall authentication process from the RADIUS device to the SDM600 centralized account management will not work properly, and vice versa.

WARNING

SDM600 provides the possibility to retain the shared secret when entering the RADIUS client to SDM600.

NOTE

6. Click OK
7. Click Save icon
On a RADIUS device, it is also important to set up the authentication mechanism to point to SDM600. Each RADIUS device has a different way of setting up such authentication mechanism. Please refer to the user manual or installation guideline of the RADIUS device.

Some RADIUS devices may require a Vendor Specific Attribute. However, in the current version of SDM600, SDM600 supports RADIUS devices that assign type of service the user has requested to the Attributes Service-Type. Normally, definition of each Attributes Service-Type can be found in the user manual of the RADIUS device.

CAUTION

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. This means if the RADIUS device supports the Attributes Service-Type for authorization, then the tasks/operations that the user can perform in that device are defined by the role or roles assigned to the user. Each RADIUS device vendor may have a different definition of what does a specific Attribute Service-Type mean in its device. For example, ABB AFS Switch defines Attribute Service-Type [1], Service-Type [6] and Service-Type [7] as Operator, Administrator and Guest respectively.

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

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

<table>
<thead>
<tr>
<th>SDM600 Roles</th>
<th>RADIUS Attribute Service-Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viewer</td>
<td>Service-Type [7]</td>
</tr>
<tr>
<td>Operator</td>
<td>Service-Type [1]</td>
</tr>
<tr>
<td>Engineer</td>
<td>Service-Type [6]</td>
</tr>
<tr>
<td>Installer</td>
<td>Service-Type [6]</td>
</tr>
<tr>
<td>SECADM</td>
<td>Service-Type [6]</td>
</tr>
<tr>
<td>SECAUD</td>
<td>Service-Type [6]</td>
</tr>
<tr>
<td>RBACMNT</td>
<td>Service-Type [7]</td>
</tr>
<tr>
<td>Administrator</td>
<td>Service-Type [6]</td>
</tr>
</tbody>
</table>

In SDM600, a user may be assigned to multiple roles. In this case, when the user accesses a RADIUS device, the user will be assigned a corresponded 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 under the installation directory (in 64-bit Operating System, it is under C:\Program Files (x86)\ABB\SDM600\bin).

2. There are two major sections that are related to the 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 (i.e. Administrator role) to RADIUS Attributes Service-Type.

3. Inside each RoleDefinitionRadiusRights section, there is one RoleToRight section and inside the RoleToRight section, there are multiple RoleToRadiusRights sections. Each RoleToRadiusRights section represent 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. The next table shows the before and after adaptation of the mapping. Note that the table only shows a snapshot of the file's content.

WARNING

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

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

<table>
<thead>
<tr>
<th>Default mapping from SDM600</th>
<th>Customized mapping by user</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;RoleDefinitionRadiusRight&gt;</code></td>
<td><code>&lt;RoleDefinitionRadiusRight&gt;</code></td>
</tr>
<tr>
<td><code>&lt;RoleDefinition&gt;</code></td>
<td><code>&lt;RoleDefinition&gt;</code></td>
</tr>
<tr>
<td><code>&lt;Revision xsi:nil=&quot;true&quot; /&gt;</code></td>
<td><code>&lt;Revision xsi:nil=&quot;true&quot; /&gt;</code></td>
</tr>
<tr>
<td><code>&lt;Definition&gt;IEC62351-8&lt;/Definition&gt;</code></td>
<td><code>&lt;Definition&gt;IEC62351-8&lt;/Definition&gt;</code></td>
</tr>
<tr>
<td><code>&lt;Roles /&gt;</code></td>
<td><code>&lt;Roles /&gt;</code></td>
</tr>
<tr>
<td><code>&lt;RoleDefinition&gt;</code></td>
<td><code>&lt;RoleDefinition&gt;</code></td>
</tr>
<tr>
<td><code>&lt;RoleToRight&gt;</code></td>
<td><code>&lt;RoleToRight&gt;</code></td>
</tr>
<tr>
<td><code>&lt;RoleToRadiusRight&gt;</code></td>
<td><code>&lt;RoleToRadiusRight&gt;</code></td>
</tr>
<tr>
<td><code>&lt;Role&gt;</code></td>
<td><code>&lt;Role&gt;</code></td>
</tr>
<tr>
<td><code>&lt;Name&gt;Viewer&lt;/Name&gt;</code></td>
<td><code>&lt;Name&gt;Viewer&lt;/Name&gt;</code></td>
</tr>
<tr>
<td><code>&lt;RoleId&gt;0&lt;/RoleId&gt;</code></td>
<td><code>&lt;RoleId&gt;0&lt;/RoleId&gt;</code></td>
</tr>
<tr>
<td><code>&lt;Rights&gt;</code></td>
<td><code>&lt;Rights&gt;</code></td>
</tr>
<tr>
<td><code>&lt;string&gt;RuggedCom-Privilege-level[guest]&lt;/string&gt;</code></td>
<td><code>&lt;string&gt;RuggedCom-Privilege-level[guest]&lt;/string&gt;</code></td>
</tr>
<tr>
<td><code>&lt;Rights&gt;</code></td>
<td><code>&lt;Rights&gt;</code></td>
</tr>
<tr>
<td><code>&lt;RoleToRadiusRight&gt;</code></td>
<td><code>&lt;RoleToRadiusRight&gt;</code></td>
</tr>
<tr>
<td><code>&lt;RoleToRadiusRight&gt;</code></td>
<td><code>&lt;RoleToRadiusRight&gt;</code></td>
</tr>
<tr>
<td><code>&lt;Role&gt;</code></td>
<td><code>&lt;Role&gt;</code></td>
</tr>
<tr>
<td><code>&lt;Name&gt;Operator&lt;/Name&gt;</code></td>
<td><code>&lt;Name&gt;Operator&lt;/Name&gt;</code></td>
</tr>
<tr>
<td><code>&lt;RoleId&gt;1&lt;/RoleId&gt;</code></td>
<td><code>&lt;RoleId&gt;1&lt;/RoleId&gt;</code></td>
</tr>
<tr>
<td><code>&lt;Rights&gt;</code></td>
<td><code>&lt;Rights&gt;</code></td>
</tr>
<tr>
<td><code>&lt;string&gt;Service-Type[1]&lt;/string&gt;</code></td>
<td><code>&lt;string&gt;Service-Type[1]&lt;/string&gt;</code></td>
</tr>
<tr>
<td><code>&lt;string&gt;RuggedCom-Privilege-level[operator]&lt;/string&gt;</code></td>
<td><code>&lt;string&gt;RuggedCom-Privilege-level[operator]&lt;/string&gt;</code></td>
</tr>
<tr>
<td><code>&lt;Rights&gt;</code></td>
<td><code>&lt;Rights&gt;</code></td>
</tr>
<tr>
<td><code>&lt;RoleToRadiusRight&gt;</code></td>
<td><code>&lt;RoleToRadiusRight&gt;</code></td>
</tr>
<tr>
<td><code>&lt;RoleToRadiusRight&gt;</code></td>
<td><code>&lt;RoleToRadiusRight&gt;</code></td>
</tr>
<tr>
<td><code>&lt;Role&gt;</code></td>
<td><code>&lt;Role&gt;</code></td>
</tr>
<tr>
<td><code>&lt;Name&gt;Engineer&lt;/Name&gt;</code></td>
<td><code>&lt;Name&gt;Engineer&lt;/Name&gt;</code></td>
</tr>
<tr>
<td><code>&lt;RoleId&gt;2&lt;/RoleId&gt;</code></td>
<td><code>&lt;RoleId&gt;2&lt;/RoleId&gt;</code></td>
</tr>
<tr>
<td><code>&lt;Role&gt;</code></td>
<td><code>&lt;Role&gt;</code></td>
</tr>
</tbody>
</table>
9.2.6.4 Integrating Windows PC Authentication into SDM600 Centralized Account Management

As a centralized account management unit, SDM600 provides the functionality to integrate Windows PC authentication into its account management functionality. This functionality is to allow users of Windows PCs that are in a workgroup to be authenticated against and managed by the SDM600 Centralized Account Management system.

If the Windows PC is part of a domain, the Windows users will be managed by and authenticated against Microsoft Active Directory (and not by SDM600)

CAUTION

To enable this, the user must download the installer to be installed on the Windows PC. This installer is generated when Windows PC option is chosen during creation of Centralized Account Management package.

1. To benefit from this feature, the Windows PC must be registered as a device in SDM600.
3. Select device or devices which will use Windows PC Authentication.
4. Click on Add new CAM Configuration button.

Figure 8.30: Add new CAM Configuration button

5. Select WindowsPC32 or WindowsPC64 protocol. The available options are 32-bit or 64-bit operating system.

NOTE

In order to find out the version of the installed Operating System on the Windows PC, open the Windows Explorer. Right click Computers and then select Properties. Information about the version of the installed Operating System can be found under System section – System Type.

6. Provide certificate validity dates and password.
7. Click OK
8. Click Save icon
9. Download installer on local computer by clicking Download configuration package icon.
10. Bring the file to the Windows PC on which the installer is to be installed.
11. Unzip the download package into a directory.
12. Run the installer.
The installer is tailored to this Windows PC. Installing the installer that is generated for another device will cause the integration of the Windows PC to the ABB SDM600 centralized account management to not work properly.

**CAUTION**

13. When the installation is completed, restart the Windows PC.

14. When the Windows PC is up and running, a new login page is shown.

   Now the user can log in into the Windows PC using the same credentials as in SDM600.

   For new users that have just been created in SDM600, it is important that they change their password before logging into the PC via ABB SDM600 Centralized Account Management for Windows PC. A local profile in the Windows PC will only be created when the user enters a valid and updated password.

**WARNING**

ABB SDM600 Centralized Account Management for Windows PC provides a way to change the mapping between a SDM600 Centralized Account Management role and a Windows operating system group. To change this mapping, navigate to your installation directory of ABB SDM600 Centralized Account Management for Windows PC and open the *GroupRoleMappingStore* file using administrator rights. The file can be opened by using a simple text editor or an XML editor.

An example of mapping be follows. In this example, the SDM600 Viewer and Operator Roles are mapped to “Some Windows Users Group”.

```xml
<GroupRoleMapping>
 <GroupName>Some Windows Users Group</GroupName>
 <RoleDefinitions>
  <RoleDefinition>
   <Revision xsi:nil="true" />
   <Definition>IEC62351-8</Definition>
   <Roles>
    <Role>
     <Name>Viewer</Name>
     <RoleId>0</RoleId>
    </Role>
    <Role>
     <Name>Operator</Name>
     <RoleId>1</RoleId>
    </Role>
   </Roles>
  </RoleDefinition>
 </RoleDefinitions>
</GroupRoleMapping>
```

Do the following:

1. Define an intended specific group role mapping. This can be done by specifying the tags `<GroupRoleMapping></GroupRoleMapping>`.
2. Within the `<GroupRoleMapping>` tags, you need to add the following information as seen in the previous example:
   - Define a new tag `<GroupName></GroupName>` that specifies the name of the Windows User Group. The “Group Name” node consists of the name of the Windows Users Group. Windows User Groups can be found in the system by navigating to the “Local Users and Groups” application. Go to **Windows Control Panel > Edit Local Users and Groups**.
   - Define a new tag `<Revision>`. This tag can be omitted.
• Define a new tag <RoleDefinitions></RoleDefinitions>. This tag is a collection of several <RoleDefinition></RoleDefinition> tags. This tag stores information on SDM600 roles that are going to be mapped to a specific Windows User Group.

• Define a new tag <Definition></Definition>. This tag is to specify available role definitions in SDM600. ABB SDM600 has two role definitions: ABB and IEC62351-8.

• Define a new tag <Roles></Roles>. This tag is a collection of several <Role></Role> definitions. Each <Role> definition contains the Name and ID information.

• In SDM600, the following roles' names and IDs are defined:

<table>
<thead>
<tr>
<th>Role Definition</th>
<th>Name</th>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABB</td>
<td>Administrator</td>
<td>-100</td>
</tr>
<tr>
<td>IEC62351-8</td>
<td>Viewer</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Operator</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Engineer</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Installer</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>SECADM</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>SECAUD</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>RBACMNT</td>
<td>6</td>
</tr>
</tbody>
</table>

After modifying the GroupRoleMappingStore.xml file, remember to save the file and restart the following services:

• ABB Workgroup Management Service
• ABB Workgroup Replication Service
• pGina Service

9.2.6.5 Integrating Windows PC Events into SDM600 Windows Event Log Forwarder

SDM600 provides possibility to register security events from Windows PC. This functionality is independent from the ABB SDM600 Centralized Account Management for Windows PC and can be installed separately.

In order to enable ABB SDM600 Windows Event Log Forwarder follow steps below:

1. Add the Windows PC as a device in SDM600 (you can skip this step if it's already done for Centralized Account Management).
2. Select a device, for which the ABB SDM600 Windows Event Log Forwarder installer will be generated.
3. Download installer on local computer by clicking **Generate** button.
4. Bring the file to the Windows PC on which the installer is to be installed.
5. Unzip the download package into a directory.
6. Run the installer.

**CAUTION**

The installer is tailored to this Windows PC. Installing the installer that is generated for another device will cause the ABB SDM600 Windows Event Log Forwarder to not work properly.

7. When the installation is completed, restart the Windows PC.

**9.2.6.6 User Account Management**

Setting up user accounts in SDM600 is a very important step. Best practices in cyber security recommend the principle of least privilege. The principle imposes on providing a user account with 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.

SDM600 offers roles that are defined in the IEC 62351 standard. The roles and their definitions according to SDM600 are the following:

- **Viewer**: provides the assigned SDM600 user rights to view (read-only) available general interfaces in SDM600
- **Operator**: provides the assigned SDM600 user rights to operate the configured SDM600
- **Engineer**: provides the assigned SDM600 user rights to configure the SDM600 application (not included: security events and centralized account management)
- **Installer**: provides the assigned SDM600 user rights to configure SDM600 application (not included: security events and centralized account management)
- **SECADM**: provides the assigned SDM600 user rights to configure SDM600 centralized account management
- **SECAUD**: provides the assigned SDM600 user rights to configure SDM600 security events management
- **RBACMNT**: provides the assigned SDM600 user rights to configure the SDM600 Role to Right mapping
- **Administrator**: provides SDM600 user rights to perform user account administration and to configure SDM600.

  A full definition of the IEC 62351 roles can be found in the standardization document. SDM600 redefines the roles according to the SDM600 application. However, SDM600 provides a UI for the user to redefine the rights for each user role.

  **NOTE**

  For managing users, a dedicated toolbar is provided.

  **NOTE**

  To add new user, click **New User**, and enter the required information.

  ![Add new user](image)

  **Figure 8.33: SDM600 Configuration - Add New User**

  Each entry is validated. Failing to comply to the formatting standard will be alerted and enough information on proper formatting will be given.

  ![Add new user format check](image)

  **Figure 8.34: SDM600 Configuration - Add New User Format Check**
It is generally recommended that you use strong, unique passwords for each of your services and accounts. If hackers gain access to the login details for one of the services that you use, they can then use that information to access any of your other online accounts where you have used the same password. Using a unique password for each account means that even in the event of a data breach in one of the services you use, your other accounts are not at risk.

**CAUTION**

SDM600 could adopt a strong password requirement according to which, a password should have at least one special character, a number, a capital letter and a small letter. An example of a strong password is `J*p2leO4>F` (ref: [http://technet.microsoft.com/en-us/library/cc756109(v=ws.10).aspx](http://technet.microsoft.com/en-us/library/cc756109(v=ws.10).aspx)).

![Add user form with password rules](image)

*Figure 8.35: SDM600 Password Requirement*

After creating a user, the administrator can assign roles to the user.

![User role assignment](image)

*Figure 8.36: SDM600 Configuration - Assign Roles to User*

**CAUTION**

For a new created user, the user must immediately change their password on next login attempt.

To delete a user, select the user, then click **Delete user**. If a user has forgotten their password, the administrator can help the user to reset the password. Select the user whose password is to be reset, then click **Reset password**. A new random password is automatically generated based on this request if the user confirms to reset the password.
When the administrator resets a user's credentials, a pop-up box with new credentials is shown. The credentials can be copied by pressing Ctrl+C. To paste the credentials, press Ctrl+V.

**NOTE**

When the E-mail Notification feature is activated in SDM600, any change of a user's credentials is automatically forwarded to the respective user.

**NOTE**

When a user's password is reset by the administrator, the user must immediately change their password on next login attempt.

**CAUTION**

### 9.2.6.7 SDM600 Password Policy Settings

SDM600 provides the possibility to configure the policy for the user password. The following options are possible:

- **Basic Settings**
  - Enable or disable password must meet policy requirements
  - Minimum password length
  - Maximum password age
  - Expire warning
  - Password history enforcement
  - Number of maximum failed login attempts
  - Lockout duration

- **Password Complexity Settings** - a password must contain at least the following properties:
  - Lowercase characters (a - z)
  - Uppercase characters (A - Z)
  - Base digits (0 - 9)
  - Non-Alphanumeric
SDM600 provides the possibility to configure the roles. As default, standard roles described in IEC62351 are configured. These roles cannot be modified or deleted.

In addition to IEC62351 roles, there is possibility to create custom roles.

Follow below steps in order to create custom role

1. click on **New role...** icon
2. Fill required information

**CAUTION**

According to IEC62351, custom roles have negative Id values

If at least one custom role has been created, then additional icons are activated

**Figure 8.40: Custom roles icons**

9.2.6.9 Replication Groups

It is possible to define groups of users, which will be replicated to the device. This functionality helps to save device memory and decrease replication time
SDM600 User Rights

SDM600 provides the possibility for an authorized user to configure the role to right mappings for the SDM600 application. This flexibility allows end users to adjust the role to right mapping according to their policy. The standard role to right mapping that is recommended by SDM600 can be seen in the following figure.

From the role to rights perspective, SDM600 is divided into five parts:

- General Information
- Engineering of the SDM600 application
- User and role management
- Disturbance record settings and monitoring
- Security event setting and reporting

### 9.2.7 Certificate Management

This feature enables SDM600 to modify default certificates settings, manage root certificate and generate device certificate for general purposes.

The information mentioned in this section should be edited with care. Misconfiguration on the certificate properties may cause SDM600 to stop work.

**WARNING**

Settings in Certificate Management tab are affecting all certificates generated by the SDM600 (including CAM certificates). Increasing default certificate key length may impact device performance.

**WARNING**

The Certificate Management setting provides the following functions to the user:

- **Root certificate handling** - allows user to import root certificates obtained from external certificate authority, regenerate self-signed root certificate and export CA private key to the file.

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

  **WARNING**

- **Default certificates creation values** - enables to set default values for key length, validity date and extended attributes for newly created certificates.

  Key length and validity date can be adjusted on certificate creation dialog.

  **NOTE**

![Certificate Management settings](image)

*Figure 8.43: Certificate Management settings*
9.2.7.1 Setting up Device certificates

SDM600 can generate general purposes certificate for every device defined in the structure. These certificates can be used for securing web connection or file transfer (if connected device is offering this function).

In order to generate certificate for device, follow steps below:

2. Select one or more device.
3. Click on Add new certificate button.

![Add new certificate button]

*Figure 8.44: Add new certificate button*

4. Define certificate key length, validity dates and certificate password.

![Certificate creation window]

*Figure 8.45: Certificate creation window*

> CAUTION

If certificates are generated for multiple devices in one step, then password for generated certificates will be the same.

5. Save newly created CAM package by hitting Save icon.
6. Copy certificate for selected device or devices.

> CAUTION

It is possible to edit certificate properties by double click on device list. When changes are done, it's necessary to click on Save icon.
9.3 User Options

SDM600 makes it possible for each user to define their own preference settings in the UI. To access this possibility, click the Options icon next to the username at the top right of the SDM600 UI.

9.3.1 User Account

In the User Account tab, it’s possible to change user relevant information such as password, email address, first name and last name.

![Options - User Account](image)

Figure 8.46: Options - User Account

9.3.2 Preferences

In the Preferences tab, it’s possible to tailor the tool’s behavior to the user’s needs.

![Options - Preferences](image)

Figure 8.47: Options - Preferences

Currently, the tool allows the following customizations:
- **Timeline Settings** is used to define the width of the dashboard time navigator. Available time ranges span from the minimum of 1 Day to the maximum of 1 Year.

- **DR Analysis Tool Definition** is used to define the preferred tool for analyzing a disturbance record entry.

  To specify the preferred DR analysis tool, the executable file of the tool must be selected. The executable file must be available on the PC from where SDM600 is accessed. In addition, the executable file should be able to take the disturbance record file as its first argument.

**NOTE**

- **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. To edit name or description of the structure items, switch this setting to desired value and go to the **Configuration tab General Settings > Structure**, click on **Enter manual structure editing mode** and double click on the tree item. These values are used by Disturbance Record export feature *(refer to chapter 10.1)*.

- **Reset Display Settings** is used to reset to default the user's display setting. The setting is applied only after the next login.

### 9.3.3 Downloads

In the **Downloads** tab, it's possible to download on the client device several items.

![Figure 8.48: Options - Downloads](image)

The following items are available for download:

- Wavewin ABB - DR Analysis Tool
- ABB SDM600 Certificates - for HTTPS connection
- Windows Agent Installer - script working on Windows PC for collecting configuration information.
- ABB SDM600 Windows Event Forwarder
- Example of CSV file for importing non IEC61850 devices.
To download the ABB SDM600 Windows Event Forwarder and the ABB SDM600 Centralized Account Management to a Windows PC, the user needs to specify the IP address where these applications are to be installed. In addition, to download the ABB SDM600 Centralized Account Management to a Windows PC, the user needs to select the operating system version. When all the necessary information is selected, SDM600 generates the installer package. The user can then extract the installer package in a directory and run the installer.

For Windows Event Log Forwarder you also need to choose a proper Network Interface. To receive communication if there is no required IP address, then go to the Configuration >> Centralized Account Mgmt. >> Refresh network interface list.

10 E-mail Notification

SDM600 provides the possibility to send e-mail notifications to users on the following events:

- A new user is created. When this option is activated, an e-mail is sent to the e-mail address of the user. The e-mail contains a notification that a user on SDM600 has been created. In addition, the initial password is sent in the e-mail.

  New users must change their password when they access SDM600 for the first time.

NOTE

- 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 a new password.

- Disturbance record arrives in SDM600. When this option is activated, SDM600 sends an e-mail notification to pre-selected users in SDM600. SDM600 provides two variants of e-mail notifications when a new disturbance record arrives in SDM600:
  - Plain e-mail notification that informs the user of the arrival of a new disturbance record.
  - E-mail notification that informs the user of the arrival of a new disturbance record and includes the corresponding PDF short report.
  - The user has the possibility to customize condition of the e-mail notification for disturbance record.

  Figure: condition editor for the email

- Information about certificate expiration. It's possible to configure how many days before certificate expiration SDM600 should inform defined users.

To set up the e-mail sending function, a user must navigate to Configuration > E-mail Notification.
Figure 9.1: Setup of SDM600 E-mail Notification

The pre-filled information in the figure above is an example. You should enter proper information according to your SMTP server and account setup. Failure to enter the required information will cause the e-mail sending function to not work properly.

WARNING

The following information is mandatory in order to setup the e-mail sending function:

- the address of a separate and running SMTP server for e-mail sending, such as smtp.yourdomain.com
- an SMTP username (some servers require full address like username@yourdomain.com in order to be able to send emails)
- an SMTP 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
- the e-mail address of the sender (this needs to be a valid e-mail address)

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

NOTE

SDM600 does not come with its own SMTP Server. In general, a user can set up their own SMTP server or it 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), please consult your IT department.

CAUTION

To use the SDM600 E-mail function, the following conditions must be fulfilled:

- Ensure that there is an SMTP server in your organization that can be used to send e-mail.
- Ensure that your firewall does not block the SMTP server traffic (normally port 25 is used).

WARNING

After entering the SMTP configuration, the e-mail notification can be activated for different events.
In SDM600 there are several notifications available:

- Disturbance Recorder notification - allows to send email to defined users, when Disturbance Record is received by the SDM600.

When Disturbance Recorder notification is enabled as well as user to whom notification will be send, then option for defining email condition is enabled.

In order to define email condition, click on **Add** link in Condition column. New window will appear.
Figure 9.4: DR email condition editor

Click on **Add (AND)** button (1), select property from the list (2), define value (3). It is possible to add another value to the current property, by clicking on **Add (OR)** button, or define rule for another property by clicking on **Add (AND)** button (1). When email condition is ready, click on **Save and close** button (4).

- User management notification - allows to send email when account has been created or password has been reset by administrator to user. SDM600 can include password in the email for account creation and password reset.
- Certificate expiration - allows to send notification emails when SDM600 certificate is about to expire. It is possible to set two notifications periods and select users who shall receive notification.

![Certificate expiration notification](image)

Figure 9.5: Certificate expiration notification

- Statistics notification - allows to send daily/weekly/monthly statistics email to target user. Statistics consist number of Disturbance Records, security events, configuration changes and user account changes within selected time range.
11 Disturbance Record Retrieval

SDM600 provides an automatic mechanism that periodically collects disturbance record data from selected devices. SDM600 automatically detects and transfers new disturbance records from selected IEDs and stores the disturbance data files in a designated database following the structure of the engineered network or substation topology.

11.1 Setting Up DR Retrieval Functionalities in SDM600

DR Retrieval in SDM600 is controlled with licenses. When a proper license is available, the user can set up SDM600 to collect disturbance records.

To set up the DR Retrieval function, please follow these steps. Remember to click Save to commit the changes after each step.

11.1.1 Configure Manual / Automatic Export

To configure the manual/automatic export of DR Files, navigate to Configuration Tab > Disturbance Record Retrieval subtab. The first aspect to configure is the filename of the exported files; there are three types of the file naming:

- Original file name
- Filename structure according to the COMNAME standard
- Custom setting: custom file name can be configured by adding to the template dedicated tags.

You can add a tag either by clicking on the predefined buttons or by manually entering the required tag – see list below. The example field provide a preview on the filename.

List of all supported tags is presented in the table below:

<table>
<thead>
<tr>
<th>Tag name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;STRUCTURE&gt;</td>
<td>Structure</td>
</tr>
<tr>
<td>&lt;STRUCTURE_DESC&gt;</td>
<td>Custom name for a structure level.</td>
</tr>
<tr>
<td>&lt;IEDG&gt;</td>
<td>IED Group</td>
</tr>
<tr>
<td>&lt;IEDG_DESC&gt;</td>
<td>Custom name for an IED Group</td>
</tr>
<tr>
<td>&lt;SUBG&gt;</td>
<td>Substation Group</td>
</tr>
<tr>
<td>&lt;SUBG_DESC&gt;</td>
<td>Custom name for a Substation Group</td>
</tr>
<tr>
<td>&lt;SUBSTATION&gt;</td>
<td>Substation</td>
</tr>
<tr>
<td>&lt;SUBSTATION_DESC&gt;</td>
<td>Custom name for a Substation</td>
</tr>
<tr>
<td>&lt;VL&gt;</td>
<td>Voltage Level</td>
</tr>
<tr>
<td>&lt;VL_DESC&gt;</td>
<td>Custom name for a Voltage Level</td>
</tr>
<tr>
<td>&lt;BAY&gt;</td>
<td>Bay</td>
</tr>
</tbody>
</table>
In addition to the tags above it's possible to define custom date or time format. In this case <DATE> or <DATE_SRV> tag must be extended with date and time format definition. For example: <DATE_(dd.MM.yy hh:mm:ss,ffff)>, all possible options are listed in: https://docs.microsoft.com/en-us/dotnet/standard/base-types/custom-date-and-time-format-strings

Custom name/Description of tree levels can be configured in User and Application Settings > Application Setting tab.

Automatically generate PDF Short Report when a disturbance record arrives to SDM600. To enable this function, navigate to Configuration tab > Disturbance Record Retrieval, and then check the Automatically generate short reports when a new disturbance record is retrieved option.

Generating of the short report is resource consuming operation, hence is recommended to not select this function on heavily loaded systems and generate report on demand instead.

WARNING

Automatically save disturbance record files to the SDM600 server folder structure when a disturbance record arrives to SDM600. To enable this function, navigate to Configuration tab > Disturbance Record Retrieval, and then check the Automatically export all disturbance recorder files to the system of the SDM600 server option.

By default, SDM600 is exporting disturbance records files to the folder structure corresponding to the substation structure. It is possible to export all Disturbance Records to the single folder. To enable this function, navigate to Configuration tab > Disturbance Record Retrieval, and then check the Export Disturbance Records to flat structure (don't create directories for each device). option.

NOTE

It is important to define a directory at the SDM600 server where such disturbance record files are to be exported. The directory structure can be defined in the provided text box. See Figure. When no specific directory is defined, SDM600 will store it directly under the installation directory <Installation directory> \ClientBin\Download\DR\. For example, in Windows 7 x64 OS, it is stored under C:\Program Files (x86)\ABB\SDM600\ClientBin\Download\DR\.

NOTE

After entering the directory into the text box for directory definition, remember to save the changes to ensure that SDM600 takes this directory into account while exporting the collected disturbance records files.

WARNING

On demand export collected disturbance records to the SDM600 server folder structure. It is possible to export
Disturbance Records files only form given date range or from selected node. To execute this function, provide the directory to store the exported DR files or pick direct download as a .zip file, then click Export all DRs Files button.

![Disturbance Records Retrieval Configuration](image)

**Figure 10.2: SDM600 DR Retrieval Configuration - Application Settings**

### 11.1.2 Enabling DR Collection for Device

To further configure the devices for disturbance record collection purposes, navigate to subtab **Devices**. This subtab shows the list of available devices based on the selection on the navigation reference area. To start collecting disturbance records from a device, make sure the **Licensed** checkbox is selected.

**WARNING**

By default, SDM600 is not activating the IEDs for disturbance record collection. UTC offset for disturbance records shall be configured before IED is activated (in **Configuration tab > General Settings > Device Settings** page – see 9.2.3).

**NOTE**

By default, SDM600 polls the disturbance record every 60 seconds. To adjust the polling frequency, navigate to the **Configuration > General Settings > Device Settings > Poll Cycle (sec)** column and enter the value in seconds (see 9.2.3).

**CAUTION**

Deactivating the DR Retrieval of an IED will cause SDM600 to delete the collected DR files.

![Device Configuration](image)

**Figure 10.3: SDM600 DR Retrieval Configuration - All Selected IEDs are Activated**
11.1.3 DR Protocol Selection for Device

By default, SDM600 communicates with the devices using IEC 61850-8-1 protocol (MMS protocol). However, SDM600 also supports devices that do not communicate using IEC 61850-8-1. Select the suitable protocol to be used to communicate with SDM600 for disturbance record retrieval. The following methods are available:

- **IEC 61850-8-1**: DR files are collected by SDM600 over 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 been already 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 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 IEC61850-8-1 algorithm, this implementation allows to cope with suboptimal data quality (e.g. creation date of the DR file always set to 1.1.1970), whereas delivering worse performance regarding CPU usage and network footprint.

- **FTP**: DR files are collected by SDM600 by using standard File Transfer Protocol.

- **SFTP**: DR files are collected by SDM600 by using SSH File Transfer Protocol. 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 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.

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

- **RTU Web API**: This method is used when DR files are collected from the RTU500 device. DR file format is recognized automatically, and suitable converter is used if needed.

11.1.3.1 Configure Parameters for DR Protocol

- **Username**: if FTP (both secure and not) or RTU Web API protocol is chosen as a way of communication, it is important to enter the respective username to access the directory of the device.

- **Password**: if FTP or RTU Web API protocol is chosen as a way of communication, it is important to enter the respective password to access the directory of the device.

- **RTU Role Name**: if RTU Web API protocol is chosen as a way of communication, it's important to enter the name of the role with defined privileges to read disturbance record files on the RTU device.

- **DR Path**: specify the directory where the disturbance record files are located. This information is valid for all types of communication.

11.1.3.2 DR Path for Directory Protocol

If Directory is selected as DR Protocol, it is important to correctly specify the DR Path. It is possible to configure two directories, so that SDM600 will make use of the secondary one if the primary one is not reachable.
NOTE

DRs will be collected from the primary directory, if reachable.
DRs will be collected from the secondary directory, if the primary is not reachable.
SDM600 will not merge the content of the two directories – only one of the two directories is used at any time.

Local Directory
If the directory is located on the same computer as the SDM600, use the following notation: `\localhost\c$\Directory`. For example, if the DR files are located under `C:\Substation_Baden\Bay1\IED1\`, then type in `\localhost\c$\Substation_Baden\Bay1\IED1\` into DR Path column of the respective IED.

Remote Directory
If the directory is located on a different computer, it is important to make sure that the directory is accessible from SDM600, i.e. by sharing the folder. While sharing the folder, it is important to ensure that the *ABB SDM600 IED Communication Service* is running under an account which has enough privileges to access the network path or the remote shared folder, i.e. same credentials, same right 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 under a computer with IP address 10.41.141.107 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 `\10.41.140.107\Substation Baden\Baden\IED2\`

In general, when there is a need to access 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 only the full UNC path to the folder on another machine is given to SDM600.

**WARNING**

In the case where the SDM600 service seems to run under an account which does not have enough privileges to access the shared folder, do the following steps:

- Navigate to Windows Start menu and type in Services, then select and click on View Local Services.
- Right click on ABB SDM600 IED Communication Service and click on Stop to stop the service.
Figure 10.6: Windows Services - Navigate to ABB SDM600 IED Communication Service’s Control and Properties

- Click on Properties, and navigate to the Log On tab.
- Click on This Account and then fill in the username and password for the account with proper privileges. It is important to ensure that this user has local administrator privileges. Note that the account in the following Figure is an example.
This case can be identified by checking whether it is possible to map the same shared folder on Windows Explorer. If mapping the same shared folder on Windows Explorer is possible, but SDM600 is not able to access the shared folder, this is an indication that due to certain setup in Windows OS, the SDM600 service is running under an account that has not enough privilege to access the shared folder.
11.2 Analyzing Disturbance Records in SDM600

In order to analyze DR files in SDM600, follow the steps below:

- Select a DR entry on the SDM600 Dashboard
- Next, double click the DR point. This action brings the user to the DR entry that is selected on the dashboard.

![SDM600 DR Analysis - Dashboard](image1)

![Clicked DR on SDM600 Dashboard is Highlighted in DR Tab](image2)

- After that, user can analyze the DR by performing one of the following actions:
  - Download the DR files (in zip file)
  - Analyze the DR by using external analysis tool - Wavewin ABB launches automatically and shows the analyzed data or other user-defined third-party analysis tool

  SDM600 allows to analyze multiple DRs at one time or merge them in ABB Wavewin. In order to open multiple DRs, select them on the list and click on Evaluate icon on the toolbar.
SDM600 provides the possibility to analyze the incoming disturbance record using a user-defined 3rd party analysis tool. To define this, navigate to User and Application Settings at the top right corner of the page. Simply click on the username. Next, navigate to the Application Settings tab and then focus on the DR analysis tool definition area. After this, the user must specify the link to the executable file.

CAUTION

For the user-defined third-party DR analysis tool to work, the tool executable should be able to take the disturbance record file name as the first argument of the executable.

WARNING

When the DR Short Report button is pressed, respective DR Short Report is generated and automatically launched in the new tab. It is possible that a browser disables pop-up windows by default. Different browsers behave differently. To enable pop-up windows on the browser, refer to the user manual of the browser.

NOTE

Information regarding the Wavewin ABB application installer is available in the document 1MRS757749 - SDM600 Installation Guide - SDM600 Client-Side Installation.
12 Security Events Settings

SDM600 offers the possibility to collect security events or logs that are sent in the format of Syslog from devices and applications. Additionally, SDM600 can also forward all events to another Syslog aggregator.

Security events in SDM600 are:

- Events that are caused by user actions in the system under SDM600.
- Events related to security issues from operating systems and security software (such as Anti-virus) of the system under SDM600.

Syslog is a standardized way for logging in computer systems. It is standardized by the IETF in RFC 5424. In most cases, the Syslog data is sent in clear text, unless the communication protocol is secured by means of encryption (for example, by using SSL). Unless the device is designed to connect to SDM600 securely, SDM600 receives the Syslog message in the clear text format.

Setting Up Security Events Collection in SDM600

For SDM600 to receive security events and store them completely in the SDM600 system, the following steps must be executed:

- The devices that send Syslog events or the computers where an application sends out Syslog events must be registered as devices in SDM600. To register a device, navigate to Configuration > Structure.
- Activate the devices in SDM600 for centralized activity logging so that SDM600 stores the events.

To activate devices for centralized activity logging, navigate to Configuration > Security Events. Activate the devices which need to send Syslog events. Remember to save the changes.

SDM600 does not store events that arrive to SDM600 if the sender is not registered in SDM600. SDM600 only shows the 100 latest events.

If a security event is received that cannot be parsed (for example due to a missing/wrong date), the raw message will be shown in the Unparsed tab.

Figure 11.1: Activation of Devices for Security Events Purpose
When SDM600 receives Syslog events from devices that are activated, SDM600 tries to map the incoming events to the pre-defined available event type according to SDM600.

**NOTE**

SDM600 provides numerous pre-defined event types. The pre-defined event types represent and relevant security events. In most cases, the pre-defined event types represent user activity events that are recognized by most industry cyber security standards. In SDM600, all user activities are cyber security relevant activities. Each SDM600 pre-defined event type has its own EventID and description. Examples of such pre-defined event types are:

<table>
<thead>
<tr>
<th>EventID</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1110</td>
<td>Log-in successful</td>
</tr>
</tbody>
</table>
Password expired, Log-in successful
Log-out (user logged out)
Device reset to factory default
User account enabled successfully
User creation failed

For a complete list of the available event types in SDM600 refer to Appendix A.

SDM600 provides a UI for the user to observe the incoming events. To view the incoming events and their event types, navigate to **Security Events tab**.

![SDM600 Security Events Tab](image)

**Figure 11.3: SDM600 Security Events Tab**

If mapping cannot be done because the Syslog event cannot be fully understood by SDM600, SDM600 categorizes the event as unknown event type (EventID 9990) and stores the event in SDM600 persistence. When the user knows more about the context of the unknown Syslog event, the user can re-categorize the unknown event type into a known event type by using the UI available in SDM600.

Map Unknown Event Type to Known Event Type

SDM600 provides an intuitive interface to map the unknown events to SDM600 known events. To conduct the mapping operation, navigate to **Configuration > Event Mappings**. In this part, all the events of unknown type (EventID 9990 and EventID 9991) are listed.
To start mapping the unknown events, do the following:

1. Click an unknown type security event for which a rule is to be created.
2. Click **Add New Rule**. A mapping rule creator window opens.
   Enter the necessary details, such as:
   - Name
   - Description
   - Rule conditions. This can be done by constructing conditions that the security events should meet.
New defined event type. After defining the rule conditions, it is important to select the new event type that is assigned to this kind of security events.
When a single rule is created, SDM600 tries to match all the available unknown types of security events to this rule.

NOTE

- Before committing to the changes, a user can preview the affected security events by clicking **Preview**.
3. To apply the changes, click **OK**. Once the rule is applied, SDM600 will map the unknown rules to the selected known event type and the newly mapped events will disappear from the list of unknown events.

NOTE

SDM600 provides the ability to export the rules to a file. This is done for backup purpose or to apply the same rules on another SDM600 installation. To import the rules, click **Import Rules** and select the backup file.
Enabling Windows PC to Send Security Events to SDM600

As a Centralized Activity Logging unit, SDM600 provides a possibility for a Windows PC to send Windows security and application events to SDM600.

Windows security events are events that are generated during login/logout activity or other security-related events specified by the system’s audit policy. By using a special SDM600 application – ABB SDM600 Windows Event Log Forwarder – SDM600 translates Windows Security Events log entries into SDM600 security events.

To enable this, the user must download the installer to be installed on the Windows PC. This installer can be found in the User and Application Settings > Downloads. Follow the steps below:

1. To benefit from this feature, the Windows PC must be registered as a device in the SDM600.
2. Download the ABB SDM600 Windows Event Forwarder and CAM Prerequisites and install it on the Windows PC.
3. Click Generate Installation for ABB SDM600 Windows Event Log Forwarder for Windows PC.
4. Click Generate.
5. Bring the file to the Windows PC on which the installer is to be installed.
6. Unzip the download package into a directory.
7. Run the installer.

The installer is tailored to this Windows PC. Installing installer that is generated for another device will cause the integration of the Windows PC to the ABB SDM600 Windows Event Log Forwarder to not work properly.

If you are in a Parent-Child system, the installer can only be generated if the Parent system is reachable. If not, the generation is disabled.

8. When the installation is completed, restart the Windows PC.
9. When the Windows PC is up and running, whenever there is a security event log entry that is triggered by the Microsoft Windows OS, the event is sent to SDM600.

It is important to regularly monitor the events that come to the SDM600 Centralized Activity Logging. Regular monitoring makes it easier to detect anomalous behavior in the amount of received logs. When there is a wrong configuration in the Windows operating system, there is a chance that a Windows PC sends lots of events. In order not to fill in the SDM600 database with unnecessary events, it is possible to temporarily disable the installed ABB SDM600 Windows Event Log Forwarder on the Windows PC. To disable the ABB SDM600 Windows Event Log Forwarder on the Windows PC, do the following:

- Go to Start program in the Windows PC.
- Select services.msc, then press Enter.
- Find ABB SDM600 Windows Event Log Forwarder.
- Right-click on the service ABB SDM600 Windows Event Log Forwarder.
- Click Stop. By stopping the service, the ABB SDM600 Windows Event Log Forwarder stops forwarding any new Windows security events.
- To enable the service again, repeat the same steps, then click Start.

By default, SDM600 maps Windows Security Events to SDM600 specific events. The mapping table is available in the Appendix B.

NOTE

Forwarding Incoming Security Events to Third Party Syslog Aggregator

It is also possible to forward incoming security events to another Syslog server or aggregator. To do so, navigate to Configuration > Security events > Forward Security Events. On the toolbar, click the button for Syslog Server...
Settings. Enter the required information for the external Syslog server. Remember to save the changes. When this external Syslog server is set up, any incoming security events are immediately forwarded to the external Syslog server.

![Image of Syslog Server Settings]

Figure 11.11: Registration of External Syslog Server - Button to Add External Syslog Server

![Image of Syslog Server Details]

Figure 11.12: Registration of External Syslog Server - Enter Server Details

WARNING

It is important to know that the Syslog events that are forwarded to the external Syslog server are not SDM600 processed Syslog events. The forwarded Syslog events are pure Syslog events that are received by SDM600. The events that are shown in the SDM600 UI are already processed by SDM600.

SDM600 Cyber Security Events

By default, SDM600 also sends out cyber security events when a user performs some actions. Most of the events are broadcast when the user makes configuration changes. SDM600 records information such as the username, time of the event, type of the event and some extra information regarding the action that triggered the event. SDM600 cyber security events are shown on the most upper part of SDM600 Dashboard.
To view SDM600 cyber security events in detail, navigate to Security Events tab. An SDM600 cyber security event can be indicated by its source, i.e. SDM600.

A list of SDM600 Cyber Security Events is available on Appendix C.
12.1 SDM600 Forwarded SYSLOG Structure

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=10.170.27.161/<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 follow:
/IPADDRESS/<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 SYSLOG message is generated. SDM600 collects SYSLOG and other messages from different connected industrial specific supported devices (e.g. RTU500 series) in isolated secure network environment and forward together dedicated multiple analysis tools or long-term storage places. Some cases the original SYSLOG message does not contain of the sender IP address. For accurate identification of the real source of the messages SDM600 always put the original host IP address to 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. Note: 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 represent the format of the Syslog messages. In ABB case it is own ABB-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 shorten SYSLOG messages.
  - SequenceNumber display messages with sequence numbers because there is a chance that more than one log message can have the same timestamp.
  - SourceDevice represent 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.
13 File Management

The SDM600 allows to store and manage device specific files like firmware and configuration. SDM600 is storing last five versions of the configuration and firmware files for each device.

Current release of SDM600 is supporting RTU500 rel. 12 family devices only.

WARNING

Before using HTTPS option, make sure that SDM600 certificate for device is generated, uploaded to the device and properly configured.

CAUTION

When new RTU device is added, SDM600 is configuring Firmware and Configuration Roles Names to default values. Make sure that user account used to connect with the RTU is assigned to these roles and proper rights are configured on RTU side. Otherwise change roles names accordingly.

In order to set up file management for the device navigate to Configuration tab > File management and configure following properties:

- **Username** - username for the account on the device
- **Password** - credentials of the account on the device
- **Use HTTPS** - securing connection with the device

Before using HTTPS option, make sure that SDM600 certificate for device is generated, uploaded to the device and properly configured.

WARNING

- **Firmware Role Name** - Name of the role with configured read/write rights for device firmware
- **Configuration Role Name** - Name of the role with configured rights for updating device configuration

CAUTION

When new RTU device is added, SDM600 is configuring Firmware and Configuration Roles Names to default values. Make sure that user account used to connect with the RTU is assigned to these roles and proper rights are configured on RTU side. Otherwise change roles names accordingly.
All RTU related user accounts configured in the SDM600 must have Viewer right in the RTU.

CAUTION

It's possible to schedule automatic backup of the device configuration. This option is configurable per device in the Update Frequency column.

After successful configuration, SDM600 allows to perform following operations:

• Read configuration from the device
• Write configuration to the device - in the newly opened window, there is possibility to choose file from the disk or file already stored in the SDM600 database.

Figure 12.2: File management icons

- Figure 12.3: Write file to the device

After successful write, device is restarted, and new configuration is activated.

WARNING

• Read firmware from the device
• Write firmware to the device - this function is opening similar window as write configuration function.
On Configuration Files and Firmware Files tabs is a list of files currently stored in SDM600. There is also possibility to download these files to the drive.

In order to download configuration or firmware file to the drive,

1. navigate to corresponding sub tab in the File management tab
2. select device, from which file will be saved on the drive
3. click on download icon

![Figure 12.4: File management - read file from the drive](image)

For the RTU specific configuration support follow this link: [http://new.abb.com/substation-automation/products/remote-terminal-units](http://new.abb.com/substation-automation/products/remote-terminal-units)
14 SDM600 Application Administration Tool

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

Please note that the SDM600 Application Administration Tool is only available on the SDM600 Server, thus it’s not accessible by the clients.

14.1 How to launch the Application Administration Tool

You can execute the SDM600 Application Administration Tool in two ways:

- **Launch it from the Start Menu**
  Navigate to Windows Start Menu on the SDM600 server, find and open the SDM600 Application Administration Tool.

  ![Figure 13.1: SDM600 Application Administration Tool - Access from Windows Start Menu](image1.png)

- **Launch it from the File System:**
  1. Navigate to the SDM600 installation folder.
  2. By default, it is under `C:\Program Files (x86)\ABB\SDM600`.
  3. Navigate to the bin folder.
  4. Locate and execute `SDM600ApplicationAdministrationTool.exe`.

![Figure 13.2: SDM600 Application Administration Tool in the bin folder](image2.png)
14.2 Restore

SDM600 Application Administration Tool provides a function 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. In order to restore a password protected backup file, the correct password must be provided.

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 select, only SDM600 configuration will be restored: disturbance records data, configuration changes and security events data are not imported.

After selecting the desired option, select the back up to restore.
Then click Restore to start the procedure. Detailed logs will be provided in the Restoration Log as shown below.

**Figure 13.5: SDM600 Application Administration Tool – Restoration Log**

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.

**CAUTION**

Here are possible anomaly events when restoring the SDM600 backup:

- 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 cancelled. 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.

**WARNING**

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 ABB 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 ABB Authentication Service, or simply conduct a full restart of the computer where SDM600 children is installed.

14.3 Backup

The SDM600 Application Administration Tool provides a function to back up the database, including both the configuration and live data. In order to prevent a malicious attacker to obtain confidential information, the backup files are 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.

Navigate to Windows Start Menu on the SDM600 server, find and open the SDM600 Application Administration Tool. Make sure that Backup tab is activated.

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

![SDM600 Application Administration Tool - Backup tab](image)

**WARNING**

Protect the backup with a strong password. Using strong passwords will thwart brute force and dictionary attacks. Be aware that there is no way to recover a lost password. If a password is lost, there is no way to restore the given backup.
14.4 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.

![SDM600 Application Administration Tool](image)

**Figure 13.7: SDM600 Application Administration Tool – Consistency Check performed**

Click on Perform button to apply automatic corrections on SDM600 database. The outcome is visible in the Output Window.

![Output Window](image)

**Figure 13.8: SDM600 Application Administration Tool – Automatic Corrections Performed**

Notice that tool will delete duplicated IP addresses from all devices, it's recommended to save logs, using Export logs button, in order to manually assign correct IP addresses.

**NOTE**
14.5 Cyber Security Event Cleanup

The SDM600 Application Administration Tool provides the possibility to clean up Cyber Security events generated by SDM600 itself.

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

![SDM600 Application Administration Tool – Ignored Events Cleaned Up](image)

**Figure 13.9: SDM600 Application Administration Tool – Ignored Events Cleaned Up**
14.6 Service Communication Configuration

The SDM600 Service Communication Configuration allows to configure the way SDM600 communicate with another SDM600 f. e. 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.

The following authentication methods are supported:

- Certificate
- Windows Account

When Windows Account is selected, the Domain, Username and Password are required.
14.7 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, Cyber Security Events, Service and Maintenance data (e.g. IED status change, Windows Application Information and Patches).

![SDM600 Application Administration Tool](image)

**Figure 13.11: SDM600 Application Administration Tool – Remove Live Data**

Note that clean-up is not undoable, and it could take several minutes. User will be asked for confirmation before starting the operation.

**NOTE**
14.8 Default User Options

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

![SDM600 Application Administration Tool](image)

It's possible to configure the following options:

- **Timeline Settings** is used to define the width of the dashboard time navigator. Available time ranges span from the minimum of 1 Day to the 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.
14.9 Data Retention Configuration

The Data Retention Service manages how long data will be stored in the SQL Database: data older than the specified number of days is permanently removed from the Database, allowing the Database size to be kept in check.

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 older event a .csv file backup will be generated in the configured backup location.
14.10 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).
   Note: "SQL Server (SDMSERVER)" service should be still running for each of them.
2. Using the Application Administration Tool, perform Manual Deprovisioning on each system.
3. Restart SDM600 services on all the affected systems.

⚠️ Failing to comply with the provided procedure will jeopardize the cleanup of the provisioning data.

WARNING
14.11 Service Data Export

The Service Data Export Tab in the Application Administration Tool provides the possibility to configure an Excel export of the Service Data information that is happening automatically and periodically.

You can enable the automatic export by ticking the checkbox. Then you must 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.
Appendix A. List of ABB SDM600 Security Event EventIDs

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Type</th>
<th>Event Description</th>
<th>SDM600 Event Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>1110</td>
<td>Event</td>
<td>Login successful</td>
<td>Security Accountability</td>
</tr>
<tr>
<td>1115</td>
<td>Event</td>
<td>Password expired; Login successful</td>
<td>Security Accountability</td>
</tr>
<tr>
<td>1120</td>
<td>Alarm</td>
<td>Login failed - Unknown user</td>
<td>Potential Security Violation</td>
</tr>
<tr>
<td>1130</td>
<td>Event</td>
<td>Login failed - Wrong credentials</td>
<td>Potential Security Violation</td>
</tr>
<tr>
<td>1140</td>
<td>Event</td>
<td>Login failed - Wrong password</td>
<td>Potential Security Violation</td>
</tr>
<tr>
<td>1150</td>
<td>Alarm</td>
<td>Login failed - Password expired</td>
<td>Security Accountability</td>
</tr>
<tr>
<td>1170</td>
<td>Alarm</td>
<td>Login failed 3 times</td>
<td>Potential Security Violation</td>
</tr>
<tr>
<td>1180</td>
<td>Alarm</td>
<td>Login failed too many user sessions</td>
<td>Potential Security Violation</td>
</tr>
<tr>
<td>1210</td>
<td>Event</td>
<td>Logout (user logged out)</td>
<td>Security Accountability</td>
</tr>
<tr>
<td>1220</td>
<td>Event</td>
<td>Logout due to user inactivity (timeout)</td>
<td>Security Accountability</td>
</tr>
<tr>
<td>1310</td>
<td>Event</td>
<td>Connection with configuration tool successful</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>1320</td>
<td>Event</td>
<td>Downloaded/wrote configuration successfully</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>1321</td>
<td>Event</td>
<td>Configuration download started</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>1322</td>
<td>Event</td>
<td>Configuration stored in the device successfully</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>1330</td>
<td>Event</td>
<td>Uploaded/read configuration successfully</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>1331</td>
<td>Event</td>
<td>Configuration upload started</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>1340</td>
<td>Event</td>
<td>Downloaded/wrote firmware successfully</td>
<td>System Maintenance</td>
</tr>
<tr>
<td>1350</td>
<td>Event</td>
<td>Uploaded/read firmware successfully</td>
<td>System Maintenance</td>
</tr>
<tr>
<td>Event ID</td>
<td>Type</td>
<td>Event Description</td>
<td>SDM600 Event Category</td>
</tr>
<tr>
<td>---------</td>
<td>--------</td>
<td>-------------------------------------------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>1352</td>
<td>Alarm</td>
<td>Stored certificates in the device successfully</td>
<td>System Operation</td>
</tr>
<tr>
<td>1356</td>
<td>Event</td>
<td>Extracted/exported archive file from device successfully</td>
<td>System Operation</td>
</tr>
<tr>
<td>1357</td>
<td>Event</td>
<td>Extracted/exported diagnosis file from device successfully</td>
<td>System Operation</td>
</tr>
<tr>
<td>1358</td>
<td>Event</td>
<td>Extracted/exported certificates from device successfully</td>
<td>System Operation</td>
</tr>
<tr>
<td>1360</td>
<td>Event</td>
<td>Viewed parameter value(s) successfully</td>
<td>System Operation</td>
</tr>
<tr>
<td>1370</td>
<td>Event</td>
<td>Viewed Security Event logs successfully</td>
<td>Security Operation</td>
</tr>
<tr>
<td>1375</td>
<td>Event</td>
<td>Viewed disturbance records successfully</td>
<td>System Operation</td>
</tr>
<tr>
<td>1380</td>
<td>Event</td>
<td>Parameter changed successfully</td>
<td>System Engineering and</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Configuration</td>
</tr>
<tr>
<td>1390</td>
<td>Event</td>
<td>Downloaded Security Event list successfully</td>
<td>Security Operation</td>
</tr>
<tr>
<td>1400</td>
<td>Event</td>
<td>Configuration deleted successfully</td>
<td>System Engineering and</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Configuration</td>
</tr>
<tr>
<td>1410</td>
<td>Alarm</td>
<td>Connection with configuration tool failed</td>
<td>System Engineering and</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Configuration</td>
</tr>
<tr>
<td>1420</td>
<td>Event</td>
<td>Download/writing configuration failed</td>
<td>System Engineering and</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Configuration</td>
</tr>
<tr>
<td>1422</td>
<td>Event</td>
<td>Device configuration update failed</td>
<td>System Engineering and</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Configuration</td>
</tr>
<tr>
<td>1430</td>
<td>Event</td>
<td>Upload/read configuration failed</td>
<td>System Engineering and</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Configuration</td>
</tr>
<tr>
<td>1440</td>
<td>Event</td>
<td>Download/writing firmware failed</td>
<td>System Maintenance</td>
</tr>
<tr>
<td>1450</td>
<td>Event</td>
<td>Upload/read firmware failed</td>
<td>System Maintenance</td>
</tr>
<tr>
<td>1452</td>
<td>Event</td>
<td>Storing/writing certificates in the device failed</td>
<td>System Operation</td>
</tr>
<tr>
<td>1456</td>
<td>Event</td>
<td>Extracting/exporting archive file from the device failed</td>
<td>System Operation</td>
</tr>
<tr>
<td>1457</td>
<td>Event</td>
<td>Extracting/exporting diagnosis file from the device failed</td>
<td>System Operation</td>
</tr>
<tr>
<td>1458</td>
<td>Event</td>
<td>Extracting/exporting certificates from the device failed</td>
<td>System Operation</td>
</tr>
<tr>
<td>1460</td>
<td>Alarm</td>
<td>Parameter change failed - no rights</td>
<td>System Engineering and</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Configuration</td>
</tr>
<tr>
<td>1470</td>
<td>Event</td>
<td>Parameter change failed - out of range</td>
<td>System Engineering and</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Configuration</td>
</tr>
<tr>
<td>1480</td>
<td>Event</td>
<td>Parameter change failed - wrong type</td>
<td>System Engineering and</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Configuration</td>
</tr>
<tr>
<td>1490</td>
<td>Event</td>
<td>Download of Security Event list failed</td>
<td>Security Operation</td>
</tr>
<tr>
<td>1500</td>
<td>Alarm</td>
<td>Deletion of configuration failed</td>
<td>System Engineering and</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Configuration</td>
</tr>
<tr>
<td>1510</td>
<td>Event</td>
<td>Software update initiated successfully</td>
<td>System Maintenance</td>
</tr>
<tr>
<td>1520</td>
<td>Event</td>
<td>Software updated successfully</td>
<td>System Maintenance</td>
</tr>
<tr>
<td>1610</td>
<td>Alarm</td>
<td>Device software update failed</td>
<td>System Maintenance</td>
</tr>
<tr>
<td>1660</td>
<td>Event</td>
<td>View of parameter failed</td>
<td>System Operation</td>
</tr>
<tr>
<td>1670</td>
<td>Event</td>
<td>View of Security Event list failed</td>
<td>Security Operation</td>
</tr>
<tr>
<td>1675</td>
<td>Event</td>
<td>View disturbance records failed</td>
<td>System Operation</td>
</tr>
<tr>
<td>Event ID</td>
<td>Type</td>
<td>Event Description</td>
<td>SDM600 Event Category</td>
</tr>
<tr>
<td>---------</td>
<td>----------</td>
<td>--------------------------------------------------</td>
<td>-----------------------------------------------------------</td>
</tr>
<tr>
<td>1710</td>
<td>Alarm</td>
<td>Device reset to factory default</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>1720</td>
<td>Alarm</td>
<td>User accounts reset to factory default</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>1730</td>
<td>Alarm</td>
<td>Admin password reset to factory default</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>2110</td>
<td>Event</td>
<td>User account created successfully</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>2112</td>
<td>Event</td>
<td>User account added to replication group successfully</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>2113</td>
<td>Event</td>
<td>User account removed from replication group successfully</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>2115</td>
<td>Event</td>
<td>User account enabled successfully</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>2117</td>
<td>Event</td>
<td>User account disabled successfully</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>2120</td>
<td>Event</td>
<td>User account deleted successfully</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>2132</td>
<td>Event</td>
<td>Addition of user account to replication group failed</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>2133</td>
<td>Event</td>
<td>Removal of user account from replication group failed</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>2135</td>
<td>Event</td>
<td>User account enabling failed</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>2137</td>
<td>Event</td>
<td>User account disabling failed</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>2140</td>
<td>Event</td>
<td>User account deletion failed</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>2160</td>
<td>Event</td>
<td>New role assigned to user successfully</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>2161</td>
<td>Event</td>
<td>Permission changed successfully</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>2162</td>
<td>Event</td>
<td>Permission added successfully</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>2170</td>
<td>Event</td>
<td>User role assignment removed successfully</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>2172</td>
<td>Event</td>
<td>User permission removed successfully</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>2180</td>
<td>Event</td>
<td>New role created successfully</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>2190</td>
<td>Event</td>
<td>Role deleted successfully</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>2210</td>
<td>Event</td>
<td>User password changed successfully</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>Event ID</td>
<td>Type</td>
<td>Event Description</td>
<td>SDM600 Event Category</td>
</tr>
<tr>
<td>---------</td>
<td>--------</td>
<td>--------------------------------------------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>2220</td>
<td>Event</td>
<td>Change of user password failed</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>2225</td>
<td>Event</td>
<td>User data changed successfully (for example, username, etc.)</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>2226</td>
<td>Event</td>
<td>Change of user data failed</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>2230</td>
<td>Event</td>
<td>New user role assignment failed</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>2231</td>
<td>Event</td>
<td>Permission change failed</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>2232</td>
<td>Event</td>
<td>Addition of permission failed</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>2233</td>
<td>Event</td>
<td>User password change failed - too short</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>2235</td>
<td>Event</td>
<td>User password change failed - policy check failed</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>2240</td>
<td>Event</td>
<td>User session role changed successfully</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>2245</td>
<td>Event</td>
<td>User session role change failed</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>2270</td>
<td>Event</td>
<td>Role assignment removal failed</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>2272</td>
<td>Event</td>
<td>User permission removed failed</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>2280</td>
<td>Event</td>
<td>New role creation failed</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>2290</td>
<td>Event</td>
<td>Role deletion failed</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>2310</td>
<td>Event</td>
<td>Password file downloaded successful</td>
<td>Security Operation</td>
</tr>
<tr>
<td>2320</td>
<td>Event</td>
<td>Password file uploaded successful</td>
<td>Security Operation</td>
</tr>
<tr>
<td>2350</td>
<td>Event</td>
<td>Download of password file failed</td>
<td>Security Operation</td>
</tr>
<tr>
<td>2360</td>
<td>Event</td>
<td>Upload of password file failed</td>
<td>Security Operation</td>
</tr>
<tr>
<td>2510</td>
<td>Alarm</td>
<td>Password file on CF card corrupted</td>
<td>Security Operation</td>
</tr>
<tr>
<td>2520</td>
<td>Alarm</td>
<td>Password file corrupted</td>
<td>Security Operation</td>
</tr>
<tr>
<td>3110</td>
<td>Event</td>
<td>TCP communication with security log subscriber successful</td>
<td>Communication</td>
</tr>
<tr>
<td>3120</td>
<td>Event</td>
<td>TCP communication with security log publisher successful</td>
<td>Communication</td>
</tr>
<tr>
<td>3150</td>
<td>Event</td>
<td>TCP communication with security log server successful</td>
<td>Communication</td>
</tr>
<tr>
<td>3190</td>
<td>Event</td>
<td>Ethernet reconnection</td>
<td>Communication</td>
</tr>
<tr>
<td>3210</td>
<td>Alarm</td>
<td>TCP communication with security log subscriber failed</td>
<td>Communication</td>
</tr>
<tr>
<td>3220</td>
<td>Alarm</td>
<td>Log data hash check failed (Log data altered)</td>
<td>Communication</td>
</tr>
<tr>
<td>3230</td>
<td>Alarm</td>
<td>TCP communication with security log publisher failed</td>
<td>Communication</td>
</tr>
<tr>
<td>3250</td>
<td>Alarm</td>
<td>TCP communication with security log server failed - Event not sent</td>
<td>Communication</td>
</tr>
<tr>
<td>Event ID</td>
<td>Type</td>
<td>Event Description</td>
<td>SDM600 Event Category</td>
</tr>
<tr>
<td>---------</td>
<td>--------</td>
<td>--------------------------------------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>3290</td>
<td>Alarm</td>
<td>Ethernet connection failure</td>
<td>Communication</td>
</tr>
<tr>
<td>3420</td>
<td>Alarm</td>
<td>Security log file deleted by user</td>
<td>Potential Security Violation</td>
</tr>
<tr>
<td>3430</td>
<td>Event</td>
<td>SEC_Security log file deleted by system</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>3440</td>
<td>Alarm</td>
<td>Security logs edited by user</td>
<td>Potential Security Violation</td>
</tr>
<tr>
<td>3710</td>
<td>Event</td>
<td>CAM server communication successful</td>
<td>Security Operation</td>
</tr>
<tr>
<td>3810</td>
<td>Alarm</td>
<td>CAM server communication failed</td>
<td>Security Operation</td>
</tr>
<tr>
<td>4110</td>
<td>Event</td>
<td>SSL connection successful</td>
<td>Security Operation</td>
</tr>
<tr>
<td>4120</td>
<td>Alarm</td>
<td>SSL connection/certificate accepted</td>
<td>Security Operation</td>
</tr>
<tr>
<td>4210</td>
<td>Alarm</td>
<td>SSL connection failed - Certificate validation failed</td>
<td>Potential Security Violation</td>
</tr>
<tr>
<td>4220</td>
<td>Alarm</td>
<td>SSL connection failed - IKE failed</td>
<td>Potential Security Violation</td>
</tr>
<tr>
<td>4310</td>
<td>Event</td>
<td>VPN connection successful</td>
<td>Security Operation</td>
</tr>
<tr>
<td>4350</td>
<td>Alarm</td>
<td>VPN connection failed - Negotiation failed</td>
<td>Potential Security Violation</td>
</tr>
<tr>
<td>4360</td>
<td>Alarm</td>
<td>VPN connection failed - IKE failed</td>
<td>Potential Security Violation</td>
</tr>
<tr>
<td>5110</td>
<td>Event</td>
<td>Manual reset</td>
<td>System Operation</td>
</tr>
<tr>
<td>5120</td>
<td>Event</td>
<td>Reset trips</td>
<td>System Operation</td>
</tr>
<tr>
<td>5130</td>
<td>Event</td>
<td>Reset LEDs</td>
<td>System Operation</td>
</tr>
<tr>
<td>5140</td>
<td>Event</td>
<td>Protection system restarted</td>
<td>System Operation</td>
</tr>
<tr>
<td>5150</td>
<td>Alarm</td>
<td>Control system restarted</td>
<td>System Operation</td>
</tr>
<tr>
<td>5152</td>
<td>Alarm</td>
<td>Control system restarted</td>
<td>System Operation</td>
</tr>
<tr>
<td>5160</td>
<td>Event</td>
<td>Gateway/RTU restarted</td>
<td>System Operation</td>
</tr>
<tr>
<td>5270</td>
<td>Alarm</td>
<td>System startup</td>
<td>System Operation</td>
</tr>
<tr>
<td>5272</td>
<td>Alarm</td>
<td>System startup failed</td>
<td>System Operation</td>
</tr>
<tr>
<td>5280</td>
<td>Event</td>
<td>System shutting down</td>
<td>System Operation</td>
</tr>
<tr>
<td>6110</td>
<td>Event</td>
<td>Test Mode started</td>
<td>System Operation</td>
</tr>
<tr>
<td>6112</td>
<td>Event</td>
<td>Starting of Test Mode failed</td>
<td>System Operation</td>
</tr>
<tr>
<td>6120</td>
<td>Event</td>
<td>Test Mode ended</td>
<td>System Operation</td>
</tr>
<tr>
<td>6130</td>
<td>Event</td>
<td>Control operation performed successfully</td>
<td>System Operation</td>
</tr>
<tr>
<td>6132</td>
<td>Event</td>
<td>Failed to perform a control operation</td>
<td>System Operation</td>
</tr>
<tr>
<td>6140</td>
<td>Event</td>
<td>Signal forced - value changed</td>
<td>System Operation</td>
</tr>
<tr>
<td>6150</td>
<td>Event</td>
<td>Test Event - to test routing configuration</td>
<td>System Operation</td>
</tr>
<tr>
<td>6160</td>
<td>Event</td>
<td>General command performed successfully</td>
<td>System Operation</td>
</tr>
<tr>
<td>6162</td>
<td>Event</td>
<td>Failed to perform a general command</td>
<td>System Operation</td>
</tr>
<tr>
<td>6170</td>
<td>Event</td>
<td>Simulation Mode started</td>
<td>System Operation</td>
</tr>
<tr>
<td>6172</td>
<td>Event</td>
<td>Starting of Simulation Mode failed</td>
<td>System Operation</td>
</tr>
<tr>
<td>6175</td>
<td>Event</td>
<td>Simulation Mode ended</td>
<td>System Operation</td>
</tr>
<tr>
<td>6180</td>
<td>Event</td>
<td>Blocked Mode started</td>
<td>System Operation</td>
</tr>
<tr>
<td>6182</td>
<td>Event</td>
<td>Blocked of Simulation Mode failed</td>
<td>System Operation</td>
</tr>
<tr>
<td>Event ID</td>
<td>Type</td>
<td>Event Description</td>
<td>SDM600 Event Category</td>
</tr>
<tr>
<td>----------</td>
<td>----------</td>
<td>-----------------------------------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>6185</td>
<td>Event</td>
<td>Blocked Mode ended</td>
<td>System Operation</td>
</tr>
<tr>
<td>6210</td>
<td>Event</td>
<td>System time set manually successfully</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>6310</td>
<td>Event</td>
<td>System time set manually failed</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>6497</td>
<td>Alarm</td>
<td>Antivirus general info event, see antivirus logs for details</td>
<td>Security Operation</td>
</tr>
<tr>
<td>6498</td>
<td>Alarm</td>
<td>Antivirus general warning event, see antivirus logs for details</td>
<td>Security Operation</td>
</tr>
<tr>
<td>6499</td>
<td>Alarm</td>
<td>Antivirus general error event, see antivirus logs for details</td>
<td>Security Operation</td>
</tr>
<tr>
<td>6510</td>
<td>Alarm</td>
<td>Debug mode started successfully</td>
<td>System Maintenance</td>
</tr>
<tr>
<td>6515</td>
<td>Alarm</td>
<td>Starting Debug Mode failed</td>
<td>System Maintenance</td>
</tr>
<tr>
<td>6520</td>
<td>Event</td>
<td>Debug Mode ended</td>
<td>System Maintenance</td>
</tr>
<tr>
<td>6550</td>
<td>Event</td>
<td>Protocol logging mode started</td>
<td>System Maintenance</td>
</tr>
<tr>
<td>6560</td>
<td>Event</td>
<td>Protocol logging mode ended</td>
<td>System Maintenance</td>
</tr>
<tr>
<td>6570</td>
<td>Event</td>
<td>Service started successfully</td>
<td>System Operation</td>
</tr>
<tr>
<td>6571</td>
<td>Event</td>
<td>Service enabled successfully</td>
<td>System Operation</td>
</tr>
<tr>
<td>6572</td>
<td>Alarm</td>
<td>Failed to start service</td>
<td>System Operation</td>
</tr>
<tr>
<td>6573</td>
<td>Alarm</td>
<td>Failed to enable service</td>
<td>System Operation</td>
</tr>
<tr>
<td>6575</td>
<td>Alarm</td>
<td>Service stopped successfully</td>
<td>System Operation</td>
</tr>
<tr>
<td>6577</td>
<td>Alarm</td>
<td>Stopping of service failed</td>
<td>System Operation</td>
</tr>
<tr>
<td>6578</td>
<td>Event</td>
<td>Task started successfully</td>
<td>System Operation</td>
</tr>
<tr>
<td>6579</td>
<td>Alarm</td>
<td>Failed to start task</td>
<td>System Operation</td>
</tr>
<tr>
<td>6580</td>
<td>Event</td>
<td>Data capturing started successfully</td>
<td>System Operation</td>
</tr>
<tr>
<td>6582</td>
<td>Event</td>
<td>Start of data capturing failed</td>
<td>System Operation</td>
</tr>
<tr>
<td>6585</td>
<td>Event</td>
<td>Data capturing stopped successfully</td>
<td>System Operation</td>
</tr>
<tr>
<td>6587</td>
<td>Event</td>
<td>Stopping of data capturing failed</td>
<td>System Operation</td>
</tr>
<tr>
<td>6590</td>
<td>Alarm</td>
<td>MCM configuration changed successfully</td>
<td>System Operation</td>
</tr>
<tr>
<td>6592</td>
<td>Alarm</td>
<td>Change of MCM configuration failed</td>
<td>System Operation</td>
</tr>
<tr>
<td>6595</td>
<td>Alarm</td>
<td>MCM configuration reset successfully</td>
<td>System Operation</td>
</tr>
<tr>
<td>6597</td>
<td>Alarm</td>
<td>Resetting of MCM configuration failed</td>
<td>System Operation</td>
</tr>
<tr>
<td>7110</td>
<td>Event</td>
<td>Switching device open</td>
<td>System Operation</td>
</tr>
<tr>
<td>7120</td>
<td>Event</td>
<td>Switching device close</td>
<td>System Operation</td>
</tr>
<tr>
<td>7310</td>
<td>Alarm</td>
<td>Hardware change detected</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>8010</td>
<td>Alarm</td>
<td>Recovery of previous configuration successful</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>8020</td>
<td>Event</td>
<td>Date and time set successfully</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>8030</td>
<td>Event</td>
<td>New certificate generated successfully</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>Event ID</td>
<td>Type</td>
<td>Event Description</td>
<td>SDM600 Event Category</td>
</tr>
<tr>
<td>----------</td>
<td>----------</td>
<td>--------------------------------------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>8040</td>
<td>Event</td>
<td>Communication system startup successful</td>
<td>System Operation</td>
</tr>
<tr>
<td>8050</td>
<td>Event</td>
<td>System backup performed successfully</td>
<td>System Operation</td>
</tr>
<tr>
<td>8060</td>
<td>Event</td>
<td>System backup started successfully</td>
<td>System Operation</td>
</tr>
<tr>
<td>8070</td>
<td>Event</td>
<td>System restore performed successfully</td>
<td>System Operation</td>
</tr>
<tr>
<td>8080</td>
<td>Event</td>
<td>System restore started successfully</td>
<td>System Operation</td>
</tr>
<tr>
<td>8210</td>
<td>Alarm</td>
<td>Recovery of previous configuration failed</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>8220</td>
<td>Event</td>
<td>Date and time setting failed</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>8230</td>
<td>Event</td>
<td>New certificate generation failed</td>
<td>System Operation</td>
</tr>
<tr>
<td>8240</td>
<td>Event</td>
<td>Communication system startup failed</td>
<td>System Operation</td>
</tr>
<tr>
<td>8250</td>
<td>Event</td>
<td>System backup failed</td>
<td>System Operation</td>
</tr>
<tr>
<td>8260</td>
<td>Event</td>
<td>Failed to start system backup</td>
<td>System Operation</td>
</tr>
<tr>
<td>8270</td>
<td>Event</td>
<td>Failed to restore the system</td>
<td>System Operation</td>
</tr>
<tr>
<td>8280</td>
<td>Event</td>
<td>Failed to start system restore</td>
<td>System Operation</td>
</tr>
<tr>
<td>9010</td>
<td>Alarm</td>
<td>Flooding attack detected</td>
<td>Potential Security Violation</td>
</tr>
<tr>
<td>9020</td>
<td>Alarm</td>
<td>Malformed packets attack detected</td>
<td>Potential Security Violation</td>
</tr>
<tr>
<td>9030</td>
<td>Alarm</td>
<td>Intrusion detected or Application blocked</td>
<td>Potential Security Violation</td>
</tr>
<tr>
<td>9040</td>
<td>Alarm</td>
<td>Intrusion detected</td>
<td>Potential Security Violation</td>
</tr>
<tr>
<td>9050</td>
<td>Alarm</td>
<td>Intrusion detected or Application blocked</td>
<td>Potential Security Violation</td>
</tr>
<tr>
<td>9060</td>
<td>Alarm</td>
<td>IDS detected unknown traffic</td>
<td>Potential Security Violation</td>
</tr>
<tr>
<td>9070</td>
<td>Alarm</td>
<td>IDS detected illegal traffic</td>
<td>Potential Security Violation</td>
</tr>
<tr>
<td>9080</td>
<td>Alarm</td>
<td>IDS detected missing traffic</td>
<td>Potential Security Violation</td>
</tr>
<tr>
<td>9110</td>
<td>Alarm</td>
<td>Firewall blocked incoming connection</td>
<td>Potential Security Violation</td>
</tr>
<tr>
<td>9120</td>
<td>Alarm</td>
<td>Firewall blocked outgoing connection</td>
<td>Potential Security Violation</td>
</tr>
<tr>
<td>9130</td>
<td>Alarm</td>
<td>Firewall stopped/disabled</td>
<td>Security Operation</td>
</tr>
<tr>
<td>9140</td>
<td>Alarm</td>
<td>Firewall started/enabled</td>
<td>Security Operation</td>
</tr>
<tr>
<td>9150</td>
<td>Alarm</td>
<td>Firewall settings/rules changed successfully</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>9210</td>
<td>Alarm</td>
<td>IPS blocked incoming packet</td>
<td>Potential Security Violation</td>
</tr>
<tr>
<td>9220</td>
<td>Alarm</td>
<td>IPS blocked incoming packet</td>
<td>Potential Security Violation</td>
</tr>
<tr>
<td>9230</td>
<td>Alarm</td>
<td>IPS stopped/disabled</td>
<td>Security Operation</td>
</tr>
<tr>
<td>9240</td>
<td>Alarm</td>
<td>IPS started/enabled</td>
<td>Security Operation</td>
</tr>
<tr>
<td>9250</td>
<td>Alarm</td>
<td>IPS settings/rules changed successfully</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>9510</td>
<td>Alarm</td>
<td>CSR approved and certificate issued successfully</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>9520</td>
<td>Alarm</td>
<td>Certificate signing request failed</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>Event ID</td>
<td>Type</td>
<td>Event Description</td>
<td>SDM600 Event Category</td>
</tr>
<tr>
<td>----------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>9610</td>
<td>Alarm</td>
<td>Certificate validation succeeded</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>9620</td>
<td>Alarm</td>
<td>Certificate validation failed - Certificate expired</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>9630</td>
<td>Alarm</td>
<td>Certificate validation failed - Certificate revoked</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>9640</td>
<td>Alarm</td>
<td>Certificate validation failed - Certificate signature check failed</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>9990</td>
<td>Event</td>
<td>Unidentified Syslog event</td>
<td>Unknown</td>
</tr>
<tr>
<td>9991</td>
<td>Event</td>
<td>Unidentified IEC 61850 event</td>
<td>Unknown</td>
</tr>
<tr>
<td>9995</td>
<td>Alarm</td>
<td>UAL Syslog FIFO receiver overflow, message overwritten</td>
<td>Security Operation</td>
</tr>
<tr>
<td>10010</td>
<td>Event</td>
<td>Device successfully entered maintenance menu due to a user action</td>
<td>System Maintenance</td>
</tr>
<tr>
<td>10012</td>
<td>Event</td>
<td>Device failed to enter maintenance menu due to a user action</td>
<td>System Maintenance</td>
</tr>
<tr>
<td>10020</td>
<td>Event</td>
<td>Device successfully forced into maintenance menu due to new state</td>
<td>System Maintenance</td>
</tr>
<tr>
<td>10022</td>
<td>Event</td>
<td>Device failed to force maintenance menu after a new state</td>
<td>System Maintenance</td>
</tr>
<tr>
<td>10030</td>
<td>Event</td>
<td>FTP server successfully activated from maintenance menu</td>
<td>System Maintenance</td>
</tr>
<tr>
<td>10032</td>
<td>Event</td>
<td>Activation of FTP server from maintenance menu failed</td>
<td>System Maintenance</td>
</tr>
<tr>
<td>10040</td>
<td>Event</td>
<td>Firmware update procedure aborted successfully</td>
<td>System Maintenance</td>
</tr>
<tr>
<td>10042</td>
<td>Event</td>
<td>Failed to abort firmware update procedure</td>
<td>System Maintenance</td>
</tr>
<tr>
<td>10050</td>
<td>Event</td>
<td>Recovery menu entered successfully</td>
<td>System Maintenance</td>
</tr>
<tr>
<td>10052</td>
<td>Event</td>
<td>Failed to enter Recovery menu</td>
<td>System Maintenance</td>
</tr>
<tr>
<td>10060</td>
<td>Event</td>
<td>Authentication disabled from Maintenance menu successfully</td>
<td>System Maintenance</td>
</tr>
<tr>
<td>10062</td>
<td>Event</td>
<td>Failed to disable authentication from Maintenance menu</td>
<td>System Maintenance</td>
</tr>
<tr>
<td>10070</td>
<td>Event</td>
<td>Change lock disabled successfully from Maintenance menu</td>
<td>System Maintenance</td>
</tr>
<tr>
<td>10072</td>
<td>Event</td>
<td>Failed to disable change lock from Maintenance menu</td>
<td>System Maintenance</td>
</tr>
<tr>
<td>10080</td>
<td>Event</td>
<td>IEC 61850 disabled successfully from Maintenance menu</td>
<td>System Maintenance</td>
</tr>
<tr>
<td>10082</td>
<td>Event</td>
<td>Failed to disable IEC 61850 from Maintenance menu</td>
<td>System Maintenance</td>
</tr>
<tr>
<td>13200</td>
<td>Event</td>
<td>Configuration transferred to the device successfully</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>13210</td>
<td>Event</td>
<td>Configuration transfer to the device started</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>13220</td>
<td>Event</td>
<td>Configuration changed successfully</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>13250</td>
<td>Event</td>
<td>Entered configuration mode successfully</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>13260</td>
<td>Event</td>
<td>Exited configuration mode successfully</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>Event ID</td>
<td>Type</td>
<td>Event Description</td>
<td>SDM600 Event Category</td>
</tr>
<tr>
<td>----------</td>
<td>---------</td>
<td>------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>13300</td>
<td>Event</td>
<td>Configuration files read/exported from the device successfully</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>13310</td>
<td>Event</td>
<td>Configuration exporting from the device started successfully</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>13400</td>
<td>Event</td>
<td>Firmware transferred to the device successfully</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>13500</td>
<td>Event</td>
<td>Firmware files read/exported from the device successfully</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>13520</td>
<td>Event</td>
<td>Certificates transferred to the device successfully</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>13560</td>
<td>Event</td>
<td>Exported/read archive file from the device successfully</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>13570</td>
<td>Event</td>
<td>Exported/read diagnosis file from the device successfully</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>13580</td>
<td>Event</td>
<td>Exported/read certificates from device successfully</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>13900</td>
<td>Alarm</td>
<td>Security logs read/exported from the device successfully</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>13910</td>
<td>Alarm</td>
<td>Security logs report generated successfully</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>14200</td>
<td>Event</td>
<td>Failed to transfer configuration to the device</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>14210</td>
<td>Event</td>
<td>Failed to start transfer of configuration to the device</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>14220</td>
<td>Event</td>
<td>Failed to change the configuration</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>14250</td>
<td>Event</td>
<td>Failed to enter configuration mode</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>14260</td>
<td>Event</td>
<td>Failed to exit configuration mode</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>14300</td>
<td>Event</td>
<td>Failed to read configuration files from the device</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>14310</td>
<td>Event</td>
<td>Failed to start export of configuration from the device</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>14400</td>
<td>Event</td>
<td>Failed to transfer firmware to the device</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>14500</td>
<td>Event</td>
<td>Failed to read firmware files from the device</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>14520</td>
<td>Event</td>
<td>Failed to transfer certificates to the device</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>14560</td>
<td>Event</td>
<td>Failed to read archive file from the device</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>14570</td>
<td>Event</td>
<td>Failed to read diagnosis file from the device</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>14580</td>
<td>Event</td>
<td>Failed to read certificates from the device</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>Event ID</td>
<td>Type</td>
<td>Event Description</td>
<td>SDM600 Event Category</td>
</tr>
<tr>
<td>----------</td>
<td>-----------</td>
<td>-------------------------------------------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>14900</td>
<td>Event</td>
<td>Failed to read security logs from the device</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>14910</td>
<td>Alarm</td>
<td>Failed to generate security logs report</td>
<td>Security Administration and Configuration</td>
</tr>
<tr>
<td>23100</td>
<td>Event</td>
<td>Password file transferred and stored in the device successfully</td>
<td>Security Operation</td>
</tr>
<tr>
<td>23200</td>
<td>Event</td>
<td>Password file read/exported from the device successfully</td>
<td>Security Operation</td>
</tr>
<tr>
<td>23500</td>
<td>Event</td>
<td>Failed to transfer password file to the device</td>
<td>Security Operation</td>
</tr>
<tr>
<td>23600</td>
<td>Event</td>
<td>Failed to read password file from the device</td>
<td>Security Operation</td>
</tr>
<tr>
<td>15010</td>
<td>Event</td>
<td>Controller mode changed to configuration mode successfully</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>15020</td>
<td>Event</td>
<td>Controller mode changed to execute mode successfully</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>15110</td>
<td>Alarm</td>
<td>Controller mode change to configuration mode failed</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>15120</td>
<td>Alarm</td>
<td>Controller mode change to execute mode failed</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>15200</td>
<td>Event</td>
<td>Bus IF mounted successfully</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>15210</td>
<td>Event</td>
<td>Bus IF unmounted successfully</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>15220</td>
<td>Event</td>
<td>Global device configuration updated successfully</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>15230</td>
<td>Event</td>
<td>Configuration data initialized successfully</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>15240</td>
<td>Event</td>
<td>Complete configuration data reloaded successfully</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>15250</td>
<td>Event</td>
<td>CCO converted module process variables removed successfully</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>15260</td>
<td>Event</td>
<td>Function diagrams commissioned successfully</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>15270</td>
<td>Event</td>
<td>CCO process variable parameterized successfully</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>15280</td>
<td>Event</td>
<td>Single parameter parameterized successfully</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>15290</td>
<td>Event</td>
<td>Single parameter simulated successfully</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>15300</td>
<td>Event</td>
<td>Bus IF mounting failed</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>15310</td>
<td>Event</td>
<td>Bus IF unmounting failed</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>15320</td>
<td>Alarm</td>
<td>Global device configuration update failed</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>15330</td>
<td>Event</td>
<td>Configuration data initialization failed</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>Event ID</td>
<td>Type</td>
<td>Event Description</td>
<td>SDM600 Event Category</td>
</tr>
<tr>
<td>----------</td>
<td>---------</td>
<td>-----------------------------------------------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>15340</td>
<td>Event</td>
<td>Complete configuration data reload failed</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>15350</td>
<td>Event</td>
<td>CCO converted module process variables removal failed</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>15360</td>
<td>Event</td>
<td>Function diagrams commissioning failed</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>15370</td>
<td>Event</td>
<td>CCO process variable parametrization failed</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>15380</td>
<td>Event</td>
<td>Single parameter parametrization failed</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>15390</td>
<td>Event</td>
<td>Single parameter simulation failed</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>15410</td>
<td>Event</td>
<td>Profibus master/slave configured successfully</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>15420</td>
<td>Event</td>
<td>Profibus channel configured successfully</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>15430</td>
<td>Event</td>
<td>Profibus parameterized channel configured successfully</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>15440</td>
<td>Event</td>
<td>Profibus master/slave configuration reloaded successfully</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>15450</td>
<td>Event</td>
<td>Profibus channel configuration reloaded successfully</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>15510</td>
<td>Alarm</td>
<td>Profibus master/slave configuration failed</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>15520</td>
<td>Alarm</td>
<td>Profibus channel configuration failed</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>15530</td>
<td>Alarm</td>
<td>Profibus parameterized channel configuration failed</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>15540</td>
<td>Event</td>
<td>Profibus master/slave configuration reload failed</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>15550</td>
<td>Event</td>
<td>Profibus channel configuration reload failed</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>15610</td>
<td>Event</td>
<td>IEC 61850 stack initialized successfully</td>
<td>System Operation</td>
</tr>
<tr>
<td>15620</td>
<td>Event</td>
<td>IEC 61850 stack configured successfully</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>15630</td>
<td>Event</td>
<td>IEC 61850 stack configuration reloaded successfully</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>15640</td>
<td>Event</td>
<td>IEC 61850 stack configuration reload failed</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>15710</td>
<td>Event</td>
<td>IEC 61850 stack initialization failed</td>
<td>System Operation</td>
</tr>
<tr>
<td>15720</td>
<td>Alarm</td>
<td>IEC 61850 stack configuration failed</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>15730</td>
<td>Event</td>
<td>IEC 61850 stack configuration reload failed</td>
<td>System Engineering and Configuration</td>
</tr>
<tr>
<td>15810</td>
<td>Event</td>
<td>Control parameter read and view from device successfully</td>
<td>System Operation</td>
</tr>
<tr>
<td>15850</td>
<td>Event</td>
<td>Operable parameters read from device into project data base successfully</td>
<td>System Operation</td>
</tr>
<tr>
<td>Event ID</td>
<td>Type</td>
<td>Event Description</td>
<td>SDM600 Event Category</td>
</tr>
<tr>
<td>---------</td>
<td>------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>15860</td>
<td>Event</td>
<td>Operable parameters transferred and stored into the device successfully</td>
<td>System Operation</td>
</tr>
<tr>
<td>15890</td>
<td>Event</td>
<td>Generic DTM event</td>
<td>System Operation</td>
</tr>
<tr>
<td>15910</td>
<td>Event</td>
<td>Failed to read control value parameter from device</td>
<td>System Operation</td>
</tr>
<tr>
<td>15950</td>
<td>Event</td>
<td>Failed to read operable parameters from device into project database</td>
<td>System Operation</td>
</tr>
<tr>
<td>15960</td>
<td>Event</td>
<td>Failed to transfer and store operable parameters into the device</td>
<td>System Operation</td>
</tr>
</tbody>
</table>
### Appendix B. Mapping Windows Events to ABB SDM600 Security Event EventIDs

<table>
<thead>
<tr>
<th>EventID</th>
<th>Successful Windows Event result</th>
<th>Fail Windows Event Result</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1102</td>
<td>3420</td>
<td></td>
<td>Security log file deleted by user</td>
</tr>
<tr>
<td>4608</td>
<td>5270</td>
<td>5272</td>
<td>System startup</td>
</tr>
<tr>
<td>4609</td>
<td>5280</td>
<td></td>
<td>System shutting down</td>
</tr>
<tr>
<td>4616</td>
<td>8020</td>
<td>8220</td>
<td>Date and time set</td>
</tr>
<tr>
<td>4624</td>
<td>1110</td>
<td></td>
<td>Login successful</td>
</tr>
<tr>
<td>4625</td>
<td></td>
<td>1130</td>
<td>Login failed</td>
</tr>
<tr>
<td>4634</td>
<td>1210</td>
<td></td>
<td>Logout (user logged out)</td>
</tr>
<tr>
<td>4647</td>
<td>1210</td>
<td></td>
<td>Logout (user logged out)</td>
</tr>
<tr>
<td>4649</td>
<td>9020</td>
<td></td>
<td>Flooding attack detected</td>
</tr>
<tr>
<td>4650, 4651</td>
<td>4310</td>
<td>4350</td>
<td>VPN connection</td>
</tr>
<tr>
<td>4652, 4653, 4654</td>
<td>4350</td>
<td></td>
<td>VPN connection failed - Negotiation failed</td>
</tr>
<tr>
<td>4704</td>
<td>2162</td>
<td>2232</td>
<td>Permission added</td>
</tr>
<tr>
<td>4705</td>
<td>2172</td>
<td>2272</td>
<td>User permission removed</td>
</tr>
<tr>
<td>4720</td>
<td>2110</td>
<td>2130</td>
<td>User account created</td>
</tr>
<tr>
<td>4722</td>
<td>2115</td>
<td>2135</td>
<td>User account enabled</td>
</tr>
<tr>
<td>4723</td>
<td>2220</td>
<td>2220</td>
<td>Change of user password failed</td>
</tr>
<tr>
<td>4724</td>
<td>2220</td>
<td>2220</td>
<td>Change of user password failed</td>
</tr>
<tr>
<td>4725</td>
<td>2117</td>
<td>2137</td>
<td>User account disabled</td>
</tr>
<tr>
<td>4726</td>
<td>2120</td>
<td>2140</td>
<td>User account deleted</td>
</tr>
<tr>
<td>4774</td>
<td>1110</td>
<td>1130</td>
<td>Login</td>
</tr>
<tr>
<td>4775</td>
<td>1130</td>
<td>1130</td>
<td>Login failed - Wrong credentials</td>
</tr>
<tr>
<td>4887</td>
<td>9510</td>
<td>9520</td>
<td>CSR approved and certificate issued successfully</td>
</tr>
<tr>
<td>4888</td>
<td>9520</td>
<td></td>
<td>Certificate signing request failed</td>
</tr>
<tr>
<td>4946, 4947, 4948, 4950</td>
<td>9150</td>
<td></td>
<td>Firewall settings/rules changed</td>
</tr>
<tr>
<td>EventID</td>
<td>Successful Windows Event result</td>
<td>Fail Windows Event Result</td>
<td>Event Description</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------------</td>
<td>---------------------------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>4976, 4977, 4978</td>
<td>4350</td>
<td>4350</td>
<td>VPN connection failed - Negotiation failed</td>
</tr>
<tr>
<td>4979, 4980, 4981, 4982</td>
<td>4310</td>
<td>4350</td>
<td>VPN connection successful</td>
</tr>
<tr>
<td>4983, 4984</td>
<td>4350</td>
<td>4350</td>
<td>VPN connection failed - Negotiation failed</td>
</tr>
<tr>
<td>5031</td>
<td>9110</td>
<td></td>
<td>Firewall blocked incoming connection</td>
</tr>
<tr>
<td>5148</td>
<td>9010</td>
<td></td>
<td>Flooding attack detected</td>
</tr>
<tr>
<td>5152</td>
<td>9210</td>
<td>9210</td>
<td>IPS blocked incoming packet</td>
</tr>
<tr>
<td>5155</td>
<td>9110</td>
<td>9110</td>
<td>Firewall blocked incoming connection</td>
</tr>
<tr>
<td>5451</td>
<td>4310</td>
<td>4360</td>
<td>VPN connection successful</td>
</tr>
<tr>
<td>5453</td>
<td>4360</td>
<td>4360</td>
<td>VPN connection failed - IKE failed</td>
</tr>
</tbody>
</table>
### Appendix C. Self-Generated SDM600 Security Events

<table>
<thead>
<tr>
<th>EventID</th>
<th>Event Description</th>
<th>Cause of Event in SDM600</th>
</tr>
</thead>
<tbody>
<tr>
<td>1110</td>
<td>Login successful</td>
<td>When a user successfully logged into SDM600</td>
</tr>
<tr>
<td>1115</td>
<td>Password expired; login successful</td>
<td>When a user manages to log in even if the user's password has expired</td>
</tr>
<tr>
<td>1130</td>
<td>Login failed - Wrong credentials</td>
<td>When a user enters a wrong combination of username and password</td>
</tr>
<tr>
<td>1210</td>
<td>Logout (user logged out)</td>
<td>When a user logged out from SDM600</td>
</tr>
<tr>
<td>2110</td>
<td>User account created successfully</td>
<td>When a new user account is successfully created</td>
</tr>
<tr>
<td>2120</td>
<td>User account deleted successfully</td>
<td>When a user account is successfully deleted</td>
</tr>
<tr>
<td>2160</td>
<td>New role assigned to user successfully</td>
<td>When a new role is successfully assigned to a user</td>
</tr>
<tr>
<td>2161</td>
<td>Permission changed successfully</td>
<td>When a user adjusts the SDM600 role to right mapping</td>
</tr>
<tr>
<td>2170</td>
<td>User role assignment removed successfully</td>
<td>When a user role is successfully removed from a user's role assignment</td>
</tr>
<tr>
<td>2210</td>
<td>User password changed successfully</td>
<td>When a user changes their password by entering correct required credentials</td>
</tr>
<tr>
<td>2220</td>
<td>Change of user password failed</td>
<td>When a user changes their password by entering a wrong combination of the required credentials</td>
</tr>
<tr>
<td>2225</td>
<td>User data changed successfully (for example, username, etc.)</td>
<td>When a user changes their data</td>
</tr>
<tr>
<td>8030</td>
<td>New certificate generated successfully</td>
<td>When a user requests SDM600 to generate a certificate and the certificate is successfully generated</td>
</tr>
<tr>
<td>8050</td>
<td>System backup performed successfully</td>
<td>When a user requests SDM600 to perform a system backup and the request is executed successfully</td>
</tr>
<tr>
<td>8230</td>
<td>New certificate generation failed</td>
<td>When a user requests SDM600 to generate a certificate and the certificate is not successfully generated</td>
</tr>
<tr>
<td>EventID</td>
<td>Event Description</td>
<td>Cause of Event in SDM600</td>
</tr>
<tr>
<td>---------</td>
<td>-------------------------------------------</td>
<td>------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>8250</td>
<td>System backup failed</td>
<td>When a user requests SDM600 to perform a system backup and the request is not executed successfully</td>
</tr>
<tr>
<td>13200</td>
<td>Configuration transferred to the device successfully</td>
<td>When a user requests SDM600 to generate configuration files for another application or device to integrate it into ABB SDM600 Centralized Account Management and Centralized Activity Logging and the configuration files successfully generated and saved to user preferred location</td>
</tr>
<tr>
<td>13220</td>
<td>Configuration changed successfully</td>
<td>When a user conducts any configuration changes in SDM600, and the configuration is successfully applied</td>
</tr>
<tr>
<td>13520</td>
<td>Certificates transferred to the device successfully</td>
<td>When a user manages to export the credential that is used to sign certificates for all devices</td>
</tr>
<tr>
<td>14200</td>
<td>Failed to transfer configuration to the device</td>
<td>When a user requests SDM600 to generate configuration files for another application or device to integrate it into ABB 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</td>
</tr>
<tr>
<td>14220</td>
<td>Failed to change the configuration</td>
<td>When a user conducts any configuration changes in SDM600, and the configuration is not successfully applied</td>
</tr>
<tr>
<td>14520</td>
<td>Failed to transfer certificates to the device</td>
<td>When a user fails to export the credential that is used to sign certificates for all devices</td>
</tr>
</tbody>
</table>
Appendix D. **Activities generating SDM600 Configuration Changed Security Event**

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