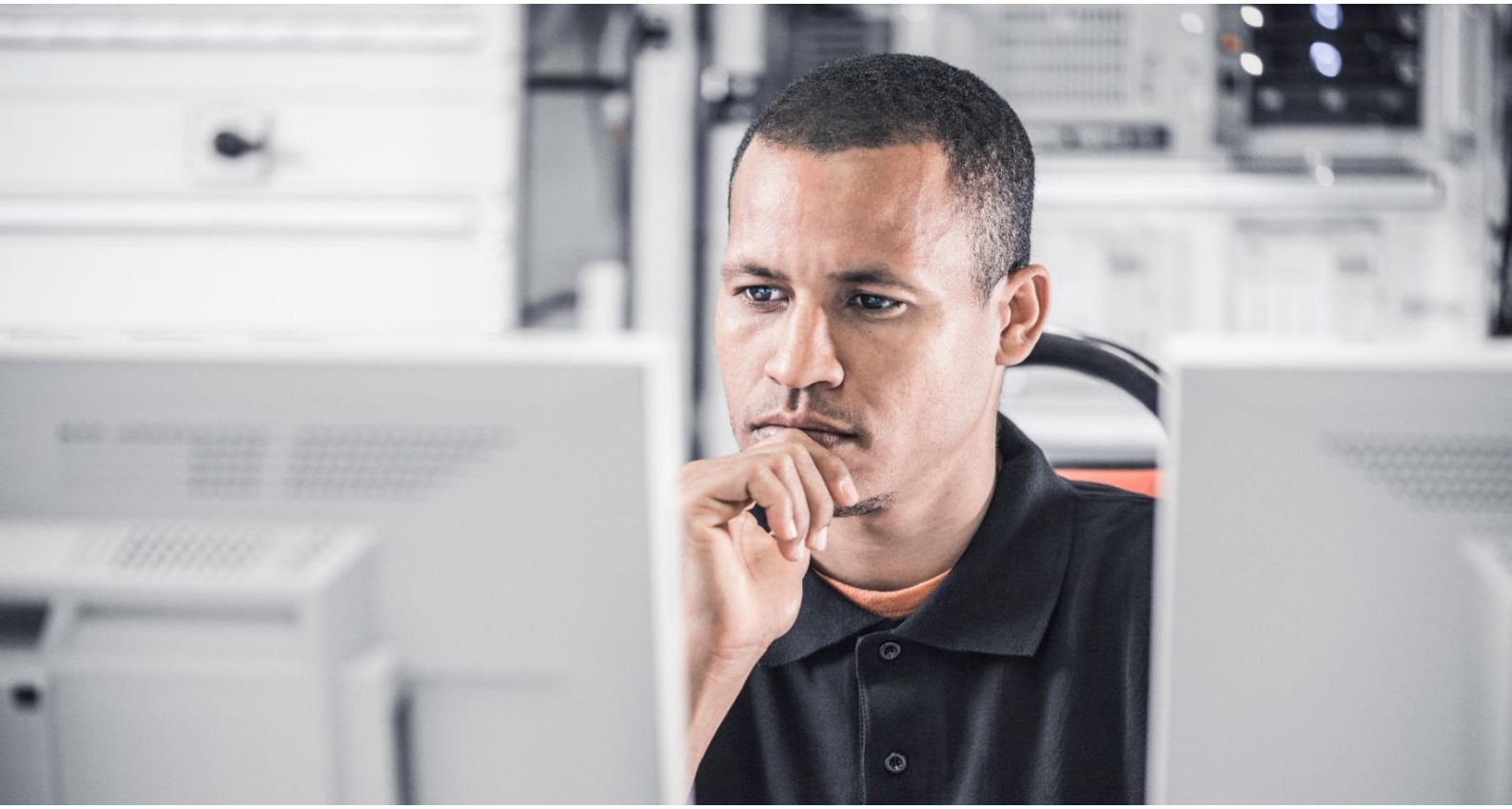
HITACHI
Inspire the Next

RELEASE NOTE | April 2023

System Data Manager – SDM600

SDM600 Ver. 1.3.1



Hitachi Energy

SDM600 1.3.1

Release Note

Introduction

This release includes new features and corrections for functional issues in SDM600.
It is a cumulative release containing all changes since the 1.2 release.

Recommendation

It is recommended to upgrade all existing SDM600 installations to this SDM600 1.3.1.
Existing licenses for SDM600 1.1 must be upgraded to use SDM600 1.2 or newer.
SDM600 has been designed to fully support the latest version of Google Chrome, which is the recommended browser.

Technical requirements and supported products

SDM600 is a generic application that supports a wide range of IEDs and other devices for its provided functionality. However, it cannot be ensured that the full functionality can be supported for all IEDs.
The supported protocols and functionality are described in the product factsheet.

Supported Operating Systems

Operating system
Windows 10 1607 LTSC and 1809 LTSC
Windows 11 21H2
Microsoft Windows Server 2016
Microsoft Windows Server 2019
Microsoft Windows Server 2022

Cyber Security Information

The following certificate is used for digital signing:
RootCA: DigiCert Trusted Root G4
Issuer: DigiCert Trusted G4 Code Signing RSA4096 SHA384 2021 CA1
Name: Hitachi Energy Ltd
Certificate Thumbprint: D5FF8F4370F9B6098B0BFC4649106B9AA2ECC086

Timestamping / Countersignatures certificate:
RootCA: DigiCert Trusted Root G4
Issuer: DigiCert Trusted G4 RSA4096 SHA256 TimeStamping CA
Name: DigiCert Timestamp 2022 - 2
Certificate Thumbprint: F387224D8633829235A994BCBD8F96E9FE1C7C73

Installer SHA256 checksum: B56447A9FB5FB5EBDD3F097E5DE4CCD962F000D75168E9D5129CC8AA9905A3DE

Documentation

Following documents are available for download:

- SDM600 Installation Guide
- SDM600 Cyber Security Deployment Guide
- SDM600 User Manual
- SDM600 Release Notes (this document)

Limitations and known issues

- SDM600 stores its data in Microsoft SQL Server 2019 Express databases.
  This variant of SQL Server has a limitation of 10GB per database (dedicated databases for disturbance recorder files, security events and configuration data are used).
  In case more than 10 GB of storage is required, the SQL Server needs to be upgraded to another edition (e.g. SQL Server Standard). This requires an additional license (product key) purchased from a local Microsoft distributor.

Drastic performance degradation has been observed even when running below the 10GB database size limitation. It is recommended to upgrade to standard SQL Server license when the DB size is larger than 7GB.

- Disturbance Recorder files with same names and file dates are not uploaded, even if the files are different (rollover of file name at the same day).

- When receiving multiple security events with identical *raw message*, SDM600 will only store and display one event. The other events will be discarded as duplicated. This is necessary to prevent *fake* duplicated messages to be created during hierarchical and hot-standby synchronization.

- Parent-Child and Hot-Standby SDM600 systems need to be in the same IP network and the default network interface must be set to the network where the SDM600 systems are connected.

- Accessing SDM600 via Remote Desktop Protocol (RDP) might lead to refresh / caching issues and is not recommended. Use the internet browser with https to access SDM600.

- When using SDM600 for RTU500 file management, it is recommended to use a dedicated user account (a service or technical account name) for the SDM600-RTU connection. Only when using a dedicated account, it can be ensured that the SDM600 caused Login/Logout events are filtered out correctly.

- Central Account Management for Windows Computer will not work for Windows 10 Version 1903 and newer.

- CSV format is currently not supported for receiving and processing of syslog messages, because it is not compliant with RFC 5424 syslog format.

- The SDM600 Standby system might appear as red immediately after HSB setup procedure; in this event, restart the SDM600 Services on the Standby PC (or the whole PC) to resolve the issue. Depending on the size to the Database, several minutes might be required for the data to be synchronized. The HSB will be available once the data have been fully synchronized.

- After updating a system to a newer SDM600 version, the re-provisioning operation is triggered.
  Because of changes in the database schema, the metadata used to synchronize SDM600 instances is no longer valid. Re-provisioning is required for synchronization to work correctly, after changes in the database schema between different SDM600 versions. Re-provisioning clears collected metadata and triggers an initial data synchronization that may take a long time. Please wait and don’t interrupt the synchronization procedure.

- To ensure the correct functionality, “Pop-up Blockers” must be configured in the browser to allow pop-ups on SDM600 website.

Installation

SDM600 is a web-based client / server system. SDM600 will be installed on a computer that can communicate with the supervised IEDs, computers and other devices. The user interface of SDM600 can be opened from the web browser either locally or from a remote computer.
The installation is described in the SDM600 Installation Guide.
SDM600 requires a license key to function during start-up and runtime.

Do not forget to **backup** and **redeploy** any modified configuration files such as ftp response parsing files (ftp_regex.txt), Radius Role2Right mapping (CAMRoleToRadiusRights.xml) or own Device Templates **before** re-installation. Always check for changes in the template files delivered with a new SDM600 installation before restoring your modified configuration.

SDM600 needs to be installed using the SDM600 installer also in virtual environments. **Simply cloning virtual machines will lead to non-functional SDM600** (unique keys and certificates which are created by the installer are required on each instance of SDM600).

Each instance of SDM600 requires unique keys and certificates. The certificates are part of the SDM600 backup, therefore **backup restoration as basis for a new SDM600 configuration in production environments is not recommended -** specifically with Parent / Child or Hot-Standby configurations.

It is recommended to **restart the computer before SDM600 installation**, specifically after uninstalling ABB Authentication Service or any other software component that forces a reboot.

SDM600 installation might fail due to MS SQL Server installation problems.
The SQL Server installation requires certain registry keys to be in place. They are added during the installation of Microsoft Edge, which creates a prerequisite on having Edge installed to successfully run the SQL Installation (and therefore the SDM Installer).
In case the SDM Installer fails due to the SQL Server installer, make sure to:

- Install Microsoft Edge if you have not yet
- Update to the latest version of Edge if it's already installed

Additionally, it has been observed that this can be resolved by **changing the Regional and Language Settings to English (United States) (en-US) during the installation process**.
After that, rerun the installation.

Upgrade

Existing SDM600 1.2 licenses are valid for SDM600 1.3.1.
Upgrading to SDM600 1.3.1 from previous versions of SDM600 is performed by installing SDM600 1.3.1 on an existing SDM600 system (including previous Service Pack or Feature Pack releases).
Before upgrading an existing system to 1.3.1, it is best practice and highly recommended to create a SDM600 backup first.

"Clearing Browsing Data" on the browser is required after the upgrade has been completed.
This operation ensures the browser is not displaying an older, cached version of SDM600.

A computer restart is required after the installation has been completed.
This operation improves the stability of the system.

SQL Server 2012 is officially no longer supported by Microsoft.
Starting from SDM600 1.2 FP3 HF3, the product is delivered with SQL Server 2019.
Starting from SDM600 1.3.1, it is mandatory to update to SQL Server 2019 to keep using the product.
Refer to the "MS SQL Server 2019 Migration Workflow" document for extensive guidance.

To upgrade Parent-Child systems, it is no longer required to disconnect all child systems from the parent.
Install SDM600 1.3.1 on top of current SDM600 installation.

To upgrade Hot-Standby Systems, stop all SDM600 Services first on the Standby System then on the Hot System, upgrade SDM600 instances to 1.3.1 and re-start services.

In case SDM600 login screen is not shown after re-installation and computer reboot, please check certificate binding in IIS configuration. When the certificate is deleted manually from the certificate store, it can happen that the binding is not re-configured.

Some releases contain improvements of the *Windows Event Log Forwarder* and *Windows Agent* components. To benefit from those changes, it is required to upgrade to the latest version of the components on all configured computers. Manually uninstall previous Versions via "Add Remove Programs", download the new installation packages from SDM600 and re-install the components.

After upgrading to 1.2 FP3 (or newer) from any 1.2 FP2 version, all existing *Windows Agent* configuration files must be updated. Refer to SDM600 Installation Guide for further information.

Silverlight is officially no longer supported by Microsoft.
The SDM600 Silverlight User Interface is no longer supported – all the improvements, bug fixes and new features will be carried out on the new React user interface available in version 1.2 FP3 (and newer).

All releases and included changes since SDM600 1.2

SDM600 1.3.1 (2023-04)

New and enhanced features
SDM600 will no longer support Microsoft SQL Server 2012 due to its end of life and to ensure product safety and security. This change was previously announced in September 2022, and we highly recommend customers migrate to SQL Server 2019 for better support and performance. The migration procedure is documented and available via the SDM600 installer.
Microsoft Windows Server 2012 is no longer supported, as it does not achieve the minimum requirements for Microsoft SQL Server 2019. Microsoft Windows Server 2022 is now officially supported.
The SDM600 User Interface can now be displayed in different languages: English (United States), German (Germany), Spanish (Spain) and Swedish (Sweden).
To increase the configuration efficiency, SDM600 introduced the possibility to clone the existing configuration from one source device to several target devices. This functionality enables the user to edit the required configuration parameters on a single device and then replicate the configuration on other target devices. To maximize the flexibility, the user can decide which configuration parameters to clone from the source to the target devices. Replicate a device's configuration on multiple devices by selecting them in the tree view, right-clicking on the source device, and choosing "Clone Configuration". Refer to the User Manual for more details.
To improve the efficiency while navigating through the devices, the tree view is displayed as collapsed by default. "Expand All" and "Collapse All" actions are available as context menu entries to quickly allow the user to expand and/or collapse all groups. Finally, to provide a more consistent navigation, the tree view will keep the status while navigating across different tabs.
A new, improved, and Hitachi Energy branded version of WaveWin has been integrated in SDM600. The installer for WaveWin 3.0.0.0 can be downloaded from the SDM600's download section.
SNMP support has been extended. Authentication now supports MD5 (obsolete), SHA1 (obsolete), SHA256, SHA384, SHA512. Privacy now supports DES (obsolete), AES, AES192, AES256.
"Device Path" has been reintroduced and it is now available for all the grids in the "Events Monitoring" section. By default, the "Device Path" is hidden, and must be manually selected in the "Column Chooser" to be visible in the grids.
General fixes and improvements
Fixed an issue that prevented users from being synchronized between parent and child instances. The issue occurred on operating systems using the German language and was caused by incorrect certificate checks. To address this, we reworked the certificate handling process, eliminating the use of strings and regular expressions to prevent erroneous failed checks.
Fixed an issue preventing milliseconds to be correctly parsed from the raw syslog message. Both the Local Time and UTC Time now contains the correctly parsed time stamp, including the milliseconds.
When creating the backup from the "SDM600 Application Administration Tool", it is now possible to select the target folder and the filename of the backup file.
In the "Fleet Management" tab, the "Created Date" value is now localized according to the language settings of the browser.
As part of our continuous effort to deliver secure and reliable software, SDM600 strengthened its cyber security position by hardening the configuration of the Microsoft SQL Server. Additional details are available in the SDM600 Cyber Security Deployment Guide
Fixed an issue causing the *DRSelector* application to occasionally open the wrong DR file when the “Inspect” (looking glass icon) functionality is used. The *DRSelector* is the client-side application used to open any DR file with the user selected application (default is Wavewin).

–

SDM600 1.3.0 (2023-02)

New and enhanced features
Active Directory Integration is now supported and can be configured in the "Account Management" area. When Active Directory integration is enabled, SDM600 will act as a device and authenticate the users against the Active Directory accounts. CAM for devices is not supported when SDM600 is configured to authenticate against Active Directory. Multiple "Domain Controllers" can be configured to increase the availability. "Emergency Users" are also available in SDM600 to ensure access to the system in the event the configured "Domain Controllers" are not available / reachable. Check the User Manual for further guidance.
Parsing of security events has been re-introduced. The following details are now visible in the Security Events data grid: Event Time (Local Time), Event Time (UTC), Device, Source, IP address, Event ID, Event Description, Username, Product Name, Raw Message.
The performance and stability have been enhanced: on bigger systems, the loading time of the events is drastically reduced.
As part of our continuous effort to deliver secure and reliable software, SDM600 strengthened its cyber security position by addressing the following cyber security vulnerabilities: • CVE-2022-3682: Unrestricted Upload of File with Dangerous Type • CVE-2022-3683: Missing Authorization • CVE-2022-3684: Unauthenticated Denial-of-Service (DoS) • CVE-2022-3687: Unauthenticated Certificate Management For more information, refer to the Cyber Security Advisory - 8DBD000138.
General fixes and improvements
Events shown in the "Event Monitoring" grids can now be sorted and filtered.
As part of the "Password Policy" handling, the workflow to handle the password expiration has been improved. A message will warn the user about the incoming password expiration. Once expired, the user can configure the new password as part of the login procedure. Check the User Manual for further guidance.
Fixed an issue causing the installer to fail when a more recent version of .NET is already installed on the system.
Fixed an issue in the custom DR export template causing the <DATE_SRV> to display a different time compared to the <TIME_SRV>.

–

SDM600 1.2 FP3 Hotfix4 release (2022-10)

New and enhanced features
The "Device Supervision" functionality has been improved to provide better support for users while troubleshooting connection and configuration issues. The connection status values have been simplified and harmonized to provide improved guidance. More details could be found in the user manual.
As part of our continuous effort to deliver secure and reliable software, SDM600 strengthened its cyber security position by removing the usage of the hardcoded credentials used to communicate with the SQL Server. During the SDM600 installation, the user is now required to enter a secure password that will be used as connection string by SDM600 towards the SQL DB. Limitations apply: When configuring the SQL Server database passwords for SDM600 instances belonging to a hierarchical and/or HSB system, the configured passwords must match! More details could be found in the User Manual and the cyber security deployment guideline.
General fixes and improvements
Fixed an issue causing DR Path to not be correctly loaded from the matching IED template.
Fixed an issue causing "Disturbance Record Retrieval Settings" to not get enabled properly when configured from the user interface.
Fixed an issue in the "SDM600 Configuration" modal dialog, causing the "SDM600 Certificate" tab to show an error message: loading other root certificates besides the SDM600 one resulted in an error when any certificate met certain conditions.
Fixed an issue in the SDM600 installer, causing the installer to occasionally fail on systems with other server application installed. Occasionally, the Anti-Virus might block the “SQL2012WarningMessageBox.exe” responsible for checking whether SQL Server 2012 is installed for SDM600 on the target system. In this case the installer will continue the installation without performing the check. Refer to the "MS SQL Server 2019 Migration Workflow" document for extensive guidance on how to perform the migration to SQL 2019.

–

SDM600 1.2 FP3 Hotfix3 release (2022-09)

New and enhanced features

Microsoft SQL Server 2012 has officially reached the End of Support (also sometimes known as *end of life*): this product will no longer receive security updates, non-security updates, bug fixes, or technical support.
As part of our continuous effort to deliver secure and reliable software, SDM600 is now delivered and fully compatible with Microsoft SQL Server 2019.
To provide the customers enough time to plan and execute a graceful SQL migration, it will be possible to use SDM600 with Microsoft SQL Server 2012 until 15-March-2023.
Whereas it is still possible to run SDM600 with Microsoft SQL Server 2012, to be eligible for complete support it is required to upgrade to Microsoft SQL Server 2019. Existing SQL Server 2012 Standard licenses are not valid for SQL Server 2019 Standard: new valid licenses must be purchased.

Refer to the "MS SQL Server 2019 Migration Workflow" document for extensive guidance.

More information about SQL 2012 End of Life could be found in the following official links from Microsoft:

- SQL 2012 End of Life
- SQL Server end of support options
- SQL 2019 Pricing
- SQL 2019 Software and Hardware Requirements

The Fleet Management tab has been improved to show a detailed view of all the collected firmware and configuration files for several RTUs. To improve the user experience, filtering and sorting functionalities are available on all the fields. Aiming to harmonize the user experience, the Fleet Management configuration fields have been moved to the Device Settings tab.

General fixes and improvements

The performance of the user interface has been greatly improved, leading to shorter loading time on the tabs.

Fixed an issue causing the deletion of an IED to remove all the matching DR files previously exported to the file system.

While editing the parameters for the Fleet Management configuration: 1) fixed an issue causing the "Firmware Rolename" to be set to empty/null after configuring the "Poll Cycle", 2) fixed an issue causing the "Poll Cycle" to be set to 20 after configuring the "Firmware Rolename".

Fixed an issue causing the creation time of the files visualized under the fleet management to not match the timestamps shown in the RTU Web UI.

Fixed an issue with the *"Do not record SDM600 caused Log-in/Log-out events"* functionality.
All relevant events are now properly filtered out when the functionality is enabled.

Fixed an issue causing the Short Report to not be generated for DR Files using CFF format.

Fixed an issue causing user added SNMP OIDs to not be correctly restored as part of a backup.

–

SDM600 1.2 FP3 Hotfix2 release (2022-06)

New and enhanced features

Evaluate DR files with a user-defined tool has been re-introduced. From the "Download" tab, in the "Configuration" window, download the "DR Selector" application and configure the tool of your choice to evaluate the collected DR files.
Check the User Manual for more details.

To increase the cyber security transparency, SDM600 has implemented the security.txt file. The purpose of the security.txt file format is to give security researchers the information they need to report their findings in a standard coordinated way. The contents of the security.txt includes a quick summary of whom to contact and where to go to find more information such as a company's PGP keys, acknowledgments, and canonical URL information.

General fixes and improvements

Fixed a sporadic DR files synchronization issue, occurring in Hierarchical and Hot/Standby systems. While synchronizing the collected DR files, identical files would generate different hashes, leading to duplicates to be shown. If your system is affected, to clean up the duplicated DR files, perform a "Consistency Check" within the "SDM600 Application Administration Tool".

It is possible to configure which columns are displayed in the grids in the "Event Monitoring" tab.

It is possible to resize the columns in the grids in the "Event Monitoring" tab.

The time is formatted according to the language settings (24 hours - AM/PM).

Few UI glitches have been addressed.

–

SDM600 1.2 FP3 Hotfix1 release (2022-05)

New and enhanced features

By right clicking a device in the tree view and clicking on "Collect Data Now", SDM600 will immediately collect new DR files (if available) and update the service data info. The functionality is available in the Device Supervision, Service Data and Event Monitoring tabs.

General fixes and improvements

For RTU devices, the content of the CAM Package has been improved and cleaned up. Duplicated certificates are no longer added to the package. All certificates required to enable and configure CAM on the RTU are readily available, even in case of SDM600 configured as Parent/Child. Finally, the correct "Extended Key Usage" value is properly added to the certificate as expected by RTU v13.3.

Fixed an issue preventing SDM600 to collect DR files from an RTU. This issue would happen when, in RTUtil, the RTU is configured to fetch DR files with File Type set to "Disturbance Recorder IEC61850 - Generic IED"

Fixed an issue causing the "DR file trigger time" to be displayed instead of the properly calculated "UTC Time".

Fixed an issue causing the "Administrator" role to be incorrectly assigned to a new user during creation. This issue would only occur if the newly created user had "Account Management" permission set as None. Unfortunately, affected users must be recreated.

Fixed an issue affecting the SNMP protocols which was causing the community string to not be sent even if configured correctly.

Fixed an issue causing manually entered service data values to not be visible in the Service Data tab. Due to a synchronization issue, the values were visible in the detailed view and in the Export, but not in the main grid in the Service Data tab.

Improved the UX for the Email Notification, fixing an issue causing emails to not be sent to the correct users.

Fixed an issue causing valid SCD files to not be loaded properly: loading an incomplete/corrupted/not compliant SCD file will no longer prevent other SCD files to be loaded successfully afterwards. Additionally, if an error occurs while loading an SCD file, then an error message is now correctly displayed in the UI informing the user the operation could not be performed.

–

SDM600 1.2 FP3 (2022-03)

New and enhanced features

The Silverlight user interface has been replaced by a more modern React user interface. The User Experience has been reworked to help the user configure the devices, navigate the tabs, and inspect the collected data in a holistic way. The React user interface allows the users to rely on modern browsers, such as Chrome, Firefox and Edge. The User Experience has been optimized for Chrome.

The new Device Settings page: the device settings functionality has been reworked so that all the settings (IED configuration, licenses, DR, security events and service data) can be edited from a single table. It's no longer required for the user to navigate between separate tabs to configure how SDM600 interacts with the devices. Everything is in the same page, one click away.

The new Events Monitoring page: As usual, events are displayed split by category: DR files, Security Events, Configuration Changes, and a new tab – All Events – showing everything at the same time.
Gone are the pages, displaying 100 events each.
Gone is automatic refreshing causing you to lose the event you were looking for.
Welcome to endless scrolling. A subtle notification warns the user when new events are available.
The same functionality but modernized. Simple to use, elegant to look at.

The brand-new Device Detail page: previously, SDM600 focused on showing data based on category: all the DR files, all the security events, all the CAM packages, all the service data. Behold the Device Detail Page: available as a context menu entry for any device, in any tree view throughout the whole tool, this refined modal dialog aggregates several useful information for a single device in one single place.

The new System Configuration page: following the concept of bringing close what belongs together, the Configuration functionality has been reworked. Every system configuration aspect is now available in one single place - setting up hierarchy, hot-standby, adding and removing devices to the structure, managing the password policies and much more.

The new Account Management page: all the aspects of setting up the Centralized Account Management, available in one location. The Role and SDM600 Permissions functionality has been reworked maximizing usability and guidance. Less clicks are required to configure the role / permission as needed and with far superior visual feedback.

General fixes and improvements

Events collected by the Windows Event Log Forwarded will be displayed with a *forged* Raw Message, aggregating the relevant data.

Fixed an issue in e-mail notification functionality, causing no mail to be sent when a new DR file was collected.
Short Report generation correctly supports the following data file type: ASCII, binary, binary32, or float32.

Limitations and differences compared to Silverlight User Interface (1.2 FP2 and earlier)
Opening Configuration Tool is no longer supported due to Cyber Security restriction in Web Browsers to launch local applications.
Opening WaveWin is no longer supported due to Cyber Security restriction in Web Browsers to launch local applications. However, WaveWin (or any other application) can be registered as standard application for opening .cfg file extensions.
Dashboard with Timeline is no longer available. A new dashboard will be made available in future releases.
The Security Event tab will now show Timestamp (both UTC and Local Time), Device, Source, Raw Message. Security Event Mapping is no longer available.
Configuration is not locked for the first user opening configuration tab.
Translations (German, Czech, Spanish) are currently not available.

–

SDM600 1.2 FP2 Hotfix11 release (2022-02)

New and enhanced features
none

General fixes and improvements
Fixed an issue in CAL service causing the service to occasionally crash.
Fixed an issue in the Backup/Restore functionality causing invalid certificates to be restored.
Improved Backup functionality to ensure no corrupted backup is created: if the backup functionality fails to collect all the required certificates, then the procedure will abort, and no corrupted backup will be created.

–

SDM600 1.2 FP2 Hotfix10 release (2021-12)

New and enhanced features
none

General fixes and improvements
Performance improvements to minimize the loading time of the Silverlight UI.
Fixed a multi-threading issue occasionally causing users, roles and replication groups not to be displayed in the UI.
Fixed multiple OSS related vulnerabilities. For more information, refer to the Cyber Security Advisory - 8DBD000074.

–

SDM600 1.2 FP2 Hotfix9 release (2021-11)

New and enhanced features
none

General fixes and improvements
When modifying the "Security Events UTC Offset", it is not required anymore to restart "ABB SDM600 Centralized Activity Logging Service" for the change to be applied.
SDM600 will not crash if the Culture Info could not be parsed due unsupported format. In case the Culture Info could not be parsed, SDM600 will fallback to en-US.
The "Security Events UTC Offset" configured for the Source device is not applied anymore to events generated by the "Windows Event Forwarder". Events generated by the "Windows Events Forwarder" are already sent in UTC Time, hence not need to apply an offset.

–

SDM600 1.2 FP2 Hotfix8 release (2021-09)

New and enhanced features
none

General fixes and improvements
Synchronization of Security Events between Parent and Child systems has been improved, leading to a faster and more stable synchronization process.
In a SDM600 Child system, WEF Installer can only be generated if the Parent is reachable. If it's not reachable, the generate button is disabled. Also, the error messages have been improved to provide more meaningful information to the user in case the generation fails.
Security Events Tab can handle large amounts of data and won't crash if loading takes more than 1 minute.
Custom Roles can be deleted.
Automatic Service Data Export is no longer available through the Web UI. It is now accessible/configurable via AAT.

–

SDM600 1.2 FP2 Hotfix7 release (2021-08)

New and enhanced features
Data Retention has been improved to remove unused SQL logs, resulting in further reduction of the SQL Server's disk space. Moreover, Data Retention service stability has been improved.

General fixes and improvements
Fleet Management support has been extended to RTU530. It is now possible to write both firmware and configuration files to RTU530 devices
The memory allocation of the IED Communication Service has been improved, fixing occasional Out of Memory exceptions on very large systems.
The selected device is correctly considered while filtering security events (issue introduced in HF6). When filtering, security events are shown when either the Device or the Source match the selected device.

–

SDM600 1.2 FP2 Hotfix6 release (2021-06)

New and enhanced features
Backup files are now password protected and can only be created using the SDM600 Application Administration Tool. Backups created with previous versions can still be restored. Any new Backup must contain a password and can only be restored if the password is available. In case the password is lost, it cannot be recovered. Therefore, make sure it is stored in a safe place. For more information, refer to the Cyber Security Advisory - 9AKK107992A4700.
New algorithm to collect DR files over MMS to minimize network and CPU load. For all the devices configured with IEC61850-8-1 as DR Protocol, the new algorithm will be used by default. It is still possible to use the older algorithm by selecting IEC61850-8-1 (safe mode) as DR Protocol.

General fixes and improvements
When a device is selected in the tree view, security events are shown for which either the "Device" field or the "Source" field are matching the selected device.
Improved information shown in the "Device Supervision" tab for devices configured with no IP address and Directory as DR Protocol.
User synchronization between Parent and Child improved to automatically recover from synchronization issues

–

SDM600 1.2 FP2 Hotfix5 release (2021-05)

New and enhanced features
DR Files with .cff extension are now supported.

When configuring Directory as DR Protocol for a device, it is possible to configure two directories, so that SDM600 will try to reach the secondary one if the primary one is not reachable.
Application Administration Tool provides a procedure to clean up corrupted provisioning data, causing parent-child and/or hot-standby synchronization issues. Detailed info could be found in the User Manual.
General fixes and improvements
WindowsAgent supports SDM600 HSB configuration. Configuration details could be found in the Installation Guide.
Automatic and Manual Export of Service Data on a Parent System includes the same information
Updated communication library to support latest RTU500 firmware versions (12.7.x and 13.x)

_

SDM600 1.2 FP2 Hotfix4 release (2021-04)

New and enhanced features
none

General fixes and improvements
Parent – Child and Hot-Standby data synchronization improved when huge amount of data must be synchronized between the SDM600 systems

_

SDM600 1.2 FP2 Hotfix3 release (2021-03)

New and enhanced features
none

General fixes and improvements
The details window in the Service Data tab is now only showing the detailed properties for the selected device.
DR Files Export will overwrite already existing files instead of failing with an error message
Upgrading to 1.2 FP2 HF3 from older SDM600 versions (before 1.2 FP2) works as expected
Windows Event Forwarder is sending the events to SDM600 Hot and Standby system in case of failover
Occasional duplicated DR Entries for IEDs using zipped COMTRADE files are avoided

_

SDM600 1.2 FP2 Hotfix2 release (2021-01)

New and enhanced features
none

General fixes and improvements
Syslog messages beginning with length information are now correctly parsed and visualized.
Device Supervision Tab is now visible and correctly showing available devices.
Custom Roles can be correctly created, added and assigned to users.
Fixed sporadic exception occurring when setting up Hot/Standby. Restarting the Standby System after initial pairing is recommended.

_

SDM600 1.2 FP2 Hotfix1 release (2020-12)

New and enhanced features
none

General fixes and improvements
Events shown in the time window are correctly filtered based on the selected device.
Manually entered values for device's properties are not overwritten by empty strings.
For Windows PC, the *SerialNumber* is correctly collected and visualized (requires WindowsAgent update on target PCs)
Updated SDM600 Installation Guide-en.pdf and SDM600 Cyber Security Guideline-en.pdf to the latest versions
DR files collected from RTU devices are now correctly handled (e.g. short report, open in Wavewin, download, …)
SDM600 UI correctly displays the tabs – without duplicates.

_

SDM600 1.2 FP2 release (2020-10)

New and enhanced features
Data Retention Policy allows to configure how long data will be stored in the SQL Database.
List of officially supported Windows versions has been updated.
General fixes and improvements
Restore functionality successfully restores a backup without compromising the LDAP functionality.
Windows Event Forwarder can be updated without uninstalling the previous version.
Long Syslog messages are correctly received and displayed.
Adding a comment to a Security Event without RAW message is now possible.
Events received from child systems are successfully forwarded by the parent (Event Forwarding).
Automatic Service Data Export can be configured with a frequency greater than 31 days.
Radius Authentication and Authorization supports Customer defined Roles

The CAMRoleToRadiusRights.xml has been updated. If you have modified this file in an older version of SDM600, make sure to merge (and not just replace the file) your changes into the new template.

The default values for the vendor dictionary has been updated.
When merging your modified vendor_dictionary file make sure that following entries are NOT included (those has been added to the default list)

```
VENDOR          15004   RuggedCom
VENDORATTR      15004   RuggedCom-Vendor-name       1    string
VENDORATTR      15004   RuggedCom-Privilege-level   2    string

VENDOR           5597   Meinberg
VENDORATTR       5597   MBG-Management-Privilege-Level    1    integer

VENDOR          90001   PhoenixMGuard
VENDORATTR      90001   Filter-ID                   1    string
```

_

SDM600 1.2 FP1 Hotfix11 release (2020-09)

New and enhanced features
Updated ABB Wavewin to H.M.6 (Re-installation on client computer required, Installation package is available from SDM600)

General fixes and improvements
Automatic/Manual Service Data export functionality is generating an Excel File at the specified local folder.
Detailed version information for Windows computers is collected. This requires fresh download from SDM600 and re-installation of the Windows Agent on the connected Computer.
Improved the collection of DR files from IEDs using zipped COMTRADE files
Improved DR file handling to avoid adding the same DR file twice to the DB
SQL Server user is created during the installation on all supported Windows versions
Device Settings changes done on a child system are also visible on the parent system.
Corrected timestamp in the exported DR filename when <TIME_SRV> is configured in a custom template.
Newly created users can now successfully change the initial password and log in.

–

SDM600 1.2 FP1 Hotfix10 release (2020-08)

New and enhanced features
Changes in the SDM600 configuration are logged, show in the Configuration Changes Tab and reported via Syslog
Syslog messages that couldn't be parsed (e.g. due to incompatible date/time format) are now displayed in its raw format in a dedicated tab

General fixes and improvements
Improved fault tolerance when reading .scd files
Windows Event Log Forwarding is working again. ***This requires manual un-installation of the existing version, fresh download from the SDM600 server and re-installation on the connected computer.***
Application Administration Tools improved. Specifically restoring of certificates and working with large databases.
Removed version information from HTTP response header following cyber security best practice.
Syslog messages larger than 480 bytes are processed to support max. syslog message length (e.g. Fortinet)
Serial Number, Configuration Version and Software Version are shown in the Service data Tab if available.

–

SDM600 1.2 FP1 Hotfix9 release (2020-07)

New and enhanced features
Windows Agent collects exact Windows Version including Build Number (required fresh download from the SDM600 server and re-installation on the connected computer)
The Service Data can be exported automatically using a defined frequency
DR, Event and Service Data can be deleted from the Data Base using the SDM600 Application Administration Tool
User and Application Settings have been renamed to “Options”. All options are user specific. The default user options can be configured in the Application Administration Tool.

General fixes and improvements
Syslog Notice Events are received and processed
Improved IED Communication Service stability and optimized the way DR files are retrieved fromIEDs
SAN's (Subject Alternative Name) attribute of the SSL/TLS certificate now include the FQDN name of the host machine. This will give the page the green HTTPS indicator that meets browser guidelines and that give visitors confidence to connect to the SDM600 website.
SDM600 installer additionally installs Microsoft URL Rewrite Module 2.0 for IIS
Syslog Message forwarding includes the full raw message received by SDM600
Security Events export in Excel contains all columns (including UTC time)
Corrected problem in parsing COMTRADE file when .cfg contains multiple lines of Sampling rate information (e.g. NOJA Power devices)

_

SDM600 1.2 FP1 Hotfix8 release (2020-05)

New and enhanced features
The “SDM600 Restore Tool” has been renamed to “SDM600 Application Administration Tool”
The Authentication Method for SDM600 Hot-Standby and Parent Child communication can be configured in the SDM600 Application Administration Tool (Certificate based for Standalone Computers and Domain User/PW for computers joined to a domain).

General fixes and improvements
IEC 61850 (MMS) File Transfer stability improvements to always close files on the devices. This helps to prevent IEDs from entering into internal relay fault status (IRF7 on Relion 615/620)
Calendar format is no longer switched
SDM600 Hot-Standby and Parent Child communication Services are no longer causing Windows Security Event 4625 (Audit Failed) on computers joined to a domain
The SDM600 structure tree navigation on the parent system is no longer collapsed each time when the data is refreshed from a child system

_

SDM600 1.2 FP1 Hotfix7 release (2020-03)

New and enhanced features
none

General fixes and improvements
Timeline limits are correctly considered to filter data (in the dashboard and lists)
RTU Firmware version is now correctly visualized when value is updated/refresh
Auto Log Out will not be triggered while executing PDF/Excel export operation.

_

SDM600 1.2 FP1 Hotfix6 release (2020-03)

New and enhanced features
none

General fixes and improvements
Improved long term stability in DR File collector Service
The Date Format doesn’t switch between different formats when selecting a new time window

_

SDM600 1.2 FP1 Hotfix5 release (2020-02)

New and enhanced features
none

General fixes and improvements
The DR file export for given time range uses the configured start and end date (in the Configuration – DR Configuration Tab)
DR Evaluation tool can be configured per user (previously it was application wide)
The default time window setting is aligned with the dashboard and can be configured per user. The initial setting will be one day
Forwarding Syslog Events from Parent System includes all Syslog Events from Child Systems
Performance Improvements in Parent / Child synchronization
Improved recover procedure for SQL Server Service in case of failure
Collecting DR files improved when using File Directory Protocol
Device information is automatically shown in the configuration tab when refreshed

_

SDM600 1.2 FP1 Hotfix4 release (2020-01)

New and enhanced features
none

General fixes and improvements
Minimized the CPU load for SDM600 Hot Standby (HSB) configuration.
Additional improvement in Windows Event Forwarder installation to make it work on Windows 10.
Automatic Export of DR files to the disk on the parent of a hierarchical works after restart of the parent.

_

SDM600 1.2 FP1 Hotfix3 release (2019-12)

New and enhanced features
Disturbance Recorder Export feature can use customer name / description as part of the exported file name
Folder names for Disturbance Recorder Export feature can be switched between structure name and customer name / description.

General fixes and improvements
Memory consumption of the IEDCommService Service was optimized, so the service uses less memory and runs more stable.
SDM600 1.2 FP1 HF2 installation problem on Non-English OS are fixed
Windows Event Forwarder installation is working on Windows 10, but still might fail on Windows 7 or Windows 8.1
SDM600 1.2 FP1 HF2 introduced a problem to generate Short reports, this is working again.
Corrected Firmware Version mismatch between Configuration and Service Data tab. To have consistent information it is required to read the Firmware in SDM600 after writing a Firmware Update to the RTU (to confirm successful installation in the RTU500). Also it is required to logout/login in order to see the updated Firmware Version in the Configuration Tab.

_

SDM600 1.2 FP1 Hotfix2 release (2019-10)

New and enhanced features
Updated to latest ABB User Activity Logging message definition (additional Event Numbers are available)
It's possible to customize the default IEC 61850 attributes read from a device (this requires direct access to the database and is only recommended via SDM600 support-line)
SDM is filtering log in / log out messages from RTU500 devices based on the user name that is configured for accessing the RTU device. It is recommended to use a dedicated user account in SDM600.

General fixes and improvements
Download button from service data tab no longer freezes SDM600 UI
Device supervision stability has been improved and provides reliable connection information
DR Short report creation will work on computers with different culture setting
Overall SDM600 status LED is also visible for users with limited SDM600 user rights
Passwords for IED connections are no longer shown
Configuration and firmware files for RTU500 file management are also updated when the file date is older than the actual configuration.
SDM600 is showing consistent information in all tables for RTU500 configuration versions.
Configuration and firmware files for RTU500 file management is no longer showing empty filenames in the "Upload Firmware" window. This will work for newly read files, older files which are already in the SDM600 Database could still have an empty filename.
Improved SQL Installation on Windows 10 1803 and newer when using specific regional formats.
The DR file viewer can be changed even if ABB WaveWin is not installed
Windows Event Forwarder installation is working on Windows 10 1803.
The Email summary report is showing correct number of configuration changes
Using Custom Properties for SNMP supports vendor specific OIDs
Custom Properties for SNMP must contain full OID. In previous versions a ".1" was added to the request.

–

SDM600 1.2 FP1 Hotfix1 release (2019-07)

New and enhanced features
None

General fixes and improvements
The option introduced in version 1.2 FP1 to not record SDM600 caused Log-In / Log-Out events was filtering out too many successful login messages. This has been corrected.
The signing of the application (XAP) is using a different time server certificate which is available as default on more Windows Systems
The device supervision has been improved (throttling the ICMP ping requests)
The installation could fail on Win10 (1801) when using newly introduced code-pages.
Under some conditions the DR file export was creating duplicated files for the same COMTRADE file on the disk when customized file name was used.

_

SDM600 1.2 Feature pack 1 release (2019-04)

New and enhanced features
Central Account Management support for RTU500 12.4
Secure FTP protocol support for DR file retrieval (FTPS implicit)
Enhanced .csv configuration import (including API supporting structure import and deletion of devices)
Updated ABB Wavewin to H.G.24 (Re-installation on client computer required, Installation package is available from SDM600)
Dashboard is showing events in local time and also considering the configured device UTC offset
New option is introduced to not record SDM600 caused Log-In / Log-Out events (e.g. events generated when SDM600 itself is reading version information from devices)
Timeline is more intuitive. The timeline shows now the selected period, backward/forward will move the time window by the selected time period
“Send test email” button added to Email configuration
Central Account Management (CAM) configuration package includes Certificate also in p7b format
Updated German and Czech translations
When importing a .scd file, devices will no longer be automatically licensed to allow UTC time offset configuration before the first COMTRADE files are collected.
Changed UTC offset to TimeZone supporting daylight saving.

General fixes and improvements
Disturbance Recorder (DR) Short report generation improved for DR files which are not fully compliant with the COMTRADE standard
Improved DR short report generation when CZ language is active
DR file export takes UTC offset of the device into account
Added fraction of hours to UTC offset configuration
DR File Export supports additional structure Levels (e.g. <BAY> for Bay name , <VL> for Voltage Level Name)
The RTU500 firmware filename is shown
RTU firmware version is shown in the File Management configuration to allow filtering
Added support for IEDs using RFC3659 compatible FTP Server (e.g. ABB REF615)
FTP_REGEX.txt file handling optimized to allow different FTP server configuration
Structure Tree View refreshing issue fixed (e.g. when adding a new Child System). Possibility to manually refresh the structure tree has been added.
Information is displayed when user tries to generate Certificates with a validity period that is longer than the SDM600 license
The MicroSCADA CAM configuration package can only be created when user confirms that SDM600 is not installed on the same computer.
Improved stability when configuring parent-child and hot-standby systems
Device connection stability (e.g. using IEC 61850) is improved
Security Event Mapping is showing newest events on first page.
Logging improved and extended to support troubleshooting
Updated information message when number of failed login attempts has been reached.
Syslog forwarding supports TCP protocol

_

SDM600 1.2 Service pack 2 release (2018-05)

New and enhanced features
Official support for Windows Server 2016
UTC Time Offset for devices can be set. Some device implementation are using local time instead of UTC in COMTRADE. To avoid misalignment, an offset from UTC can be defined (default value is 0, which means the time is stored in UTC). SDM600 stores all time information in UTC and displays it according the setting of the Client PC.
Support for RTU500 series HMI project File.
Project name of RTU500 configuration files is shown.
Support for SQL Server 2014 SP2 (and newer) and 2016 SP1 (and newer) database engine. (SDM600 default is still SQL Server 2012). Migration to other than SDM600 default Server is manual work and not described in SDM600 documentation.

General fixes and improvements
German translation reviewed and misleading translations have been corrected.
Content of .pdf and .xls exports are synchronized.
Security Events tab is automatically refreshed every minute.
Configuration import from .csv allows to add IEDs without DR functionality.
Certificate expiration email formatting updated
The OR condition in security events mapping is fixed
Reading IEC 61850 version information from valRef and paramRev are corrected
DR trigger time (milliseconds) is rounded and shown properly
Cyber Security related upgrades of components (open SSL)

_

SDM600 1.2 Service pack 1 release (2017-06)

New and enhanced features
The “Disturbance Records“ list can be automatically refreshed every minute to show new COMTRADE files
The “Cyber Security Events” list can be automatically refreshed every minute to show new Syslog events
The disturbance recorder trigger time includes milliseconds
The daily aggregation of Security Events can be configured in the dashboard. Using the aggregation feature will reduce the loading time in case of many security events.

General fixes and improvements
The “Disturbance Records“ list is sorted correctly according the trigger time. It is now based on the actual Date/Time instead of the textual representation
The CSV template for importing an SDM600 structure contains better configuration examples
Disturbance Recorder trigger channel calculation is more robust and will not slow down the whole SDM600 DR functionality in case COMTRADE files contain values outside of the standard.
Certificate expiration email message content is cleaned up.
Poll cycle setting is moved to “Configuration” -> “General Settings” tab and is applicable also for other applications like Service data retrieval.
Switching between different user interface languages (e.g. to the German translation) has been fixed
The agent to collect version information from Windows systems was not starting automatically all the times

_

SDM600 1.2 Release (2017-02)

New and enhanced features
Several COMTRADE Files can be opened simultaneously and subsequently merged in Wavewin
DR File retrieval from RTU500 for COMTRADE based files
Software version information can be retrieved from SNMP capable devices and Windows Computers.
Configuration and firmware file management for RTU500 (Rel.12 and newer)
Launching of native or web based configuration tool for devices
Import SDM600 configuration from .csv file
Rule based Email Notifications
Customizable logon Banner
DR file export supports flexible renaming of original DR Files including COMNAME standard

Improvements
Support for Microsoft Windows 10.
Superior overview in the SDM600 Dashboard
Time window handling improved
Support for more devices and SDM600 child systems (limits are documented in the SDM600 factsheet).
License usage shown in SDM600 Supervision Tab
NERC-CIP rating can be set per device
All Grids can be exported to Excel and include structure info e.g. the full path to the device
Indication when DB size is about to exceed SQL express limits
Dedicated event list for configuration changes
Additional email notification options for certificate expiry and statistics.
Additional email notification options for statistics (daily, weekly, and monthly).
Commented events are visualized in the dashboard
SDM600 Restore Utility supports creation of backups
Option to backup only SDM600 configuration data
Unknown Security Events mapping - rules handling (selecting target events, deleting multiple rules)
New description attribute for user accounts
Support DR file import from nested Windows Folders
Support for COMTRADE 2013
Robustness for COMTRADE file handling for trigger channel and short report generation improved
Extended password policy. Number of failed login attempts to lock the account and lockout duration
Support for CAM/CAL on all network interfaces

Hitachi Energy
Grid Automation
PL 688
FI-65101 Vaasa, Finland