System Data Manager SDM600
Cyber Security Guideline
Trace back information:
Workspace SDM600 version a22
Contents

1 Copyrights ........................................................................................................... 5
2 Introduction ........................................................................................................ 7
3 Network Configuration Security Recommendation ................................. 9
   3.1 Virtual Private Network (VPN) ............................................................... 9
   3.2 Network Devices .................................................................................. 9
4 Windows OS Security Recommendation .................................................. 11
   4.1 BIOS settings ...................................................................................... 11
   4.2 Data Execution Prevention (DEP) ....................................................... 11
   4.3 Removing unused programs ............................................................... 11
   4.4 Windows Updates/Patch management ............................................. 12
   4.5 Virus scanner ..................................................................................... 12
   4.6 Disabling devices ............................................................................... 14
   4.7 Configurable logon/warning banner ............................................... 14
   4.8 User Account Control (UAC) ............................................................ 15
   4.9 Firewall (ports and services) ............................................................. 15
   4.10 Database password .......................................................................... 16
1 Copyrights

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

In no event shall ABB Oy be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, nor shall ABB Oy 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 ABB Oy, 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.

Copyright © 2017 ABB Oy. All rights reserved.

Trademarks

ABB is a registered trademark of ABB Group. All other brand or product names mentioned in this document may be trademarks or registered trademarks of their respective holders.

Guarantee

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

Third Party Copyright Notices

List of third Party Copyrights notices are documented in "about.htm" under the installation directory.
2 Introduction

This document contains general information on a good practice to secure the computer on which SDM600 is installed. The guide is intended for persons and project engineers responsible for information technology and information security and for system verification testers. They all are expected to have general familiarity with topics in the following areas:

- PCs, servers, and Windows operating systems
- Networking, including TCP/IP and concept of ports and services
- Security policies
- Firewalls
- Anti-virus
- Application whitelisting
- Remote and secure communication

This guide assumes the following in the SDM600 servers:

- Windows Update is performed manually.

⚠️ After Windows update, the computer automatically reboots in order for changes to take effect.

ℹ️ ABB recommends to update the system after the SDM600 installation to the latest ABB verified patch level of all installed ABB software products. For other vendors' software products, refer to the respective documentation.

⚠️ It's strongly recommended to check if SDM600 and IIS services are working after applying update on Windows or MS SQL Database.

- Uninterruptable Power Sources (UPS) is not controlled by the server.
- Wireless network configuration is not used.

During the installation of SDM600, security settings such as firewall, security policies and disabling Windows system services are not automatically configured. This is because the SDM600 installation may conflict with the existing security settings on computers where it is not allowed to modify these settings.
3 Network Configuration Security Recommendation

SDM600 is a server application. It is essential to assign a static IP address to ensure smooth operation of the SDM600 functionalities. The IP address is composed of four numbers in the range from 0 to 255. The numbers are separated with dots, for example, 192.168.0.1. Because every computer in an IP network must have a unique IP address, careful planning of IP addresses throughout the whole system is important. Particularly due to the centralized functions that are offered by SDM600. Ensure that IP address planning considers also the future needs of network addresses in your system.

In general, ABB does not recommend that domains and wireless networks are used in the SDM600 system due to the high reliability that is required of the control system.

3.1 Virtual Private Network (VPN)

This guideline considers that the IP communication between the SDM600 at the substation level (SDM600 Child) and the SDM600 that is installed at the Network Control Center (SDM600 Parent) is handled via a dedicated wide area link that is not exposed for public access. The use case is to protect the dedicated link against man-in-the-middle attacks by guaranteeing confidentiality, integrity, and authentication. This can be achieved by establishing a Virtual Private Network (VPN) by using IPSec. If the SDM600 Parent is to be connected using IPSec, every SDM600 Child has to connect to the SDM600 Parent using the same method (IPSec). Consequently, the IPSec configuration must be done on all machines that need to communicate with each other using IPSec.

IPSec encryption is a Central Processing Unit (CPU) consuming activity that can affect the maximum throughput and the CPU utilization. To determine the effect of IPSec encryption for data throughput and CPU consumption, it is important to verify this with tests.

3.2 Network Devices

Network devices, such as switches, routers, firewalls, intrusion detection systems, modems, and wireless devices, are not in the scope of this security guide. From the security point of view, these devices should be enabled for the following features:

- Logging
- Patches/Updates
- Backup/Recovery

For more information, see the device manuals.
4 Windows OS Security Recommendation

The Windows operating system in general can be protected from malicious attacks with the latest service packs and security updates, firewalls, security policies, application whitelisting, and virus scanners. To reduce the attack surface in computers where SDM600 is installed, programs and services not used can also be uninstalled or disabled.

The following sections show an overview of different ways to secure the operating systems on which SDM600 is installed.

4.1 BIOS settings

The following settings must be applied:

- Passwords are enabled.
- Remote wake-up/Wake on LAN is disabled.

This has to be configured manually.

4.2 Data Execution Prevention (DEP)

Data Execution Prevention (DEP) is a security feature that can help prevent damage to the user's computer from viruses and other security threats. DEP can help protect the user's computer by monitoring that different programs use the system memory safely. If a program tries to execute code from the memory in an incorrect way, DEP closes the program. DEP automatically monitors the essential Windows programs and services.

The default configuration of the operating system is used.

4.3 Removing unused programs

The following software is not used by SDM600 and can be manually removed from Windows. These programs can normally be found on desktop operating systems, such as Windows 7.

<table>
<thead>
<tr>
<th>Windows Component</th>
<th>Added/Removed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outlook Express</td>
<td>Manually Removed</td>
</tr>
<tr>
<td>Messenger</td>
<td>Manually Removed</td>
</tr>
<tr>
<td>MSN Explorer</td>
<td>Manually Removed</td>
</tr>
<tr>
<td>Windows Media Player</td>
<td>Manually Removed</td>
</tr>
</tbody>
</table>

This software has to be deleted manually.
4.4 Windows Updates/Patch management

There are nine update classifications defined by Microsoft. These include, for example, critical updates, drivers, security updates and service packs. The compatibility of the SDM600 product with the latest Microsoft security updates and service packs is tested and verified monthly by ABB. The report does not cover computers from which SDM600 is accessed remotely. Nonetheless, in general it is recommended to install all Windows updates.

Windows Update vs. Microsoft Update

Windows Update only gets updates for the Windows operating system. For other installed Microsoft products, Microsoft Update should be used instead. This has to be configured manually.

ABB recommends to update the system after the SDM600 installation to the latest ABB verified patch level of all installed ABB software products. For other vendors’ software products, refer to the respective documentation.

4.5 Virus scanner

Anti-virus software is highly recommended on computers that have SDM600 installed to prevent the execution of unknown software on a machine (for example, due to enabling of removable devices or USB ports).

Virus scanners distinguish between on-access scanning (only files that are currently requested to load are checked) and on-demand scanning (all files are checked during a scheduled scan). The minimum requirements for the virus scanner are on-demand scanning and virus definition updating features.

On-access virus scanners on servers are a trade-off between security and performance. We recommend that the performance of the system is tested with normal virus scanner settings. If the performance is not acceptable, it can be enhanced with various settings available in some virus scanner programs, such as excluding certain directories or files (those that are frequently used) in on-access scanning and on-demand scanning. For example, event logs, databases and some custom file types that are accessed continuously should be put in the exception list, in other words, those files are not on-access scanned.

The operation of anti-virus software can influence the performance of the PC.

Here are some ways for ensuring that a computer's performance is not significantly affected by the running anti-virus software.
CPU utilization

- Restrict the CPU utilization to 20%.
- After modifying this setting, it is recommended to run the on-demand scan once for local disks to ensure that it finishes within an acceptable amount of time.

On-access scanning

- Scan only local disks, network scan is disabled (when each machine has its own virus scanner).
- Disable email scans.
- Enable the following settings:
  - Buffer overflow protection
  - Access protection
  - Script scan

On-demand scanning

- Initiated periodically or manually.
- Initiated manually if the system owner has found virus infected files on other computers in the enterprise, for example, in the office network or on maintenance laptops or similar.
- Scan only local disks, network scan is disabled (when each machine has its own virus scanner).
- Scanning should be done when normal system activity is low.
- All items excluded in on-access scanning should be included in the scan.

Handling of infected files

- Automatic clean first, then quarantine. Any infected files must be manually deleted by a security specialist.
- Antivirus software should not be allowed to clean, quarantine or delete SYS600 processes.
- Reporting:
  - Maintenance personnel should check the virus scanner log files on each site visit. If viruses are detected, the issue must be escalated to the responsible personnel.
  - There are several methods to report virus detection, such as email, printout to printer, sending to a computer's syslog, launching a program locally (for example, a SCIL program or VB script), or sending via SNMP Trap, to one or more computers. Sending an SNMP is the preferred method.

Scan engine and virus definition updates

- It is recommended that scan engines and virus definitions are automatically updated. However, enabling this feature on all machines connected to the automation system network is not a recommended practice. For a more secure and reliable deployment of virus definitions, a central management (for example, F-Secure Policy Manager,
McAfee® ePolicy Orchestrator, or Symantec Endpoint Protection Manager) and update deployment host can be set up on a corporate intranet. This allows a system administrator to have control over when updates are made. A direct Internet connection should only be allowed for the duration of the download and closed after downloading is finished.

- If there are redundant servers, it is recommended that the scan engine and virus definitions are updated to these servers first. Reboot the server, open the monitor, and perform some functional testing, for example, opening process, event, alarm displays and control dialogs.
- New virus definition files should be taken into use immediately. See the recommendation for redundant servers above.
- Some scan engine updates may override the current scan settings. In possible problem situations, this should be checked.

This has to be configured manually.

**Patch management**

It is recommended that the scan engine and virus definition files are updated regularly. Verify that the settings introduced above are preserved and that the performance and functionality of the system is acceptable after updates.

Theoretically, a new virus definition file can arrive that can compromise the proper functionality of the system. Testing the system against every new virus definition file is obviously not feasible. Therefore, we recommend that the full system is backed up before updating virus definition files.

### 4.6 Disabling devices

In general, it is a good practice to disable any unused devices in your system. This may include USB ports, CD/DVD drives or communication ports. This has to be configured manually. To disable devices, navigate to `devmgmt.msc` (Device Manager) and look for the devices to be disabled.

**Disabling autorun functionality**

If it is not possible to disable a device, it is good to disable the autorun functionality of the device. To prevent the automatic start of malicious code contained in a removable device, the autorun functionality must be disabled. For more information, see How to disable the Autorun functionality in Windows [http://support.microsoft.com/kb/967715/en-us](http://support.microsoft.com/kb/967715/en-us).

### 4.7 Configurable logon/warning banner

The computer must present a warning banner for authorized and unauthorized users at all access points. This is needed for successfully prosecuting unauthorized users who use the computer improperly.
To modify texts in warning banners:
1. Open Registry Editor to modify the Windows OS banner.
2. Go to the following registry keys:
   • `MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption`
   • `MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText`

A warning banner affects the Windows automatic logon (autologon) feature. The banner has to be acknowledged by pressing the **OK** button. After this, automatic logon occurs and the programs placed to the Startup folder will start.

It is not recommended to use the Windows automatic logon feature, since Windows stores the username and password in cleartext in the Windows registry. This is a security risk. If the end user accepts this risk, the workaround is to clear the above-mentioned Windows registry keys.

### 4.8 User Account Control (UAC)

UAC is a security feature in Windows 7, Windows Server 2008 R2 and later versions. UAC is recommended to be enabled in SDM600 and computers that are used to access SDM600. If the program requires privilege elevation, the behaviour is the following:

- For administrators: Prompt for consent. A dialog is shown where either **Continue** or **Cancel** can be selected. In Windows Server edition, value Prompt for consent for non-Windows binaries is used.
- For standard users: A message box stating that a program has been blocked is shown. This setting was introduced in Windows 7, Server 2008 R2 and later versions.

A shield is used in the program icon to indicate that it requires administrative privileges to run. This is automatically detected by the operating system if, for example, Run as administrator flag is set in the file properties or if the program has previously asked for administrative privileges.

### 4.9 Firewall (ports and services)

Windows Firewall is a stateful firewall that can be configured to restrict all inbound connections, but cannot filter or block any outbound connections. However, both Windows 7, Server 2008 R2 or later versions support blocking outbound connections. The ports and services used by SDM600 as well as the default firewall settings are listed in SDM600 User Manual. We recommend to use hardware firewalls since software firewalls may affect the performance and thus should not be used.
4.10 Database password

The SDM600 installs with pre-configured Database password. It is possible to change database password and configure SDM600 to work with updated credentials.

⚠️ Make following changes with caution. Improper configuration will break replication between connected systems, or would make SDM600 stop working!

⚠️ Weak database password can compromise SDM600 security. Create strong password, which is long (at least 10 characters) and is combination of uppercase, lowercase letters, numbers and special characters (like !,@,#,$, etc).

In order to update SDM600 database password, follow setps below:

1. Stop all SDM600 services.
   Run services.msc and stop all services which name begins with “ABB SDM600”
2. Update password in database.
   Using Microsoft SQL Management Studio
   Run SQL Management Studio and on login screen put COMPUTER_NAME\SDMSERVER as Server Name (COMPUTER_NAME should be replaced with computer name where SDM is installed). As Authentication method select Windows Authentication (depending on system configuration, you might need to log in as administrator).
   Select File -> New -> Query with current connection, and paste below query:

   ```sql
   ALTER LOGIN [SDM600User] WITH PASSWORD=N'NEW_PASSWORD' UNLOCK
   ```
   Replace NEW_PASSWORD with your password. And press Execute.
   Using command line (if SQL Management Studio is not installed)
   Run command line as administrator (Press Start, then type cmd, then press with right mouse button on Command Line and select run as administrator).
   Change in below line NEW_PASSWORD to your password and paste into opened command line.
   For 64 bit Windows:

   ```cmd
   "c:\Program Files (x86)\Microsoft SQL Server\110\Tools\Binn\OSQL.EXE" -S %COMPUTERNAME\%\SDMSERVER -E -Q "ALTER LOGIN [SDM600User] WITH PASSWORD=N'NEW_PASSWORD' UNLOCK"
   ```

   For 32 bit Windows:

   ```cmd
   "c:\Program Files\Microsoft SQL Server\110\Tools\Binn\OSQL.EXE" -S %COMPUTERNAME\%\SDMSERVER -E -Q "ALTER LOGIN [SDM600User] WITH PASSWORD=N'NEW_PASSWORD' UNLOCK"
   ```

In SDM directory (by default in C:\Program Files (x86)\ABB\SDM600) find connections.example.config.

Copy it to another directory (ie. Desktop), open in notepad and change all occurrences of NEW_PASSWORD to your password. Save file, rename it to connections.config and copy to SDM bin directory (C:\Program Files (x86)\ABB\SDM600\bin). You should replace existing file.

4. Encrypt configuration file (optional)

Optionally it is possible to encrypt file with password. To do it, open command line (see updating database password for details), and type below command (update SDM600 path if required).

For 64 bit Windows:

"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe" -pef "connectionStrings" "C:\Program Files (x86)\ABB\SDM600" -prov "DataProtectionConfigurationProvider"

For 32 bit Windows:

"C:\Program Files\Microsoft SQL Server\110\Tools\Binn\OSQL.EXE" -S %COMPUTERNAME%\SDMSERVER -E -Q "ALTER LOGIN [SDM600User] WITH PASSWORD=N'NEW_PASSWORD' UNLOCK"

5. Start SDM600 services.

After above steps you can start SDM600 services. Open services.msc, and start all services which name begins with “ABB SDM600”.

Below you can find template of connections.config file.

```xml
<?xml version="1.0" encoding="utf-8" ?>
<connectionStrings>
  <add name="LoggingDataContainer"
      connectionString="Server=.\SDMSERVER;Database=SDM600LoggingData;UserID=SDM600User;Password=NEW_PASSWORD;multipleactiveresultsets=True;" providerName="System.Data.SqlClient" />
  <add name="ConfigDataContainer"
      connectionString="Server=.\SDMSERVER;Database=SDM600ConfigurationData;UserID=SDM600User;Password=NEW_PASSWORD;multipleactiveresultsets=True;" providerName="System.Data.SqlClient" />
  <add name="LiveDataContainer"
      connectionString="Server=.\SDMSERVER;Database=SDM600LiveData;UserID=SDM600User;Password=NEW_PASSWORD;multipleactiveresultsets=True;" providerName="System.Data.SqlClient" />
  <add name="EventDataContainer"
      connectionString="Server=.\SDMSERVER;Database=SDM600EventData;UserID=SDM600User;Password=NEW_PASSWORD;multipleactiveresultsets=True;" providerName="System.Data.SqlClient" />
  <add name="ConfigDataContainer_Remoted"
      connectionString="Server=SDM600_REMOTE_IP_ADDRESS\SDMSERVER,58900;Database=SDM600ConfigurationData;UserID=SDM600User;Password=NEW_PASSWORD;trustServerCertificate=false;encrypt=false;multipleactiveresultsets=True;" providerName="System.Data.SqlClient" />
  <add name="LiveDataContainer_Remoted"
      connectionString="Server=SDM600_REMOTE_IP_ADDRESS\SDMSERVER,58900;Database=SDM600LiveData;UserID=SDM600User;Password=NEW_PASSWORD;trustServerCertificate=false;encrypt=false;multipleactiveresultsets=True;" providerName="System.Data.SqlClient" />
  <add name="EventDataContainer_Remoted"
      connectionString="Server=SDM600_REMOTE_IP_ADDRESS\SDMSERVER,58900;Database=SDM600LiveData;UserID=SDM600User;Password=NEW_PASSWORD;trustServerCertificate=false;encrypt=false;multipleactiveresultsets=True;" providerName="System.Data.SqlClient" />
</connectionStrings>
```
<add name="EventDataContainer_Remoted"
    connectionString="Server=SDM600_REMOTE_IP_ADDRESS\SDMSERVER,58900;Database=SDM600EventData;User ID=SDM600User;Password=NEW_PASSWORD;trustServerCertificate=false;encrypt=false;multipleactiveresultsets=True;"
    providerName="System.Data.SqlClient"/>
</connectionStrings>