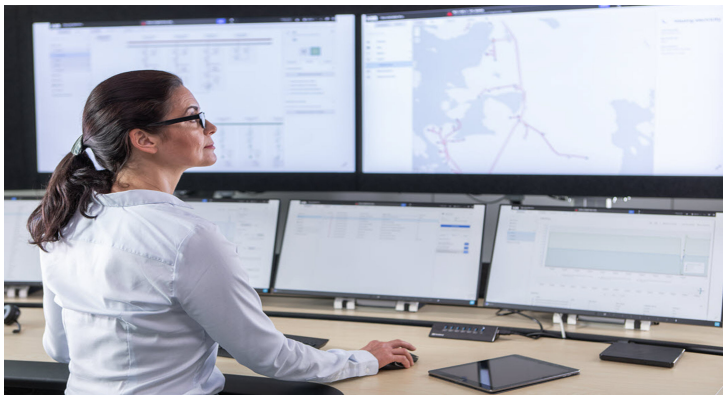
GRID AUTOMATION PRODUCTS

MicroSCADA X

Cyber Security Deployment Guideline



Document ID: 1MRK 511 485-UEN
Issued: March 2021
Revision: A
Product version: 10.2

Table of contents

Section 1 Copyrights

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

In no event shall Hitachi 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 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 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.

Trademarks

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

Guarantee

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

Third Party Copyright Notices

List of Third Party Copyright notices are documented in "3rd party licenses.txt" and other locations mentioned in the file in SYS600 and DMS600 installation packages.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (https://www.openssl.org/). This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Section 2 Introduction

2.1 This manual

This document is a cyber security guide for MicroSCADA X Control System SYS600 (hereafter SYS600) and MicroSCADA X Distribution Management System DMS600 (hereafter DMS600). See product versions from Section 2.5.

There are quick configuration instructions at the end of this document to configure server and workplace in easy steps, see Appendix A. The major part of the configuration can be done automatically with a security configuration tool, ABB Security Compliance Manager (SCM).

The installaction package for the ABB SCM tool can be downloaded from the MicroSCADA partner portal.

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

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

Information icon alerts the reader to relevant factors and conditions.

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

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

2.3 Intended audience

This manual is intended for installation personnel, administrators and skilled operators to support installation of the software.

2.4 Document conventions

The following conventions are used for the presentation of material:

- The words in names of screen elements (for example, the title in the title bar of a dialog, the label for a field of a dialog box) are initially capitalized.
- Capital letters are used for file names.
- Capital letters are used for the name of a keyboard key if it is labeled on the keyboard. For example, press the CTRL key. Although the Enter and Shift keys are not labeled they are written in capital letters, for example, press ENTER.
- Lowercase letters are used for the name of a keyboard key that is not labeled on the keyboard. For example, the space bar, comma key and so on.
- Press CTRL+C indicates that the user must hold down the CTRL key while pressing the C key (in this case, to copy a selected object).
- Press ALT E C indicates that the user presses and releases each key in sequence (in this case, to copy a selected object).
- The names of push and toggle buttons are boldfaced. For example, click **OK**.
- The names of menus and menu items are boldfaced. For example, the **File** menu.
    - The following convention is used for menu operations: **Menu Name/Menu Item/ Cascaded Menu Item**. For example: select **File/Open/New Project**.
    - The **Start** menu name always refers to the **Start** menu on the Windows Task Bar.
- System prompts/messages and user responses/input are shown in the Courier font. For example, if the user enters a value that is out of range, the following message is displayed: `Entered value is not valid`.
  The user may be told to enter the string MIF349 in a field. The string is shown as follows in the procedure: `MIF349`
- Variables are shown using lowercase letters: sequence name

2.5 Document revisions

Revision	Version number	Date	History
A	MicroSCADA X SYS600 10.2, SDM600 1.2	31.03.2021	Document updated for SYS600 10.2 and SDM600 1.2 releases

Section 3 General

This document is a security guide for MicroSCADA X Control System SYS600 and MicroSCADA X Distribution Management System DMS600. The guide is intended for software and project engineers, and system verification testers and they 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

Operating systems (with the latest service packs) covered in this document are:

- Server operating systems: Windows Server 2012 R2, 2016, 2019
- Desktop operating systems: Windows 8.1, 10

The guide assumes that in servers:

- Windows Update is disabled, for example, WSUS used instead
- Uninterruptable Power Sources (UPS) is not controlled by the server
- Wireless network configuration is not used
- Audio is not used
- There are printers connected to the server

This guide assumes that in workplaces:

- Windows Update is disabled, for example, WSUS used instead
- Wireless network configuration is not used
- There are printers connected to the workplace

However, the guide does not specify the network configuration (forests, domains, organizational units) where the MicroSCADA X system is installed.

This section provides general information as well as information on assumptions, operating systems and MicroSCADA X versions this guide covers. The system is secured by configuring the network, uninstalling irrelevant software, disabling some Windows system services, configuring the firewall settings, configuring application whitelisting, and applying security policies. Configuring network is discussed in Section 4. Security settings in this document are divided into the following categories:

- Security settings in Windows operating systems and MicroSCADA X servers (Section 5)
- Security settings in MicroSCADA X workplace computers (Section 6)
- Security features available in SYS600 and DMS600 products (Section 7)

There are security settings that are automatically configured in the product and those that need to be configured manually. For example, a Windows administrator user account is created during SYS600 installation and a password is prompted for the MicroSCADA user. Since this is an administrator user account, it is the responsibility of the system administrator to choose a valid and secure password for this account.

MicroSCADA X SYS600 uses symmetric and asymmetric cryptographic algorithms, which are used for data encryption, such as information, messages, text, etc. SSL versions/protocols such as TLS 1.0/1.1/1.2 are used with high encryption cipher suites, greater than or equal to 128-bit key length. Hashing algorithms are used, for example, for authentication/password protection purposes.
By default, all MicroSCADA X SYS600 licenses include above mentioned cryptographic functionality. Depending on market requirements or country restrictions some licenses can be sold without data encryption of information and messages. That is, cryptographic functionality is disabled by the manufacturer by the means of the licensing.

Other Windows server security settings such as firewall, security policies and disabling Windows system services are not automatically configured during the SYS600 or DMS600 installation. This is due to fact that the installation may conflict with existing security settings on some computers where it is not allowed to modify these. To apply security settings, such as firewall rules, security policies and disabling unused Windows system services, after MicroSCADA X product installation, run a security configuration tool, ABB Security Compliance Manager (SCM), see Appendix A 1.1.

There is general security guide for control systems and operating systems on the Hitachi ABB Power Grids website [ABBSEC09]. Microsoft also has security guides for different operating systems [MSSEC09].

MicroSCADA X SYS600C includes both SYS600 and Windows server specific security settings by default. However, it is the responsibility of the project engineer to:

- Activate pre-configured Windows user accounts that are meant for operators and engineers (ScOperator etc.)
- Open Windows Firewall ports for the used communication protocols
- If there are new applications installed, these should be allowed to run in Windows AppLocker

For more information, see Appendix A 1.3.

A=automatically configured in the product, SCM=security configuration tool, M=manual configuration

Table 1: Deployment of security features in MicroSCADA X products

Security feature	SYS600 installation	SYS600C	SYS600	DMS600	Remarks
Windows users and groups	- 1)	A+M 2)	A+M 2)	SCM+M 2)	1) MicroSCADA user account is automatically created during installation. Password should be longer than 15 characters. 2) Some user accounts have to be enabled manually
OPC/DCOM settings for server-workplace communication	-	A+M	M	M	See [SYSINS]
Firewall settings (ports and services)	-	A	SCM+M	SCM+M	Enable ports for used communication protocols according to customer specifications.
Virtual Private Network (VPN)	-	A	M	M	
BIOS settings	-	A	M	M	
Removing unused programs	-	A	M	M	
Disabling system services	-	A	SCM	SCM	
SNMP	-	A	M	M	
Security policies	-	A	SCM	SCM	
Microsoft Update	-	M	M	M	Not installed/services disabled. WSUS or manual installation to be used instead. The latest service packs and security updates are tested and verified.
User Access Control (UAC)	-	A	SCM	SCM	
Application whitelisting	-	A	SCM	SCM	
Virus scanner	-	M	M	M	Installation manuals exist for some virus scanner software and virus definitions of those software versions are verified and tested.
Disabling devices					
- DVD/CD-ROM drives	-	A	SCM	SCM	
- USB Mass Storage	-	A	SCM	SCM	
- Serial port	-	M	M	M	
- Floppy disk controller	-	M	M	M	
- Sound, video controller	-	M	M	M	

Table continues on next page

Security feature	SYS600 installation	SYS600C	SYS600	DMS600	Remarks
Disabling autorun functionality	-	A	SCM	SCM	
Backing up and restoring	-	M	M	M	
SYS600 user management and authorization	-	A	M	-	
DMS600 user management and authorization	-	-	-	M	
Encryption of SYS600 internal communication	-	A	A	-	
Encryption and authentication of process and control center communication according to IEC62351-3 and -5	-	M	M	-	

3.1 Definitions and Abbreviations

Table 2: Terminology

Term	Description
DCOM	Distributed Component Object Model
NCC	Network Control Center
OPC	Open connectivity specification by OPC foundation
SCADA	Supervisory Control and Data Acquisition
SCM	ABB Security Compliance Manager, a security configuration tool
SCW	Security Configuration Wizard
SYS600	MicroSCADA X Control System SYS600
SYS600C	MicroSCADA X SYS600C
DMS600	MicroSCADA X Distribution Management System DMS600
TCP/IP	Transmission Control Protocol/Internet Protocol
WSUS	Windows Server Update Services
MicroSCADA X	Product family including SYS600 and DMS600

3.2 Reference Documents

Table 3: References

Ref	Document title
[ABBSEC09]	Hitachi ABB Power Grids Security – Control Systems, Hitachi ABB Power Grids
[APPLOC12]	Windows AppLocker, Microsoft
[DMSINS]	DMS600 Installation Manual, Hitachi ABB Power Grids
[DMSSYS]	DMS600 System Administration Manual, Hitachi ABB Power Grids
Table continues on next page	

Ref	Document title
[HISADM]	SYS600 Historian Configuration and Administration Manual
[LEMNOS11]	The Lemnos Interoperable Configuration Profile - IPSec
[MSDCOM04]	The default dynamic port range for TCP/IP has changed, Microsoft How to configure RPC dynamic port allocation to work with firewalls, Microsoft
[MSDEP]	Data Execution Prevention, Microsoft.
[MSPASS09]	Strong passwords, Microsoft.
[MSSEC09]	Windows OS Security Guides, Microsoft. Search for Security Guide and refine the search by giving a specific OS name, for example, Windows Server 2008
[MSTHRE05]	Threats and Countermeasures Guide: Security Settings in Windows Server 2016, Microsoft.
[MSWS03]	Microsoft Security Compliance Toolkit, Microsoft.
[SYSAPL]	SYS600 Application Design manual, Hitachi ABB Power Grids
[SYSCON]	SYS600 System Configuration manual, Hitachi ABB Power Grids
[SYSINS]	SYS600 Installation and Administration manual, Hitachi ABB Power Grids
[SYSOBJ]	SYS600 System Objects manual, Hitachi ABB Power Grids
[WSUS]	Windows Server Update Services, Microsoft.
[SYSCUG]	SYS600C Users Guide, Hitachi ABB Power Grids
[UAC]	What are User Account Control settings?, Microsoft.

Section 4 Configuring network

Each host in a TCP/IP network has a unique identifier, called an IP address. 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 on an IP network must have a unique IP address, careful planning of IP addresses throughout the whole system is important. Make sure to take care of the future needs in address areas when planning large networks. A host can have multiple IP addresses, as shown in the Figure 1. A static IP addressing should be used in SYS600 system; see Configure a Static IP Address and [SYSINS, Host names] for more information.

Wireless networks are not recommended in a SYS600 system due to the high reliability that is required of the control system.

If SYS600 is installed in a Windows Active Directory domain environment, it is important to design the domain architecture correctly to meet the high reliability needs of the particular SYS600 system. For more information, see Active Directory Domain Services, Microsoft.

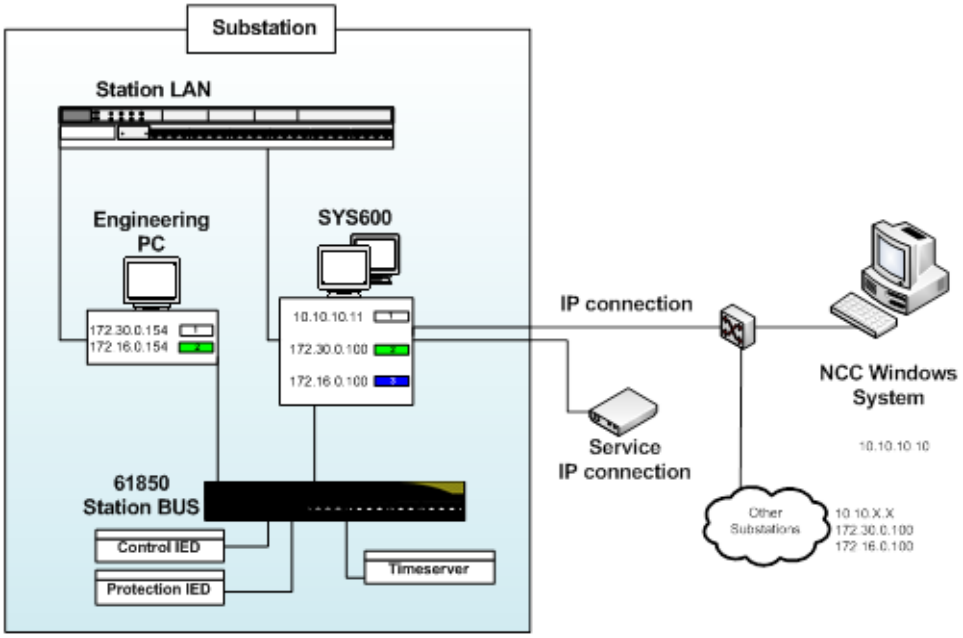


Figure 1: An example of SYS600 with NCC connection

MicroSCADA X products do not use IPv6. To disable IPv6 on network adapter, open Network and Sharing Center, select Change adapter settings, select a network adapter and right-click for properties, uncheck the box for Internet Protocol Version (TCP/IPv6) and then click OK.

See Appendix B to review secure and insecure communication protocols used in MicroSCADA X products and recommendations how to secure communication protocols.

4.1 Virtual Private Network (VPN)

This guideline considers the IP communication between SYS600 server and the Network Control Center (NCC) / Regional Control Center (RCC) via a dedicated wide area link that is not exposed to public access. The use case is to protect the dedicated link against man-in-the-middle attacks by guaranteeing confidentiality, integrity, and authentication via IPSec, using pre-shared key authentication. These instructions are also applicable to DMS600 systems.

The IPSec configuration must be done on all machines that should communicate with each other by IPSec. The configuration is shown in Appendix F.

IPSec encryption is a CPU consuming activity that can affect the maximum throughput and the CPU utilization. In order to determine the effect of IPSec encryption for data throughput and CPU consumption, it is important verify this with tests.

4.1.1 Use cases

4.1.1.1 NCC Communication

This use case features the IP communication between SYS600 and the NCC via a dedicated wide area link, which can be a glass fiber optics communication link, a microwave radio link, or a leased line that is not exposed to public access. The use of IPSec/VPN technology ensures that the transmitted data is not readable to eavesdroppers and vulnerable man-in-the-middle attacks. In addition, both SYS600 and NCC can authenticate using pre-shared keys before establishing the communication link.

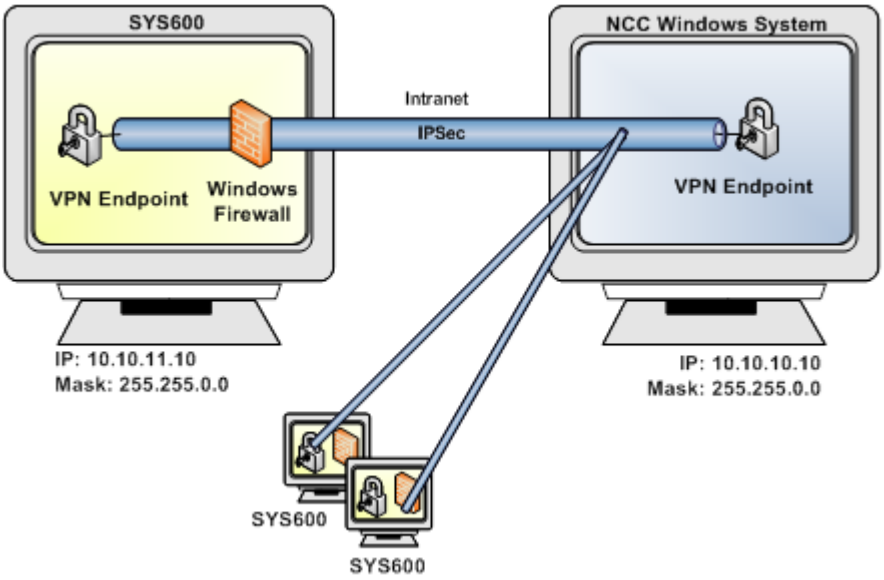


Figure 2: NCC communication

Figure 2 visualizes a possible setup for the use case. The VPN connections are illustrated as blue tubes, and multiple SYS600 devices are connected to the NCC system via the operator's internal IP network.

In case no network address translation (NAT) mechanism is used between SYS600 and NCC, IPSec can be run in transport mode, which encrypts all data of an IP packet but leaves the IP header intact, which allows for fast delivery.

4.1.1.2 Maintenance Access via Remote Desktop Protocol (RDP)

An alternative access to SYS600 is the use of the Remote Desktop Protocol (RDP). RDP provides a graphical interface for SYS600 on another computer. The RDP access should be restricted to Intranet access only. Authentication is done by conventional Windows user login. RDP uses encryption to protect all transmitted data, but it is still recommended to also use IPSec/VPN for maintenance access.

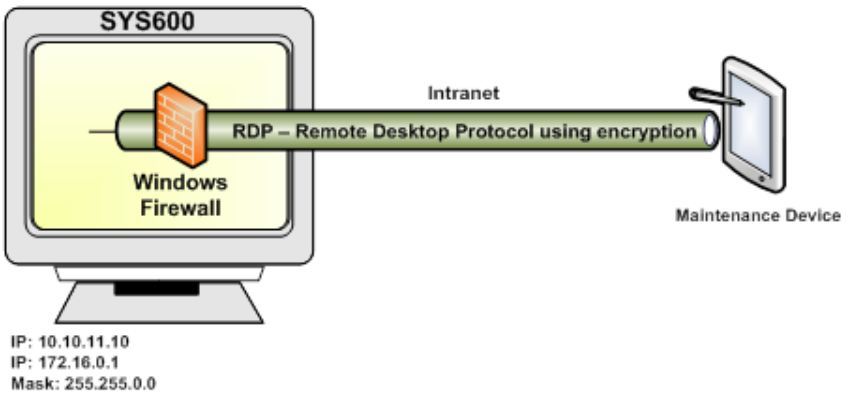


Figure 3: RDP Maintenance Access via VPN

Note that the firewall must accept incoming RDP connections, and the maintenance device connected to the VPN must be able to access SYS600's RDP port. As SYS600 has access to the station bus, the service engineer connected to SYS600's desktop can access the station bus via SYS600's desktop.

4.1.1.3 HSB communication

Another use case affects communication between a master SYS600 device and its redundant hot-standby-system via a wide area network connection. This link should be protected against man-in-the-middle attacks by guaranteeing confidentiality, authenticity, and authentication. This use case is comparable to NCC communication.

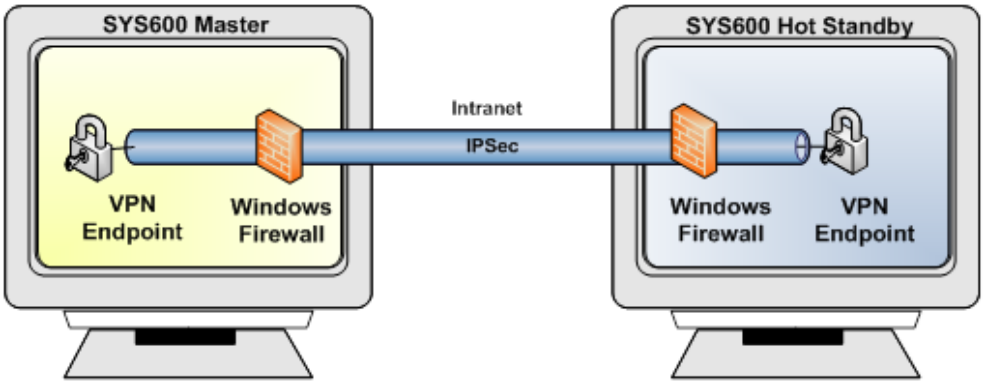


Figure 4: SYS600 to SYS600 communication

See Appendix F to configure VPN.

4.2 Network Devices

Network devices, such as switches, routers, firewalls, intrusion detection systems, modems, and wireless devices, are not part of this security guide. From a 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.

Section 5 Configuring security settings for Windows OS and MicroSCADA X servers

Windows servers are protected with latest service packs and security updates, firewalls, security policies, application whitelisting, and virus scanners. To reduce the attack surface in servers, programs and services not used can also be uninstalled or disabled. See Table 1 to check the security features automatically configured to the server. Some products need manual configuration.

Each of the sections below ends with either "This has to be configured manually" or "This is configured automatically". The first statement means that security setting has to be manually configured. The latter means that there is a security configuration tool to automate the configuration process. This process is described in Appendix A 1.1.

5.1 BIOS settings

The following settings must be applied:

- Password(s) are enabled
- Remote wake-up/Wake on LAN is disabled
- Boot sequence/priority: Disable boot devices, which are not required and leave only boot from hard disk.

This has to be configured manually.

5.2 Data Execution Prevention (DEP)

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 programs to make sure they use system memory safely. If a program tries running (also known as executing) code from memory in an incorrect way, DEP closes the program. DEP automatically monitors essential Windows programs and services. [MSDEP]

The default configuration of the operating system is used.

5.3 Removing unused programs

The following software is not used by SYS600 and DMS600 and can be manually removed from Windows through **Control Panel** (current Windows versions). These programs are normally found on desktop operating systems, such as Windows 10. On server operating systems, these are disabled by default.

Windows Component	
Windows Media Player / Media Features	Remove manually
Games	Remove manually
Windows Defender (in Windows 10 only when a 3rd party security program is used)	Remove manually, and uncheck **Windows Defender > Settings > Administrator > Turn on this app**. More details in section Virus scanner.
Microsoft Office	In some customer systems, Microsoft Office is installed. Remove features such as PowerPoint and Outlook from installation. Only leave features that are actually used, for example, Excel and Word. See Office documentation how to uninstall individual components from full installation.

This has to be configured manually.

5.4 Disabled system services

Enabled and disabled system services are listed in Appendix C.

This is configured automatically using security configuration tool.

5.5 Microsoft Update/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 MicroSCADA X products with the latest Microsoft security updates and service packs is tested and verified monthly. The test results can be found from the partner portal if you are a certified system integrator or if you are an end user, these reports can be made available to you based on your service agreement. The reports do not cover workplace computers but it is recommended to install all updates.

5.5.1 Windows Update vs. Microsoft Update

Windows Update only gets updates for Windows operating system. MicroSCADA X products are using other Microsoft products such as SQL Server and therefore, Microsoft Update should be used instead. See the Figure 5 to start getting updates for other products also.

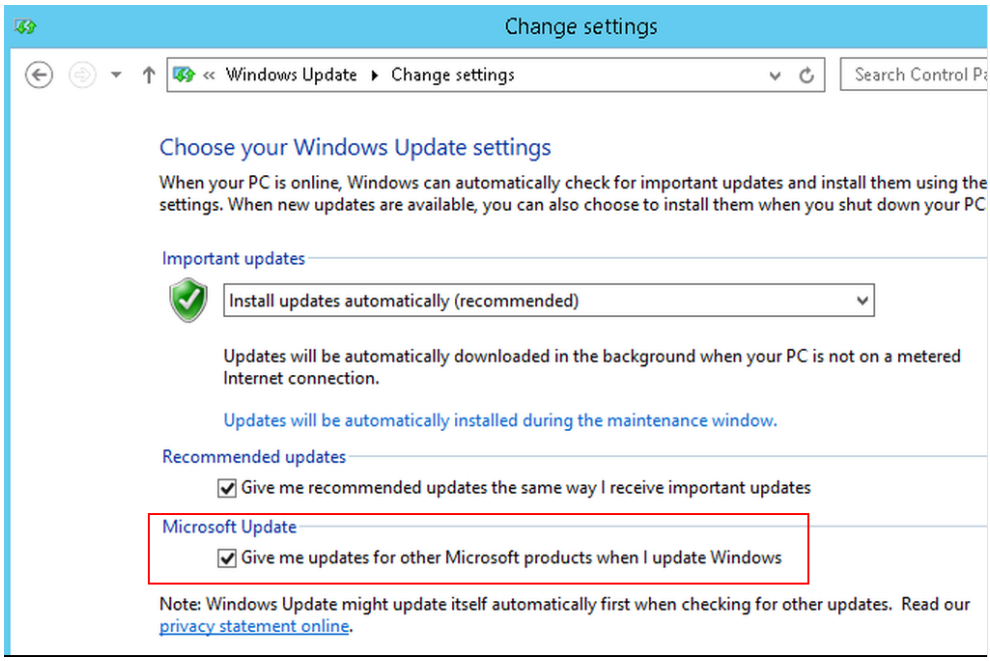


Figure 5: Microsoft Update Windows Server 2012

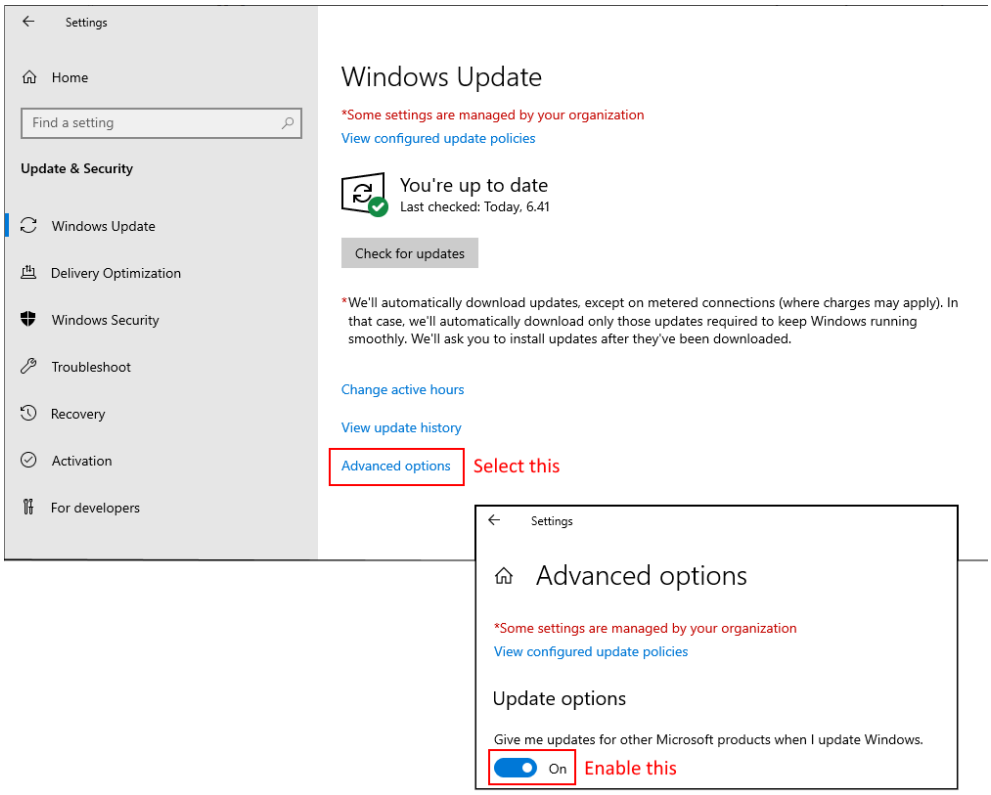


Figure 6: Microsoft Update Windows Server 2019

5.5.2 Configuration

A dedicated server, Microsoft Windows Server Update Services (WSUS), can be used for updating servers and workplaces. For more detailed information, see [WSUS].

To manually get Windows security updates for the standalone server, Microsoft Update Catalog can be used:

1. Check tested and verified security updates from MicroSCADA X Patch Compatibility Reports (linked above) for different operating systems.
2. Go to http://catalog.update.microsoft.com
3. Enter the bulletin ID mentioned in the patch compatibility report and the operating system of the server to the search field, for example, "4530715 Windows 2019" and press **Search**.
4. There might be several search results, for example, for different server architectures. Find the correct security update for the architecture and press **Add** to add it to the basket.
5. Repeat steps 3 and 4 for each security update.
6. Click **Show basket** and the content of the basket is shown.
7. Click **Download** to save all security updates in the basket to the disk. Create a new folder for the security updates, for example, *2019-12* indicating a year and a month of security updates.

This has to be configured manually.

5.6 Virus scanner

Whenever it cannot be guaranteed that unknown software is not executed on a machine (for example, due to enabling of removable devices or USB ports), the use of anti-virus software is highly recommended on servers, workstations, and maintenance laptops.

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). 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 testing the performance of the system 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 which are accessed continuously should be put in the exception list, that is, those files are not on-access scanned.

Various settings available in virus scanner programs for enhancing performance are shown below.

- Windows operating system directories should not be excluded
- Some virus scanner programs may not have the settings shown below

5.6.1 CPU Utilization

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

5.6.2 On-access scanning

- Scan only local disks, network scan is disabled (when each machine has its own virus scanner).
- Disable email scans.
- In general, nothing should be excluded from scanning, but in case there are some performance issues:
  - SYS600: <drive>\sc\apl*.* (including subdirectories) are frequently used. If this does not solve issues then exclude the whole sc directory.
  - DMS600: <drive>\DMS600*.*
- Excluded files:
  - Archive files such as .cab, .rar, and .zip
- Other settings
  - Enable buffer overflow protection
  - Enable access protection
  - Enable script scan

5.6.3 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 the like
- 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

5.6.4 Handling of infected files

- Automatic clean first, then quarantine. Deleting must be done manually by security specialist.
- Antivirus should not be allowed to clean, quarantine or delete SYS600 processes.
- Reporting:
  - Maintenance personnel should check virus scanner log files on each site visit. In case of virus detection, the issue must be escalated 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.

5.6.5 Scan engine and virus definition updates

- It is recommended that scan engines and virus definitions are updated automatically. 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. Note that a direct Internet connection should only be allowed for the time everything is downloaded; the connection is closed after downloading is finished. General guidelines are provided in [ABBSEC09, Balancing the

Demands of Reliability and Security: Cyber Security for Substation Automation, Protection and Control Systems].

- If redundant servers exist, it is recommended to update scan engine and virus definitions to these servers first. Reboot the server, open 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 above recommendation for redundant servers.
- Some scan engine updates may override current scan settings. In possible problem situations, this should be checked.

This has to be configured manually.

5.6.6 Patch management

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

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

For information on installing McAfee and Symantec virus scanners, contact the partner portal if you are a certified system integrator. If you are an end user, documentation is available based on service agreement. The compatibility of MicroSCADA X product with the latest upgrades and virus definitions is tested and verified monthly for some virus scanner programs. We recommend that servers are updated according to MicroSCADA X SYS600 Patch Compatibility Report and MicroSCADA X DMS600 Patch Compatibility Report.

5.7 Disabling devices

In any type of a server it is a good practice to disable the devices not used. This may include USB ports, CD/DVD drives, communication ports, and floppy disc controllers.

This has to be configured manually.

Run devmgmt.msc (Device Manager) and look for the devices to be disabled.

The following figure shows the disabling of DVD/CD-ROM driver, Floppy Disk Driver, Sound, Video and Game controller, and finally the Universal Serial Bus (USB) ports.

Do not disable a device if it will be used, for example, USB license keys, alarm sounds, or software installations.

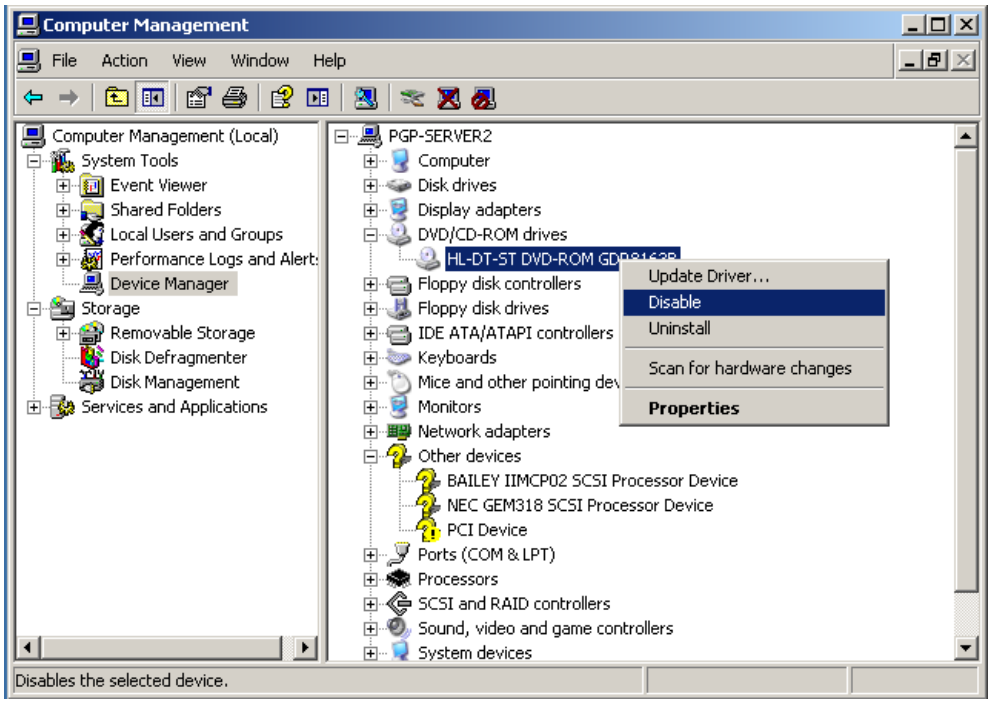


Figure 7: Disabling DVD/CD-ROM

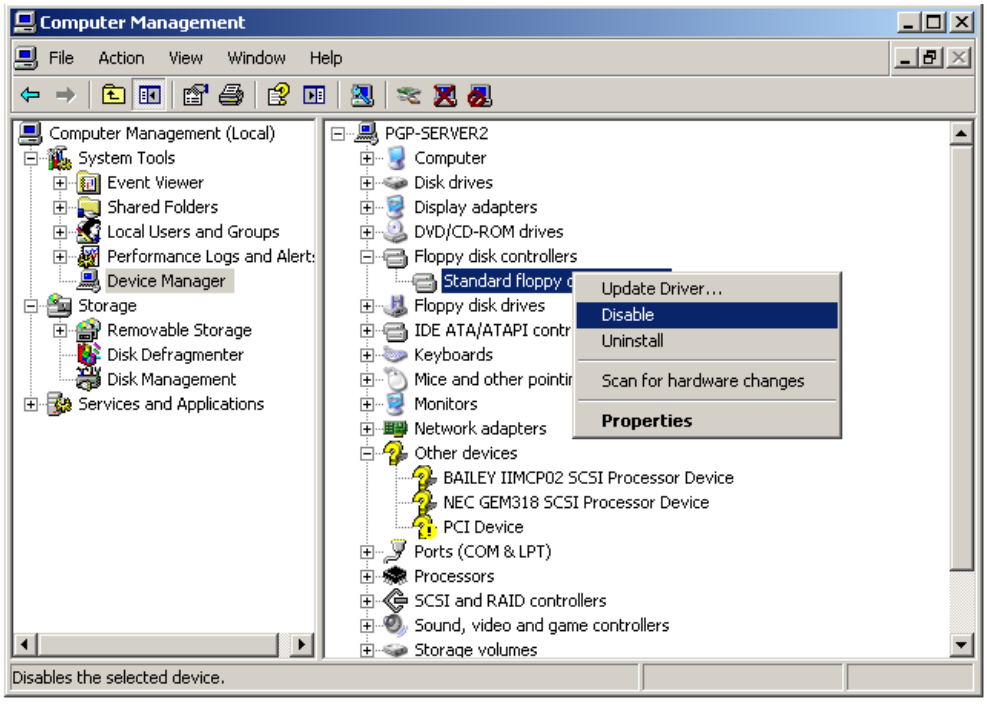


Figure 8: Disabling Floppy disk controller

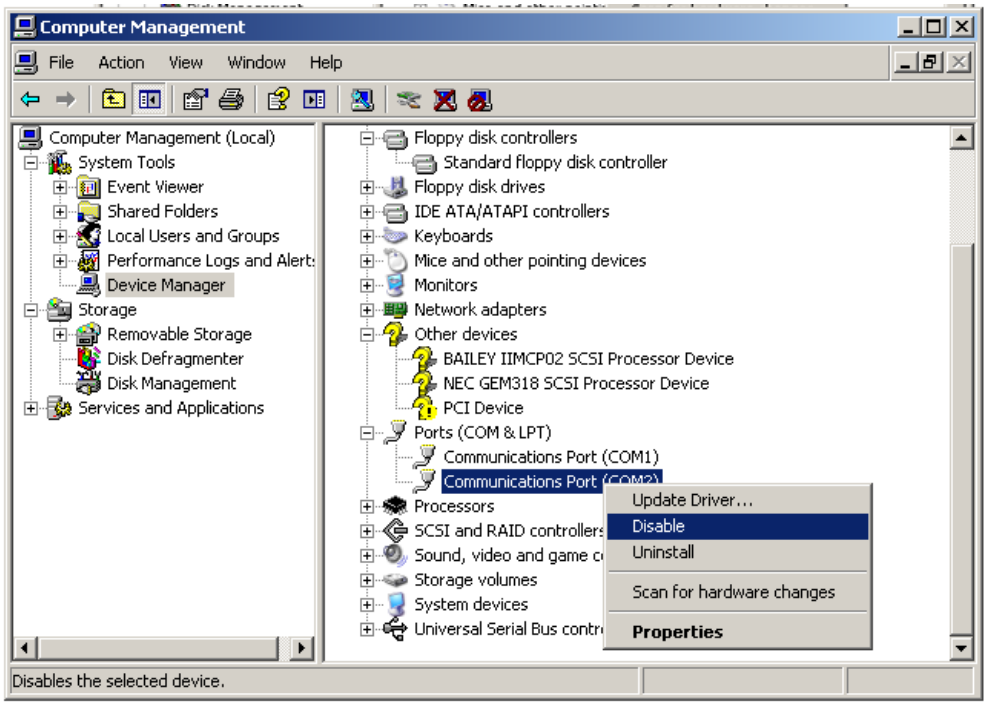


Figure 9: Disabling Serial port

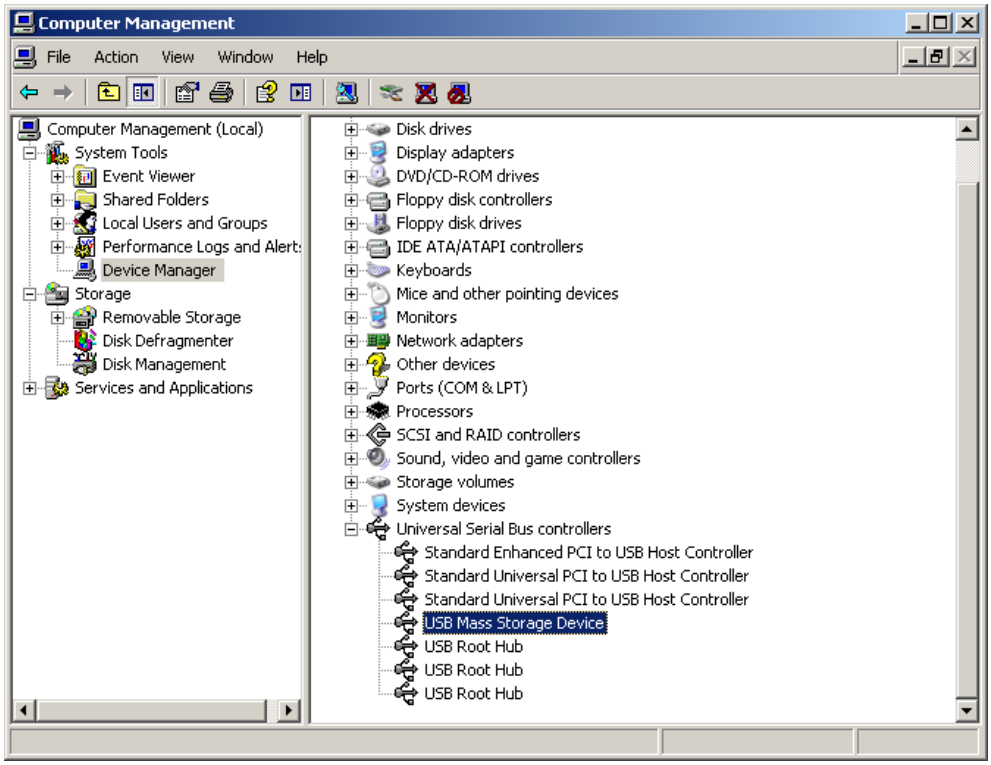


Figure 10: Disabling USB Mass Storage Device, see also http://support.microsoft.com/kb/823732.

5.7.1 Disabling autorun functionality

Whenever the disabling of a device is not possible, it is good practice to disable the autorun functionality of the device. In order to prevent the automatic start of malicious code contained in a removable device, autorun functionality must be turned off. For more information, see How to disable the Autorun functionality in Windows, http://support.microsoft.com/kb/967715/en-us.

This is configured automatically using security configuration tool.

5.8 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 improperly use the computer. Warning banners in SYS600 are configurable and are located in:

- Windows OS login
- SYS600 Monitor Pro login
- SYS600 Monitor login

Workplace X and WebUI have pre-configured warning banners, and currently they can't be modified.

To modify texts in warning banners:

1. Start Registry Editor to modify Windows OS banner
2. Go to the following keys:
   - MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption
   - MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText
3. Start Monitor Pro, select **Tools/Engineering Tools/Display Builder** and open sc\prog\graphicsEngine\lib\views\Startup.v to modify the SYS600 Monitor Pro banner
4. Start Monitor Pro, select **Tools/Engineering Tools/Tool Manager/Dialog Editor** and open sc\sa_lib\base\bbone\use\BGU_LOGIN.VSO to modify the SYS600 Monitor banner

A warning banner affects to Windows automatic logon (autologon) feature. The banner has to be acknowledged by pressing the **OK** button. After pressing the button automatic logon occurs and programs placed to Startup folder will start.
Note! It is not recommended to use Windows automatic logon feature, since Windows stores the user name and the password in cleartext in the Windows registry. This is a security risk. If the end-user accepts this risk, the workaround is to clear above Windows registry keys.

This is configured automatically using security configuration tool, pre-configured dialogs and process displays.

5.9 User Account Control (UAC)

UAC is a security feature available in current Windows versions. UAC should be enabled in all servers and workplaces. If the program requires privilege elevation, the behaviour is following:

- For administrators: Prompt for consent. A dialog is shown where either Continue or Cancel can be selected.
- For standard users: When a standard user attempts to perform a task that requires an administrative access a credential prompt is presented.

A user with administrative privileges starts programs by default with non-admin privileges. If administrative privileges are needed, for example, to write some file with Notepad to the file system where Windows standard users do not have permissions to write, this write will fail. Start programs with "Run as administrator" if you need administrative privileges. A consent dialog is shown that program is to be run with administrative privileges.

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. For more information, see [UAC].

This is configured automatically using security configuration tool.

5.10 OPC and DCOM

The usage of OPC communication between the OPC client and the server requires that Distributed COM (DCOM) has been properly configured in the Windows operating system. This includes configuring mutual user accounts between computers, system-wide DCOM settings, OPC server specific DCOM settings, and firewall rules.

Distributed Component Object Model (DCOM) uses the Remote Procedure Call (RPC) dynamic port allocation. By default, RPC dynamic port allocation randomly selects the port numbers. One can control which ports RPC dynamically allocates for incoming communication and then configure the firewall to confine incoming external communication to only those ports and port 135 (the RPC Endpoint Mapper port) [MSDCOM04].

This has to be configured manually, see [SYSINS, Opening Monitor Pro using Remote Desktop Services] and [DMSSYS, Connecting OPC]

From SYS600 9.4 version, OPC Data Access Server requires authentication. A SYS600 login is required from OPC clients connected to the system via OPC Data Access Server (OPCS). This setting can be found from sys_bascon.com configuration file.

5.11 Simple Network Management Protocol (SNMP)

By default, SNMP services are enabled in MicroSCADA X server security settings. These services must be installed on the computer first through Programs/Windows features. SNMP version 3 or later should be used.

This is configured automatically using security configuration tool.

5.12 Security policies

Security policies are based on security templates from Microsoft [MSWS03]. These policies are modified for MicroSCADA X product purposes in servers and workplaces. The templates are categorized into the following sections:

- Account policies
- Audit policy
- User rights
- Security options
- Event log
- System services

This is configured automatically using security configuration tool. See Appendix A 1.1. See also Appendix D to see the changes to default values.

5.13 Firewall (ports and services)

Windows Firewall is a stateful firewall, which can be configured to allow/block inbound and outbound connections in current Windows versions. Windows Firewall settings configured using the security configuration tool are **not** configured to the public network profile. The computer might detect itself to the public network meaning that almost all traffic will be blocked by Windows Firewall. The scope options for the firewall settings are ALL or SUBNET. SUBNET is a general setting option allowing only local network (subnet) traffic through the firewall. For more information, see Windows Defender Firewall with Advanced Security.

Other general settings are:

- Firewall: enabled, block inbound, allow outbound
- Logging: enabled, %windir%\pfirewall.log, 32767kB
- Notify when an application is blocked.

Ports and services used by MicroSCADA X products as well as default firewall settings are listed in Appendix B. We recommend using both hardware and software firewalls to have a well-protected system.

This is configured automatically using security configuration tool, see Appendix A 1.1.

5.14 User account management

Below table lists Windows users and groups, which are preconfigured in the SYS600C device with security configuration tool. MicroSCADA user account is created during SYS600 installation, as well as Windows OS groups. There is an option to install preconfigured Windows groups during DMS600 installation.

To create new Windows user accounts, see Appendix A 1.3.1. Do not give administrative rights (membership of Administrators) to operators, viewers, and engineers. Only system administrators should have administrative rights. See also SYS600 and DMS600 Section 7.1 to see other user accounts used in the product.

Table 4: SYS600 Windows users and groups

User account type	Name	Password	Privileges	Remarks
Windows OS user	MicroSCADA	Configurable	Administrator	Created during the SYS600 installation. Use **SYS600 Control Panel** to change this password so that DCOM settings are automatically configured. Used by the MicroSCADA service, interactive logon is not allowed.
Windows OS user	ScAdmin	Configurable	Administrator	Created by security configuration tool. The built-in Administrator user account name is renamed to ScAdmin, see also caution below.
Windows OS user	ScEngineer	Configurable	Standard user	Created by security configuration tool. The user account is disabled by default. End-users may enable this user and create a password.
Windows OS user	ScOperator	Configurable	Standard user	See above
Windows OS user	ScViewer	Configurable	Standard user	See above
Windows OS groups	ScSecAdmins ScSecAuditors ScRBACManagers ScSysAdmins ScEngineers ScOperators ScViewers	N/A	N/A	Created during installation of SYS600. Other security areas such as Local security policy, Application whitelisting and Windows standard user (file system permissions) are based on these groups. See Section 7.2.

The built-in Administrator user account name is renamed during the hardening. Administrator user account name cannot be used to login to the computer anymore, ScAdmin must be used instead. This means that before adding new users to the server, there are two administrative users only: MicroSCADA and ScAdmin.

Keys to password strength: length and complexity

- An ideal password is long and has letters, punctuation, symbols, and numbers.
- Whenever possible, use at least 14 characters or more.
- The greater the variety of characters in the password, the better.
- Use the entire keyboard, not just the letters and characters used or seen most often.

This is configured automatically using security configuration tool.

5.15 Application whitelisting

Windows AppLocker is a feature in Windows OS's that allows the user to specify which users or groups can run particular applications in the organization based on unique identities of files. If the AppLocker is used, rules to allow or deny applications from running can be created. Today's organizations face a number of challenges in controlling application execution, including the following:

- Which applications should a user have access to run?
- Which users should be allowed to install new software?
- Which versions of applications should be allowed? [APPLOC12]

This is configured automatically using security configuration tool. See Appendix E.

5.16 Backing up and restoring

The following instructions are taken from [SYSCUG].

5.16.1 Taking backup

Backing up the MicroSCADA X server with disc imaging software (for example Acronis True Image or Norton Ghost) is highly recommended. The image should be saved on a network drive or on a USB flash drive. Refer to the instructions from the disc imaging software manufacturer on how to accomplish this.

Recommendations for image backup:

- Servers: every 3 months.
- Workplaces: every 6 months.

This has to be done manually.

5.16.2 Restoring backup

The method for restoring the disc image depends on the disc imaging software. Refer to the instructions from the disc imaging software manufacturer on how to accomplish this.

This has to be done manually.

Section 6 Configuring security settings for SYS600, SYS600 Historian and DMS600 workplaces

To harden the workplace computers, see Appendix A 1.2.

The preferred technology between the SYS600 server and the remote workplace computer is Workplace X or WebUI (via browser). For more information about opening monitors, see [SYSINS, Opening SYS600 Monitor Pro].

To support applications not build with new graphics, a monitor (Monitor Pro or classic monitor) needs to be opened. For this purpose an installation of the SYS600 software into SYS600 Workplace computers is not required. It is enough that SYS600 Workplace computer has software installed enabling a remote connection to the SYS600 Server. A monitor can be opened either on the server computer or through a remote connection. If the SYS600 Workplace is a remote computer, connection to the server computer is established over the network by using the remote client. By default, the SYS600 service is started in the server directly after Windows has been started. This is an automatic startup of the service, that is, no user needs to log in.

Windows automatic logon feature has been used on the server machine to automatically open MicroSCADA monitors in remote SYS600 workplaces. However, the use of this feature of the Windows operating system is not recommended since Windows stores the user name and the password in cleartext in the Windows registry, which is a security risk.

6.1 Securing Vtrin client and SYS600 Historian server communication

Historian server installation creates a self-signed certificate, which is used to encrypt communication between Vtrin client and Historian server. The certificate is imported to the workstation computer where Vtrin client is to run. For more information, see [HISADM, Managing Client Software Distribution]

Section 7 Configuring security features in SYS600, SYS600 Historian and DMS600 products

This section lists the security features such as user account management and authorization available in the MicroSCADA X products.

All the settings presented in this section have to be configured manually.

7.1 User account management

MicroSCADA X products SYS600 and DMS600 have their own user account management and they allow user account creation, modification, and removal. They support several user accounts. The products allow user roles with individually configurable permissions. User names are associated with a certain user profile that restricts the user's access rights to the system. For Windows operating system related user accounts, see Section 5.14. SYS600 Historian authentication is based on Windows user accounts. It does not have user management of its own.

SYS600 supports local and centralized user account management scenarios. For centralized management, a separate feature ABB Authentication Service has to be installed that then communicates with SDM600 server. For more information, [SYSINS, Authentication Service].

Windows single sign-on

From SYS600 9.4 FP2 HF2 version onwards there is Windows single-sign-on (SSO) functionality. For more information, see [SYSOBJ, WS attribute] and [SYSAPL, Windows single sign-on].

Table 5: SYS600, SYS600 Historian and DMS600 users and groups

User account type	Name	Password	Privileges	Remarks
SYS600 application	Configurable	Configurable	Administrator	There are no preconfigured user accounts in SYS600 application. By default, the first user logging onto SYS600 Monitor Pro after the SYS600 installation automatically gets system administrator privileges and is able to use the user account management tools for SYS600. For more information, see [SYSAPL, User Management].
SYS600 application (anonymous user)	Configurable	N/A	Configurable	There are no anonymous users by default in SYS600 application. However, it is possible to create, for example, a user having no password and with viewer privileges. For more information, see [SYSAPL, User Management]. **Warning!** By enabling this feature the product behavior is against industry cyber security recommendations/standards. It enables to operate the system from remote computer anonymously with admin privileges (if configured).
SYS600 CET/MS SQL Server database	SystemUser	Configurable	Administrator	Created during SYS600/CET installation. Password can be changed from CET or by using SQL Server tools. SQL Server database users cannot be used for login to the Windows operating system. By default, Mixed mode authentication is configured by SYS600/CET installation.
SYS600 CET/MS SQL Server database	sa	Configurable	Administrator	Created during SYS600/CET installation. Password can be changed from SQL Server tools, see link.
SYS600 IEC62351-5 based authentication for DNP3 and IEC60870-5-101/104	Configurable	N/A	Configurable	Created during communication engineering (Authority Tool) if IEC62351-5 based authentication is enabled.
SYS600 communication protocols	Configurable	Configurable	Configurable	Created during communication engineering. For example, IEC 61850 MMS and FTP protocol users and passwords may be needed for communication to IEDs, for example, disturbance recording. Other protocols such as LON, SPA, IEC60870-5-101, IEC60870-5-104 may require protocol specific user credentials.
SYS600 Historian	Configurable	Configurable	Configurable	SYS600 Historian uses Windows user accounts. It does not have separate user management of its own. These users have to be assigned a membership to rtdb-* Windows groups.

Table continues on next page

User account type	Name	Password	Privileges	Remarks
DMS600 WS/NE	ADMIN	Configurable	Administrator	Created during DMS600 installation. To prevent unauthorized access to the system, the password of this user has to be changed right after the DMS600 installation.
DMS600 MS SQL Server database	sa	Configurable	Administrator	Created during DMS600 installation when MS SQL Server Express is installed. This user is automatically created by the Express installation and it is by default disabled. Password can be changed from SQL Server tools, see link. By default, Windows authentication is used by DMS600.
DMS600 SCIL API	Configurable	Configurable	Administrator	Created during DMS600-SYS600 interoperability configuration. This is a legacy protocol: The use of SCIL API has been replaced with OPC communication. **Note!** User credentials are stored in plaintext in the filesystem.

To configure user accounts in SYS600:

1. Open SYS600 Monitor Pro.
2. Open **Tools/Engineering Tools/User Management...**

To get information about user accounts in SYS600 Historian:

1. Open Vtrin client
2. Select **Maintenance > System > Users** to get information about users
3. Select **Maintenance > System > Vtrin > Roles** to manage and get information about roles

To configure user accounts in DMS600:

1. Open DMS600 Workstation
2. Select **Settings > User Manager...**

In addition to user roles, DMS600 also has a region management for each user.

7.2 File system permissions

File system permissions restrict user access to the product installation directory and system files and those also allow granting more permissions for non-admin user accounts. MicroSCADA X supports running operator applications such as SYS600 Monitor Pro, DMS600 Workstation and Vtrin historian client as non-admin user accounts. Following file system permissions are deployed by security configuration tool:

Windows user group s	Permissions
ScViewers, ScOperators	Read and execute permissions to the product installation directory. In SYS600 modify permissions are given to sc\apl\<aplname>\PAR and PICT directories to write user or tool specific information. These permissions are required by Monitor Pro, for example. In DMS600 modify permissions are given to DMS600\doc and logs directories. These permissions are required by DMS600 Workstation and Network Editor, for example.
ScEngineers, ScSysAdmins	Full permissions to the product installation directory. The user running the security configuration tool is automatically assigned to ScSysAdmins group. These permissions are required by engineering tools, for example, those available in Tool Manager dialog and also Communication Engineering Tool (SYS600).
RTDB-admin RTDB-operator RTDB-readonly	In addition to file system permissions, in SYS600 Historian these groups are used to limit access to Vtrin tree. RTDB-admin: Apply Vtrin administrator users (for example Administrator and MicroSCADA) as the member of this group to have full access within Vtrin user interface. RTDB-operator: Apply Vtrin users (for example Engineer) as the member of this group to have limited access control to the tree view nodes/leafs and to have those hidden. RTDB-readonly: Apply Vtrin users (for example User) as the member of this group to have mostly Read and Execute access rights.

7.3 Password policies

MicroSCADA X products support passwords with alphanumeric and special characters. Uppercase (A-Z) and lowercase (a-z) characters as well as characters from other character sets (localization) are also supported. Password handling is case-sensitive.

By default, password complexity is disabled. The system administrator may enable password complexity. Other settings include a minimum password length, as well as forcing different characters to be used in the password (a combination of alphanumeric and special characters). The maximum password length is 63 bytes (63 ASCII characters).

To configure password policies in SYS600:

1. Open SYS600 Monitor Pro.
2. Open **Tools/Engineering Tools/User Management...**
3. In the user management dialog, open **Tools/Password Policy...**

For more information, see [SYSAPL, User Management].

SYS600 Historian user accounts are managed by Windows operating system, see **secpol.msc > Account Policies > Password Policy**

To configure password policies in DMS600:

1. Open DMS600 Workstation
2. Open **Settings > User Manager...**
3. In the user management dialog, open **Password Policy...**

For more information, see [DMSSYS].

Keys to password strength: length and complexity

- An ideal password is long and has letters, punctuation, symbols, and numbers.
- Whenever possible, use at least 14 characters or more.
- The greater the variety of characters in the password, the better.
- Use the entire keyboard, not just the letters and characters used or seen most often.

7.4 Authentication and authorization

There is individual user authentication to control access to MicroSCADA X products that allows tracing operations back to individual user accounts for the purpose of accountability. Products support role management that can be given individually configurable permissions, which are used in authorization. For more information, see:

- [SYSAPL, sections User Management and Authorization]
- [DMSSYS, sections User and Region Management and User Level Rights]
- [HISADM, sections Access Control and Roles]

7.5 User session and inactivity time-out

MicroSCADA X SYS600, SYS600 Historian and DMS600 workstations operate in Windows operating system. It is possible to configure the user inactivity time and lock the workstation in the Windows screensaver settings. In newer operating systems such as Windows 10 inactivity timeout is 15 minutes and it controlled by a registry setting. This setting can be disabled by running SCM security baselines (HKLM\Software\Microsoft\Windows \CurrentVersion\Policies\System\InactivityTimeoutSecs=0).

SYS600 product also has user session and inactivity time-out after certain period of time. The time period is given in hours (from 1 to 255). It is also possible to configure session expiration notifications. When user is logged out from SYS600 after some time period, the user is also logged out from DMS600.

To configure user session and inactivity time-out in SYS600:

1. Open SYS600 Monitor Pro.
2. Open **Tools/Engineering Tools/User Management...** and select Timeouts.

This setting affects also to Workplace X and WebUI sessions. For more information, see [SYSAPL, User Management].

7.6 User activity logging

MicroSCADA X system can be configured to log events from the process, such as switching device opened/closed and these are shown in the event list. Furthermore, the user activity events related to security are logged. This includes events such as:

- Login success/failure
- Logout
- User created/deleted
- Role created/deleted/assigned
- Password changed/expired

In addition to these, communication modules may log security and diagnostic related UAL events. See protocol specific manuals for details.

Furthermore, these events can be forwarded to external log servers such as Syslog or ArcSight. Windows operating system also includes events, which can be accessed with Windows Event Viewer.

For more information, see [SYSCON, User Account Logging] and [DMSSYS, User Activity Logging] and [HISADM, Diagnostics].

7.7 SYS600 hardening options

SYS600 system configuration settings are protected through file system permissions and restrictions on remote connection. Workplace X and WebUI are preferred ways to use application. However, due to backward compatibility reasons SYS600 Workplaces can connect the server through Remote Desktop Services. Remote connection should be configured so that the user of the SYS600 Workplace only has access to the SYS600 Monitor Pro application, that is, the user has no permissions to open other applications in the server machine. For more information, see [SYSINS, SYSCON].

File system permissions are configured automatically during the installation of SYS600. Remote connection has to be configured manually.

SYS600 base system contains system hardening attribute SYS:BHD. This attribute can be used for toggling certain cyber security features on and off. The exact list of attributes and their values are described in the SYS600 Base System Objects manual. The default values are recommended when system is set up. On production systems the REQUIRE_KNOWN_ACP_CERTIFICATE should be set to TRUE. In certain legacy configurations it might be necessary that certain security features are turned off. This should be done only when system can't be set up otherwise. For more information, see [SYSCON, Encrypted communication].

7.7.1 PostgreSQL related firewall configuration

MicroSCADA X is using the PostgreSQL to store user settings related to Workplace X. In one node systems, the connection to the PostgreSQL database is needed only from the localhost, but in HSB configurations the remote HSB pairs need the PostgreSQL port to be open. By default, it is TCP port 5432, but in custom configurations it can be different.

SCM creates the required firewall rules for PostgreSQL connections which are set to disabled. The Remote Address is set to 127.0.0.1 by default.

Before SCM 1.6, which is released with SYS600 10.2, the rules were set to enabled and Remote Address was set to *Local Subnet*.

If you are not using SCM in your systems, you can create the rule(s) manually.

Inbound Rules

Name	Profile	Enabled	Action	Local Address	Remote Address	Protocol	Local Port
sys600: pgsql	Domain	No	Allow	Any	127.0.0.1	TCP	5432
sys600: pgsql	Private	No	Allow	Any	127.0.0.1	TCP	5432

Figure 11: Firewall rules for PostgreSQL created by SCM

While configuring the HSB system, enable the firewall rule and allow the connections only from the remote HSB server. This must be done on all HSB servers.

1. Go to **Start/Windows Defender Firewall with Advanced Security**.
2. Select **Inbound Rules**.
3. Find the *sys600: pgsql* rule, right click on the rule with the correct Profile (Domain/Private, depends whether this server is domain joined or not) and select **Properties**.
4. Go to **Scope** tab and add/edit the correct remote HSB server IP address and click **OK**. You can add multiple remote addresses, if necessary.
5. Go to **General** tab, select **Enabled** and click **OK**.

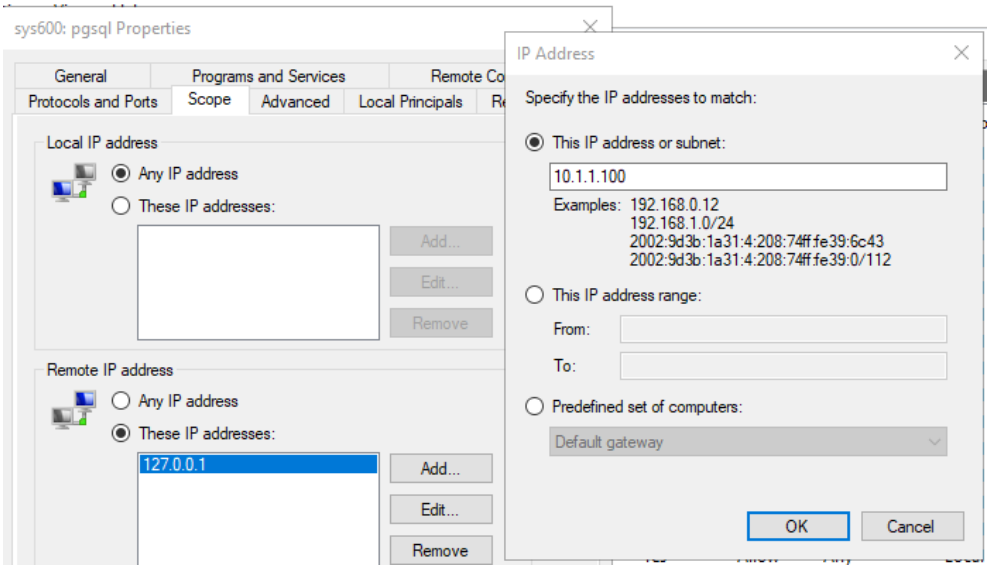


Figure 12: Adding the IP address of the remote HSB pair to the firewall rule

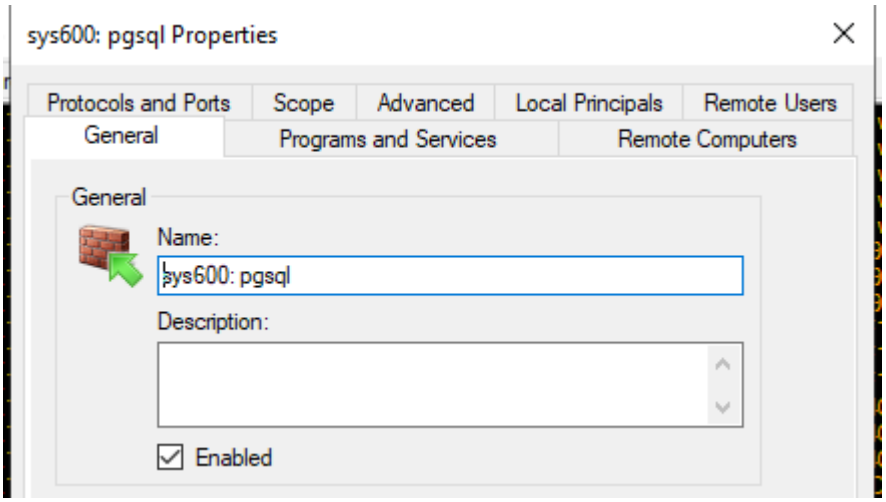


Figure 13: Enabling the PostgreSQL firewall rule

Now the rule is **Enabled**, and the connection is allowed only from the remote HSB server IP, as shown in the Figure 14.

Figure 14: PostgreSQL firewall rule is enabled with the correct remote IP address

7.8 SYS600 Historian hardening options

7.8.1 Securing Data source and Historian server communication

SYS600 data source connection to Historian server database is established using WebSocket Secure communication (SYS600 Historian 1.2 or later). The connection string to be used is wss://<host>/history in the SYS600 database logging profile configuration. For more information about data source configuration, see [SYSCON, Historian] and [SYSAPL, SYS600 Historian]

7.9 DMS600 hardening options

DMS600 system configuration settings are mainly stored to the relational database. Authentication is required to read and write to the database. It is recommended to use Windows authentication and preconfigured Windows groups such as ScViewers and ScOperators to access the database. For more information, see [DMSINS, Database Server Installation].

Use of TLS Version 1.0 is flagged as an old version (from July 2018) by several security auditing tools based on PCI DSS (payment card industry security standard). MS SQL Server 2014 installed with DMS600 must have TLS 1.0 enabled to use DMS600 applications. TLS 1.0 is controlled by MACHINE \SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols \TLS 1.0\Server\Enabled registry setting. TLS 1.0 setting is enabled in DMS600 security baseline included in the security configuration tool (SCM).

DMS600 Workstation and Network Editor can be opened with non-admin rights (Windows standard user). There are some file system permissions, which are needed and these are configured automatically using security configuration tool.

7.10 Certificate management

Private keys, which are used in encrypted communication, should not be left unprotected in the file system and must be protected with access control lists (ACL). Verify that only users needing read/write access have permissions to access private keys. This is normally Administrators group in Windows. SYS600 10.0 installation protects many of certificates listed below automatically. However, in customer deployments it is required to manually configure access control list of certificates needed, for example, in DNP 3.0 and IEC60870-5-104 secure communication.

Secure communication such as HTTPS use private keys and public certificates to encrypt communication channels. By default, self-signed certificates are generated when the product is initialized. It is recommended to replace self-signed certificates with certificates generated by, for example, internal certificate authority (CA). Following table lists certificates used in SYS600.

Table 6: Certificates used in SYS600

Description and usage	Location	Protection	Supports externally generated certificates	Remarks
Web server secure communication (https)	Windows certificate store > Certificates (Local Computer) > Personal > Certificates: MicroSCADA Private key and public certificate (self-signed certificate)	Self-signed certificate is accessible for Administrators group and LocalService account in Windows certificate store.	Yes	• Self-signed certificate is created at MicroSCADA startup. • Documentation: see System Configuration Manual > Configuring web server.
IEC60870-5-104 secure communication between master and slaves. IEC 60870-5-104 secure authentication (IEC/TS 62351-5) with TLS (IEC62351-3). TLS should only be used when secure authentication is configured. By default, there is no secure authentication.	Location of private key and public certificates can be chosen freely, for example, by creating a new directory such as sc \prog\pc_net\ certs\.	ASCII PEM format, human readable. Passphrase protection can be configured.	Yes	• Self-signed certificate is created according to IEC 60870-5-104 protocol settings if configured. • Documentation: SYS600 IEC 60870-5-104 Slave Protocol Manual > Instructions > Configuration > Communication system configuration > Security attributes; SYS600 System Configuration Manual > Configuration > Configuring process communication > Configuring process communication units > Secure communication using TLS (IEC 62351-3)

Table continues on next page

Description and usage	Location	Protection	Supports externally generated certificates	Remarks
DNP 3.0 secure communication between master and slaves. DNP 3.0 v5 secure authentication (IEC/TS 62351-5) with TLS (IEC62351-3). TLS should only be used when secure authentication is configured. By default, there is no secure authentication.	See IEC 104 above	See IEC 104 above	Yes	• Self-signed certificate is created according to DNP 3.0 protocol settings if configured. • Documentation: SYS600 DNP v3.00 Slave Protocol Manual > Instructions > Configuration > Communication system configuration > Security attributes; SYS600 System Configuration Manual > Configuration > Configuring process communication > Configuring process communication units > Secure communication using TLS (IEC 62351-3)
Hot-stand-by (HSB) replication secure communication	sc\sys\active\sys_ \keys file or directory Private key and public certificate (self-signed certificate)	ASCII PEM format, human readable.	No	• Self-signed certificate is created at MicroSCADA startup. • Documentation: SYS600 System Configuration Manual > Encrypted communication.
Postgre database replication secure communication	Programdata\abb \microscada pro \postgresql \postgredata \server.key Programdata\abb \microscada pro \postgresql \postgredata \server.crt	ASCII PEM format, human readable.	Yes	• Self-signed certificate is created at MicroSCADA startup. • Documentation: No

Table continues on next page

Description and usage	Location	Protection	Supports externally generated certificates	Remarks
Remote desktop protocol (RDP)	Windows certificate store > Certificates (Local computer) > Remote desktop > Certificates	Self-signed certificate is accessible for Administrators group only in Windows certificate store. Private key cannot be exported.	Yes	• By default, self-signed certificate is created for RDP by Windows. Users can replace this. However, from the security perspective it is more important to configure Network Level Authentication (NLA) for RDP. • Documentation: Using custom certificate in RDP, see link. Configure NLA, see link.
Used for DuoDriver drivers	Sc\setup\duodriver\ vendor.cer	-	-	• Included in the installation package. Do not modify. • Documentation: Duodriver 5.0 Installation Guide.
Used for license protection	Sc\prog \61850_opc_server\ cet\ bin\ iec61850 libraries\ chpau.pfxserver.key	-	-	• Included in the installation package. Do not modify. • Documentation: No

7.11 Resetting administrator password

This feature is used if the SYS600 system administrator's user name or password is lost. In this case, it is possible to login to the system using a temporary password. For more information, see [SYSOBJ, EY attribute].

This feature is used if the DMS600 administrator's user name or password is lost. To reset password:

1. Open relational database and find user management table
2. Remove user account 'admin'
3. Close the database and login with 'admin' user name, see [DMSSYS, User Management]. Change the password immediately.

7.12 Backdoors

The following feature has a backdoor to the system: Resetting administrator password.

To reset SYS600 administrator password, Windows user has to have administrative privileges to the Windows operating system. If the attacker has these privileges, then the system has

already been compromised and it is, for example, possible to install keylogger to find users and passwords of the industrial control system.

Section 8 Standard compliance statement

Cyber security issues have been the subject of standardization initiatives by ISA, IEEE, or IEC for some time. Hitachi ABB Power Grids plays an active role in all these organizations, helping to define and implement cyber security standards for power and industrial control systems. Hitachi ABB Power Grids participates in the development by delegating subject matter experts to the committee working on the respective standard.

Hitachi ABB Power Grids strongly recommends to use also existing common security measures available in the market, for example, VPN for secure Ethernet communication.

Table 7: Overview of cyber security standards

Standard	Main focus
NERC CIP	NERC CIP cyber security regulation for North American power utilities
IEC 62443-4-1 IEC 62443-4-2	Product and product development security
IEC 62351	Data and communications security
IEEE 1686	IEEE standard for substation intelligent electronic devices (IEDs) cyber security capabilities

Hitachi ABB Power Grids has identified cyber security as a key requirement and has developed a large number of product features to support the international cyber security standards such as NERC CIP, IEEE 1686 and IEC 62351/62443.

Appendix A Quick Configuration Guideline

In this section, the configuration of computers (both servers and workplaces) used in MicroSCADA X systems is described in simple steps.

In order to reduce the risk of having malware planted into the system in the engineering phase, deploying security settings right after installing MicroSCADA X software is recommended and that basic security steps are taken to secure all computers in the system. MicroSCADA X product includes a security configuration tool for configuring several security categories in the computer:

- **Windows users and groups**: Users and respective groups are created according to IEC 62351 roles. Non-admin user accounts are automatically created. Note that configurations of other security categories, namely Application Whitelisting, Local security policy, and File system permissions, are based on these groups.
- **Firewall**: Enables firewall and preconfigures product specific ports. Communication protocols are by default blocked.
- **Local security policy**: Secures the computer with Password policy, Account policy etc.
- **Services**: Unnecessary services are disabled
- **Windows standard user/File system permissions**: Restricts user access to MicroSCADA X installation folder and assigns permissions for non-admin user accounts automatically.
- **Audit policies**: Configures what events are logged into Windows event logs.
- **Application whitelisting**: Windows AppLocker is used to restrict access to programs.

Security configuration tool overrides current security configuration of the computer. This might be a problem if some 3rd party software has made changes to the system, for example, to firewall rules. If these changes are known they can be defined in a custom baseline, which is then enforced along with MicroSCADA X baselines and thus reducing the problems. In addition to firewall rules, local security policies and especially user rights assignments might produce problems. The security configuration tool is designed to take into account user rights where other than built-in Windows group is used. For example, if some 3rd party backup software has created an individual Windows user account and changed user rights, then security configuration tool does not remove this setting.

Windows user accounts and groups/local security policies

During the hardening, Windows user accounts and groups are created and built-in Administrator user account name is renamed. Administrator user account name cannot be used to login to the computer anymore, ScAdmin must be used instead. However, home folder will still be named as Administrator. Created users and groups are:

- Administrator renamed to ScAdmin (member of Administrators)
- ScEngineer, ScOperator, and ScViewer (member of Windows standard users, accounts are disabled by default)
- ScSecAdmins, ScSecAuditors, ScRBACManagers, ScSysAdmins, ScEngineers, ScOperators, and ScViewers groups

Tool configuring other security areas, such as Local security policy and Application whitelisting, are based on these users and groups.
It is recommended to deploy security settings locally to avoid remote access denied problems.
Before configuring security settings, the server should be updated with the latest service packs and security updates.

User Account Control (UAC)

A user with administrative privileges starts programs by default with non-admin privileges. If administrative privileges are needed, for example, to write some file to the file system where Windows standard users do not have permissions to write, this write will fail. Start programs with "Run as administrator" if you need administrative privileges. A consent dialog is shown that program is to be run with administrative privileges.
For more information, see Appendix A 1.4.

Create strong passwords

- An ideal password is long and has letters, punctuation, symbols, and numbers.
- Whenever possible, use at least 14 characters or more.
- The greater the variety of characters in the password, the better.
- Use the entire keyboard, not just the letters and characters used or seen most often.

1.1 Securing MicroSCADA X server

BIOS SETTINGS

- Password(s) is enabled

- Remote wake-up/Wake on LAN is disabled

MICROSOFT UPDATES

Before configuring security settings, the computer needs to be updated with the latest security updates and service packs from Windows that are tested and certified. The test results can be found from the partner portal if you are a certified system integrator or if you are an end user, these reports can be made available to you based on your service agreement.

REMOVE UNUSED PROGRAMS

See Section 5.3

RUNNING HARDENING

To run hardening in MicroSCADA X server:

1. Browse to \Program Files (x86)\ABB\MicroSCADA Pro\ABB.SCM\ and run ABB.SCM.exe security configuration tool with admin rights, or from start menu folder MicroSCADA X run the "Security Compliance Manager" with admin rights
2. Check that selected baselines are according to the server, for example, Windows Server 2019/microscada/SYS600 10 server. **Note!** If there are several Hitachi ABB Power Grids products installed, for example, SYS600 and DMS600 in the server, follow instructions in the Help page of the tool.
3. Press **Audit**. It will take a while to finish. Log page gives details of the audit process and there is also a log file that can be accessed.
4. After auditing is finished, select all security categories in the tree and press **Enforce** to continue. It will take a while to finish. Log page gives details of the audit process and there is also a log file that can be accessed.
5. Reboot the computer

You can visit the Help page in the security configuration tool at any time.

1.2 Securing MicroSCADA X workplace

BIOS SETTINGS, MICROSOFT UPDATES, REMOVE UNUSED PROGRAMS

Same settings as in MicroSCADA X server are applied, see Appendix A 1.1.

RUNNING HARDENING

To run hardening in the workplace computer:

1. Copy \Program Files (x86)\ABB\MicroSCADA Pro\ABB.SCM\ folder on the USB stick. From the USB stick, run ABB.SCM.exe security configuration tool.
2. Check that selected baselines are according to the computer, for example, Windows 10/ Microscada/SYS600 10 workstation.
3. Press **Audit**. It will take a while to finish. Log page gives details of the audit process.
4. After auditing is finished, select all security categories in the tree and press **Enforce** to continue.
5. Reboot the computer

You can visit the Help page in the security configuration tool at any time.

1.3 Maintenance

1.3.1 Adding new Windows users

Always assign a membership of ScOperators, ScEngineers, ScViewers or ScSysAdmins for the new Windows user since scripts configuring other security areas such as Local security policy and application whitelisting are based on these groups.
Do not give administrative rights (membership of Administrators) to operators/viewers/engineers. Only system administrators should have administrative rights.
Note that Windows standard users or users with less privileges should have additional file system permissions to SYS600 and DMS600 system, see Appendix A 1.3.3.

Preconfigured Windows user accounts and groups are created in the hardening script.

To add a new remote operator and system administrator:

1. Add new Windows user, for example, ScOperator2 and ScAdmin2
2. Add a membership of ScOperators, Remote Desktop Users for ScOperator2 (non-admin)
3. Add a membership of Administrators, ScSysAdmins for ScAdmin2 (admin)

This can be achieved with lusrmgr.msc tool or with following commands to the command prompt:

```
net user ScOperator2 <password> /add
net localgroup ScOperators ScOperator2 /add
net localgroup "Remote Desktop Users" ScOperator2 /add
net user ScAdmin2 <password> /add
net localgroup ScSysAdmins ScAdmin2 /add
net localgroup Administrators ScAdmin2 /add
```

1.3.2 Adding/installing new programs

Allowing programs through Windows Firewall

Hardening and enables Windows Firewall and blocks each program that has no defined rules, and notifies the user of the program blocking.

The default firewall settings in SYS600 product block all communication protocols, such as DNP, ELCOM-90, and IEC60870-5-104. Therefore, ports for the used communication protocols must be manually opened. To customize firewall settings in a single computer:

1. Windows 10/Server 2012R2/2016/2019: Run wf.msc and browse to Inbound Rules. Find the communication protocols from the list, for example, “SYS600: DNP 3.0 Slave”, and enable/disable the rule according to customer specifications. A green balloon means that the traffic is allowed. A grey balloon means that the traffic is blocked. Confirm the changes when done.
2. DMS600 specific firewall ports are indicated with 'DMS600' prefix

If a new program needs to be allowed to several computers or to each delivered computer, the best way is to create a custom baseline, which is then enforced to all computers. For more information, see Help page on the security configuration tool.

“SYS600:“ and “DMS600:” prefix is used in the rule names to help finding settings.

Allowing programs to run in Windows AppLocker

In current Windows versions, AppLocker is used for application whitelisting.

To allow a program to run in a single computer:

1. Run secpol.msc (Local Security Policy)
2. Browse to **Security Settings/Application Control Policies/AppLocker/Executable Rules**
3. Right-click Rules area and select **Create new rule...** and enter following information:
   - Permission: Allow
   - Group: ScEngineers / ScOperators / ScViewers etc.
   - Condition: Publisher (signed) or Path (unsigned)
   - Reference file or Path: Browse and select executable file
   - Name: Use prefix to indicate user group, for example, "eng: ", and "oper: ". See examples in existing rules.
4. Press **Create**

If a new program needs to be allowed to several computers or to each delivered computer, the best way is to create a custom baseline, which is then enforced to all computers. For more information, see Help page on the security configuration tool.

1.3.3 Adding new SYS600 applications

Operators, viewers, and engineers can use non-admin Windows user accounts. However, these user accounts require a few permissions. File system permissions for non-admin users are configured automatically in the security configuration tool. To prepare computer for non-admin users:

1. Open security configuration tool
2. Audit the computer, select to enforce Windows standard users category and Press Enforce. This will prepare all SYS600 applications found under sc\apl to non-admin users.

1.3.4 Adding Windows features

The table below shows the services, which have to be changed from the default if a functionality is required. For example, to take audio in use the following commands can be used for each service listed below:

```
sc config AudioSrv start= auto
sc start AudioSrv
```

Functionality	Display Name	Service Name
Wireless Connection	Wireless Zero Configuration	WZCSVC
Sounds	Windows Audio	AudioSrv AudioEndpointBuilder MMCSS
HASP License Key	Sentinel HASP License Manager	hasplms
Windows Updates	Background Intelligent Transfer Service Automatic Updates	bits wuauserv

1.3.5 Troubleshooting

Windows 7 and later versions support *network location awareness* . The operating system detects the following network location types automatically: Public, Private, and Domain. If the computer automatically changes the network location to Public, where the firewall rules are the most restrictive, some SYS600 functionalities are blocked. The network location of SYS600 server and workplace should be Private or Domain. To manually change the location, see Appendix Configuring network location.

When troubleshooting network problems, it is recommended to check the firewall logs (Windows Firewall: %windir%\pfirewall.log). It is also possible to disable firewall temporarily to solve network problems. Windows event logs, especially Security, Application, and System logs may have events related to security/access problems. Windows AppLocker has a log, where blocked applications can be found. The log can be accessed from **Event Viewer/ Applications and Services Logs/Microsoft/Windows/AppLocker**. AppLocker can also be set to Audit Only mode, which means that applications are allowed to run and the log contains events of when the application would have been blocked if the rules were enforced.

Configuring network location

The firewall profiles associated with the currently detected network location types are the ones that are applied to the computer. Windows Firewall rules in security baselines are not configured to the Public network profile, which is used for unidentified networks. Security configuration tool detects public networks and warns about that.

To check the current network location manually:

1. Open **Control Panel/Network and Sharing Center**.
2. Check all items in the section View your active networks and their network location.
3. If the used network location is Public, then the network connection needs to be modified.

If a user manually changes the network profile of an unidentified network from the Network and Sharing Center, the new setting will only apply until a change, such as a new gateway, disconnect/reconnect, reboot, new IP settings, etc., on that connection occurs. If the network is not a Domain network and there is no default gateway configured, or the gateway is not available, the network will be categorized as unidentified and the Public profile and Public firewall policy will be applied to the computer.

Normally, in MicroSCADA X system, a static IP addressing is used. If the network adapter has a static IP address and a subnet mask but not a default gateway, the operating system does not recognize the Private network. To change the default gateway from Network and Sharing Center:

1. Click **Change adapter settings**
2. Right-click the network adapter, for example, Local Area Connection, and select **Properties**
3. Select **Internet Protocol Version 4** and click **Properties**
4. In the **General** tab, in addition to IP address and Subnet mask, add Default gateway address.
5. Click **OK**
6. Go back to Network and Sharing Center and the operating system should have recognized the Private network

For more information, see Microsoft documentation
Windows Defender Firewall with Advanced Security.

1.4 Rollback

See Help in the security configuration tool.

Appendix B Ports and Services

General firewall settings are as follows:

- Firewall: enabled, block inbound, allow outbound
- Logging: enabled, %windir%\pfirewall.log, 32767kB
- Notify when an application is blocked

Since all inbound traffic is blocked by default, there are exceptions (firewall rules) which need to be configured. Windows Firewall rules are configured automatically using security configuration tool, see Appendix A 1.1.

The columns in the tables below mean the following:
Port number configurable: System is designed so that this port number can be easily changed via the service specific configuration method.
Port status: Is the port designed to be always open, or should it be opened only when the system configuration requires access to this specific service.
Configured by SCM: Does the SCM tool create a firewall rule for this port, and is the rule enabled (open) or disabled (closed) by default.

Communication protocols and TCP port numbers such as DNP3, IEC60870-5-104 and Modbus are well-known by port scanners and receive more connection attempts than other port numbers. See below table if the inbound port number is configurable for the communication protocol.

Table 8: Windows Operating System Services

		Inbound listening					
Service:	**Service Description**	**Port number**	**Port number configurable**	**Port status**	**Configured by SCM**	**Miscellaneous**	**Used by**
msrpc / dcom-scm	Remote procedure call / DCOM Service Control Manager	TCP 135		Always Open	Open	Inbound range for DCOM servers are automatically restricted by scripts, see also [MSDCOM04]	[System, svchost.exe]
netbios-ssn	Netbios Session Service	TCP 139		Always Open	Open		[System]
microsoft-ds	Microsoft Active Directory, shares	TCP 445		Always Open	Open		[System]
microsoft-ds	Microsoft Active Directory, shares	UDP 445					[System]
ntp	SNTP - Simple network time protocol	UDP 123		Always Open	Open		[System]
Netbios-ns	Netbios Name Service	UDP 137		Always Open	Open		[IEC 61850 OPC Server]
Netbios-dgm	Netbios Datagram Service	UDP 138		Always Open	Open		[System]

Table continues on next page

		Inbound listening					
Service:	**Service Description**	**Port number**	**Port number configurable**	**Port status**	**Configured by SCM**	**Miscellaneous**	**Used by**
lsakmp	IPSec in Windows	UDP 500		Always Open	Open		[System]
lsass.exe	sae-urn, IPsec NAT-Traversal	UDP 4500		Always Open	Open		[System]
wininit.exe, svchost.exe etc.		* TCP 49152-49158	X	Always Open			[System] *) Dynamic port range can be configured

Table 9: SYS600

SYS600	**Inbound (listening)**					
Service:	**Port number**	**Port number configurable**	**Port status**	**Configured by SCM**	**Description**	**Security**
node.exe	TCP 80 (http)		Configurable		By default, http port (TCP 80) and https port (TCP 443) are both open. http port redirects all traffic to https port. Thus all communication is secure. If https is configured not to used (disabled in SYS600 Control Panel), then http port is not secure meaning that http traffic is plaintext.	Secure:Yes and no Limit or block access to this port from remote computers depending if the web server is used for operator workplaces.
node.exe	TCP 443 (https)	X	Configurable	Open	Web server hosting web-based applications, for example, internal tools and operator workplaces (Workplace X). This port was only listening connections from localhost computer in SYS600 9.4 FP2 version but in SYS600 10.0 it is listening connections from remote computer	Secure: Yes Limit or block access to this port from remote computers depending if the web server is used for operator workplaces.
postgres.exe	TCP 5432	X	Configurable (Needed for HSB configurations)	Closed	PostgreSQL database for storing setting values. This port is also used for replicating database between HSB computers. Port can be configured in SYS_BASCON.COM, default is 5432.	Secure:Yes
inet.exe	TCP 21844		Always Open	Open	Hot-stand-by communication (APL-APL). This traffic is encrypted. For more information, see [SYSCON, Encrypted communication].	Secure:Yes

Table continues on next page

SYS600	Inbound (listening)					
Service:	**Port number**	**Port number configurable**	**Port status**	**Configured by SCM**	**Description**	**Security**
inet.exe	TCP 21845		Always Open	Open	External OPC DA Clients connect to this port and process data is received through this port.	Secure:No
inet.exe	TCP 21846		Always Open	Open	Used by SYS600 base system processes for internal communication.	Secure:No
java.exe (Apache QPID Broker)	TCP 5672		Localhost connections only		Apache QPID Broker. Accepts localhost connections only.	Secure:No
LogService.exe	TCP 21850		Configurable		MicroSCADA system log/events, MicroSCADA system version information, and application state information. This port is used by Notify window.	Secure:No Limit or block access to this port from remote computers.
aopcs.exe	Dynamic TCP, see [MSDCOM04]	X	Configurable	Open	MicroSCADA Application OPC Server requires DCOM port 135 to be open	N/A
opcs.exe	Dynamic TCP, see [MSDCOM04]	X	Always Open	Open	MicroSCADA OPC Data Access Server requires DCOM port 135 to be open	N/A
Opcenum.exe	Dynamic TCP, see [MSDCOM04]	X	Always Open	Open	OpenRemoteDesktop program uses this service	N/A
hasplsm.exe	UDP and TCP 1947		Configurable	Closed	Aladdin HASP License Manager Service for handling USB license keys	Secure:No
(Web server for Java API)	-	-	-		Java API requires a web server. See web server manuals for port configuration.	Secure:No
bdu_ssiser.exe	TCP 1333	X	Configurable		DMS600 Server Application uses for SCIL-API connection	Secure:No

All master protocols using TCP/IP (IEC60870-5-104 master, DNP3.0 TCP master, Modbus TCP, SPA-TCP) operate as TCP clients. Consequently, no protocol specific port numbers are reserved.

Unauthenticated and unencrypted plain-text network communications protocols are a security risk. Review Security column in each table to see whether communication protocol supports authentication and secure communication (encrypted traffic). Each open TCP/UDP port provides a possible access path for an attacker that can be used to send exploits and receive data. To mitigate risks:

- Know your network perimeter, zones and conduits. Use firewalls to limit access to machines. Do not mix Office/Corporate LAN with Industrial Control System LAN.
- All unneeded applications and services (TCP/UDP ports) should be removed/stopped. Use firewalls to limit access to ports.
- Encrypt communication by using IPSec/VPN tunnels between machines if there is no built-in security mechanism.
- Use latest product versions to get new security enhancements.

Table 10: SYS600 - Communication protocols

	Inbound (listening)					
Service:	**Port number**	**Port number configurable**	**Port status**	**Configured by SCM**	**Description**	**Security**
IEC60870-5-104 Slave	TCP 2404	X	Configurable	Closed	IEC 60870-5-104 for telecontrol equipment and systems with coded bit serial data transmission in TCP/IP based networks for monitoring and controlling geographically widespread processes. Network Control Center (NCC).	Secure: No Threat: Through the communication protocol it is possible to control electric network.
IEC60870-5-104 Secure Authentication Slave	TCP 19998	X	Configurable		Secure communication for IEC60870-5-104	IEC60870-5-104 secure communication is authenticated and encrypted.
IEC60870-5-104 Slave - Communication lines	TCP 2501-2514	X	Configurable		Accepts localhost connections only, open only a short period of time in system startup.	N/A
IEC60870-5-104 Master - communication lines	TCP 2501-2514	X	Configurable		Accepts localhost connections only, open only a short period of time in system startup.	N/A
DNP 3.0 Secure Authentication Version 5 LAN/WAN Slave	TCP 19999	X	Configurable	Closed	Secure communication for DNP 3.0	DNP 3.0 secure communication is authenticated and encrypted.

Table continues on next page

	Inbound (listening)					
Service:	**Port number**	**Port number configurable**	**Port status**	**Configured by SCM**	**Description**	**Security**
DNP 3.0 LAN/WAN Slave	UDP and TCP 20000	X	Configurable	Closed	The Distribute Networks Protocol (DNP) 3.0 LAN/WAN is a standards-based communication protocol designed for electric utility, water, oil & gas and security systems.	Secure: No. Use DNP 3.0 Secure instead. Threat: Through the communication protocol it is possible to control electric network.
DNP 3.0 LAN/WAN Slave - Communication lines	TCP 2501-2514	X	Configurable		Accepts localhost connections only, open only a short period of time in system startup.	N/A
DNP 3.0 LAN/WAN Master - Communication lines	UDP and TCP 2501-2514	X	Configurable		Accepts localhost connections only, open only a short period of time in system startup.	N/A
Modbus TCP/IP Slave	TCP 502	X	Configurable	Closed	Modbus Protocol is a messaging structure used to establish master-slave/client-server communication between intelligent devices. It is used in gas and oil and substation applications but also in building, infrastructure, transportation and energy applications. There is no built-in security in Modbus protocol.	Secure: No Threat: Through the communication protocol it is possible to control electric network.
Modbus TCP/IP Master - Communication lines	TCP 2501-2514	X	Configurable		Accepts localhost connections only, open only a short period of time in system startup.	N/A
SPA-TCP - Communication lines	TCP 2501-2514	X	Configurable		Accepts localhost connections only, open only a short period of time in system startup.	N/A
ELCOM-90 Provider	TCP 6997	X	Configurable	Closed	ELCOM-90 is used to transfer information between control centers and it is inter-control center communication protocol (ICCP).	Secure:No Threat: Through ELCOM-90 it is possible to control remote systems.

Table continues on next page

	Inbound (listening)					
Service:	**Port number**	**Port number configurable**	**Port status**	**Configured by SCM**	**Description**	**Security**
ELCOM-90 UserElem	TCP 6998	X	Configurable	Closed	Inter-process communication	Secure:No Threat: Through ELCOM-90 it is possible to control remote systems.
ELCOM-90 Admin	TCP 6999	X	Configurable	Closed	Used to debug Provider	Secure:No
Opcs_iec61850.exe	Dynamic TCP, see [MSDCOM04].	X	Configurable		IEC 61850 OPC DA Server. By default accepts local COM/ DCOM connections only.	Secure:No Threat: Through the communication protocol it is possible to control electric network.
Opcs_iec61850.exe	TCP 123	X	Configurable		IEC 61850 OPC DA Server, which contains SNTP Server as TCP/IP Server (IEDs synchronizes time with this) and also SNTP Client. See ntp service.	Secure:No
61850_server.exe	TCP 102		Configurable	Open	IEC 61850 Server (10.1 and later). IEC 61850 (MMS) server is a TCP/IP server.	Secure:No Threat: Through the communication protocol it is possible to control electric network.
61850_server.exe	TCP 3782		Configurable	Open	IEC 61850 Server (10.1 and later). IEC 61850 (MMS) server is a TCP/IP server. Used for secure MMS.	Secure: Yes

Table 11: SYS600 – Remote Access

	Inbound (listening)					
Service:	**Port number**	**Port number configurable**	**Port status**	**Configured by SCM**	**Description**	**Security**
Microsoft Windows Remote Desktop Services	TCP 3389		Configurable	Open	Microsoft Windows Terminal Services [Terminal Server Client, RDP Client]	Remote desktop sessions operate over an encrypted channel.
Citrix ICA	TCP 1494		Configurable		MetaFrame Application Server for Windows / Citrix ICA	Remote desktop sessions operate over an encrypted channel.

Table 12: SYS600 Historian 1.3

SYS600 Historian	Inbound (listening)					
Service:	**Port number**	**Port number configurable**	**Port status**	**Configured by SCM**	**Description**	**Security**
Vtrin-NetServer.exe	TCP 443	X	Always Open	Open	This port is used by client and data collector nodes connecting Historian database. ClickOnce installation of Historian client.	Secure:Yes
Vtrin-NetServer.exe	Dynamic TCP	X	Always Open		This port is used for HTTP communication but in SYS600 Historian 1.3 only TCP 443 (HTTPS) is used/ enforced.	N/A

Table 13: SYS600 Historian 1.1

SYS600 Historian 1.1 and earlier	Inbound (listening)				
Service:	**Port number**	**Port number configurable**	**Port status**	**Description**	**Security**
IIS	TCP 80	X	Always Open	ClickOnce installation of Historian client	Secure:No
SimbaServer.exe	TCP 1583	X	Always Open	ODBC/SQL interface for system configuration	Secure:No
OPC UA Server	TCP and UDP 4840-4843	X	Configurable	OPC UA is a machine-to-machine communication protocol for industrial automation	Secure:Yes
Vtrin-NetServer.exe	TCP 7605	X	Configurable	Kerberos authentication (if used)	Secure:No
Vtrin-NetServer.exe	TCP 7606	X	Always Open	Historian client access to the server	Secure:No
Vtrin-NetServer.exe	UDP 7609	X	Configurable	Multicast events from server to client for the system internal communication	Secure:No
Vtrin-NetServer.exe	TCP 7614	X	Always Open	System internal data & configuration transfer	Secure:No
Vtrin-NetServer.exe	TCP 7618	X	Configurable	Events from server to client for the system internal communication	Secure:No

Table 14: DMS600 4.5 (in addition to those listed in DMS600 4.4)

	Inbound (listening)					
Service:	**Port number**	**Port number configurable**	**Port status**	**Configured by SCM**	**Description**	**Security**
PostgreSQL	TCP 5433	X	Only localhost		PostgreSQL instances used by WebMap.	
dmsservice.exe	TCP 9000	X	Always Open	Closed	This service provides background maps for electric network and also network state data.	Secure: No. Communication is encrypted (HTTPS) but it is not authenticated. Threat: It might be possible to access electric network maps and network state data.

Table 15: DMS600 4.4

	Inbound (listening)					
Service:	**Port number**	**Port number configurable**	**Port status**	**Configured by SCM**	**Description**	**Security**
Ms-sql-s	TCP and UDP 1433		Always Open	Open	Microsoft SQL Server	Secure:Yes, see link
Ms-sql-m	TCP and UDP 1434		Always Open	Open	Microsoft SQL Monitor	Secure:Yes, see link
DMSSocketService.exe	TCP 51772	X	Always Open	Open	DMS Socket Service, communication between applications [DMS600 SA, WS, NE] and DMS Service.	Secure: No Threat: Through the communication protocol it might be possible to access manual process points and tamper outage/ interruption data.
UnknownSocketService.exe	TCP 51773		Configurable	Open	Socket service to be used by 3rd party programs for sending messages	Secure: No Threat: Through the communication protocol it might be possible to access manual process points and tamper outage/ interruption data.
DMS Service Framework	TCP 51777		Always Open	Open	DMS600 Service Monitor	Secure: Yes

Table continues on next page

	Inbound (listening)					
Service:	**Port number**	**Port number configurable**	**Port status**	**Configured by SCM**	**Description**	**Security**
DMS SA Service, DMS600SA.exe	TCP 51785		Always Open	Open	DMS600 Service Monitor uses this service to, for example, enable/disable SCIL-API connection, see SYS600 ports (TCP 1333).	Secure: No Threat: It might be possible to control DMS SA Service.
CaCe Fault Receiver	TCP 8086		Configurable	Open	Tieto Care Center (CaCe) WMS. Work management system and LV reporting and fault information. Optional software, depending customer license/needs.	Secure: No Threat: It might be possible to access work management system and fault information.
CaCe Fault Sender	TCP 8087		Configurable	Open	Tieto Care Center (CaCe) WMS. Work management system and LV reporting and fault information. Optional software, depending customer license/needs.	Secure: No Threat: It might be possible to access to work management system and fault information.
PowerGrid NIS Server, PG Server TECS-service	TCP 3000		Configurable	Open	Tieto PowerGrid NIS (Network Information System). Network information, customer and energy data. Optional software, depending customer license/needs.	Secure: No Threat: It might be possible to access electric network, customer and energy data.
AMR (http)	TCP 80	-	Configurable	Open	Automatic Meter Reading (AMR), energy data. Microsoft Internet Information Server (IIS) runs AMR Service. Optional software, depending customer license/needs.	Secure: No Threat: It might be possible to access energy data.
AMR (https)	TCP 443	-	Configurable	Open		Secure: Yes

Table 16: SDM600 1.2

	Inbound (listening)			
Service	**Port number**	**Port status**	**Configured by SCM**	**Description**
ICMP		Open	Open	ICMP Ping
SFTP	TCP 22	Configurable	Close	Port used only if SFTP file transfer option is used for Disturbance Records retrieval.
LDAP	TCP 389	Open	Open	SDM600 Centralized Account Management (LDAP Authentication)
HTTPS	TCP 443	Open	Open	HTTPS web access

Table continues on next page

	Inbound (listening)			
Service	**Port number**	**Port status**	**Configured by SCM**	**Description**
SYSLOG	UDP 514	Open	Open	Centralized Activity Logging Service (Syslog over UDP)
LDAPS	TCP 636	Open	Open	Centralized Account Management secure connection (LDAP Authentication)
FTPS	TCP 989-990	Configurable	Close	Port used only if FTPS file transfer option is used for Disturbance Records retrieval.
SQL Server	TCP 1433	Open	Open	SQL Server
Syslog	TCP 1468	Open	Open	Centralized Activity Logging Service (Syslog over TCP)
RADIUS (TCP)	TCP 1812	Open	Open	Centralized Account Management Service (RADIUS communication)
RADIUS (UDP)	UDP 1812	Open	Open	Centralized Account Management Service (RADIUS communication)
SQL Server	TCP 58900	Open	Open	SQL Server
HRC Init	TCP 59100-59199	Open	Open	SDM600 internal service (Parent-Child Initialization)
CAL Event Aggregator	TCP 59200	Open	Open	SDM600 internal service (Centralized Activity Logging Service)
SDM Clustering	TCP 59960	Configurable	Close	Parent/child, needed only on the child system
HSB Init/HRC Run	TCP 59990-59999	Open	Open	SDM600 internal service (Parent - Child, HotStandby Initialization)
HSB Run	TCP 60000-600010	Open	Open	SDM600 internal service (Hot - Standby)
HRC Migration	TCP 61743	Configurable	Close	SDM600 internal service - open only during migration from previous versions of SDM600

Appendix C Windows System Services

Windows system services are described in detail in Threats and Countermeasures Guides.

The settings below are a collection of services which are automatically disabled by security configuration tool.

Not all services are running in each operating system, and may not even exist. The detailed list of recommended service settings can be found from security configuration tool. The security configuration is deployed so that it ignores the unavailable services. Therefore, it is normal to have these kinds of messages in the log file:

- Error 1060: The specified service does not exist as an installed service. Error opening <service name>.
- Error 1060: The specified service does not exist as an installed service. Opening service <service name> for stop access failed.
- Legacy audit settings are disabled. Skipped configuration of legacy audit settings.

Some functionalities need certain services to be enabled. To enable some feature, see Appendix A 1.3.4.

Table 17: Disabled Windows system services

Service	Display Name
Alerter	Alerter
ALG	Application Layer Gateway Service
aspnet_state	ASP .NET State Service
AudioEndpointBuilder	Windows Audio Endpoint Builder
AudioSrv	Windows Audio
Browser	Computer Browser
bthserv	Bluetooth Support Service
CiSvc	Indexing Service
ClipSrv	ClipBook
CscService	Offline Files
ehRecvr	Windows Media Center Receiver Service
ehSched	Windows Media Center Scheduler Service
Fax	Fax
ftpsvc	Microsoft FTP Service
Helpsvc	Help and Support
IISAdmin	IIS Admin
ImapiService	IMAPI CD-Burning COM Service
IPBusEnum	PnP-X IP Bus Enumerator
Mcx2Svc	Media Center Extender Service
Messenger	Messenger

Table continues on next page

Service	Display Name
MMCSS	Multimedia Class Scheduler
Mnmsrvc	NetMeeting Remote Desktop Sharing
MSFtpsvc	FTP Publishing Service
NetDDE	Network DDE
NetDDEdsdm	Network DDE DSDM
pla	Performance Logs & Alerts
QWAVE	Quality Windows Audio Video Experience
RDSessMgr	Remote Desktop Help Session Manager Service
RemoteRegistry	Remote Registry
SCardSvr	Smart Card
Schedule	Task Scheduler
SensrSvc	Adaptive Brightness
SMTPSVC	Simple Mail Transfer Protocol
SCPolicySvc	Smart Card Removal Policy
srservice	System Restore Service
Stisvc	Windows Image Acquisition
SysmonLog	Performance Logs & Alerts
TabletInputService	Tablet PC Input Service
TapiSrv	Telephony
TlntSvr	Telnet
TrkSrv	Distributed Link Tracking Server
TrkWks	Distributed Link Tracking Client
Upnphost	Universal Plug and Play Device Host
UPS	Uninterruptable Power System
W3SVC	World Wide Web Publishing
WbioSrvc	Windows Biometric Service
WebClient	Web Client
Wlansvc	WLAN AutoConfig
WmdmPmSN	Portable Media Serial Number Service
WMPNetworkSvc	Windows Media Player Network Sharing Service
WPCSvc	Parental Controls
WZCSVC	Wireless Zero Configuration

Table 18: Enabled Windows system services

Service	Display Name
appidsvc	Application Identity (AppLocker)
SNMP	
SNMPTRAP	

Appendix D Security Policies

The table below shows an overview what settings are changed in the MicroSCADA X servers and workplaces compared to the hardened operating system settings (Microsoft Security Compliance Manager baselines). Full listing of changed settings can be seen from the security configuration tool.

Table 19: MicroSCADA X security policies

Setting Name	Default Value	MicroSCADA X Server	MicroSCADA X Workplace	Remarks
Maximum password age	42 days	-1 or 0	Not defined	MicroSCADA user account never expires
Minimum password age	0 days	0	Not defined	MicroSCADA user account never expires
Account lockout threshold (LockoutBadCount)	0 invalid login attempts	10	10	Note! A denial-of-service attack can occur if an attacker abuses the Account lockout threshold setting and repeatedly attempts to log on to an account.
Account lockout duration (LockoutDuration)	Not defined	1	1	The account will be locked a duration of 1 minute
Reset account lockout counter after (ResetLockoutCount)	Not defined	1	1	
Deny access to this computer from the network	Guests	Guests, ANONYMOUS LOGON	Not defined	
Allow log on through Terminal Services	Administrators, Remote Desktop Users	Administrators, Remote Desktop Users	Not defined	
Deny log on locally	Guests	Guests, MicroSCADA	Not defined	MicroSCADA user account is only used to running the service. It is not meant for interactive purposes.
Deny log on through Terminal Services	Not defined	Guests, MicroSCADA	Not defined	MicroSCADA user account is only used to running the service. It is not meant for interactive purposes.
Log on as a service	Not defined	MicroSCADA	Not defined	

Table continues on next page

Setting Name	Default Value	MicroSCADA X Server	MicroSCADA X Workplace	Remarks
Accounts: Rename guest account	Guest	Guestrenamed	Guestrenamed	Guest account is disabled, however still renaming
Accounts: Rename built-in Administrator account	Administrator	ScAdmin	ScAdmin	Administrator user name cannot be used to login to Windows anymore. ScAdmin should be used instead with same password.
Accounts: Enable Administrator account	Disabled	Enabled	Enabled	The server should not have hidden user accounts
Devices: Restrict CD-ROM access to locally logged-on user only	Disabled	Enabled	Enabled	Remote control is denied
Devices: Restrict floppy access to locally logged-on user only	Disabled	Enabled	Enabled	Remote control is denied
User Account Control: Disable UAC remote restrictions (localaccounttoken filterpolicy)	0	1	1	1 = remotely connect with full administrator rights
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode (consentpromptbehavioradmin)	Prompt for consent for non-Windows binaries	Prompt for consent	Prompt for consent	If the user wants administrator privileges, "run as administrator" have to be used to open a program.
Interactive Logon: Message title for users attempting to logon	Not defined	NOTICE TO USERS	NOTICE TO USERS	Login warning banner
Interactive logon: Message text for users attempting to log on	Not defined	WARNING: This is a private system. Do not attempt to logon unless you are an authorized user. Any authorized or unauthorized access and use may be monitored and can result in criminal or civil prosecution under applicable law.	WARNING: This is a private system. Do not attempt to logon unless you are an authorized user. Any authorized or unauthorized access and use may be monitored and can result in criminal or civil prosecution under applicable law.	Login warning banner
Interactive logon: Do not display last user name	Disabled	Enabled	Enabled	

Table continues on next page

Setting Name	Default Value	MicroSCADA X Server	MicroSCADA X Workplace	Remarks
RPC: Remote Procedure Call dynamic port range	Not defined	50000-50100	50000-50100	
Terminal server: Enable Remote Desktop (fDenyTSConnections)	Remote desktop disabled	Remote desktop enabled	Remote desktop enabled	
Terminal server: Security level	1 (Medium)	2 (High)	2 (High)	
Terminal server: Minimum encryption level	2 (Client compatible)	3 (High, 128-bit)	3 (High, 128-bit)	

Appendix E Application Whitelisting - Applications and Permissions

Applocker rules are implemented for certain Windows groups such as ScEngineers, ScOperators and ScViewers. Users being member of ScSysAdmins group are also members of Administrators group and this is why there are no rules for ScSysAdmins group. Administrators group has full access to all applications. Rules that are defined for ScOperators group are also given to ScViewers, and ScEngineers groups. ScEngineers group has some extra rules needed for engineering. Windows Installer, Script, and Packaged app rules, where available, have default values.

Note that Everyone is allowed to execute applications in the Windows and Program Files folders but there are exceptions: cmd.exe, regedit.exe, regedt32.exe, and regsvr32.exe.

Action	User	Name	Condition	Exceptions
Allow	BUILTIN\Administrators	(Default Rule) All files	Path	
Allow	Everyone	All files located in the Windows folder	Path	Yes
Allow	Everyone	(Default Rule) All files located in the Program Files folder	Path	
Allow	SECW2008HSB2\ScEngineers	eng: cmd.exe	Publisher	
Allow	SECW2008HSB2\ScEngineers	eng: ABB PROTECTION AND CONTROL IED MANAGER from O=ABB OY, L...	Publisher	
Allow	SECW2008HSB2\ScEngineers	eng: C:\sc\PROG\OPC_CLIENT\DA_CLIENT\DAOPCCP.EXE	Path	
Allow	SECW2008HSB2\ScEngineers	eng: C:\sc\PROG\61850_OPC_SERVER\MANAGEMENT\BIN\DCOMPERM.EXE	Path	
Allow	SECW2008HSB2\ScEngineers	eng: C:\sc\prog\exec\picv.exe	Path	
Allow	SECW2008HSB2\ScEngineers	eng: C:\sc\prog\sa_lib\InstanceHandler.exe	Path	
Allow	SECW2008HSB2\ScEngineers	eng: C:\sc\prog\sa_lib\ControlDlgLaunch.exe	Path	
Allow	SECW2008HSB2\ScEngineers	eng: C:\sc\prog\sa_lib\FrameWindow.exe	Path	
Allow	SECW2008HSB2\ScEngineers	eng: C:\sc\prog\graphicsEngine\system\DVDraw.exe	Path	
Allow	SECW2008HSB2\ScEngineers	eng: C:\sc\PROG\OPC_CLIENT\DA_CLIENT\DAOPCCL.EXE	Path	
Allow	SECW2008HSB2\ScEngineers	eng: C:\sc\prog\exec\vrescopy.exe	Path	
Allow	SECW2008HSB2\ScEngineers	eng: C:\sc\PROG\OPC_CLIENT\DA_CONFIG_TOOL\DAOCT.EXE	Path	
Allow	SECW2008HSB2\ScEngineers	eng: C:\sc\prog\exec\notify.exe	Path	
Allow	SECW2008HSB2\ScEngineers	eng: C:\sc\Stool\Misc\7z.exe	Path	
Allow	SECW2008HSB2\ScEngineers	eng: C:\sc\prog\exec\picn.exe	Path	
Allow	SECW2008HSB2\ScEngineers	eng: C:\sc\prog\sa_lib\MicroSCADASCLImport.exe	Path	
Allow	SECW2008HSB2\ScEngineers	eng: C:\sc\prog\exec\OPCENUM.EXE	Path	
Allow	SECW2008HSB2\ScEngineers	eng: C:\sc\prog\pcm_client\IedPcm.exe	Path	
Allow	SECW2008HSB2\ScEngineers	eng: C:\sc\prog\exec\mons.exe	Path	
Allow	SECW2008HSB2\ScOperators	oper: C:\sc\prog\pcm_client\IedPcm.exe	Path	
Allow	SECW2008HSB2\ScOperators	oper: C:\sc\prog\sa_lib\ControlDlgLaunch.exe	Path	
Allow	SECW2008HSB2\ScOperators	oper: C:\sc\prog\exec\picv.exe	Path	
Allow	SECW2008HSB2\ScOperators	oper: C:\sc\prog\exec\notify.exe	Path	
Allow	SECW2008HSB2\ScOperators	oper: C:\sc\prog\sa_lib\InstanceHandler.exe	Path	
Allow	SECW2008HSB2\ScOperators	oper: C:\sc\prog\exec\mons.exe	Path	
Allow	SECW2008HSB2\ScOperators	oper: C:\sc\prog\sa_lib\FrameWindow.exe	Path	
Allow	SECW2008HSB2\ScOperators	oper: C:\sc\prog\exec\picn.exe	Path	
Allow	SECW2008HSB2\ScOperators	oper: C:\sc\prog\exec\OPCENUM.EXE	Path	
Allow	SECW2008HSB2\ScViewers	view: C:\sc\prog\exec\picn.exe	Path	
Allow	SECW2008HSB2\ScViewers	view: C:\sc\prog\sa_lib\InstanceHandler.exe	Path	
Allow	SECW2008HSB2\ScViewers	view: C:\sc\prog\sa_lib\ControlDlgLaunch.exe	Path	
Allow	SECW2008HSB2\ScViewers	view: C:\sc\prog\exec\notify.exe	Path	
Allow	SECW2008HSB2\ScViewers	view: C:\sc\prog\exec\OPCENUM.EXE	Path	
Allow	SECW2008HSB2\ScViewers	view: C:\sc\prog\sa_lib\FrameWindow.exe	Path	
Allow	SECW2008HSB2\ScViewers	view: C:\sc\prog\pcm_client\IedPcm.exe	Path	
Allow	SECW2008HSB2\ScViewers	view: C:\sc\prog\exec\picv.exe	Path	
Allow	SECW2008HSB2\ScViewers	view: C:\sc\prog\exec\mons.exe	Path	

Figure 15: Windows AppLocker rules for SYS600

There are no application whitelisting rules for DMS600.

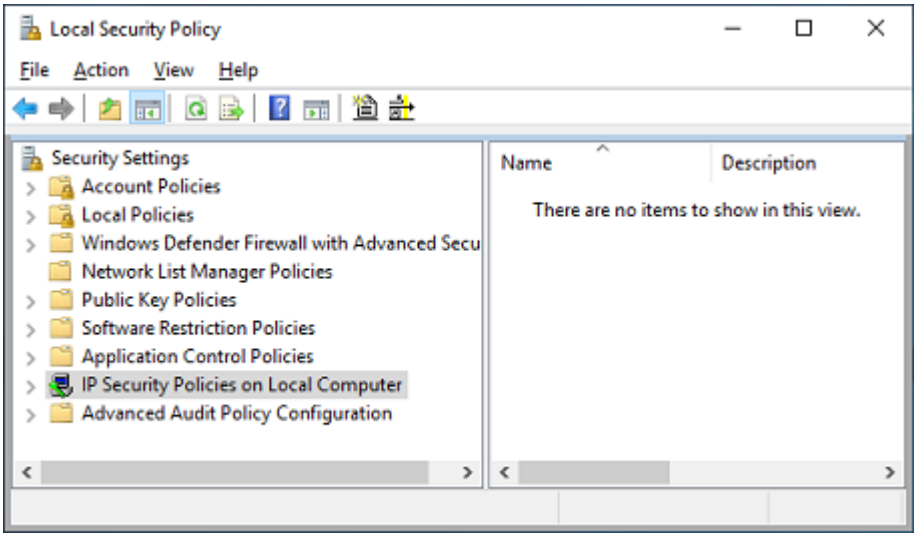
Appendix F Virtual Private Network

The configuration for Windows Server 2019 is shown below. Same method applies to other Windows Server versions.

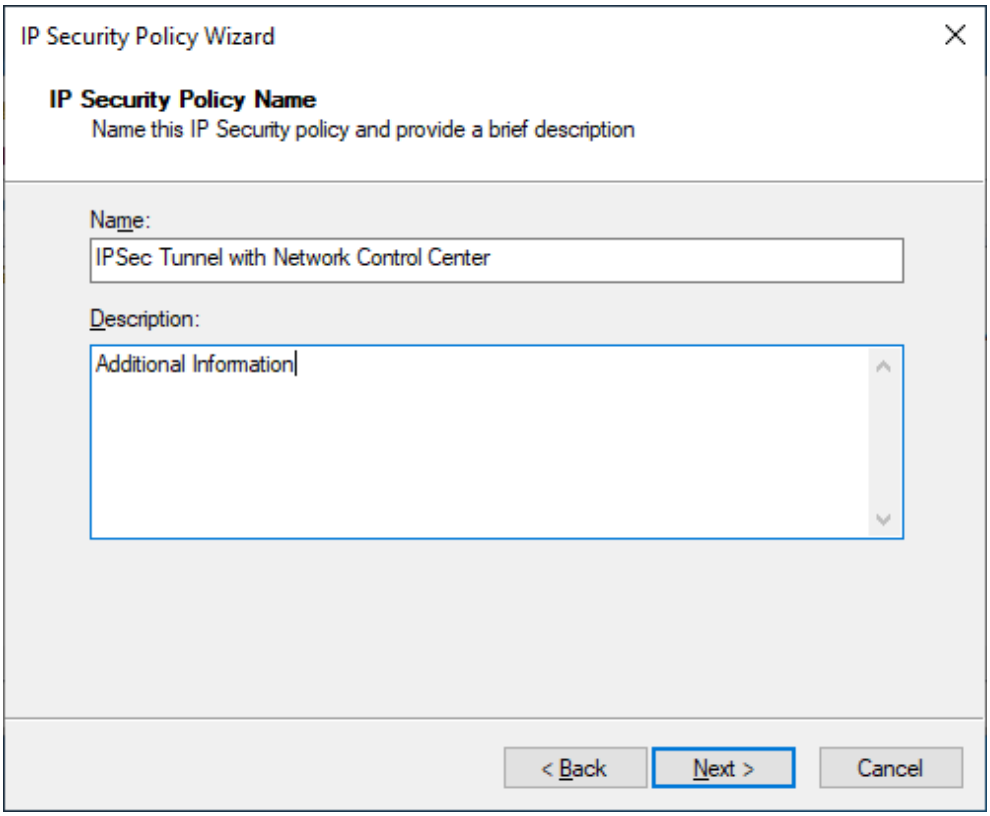
1.1 Create IPSec Policy

An IPSec policy secures all IP traffic that is specified in the configured IPSec filters. The decision to allow unsecured IP traffic is up to the user. To configure SYS600 for IPSec transport mode:

1. Open the **Start** menu, click **Run**, and type in secpol.msc to start the IP Security Policy Management snap-in.

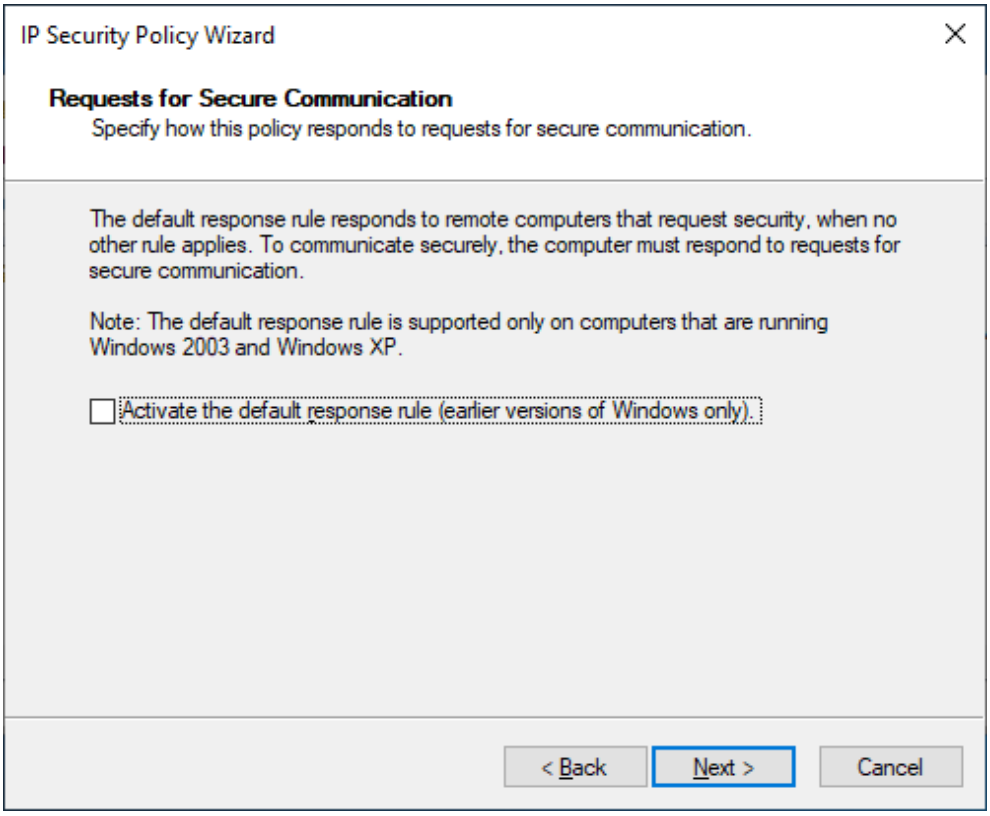


2. Right-click IP Security Policies on Local Computer, and then click Create IP Security Policy.
3. Click **Next**, and type in a name for the policy (for example, **IPSec Tunnel with Network Control Center**).



4. Click to clear the **Activate the default response rule** check box, and then click **Next**.

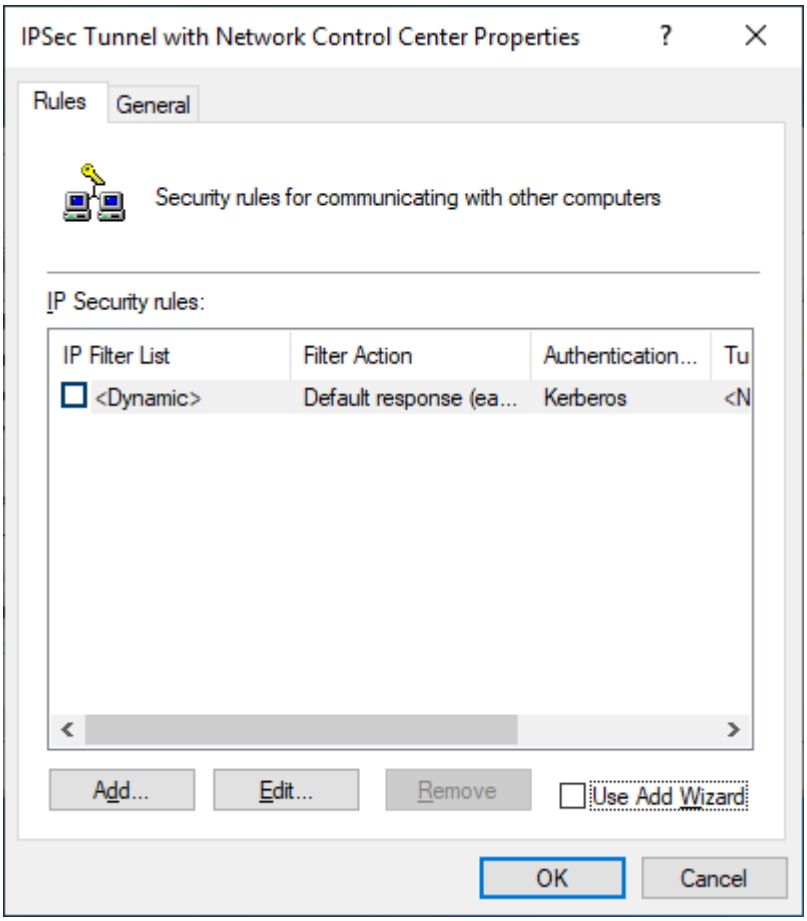
5. Add additional information in the Description box if desired. Click **Next**.



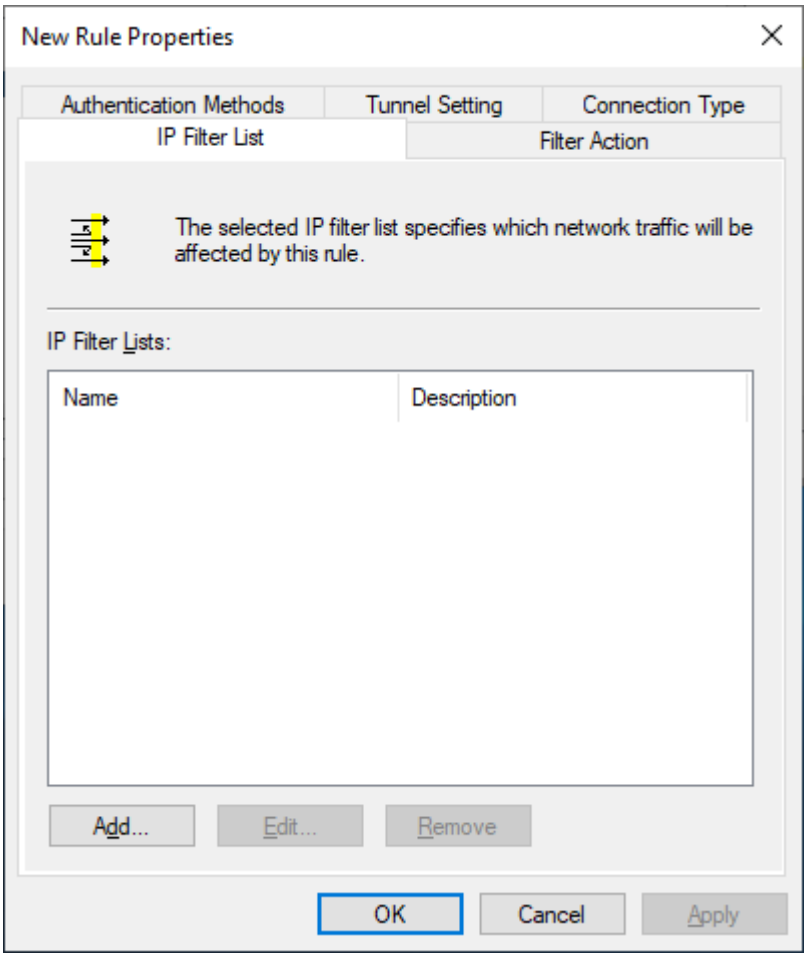
6. Click **Finish** (leave the Edit check box selected).

1.2 Build a Filter List from SYS600 to NCC

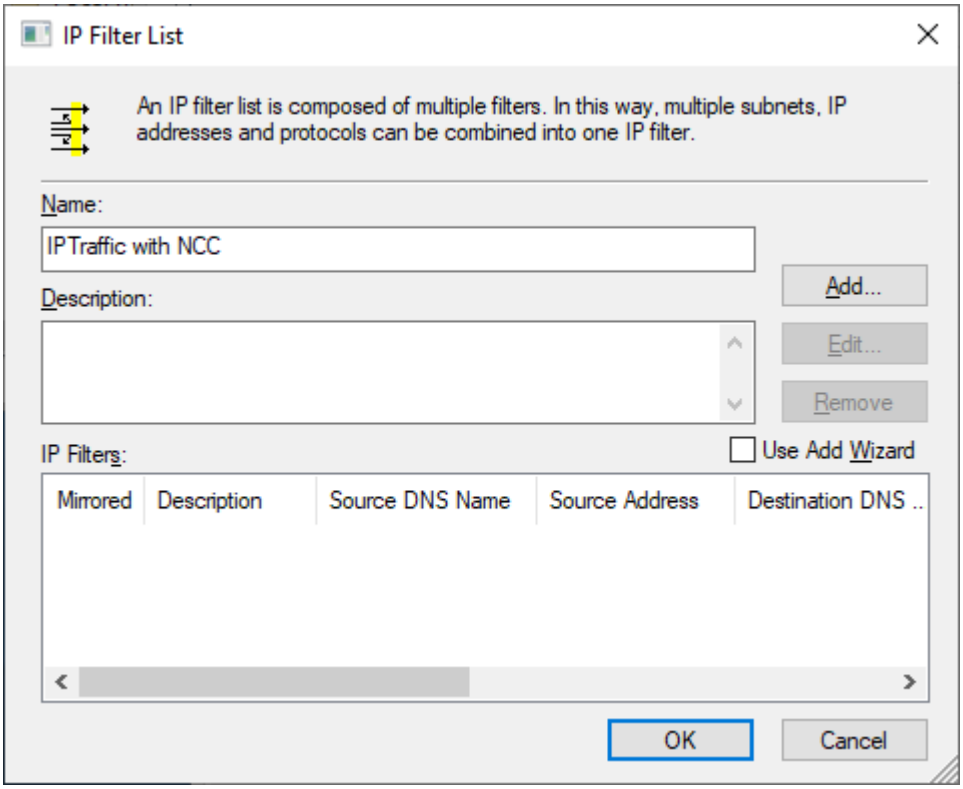
1. In the new policy properties, click to clear the **Use Add Wizard** check box, and then click **Add** to create a new rule.



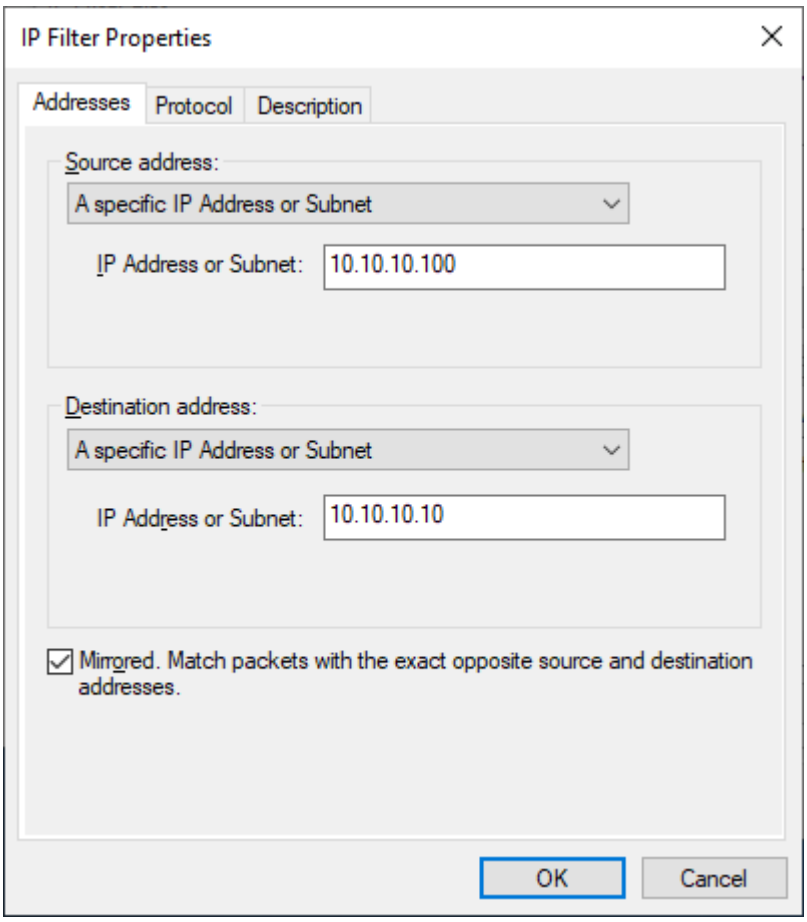
2. Click the **IP Filter List** tab, and then click **Add**.



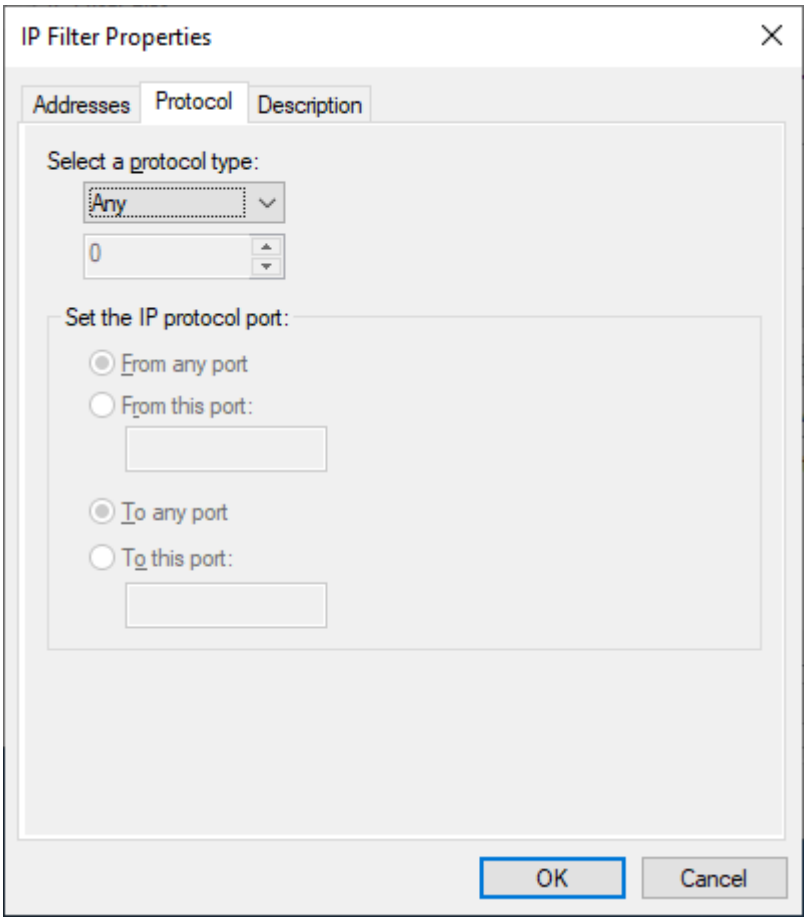
3. Type in an appropriate name for the filter list (for example, IP traffic to NCC), click to clear the **Use Add Wizard** check box, and then click **Add**.



4. In the **Source address**, click **A specific IP Address**, and type the IP Address of SYS600 towards NCC (the IP address that communicates with the NCC), as this filter should only apply to the network interface connected to the WAN.



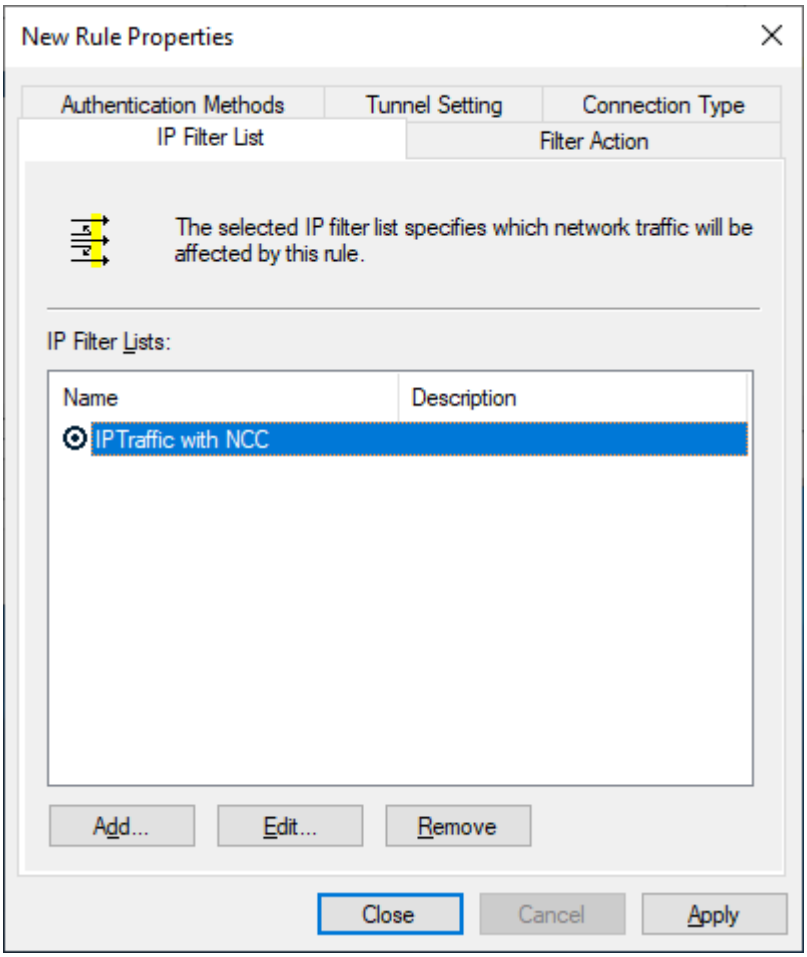
5. In the **Destination address** box, click **A specific IP Address**, and then type the IP Address of the NCC (the NCC's IP address that SYS600 connects to).
6. Leave the **Mirrored** selected.
7. Click the **Protocol** tab. Make sure that the protocol type is set to **Any** because IPSec does not support protocol-specific or port-specific filters.



8. If a description for the filter is desired, click the **Descriptions** tab. Click **OK**.
9. Click **OK** to close IP Filter List dialog.

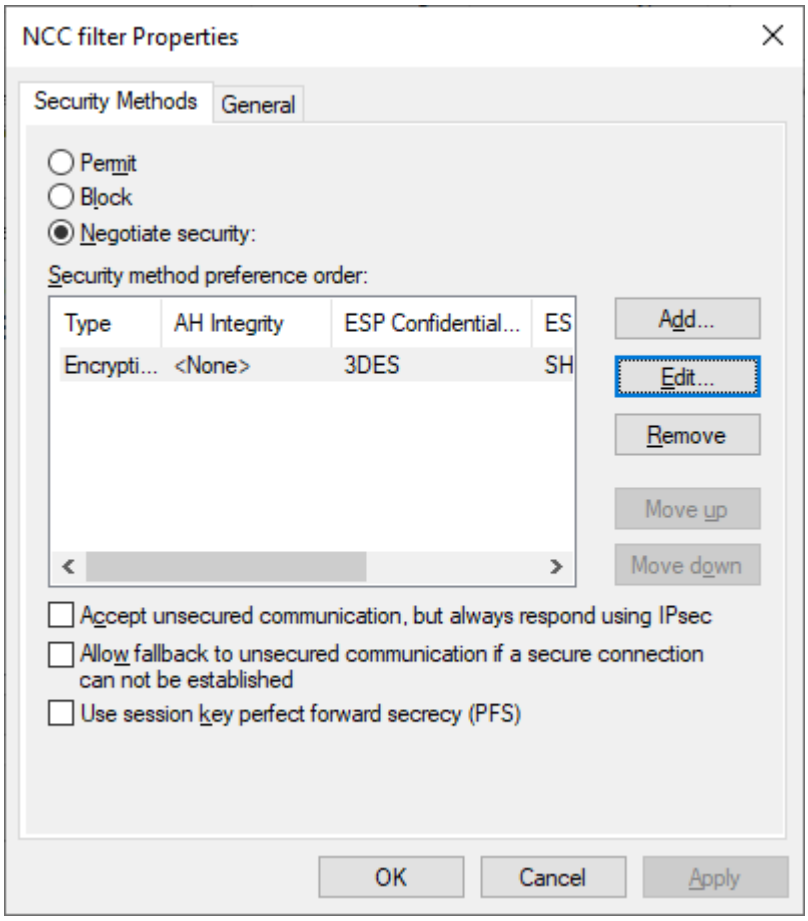
1.3 Configure a Rule for the communication

1. Click the **IP Filter List** tab, and then click to select the created filter list.



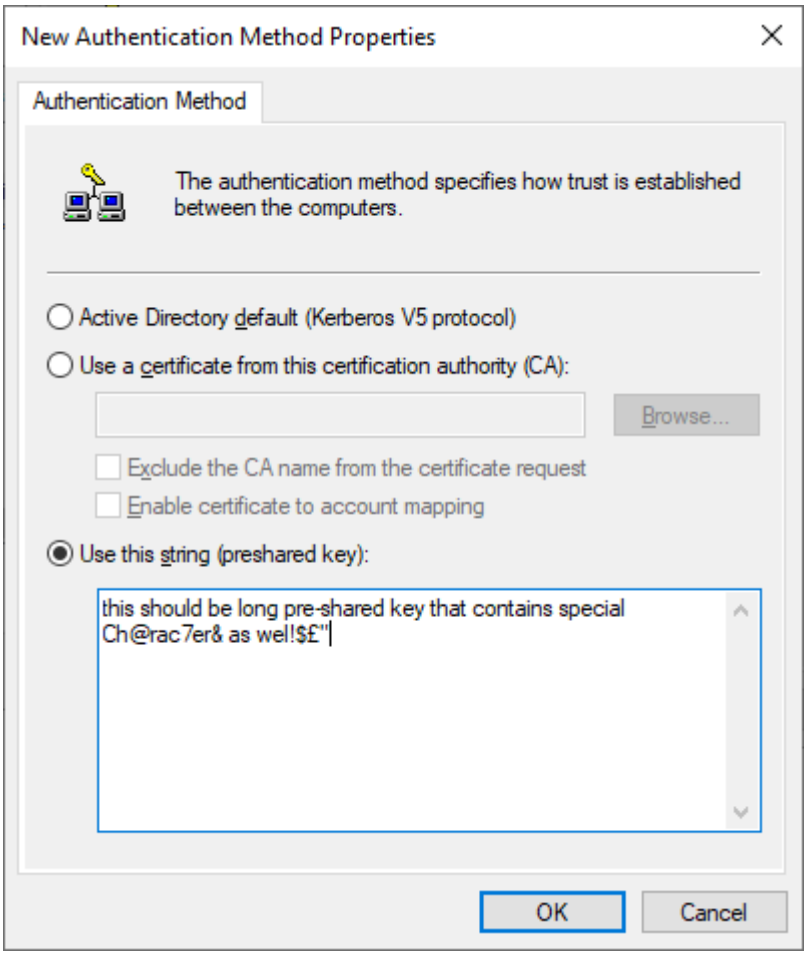
2. Click the **Tunnel Setting** tab, click This rule does not specify an IPSec tunnel.
3. Click the **Connection Type** tab, click **Local area network (LAN)**
4. Click the **Filter Action** tab, unselect the option Use Add Wizard, click Add. In New Filter Action Properties window choose Security Methods tab, and select one of the options
   - Permit - Permits unsecured IP packets to pass through.
   - Block - Blocks unsecured IP packets to pass through.
   - Negotiate Security – Traffic is handled based on configuration done from Add-button, recommendation is to use Integrity and encryption. For debugging purposes Integrity only can be used.
5. Click the General tab, and give name for the filter

None of the check boxes at the bottom of the Filter Action dialog box are selected as an initial configuration for a filter action that applies to tunnel rules.

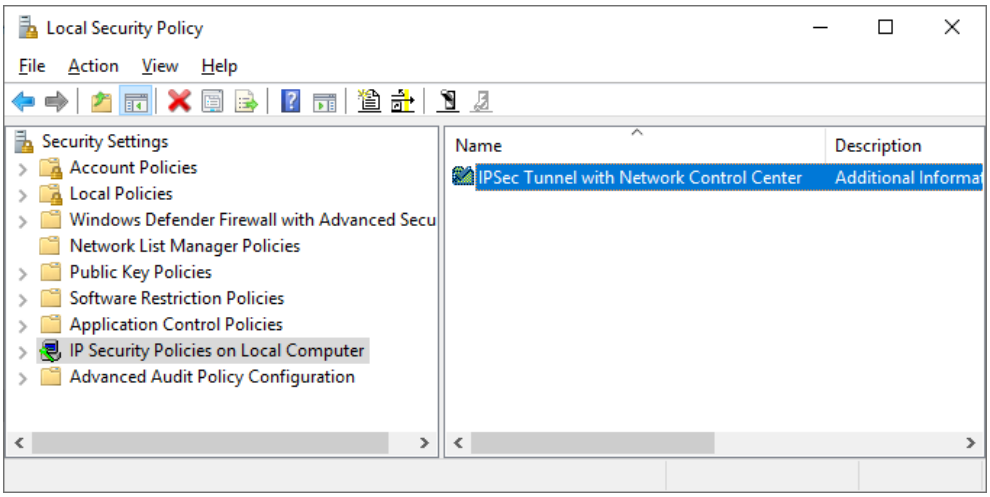


As the currently configured IP Filter rule matches only a single IP, it does not discard non-IPSec traffic originating from a different wide area network IP address. In order to prohibit any non-IPSec connections from the wide area network, the IP filter list has to match the subnet of the wide area network, and the Filter Action has to be set to “Negotiate Security”.

6. Click the **Authentication Methods** tab to configure the authentication method.
7. Click **Add**.
8. Select Use a certificate from this certification authority (CA) if there is a possibility to use such certificate (preferred), or Use this string (preshared key) and enter a long key that also contains special characters. This string must be the same on the machine that matches the IP filter rule (in this case, the NCC). Click **OK**.



9. **Mark** the default **Kerberos method** and click **Remove** the inquiry. Click **Close** to close New Rule Properties dialog.
10. Click **OK**.
11. In the **Local Security Settings,** right-click on the created rule (for example, IPSec Tunnel with Network Control Center) and select **Assign** The rule indicates by a green dot that it is active. Close the Local Security Settings.



Repeat the steps for all machines that should use IPSec. It is possible to export and import the policies on a different computer. Here are the instructions:

1. In the **Local Security Settings,** where the VPN configuration is set, select IP Security Policies on Local Computer.
2. Select **Action/All Tasks/Export Policies...** and write a file name.
3. In the other computer, where VPN configuration is needed: open Local Security Settings and select **IP Security Policies on Local Computer**.
4. Select **Action/All Tasks/Import Policies...**.
5. Select a file exported in item 2 and press **Import/OK**.
6. The rules should be checked and adapted, for example, swap Source address and Destination address in IP Filter Properties dialog.

For IPSec interoperability between different devices and vendors, see configuration profile in [LEMNOS11].

Appendix G Introduction to SCADA Security

The following excerpt is taken from Supervisory Control and Data Acquisition (SCADA) Systems, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, cisa.gov.

In today's corporate environment, internal networks are used for all corporate communications, including SCADA. SCADA systems are therefore vulnerable to many of the same threats as any TCP/IP-based system.

Security in an industrial network can be compromised in many places along the system and is most easily compromised at the SCADA host or control room level. SCADA computers logging data out to some back-office database repositories must be on the same physical network as the back-end database systems, or have a path to access these database systems. This means that there is a path back to the SCADA systems and eventually the end devices through their corporate network. Once the corporate network is compromised, then any IP-based device or computer system can be accessed. These connections are open 24x7 to allow full-time logging, which provides an opportunity to attack the SCADA host system with any of the following attacks:

- Use a Denial of Service (DoS) attack to crash the SCADA server, leading to a shutdown condition (System Downtime and Loss of Operations)
- Delete system files on the SCADA server (System Downtime and Loss of Operations)
- Plant a Trojan and take complete control of system (Gain complete control of system and be able to issue any commands available to Operators)
- Log keystrokes from Operators and obtain usernames and passwords (Preparation for future take down)
- Log any company-sensitive operational data for personal or competition usage (Loss of Corporate Competitive Advantage)
- Change data points or deceive Operators into thinking control process is out of control and must be shut down (Downtime and Loss of Corporate Data)
- Modify any logged data in remote database system (Loss of Corporate Data)
- Use SCADA Server as a launching point to defame and compromise other system components within corporate network.

For a company to protect its infrastructure, it should undertake the development of a security strategy that includes specific steps to protect any SCADA system. Such a strategy may include the following approach.

Developing an appropriate SCADA security strategy involves analysis of multiple layers of both the corporate network and SCADA architectures including firewalls, proxy servers, operating systems, application system layers, communications, and policy and procedures. Strategies for SCADA Security should complement the security measures implemented to keep the corporate network secure.

The figure below illustrates the typical corporate network "ring of defenses" and its relationship with the SCADA network. Successful attacks can originate from either Internet paths through the corporate network to the SCADA network, or from internal attacks from within the corporate office. Alternatively, attacks can originate from within the SCADA network from either upstream (applications) or downstream (RTUs) paths. What is an appropriate configuration for one installation may not be cost-effective for another. Flexibility and the employment of an integrated and coordinated set of layers are critical in the design of a security approach.

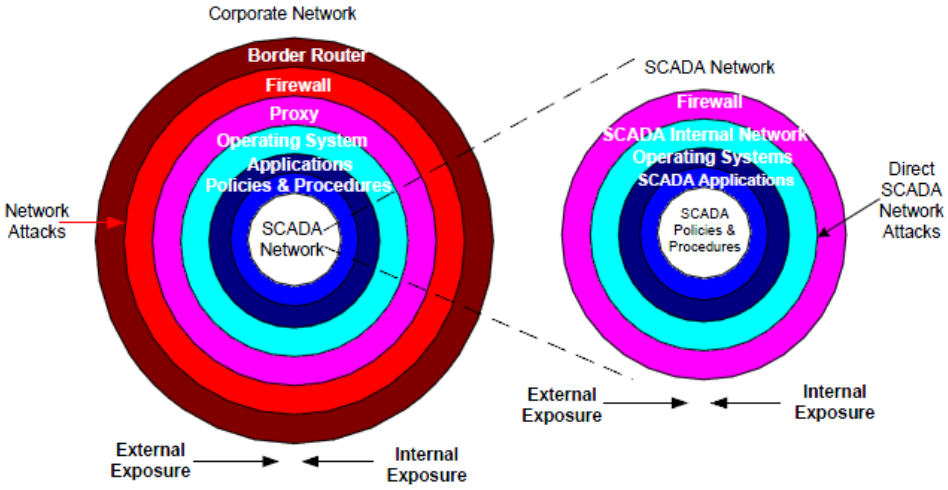


Figure 16: Relationship Between Corporate and SCADA Networks

Most corporate networks employ a number of security countermeasures to protect their networks. Some of these and a brief description of their functions are as follows:

- **Border Router and Firewalls:** Firewalls, properly configured and coordinated, can protect passwords, IP addresses, files and more. However, without a hardened operating system, hackers can directly penetrate private internal networks or create a Denial of Service condition.
- **Proxy Servers:** A Proxy server is an internet server that acts as a firewall, mediating traffic between a protected network and the internet. They are critical to re-creating TCP/IP packets before passing them on to, or from, application layer resources such as Hyper Text Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP). However, the employment of proxy servers will not eliminate the threat of application layer attacks.
- **Operating Systems:** Operating systems can be compromised, even with proper patching, to allow network entry as soon as the network is activated. This is due to the fact that operating systems are the core of every computer system and their design and operating characteristics are well-known worldwide. As a result, operating systems are a prime target for hackers. Further, in-place operating system upgrades are less efficient and secure than design-level migration to new and improved operating systems.
- **Applications:** Application layer attacks; that is, buffer overruns, worms, Trojan horse programs and malicious ActiveX code can incapacitate anti-virus software and bypass the firewall as if it wasn't even there.
- **Policies and Procedures:** Policies and procedures constitute the foundation of security policy infrastructures. They include requiring users to select secure passwords that are not based on a dictionary word and contain at least one symbol, capital letter, and number, and should be over eight characters long. Users should not be allowed to use the name of their spouse, child or pet as their password.

The above list is common to all entities that have corporate networks. SCADA systems for the most part coexist on the same corporate network, as seen in the figure above. The following list suggests ways to help protect the SCADA network in conjunction with the corporate network:

- **SCADA Firewalls:** SCADA Systems and Industrial Automation Networks, like corporate network operating systems, can be compromised using similar hacking methods. SCADA systems frequently go down due to other internal software tools or employees who gain access to the SCADA systems, often without any intention to take down these systems. For these reasons, it is suggested that strong firewall protection to wall off the SCADA networking systems from both the internal corporate network and the Internet be

implemented. This would provide at least two layers of firewalls between the SCADA networking systems and the Internet.

- **SCADA Internal Network Design:** SCADA networks should be segmented off into their own IP segment using smart switches and proper sub-masking techniques to protect the Industrial Automation environment from the other network traffic, such as file and print commands. Facilities using Wireless Ethernet should use sufficient encryption, for example, WPA or WPA2.
- **SCADA Server Operating Systems:** Merely installing a firewall or segmenting SCADA IP addresses will not ensure their SCADA Infrastructure is secure. An experienced hacker can often bypass firewalls with ease and can even use Address Resolution Protocol (ARP) trap utilities to steal Media Access Control (MAC) addresses. The hacker can also deploy IP spoofing techniques to maneuver through switched networks. Operating systems running the SCADA applications must also be maintained. SCADA applications on Windows NT, 2000, or XP are properly patched against the latest vulnerabilities, and all of the default NULL NT accounts and administrator accounts have been removed or renamed. SCADA applications running on UNIX, Linux, Novell, or any other operating system (OS), must also be maintained as above. All operating systems have back doors and default access accounts that should be removed and cleaned off of these SCADA servers.
- **SCADA Applications:** One must also address security within the SCADA application itself. Trojan horses and worms can be inserted to attack application systems, and they can be used to manipulate data or issue commands on the server. There have even been cases of Trojan horses being deployed that completely emulate the application. The operator or user thinks that he is clicking on a command to stop a pump or generate a graph of the plant, but he is actually clicking on buttons disguised to look like the SCADA screen, and these buttons start batch files that delete the entire hard drive, or send out pre-derived packets on the SCADA system that turn all outputs to the ON or “1” state. Trojan horses and viruses can also be planted through an email opened by another computer in the network, and then it is silently copied over to adjacent SCADA servers, where they wait until a specified time to run. Plant control rooms will often have corporate computers with the Internet and email active on them, within the same physical room and on the same network switches as SCADA computers. Methodologies to mitigate against these types of situations are: the use of anti-virus software running on the computer where the SCADA application resides; systems administrators disabling installation of any unauthorized software unless the user has administrator access; and policies and procedures applicable to SCADA systems,
- **SCADA Policies and Procedures:** SCADA policies and procedures associated with remote vendor and supervisory access, password management, etc. can significantly impact the vulnerabilities of the SCADA facilities within the SCADA network. Properly developed policies and procedures that are enforced will greatly improve the security posture of the SCADA system.

In summary, these multiple “rings of defense” must be configured in a complementary and organized manner, and the planning process should involve a cross-discipline team with senior staff support from operations, facility engineering, and information technology (IT). The SCADA security team should first analyze the current risks and threat at each of the rings of defense, and then initiate a work plan and project to reduce the security risk.

For more information, see [ABBSEC09].

Hitachi ABB Power Grids
Grid Automation Products
PL 688
65101 Vaasa, Finland

https://hitachiabb-powergrids.com/microscadax

Scan this QR code to visit our website

1MRK 511 485-UEN