

SIEMENS

SICAM / SIPROTEC System Hardening for Substation Automation and Protection

V1.50

User Guide

Preface

Table of Contents

Introduction

1

Secure System Architecture

2

System Hardening

3

Access Control and Account Management

4

Security Logging and Monitoring

5

Security Patching

6

Malware Protection/Prevention

7

Backup and Restore

8

Secure Remote Access

9

Appendix

A

List of Required Open Ports

B

Literature

**NOTE**

For your own safety, observe the warnings and safety instructions contained in this document, if available.

Disclaimer of Liability

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

Document version: E50417-H8940-C619-A6.01

Edition: 01.2024

Version of the product described: V1.50

Copyright

Copyright © Siemens 2024. All rights reserved.

The disclosure, duplication, distribution and editing of this document, or utilization and communication of the content are not permitted, unless authorized in writing. All rights, including rights created by patent grant or registration of a utility model or a design, are reserved.

Trademarks

SIPROTEC, DIGSI, SIGRA, SIGUARD, SIMEAS, SAFIR, SICAM, Insights Hub, and OT Companion are trademarks of Siemens. Any unauthorized use is prohibited.

Preface

Purpose of the Manual

This document is a guideline to design a substation based on SIPROTEC and SICAM products in a secure manner. The guideline addresses the following domains:

- Secure network topology
- Firewalls and Network-based Intrusion Detection Systems (NIDS)
- Malware protection and prevention
- User management and role-based access control
- Business continuity and disaster recovery
- System hardening

Target Group

This document is primarily intended for persons working in the following areas:

- Sales of systems and equipment
- Project planning/implementation

Target Audience

Administrators and system engineers

Scope

This manual applies to the substation automation systems based on SICAM, SIPROTEC, and SIMEAS products.

Additional Support

For questions about the system, contact your Siemens sales partner.

Customer Support Center

Our Customer Support Center provides a 24-hour service.

Siemens Electrification & Automation

Global Support

Single entry point

Phone: +49 9131 1743072

E-mail: support.ea.si@siemens.com

Training Courses

You can request the individual training course offer at our Training Center:

Siemens AG

Siemens Power Academy TD

Phone: +49 911 9582 7100

Humboldtstraße 59
90459 Nuremberg
Germany

E-mail: poweracademy@siemens.com
Internet: www.siemens.com/poweracademy

Notes on Safety

This document is not a complete index of all safety measures required for operation of the equipment (module or device). However, it comprises important information that must be followed for personal safety, as well as to avoid material damage. Information is highlighted and illustrated as follows according to the degree of danger:



DANGER

DANGER means that death or severe injury **will** result if the measures specified are not taken.

- ✧ Comply with all instructions, in order to avoid death or severe injuries.
-



WARNING

WARNING means that death or severe injury **may** result if the measures specified are not taken.

- ✧ Comply with all instructions, in order to avoid death or severe injuries.
-



CAUTION

CAUTION means that medium-severe or slight injuries **can** occur if the specified measures are not taken.

- ✧ Comply with all instructions, in order to avoid moderate or minor injuries.
-

NOTICE

NOTICE means that property damage **can** result if the measures specified are not taken.

- ✧ Comply with all instructions, in order to avoid property damage.
-



NOTE

Important information about the product, product handling or a certain section of the documentation which must be given attention.

OpenSSL

This product includes software developed by the OpenSSL Project for use in OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

This product includes cryptographic software written by Eric Young (ey@cryptsoft.com).

Table of Contents

	Preface	3
1	Introduction	12
	1.1 Scope/Overview.....	13
	1.2 Principles.....	13
2	Secure System Architecture	14
	2.1 Principles of a Secure Substation Configuration.....	15
	2.2 Network Segmentation.....	17
	2.3 Recommendations.....	18
	2.3.1 Selecting a Right Version of the Microsoft Windows Operating System	18
	2.3.2 Securing Communication between Trusted Zones.....	18
	2.3.3 Virtualization.....	19
	2.4 Firewall.....	20
	2.4.1 Host-Based Firewalling.....	20
	2.4.2 RUGGEDCOM Network Firewall with Router Functionality.....	21
	2.4.2.1 Configuration of the Firewall.....	21
	2.4.2.2 Definition of Firewall Zones (fwzone).....	22
	2.4.2.3 Definition of Firewall Interfaces (fwinterface).....	23
	2.4.2.4 Definition of Firewall Policies (fwpolicy).....	24
	2.4.2.5 Definition of Firewall Rules (fwrule).....	25
	2.4.2.6 Source-Zone Examples.....	26
	2.4.2.7 Switching the Firewall ON.....	27
	2.4.3 Maintenance.....	27
	2.4.3.1 Export of the Configuration.....	27
	2.4.3.2 Adaptation of the Config File.....	28
	2.4.3.3 Uploading and Activating a Manually Modified Config File.....	29
	2.4.4 Blocked Access Due to FW Config Mistakes.....	30
	2.5 Fortigate Firewall.....	32
	2.5.1 Introduction.....	32
	2.5.2 Fortigate Firewall Network Configuration.....	32
	2.5.3 Setup of the Network for the Substat-02 Virtual Domain (VDOM).....	33
	2.5.4 Setup Firewall Rules in VDOM.....	38
	2.5.4.1 Example 1: Engineering Station (ES) in DMZ to Web HMI system in the Control Center.....	38
	2.5.4.2 Remote Host in Remote Zone to Engineering Station in the DMZ	40
	2.5.4.3 Additional Information on the Fortigate Firewall.....	42
	2.5.4.4 Recommendations.....	42
	2.6 IP Communication with the IEC 62351.....	44
	2.6.1 Fulfilling the IEC 62351-3.....	44
	2.6.2 Fulfilling the IEC 62351-4.....	44
	2.6.3 Fulfilling the IEC 62351-5.....	44

2.6.4	Fulfilling the IEC 62351-9.....	44
2.6.5	Use Case: Securing Communication using IEC 60870-5-104.....	44
2.6.5.1	Preconditions.....	45
2.6.5.2	Configuration of CP8050 for IEC 104 TLS Communication in Toolbox	46
2.6.5.3	Import of EST Communication Certificates in CP8050.....	50
2.6.5.4	Configuration of SICAM PAS for IEC 104 TLS Communication.....	52
3	System Hardening.....	57
3.1	Hardening Principles.....	58
3.2	Product-Hardening Tips.....	58
3.3	General.....	58
3.3.1	Hardware.....	58
3.3.1.1	Server Rack Setup.....	58
3.3.1.2	Disabling All Wireless Connections.....	59
3.3.1.3	No Cordless Keyboards.....	59
3.3.1.4	No Biometric Authentication Devices.....	59
3.3.1.5	Boot and BIOS Passwords.....	59
3.3.1.6	Disabling Wake-On LAN.....	60
3.3.1.7	Disabling Hardware Virtualization.....	60
3.3.1.8	Define System Boot-Up Sequence.....	60
3.3.2	Windows General.....	60
3.3.3	The Group Policy Object in Windows.....	61
3.3.3.1	Why is the Group Policy Object Useful?.....	61
3.3.3.2	Center for Internet Security (CIS) Benchmarks and Remediation Kits.....	61
3.4	Siemens Products.....	63
3.4.1	SIPROTEC 5/DIGSI 5.....	63
3.4.1.1	SIPROTEC 5 Devices.....	63
3.4.1.2	Block IEC 61850 Settings Changes.....	63
3.4.2	SICAM A8000.....	64
3.4.2.1	Deactivation of Unnecessary System and Communication Services.....	64
3.4.3	SICAM PAS.....	66
3.4.3.1	Firewall Settings for Windows.....	66
3.4.4	SICAM SCC.....	66
3.4.4.1	Firewall Settings for Windows.....	66
3.4.5	RuggedCom Switch.....	66
3.4.5.1	Change all Default Passwords.....	66
3.4.5.2	Deactivation of Unused Switch Ports.....	66
3.4.5.3	Deactivation of Unused Protocols.....	67
3.4.5.4	SNMP Configuration.....	67
3.4.6	RuggedCom Router.....	67
3.4.6.1	Change all Default Passwords.....	67
3.4.6.2	Deactivation of Unused Switch Ports.....	68
3.4.6.3	Use Secure Protocols.....	68
4	Access Control and Account Management.....	69
4.1	Least Privilege.....	70
4.2	Account-Management Configuration Instructions.....	71
4.2.1	Topology.....	71
4.2.2	Primary Domain Controller (PDC).....	71
4.2.2.1	Installation of Primary Domain Controller (PCD)	71
4.2.2.2	Configuration of a Domain Controller (DC).....	79
4.2.3	Domain.....	84
4.2.3.1	Adding Clients to the Domain.....	84
4.2.3.2	Group Policies (Domain).....	86

4.2.3.3	Group-Policy Management.....	86
4.2.3.4	Group Policy Export/Import Function (Domain Controller).....	89
4.2.3.5	DG Group Policy Object.....	91
4.2.4	Read-Only Domain Controller.....	91
4.2.4.1	Setting the Read-Only Domain Controller (RODC).....	91
4.2.4.2	Force Replication Manually.....	95
4.2.4.3	Password Replication Policy (PRP).....	95
4.3	Role-Based Access Control for Field-Level Devices.....	100
4.3.1	Network Policy Server (NPS).....	101
4.3.1.1	Network Policy Server for RADIUS.....	101
4.3.1.2	Installation of Network Policy Server.....	101
4.3.2	NPS Setup and Verification of Server Settings.....	102
4.3.2.1	Registering Network Policy Server in the Active Directory.....	102
4.3.2.2	Port Numbers.....	105
4.3.2.3	Policies.....	107
4.3.3	User Management of the SIPROTEC/SICAM Device.....	107
4.3.3.1	Windows User Groups and User Settings.....	108
4.3.3.2	Add Global Security Groups.....	108
4.3.3.3	Local Users for SIPROTEC 5 Devices.....	110
4.3.3.4	Creation of Password Policy Objects.....	112
4.3.3.5	Assigning a Password Settings Object (PSO) to a User Group or a User.....	113
4.3.3.6	Configuration of a Network Policy Server (NPS).....	118
4.4	Public Key Infrastructure (PKI).....	127
4.4.1	Digital Certificates.....	128
4.4.1.1	Registration Authority.....	129
4.4.1.2	Certificate Revocation List (CRL).....	129
4.4.2	PKI Workflow.....	129
4.4.3	Creating Key Material.....	130
4.4.4	Using SICAM GridPass to Create Key Material.....	131
4.4.4.1	Overview.....	131
4.4.4.2	Workflow.....	132
4.4.4.3	Integration.....	132
4.4.4.4	Operating Overview.....	133
4.4.4.5	Web UI Access.....	133
4.4.4.6	CRL Server.....	134
4.4.4.7	EST Server.....	134
4.5	OpenLDAP.....	135
4.5.1	Overview.....	135
4.5.2	Installing OpenLDAP Debian Buster (11).....	135
4.5.3	OpenLDAP Attribute Certificates.....	140
4.5.4	Using Active Directory in an OpenLDAP Environment.....	140
4.5.5	LDAP and Microsoft Active Directory.....	142
4.6	Device-Specific Configuration Notes.....	143
4.6.1	SICAM SCC.....	143
4.6.1.1	Setting Up User Authorizations.....	143
4.6.2	SICAM PAS.....	146
4.6.2.1	Setting Up User Administration.....	146
4.6.3	SIPROTEC 5 and DIGSI 5.....	146
4.6.4	SICAM A8000/SICAM Device Manager.....	147
4.6.5	RuggedCom Switch RSG2100.....	147
4.6.6	RuggedCom RX 1400/RX1500	147

5	Security Logging and Monitoring	149
5.1	General.....	150
5.2	Logging Architecture.....	151
5.3	Logging Windows System.....	151
5.3.1	Viewing Remote Logs in the Windows Event Viewer	152
5.3.2	Firewall Logs.....	157
5.3.3	PowerShell Logs.....	158
5.4	Logging with Syslog.....	158
5.4.1	Logging with Syslog.....	158
5.4.2	syslog Client.....	159
5.4.3	syslog Server.....	160
5.4.3.1	General.....	160
5.4.3.2	Syslog Server with NXLog.....	160
5.5	Logging in Siemens Products.....	161
5.5.1	SIPROTEC 5.....	161
5.5.1.1	Configuring the Central Syslog Server.....	162
5.5.2	SICAM PAS.....	163
5.5.2.1	SICAM PAS Security Log Events.....	163
5.5.2.2	Configuring Syslog.....	163
5.5.3	RuggedCom Switch RSG2100.....	164
5.5.3.1	Alarm Configuration for Syslog.....	164
5.5.3.2	Display Syslog Information.....	165
5.5.3.3	Syslog Server Connection.....	165
5.5.4	RuggedCom Router RX1500.....	167
5.5.4.1	Alarm Configuration for Syslog: Event Configuration.....	167
5.5.4.2	Firewall Log Setup.....	168
5.5.4.3	Display Syslog Information.....	169
5.5.4.4	Syslog Server Connection.....	170
5.6	Recommendations.....	172
5.6.1	SIEM as a Service.....	173
6	Security Patching	174
6.1	General Instruction.....	175
6.2	Updating Windows Operating System.....	175
6.2.1	Downloading the Latest Security Patch.....	175
6.2.2	Downloading the Latest Security Patch for Legacy Systems.....	176
6.2.3	Installing the Patches.....	177
6.2.4	Checking the Patches with SICAM SDM.....	178
6.3	Automated Patching.....	178
6.3.1	Installation and Setup.....	178
6.3.1.1	Installation and Setup.....	178
6.3.1.2	WSUS and IIS Installation.....	179
6.3.1.3	Installation of the WSUS Server Role.....	179
6.3.1.4	Report Viewer.....	180
6.3.1.5	Setup of the WSUS Export Server.....	180
6.3.1.6	Setup of the WSUS Import Server.....	182
6.3.1.7	Setup of the WSUS Clients – Connecting Clients to the WSUS Import Server.....	183
6.3.2	Update Procedure.....	184
6.3.2.1	Download all Updates on the WSUS Export Server.....	184
6.3.2.2	Export the Updates and Meta Data.....	185
6.3.2.3	Import the Updates and Meta Data on the WSUS Import Server.....	185

6.3.2.4	Approving Updates for the Different Client/Computer Groups on the WSUS Import Server.....	186
6.3.3	Event Logs.....	187
6.4	Update Instructions for Siemens Products.....	187
6.4.1	DIGSI 5 Engineering Software.....	187
6.4.2	SIPROTEC 5.....	188
6.4.3	SICAM A8000 Series/SICAM RTUs.....	188
6.4.3.1	SICAM TOOLBOX.....	188
6.4.3.2	SICAM Device Manager.....	188
6.4.4	RuggedCom Switch RSG2100.....	189
6.4.5	RuggedCom Router RX1500.....	190
7	Malware Protection/Prevention.....	193
7.1	Motivation.....	194
7.2	Windows Defender.....	194
7.2.1	Blacklisting Solution with Windows Defender.....	194
7.2.1.1	Setting up/Configuring Windows Defender Antivirus.....	195
7.2.1.2	Configuring Windows Defender Antivirus via Local GUI.....	196
7.2.1.3	Updates for Windows Defender Antivirus.....	197
7.2.1.4	Feature Updates of Windows Defender Antivirus Platform.....	198
7.2.1.5	Update File Location.....	198
7.2.1.6	Logging of Windows Defender Antivirus.....	199
7.2.1.7	Microsoft Windows Defender Antivirus on Microsoft Windows Server 2016.....	200
7.2.2	Whitelisting Solution with Windows Defender.....	200
7.2.2.1	Windows Defender Application Control (WDAC).....	201
7.2.2.2	Windows Defender Exploit Protection.....	201
7.2.2.3	Configuration Process for WDAC.....	201
7.2.2.4	Creating and Deploying a Policy.....	202
7.2.2.5	Installation of Updates.....	205
7.2.2.6	WDAC Event Logs.....	207
7.2.2.7	Disabling WDAC.....	208
7.2.2.8	PowerShell Command Summary.....	208
7.2.2.9	Whitelist Creation.....	209
7.2.2.10	Whitelist Merging Test.....	209
7.2.2.11	Configuration Details of Policies.....	209
7.2.2.12	WDAC Audit Mode.....	212
7.2.2.13	Signing of a WDAC Policy – Protection Against Tampering (Optional).....	212
7.2.2.14	Prerequisites.....	212
7.2.2.15	Known Issues.....	213
7.2.3	Windows Defender Exploit Protection.....	213
7.2.3.1	Exploit Protection Configuration.....	214
7.2.3.2	HW Requirements.....	221
7.3	Malware Protection for Siemens Products.....	222
7.3.1	SICAM PAS Station Controller.....	222
7.3.2	SICAM SCC HMI PC.....	222
7.3.3	SICAM A8000 Series/SICAM RTUs.....	222
7.3.4	SIPROTEC 5/DIGSI 5 Devices.....	222
7.3.5	Service PC.....	223
7.4	Recommendations.....	223
8	Backup and Restore.....	224
8.1	General.....	225
8.1.1	Illustrated Concept.....	225

8.1.2	Introductory Notes.....	225
8.2	Concept.....	226
8.2.1	Overview.....	226
8.2.2	Data Types (What).....	226
8.2.2.1	Archiving Real-Time Data.....	227
8.2.2.2	Archiving Firmware.....	227
8.2.3	Backup Schedule (When).....	227
8.2.4	Backup Media (Where).....	228
8.2.4.1	Local Backup Storage Recommendation 1: Removable Media (External Hard Disks).....	228
8.2.4.2	Local Backup Storage Recommendation 2: NAS (Network-Attached Storage) Server.....	229
8.2.4.3	Online Backup Storage Recommendation 1: File System on Operate SharePoint....	229
8.2.4.4	Online Backup Storage Recommendation 2: Online Cloud Services.....	229
8.3	Disaster Recovery.....	229
8.3.1	Recovery Process.....	230
8.3.2	Disaster Recovery Strategy.....	232
8.3.3	Test Procedure.....	235
8.4	Backup Procedure for Siemens Products.....	235
8.4.1	IED SIPROTEC (with DIGSI).....	235
8.4.1.1	Archiving/Retrieving a Project.....	235
8.4.2	SICAM PAS.....	238
8.4.2.1	Local Backup Storage Recommendation 2: NAS (Network-Attached Storage) Server.....	238
8.4.2.2	Archiving Project Data.....	238
8.4.2.3	Dearchiving Project Data.....	238
8.4.2.4	Dearchiving Large Project.....	239
8.5	SICAM SCC.....	239
8.5.1	Backup the SICAM SCC Database.....	239
8.5.2	Restore the SICAM SCC Database.....	239
8.5.3	Backup SICAM SCC Real-Time Data.....	240
8.5.4	Alarm Logging Archive Backup.....	240
8.5.5	Tag Logging Archive Backup.....	242
8.5.6	Restore Archive Backup.....	243
8.6	Archiving of Engineering Tools.....	245
9	Secure Remote Access.....	247
9.1	cRSP (common Remote Service Platform).....	248
9.1.1	Siemens-Owned Access.....	248
9.1.2	Customer-Owned Access.....	248
9.1.3	Activate Windows RDP.....	249
9.1.4	Network Setup – Firewall/NAT.....	251
9.1.4.1	Interface Settings.....	252
9.1.4.2	Firewall Policy/Rule Settings.....	252
9.1.4.3	NAT – Network Address Translation.....	252
9.1.5	Test the cRSP Access.....	253
9.1.5.1	cRSP Settings.....	253
9.1.5.2	Logon to the cRSP.....	254
9.1.6	Applications for Remote Monitoring and Control.....	256
9.1.6.1	Remote Desktop (RDP).....	256
9.1.6.2	Applications for the Transfer of Files.....	258

9.1.6.3	File Transfer on Remote Site.....	259
A	Appendix.....	263
A.1	Abbreviations.....	264
B	List of Required Open Ports.....	265
B.1	SICAM PAS/PQS, SICAM SCC.....	266
B.2	SIPROTEC 5/DIGSI 5.....	268
	Literature.....	269

1 Introduction

1.1	Scope/Overview	13
1.2	Principles	13

1.1 Scope/Overview

Digitization has improved the interconnectivity of automation systems tremendously. Today, our systems are more connected than ever. This is due to the advancement in technology that customers are incorporating the interconnected Servers, Computers, HMIs, PLCs, and Sensors. With the advancements in Industrial Internet of Things (IIoT) there is a convergence of sensors and field devices into the network. This convergence while provides huge business benefit but also exposes entire networks to security threats such as hacking, malware, worms, and viruses. Additionally, the increased use of common software and operating systems, for example, Windows® and Linux, and standard communication protocols such as TCP/IP-based protocols, have also raised vulnerability.

Protection against attacks and continued availability of systems needs focus on cybersecurity during planning and designing the systems itself. Planning for security at the outset provides for a more complete and cost-effective system. Planning cybersecurity during system design also ensures that security features are supportable – attempting to retrofit secure measures into existing environments is often ineffective and cost-prohibitive. Security must be addressed at all levels of the development process.

This document provides guidelines for designing secure automation systems that employ the Siemens Energy Automation products. The guide is intended for use throughout the product lifecycle and is updated whenever major changes are made to the described products.



NOTE

This Guide provides cybersecurity implementation in the Substation assuming basic understanding of the concepts described in this document. Siemens also provides detailed guide on all the concepts and step-by-step guide for a variety of configurations as a service. Contact the local siemens SI Support for details.

1.2 Principles

Cybersecurity is not a onetime exercise and needs continuous efforts. What that means is a single protection mechanism gives protection against threats known point in time only. To achieve continued protection Defense-in-depth needs to be implemented with continuous monitoring of security events and incidents.

The defense-in-depth security concept includes defense strategies designed to protect against inter alia following threats:

- Denial of Service
- Circumvention of specific security mechanisms, such as **Man in The Middle** (MITM)
- Intentional maloperation through permitted actions, such as password theft
- Maloperation through non-configured access rights
- Data spying, for example, of recipes and business secrets or operational plans for plants and their security mechanisms
- Manipulation of data, for example, to downplay the importance of alarms
- Deletion of data, for example, log files to cover up attack activities

The following defense strategies serve as an overall approach to supplement the required security in the substation:

- Defense in Depth
- Appropriate network-topology design / segmentation
- Least privilege principle
- Timely response to security events
- Continuous Threat monitoring

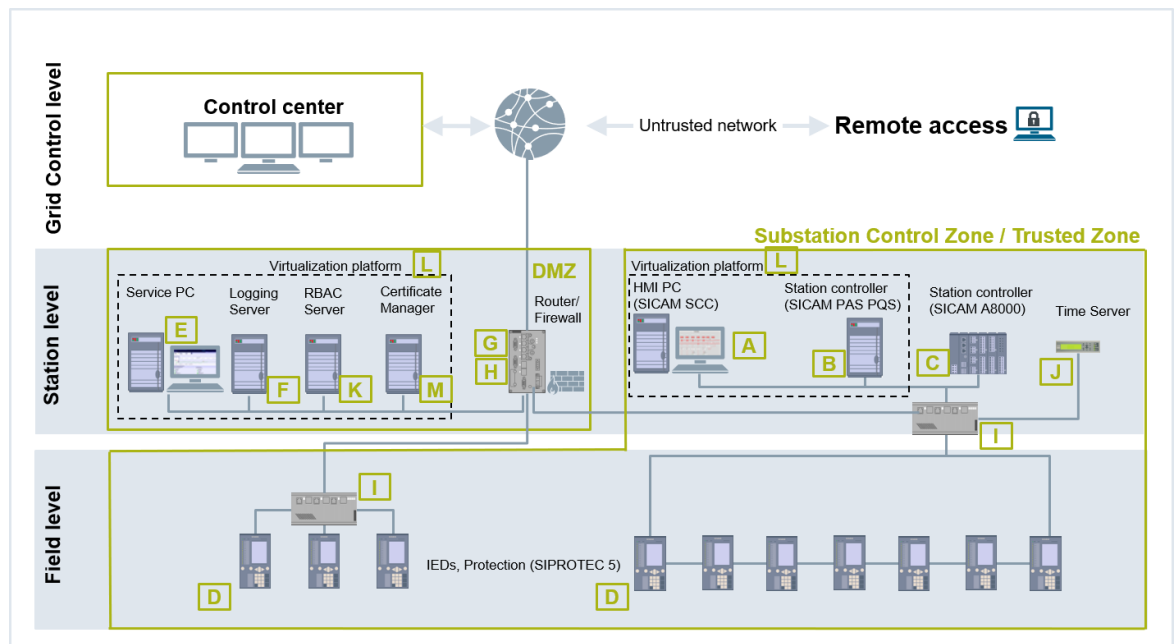
2 Secure System Architecture

2.1	Principles of a Secure Substation Configuration	15
2.2	Network Segmentation	17
2.3	Recommendations	18
2.4	Firewall	20
2.5	Fortigate Firewall	32
2.6	IP Communication with the IEC 62351	44

2.1 Principles of a Secure Substation Configuration

The first step to cybersecurity is defining a secure system architecture while implementing an automation system. The figure below shows a typical cybersecurity architecture and based on Siemens Secure Substation Blueprint. While designing a cybersecurity architecture it is important to address not only the individual requirements but also defense-in-depth. The security should start at the design phase itself. The following sections in this chapter would help in implementation of the communication network of a substation automation system together with Siemens Energy Automation products. The compatibility of these cited measures, network topologies, security products, or power-system components with communication protocols used in this environment has been tested and proved.

A typical substation system comprises a Substation Control Zone and Demilitarized Zone (DMZ) protecting this Control Zone. Both typically reside at same physical location. All IP-based communication to and from the substation control zone passes through the substation firewall (G/H in figure below). This comprises communication related to process-control with a connected trusted control center zone and optional remote access users.



[sc_Secure Substation Architecture, 1, en_US]

Figure 2-1 Secure Substation Architecture

Table 2-1 Figure Reference

Legend	Description
A	SICAM SCC Human Machine Interface (HMI) for local control and monitoring, hosted on a Windows Operating System. This is a single point of control and monitoring inside the substation.
B	SICAM PAS/PQS Station Controller application hosted on a Windows Operating system, as alternative to C
C	SICAM A8000 Station Controller RTU, as alternative to B
D	SIPROTEC 5 Protection and Control IEDs
E	Service PC Host of all engineering tools and Single point of all engineering accesses, hosted on a Windows Operating System. The Service PC acts as a jump host for remote access.

Legend	Description
F	Substation Central Security Logging Server Collects all security Logs from the components of the system. Source for all security logs for a superordinate SIEM system
G	Router with firewall, RUGGEDCOM firewall hosted on a ROX Operating System
H	Router with firewall and integrated Intrusion Detection System
I	Network switch
J	Time server
K	Active Directory Server and RADIUS Server Built as a Read Only Domain Controller (RODC) hosted on a Windows Operating System
L	Virtualization platform Microsoft HyperV hosted on a Windows Operating System Optional implementation instead of dedicated hardware
M	Certificate Manager, SICAM GridPass hosted on a Windows Operating System

**NOTE**

It is crucial to implement security measures fitting the actual needs of a specific plant. To achieve this, a threat analysis considering the targets and impacts of security attacks on a plant is necessary starting with the planning phase of a plant.

Siemens also recommends analyzing the implemented cybersecurity measures regularly and adapting it if the threat conditions change. Setting up a secure substation configuration follows a few principles.

Principle 1: Network Segmentation

The first and most important principle is the network segmentation as described in the next chapter. To avoid an incident or limit the damage of an incident that already happened, the secure substation must be set up as an environment where the communication possibilities are as restricted as possible. To reach that goal, the network borders must be secured using firewalls. Furthermore, the communication between the network segments must be secured, for example, with a virtual private network (VPN).

Principle 2: Secure Configuration

The correct configuration of a firewall and a VPN is as important as the firewall and the VPN themselves. A firewall must be configured with a **default drop rule** where every packet that is not explicitly allowed will be dropped. This default rule must be active for packets coming from the directly connected network but also coming from the VPN tunnel. After that, only dedicated and known communication relations must be allowed. This can be done with the IP address of the source and the destination and the protocols port used in that specific communication relation.

Principle 3: Least Privilege

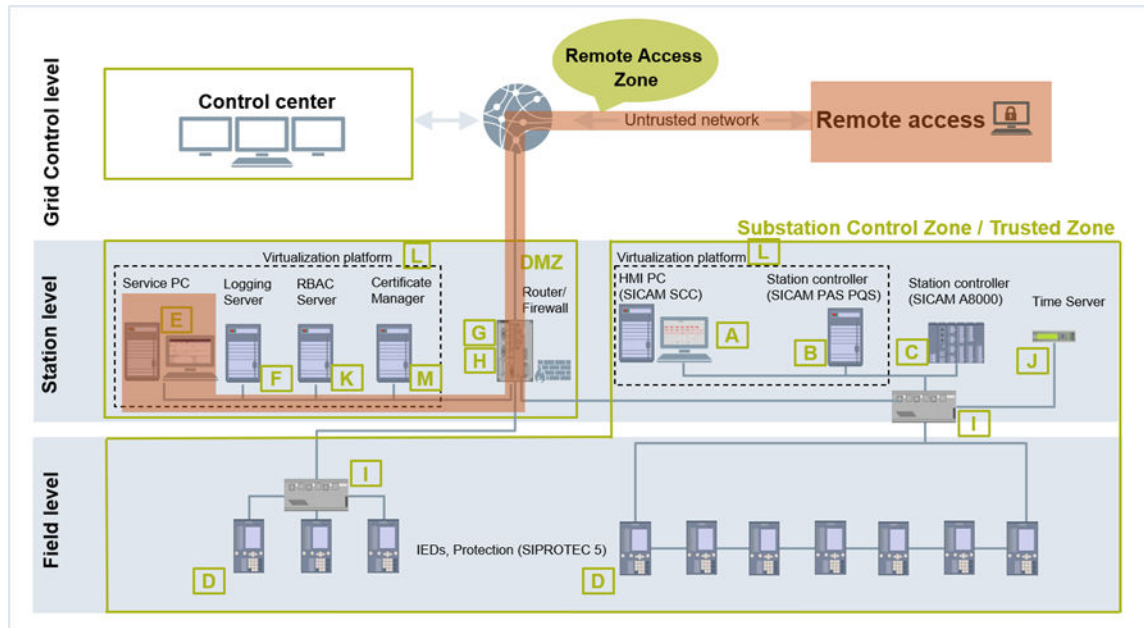
While Implementing VPN, though it is easy to have single VPN group for all participants but this defeat **least privilege** principle and the strategy of network segmentation because a VPN connects networks on IP layer. Therefore, every communication relation needs a VPN group. Of course, one VPN group is enough for more than one communication relation, which is using the same VPN gateways.

Principle 4: Continuous Monitoring

One more important principle is the monitoring of your network. To identify attacks or suspicious irregularities, it is important to have a central logging server collecting critical information from all involved components of the secure substation like dropped packets of a firewall or error entries in a Windows event log system.

2.2 Network Segmentation

Achieving absolute or 100 percent security as well as preventing every security incident is not possible. Thus, the system, including its network topology, must be designed to limit the damage caused by an incident. Network segmentation provides for the segmentation of a substation network into subnetworks. This approach should be accompanied by controlling the network traffic across the borders of the subnetworks using Virtual Private Networks (VPN) and firewall technologies.



[sc_zone_architecture, 1, en_US]

Figure 2-2 Zone Architecture

This chapter describes how a substation network could be segmented into different zones.

Description of the Certain Zones

Substation Control Zone

The Substation Control Zone is the trusted logical zone with field level devices and station controller equipment.

At field level the devices such as the IEDs and Protection devices like SIPROTEC 5 are located. For connecting these devices, a mixed configuration with optical fiber and electrical network interfaces may exist based on the substation operator's requirements. IEDs connected either via a serial protocol like IEC 60870-5-101, IEC 60870-5-103, or TCP/IP-based IEC 61850 MMS/GOOSE, DNP3 are in this zone.

To achieve optimum security, the interfaces for configuration are separated from the process-data interface. The systems-control network and the network for remote access shall be separated entirely by selection of an independent Ethernet port for communication between the device and DIGSI5. To access SIPROTEC 5 via network, an Ethernet hub shall be used. This would allow a SIPROTEC Device to be accessed from Engineering Station located outside of the substation.

The Station Controller SICAM PAS and the SICAM SCC (Local HMI) can be configured in the following ways:

- SICAM PAS installed on Industrial PC with Full Server and DIP (option: redundant configuration)
- SICAM SCC installed on regular PC with Windows 10 with latest updates

Alternatively, the SICAM PAS and SICAM SCC can be installed on a Single Physical Server using Virtualization platforms HyperV Over a Windows Operating System. The Control Zone also includes Time Synchronization Server.

Demilitarized Zone (DMZ)

The Demilitarized Zone (DMZ) contains Servers for services such as Certificate Management, User Management, Logging and Service PC. The Certificate Manager is SICAM Grid Pass installed on a Windows Server. These Servers can also be installed on a Virtualized System using HyperV over a Windows Operation System. DMZ is protected using a dedicated Firewall such as RUGGEDCOM firewall hosted on a ROX Operating System or an Integrated Firewall cum Intrusion Detection System (IDS).

Remote Access Zone

Remote Access is for various purposes and mainly for troubleshooting. The Access to Substation is only via Service PC in DMZ. The Remote Access connection shall be protected and secured. The Secure Remote Access using Siemens cRSP shall be used for remote access.

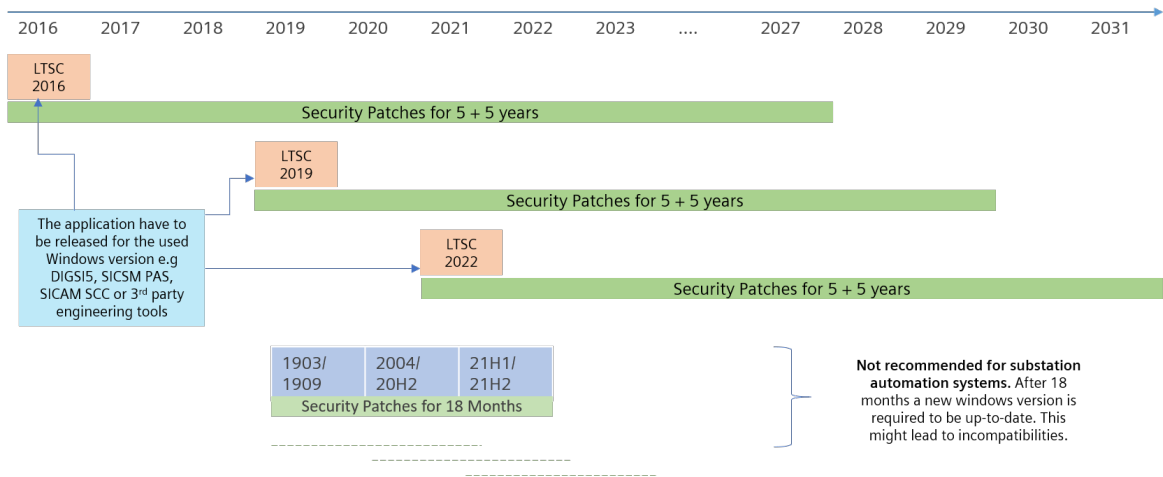
2.3 Recommendations

This document provides guide to operate and maintain a Substation securely. While designing a secure system is the first step, selection of secure components is also very crucial. Patching and updating is a very important task in security and selection of components with long-term service and support is very important as upgrades are time consuming and needs through compatibility testing before deployment.

When the communication is trespassing a secure trusted zone, additional security measures are required to ensure its confidentiality. Encryption along with a firewall shall be used to achieve this. Section 2.3.2 [Securing Communication between Trusted Zones](#) describes use case for such communication.

2.3.1 Selecting a Right Version of the Microsoft Windows Operating System

Windows comes in various variants and support lifecycle. The following figure shows the typical windows operating systems' lifecycle. It is important to select Windows with long-term support life. It is recommended not to select Windows Operating System with smaller lifecycle.



[sc_Selecting right version of Windows, 1, en_US]

Figure 2-3 Selecting Right Version of Windows

For more information on the Microsoft Windows Operating System lifecycle, refer to <https://support.microsoft.com/en-in/help/13853/windows-lifecycle-fact-sheet>.

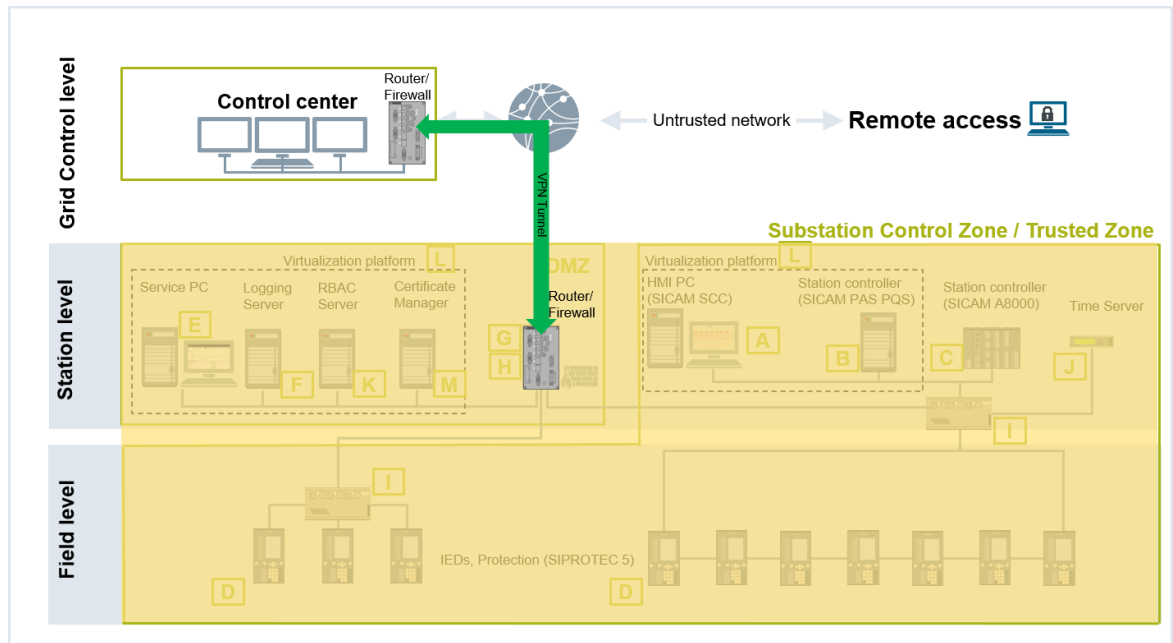
2.3.2 Securing Communication between Trusted Zones

When the communication is traversing the secure zone boundaries (Trusted Network to Untrusted Network) it requires additional security measures to maintain data integrity and/or confidentiality. An example of such

a communication is the communication channel from the substation site to the control center site which is typically located at 2 different sites geographically. Normally this communication channel traverses unsecure or unknown networks.

Use of Virtual Private Network (VPN) is recommended for such communications. VPN is generally of two types – IPsec-based VPNs and TLS-based VPNs. In general, IPsec connects networks and TLS secures protocols because IPsec runs on network layer and TLS on transport layer according to the OSI layer model.

To secure communication between zones site-to-site VPN is recommended. Usually this is achieved using an IPsec protocol which ensures authentication, integrity, and confidentiality of the network traffic via the untrusted network. An example VPN configuration looks as follows:



[sc_Site-to-Site VPN, 1, en_US]

Figure 2-4 Site-to-Site VPN



NOTE

To configure a site-to-site VPN, 2 IPSEC endpoints are required. Also, routing settings on both routers must be done in advance.

2.3.3 Virtualization

Virtualization provides significant infrastructure and operational benefits compared to hardware-based solution such as:

- Reduction of Hardware/Software cost
- Reduction of Maintenance efforts
- Support of additional client systems
- Increased availability
- Simplification of Compatibility Tests

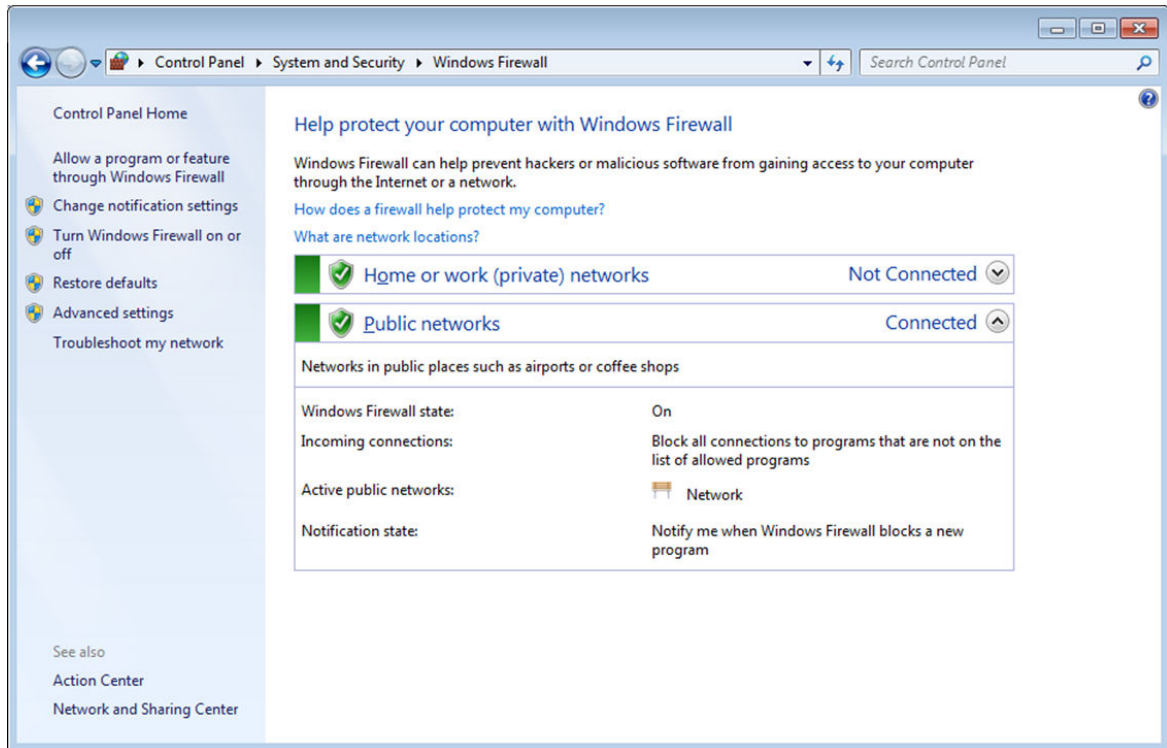
Few of the component of a substation may be deployed in a virtualized system. But the security of host operating system as well as the virtualized systems shall be ensured in accordance with the measures described in this manual.

2.4 Firewall

2.4.1 Host-Based Firewalling

According to the Defense-In-Depth strategy, Siemens recommends enabling the host-based firewall functionality included with the Windows Operating System.

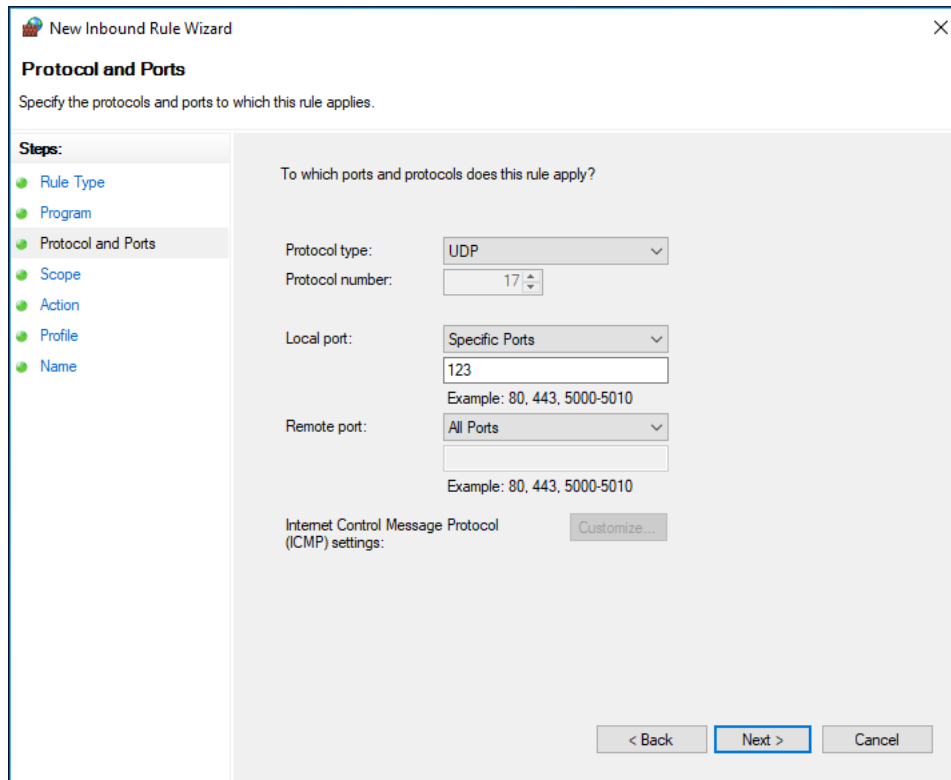
- ✧ In Windows, open your Firewall configuration, **Change settings** and activate the Firewall



[sc_windows_firewall_config.1, en_US]

Figure 2-5 Windows Firewall Configuration

- ✧ Disable all the default firewall rules and enable only those communications which are necessary for the Substation operations. Add a Server Port for accepting incoming connections if necessary. For example, if the Server acts as NTP server, accept incoming connections also on UDP Port 123.



[sc_ntp_server_port, 2, en_US]

Figure 2-6 NTP Server Port Enabling

Besides the “network core” service, there may be additional requirements such as: (refer appendix for more detail):

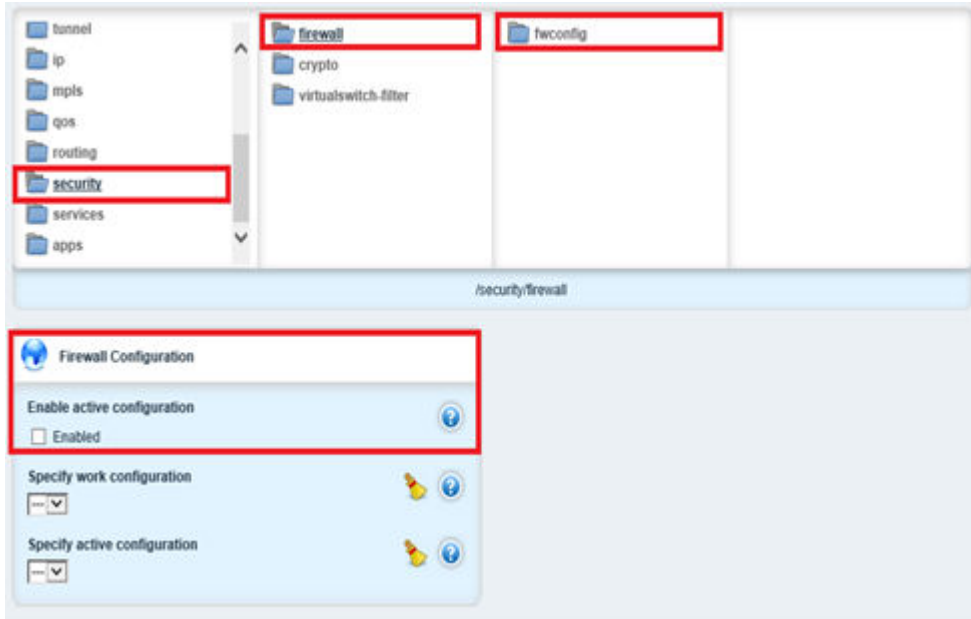
- The Exception for File and Printer Service (Port 139/445) for shared folders on Server or Network Discovery if desired.
- The Remote Event Log Management if Remote Access for Logging is used.

2.4.2 RUGGEDCOM Network Firewall with Router Functionality

The Siemens Secure Substation Blueprint architecture is tested with RUGGEDCOM Firewall cum Router that is based on a stateful Inspection to secure traffic between the Grid Control Center and DMZ from Trusted/ Substation Control Zone. The following chapter shows the configuration for a RuggedCom RX1500/1400 router.

2.4.2.1 Configuration of the Firewall

- ✧ To configure the firewall functionality of the router, browse to security, firewall, and fwconfig. At this stage, a firewall configuration needs to be created and it should be named in a clearly identifiable way, e.g.: **FW1**.



[sc_Configuring a Ruggedcom Firewall, 1, en_US]

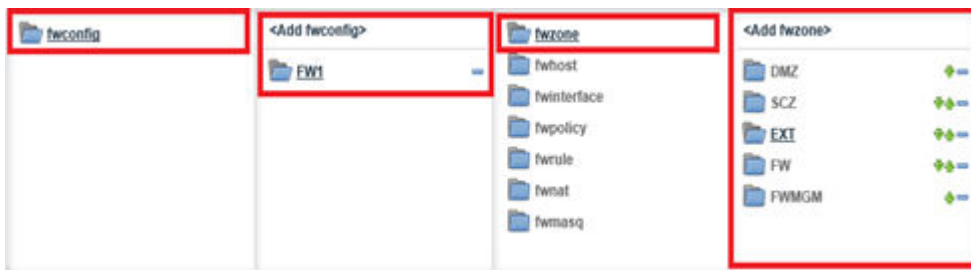
Figure 2-7 Configuring a Ruggedcom Firewall

2.4.2.2 Definition of Firewall Zones (fwzone)

Now, different firewall zones need to be created. Click in fwzone and add the below basic setup zones:

Firewall Zones	
DMZ	Demilitarized Zone
SCZ	Substation Control Zone
FW	Router (Firewall)
EXT	External Customer Network (may be connected via corporate network or Control Center)
MGM	Management Zone
FWMGM	Firewall Management Front Port

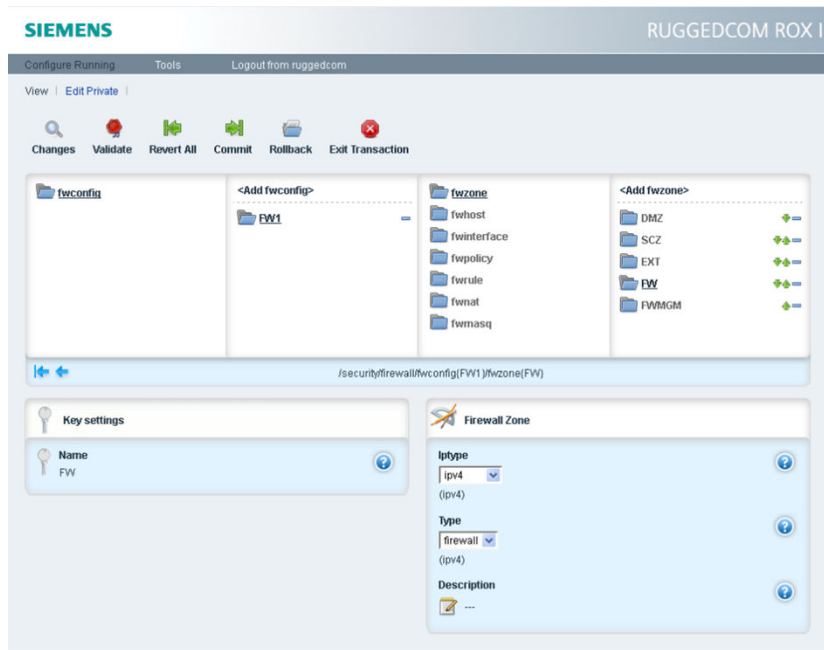
DMZ/SCZ/EXT/MGM zones will be used for the connected network, **FWMGM** zone will be used for the Management Front Port, which is commonly used for maintenance purpose and the **FW** zone as a special area, because it represents the router/firewall itself.



[sc_Defining Zones in a Ruggedcom Firewall, 1, en_US]

Figure 2-8 Defining Zones in a Ruggedcom Firewall

All Zones should be assigned to IP type **IPv4**, except **FW** zone, which must be assigned to **firewall**. The following figures show the assignment of each type for individual areas:



[sc_Assigning IP types to zones in a Ruggedcom Firewall, 1, en_US]

Figure 2-9 Assigning IP Types to Zones in a Ruggedcom Firewall

✧ Activate the changes by pressing **Commit** on the top Menu.

2.4.2.3 Definition of Firewall Interfaces (fwinterface)

The next step is creating the relationship between the zones and the router interfaces:

- Management front port = fe-cm-1
- Slot 1m1 port 6 = fe-1-6
- Virtual switch 2 = switch.0002
- Virtual switch 3 = switch.0003
- Virtual switch 4 = switch.0004

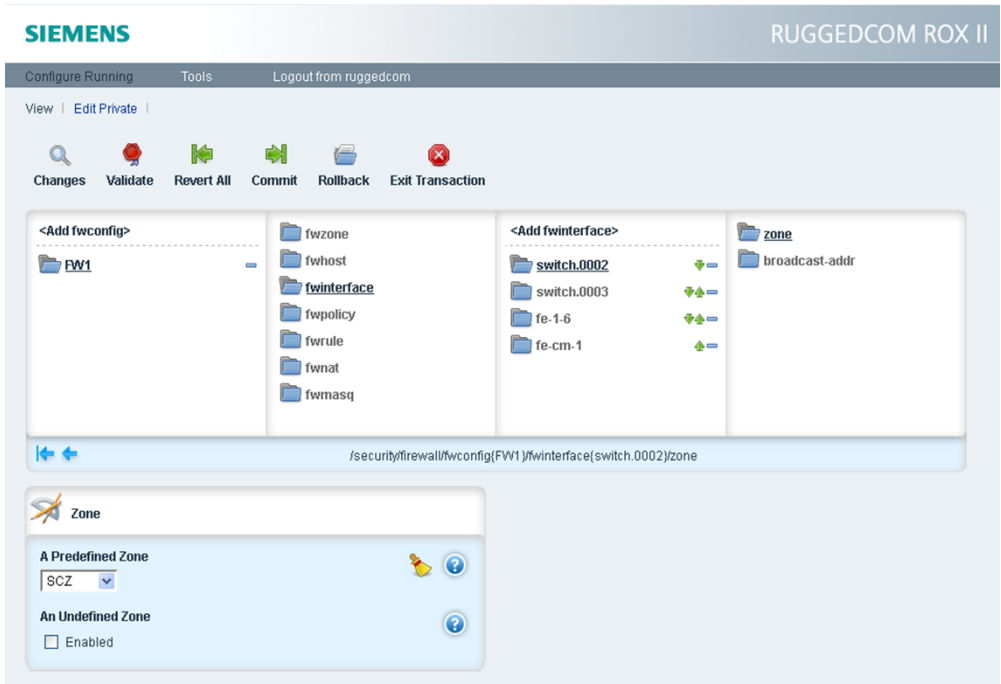


NOTE

Each interface must be created exactly with the same name as each interface name in the router under the folder IP.

Each interface must be assigned to one of the zones. The following figures show the assignment of the different interfaces to the corresponding zone in the Web interface.

✧ Navigate under FW1 (created firewall) and fwinterface, select **Add fwinterface**.



[sc_Defining firewall interface in a Ruggedcom Firewall, 1, en_US]

Figure 2-10 Defining Firewall Interface in a Ruggedcom Firewall

Only the FW zone will be without a physical interface.

2.4.2.4 Definition of Firewall Policies (fwpolicy)

Next step is to define the default Firewall Policies. In general, two main policies are used to define the information exchange between two or more zones. Each policy defines one action (accept or drop), one source area and one destination area. The following table shows the policies configured in this firewall:

Table 2-2 Firewall Policy Rules

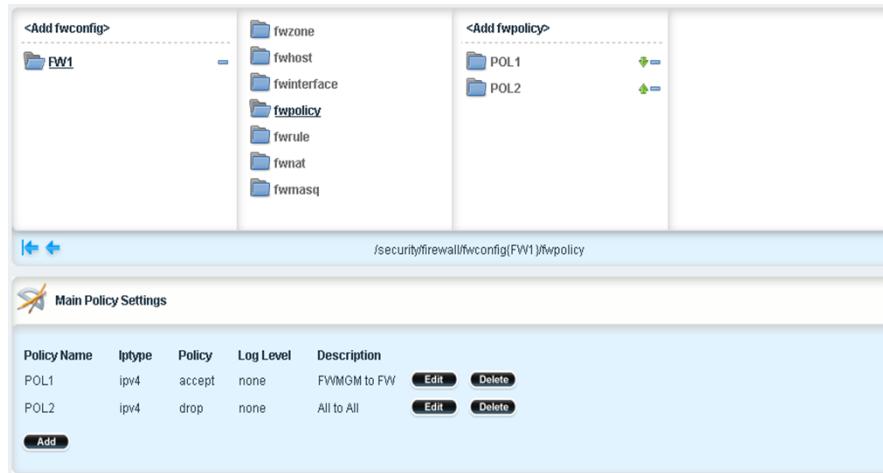
Policy Name	Policy	Description	Source Zone	Destination Zone
Pol1	Accept	Accept all traffic from FWMGM to FW	FWMGM	FW
Pol2	Drop	Drop all traffic from All to All	All	All



NOTE

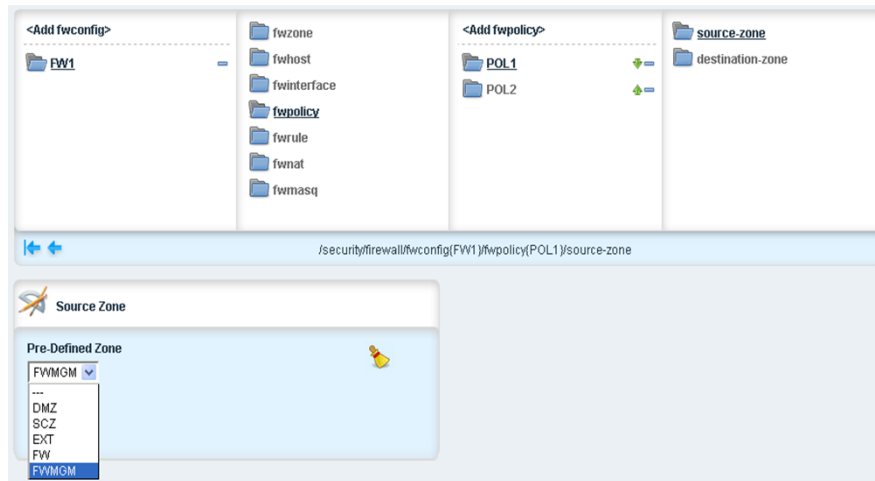
Pol1 in this example is a temporary policy and could be disabled after the final firewall configuration.

The following figures show how the policies look in the web browser, and where the zones (source and destination) are assigned for a policy:



[sc_adding fwpolicy, 1, en_US]

Figure 2-11 Adding fwpolicy



[sc_Defining firewall policy in a Ruggedcom Firewall, 1, en_US]

Figure 2-12 Defining Firewall Policy in a Ruggedcom Firewall

2.4.2.5 Definition of Firewall Rules (fwrule)

Defining firewall rules requires 4 important steps to be taken:

- Action to be taken e.g **Accept** or **Drop**
- Source of the network package which is represented as IP address/Subnet
- Destination of the network package also represented as IP address/Subnet
- Network Protocol used in the communication

Table 2-3 Defining Firewall Rules in a RUGGEDCOM Firewall

Protocol	Communication	Ports (Source/Destination)
FTP (File Transfer Protocol)	TCP	21/21
SNMP (Simple Network Management Protocol)	UDP	161/162
NTP (Network Time Protocol)	UDP	123/123
RDP (Remote Desktop Protocol)	TCP	>1024/3389
HTTP (Hypertext Transfer Protocol)	TCP	>1024/8080

Protocol	Communication	Ports (Source/Destination)
HTTPS (Hypertext Transfer Protocol Secure)	TCP	any/443
IEC 104	TCP	2404/2404
IEC 61850	TCP	any/102
MODBUS	TCP	502/502

- ✧ Navigate to the firewall rule and add fwrule.
- ✧ Assign the IP of the source and the port which should be open to allow communication.
- ✧ Assign the IP of the destination and the port which should be open to allow the communication.
- ✧ Configure the communication protocol according to the preceding table.

2.4.2.6 Source-Zone Examples

Source Zone 1 (SCZ)

Substation Level with Access only for Certain Devices via Defined Protocols	
DMZ	File transfer from SICAM SCC to Remote Access Workstation over Internet
	SNMP from Substation Control Zone to Remote Access Workstation/Gateway

Source Zone 2 (DMZ)

With Access only for Certain Devices via Defined Protocols	
SCZ	RDP from Remote Access Workstation to SICAM SCC
	File transfer from Remote Access Workstation to SICAM SCC
	NTP from Remote Access Workstation to NTP Server in SCZ
EXT	Antivirus Pattern Update from Remote Access Workstation to EXT SCADA Anti-Virus Distribution Server

Source Zone 3 (EXT)

With Access only for Certain Devices via Defined Protocols	
SCZ	IEC 60870-5-104 from EXT SCADA to SICAM PAS in SCZ
DMZ	RDP from EXT SCADA RDP Client to Remote Access Workstation
	File Transfer from EXT SCADA File Service to Remote Access Workstation

Example

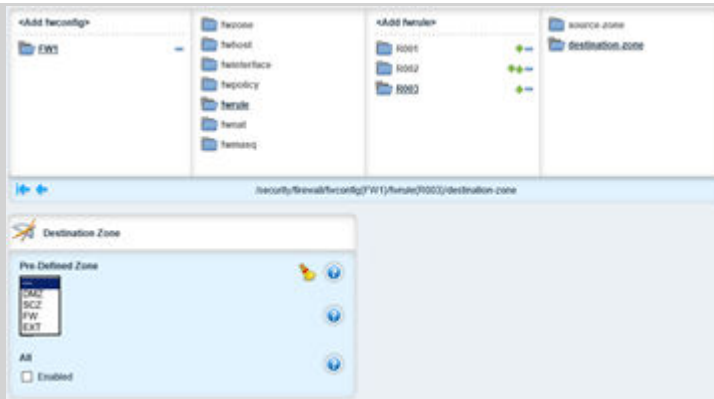
The aim of these rules is to allow the configuration of the router with IP e.g. 172.16.11.1 through the Service PC with IP e.g. 172.16.11.6 located in the DMZ. The source and destination zones must be defined as per the following table:

Table 2-4 Firewall-Rule Sample

Rule Name	Source Zone/Host	Destination Zone/Host
001	DMZ / 172.16.11.6	FW / 172.16.11.1

Additional options, such as Protocol (tcp/udp/all), destination Port (445), and the source Port (if known) should be configured to limit the possibility of access as much as possible.

The following figures illustrate where the source and destination zones are assigned.



[sc_Assigning source destination zones in a Ruggedcom Firewall, 1, en_US]

Figure 2-13 Assigning Source/Destination Zones in a RUGGEDCOM Firewall

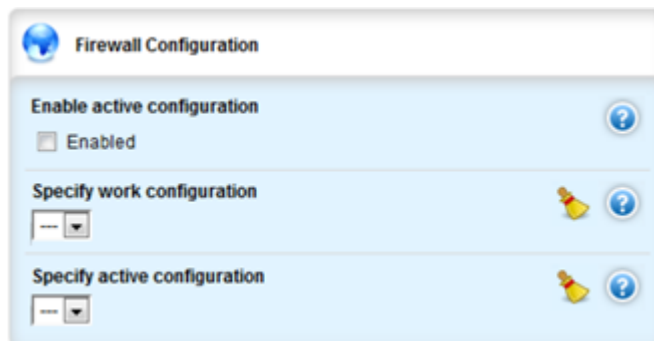
Rule Name	Action	Source Zone Hosts	Destination Zone Hosts	Log Level	Protocol	Source Port	Destination Port	
001	accept	172.16.11.6	172.16.11.1	none	tcp	1024:65535	445	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

[sc_A sample rule a Ruggedcom Firewall, 1, en_US]

Figure 2-14 A Sample Rule a Ruggedcom Firewall

2.4.2.7 Switching the Firewall ON

- ✧ To enable the Firewall, navigate to **Security** → **Firewall**.



[sc_Switching ON a Ruggedcom Firewall, 1, --]

Figure 2-15 Switching ON a RUGGEDCOM Firewall

- ✧ Check the **Enabled** check box in the **Enable active configuration** and select the configured FW e.g. FW1 for **Specify work configuration/Specify active configuration** and commit the change.

2.4.3 Maintenance

2.4.3.1 Export of the Configuration

To export the parameters from the router, the first step is to create the file in the router. This can be done via the main Web interface under **admin** as well as via the command line interface.

The following description uses the command set based on FW Version ROX 2.15.1.

Creating the File

- ✧ Go in the Web browser to the option **Tools** in the middle of the top menu CLI.
- ✧ From there, start the command-line editor (**Start**).

- ✧ Create a configuration file with the name **ConfRouter_yymmdd_hhmm.txt**.
- ✧ Type in **config** and press **Enter** to change to the configuration mode, e.g. **saveConfRouter_160108_1510.txt** and press **Enter**.

The following figure gives an idea how this step looks like.



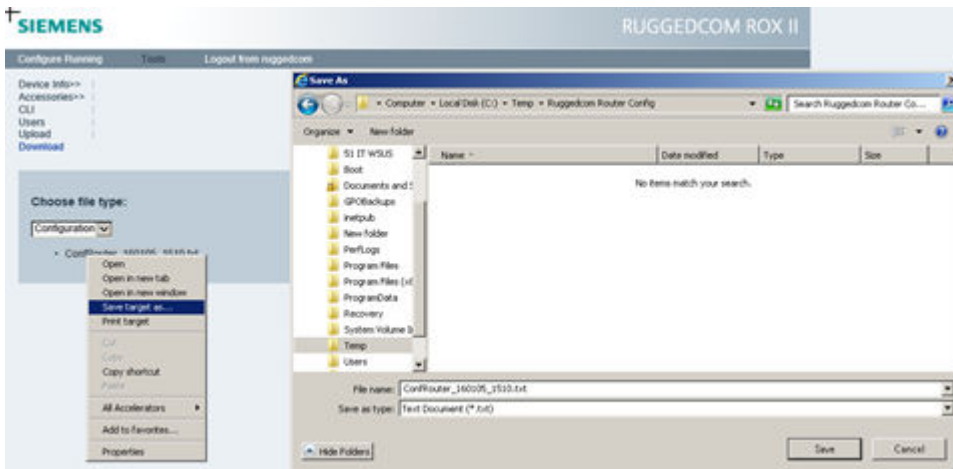
[sc_Exporting Configuration of a Ruggedcom Firewall, 1, en_US]

Figure 2-16 Exporting Configuration of a Ruggedcom Firewall

The file has been created and can be downloaded to a directory in the computer where the Internet browser is being used.

Downloading the File

- ✧ Go to the option **Download**, right-click the file, and click **Save target as...** to save it to the PC.



[sc_Saving Configuration of a Ruggedcom Firewall, 1, en_US]

Figure 2-17 Saving Configuration of a Ruggedcom Firewall

2.4.3.2 Adaptation of the Config File

The file downloaded in the previous step can be modified with an html/text editor (e.g. Notepad++.exe). The Structure of the Config File follows the Menu like the Web interface starting from left to the right. Modification to the configuration file can be done following this structure.

- ✧ To reduce the firewall loading time while committing changes, it is advised to make only needed changes and delete the rest of the parts in the file. This will keep the previous rule untouched.
For example, if only firewall rules are to be modified, delete all entries above **security** and below the latest rule set.

- ◇ After the latest rule set, close each menu that was moved up to the Rules via exclamation mark as shown in the following figure.

```
1 config private
2 security
3   firewall
4     FWConfig FW1
5       fwrule R001
6         action accept
7         source-zone all
8         destination-zone all
9         protocol icmp
10        description "icmp all"
11       !
12      fwrule R002
13        action                accept
14        source-zone DME
15        source-zone-hosts    172.16.11.6
16        destination-zone FW
17        destination-zone-hosts 172.16.11.1
18        protocol             tcp
19        source-ports         1024:65535
20        destination-ports    443
21        description          "Web Interface Routers"
22       !
23      fwrule R003
24        action                accept
25        source-zone EXT
26        source-zone-hosts    10.1.10.41
27        destination-zone SCZ
28        destination-zone-hosts 172.16.21.11
29        protocol             udp
30        source-ports         123
31        destination-ports    123
32        description          "NTP connection to customer master clock"
33       !
34     !
35   !
36 !
37 commit
38 abort
```

[sc_Editing a configuration file, 1, en_US]

Figure 2-18 Editing a Configuration File

2.4.3.3 Uploading and Activating a Manually Modified Config File

Uploading the Config File to a Router

The uploading of the configuration file in a router can be performed through the following steps:

- ◇ In the Web interface, go to **Tools** in the top menu and **Upload**.
- ◇ Select the type of file **Configuration**, click **Browse...**, and select the corresponding file, e.g. **ScriptRules150108ScriptRulesExample.txt**.
- ◇ Click **Send** to load the file in the router.



[sc_Importing a Configuration file in a Ruggedcom Firewall, 1, en_US]

Figure 2-19 Importing a Configuration File in a Ruggedcom Firewall

Activating the Config File

Once the file has been uploaded into the router, it can be activated.

- ✧ Go back to **Tools** and **CLI**.
- ✧ Start the line editor (**Start**), type **config** and **Source ScriptRulesExample.txt**, and press **Enter**. (The load of changes must be ready in less than one minute!)



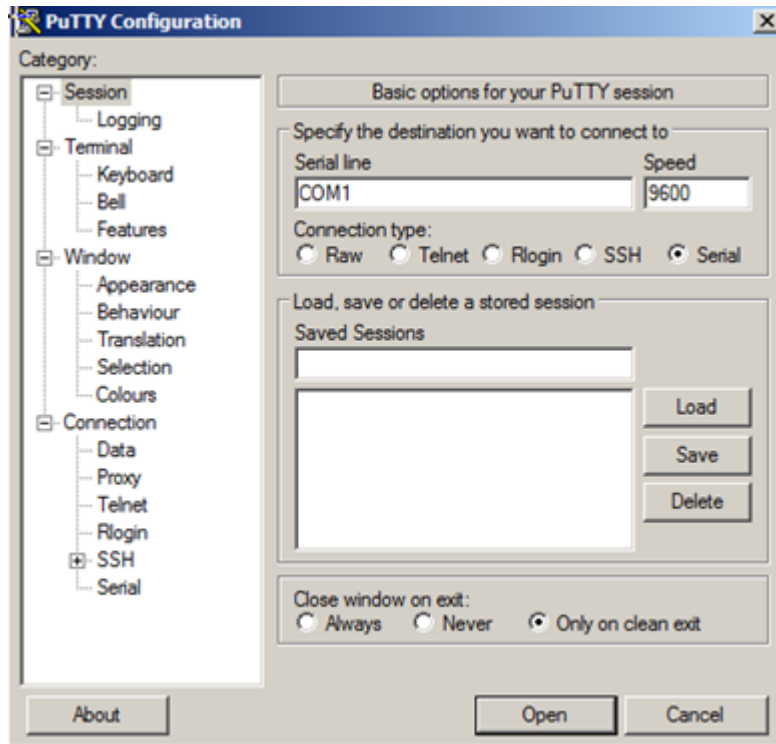
NOTE

If a complete configuration needs to be loaded, use **overwrite** instead of **merge**.

2.4.4 Blocked Access Due to FW Config Mistakes

It can happen that by mistakes, wrong firewall-rule settings were applied during the configuration load up which could block the access to the Web Interface of the router. Alternatively, the firewall can get switched off via the serial interface.

- ✧ To resolve this, connect a PC via a serial straight cable to the serial front port of the RX1500 and start a serial console session via Hyper Terminal or Putty (third-party tool).



[sc_Connecting a Ruggedcom Firewall using Serial port, 1, en_US]

Figure 2-20 Connecting a Ruggedcom Firewall Using Serial Port

✧ Via a Terminal, set up the Com Port speed to 57.6 kbps and the connection type as **serial**.

Configure the terminal as follows:

- 57 000 bps
- No parity
- 8 bits
- Set the terminal type to VT100
- Disable hardware and software flow control

✧ Start a new console session and login to the RX1500 via Login User with PW (default admin/admin).

✧ Navigate to the FW configuration by using the following commands:
ruggedcom# → Config → security → firewall

Now, **ruggedcom(config-firewall)#** should be reached.

✧ Enable the firewall by typing:
security firewall enable

- or -

✧ Disable the firewall by using the **no** version of the command:
no security firewall enable

✧ Type **commit** and press **Enter** to save the changes.

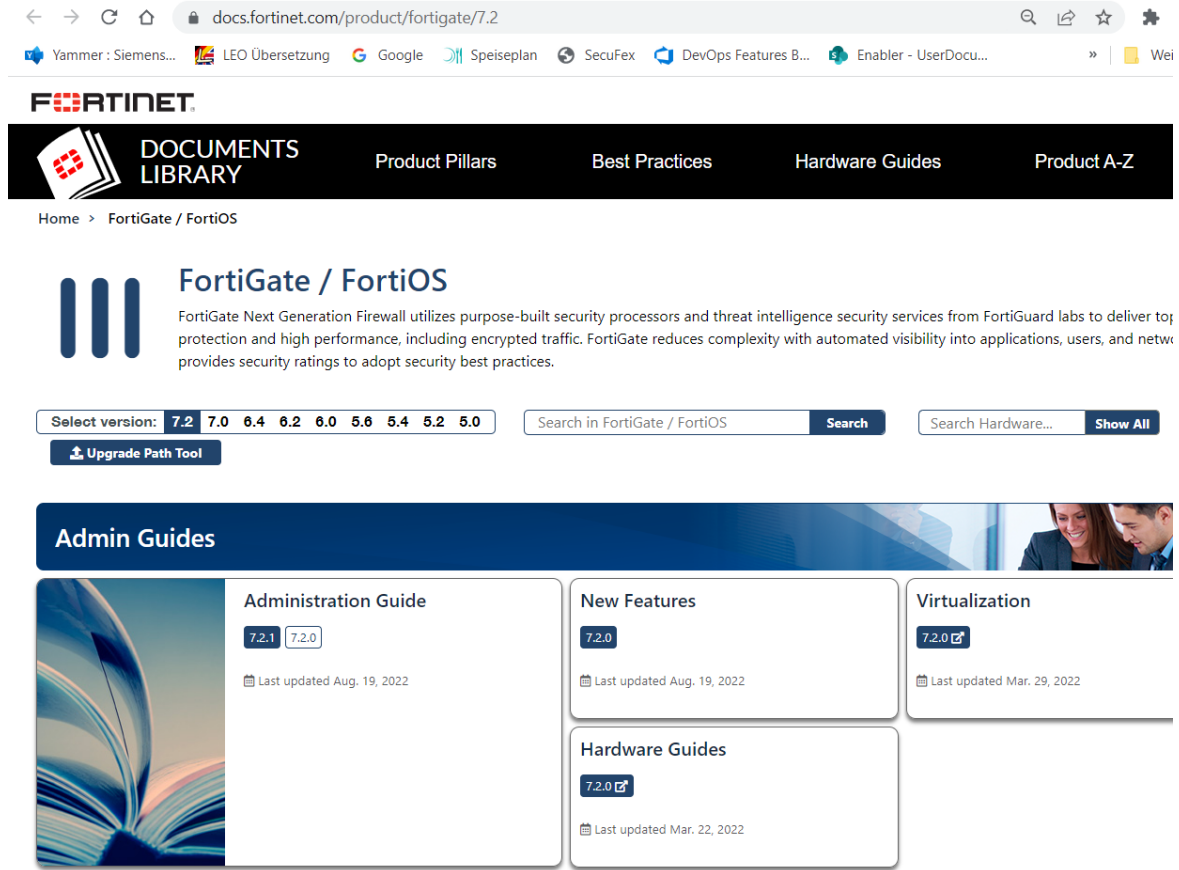
- or -

✧ Type **revert** and press **Enter** to cancel.

2.5 Fortigate Firewall

2.5.1 Introduction

As an alternate to the RUGGEDCOM firewall, Siemens recommends the use of the FortiGate firewall. The following section describes setting up a FortiGate firewall. For detailed documentation about the FortiGate firewall refer to <https://docs.fortinet.com/product/fortigate/>.

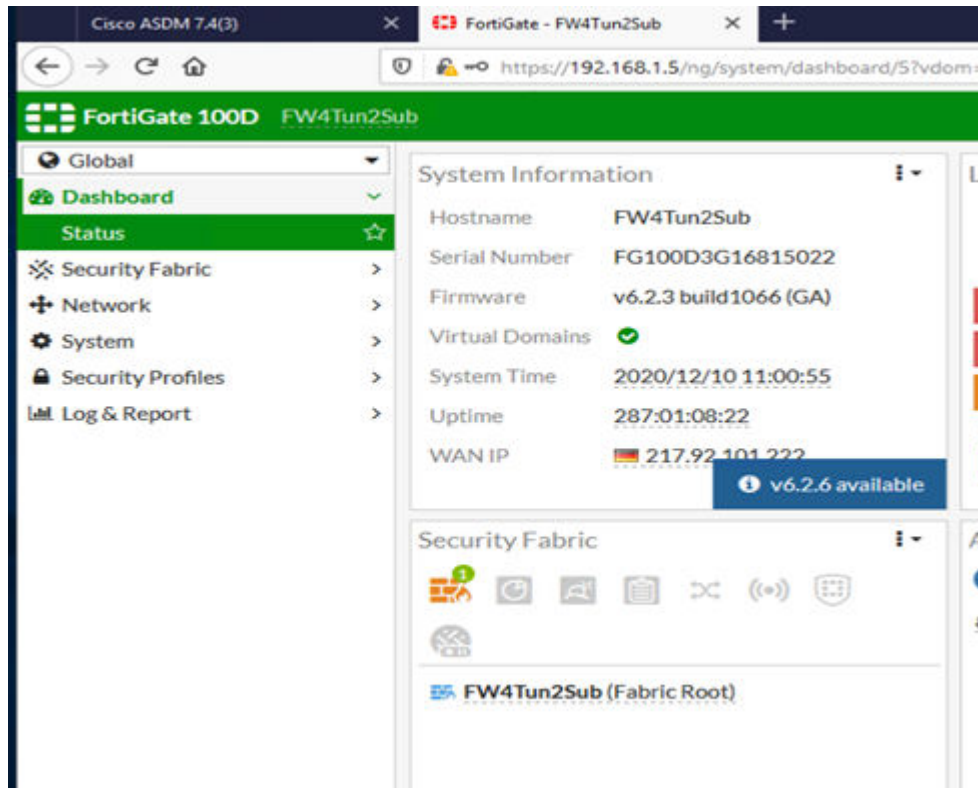


[sc_Fortigate Firewall Web-interface, 2, en_US]

Figure 2-21 Fortigate Firewall Web Interface

2.5.2 Fortigate Firewall Network Configuration

The firewall interface can be accessed via logging in into the Web interface of the management interface. The logged-in interface shows the Global System. The global configuration parameters and the virtual Domains (VDOM) can be configured here. Virtual domains (VDOMs) are a method of dividing a Fortigate unit into 2 or more virtual units that function as multiple independent units. VDOMs can provide separate firewall policies and, in NAT/Route mode, completely separate configurations for routing and VPN services for each connected network or organization



[sc_FortiGate web site after the login, 1, en_US]

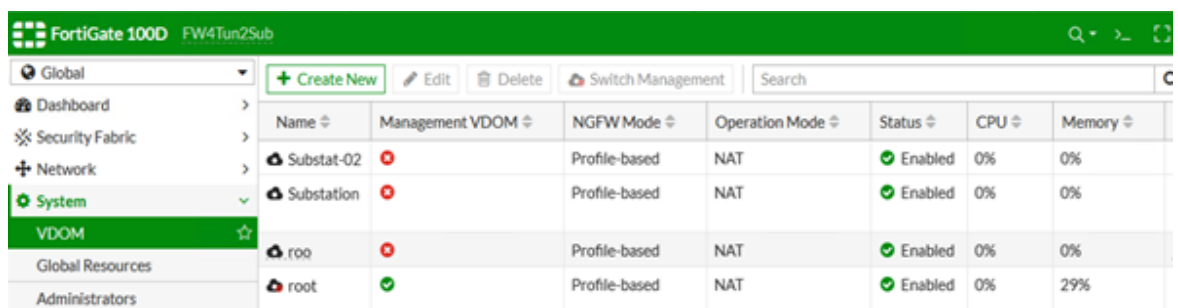
Figure 2-22 FortiGate Web Site After the Login

The VDOM can be created at the System-Menu using VDOM subsection as shown below. The **Create New** function creates new VDOM for example Substat-02 (Figure 2-23).



NOTE

The name of Virtual Domain (VDOM) is restricted to 11 letters.



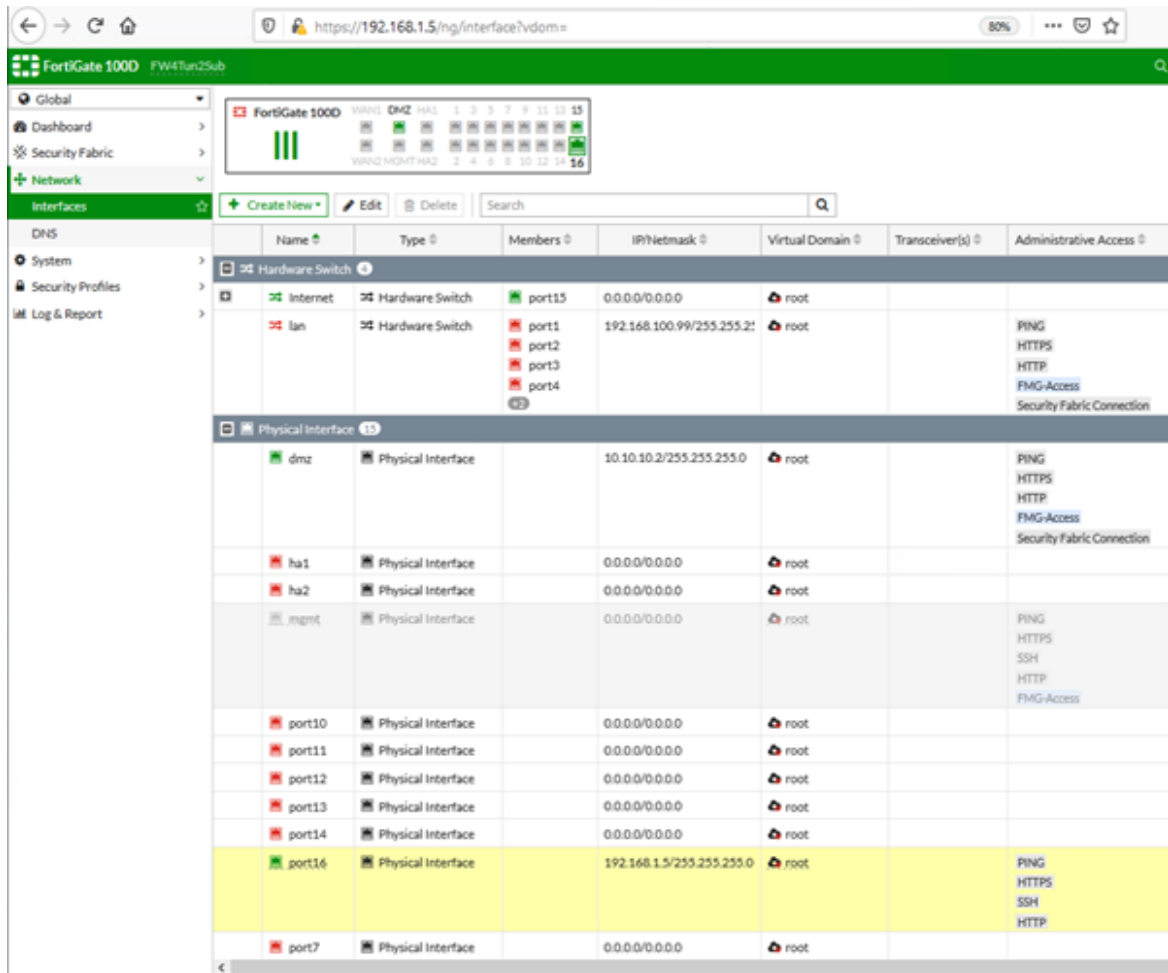
[sc_At the System Menu you find the VDOM sub chapter to create a new VDOM, 1, en_US]

Figure 2-23 At the System Menu you find the VDOM Sub Chapter to Create a New VDOM

2.5.3 Setup of the Network for the Substat-02 Virtual Domain (VDOM)

✧ To assign an interface to a VDOM, select the **GLOBAL** system and select the **Network** menu.

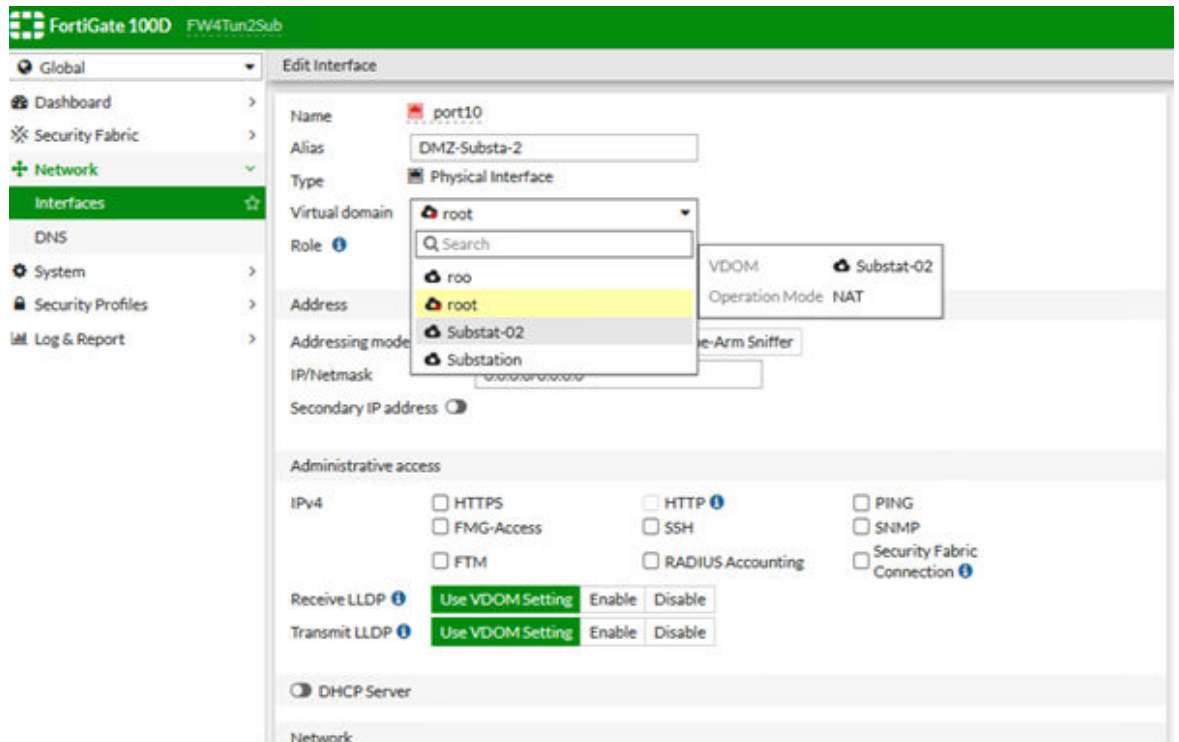
The **Interfaces** subsection shows all physical network interfaces to which each VDOM (Virtual Domain) belongs to.



[sc_Interface List in the Network Menu of the GLOBAL system of the FortiGate Firewall, 1, en_US]

Figure 2-24 Interface List in the Network Menu of the GLOBAL System of the FortiGate Firewall

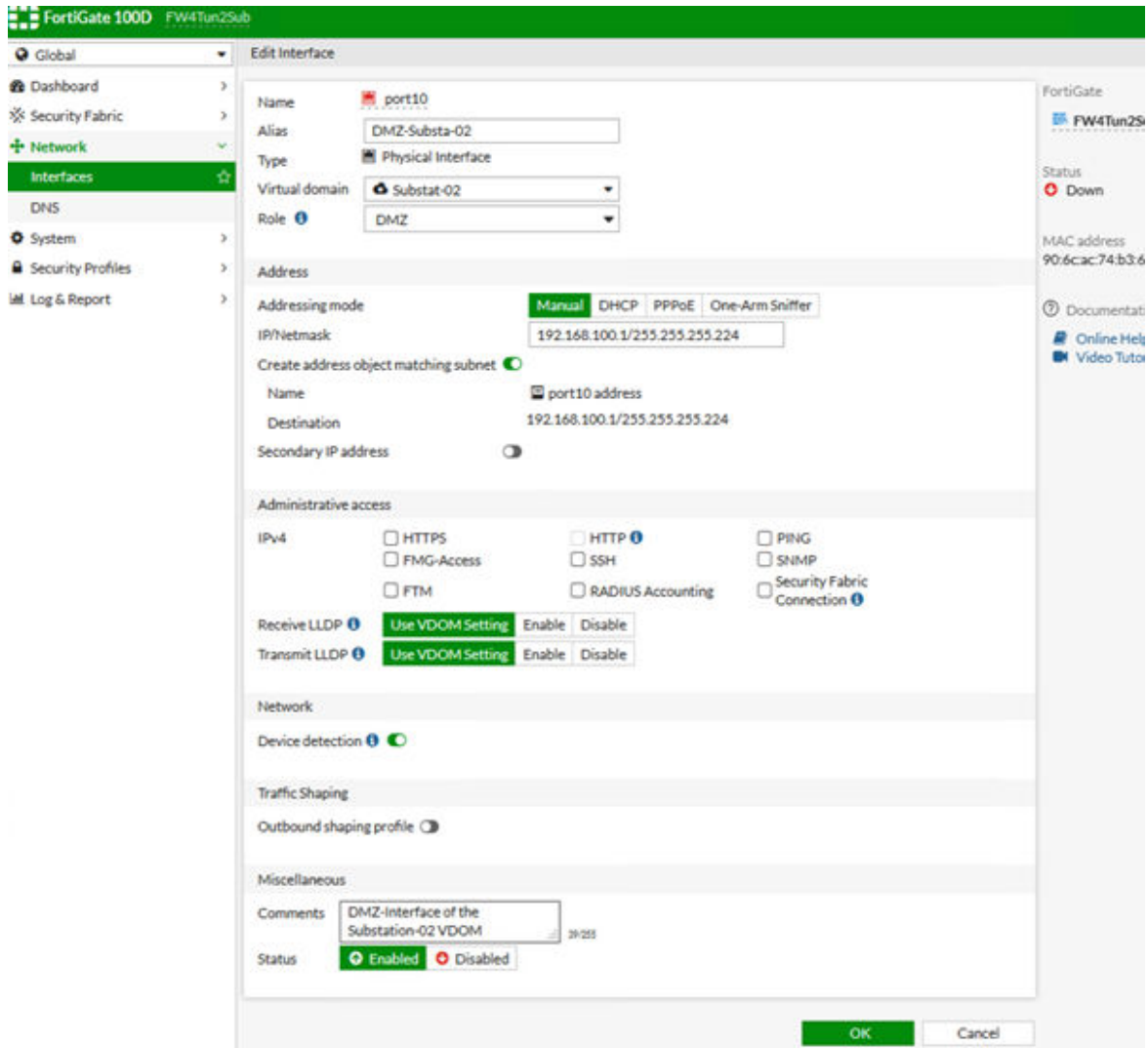
- ✧ Select the interface needed to **move** between the VDOMs, for example, port 10, and double-click. The Edit Interface function opens the interface menu.
- ✧ Select the VDOM defined before.



[sc_Interface Menu to setup the VDOM and Role any other important interface attribute, 1, en_US]

Figure 2-25 Interface Menu to Setup the VDOM and Role any Other Important Interface Attribute

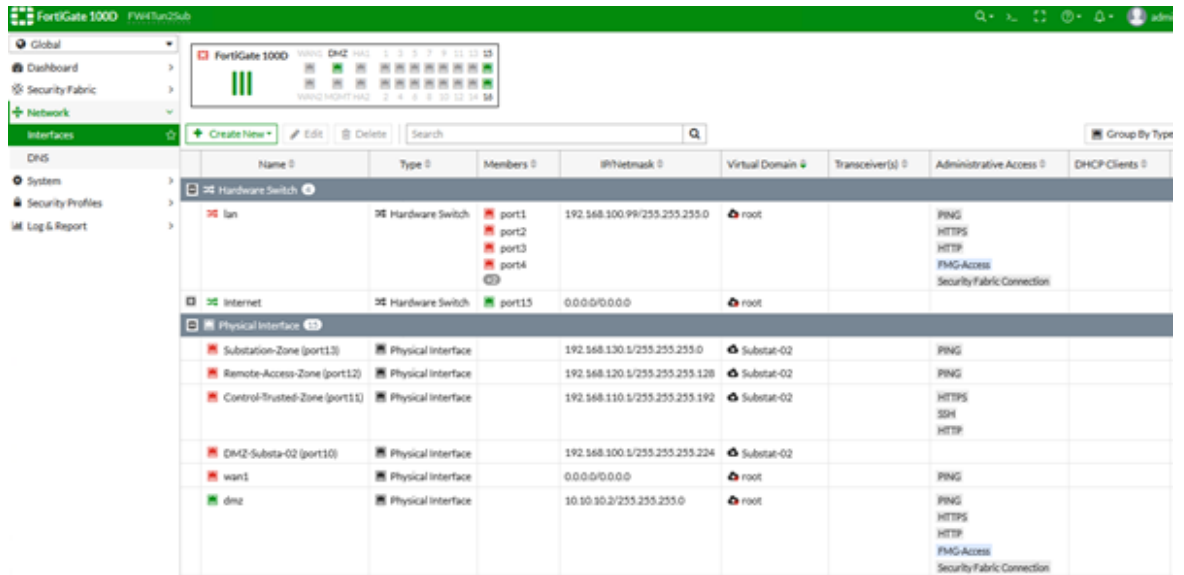
- ✧ If the port is used for the DMZ interface (as in this example), then the role should be DMZ because you want to use port 10 as a DMZ interface (see the following figure) additionally to the DMZ interface given by the Fortigate System Port.
For all the other zone interfaces like Control/Trust zone, Substation zone, or Remote access, **LAN** should be selected as role.



[sc_Interface Attributes of the DMZ-Interface of the VDOM Substat-02, 1, en_US]

Figure 2-26 Interface Menu to Setup the VDOM and Role any other Important Interface Attribute

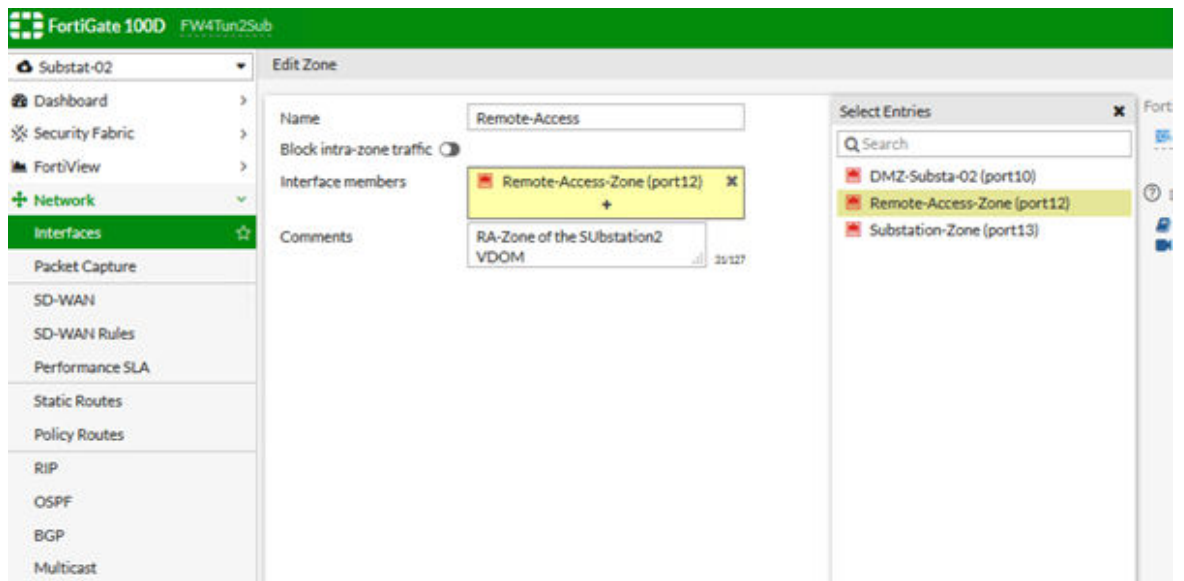
- ✧ The other attributes of the interface can be selected based on the requirements. All the configured interfaces can be seen like the following list of the interfaces in the Network Menu:



[sc_List of the Zone interfaces of the VDOM Substat-02, 1, en_US]

Figure 2-27 List of the Zone Interfaces of the VDOM Substat-02

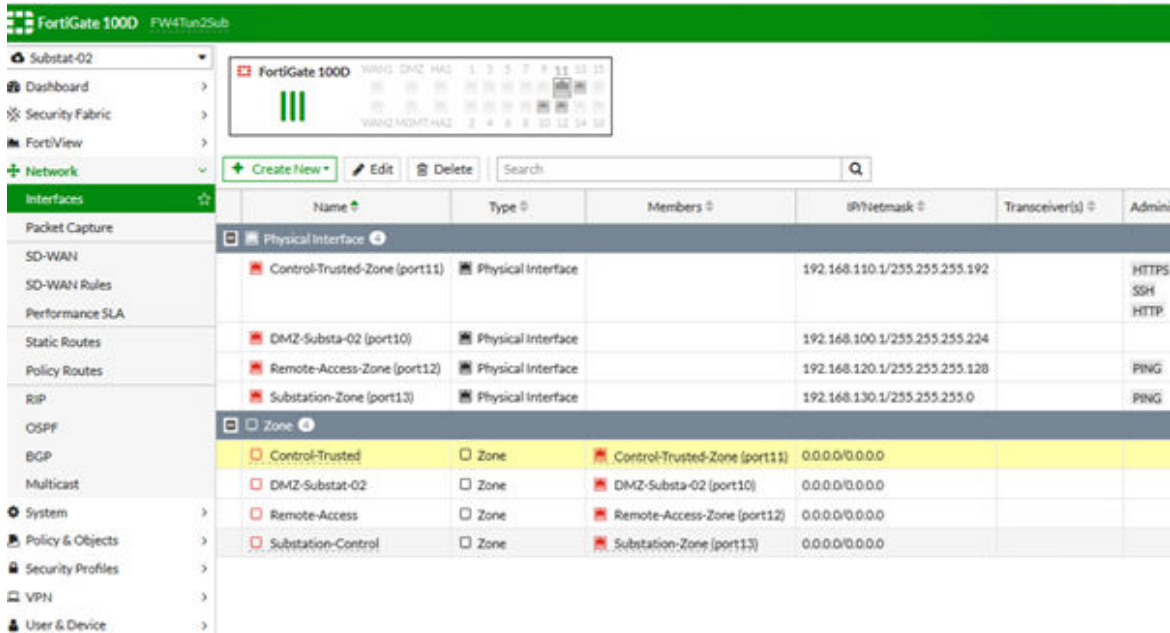
- ✧ After the definition of the interfaces, change to VDOM Substat-02 and go to the Network and Interfaces subsection. Link them together by double-clicking the zone. The Zone menu appears. Select the interface member for the zone:



[sc_Add the interface to the Zone, 1, en_US]

Figure 2-28 Add the Interface to the Zone

- ✧ After assigning the interface members you will get the following list as a result:



[sc_Interfaces and Zones of the Substat-02 VDOM, 1_en_US]
 Figure 2-29 Interfaces and Zones of VDOM Substat-02

2.5.4 Setup Firewall Rules in VDOM

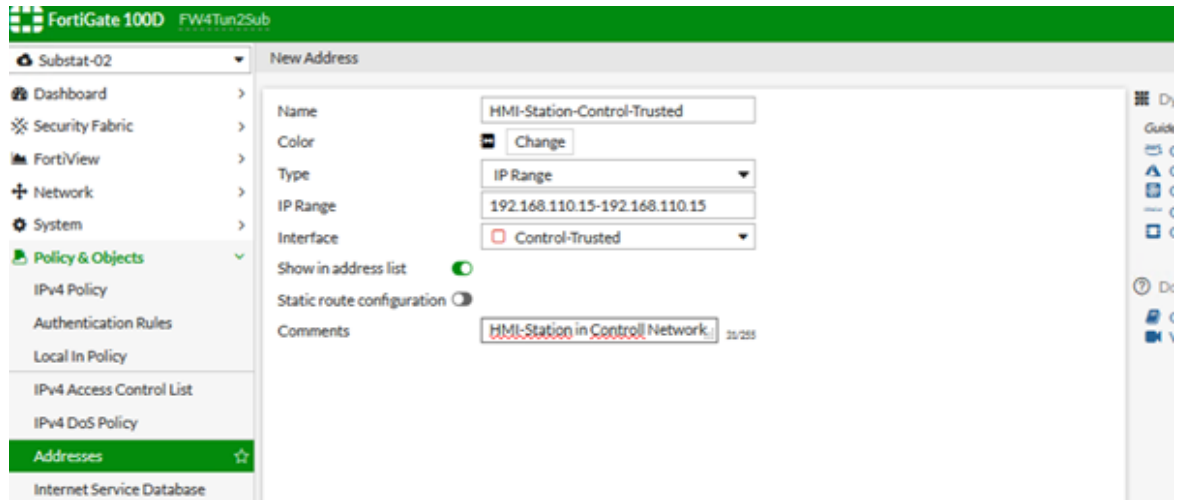
In the following section FortiGate configuration based on the Secure Blueprint Architecture is explained. The communication is established for:

- Engineering Station/Service PC (ES) in DMZ to Web HMI system in the Control Center
- Remote Host in Remote Zone to Engineering Station in the DMZ

2.5.4.1 Example 1: Engineering Station (ES) in DMZ to Web HMI system in the Control Center

The following configuration is used for this example:

- Engineering Station in DMZ: IP 192.168.100.10
- Communication Type: TCP HTTPS Port 445
- HMI in Control Zone IP 192.168.110.15
- ✧ Set up the address objects: At **Policy & Objects** define the address object for the Engineering Station and for the HMI Station.



[sc: Definition of the HMI-Address-Object, 1, en_US]

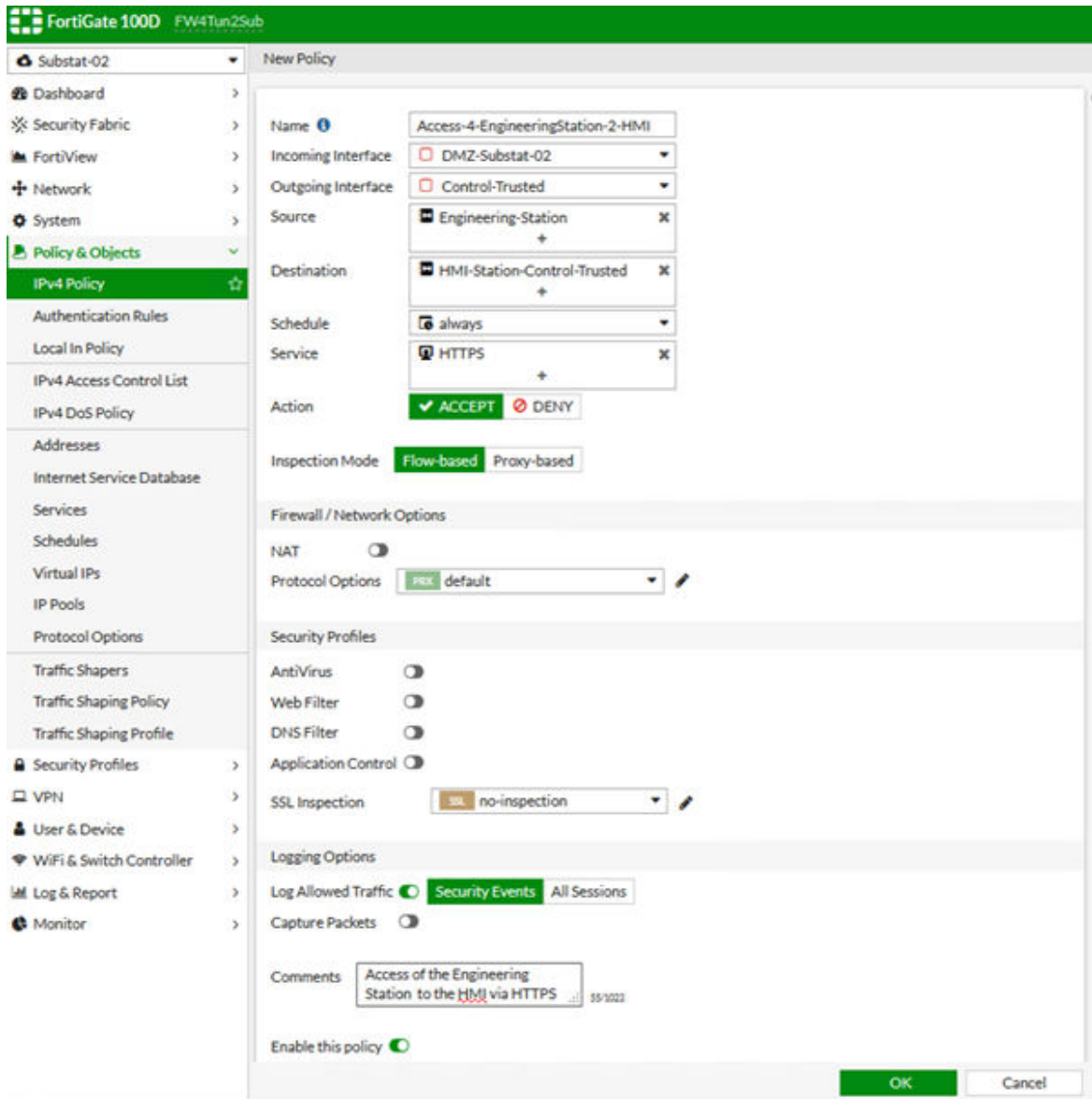
Figure 2-30 Definition of the HMI-Address-Object



NOTE

About object naming: Address objects can be networks, interfaces of Firewall, or network nodes with more than one interface. A good practice to name i.e. a host is to add the zone or the zone-name abbreviation with it so HMI-Station-Control-Trusted or shorter HMI-Station-CT or Engineering-Station-dmz.

✧ Define the rule:



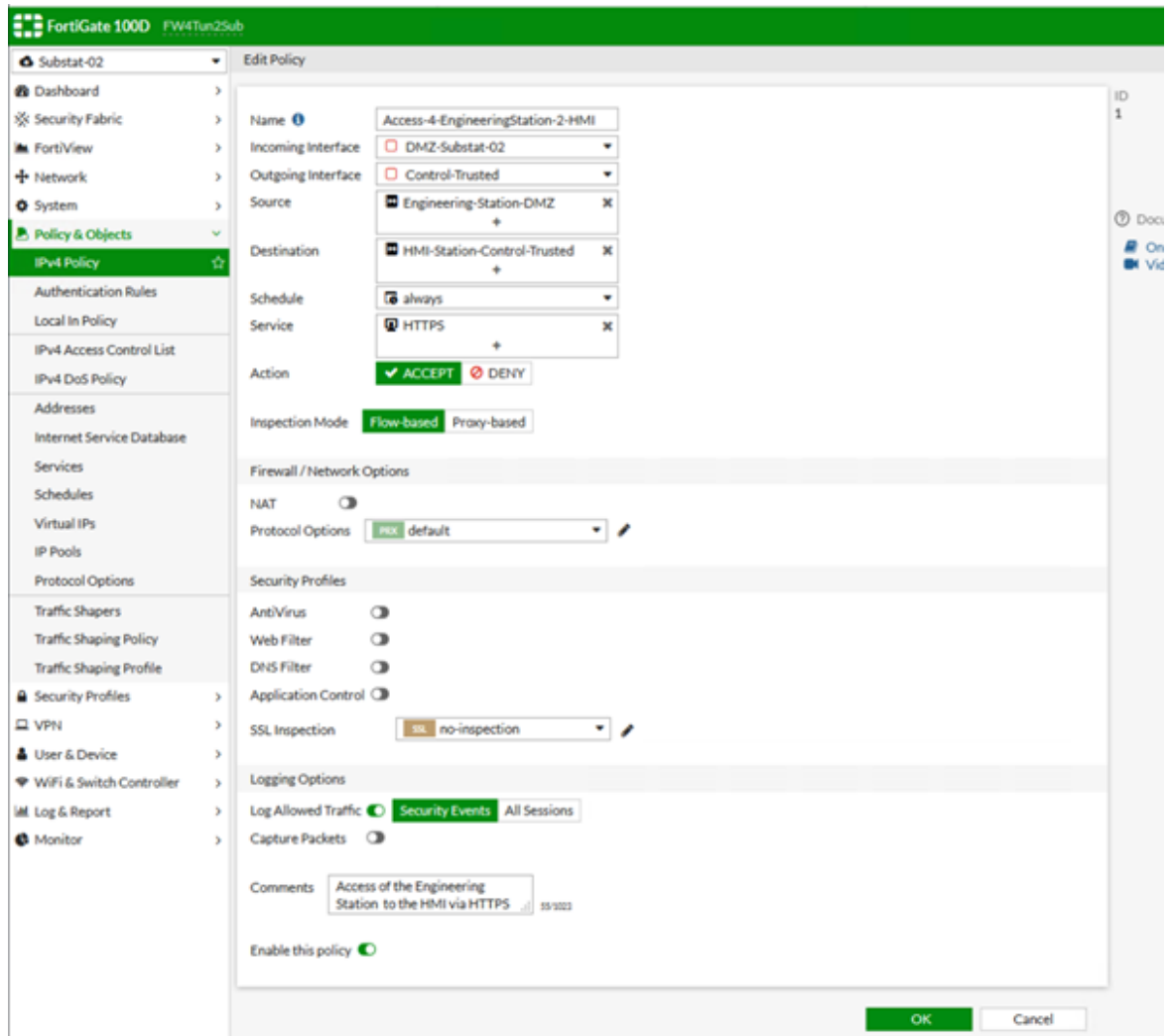
[sc_Rule setup for a connection between Engineering Station and HMI Station, 1, en_US]

Figure 2-31 Rule Setup for a Connection Between Engineering Station and HMI Station

2.5.4.2 Remote Host in Remote Zone to Engineering Station in the DMZ

The following configuration is used for this example:

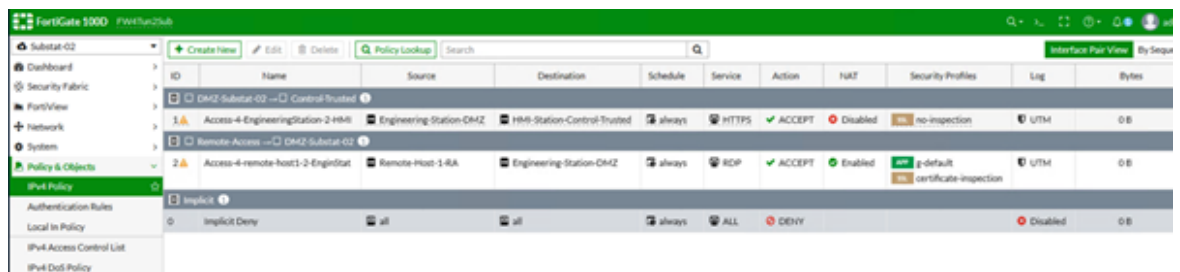
- Remote host in the remote access zone: IP 192.168.120.10
 - Communication type: TCP RDP Port 3389
 - Engineering station in DMZ: IP 192.168.100.10
- ◇ Define the address objects.
- ◇ Set up the rule.



[sc_Second Rule definition, 1, en_US]

Figure 2-32 Second Rule Definition

The 2 firewall example rules created can be seen in the **IP4 Policy** subsection of the **Policy & Object** menu.



[sc_The first two Rules of the firewall, 1, en_US]

Figure 2-33 The First two Rules of the firewall

The substation environment is more complex and has more rules which keep increasing based on the requirements. It is recommended that all the rules should have a **speaking comment** giving at least the information between what nodes and why or who has made this requirement. This allows to trace back why the rule was configured.

2.5.4.3 Additional Information on the Fortigate Firewall

The Fortigate firewall is a very powerful network component and contains not only the firewall rule engine, but also an Intrusion Detection System (IDS). This allows deep packet inspection for the traffic from VPN or other applications. Enabling the IDS helps in detecting threats as well as troubleshooting the network.

2.5.4.4 Recommendations

A typical firewall controls traffic based on rules which are mapped to port numbers, IP addresses, and instruction to deny or allow the traffic. An Intrusion Detection System (IDS) on the other side looks deep into the network traffic to alert intrusions inside the network. Firewalls limit access between networks to prevent intrusion and do not signal an attack from the allowed network. An IDS describes a suspected intrusion once it has taken place and signals an alarm. An IDS also watches for attacks that originate from within a system. This is traditionally achieved by examining network communications, identifying heuristics and patterns (often known as signatures) of common computer attacks, and alerting operators.

Table 2-5 IDS Versus Firewall

IDS	Firewall
Remote Desktop	RDP
Located inside a network	Located at a border of a network
Evaluate complete traffic	Filters in and outgoing traffic
Does not block connections	Block connections
Report suspicious traffic	Can Report blocked packages only

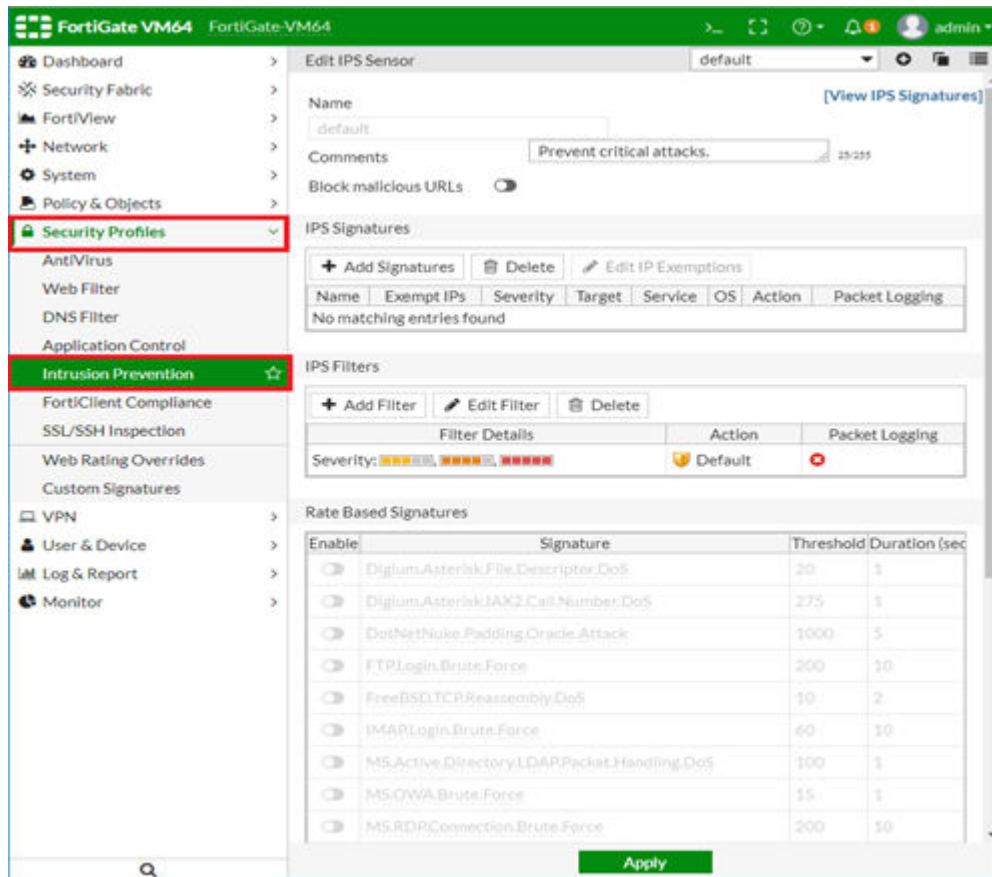
Fortigate: Firewall with Intrusion Detection System

Siemens recommends using the Fortigate firewall to achieve the IDS within a Substation Energy Automation System. It is recommended to configure Fortigate in **detection** mode only, so that it cannot block legitimate traffic. In general, signatures should not be set to block in this mode.

The first step to configure the IDS in the Fortigate firewall is to create an IPv4 policy. This policy includes the IP addresses for which the traffic is allowed in the firewall.

The Intrusion Detection in the Fortigate is achieved using the IPS functionality in **Monitor only** mode.

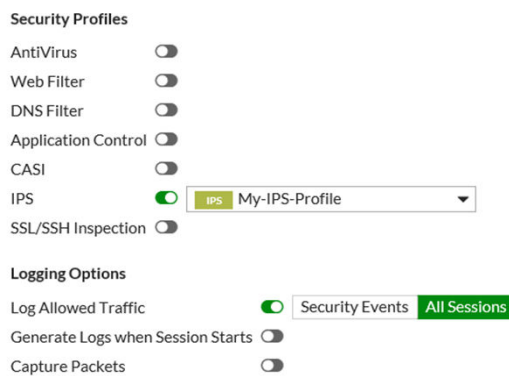
- ✧ Navigate to **Security Profiles** → **Intrusion Prevention** and click + to create a new IPS profile.
- ✧ Edit the new security profile and click + **Add Filter**.
- ✧ Select **All Severities**, as shown in the screenshot and set the **Action** to **Monitor**. Do not enable Packet logging.



[sc_Configuring IDS in FortiGate Firewall, 1, en_US]

Figure 2-34 Configuring IDS in FortiGate Firewall

✧ As a next step, enable the IPS Profile for the IPv4 Policy, as shown in the following figure. Accept the changes by clicking **OK**.



[sc_Enabling IDS in Fortigate Firewall, 1, en_US]

Figure 2-35 Enabling IDS in Fortigate Firewall

The Intrusion Detection System is now active.

2.6 IP Communication with the IEC 62351

2.6.1 Fulfilling the IEC 62351-3

The scope of the IEC 62351 standards is information security for power system control operations. IEC 62351-3 specifies how to provide the following for SCADA and telecontrol protocols that use TCP/IP as a transport layer:

- Confidentiality
- Tamper detection
- Message level authentication

IEC 62351-3 specifies how to secure TCP/IP-based protocols through constraints on the specification of the messages, procedures, and algorithms of Transport Layer Security (TLS) (defined in RFC 5246 for TLS 1.2) so that they are applicable to the telecontrol environment of IEC TC57

As recommended in the IEC 62351 standard, this solution also uses the following:

- X.509 certificates
- A Certifying Authority environment
- TLS authentication and encryption

SICAM PAS has an IEC 62351-3/-5 and IEC 60870-5-7 conform implementation via Security Add-on package for the TCP protocols DNP3 and IEC 60870-5-104. The SICAM 230 as a legacy product as also older versions of SICAM SCC are extensible to support IEC 62351-3 for IEC 60870-5-104.

2.6.2 Fulfilling the IEC 62351-4

IEC 62351-4 applies to IEC 61850 MMS (Manufacturing Message Specification) Servers and Clients at the Substation automation and protection levels. Currently, IEC 61850 MMS communication between SICAM PAS Software Application and SICAM A8000 RTUs can be secured using the Transport Layer Security (TLS 1.2).

2.6.3 Fulfilling the IEC 62351-5

IEC 62351-5 applies to IEC 60870-5 and DNP3 derivatives. SICAM PAS supports the first edition of IEC 62351-5 for DNP3 TCP master and slave as well as IEC 60870-5-104 master and slave using TLS 1.2. SICAM A8000 supports the DNP3 slave and IEC 60870-5-104 slave using TLS 1.2.

2.6.4 Fulfilling the IEC 62351-9

IEC 62351-9 refers to the cybersecurity key management for power-system equipment. SICAM GridPass is the Siemens solution to manage the cryptographic key within the substation control system. It allows to create, maintain, and revoke the cryptographic keys.

2.6.5 Use Case: Securing Communication using IEC 60870-5-104

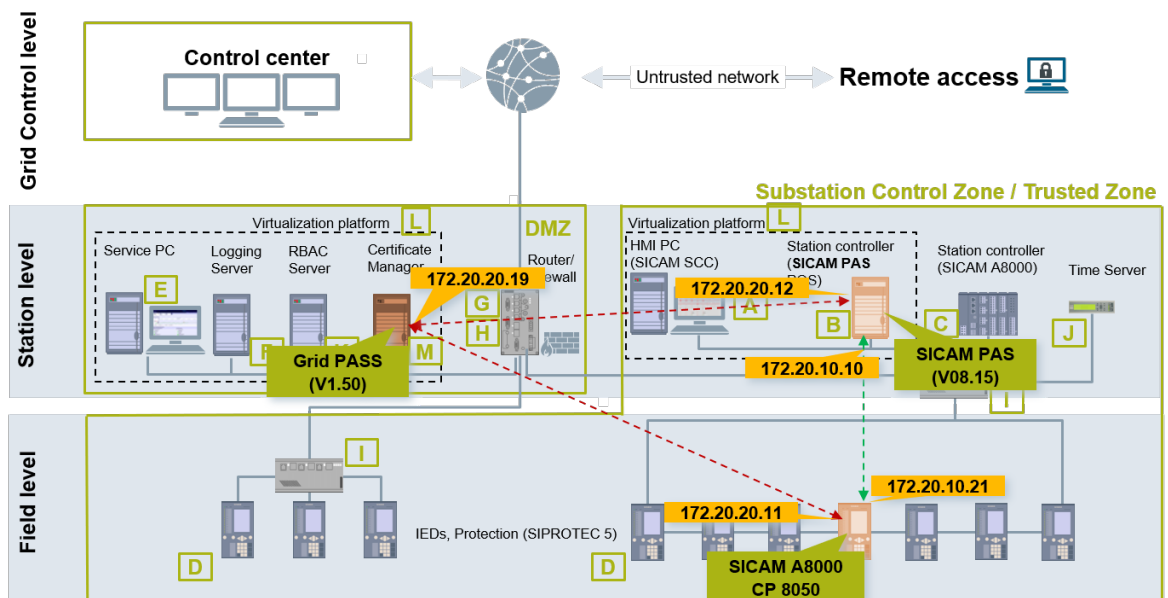
The following configuration shows how the SICAM GridPass generated certificate is used to secure communication between SICAM PAS and SICAM A8000 CP 8050.

The example explains:

- How to generate the certificate in SICAM GridPass placed in DMZ
- How to import the certificate in SICAM PAS and CP8050
- How to encrypt the communication using the certificates

2.6.5.1 Preconditions

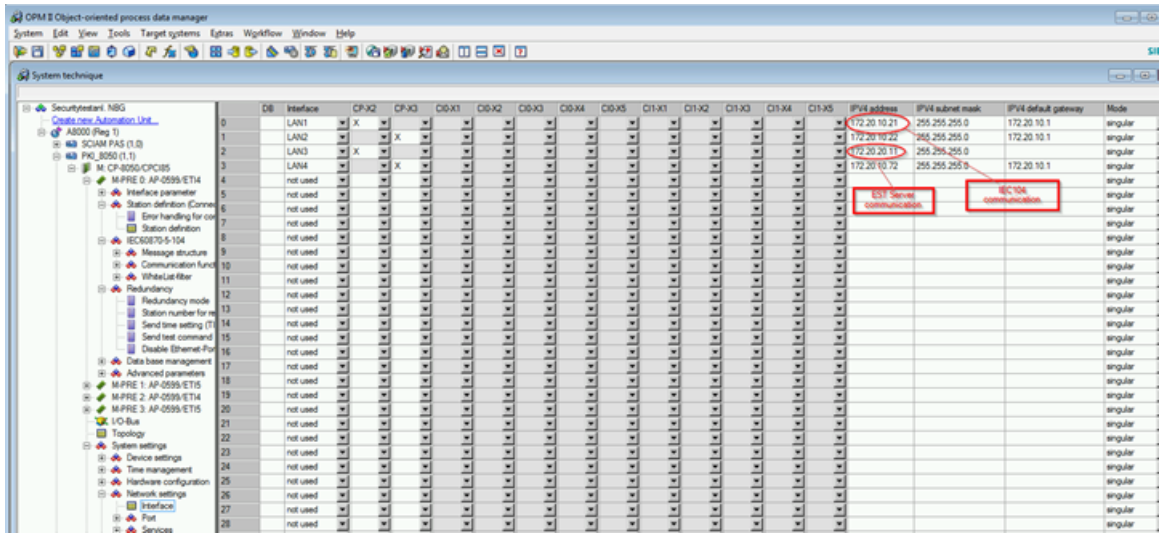
- SICAM PAS V08.15 or later, GridPass V1.50 or later are used.
- CA and client certificates for EST communication are created in GridPass.
- Certificates for TLS communication are generated by GridPass.
- SICAM A8000 CP8050 delivers a current I2 value to SICAM PAS via IEC 104 communication protocol.
- The following IP addresses were given in the example: Broadcast is 255.255.255.0 in both networks:
 - GridPass for EST communication: 172.20.20.19
 - Sicam PAS for EST communication: 172.20.20.12
 - CP8050 for EST communication: 172.20.20.11
 - Sicam PAS for IEC104 communication: 172.20.10.10
 - CP8050 for IEC104 communication: 172.20.10.21



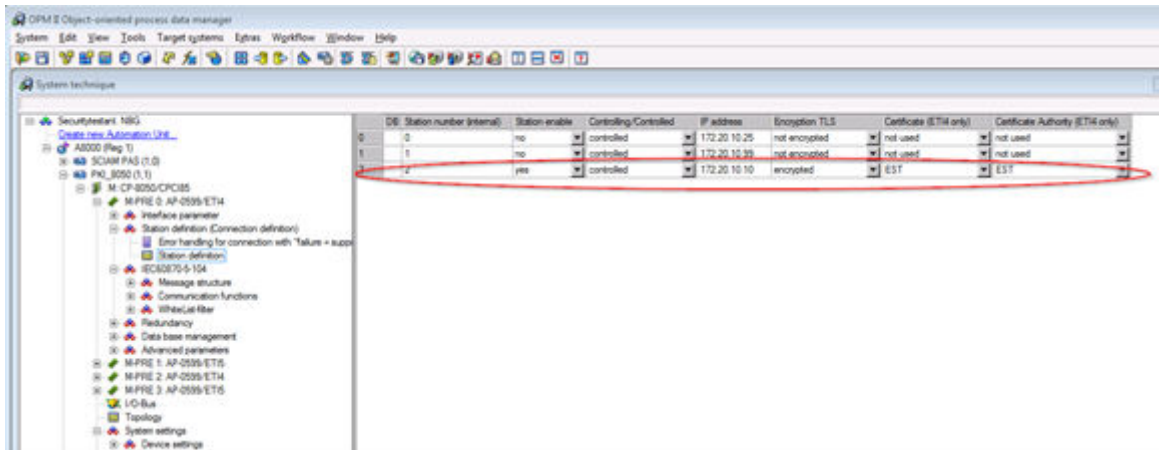
[sc_Use Case_Securing Communication using IEC 60870-5-104_1_en_US]

Figure 2-36 Use Case: Securing Communication using IEC 60870-5-104

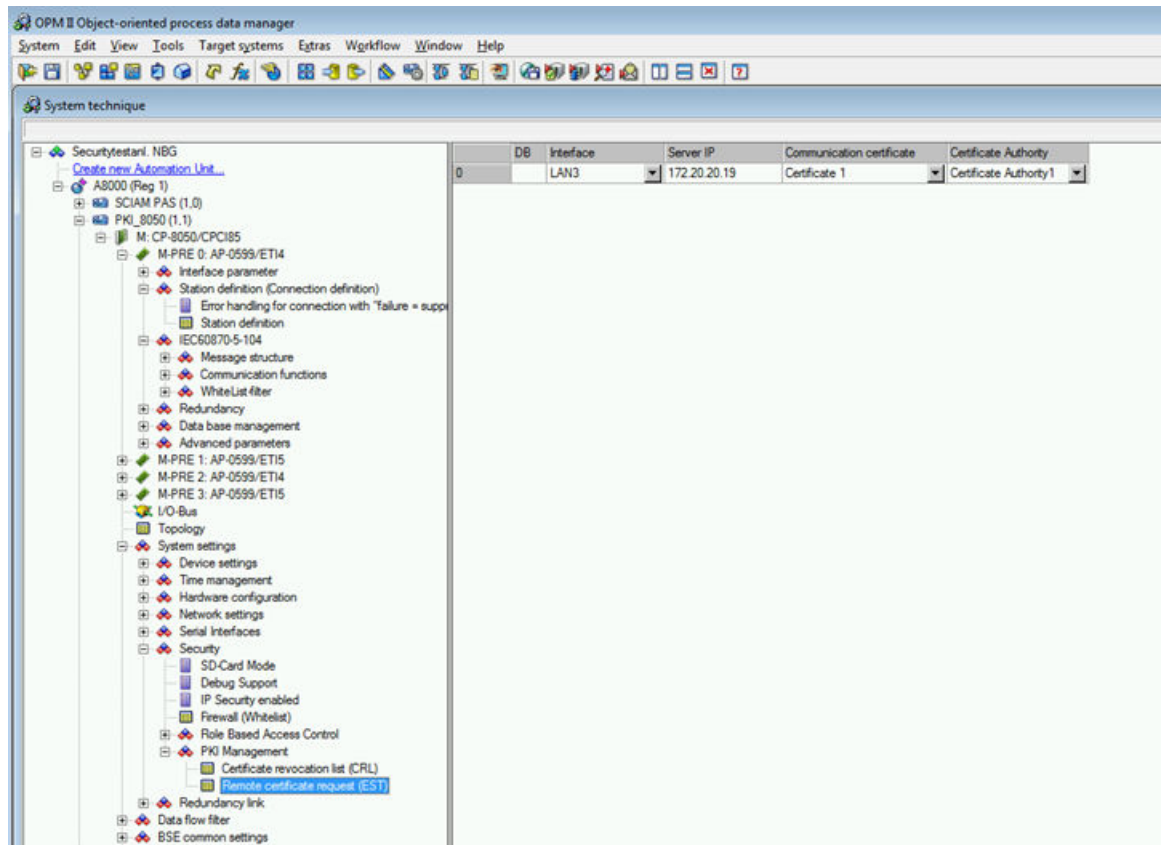
2.6.5.2 Configuration of CP8050 for IEC 104 TLS Communication in Toolbox



[sc_Network settings-Interface, 1, en_US]
 Figure 2-37 Network settings → Interface

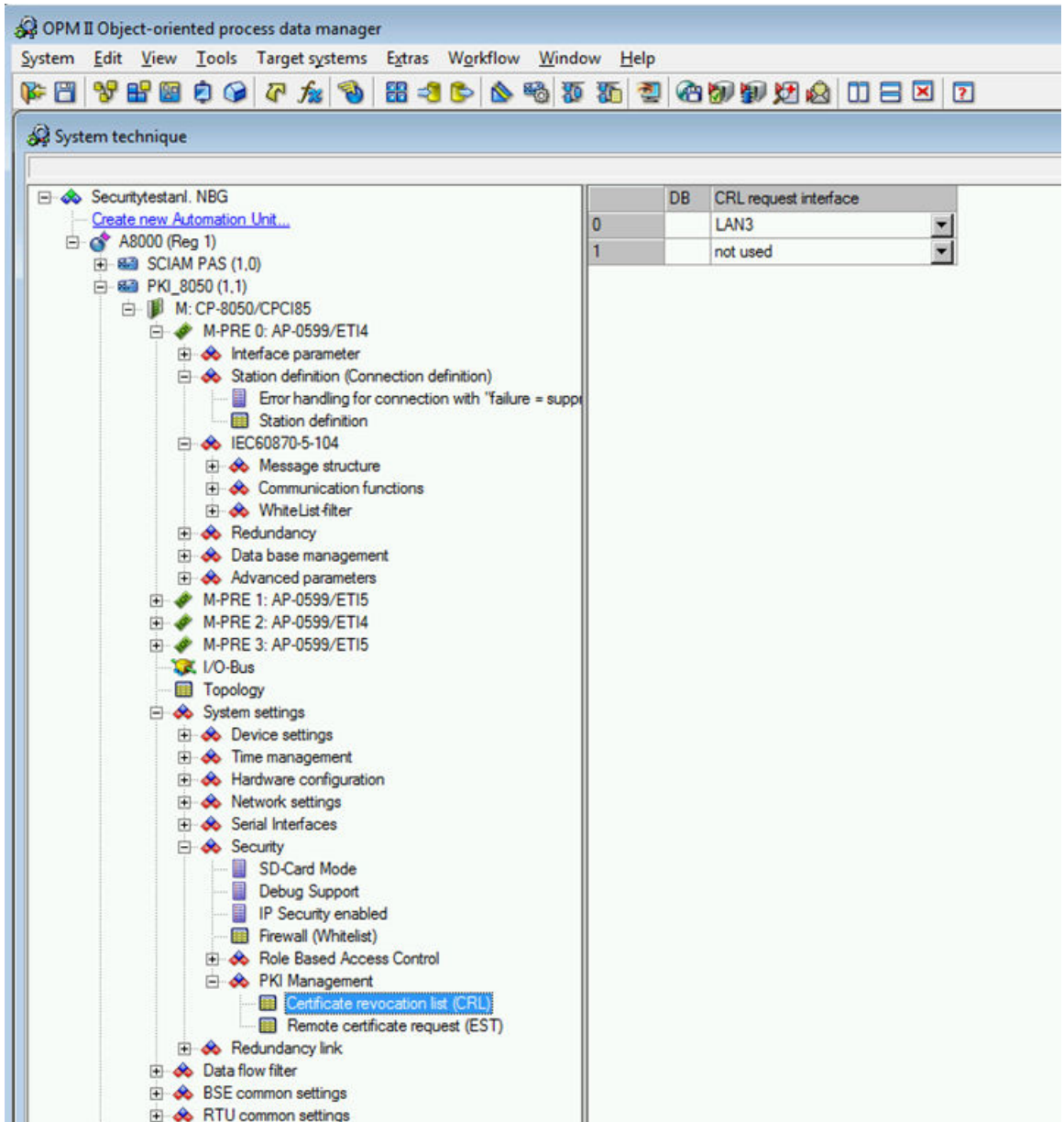


[sc_Station definition for TLS communication, 1, en_US]
 Figure 2-38 Station Definition for TLS Communication



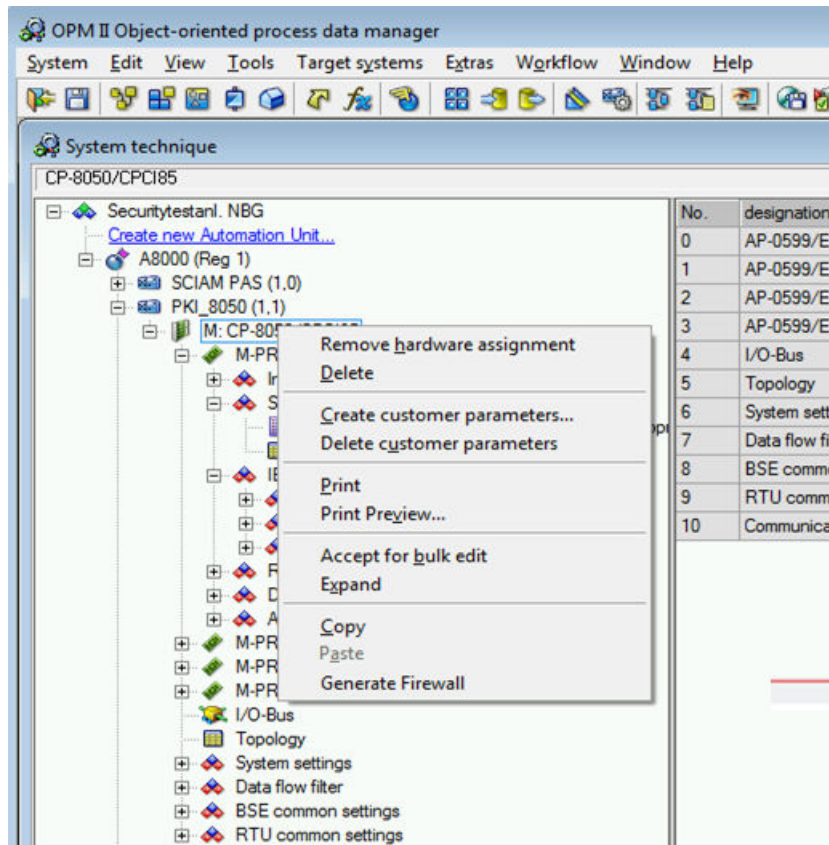
[sc_System Settings-Security-PKI Management-Remote certificate request EST, 1, en_US]

Figure 2-39 System Settings → Security → PKI Management → Remote Certificate Request EST



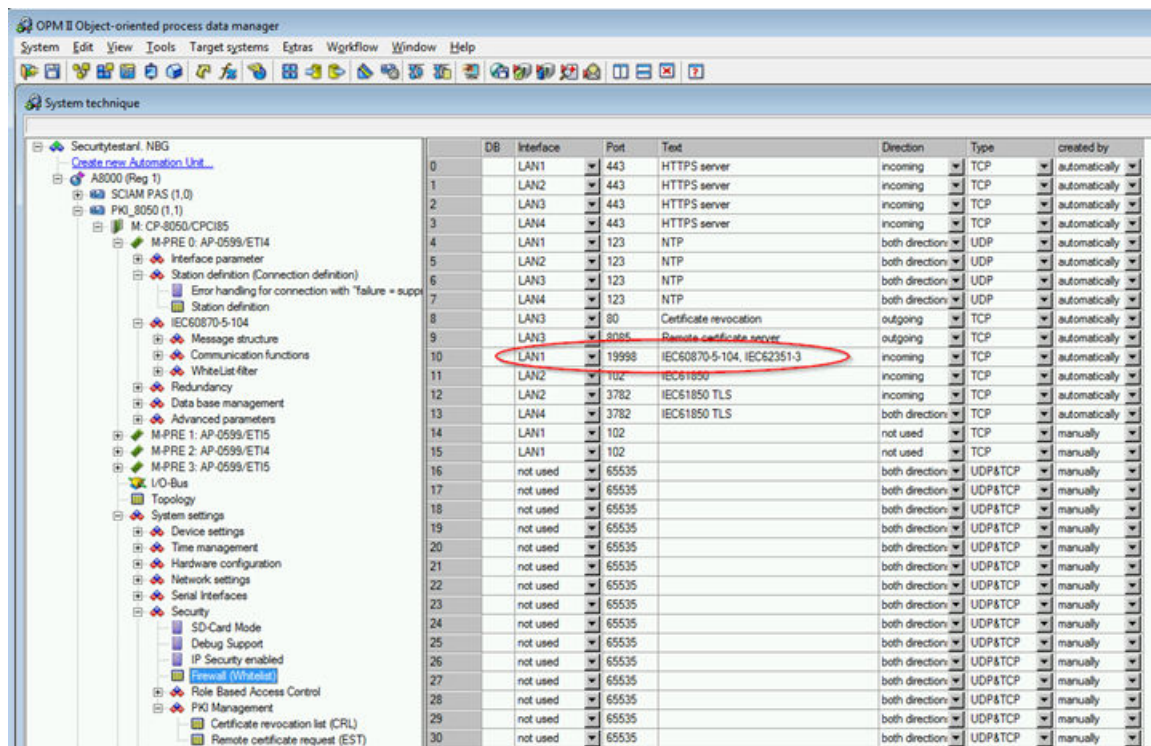
[sc_System Settings-Security-PKI Management-Certificate revocation list-CRL_1_en_US]

Figure 2-40 System Settings → Security → PKI Management → Certificate Revocation List (CRL)



[sc_Generate Firewall, 1, en_US]

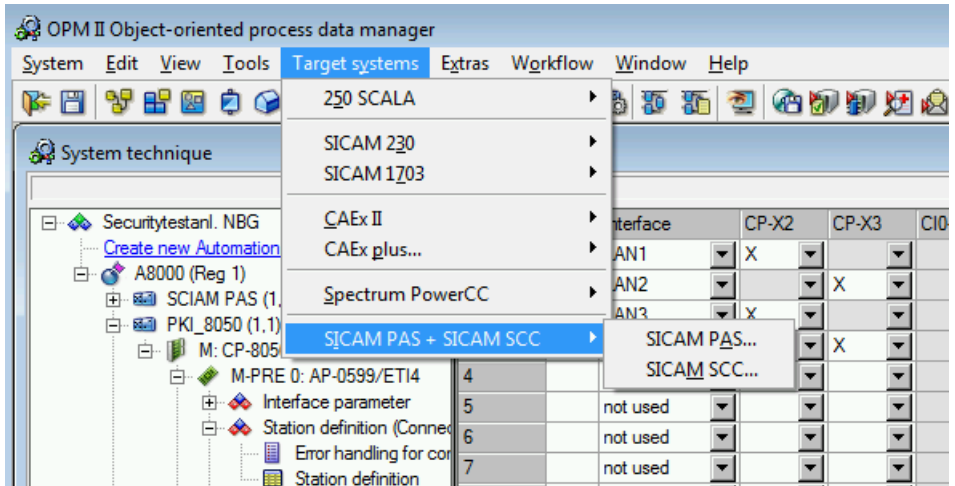
Figure 2-41 Generate Firewall



[sc_For IEC104 TLS communication the port 19998 will be open in firewall, 1, en_US]

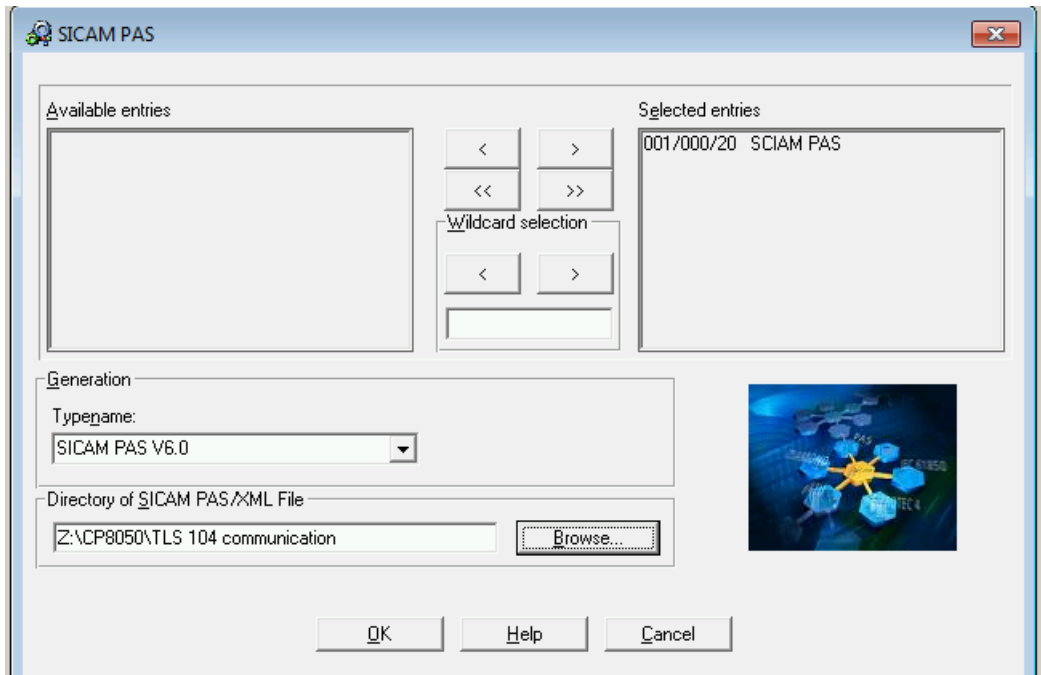
Figure 2-42 For IEC104 TLS Communication the Port 19998 will be Open in Firewall

The XML file for SICAM PAS import must be exported in the Toolbox.



[sc_xml file export for SICAM PAS, 1, en_US]

Figure 2-43 XML File Export for SICAM PAS

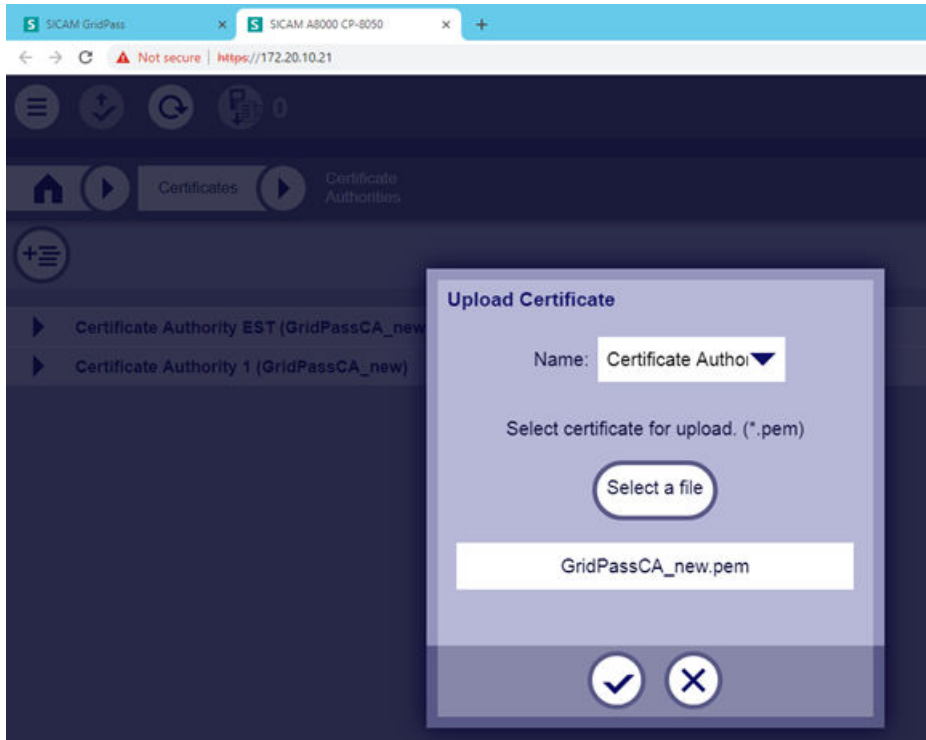


[sc_xml file export for SICAM PAS select directory, 1, en_US]

Figure 2-44 XML File Export for SICAM PAS Select Directory

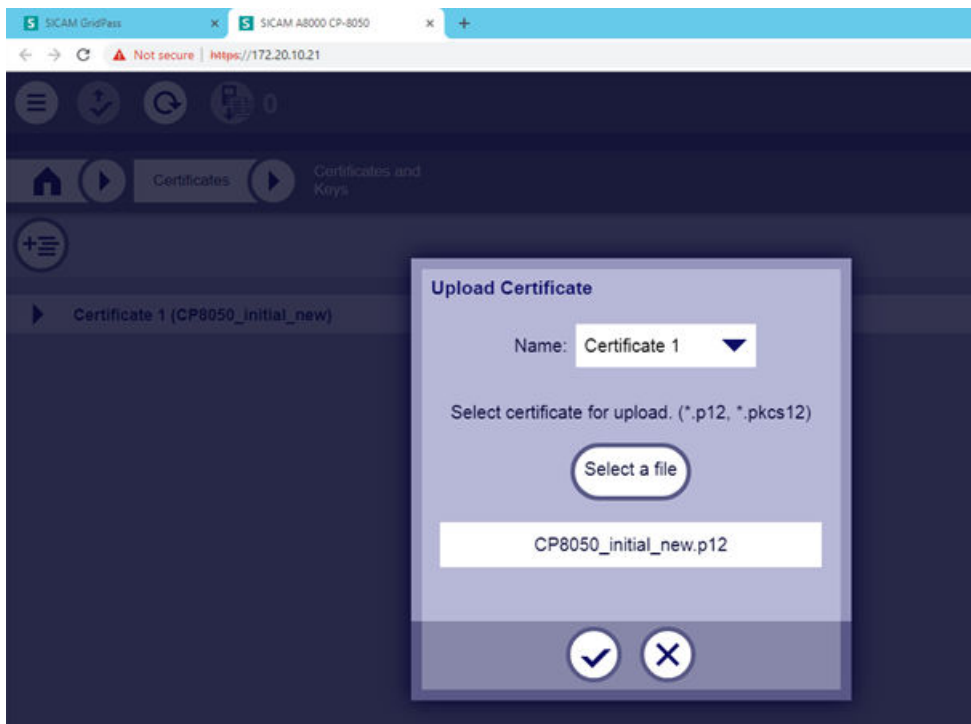
2.6.5.3 Import of EST Communication Certificates in CP8050

In GridPass, the certificates for Certificate Authority and CP8050 Client were created and exported for CP8050. These certificates are necessary for the EST communication between CP8050 and GridPass. Via this EST communication, CP8050 requests server certificates for the IEC 104 communication **CP8050/SICAM PAS**.



[sc_Import CA certificate to Certificate Authority1_1_en_US]

Figure 2-45 Import CA Certificate to Certificate Authority 1

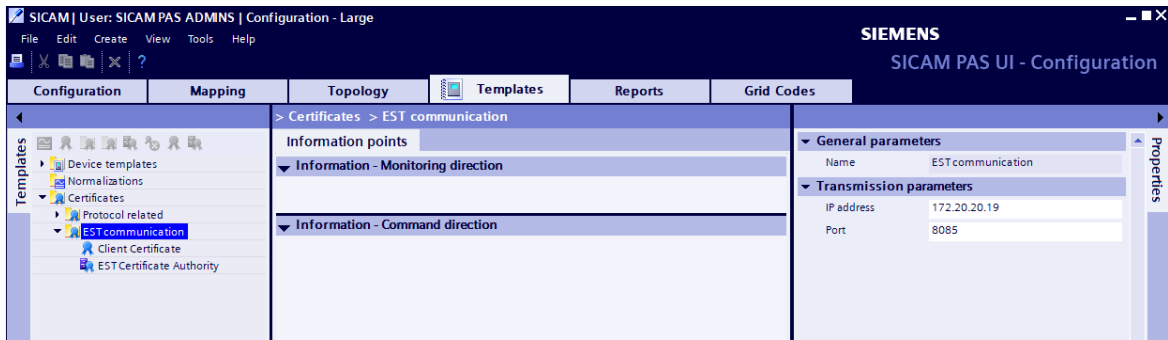


[sc_Import Client Certificate to Certificate 1_1_en_US]

Figure 2-46 Import Client Certificate to Certificate 1

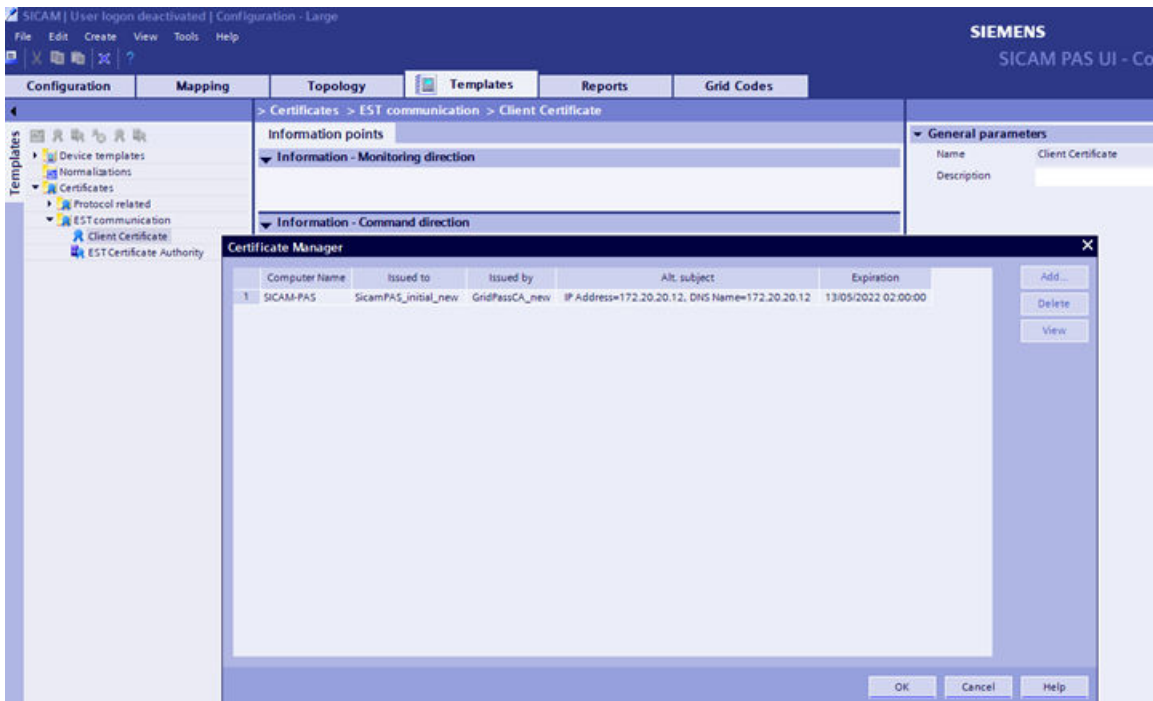
2.6.5.4 Configuration of SICAM PAS for IEC 104 TLS Communication

- ✧ First import the CA and the client certificate for the EST communication into the SICAM PAS templates. The IP address of the EST server must be written in the transmission parameters of the EST communication.



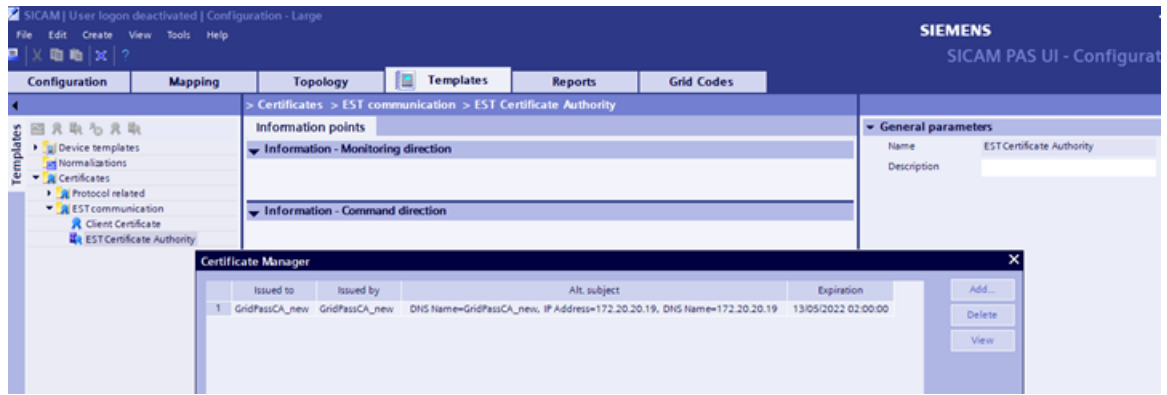
[sc_Transmission parameters GridPass EST server, 2, en_US]

Figure 2-47 Transmission Parameters GridPass/EST Server



[sc_Client Certificate import via Certificate Manager, 1, en_US]

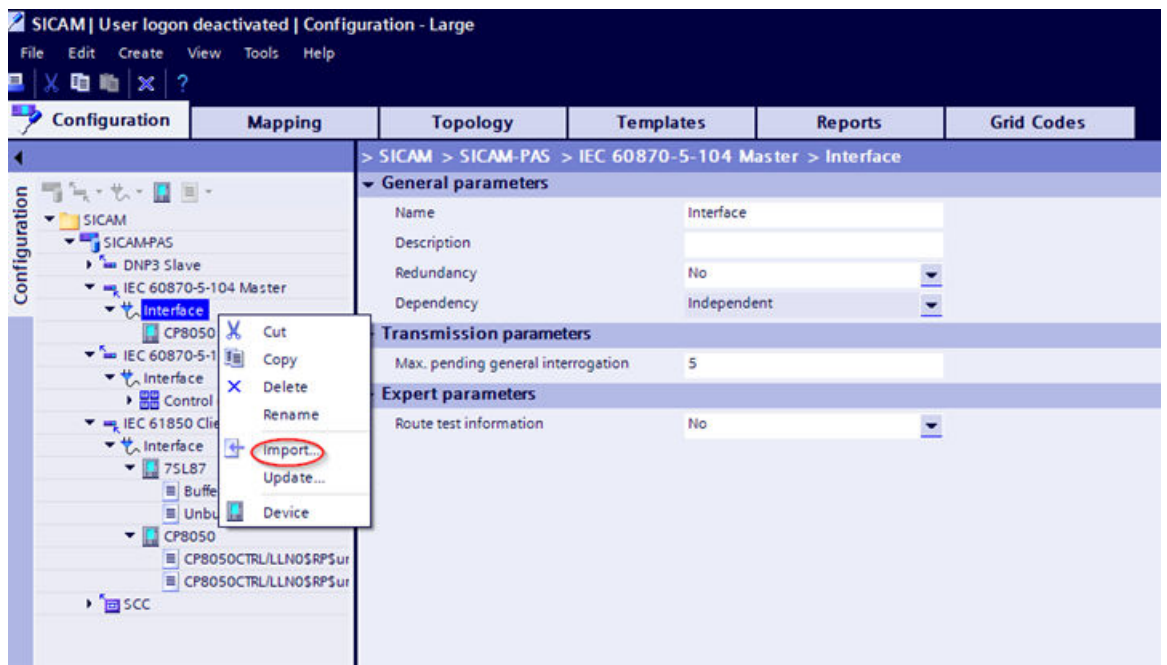
Figure 2-48 Client Certificate Import via Certificate Manager



[sc_Certificate Authority Certificate import via Certificate Manager, 1, en_US]

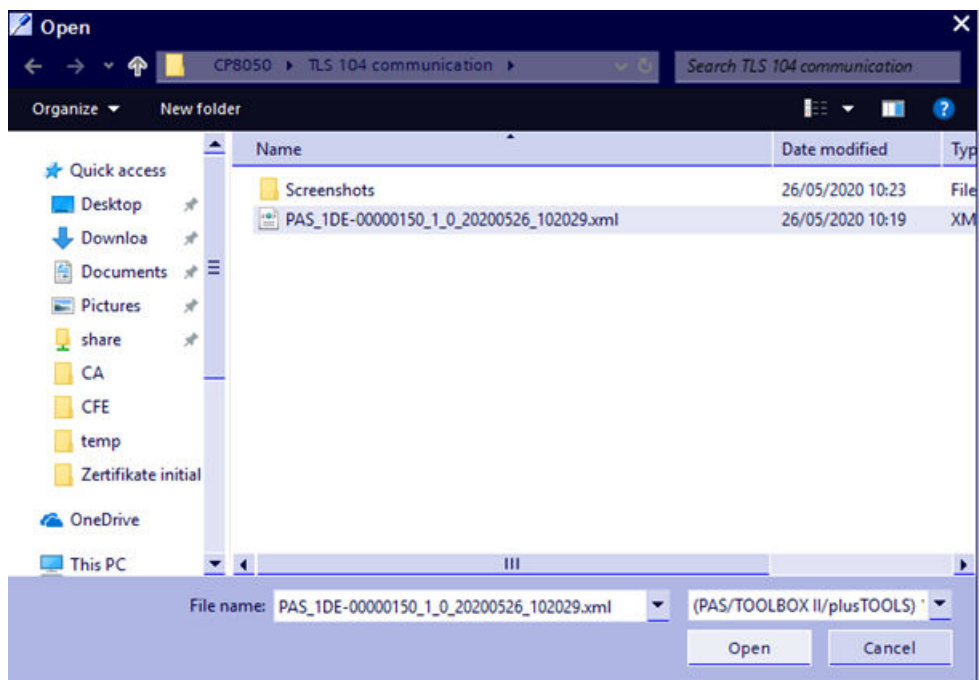
Figure 2-49 Certificate Authority Certificate Import via Certificate Manager

✧ For creating the IEC 60870-5-104 Master interface, import the XML file that was exported in the Toolbox.



[sc_XML import of CP8050 data, 1, en_US]

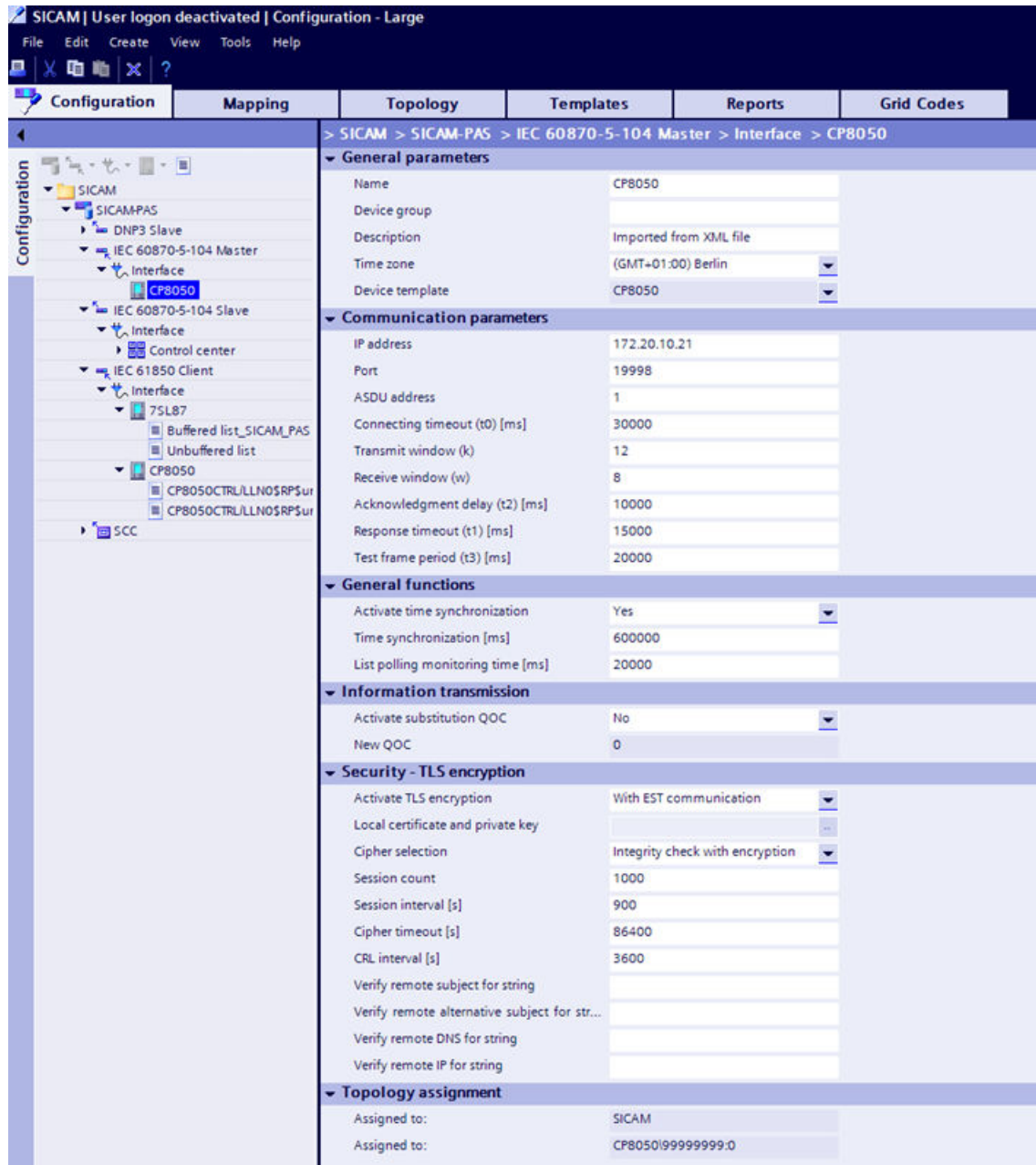
Figure 2-50 XML Import of SICAM CP-8050 Data



[sc_xml-file, 1, en_US]

Figure 2-51 XML File

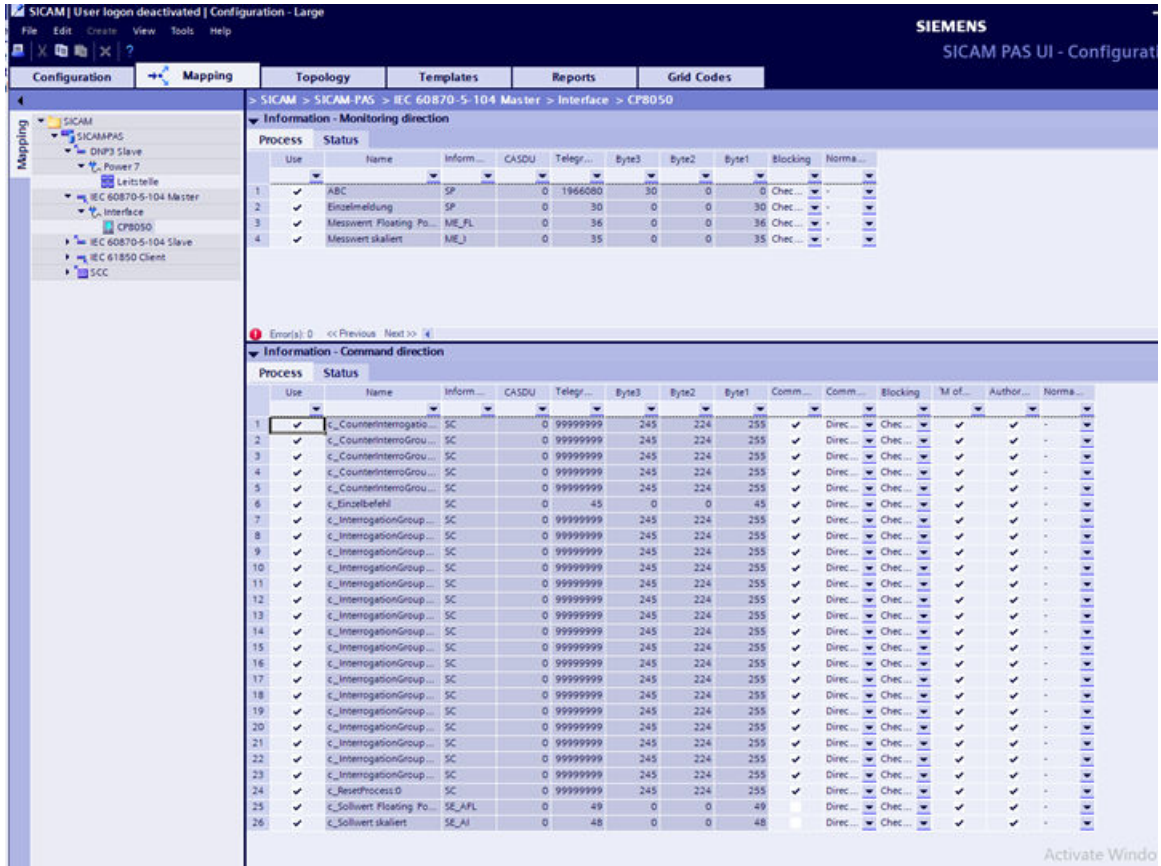
- ✧ To activate the TLS communication set **Security TLS encryption** → **Activate TLS encryption to with EST communication.**



[sc_TLS encryption in SICAM PAS, 1, en_US]

Figure 2-52 TLS Encryption in SICAM PAS

In the following, there is an example for signals which were mapped.



[sc_Mapped IEC104 signals, 1, en_US]
 Figure 2-53 Mapped IEC104 Signals

3 System Hardening

3.1	Hardening Principles	58
3.2	Product-Hardening Tips	58
3.3	General	58
3.4	Siemens Products	63

3.1 Hardening Principles

Hardening reduces the attack surface of the products and solutions by means of secure configuration. This is reached, e.g., by removing unnecessary software, unnecessary user names or logins, disabling unused ports, or OS hardening. Siemens provides guidelines on hardening for products and systems and can support operators in the hardening of their infrastructure. Hardening a substation automation system starts with activation of security settings of every component of such a system. This includes:

- Protecting the hardware from physical access to the ports and media such as USB, DVD drive, and network ports
- Securing the BIOS of the system
- Hardening the operating system
- Hardening the applications

The following section describes the recommended Hardening setting for all the above components.

3.2 Product-Hardening Tips

Hardening a substation automation system starts with activation of security settings of every component of such a system. The Siemens Energy Automation products have a description about product-related hardening. It includes, among others, the following topics:

- Malware prevention
- Appropriate use of role-based access
- Approach to disable unused network ports and services

For product-specific hardening guides, refer to:

- */10/ Description of the PowerShell constrained language mode: <https://devblogs.microsoft.com/powershell/powershell-constrained-language-mode/>*

3.3 General

3.3.1 Hardware

The hardening measures also can be applied to the hardware itself, by reducing the not utilized interfaces and by application of other measures.

3.3.1.1 Server Rack Setup

The first step towards enhanced security is to block the physical access to a system. Keeping the computers in a locked computer room or at least in a locked panel subject to access control can significantly reduce the risk of unauthorized intrusion into the network.

Reliable protection against infections via hardware interfaces can be established by providing mechanical protection of interfaces against unauthorized use.

This includes:

- Placing the PC or programmable controller in an enclosed control cabinet
- Access protection for keyboard and mouse using locked drawers under the screen
- Blocking of unused hardware interfaces (e.g., network ports and USB ports)

3.3.1.2 Disabling All Wireless Connections

Bluetooth and Wi-Fi provide another method to transfer information between various devices such as mobile phones, laptops, PDAs, PCs, printers, over a determine-range wireless link.

Depending on actual project needs, it is a general recommendation not to use any wireless communication in a substation-automated network.

First would be to avoid purchasing equipment that comes with Bluetooth or Wi-Fi hardware. If this is not possible, a removal of Bluetooth and Wi-Fi hardware is the way to ensure that the wireless components remain disabled or the driver should be deinstalled from the operating system and automatic access to the default Windows drivers should get blocked in the Windows registry. Only users with administrator rights should be able to make changes to the operating system. See your system hardware manual which should contain information on its Bluetooth and Wi-Fi capabilities.

3.3.1.3 No Cordless Keyboards

Cordless keyboards of any kind can be easily intercepted using cheap electronic equipment. This means a malicious person can intercept the keyboard-to-computer communication, thus getting hold of passwords and other sensitive communication in clear text. Normally, the malicious person does not have to hide near the computer because most keyboard signals can still be reconstructed in more than 30 meters. Some keyboard manufactures have started incorporating encryption technologies into their cordless keyboards. Currently we do not have enough information whether the implementations of encryption features can guarantee protection against the attack described above.

If a need for wireless keyboards arises (simple radio, infrared, or Bluetooth), all possible ways of using a wired keyboard instead must be investigated first.

3.3.1.4 No Biometric Authentication Devices

Some companies offer fingerprint authentication mouse/keyboard devices with capacitive fingerprint sensors. A couple of ways are known to defeat these and other biometric authentication devices.

These devices might be suitable for home application, but the potential risks prohibit using them in a corporate environment.

Remove biometric authentication devices. PKI-based smart cards are the preferred mechanism for strong authentication. However, biometric authentication devices that complement the use of smart cards are permitted – for example a fingerprint sensor on a smart-card reader for granting access to the smart card.

The BIOS is the most basic software which operates the computer functions. Apply the correct configurations to it to ensure that your system does not have any open vulnerabilities.

3.3.1.5 Boot and BIOS Passwords

The BIOS setup contains some settings that are security-relevant, e.g. boot sequence, boot password, wake-on LAN, system time, etc. Changes to these settings should only be made by the administrator of the system. This can be achieved by setting a BIOS access password. A BIOS boot password prevents a computer from starting up without providing an additional credential. Set a BIOS access password. Set a computer boot password if there are no strong reasons against it. The implementation depends on the specific BIOS version of the system. For details on BIOS settings, refer to the manual of the computer or main board.



NOTE

The boot password (but not the BIOS access password) can be omitted in the following cases:

- A server is supposed to boot automatically after a system failure. Implement security measures like a lockable cabinet for this type of servers and do not set a boot password.
- The system was configured to only allow one OS to be booted, i.e. no dual boot, only boot from built-in hard disk.
- The computer is protected by a full hard disk encryption program like Safeguard Easy that requires a password prior to booting from local hard disk.
- Many users within an office are using the same machine, and all would need to know the boot password.

The implementation depends on the specific BIOS version of the system. For details on BIOS settings, refer to the manual of the computer or main board.

3.3.1.6 Disabling Wake-On LAN

Some network adapters allow waking-up a shutdown system via the network. A malicious person at a remote network location can use this feature to start a system remotely to attack it thereafter.

Disable the BIOS setting **wake-on LAN**.



NOTE

This feature might be used by a UPS unit to provide a controlled system startup. In those cases, it is admissible to leave the wake-on LAN setting enabled.

3.3.1.7 Disabling Hardware Virtualization

New processor architectures like Intel I7, Xeon, and third-generation AMD Opteron support virtualization on a hardware level. That means that it no longer requires a host operating system to serve as a base for virtual machines. This feature is critical to security since it opens a space where new kinds of root kits can potentially hide without any chance of being recognized. As a precaution, virtualization should be disabled when not used.

Disable the virtualization feature of your CPU under **CPU Features** if supported by the BIOS setup and if virtualization is not needed.

Enter the BIOS setup. Navigate to **CPU Features** and verify that **Virtualization Technology** is set to **disabled**.



NOTE

In other BIOS versions or on other platforms, the setting might have a slightly different name or it might not exist at all.

3.3.1.8 Define System Boot-Up Sequence

When the computer power is first turned on, the startup follows a sequence of actions. The system will now attempt to determine the sequence of devices to load (based on the settings stored in the BIOS) to start the operating system. If it points to the DVD drive, it then searches for a CD disk. If it does not detect a bootable disk in the DVD drive, the system displays an error message. If the CD drive does not contain a DVD, it bypasses the first bootup device and detects the second device, which is usually the hard disk. It will then start by reading the boot code instructions located in the master boot record and copies all execution into the memory when the instructions are validated, and no errors are found.

A malicious person could boot up the system using a bootable DVD or USB stick to attack it thereafter.

- Disable system boot from USB.
- Configure the HDD with designated OS as priority boot.
- Remove unnecessary boot devices from the boot list.

3.3.2 Windows General

Hardening of Windows operating systems is a challenging topic. The recommended solution for the Windows environment hardening by Siemens is to apply the CIS CAT Remediation Kit package provided by the Center for Internet Security (CIS) as a baseline. CIS is a forward-thinking, non-profit entity that harnesses the power of a global IT community to safeguard private and public organizations against cyber threats through recognized best practices for securing IT systems and data against the most pervasive attacks.

It is important to note that the application of CIS CAT Remediation Kit may implicate in malfunctions to the system, so it is important to evaluate which measures of the Remediation Kit do not compromise the communication and the Siemens engineering tools.

The operating-system hardening measures must be applied for all Microsoft Windows based systems in the network. The Secure Substation solution must be as much compliant as possible with CIS benchmarks

recommendations. Some exceptions for these benchmarks can exist, as eventually some recommendations can lead to any kind of incompatibility. These exceptions shall be documented by the substation operators. For more information, visit the Website: <https://www.cisecurity.org/>.

The Siemens Computer Emergency Response Team (CERT) also provides hardening recommendations time to time based on the products. Website: <https://www.cert.siemens.com/>.

The Siemens Computer Emergency Response Team represents:

- Worldwide neutral consulting and support for network and system operators
Information Security (InfoSec) organizations
Information Security (InfoSec) service providers of all Siemens companies to prevent incidents (internal and external hacking, denial of service attacks, ...) and to limit their impact
Providing information on vulnerabilities and appropriate countermeasures (incl. checklists)
Representing Siemens in FIRST and towards other CERTs/IRTs
Information on tools for securing computer networks, propose tool strategies, and provide tools (public domain, licensing, programming)
Support on incident handling (detection, investigation, limitation of damage)

3.3.3 The Group Policy Object in Windows

Group Policy is an infrastructure that allows to implement specific configurations for users and computers. Group-Policy settings are contained in the Group-Policy objects (GPOs), which are linked locally and to the following Active Directory service containers: sites, domains, or organizational units (OUs). The settings within GPOs are then evaluated by the affected targets, using the hierarchical nature of the Active Directory. Consequently, Group Policy is one of the top reasons to deploy the Active Directory because it allows to manage user and computer objects. An Active Directory is not required for a GPO. GPOs can also be used in a standalone environment.

3.3.3.1 Why is the Group Policy Object Useful?

The settings are mandatory and should be deployed in the Service PC, the PAS running machine and the HMI. The deployment is time consuming and when it's carried out manually it can cause mistakes. For that reason, an automated deployment is helpful and recommended.

Refer to <https://www.microsoft.com/en-us/download/details.aspx?id=55319>.

3.3.3.2 Center for Internet Security (CIS) Benchmarks and Remediation Kits

CIS provides **Remediation Kits** to patch the system to make it in accordance with a CIS benchmark, hardening Windows operation system through GPOs (Group Policy Objects) or Linux through scripts. A list of remediation contents can be found on:

Refer to <https://www.cisecurity.org/cis-securesuite/cis-securesuite-remediation-content/>.



NOTE

The CIS Remediation Kits are only available for paying members of CIS Secure suite.

The remediation kits provided by CIS can patch the operation system with several security measures at once, avoiding time consuming and human mistakes with individual implementations. Therefore, this hardening guide document will likely follow CIS measures as much as possible once some exception can also take place for our products.

Create Login

First, it is necessary to create a login at CIS.

- ◇ Browse www.cissecurity.org and click **Login**.
You will be redirected to the CIS WorkBench website.
- ◇ Log in to the WorkBench by providing username and password.

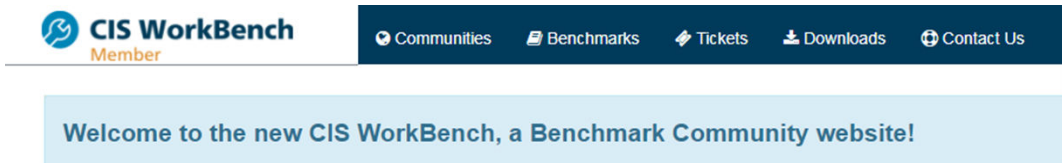


[sc_Logging in to CIS Work bench, 1, en_US]

Figure 3-1 Logging in to CIS Work Bench

Download

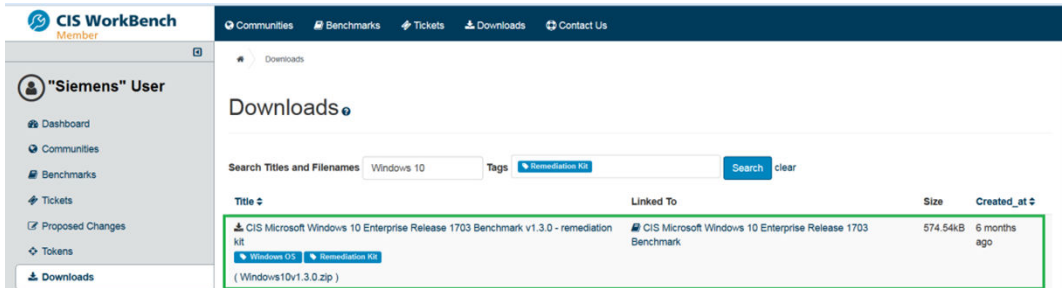
- ✦ After logging in, click the **Downloads** link.



[sc_Logged in screen CIS Work bench, 1, en_US]

Figure 3-2 Logged in Screen CIS Work Bench

- ✦ Enter **Windows** in the **Search Titles and Filenames** field and **Remediation Kit** in the **Tags** field.
- ✦ Then, click the remediation kit link to start downloading.



[sc_Searching Windows 10 Benchmark Remediation in WorkBench, 1, en_US]

Figure 3-3 Searching Windows 10 Benchmark Remediation in WorkBench



NOTE

The downloaded file should contain several folders which represent different levels of compliance.

Name	Size	Packed Size	Modified
BITLOCKER	150 130	17 989	2017-01-27 12:22
COMP-L1	454 333	43 886	2017-01-27 12:22
COMP-L2	130 692	17 856	2017-01-27 12:22
IPv6 Template	1 000	475	2017-01-27 12:22
USER-L1	51 588	8 829	2017-01-27 12:22
USER-L2	25 179	4 691	2017-01-27 12:22
readme.txt	1 510	715	2017-01-26 14:00

[sc_Locating the Downloaded Windows 10 Benchmark Remediation File, 1, en_US]

Figure 3-4 Locating the Downloaded Windows 10 Benchmark Remediation File

3.4 Siemens Products

3.4.1 SIPROTEC 5/DIGSI 5

3.4.1.1 SIPROTEC 5 Devices

Recommended hardening settings for SIPROTEC 5 devices are documented in the SIPROTEC 5 manual which also provides a communication matrix showing all supported protocols. Refer to Appendix B for required open ports. By default, only the connection to DIGSI 5 is activated in the device. All other Ethernet services and ports are deactivated in the device by default and can be activated using DIGSI 5. Because of the secure default configuration, there is no open interface for potential attackers and only used services are activated in the network.

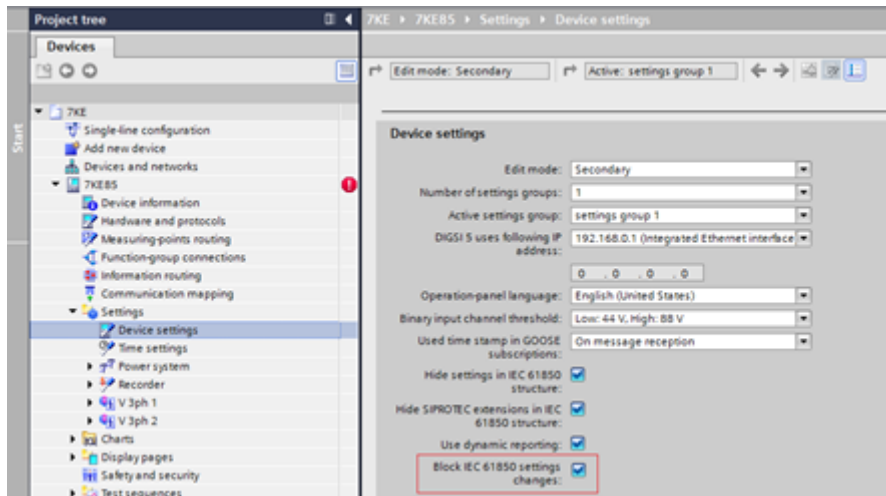
SIPROTEC 5 is shipped with installed security measures already, including the following measures:

- The devices implement an internal firewall for controlling/blocking network traffic.
- Firmware updates are protected by digital signatures.
- Web Server should be deactivated
- Use of SNMP V3
- For further clarification, see operational security and access control in the SIPROTEC 5 manual.

3.4.1.2 Block IEC 61850 Settings Changes

To avoid unwanted setting changes via IEC 61850, it is recommended to block IEC 61850 setting changes if the functionality is not needed for the operational management of the system.

- ✧ To perform the block, navigate to **Settings** → **Device settings**.
- ✧ Check the box **Block IEC 61850 settings changes**.



[sc_Hardening SIPROTEC5, 1, en_US]

Figure 3-5 Hardening SIPROTEC 5

This is valid for SIPROTEC 5 devices with version V07.00 and higher.

3.4.2 SICAM A8000

The hardening measures for the SICAM A8000 series/SICAM RTUs include the following:

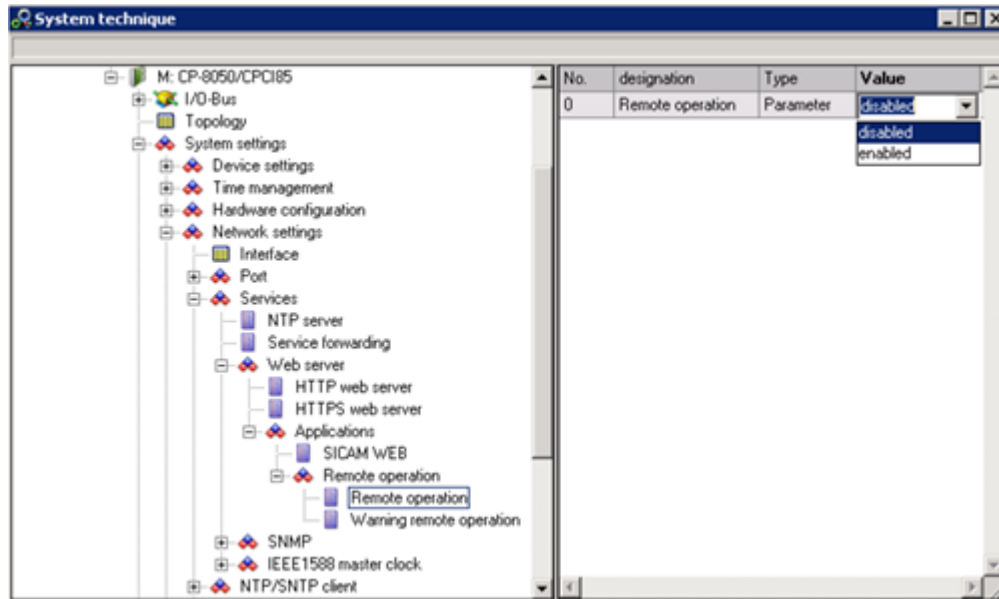
- Deactivation of unnecessary system and communication services (remote operation, remote maintenance, NTP, WEB...)
- Deactivation of unnecessary standard users (WEB)
- Activation of configuration options that increase security
- Measures for restricted distribution of system settings messages

3.4.2.1 Deactivation of Unnecessary System and Communication Services

Remote Operation

In remote operation, SICAM TOOLBOX II/SICAM Device Manager does not connect with a SICAM RTU by means of a local parameterization cable, rather over a network interface using TCP/IP (with activated Listener Service in SICAM RTUs).

With LAN protocols, the remote operation is deactivated by default in SICAM RTUs. If necessary, this can be activated individually. The corresponding parameter **Remote Operation** can be found in the system-technical parameter setting either on the BSE (e.g.: CPC80, CPCX26, PCCX26, CPC185) or PRE (e.g.: ETA3, ETA4, ETA5).



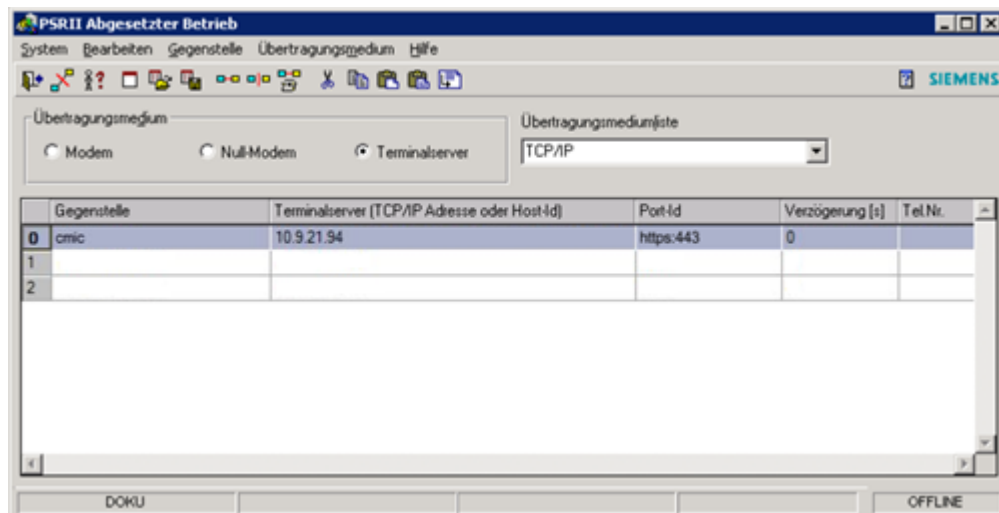
[sc_SICAM CP-8050 – CPC185, 1, en_US]

Figure 3-6 Example: SICAM CP-8050 – CPC185

Establish an HTTP(S) Connection with Blocked ICMP-ECHO

In case of a blocked ICMP-ECHO in a firewall between SICAM TOOLBOX II and SICAM RTUs, it is not possible per default to establish an automatic connection. By additional definition of the desired connection type, it is possible to bypass this block.

The corresponding parameter – **Port-ID** – can be found in the phone list of the remote operation (System – Remote Operation).



[sc_Establish a HTTP(S)-connection with blocked ICMP-ECHO, 1, en_US]

Figure 3-7 Establish a HTTP(S) Connection with Blocked ICMP-ECHO

Table 3-1 Table Port-ID

Port-ID	Description
HTTPS:443	Connection to port 443 Industrial security is established via HTTPS
http:80	Connection to port 80 is established via http
2001	Connection to port 2001 established

The ports http(80) or HTTPS(443) are available in new SICAM RTUs systems/firmwares like, SICAM A8000.

3.4.3 SICAM PAS

3.4.3.1 Firewall Settings for Windows

Enable the Windows firewall with advanced security, (FWwAS) and apply a product-specific configuration as provided by product hardening instructions.

<https://support.industry.siemens.com/cs/document/109758083/sicam-pas-pqs-installation?dti=0&pnid=24615&lc=en-US>

Ports/programs/services that must be configured as exceptions if required are described in the manual of installation in chapter *Firewall Configuration*.

3.4.4 SICAM SCC

3.4.4.1 Firewall Settings for Windows

During the installation, SICAM SCC configures the Windows software firewall automatically. Other firewalls must be properly configured before installation.

Download the SICAM SCC user manuals via the following link: https://support.industry.siemens.com/cs/attachments/109756817/scc_b.pdf?download=true

SICAM SCC needs certain communication ports for the communication in the network. If these ports are occupied by other programs like e.g. an already installed SQL server, the communication of SICAM SCC can be disturbed.

The port settings can be checked in command line using the following command: `netstat -a -n -o`

The following PIDs can be found in the window Processes of the Windows Task Manager; for this purpose, activate the column **PID** in the menu **Select view/columns**.

3.4.5 RuggedCom Switch



NOTE

The described hardening measures for the used Ruggedcom switches are based on documentation for the Ruggedcom switch type RSG2100. All links to the original documents refer to this switch type. Other Ruggedcom switches like RS900 and RS900G are based on the same philosophy so that similar settings apply.

3.4.5.1 Change all Default Passwords

By default, all RuggedCom switches come with default passwords for the users Admin, Operator, and Guest. These passwords must be changed. New passwords should be created according to agreed complexity rules.

The password should be changed after the first login for security reasons.

For more information on how to configure a RuggedCom ROS device Switch (for example, RSG2100), refer to the actual *RuggedCom* manual.

3.4.5.2 Deactivation of Unused Switch Ports

For safety measures, it is important that potential attackers get no physical access to the SCADA network. In case the attacker is privileged to have access to the setup, the next step is to secure the point where he could enter the network by connecting his own devices. For this, it is important to deactivate all unused switch ports.

- ✧ Select the **Disabled** state for each unused port.

3.4.5.3 Deactivation of Unused Protocols

Insecure access methods, such as RSH, Telnet, and TFTP, should be disabled in accordance with the organization's communication network security design and corresponding policies. RSH, Telnet, and TFTP are TCP/IP network protocols which are helpful in assessing distant computer terminals but offers weak security. Data is not encrypted naturally when it is sent over the network. If any user has access to a network router and gateways and the system is based on one of those protocols, he can capture the data packets containing any information and related to anyone.

- ✧ Deactivate the possibility of access to the device via RSH, Telnet, and TFTP.
Use secure alternatives (SSH, Web access via https) instead, if required.

Disabling RSH, Telnet, and TFTP

For disabling RSH, Telnet and TFTP on a RuggedCom switch (for example RSG2100), you must set up the following settings under IP services:

- ✧ Set the number of **Telnet Sessions Allowed** to 0.
- ✧ Set the pop down menu **TFTP Server** to **Disabled**.
- ✧ Tick the RSH server as **Disabled**.

Inactive Timeout	60 min
Telnet Sessions Allowed	Disabled
Web Server Users Allowed	Disabled
TFTP Server	Disabled
Modbus Address	Disabled
SSH Sessions Allowed	4
MMS Sessions Allowed	Disabled
RSH Server	Disabled
IP Forwarder	Disabled
Max Failed Attempts	10
Failed Attempts Window	5 min
Lockout Time	60 min

For more information, refer to the actual *RuggedCom manual*, chapter *IP Services*.

3.4.5.4 SNMP Configuration

ROS supports the Simple Network Management Protocol versions 1 (SNMPv1), 2 (SNMPv2c), and 3 (SNMPv3). The SNMPv3 protocol provides secure access to devices by a combination of authentication and packet encryption over the network. Default passwords or names like the community name **Public** should be changed to something uncommon.

If supported by the whole network devices, it is recommended to use SNMPv3.
SNMP shall be disabled on each device where it is supported but not required.

3.4.6 RuggedCom Router



NOTE

The described hardening measures for the used RuggedCom routers are based on the documentation for the RuggedCom switch type RX1500. All links to the original documents refer to this router type. Other RuggedCom routers may be based on the same philosophy so that similar settings apply.

3.4.6.1 Change all Default Passwords

By default, all RuggedCom routers come with default passwords for the users Admin, Operator, and Guest. These passwords must be changed. New passwords should be created according to agreed complexity rules.

The password should be changed after the first login for security reasons.

3.4.6.2 Deactivation of Unused Switch Ports

- ✧ Select the **Disabled** state for each unused port.



NOTE

For more information on how to configure a RuggedCom router (for example RX1500), refer to the actual *RuggedCom manual*: chapters *Managing Switched Ethernet Ports* and *Managing Routable Ethernet Ports*.

3.4.6.3 Use Secure Protocols

- ✧ Deactivate the possibility of network discovery via the Link Layer Discovery Protocol.

4 Access Control and Account Management

4.1	Least Privilege	70
4.2	Account-Management Configuration Instructions	71
4.3	Role-Based Access Control for Field-Level Devices	100
4.4	Public Key Infrastructure (PKI)	127
4.5	OpenLDAP	135
4.6	Device-Specific Configuration Notes	143

4.1 Least Privilege

Restricting the Access to the System

Create a special Windows user group for the installed program. Only users that belong to this group should be allowed to start the program and browse to these folders. This user group should have only read access to the program folders, but only if necessary. Normal Windows user accounts should not have the rights to start the program or browse to the program folders.

Create only users that are members of the Windows user group and your defined program group.



NOTE

Never use an administrator account for normal computing. This measure grants a high level of security to avoid the infiltration of malware DLL or EXE files.

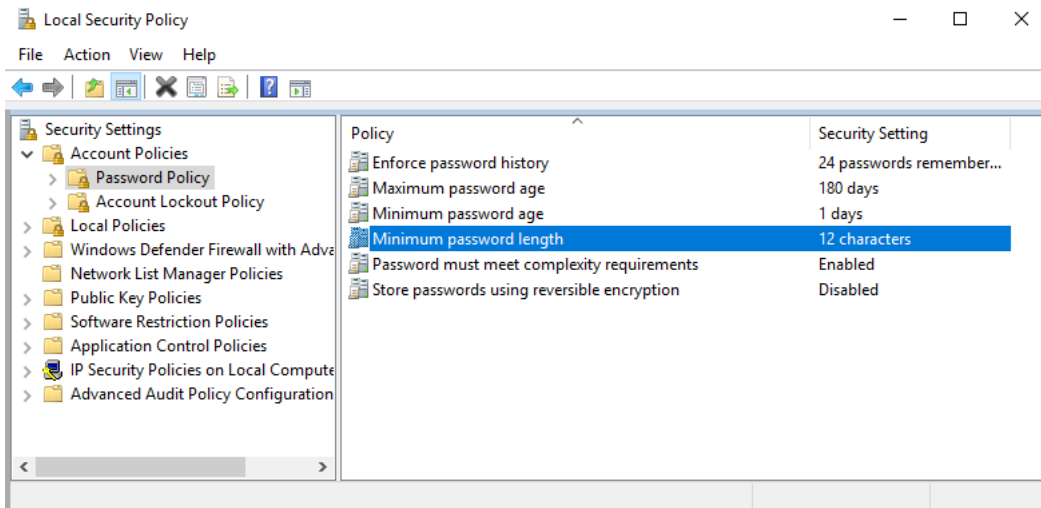
In many cases, it is recommended to establish a domain concept with proper password rules as a local policy-based user group set.

Restricting the Access to the Computers

The first step towards enhanced security is to block the access to a system. Keeping the computers in a locked computer room subject to access control can significantly reduce the risk of unauthorized intrusion into the network.

Be aware of the following additional points:

- Use only personal user accounts. Do not use accounts shared by several users.
- Set the password directives very restrictively:
 - The minimum password length is 8 characters.
 - The password must include uppercase and lowercase letters, numerals, and special characters.
- Passwords must expire after 90 days at the latest.



[sc_password_security, 2, en_US]

Figure 4-1 Password Security

- Users shall only be granted rights which are necessary for their tasks. For example, only the administrator can install software or delete Windows events.
- Activate the password-protected screensaver. Siemens recommends using the standard Windows screen-saver.
- If not necessary for operation, only the administrator shall have the rights required for connecting USB devices.

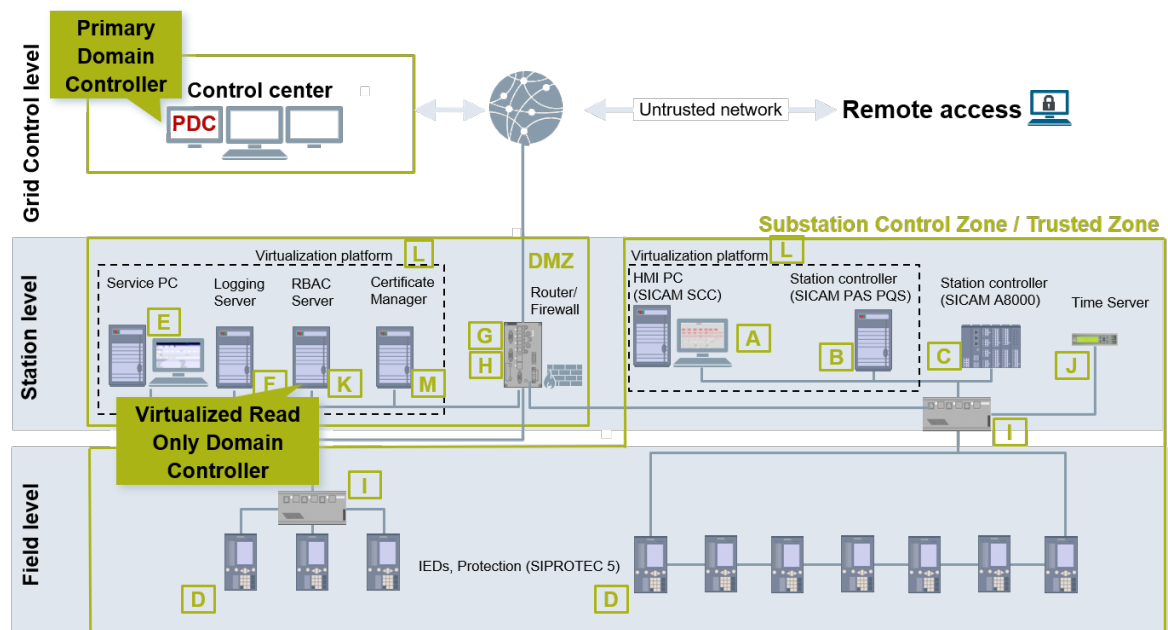
4.2 Account-Management Configuration Instructions

The parent/child domain control where the parent domain is situated in the control center level and child domain is at substation level may cause some discrepancy while referring to the administration and when there is connection loss between parent and child domain. To overcome this, it is strongly recommended to integrate the domain and to use a single domain as Primary Domain Controller (PDC).

The Primary Domain Controller shall be situated at control center level and a Read Only Domain Controller (RODC) at the substation level. The detailed process to set up a Primary Domain Controller and Read Only Domain Controller is described in the following chapters.

4.2.1 Topology

The installation of a writable domain controller and Read Only Domain Controller follows in principle the same workflow except for one setting where you define the RODC role.



[sc_Domain Controller Topology, 1, en_US]

Figure 4-2 Domain Controller Topology

4.2.2 Primary Domain Controller (PDC)

4.2.2.1 Installation of Primary Domain Controller (PCD)

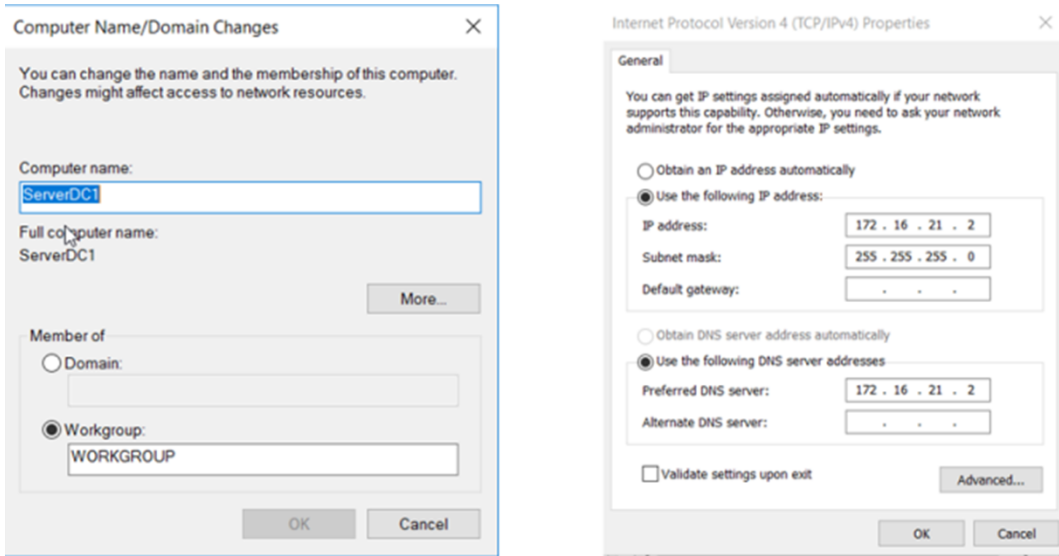
- ◇ Log in as the Built-In Administrator.



NOTE

Do not change the name during the Server 2016 installation, as this could cause problems with the identification of the Built-In Administrator. A normal user with administrator rights may not have the full permission for installing and running all services for the domain.

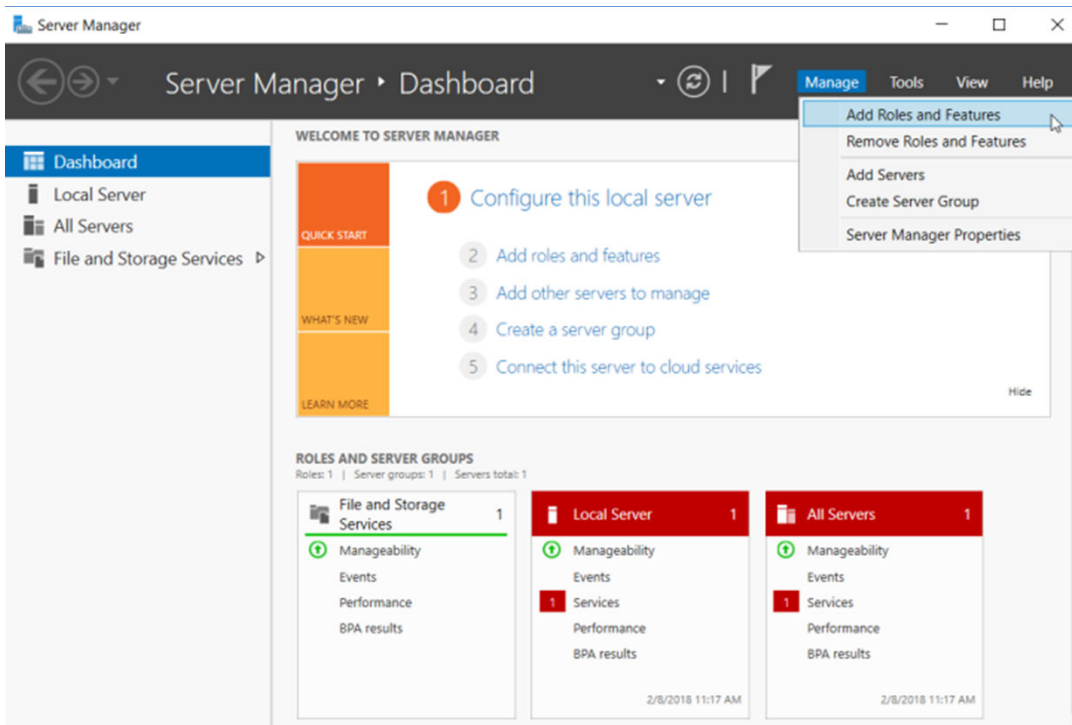
- ◇ Before starting the domain services configuration, it is important to set the Domain Controller's computer name and its static IP Address.



[sc_Domain Controller's Computer Name and Static IP, 1, en_US]

Figure 4-3 Domain Controller's Computer Name and Static IP

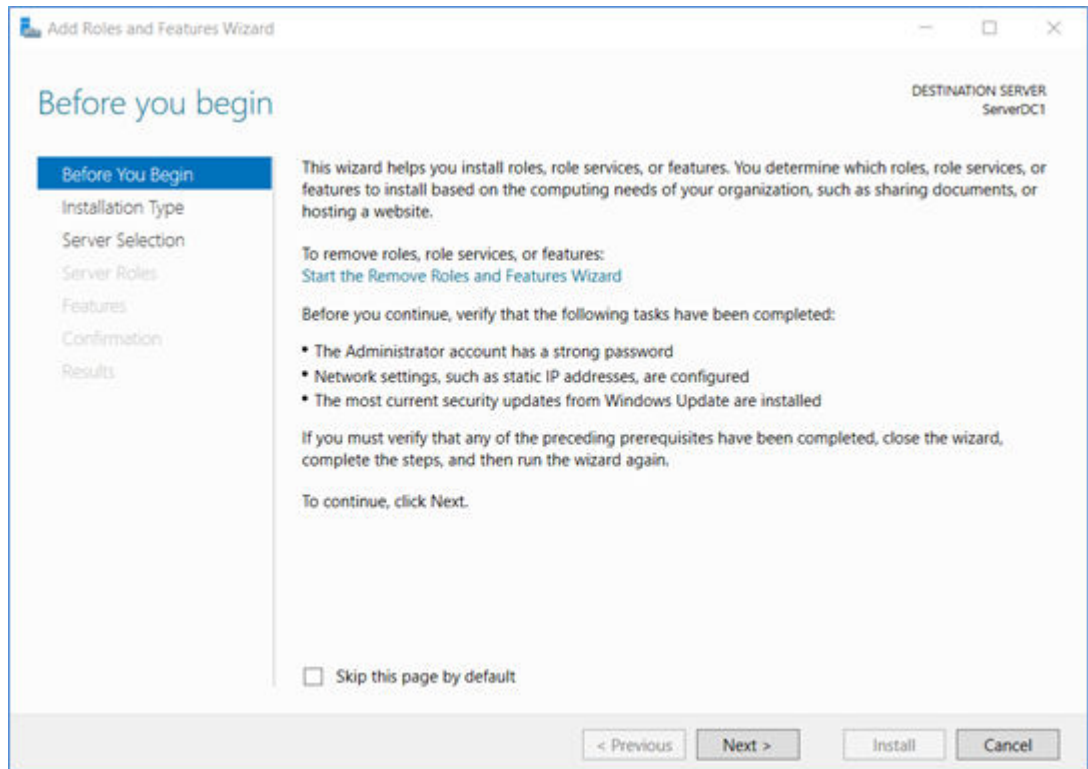
- ✦ After that, execute the Server Manager by clicking the **Start** → **Server Manager**.
The **Server Manager Dashboard** will be displayed.
- ✦ Click the superior menu **Manage** → **Add Roles and Features**.



[sc_Select Add Role Feature, 1, en_US]

Figure 4-4 Select Add Role Feature

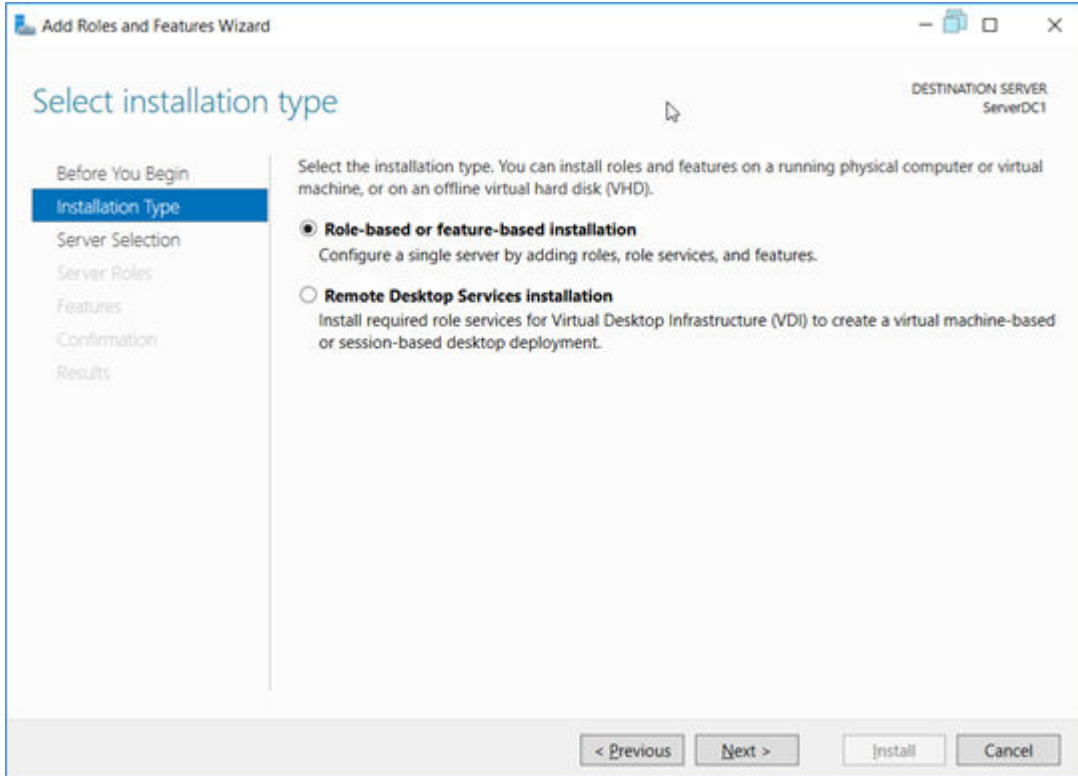
- This brings up the configuration Wizard, starting with the **Before You Begin** page.
- ✦ Read the information on this page and click **Next**.



[sc: Add Role wizard, 1, en_US]

Figure 4-5 Add Role Wizard

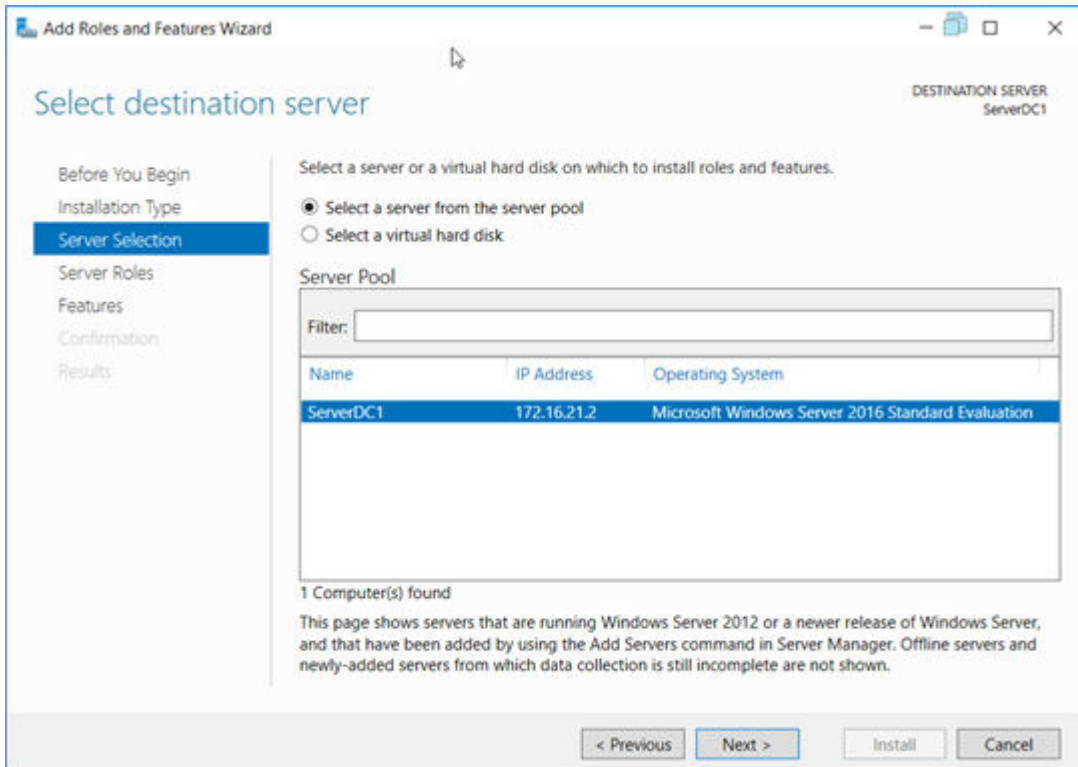
- ✧ The installation type allows user to install services in a local or remote server. The remote server deployment (Remote Desktop Services installation) can also include more than one server if necessary. For our purposes, the local server deployment (Role-based or feature-based installation) should be chosen.



[sc_Installation Type, 1, en_US]

Figure 4-6 Installation Type

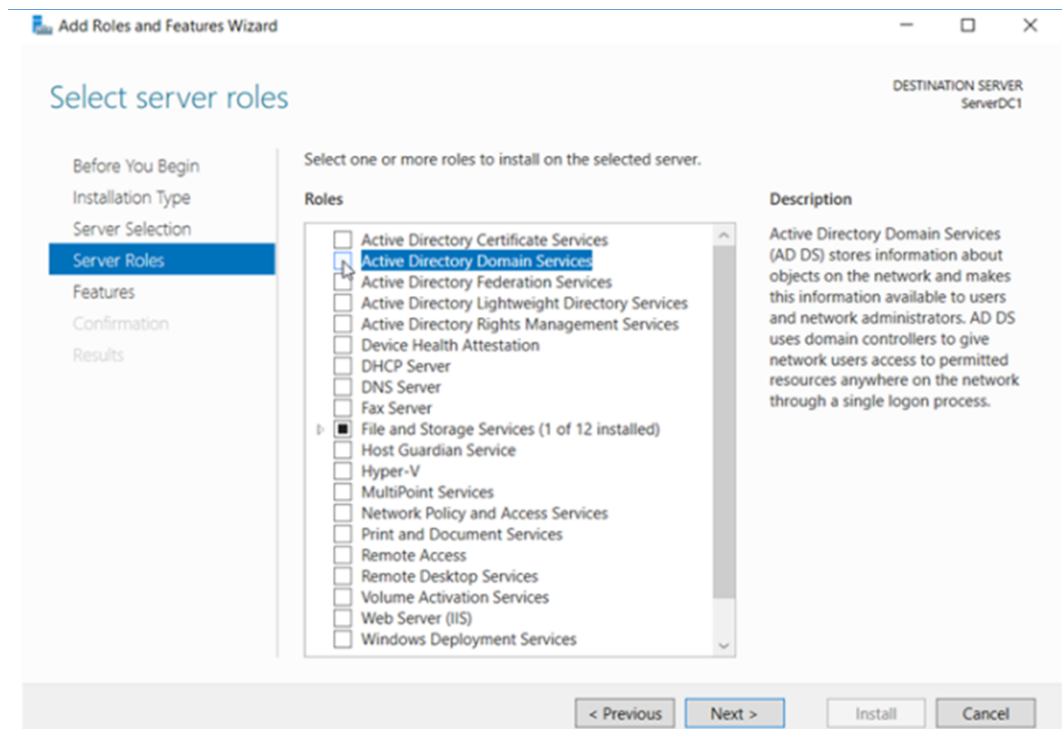
✧ Select the local server to become Domain Controller.



[sc_Select Destination Server, 1, en_US]

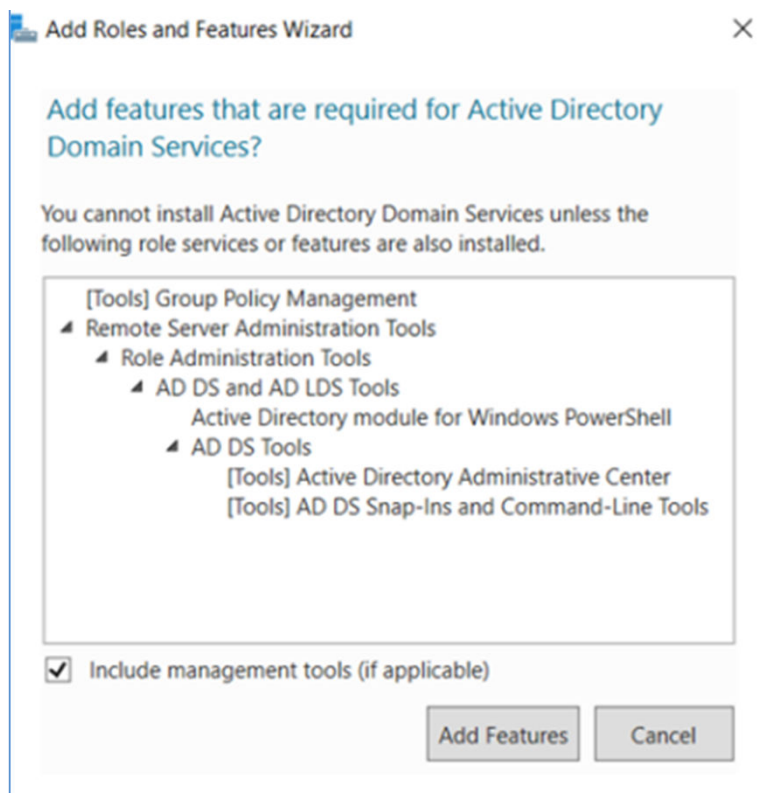
Figure 4-7 Select Destination Server

- ✧ Select which server roles you want to install. Select the **Active Directory Domain Services** by marking the corresponding checkbox.



[sc_Selecting Server Roles, 1, en_US]

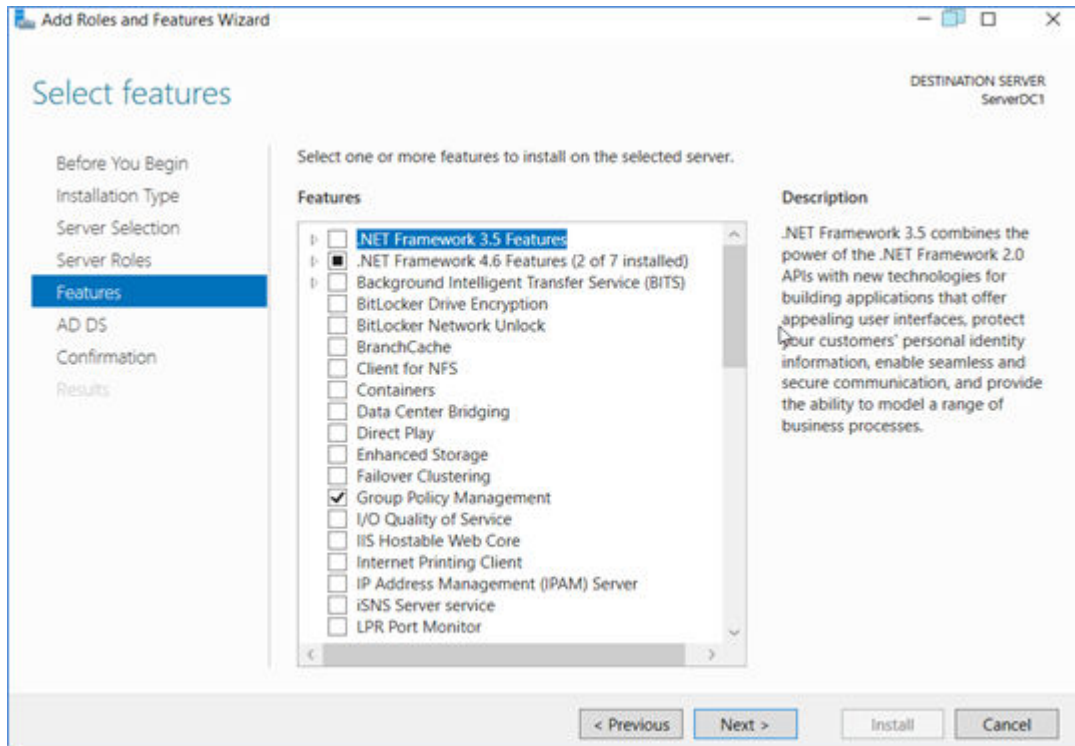
Figure 4-8 Selecting Server Roles



[sc_Features of AD Domain Services, 1, en_US]

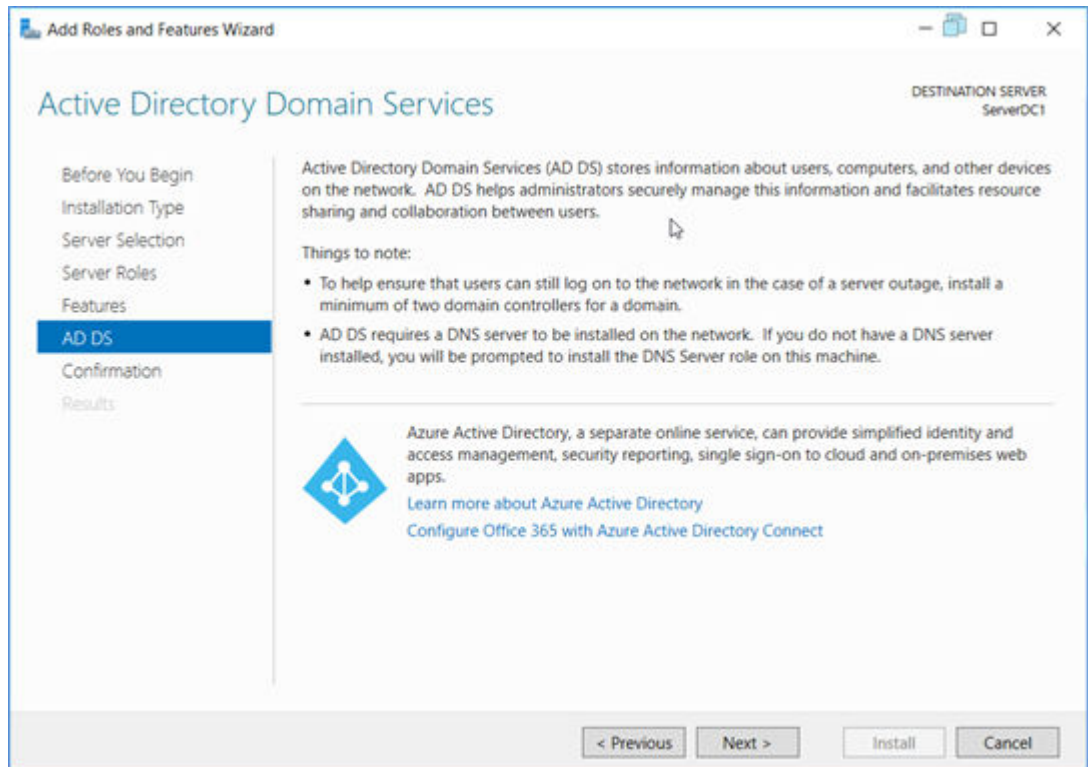
Figure 4-9 Features of AD Domain Services

- ✧ Note that the wizard will show you a number of features that will be installed along with the Active Directory Server Role. Click the **Add Features** to get those features installed with the Active Directory Server Role.
- ✧ The required features will be checked automatically and then, click **Next**. After selecting the Active Directory DC Server Role, you will see information about that server role.



[sc_Adding Group Policy Management, 1, en_US]

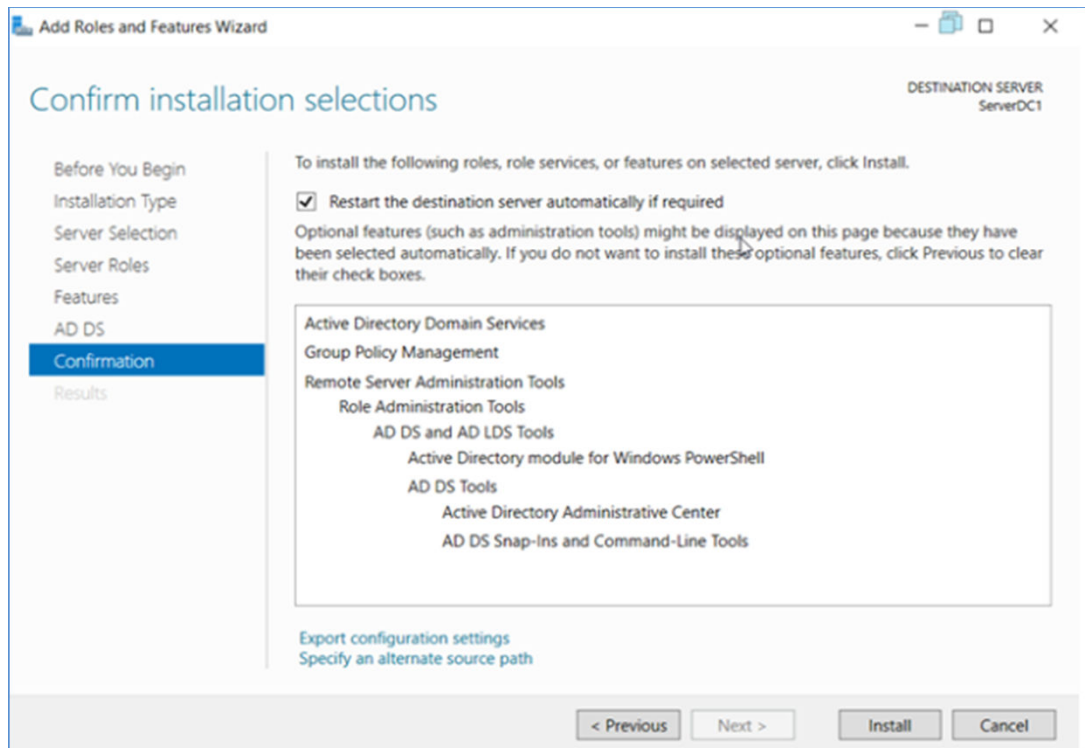
Figure 4-10 Adding Group Policy Management



[sc_Selecting AD Domain Service, 1, en_US]

Figure 4-11 Selecting AD Domain Service

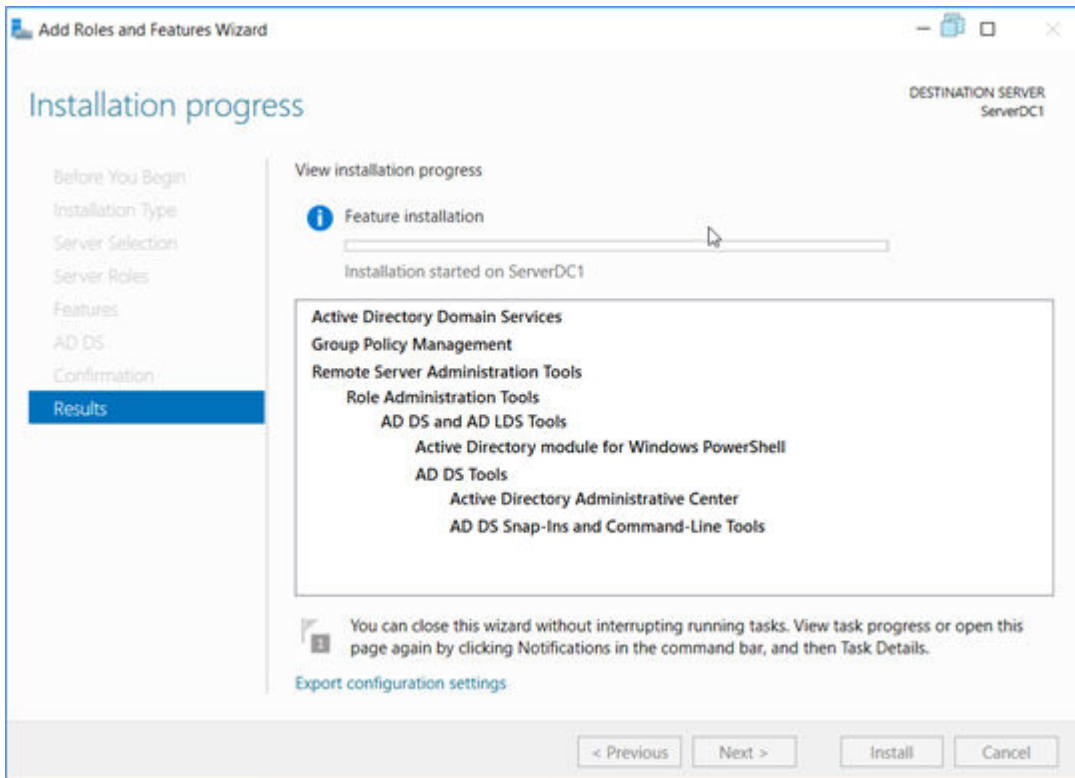
✧ Now, the AD is ready to be installed. You can tick **Restart the destination server automatically if required** for this first time, but it is not recommended for the next necessary installations.



[sc_Installation Confirmation, 1, en_US]

Figure 4-12 Installation Confirmation

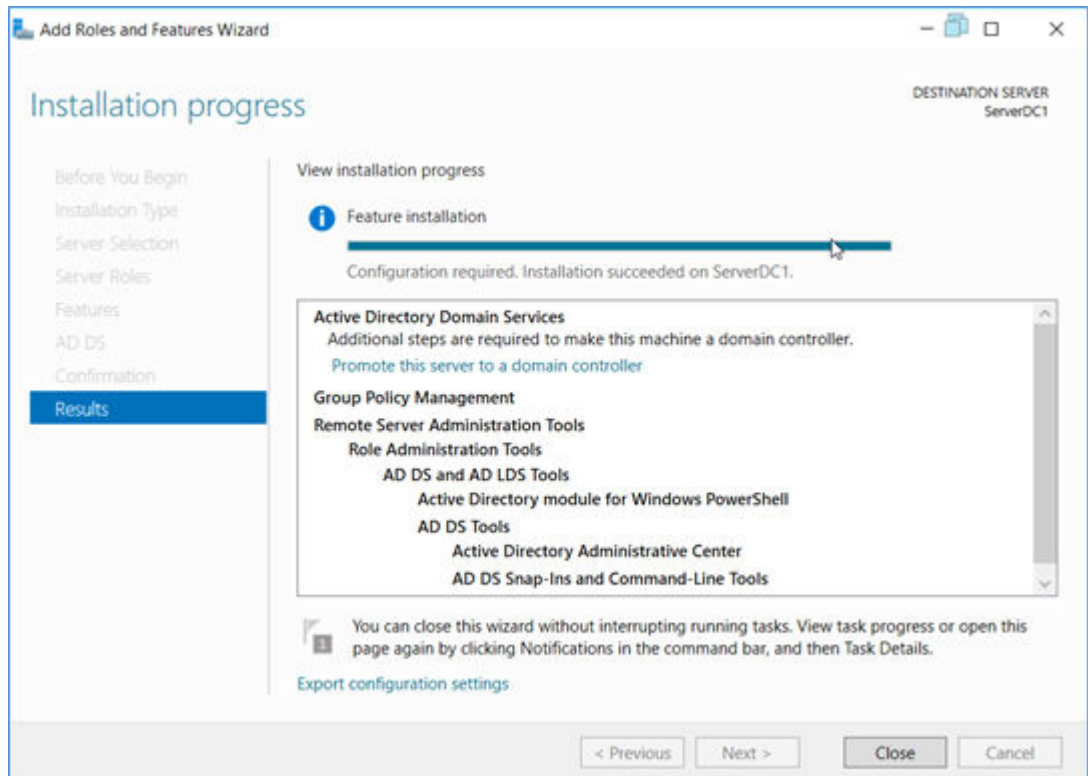
You can follow the installation status through the progress bar.



[sc_Installation Results, 1, en_US]

Figure 4-13 Installation Results


After concluded, a message will inform you that installation was succeeded but configuration is now required.

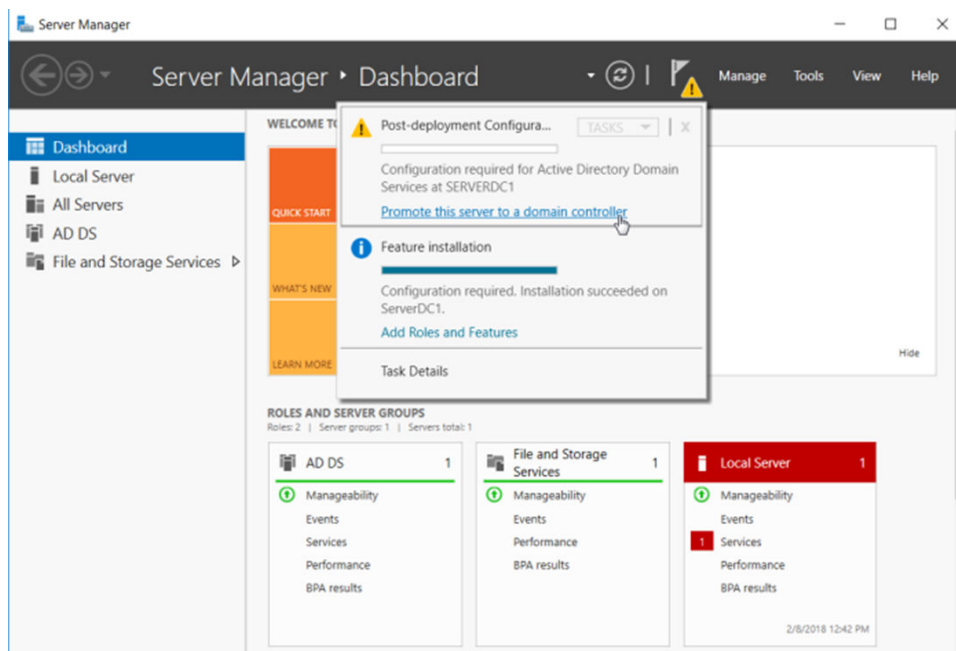


[sc_Feature Installation, 1, en_US]

Figure 4-14 Feature Installation

4.2.2.2 Configuration of a Domain Controller (DC)

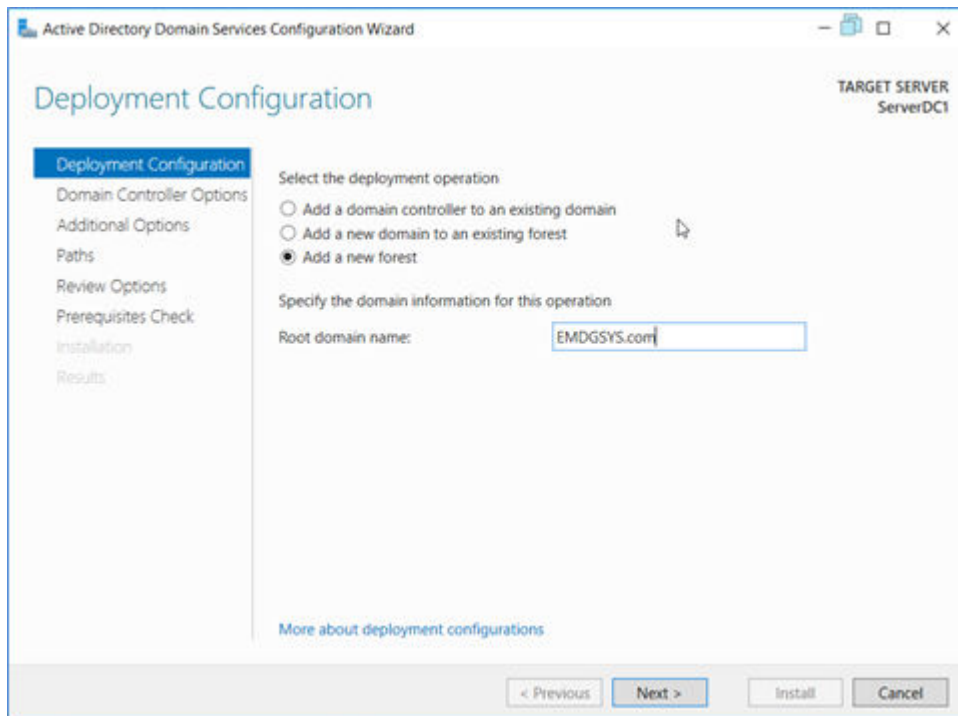
- ✧ After the installation of DC, the notification menu (as a **flag**) will raise an alert  and a link **Promote this server to a DC** will be available for you to start the configuration of the DC.



[sc_Configuration of Domain Controller, 1, en_US]

Figure 4-15 Configuration of Domain Controller

- ✧ In the **Deployment Configuration**, select **Add a new forest**. For example, the domain **EMDGSYS.com** is used.

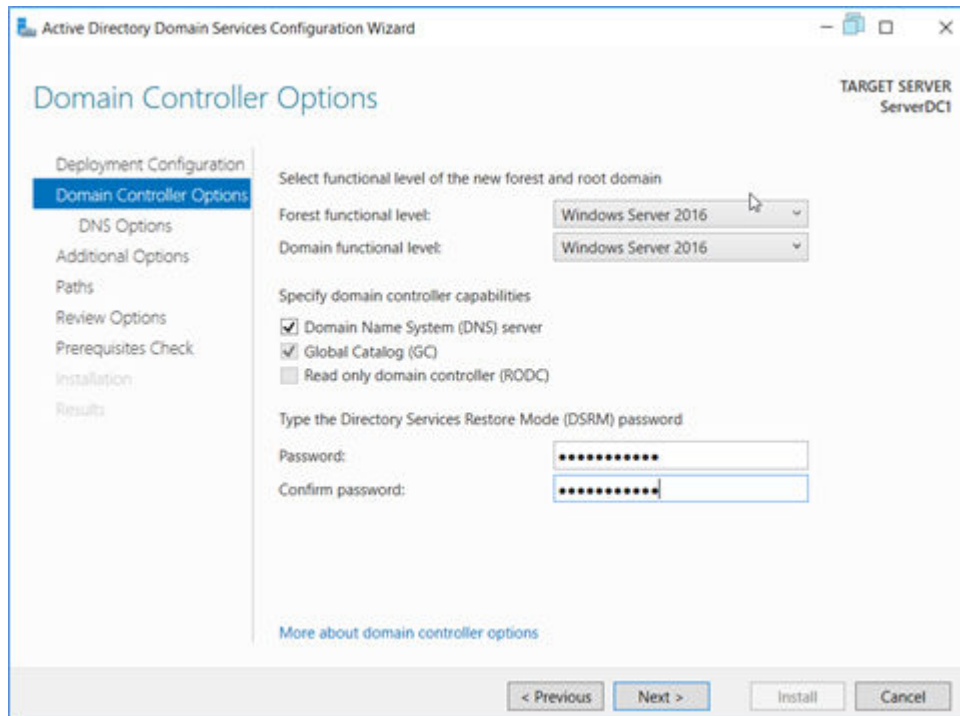


[sc_Adding new forest, 1, en_US]

Figure 4-16 Adding New Forest

- ✧ In the **Domain Controller Options**, select **Windows Server 2016** as **Forest functional level** and **Domain functional level**.
- ✧ In the **Type the Directory Service Restore Mode (DSRM) password** section, enter a strong password in the **Password** and **Confirm password** text boxes.
- ✧ Tick the box **Domain Name System (DNS) server**.

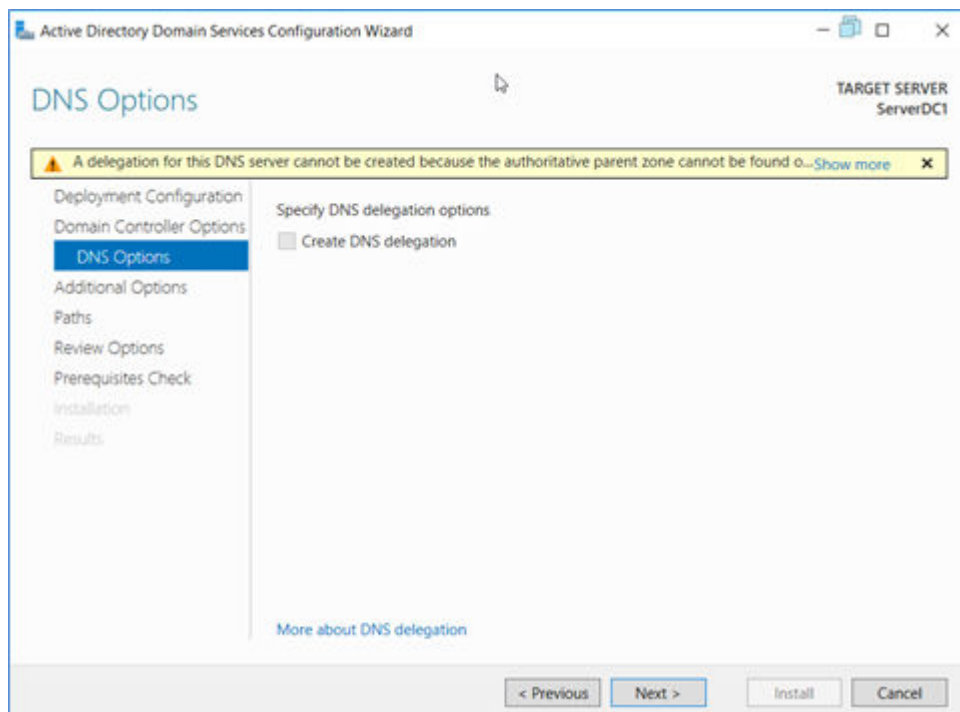
The **Global Catalog (GC)** option is checked and not an option because this is the only DC so far in this domain, so it has to be a Global Catalog server. The **Read only domain controller (RODC)** option is deselected because you have to have another non-RODC on the network to enable this option.



[sc_Selecting PDC options, 1, en_US]

Figure 4-17 Selecting PDC Options

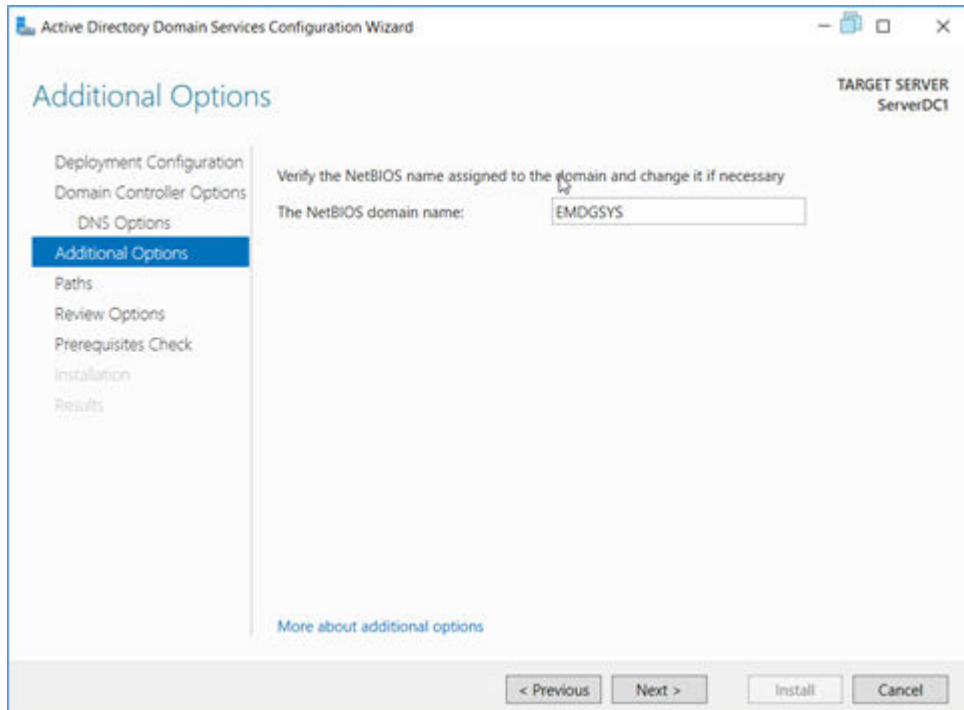
✧ Click **Next** to continue.



[sc_DNS options, 1, en_US]

Figure 4-18 DNS Options

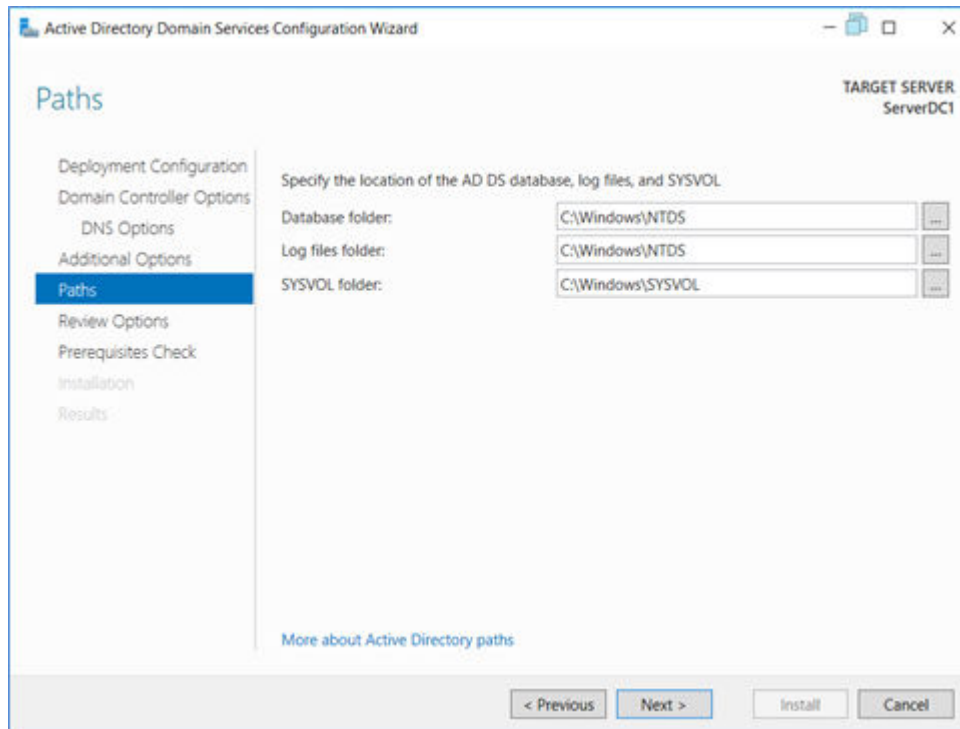
- ✧ In the **DNS Options**, you will be informed that a delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. The reason is that this is the first DC on the network. Click **Next** to continue.
- ✧ In the **Additional Options**, confirm the **NetBIOS domain name**.



[sc_Additional Options, 1, en_US]

Figure 4-19 Additional Options

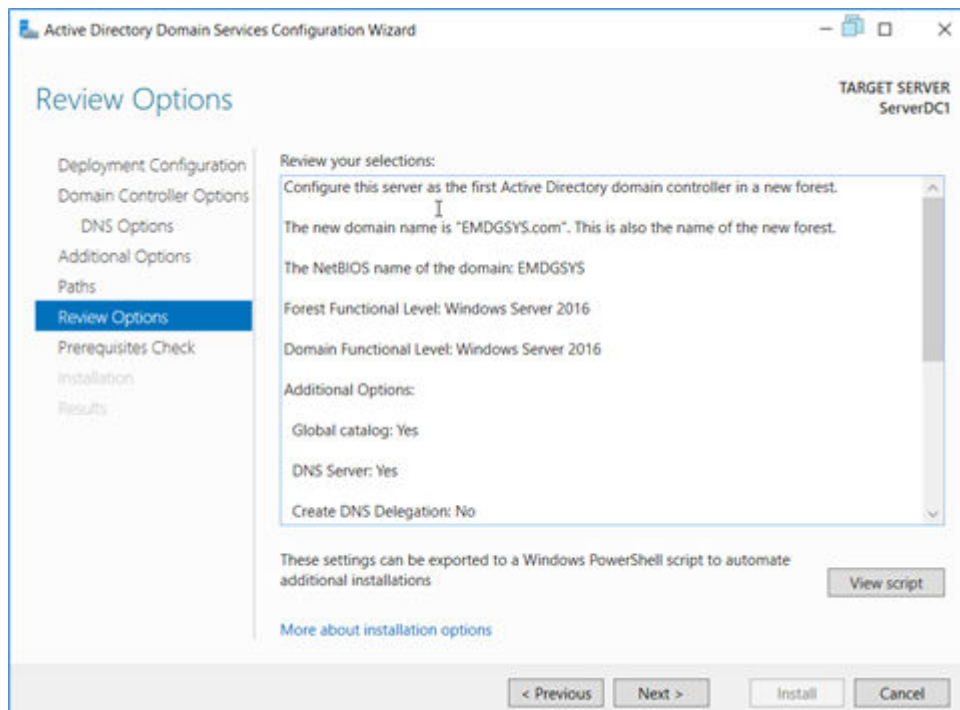
- ✧ In **Paths**, leave the **Database folder**, **Log files folder**, and **SYSVOL folder** in their default locations and click **Next**.



[sc_Selecting file paths, 1, en_US]

Figure 4-20 Selecting File Paths

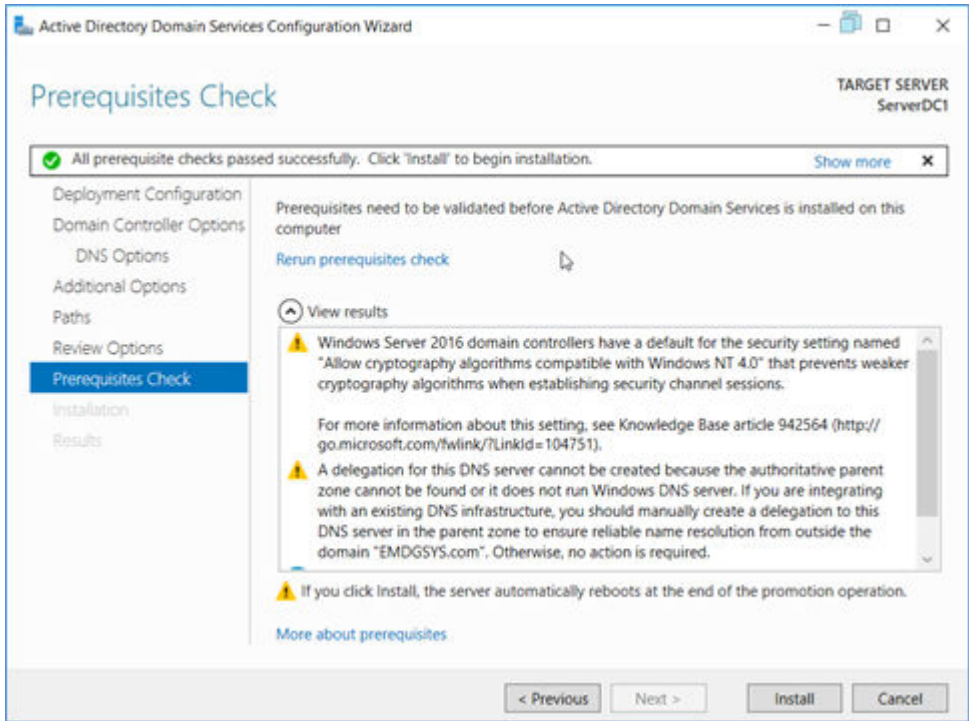
✧ In **Review Options**, confirm the information and click **Next**.



[sc_Review Option PDC, 1, en_US]

Figure 4-21 Review Options PDC

✧ In **Prerequisites Checks**, check all prerequisites checks and click **Install**.



[sc_Prerequisite Check PDC, 1, en_US]

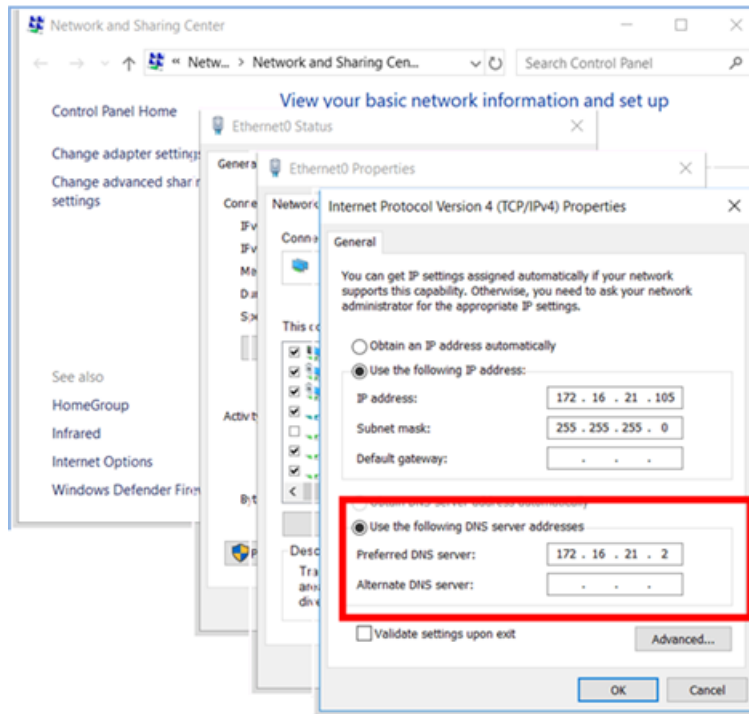
Figure 4-22 Prerequisite Check PDC

The machine will automatically restart since we selected that option. The installation will be complete when you log on. The DNS service was installed during Active Directory installation.

4.2.3 Domain

4.2.3.1 Adding Clients to the Domain

- ✧ Set the Domain Controller IP Address as the DNS Server.

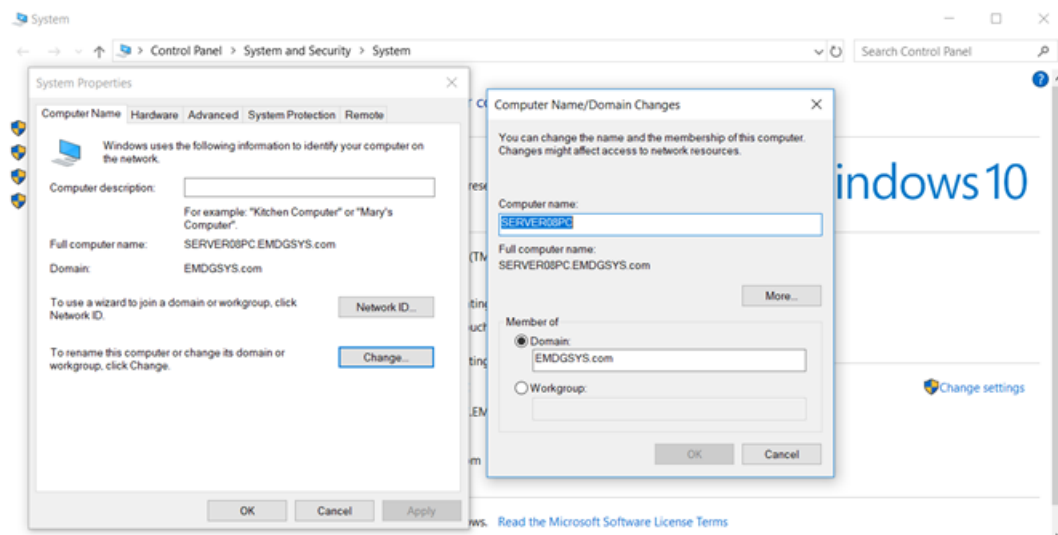


[sc_Setting Domain Controller IP Address, 1, en_US]

Figure 4-23 Setting Domain Controller IP Address

Adding the PC to the Domain

- ✧ Go to **Control Panel** → **System** → **Computer name, domain, and workgroup settings** and click **Change Settings**.
- ✧ Go to the Tab **Computer Name** and click **Change...**.
Tick **Domain** and fill in the name of the domain you want to join.
- ✧ Click **OK**.
If the Domain is not enabled to be ticked, change the computer name first, restart, and then retry this step.

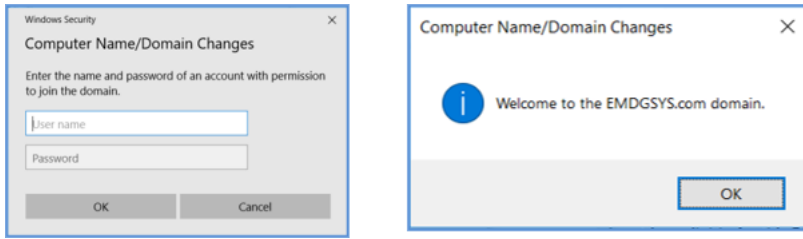


[sc_Adding a Computer to Domain, 1, en_US]

Figure 4-24 Adding a Computer to Domain

- ✧ To complete the task and join the domain, if asked, you must provide the domain admin user and password.

A welcome screen will be displayed on the computer after successful ingress to the domain. The restarting of the client machine is mandatory.



[sc_Enter Password and Finish Setting up, 1, en_US]

Figure 4-25 Enter Password and Finish Setting Up

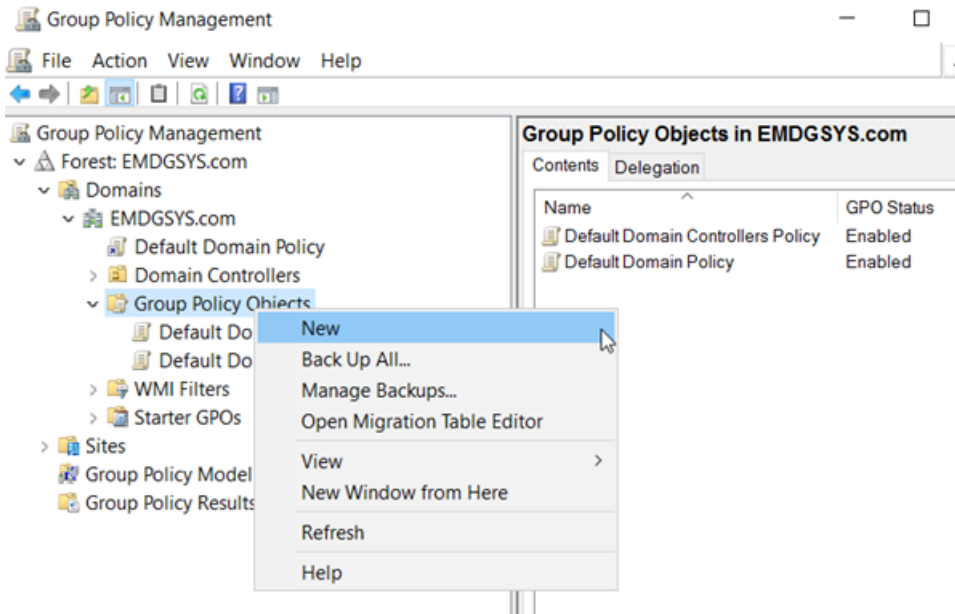
4.2.3.2 Group Policies (Domain)

If there are group policies objects (GPOs) to be associated with created domains, this section may help with instructions about their actualization and management.

4.2.3.3 Group-Policy Management

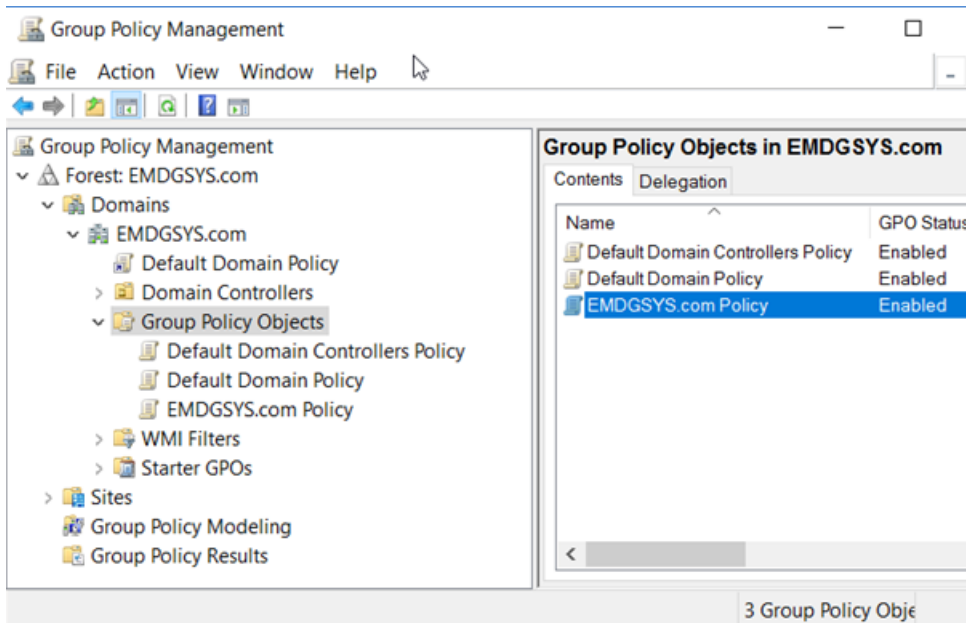
To set up the Group Policies for the domain, proceed as follows:

- ✧ Go to **Start** → **Windows Administrative Tools** → **Group Policy Management**.
- ✧ Expand the left tree underneath **Forrest: <Domain>**, **Domains**, and your local Domain.
- ✧ Under **Group Policy Object**, you will find the **Default Domain Policy**. Here, we will insert a new policy with personalized settings for the domain.
- ✧ Right-click the folder **Group Policy Object** and select **New**.
- ✧ Insert a name and click **OK** (for example, **EMDGSYS.com Policy**).



[sc_Adding Group policy Objects, 1, en_US]

Figure 4-26 Adding Group Policy Objects

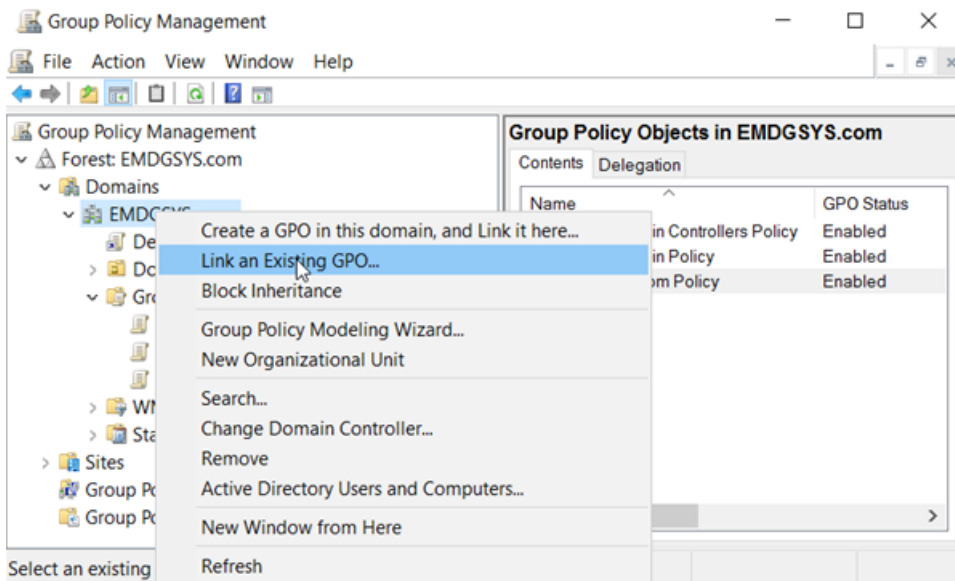


[sc_Selecting GPO, 1, en_US]

Figure 4-27 Selecting GPO

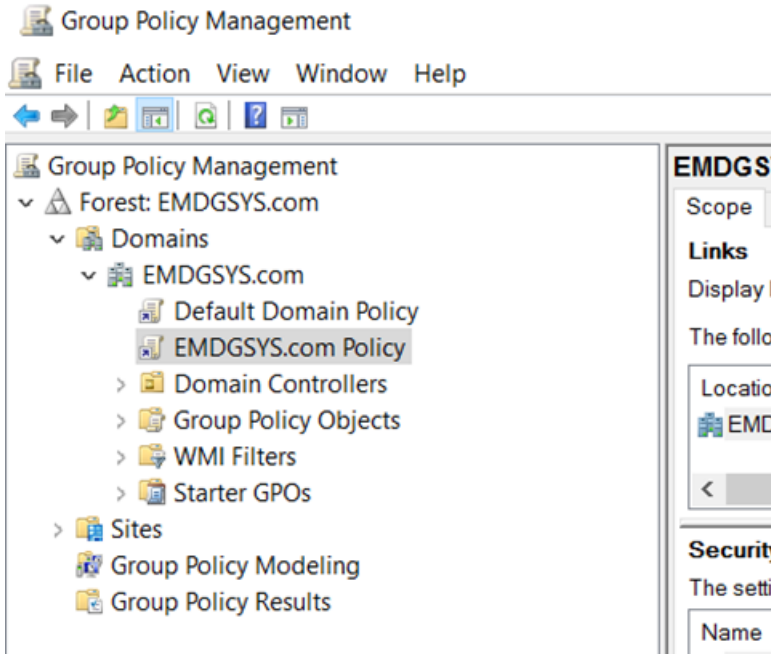
Now, the policy needs to be linked with the domain.

- ✧ Go in the tree one level higher, right-click the folder with your domain name (in our example **EMDGSYS.com**), select **Link an Existing GPO...** and select your previously created **Group Policy Object**.



[sc_Linking existing GPO, 1, en_US]

Figure 4-28 Linking Existing GPO



[sc_Linking existing GPO Selecting Domain, 1, en_US]

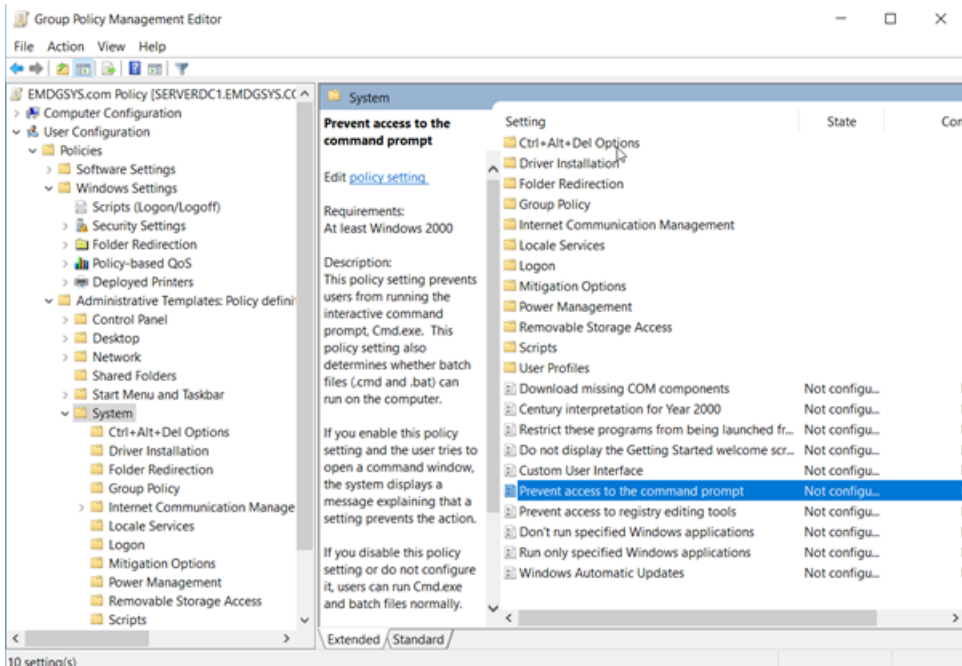
Figure 4-29 Linking Existing GPO Selecting Domain

- ❖ Repeat the steps for the folder **Domain Controllers**, one level underneath.

Modifying the Group Policy

Now we have to modify our own group policy.

- ❖ Right-click the object that we have created before and select **Edit...** to open the **Group Policy Management Editor**.



[sc_Linking existing GPO to Domain Controller, 1, en_US]

Figure 4-30 Linking Existing GPO to Domain Controller



NOTE

For more details on the group policies, refer to the chapter [3 System Hardening](#)

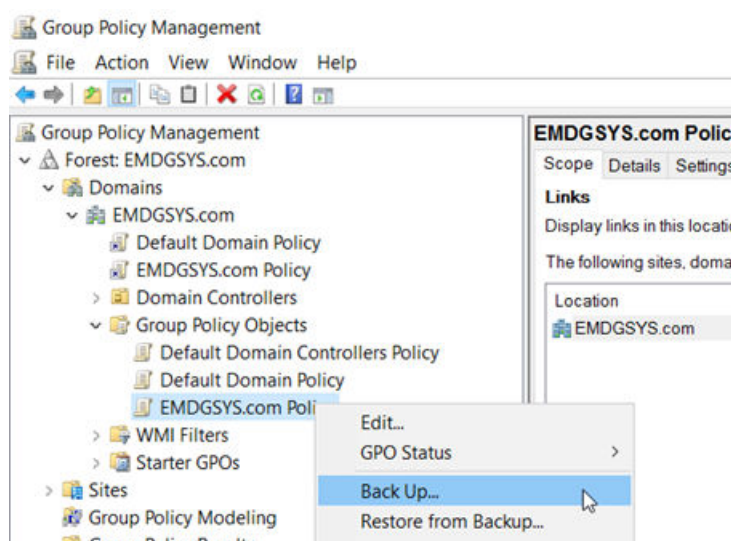
4.2.3.4 Group Policy Export/Import Function (Domain Controller)

The Group Policy (GP) Management offers a functionality for importing/exporting a group-policy object. This is maybe useful in case group policy changes are required

- ✧ Go to **Start** → **Administrative Tools** → **Group Policy Management**.
- ✧ Expand the left tree underneath **Forrest: <Domain>**, **Domains**, and your local Domain.
- ✧ Select your **Group Policy Object (GPO)**.

Export (Backup)

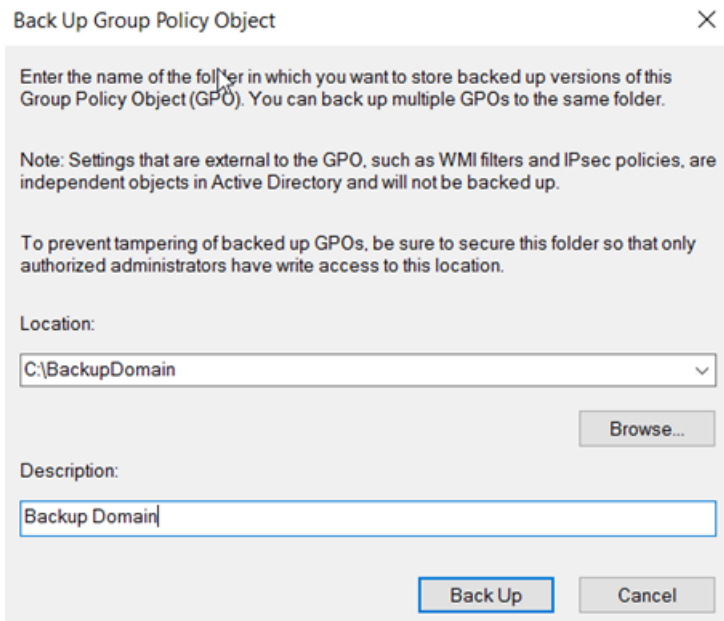
- ✧ Right-click the GPO you want export and select **Back Up...**



[sc_Exporting GPO, 1, en_US]

Figure 4-31 Exporting GPO

- ✧ Enter the **Location** and a **Description**.



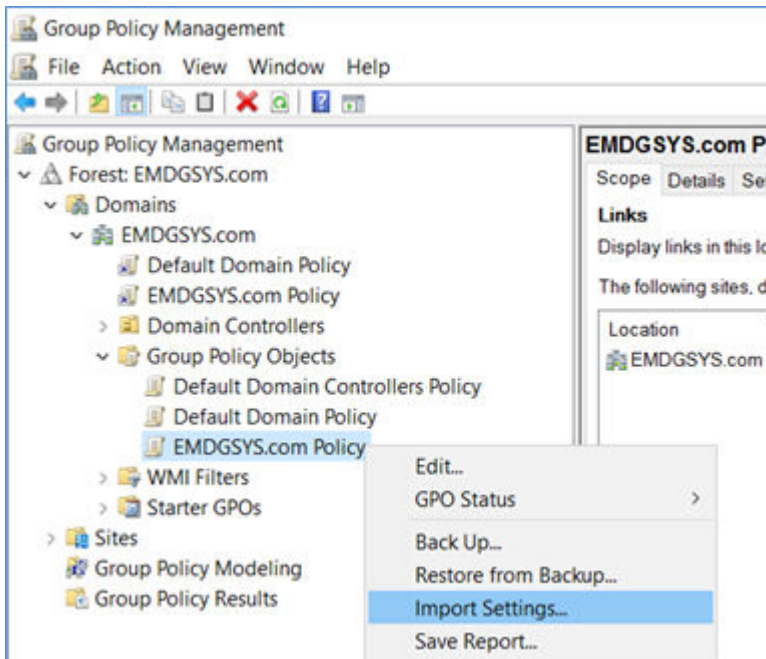
[sc_Choosing export location, 1, en_US]

Figure 4-32 Choosing Export Location

- ✧ Click **Back Up**.

Import

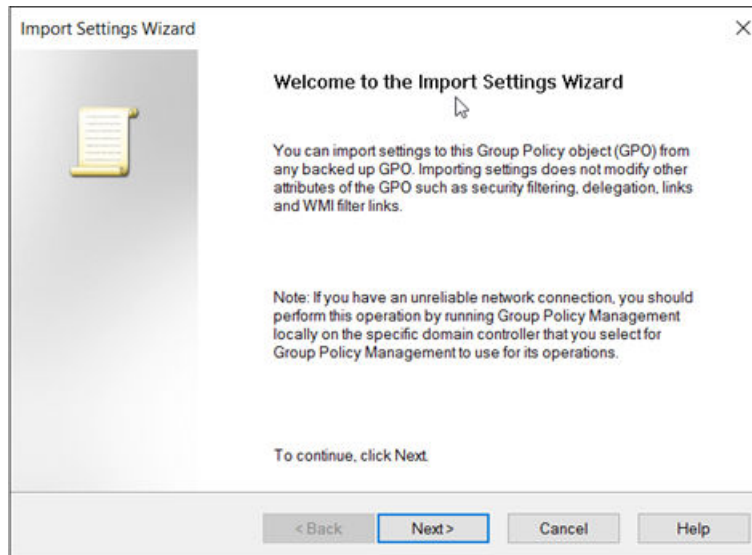
- ✧ Right-click the GPO you want to update with an import file.
- ✧ Select **Import Settings....**



[sc_Importing GPO, 1, en_US]

Figure 4-33 Importing GPO

A wizard will guide you through the rest of the process.



[sc_importing GPO Setting Wizard, 1, en_US]

Figure 4-34 Importing GPO Setting Wizard

The difference between a backup restore and the import is simple. Restore will replace the whole GPO with the backup file. An import will just modify the settings which are different from the GPO which will be updated. It is recommended to make always a backup before you make any Import.

4.2.3.5 DG Group Policy Object

The recommended group policies measures should come from the **remediation kits** provided by the Center for Internet Security (CIS). These remediation kits can patch the operating system with several security measures at once, avoiding time consuming and human mistakes during implementations.



NOTE

The GPO needs to be reviewed, adjusted, and verified per station according to the applicable project requirements. Some exceptions may exist and must be considered. You can use the recommended tooling Microsoft SCM version 3.0 (or greater) to view, update, import and export, compare, and duplicate security and compliance baselines.

4.2.4 Read-Only Domain Controller

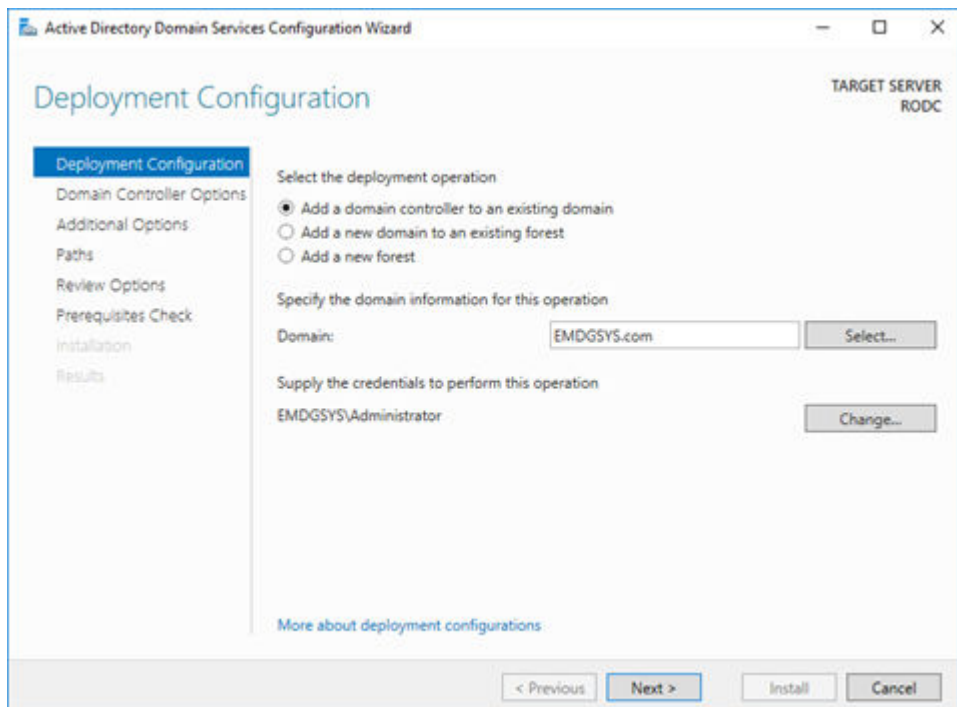
4.2.4.1 Setting the Read-Only Domain Controller (RODC)

The RODC runs on a Windows Server 2019 operating system. Refer to <http://www.rebeladmin.com/2014/10/step-by-step-guide-to-install-read-only-domain-controller-rodcl>

Configuring IP Setting and Adding the Server

After OS installation, configure the IP setting and add the server to the Active Directory.

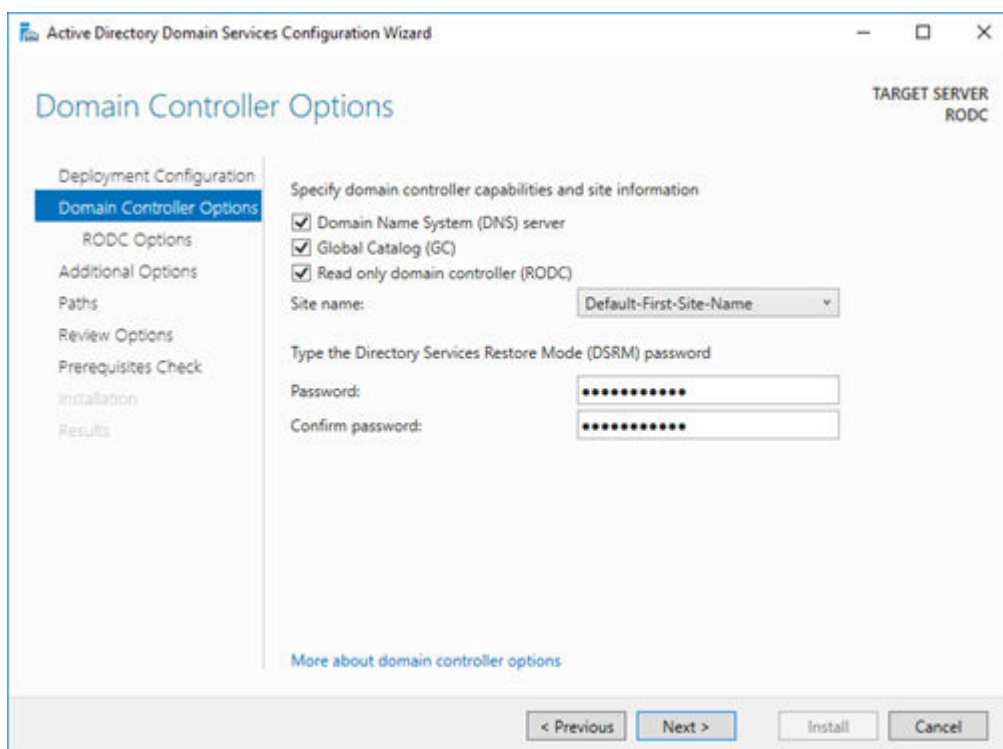
- ✧ In the **Server Manager Dashboard**, go to the **AD DS** tab.
- ✧ There is a notification under a yellow background **Configuration required for Active Directory Domain Services**. Select **More**.
- ✧ In the **All Servers Task Details and Notifications** window, select **Promote this server to a domain...** to open next window.
- ✧ In the **Active Directory Domain Services Configuration Wizard** window, select **Add a domain controller to an existing domain** and click **Select...** to specify the domain information.



[sc_RODC Deployment Configuration, 1, en_US]

Figure 4-35 RODC Deployment Configuration

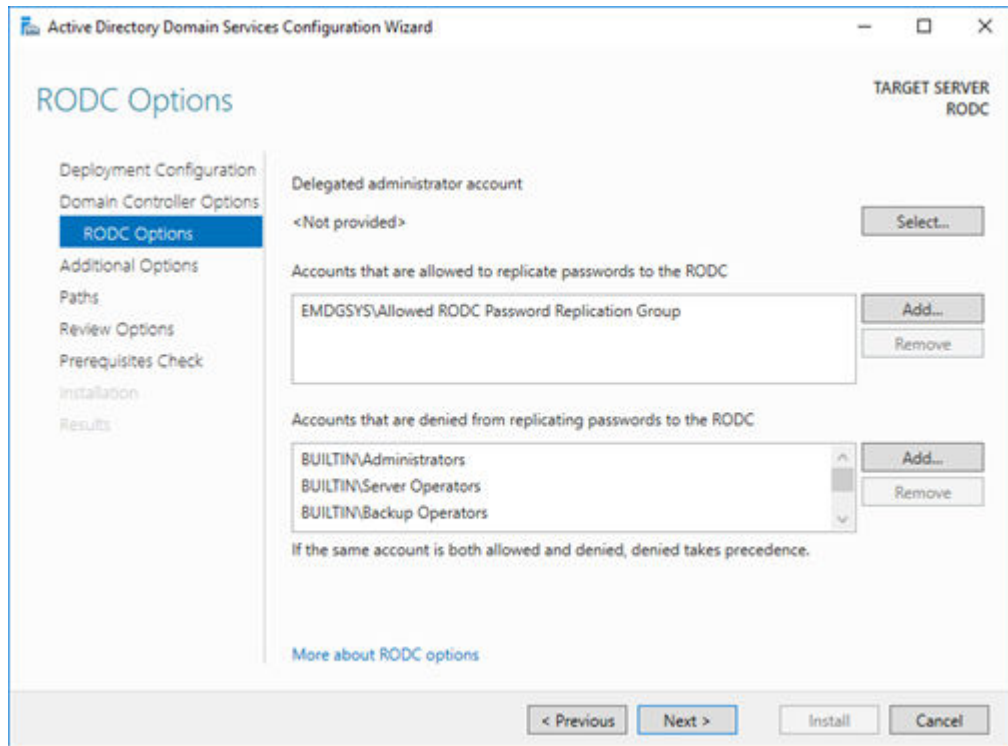
✧ There are 3 checkboxes that should be selected, then fill passwords fields.



[sc_Setting up RODC Domain Controller Options, 1, en_US]

Figure 4-36 Setting Up RDOC Domain Controller Options

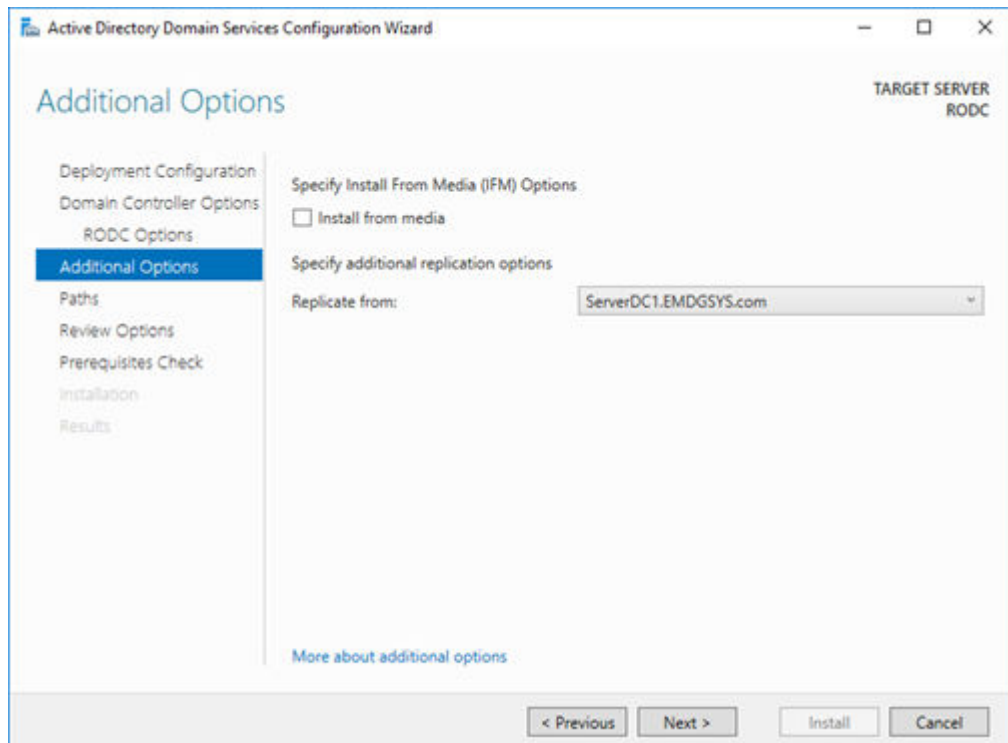
✧ In the **RODC Options**, keep the default configuration.



[sc_RODC options, 1, en_US]

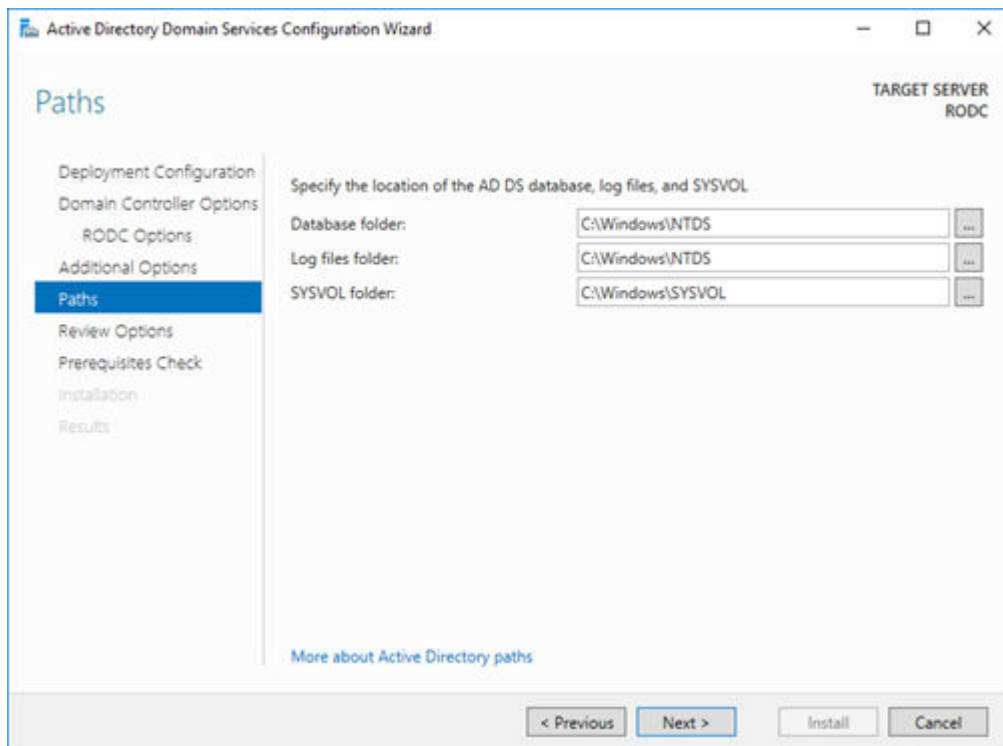
Figure 4-37 RODC Options

- ✧ In the **Additional Options** and in **Paths**, again keep default configuration and continue with **Next** until it allows you to begin installation.



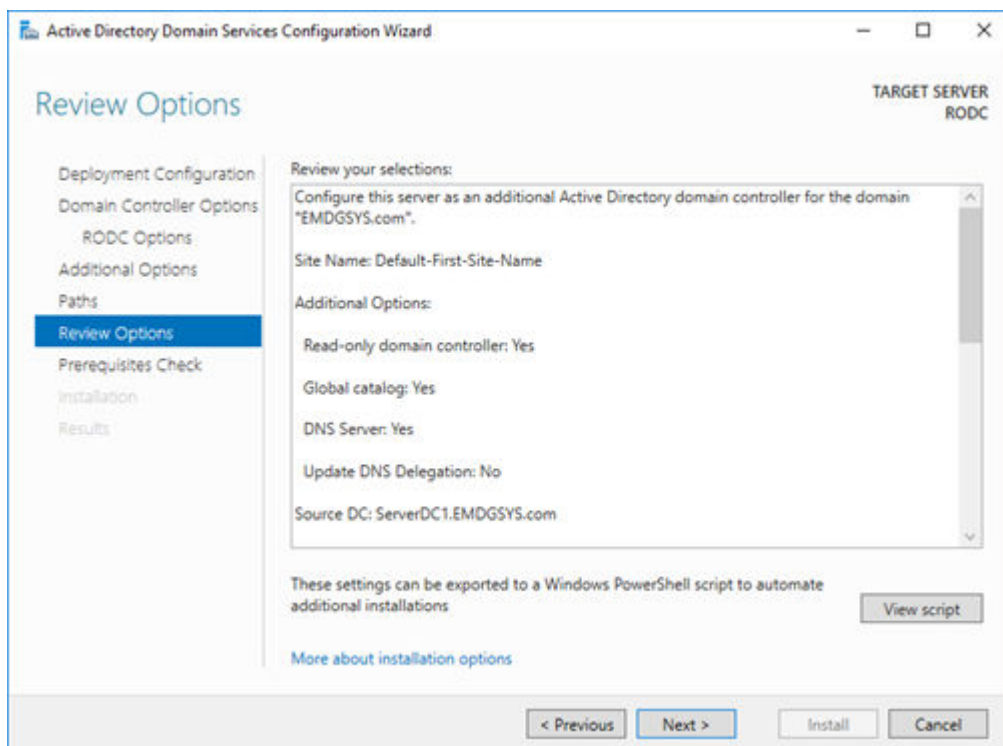
[sc_RODC Additional Options, 1, en_US]

Figure 4-38 RODC Additional Options



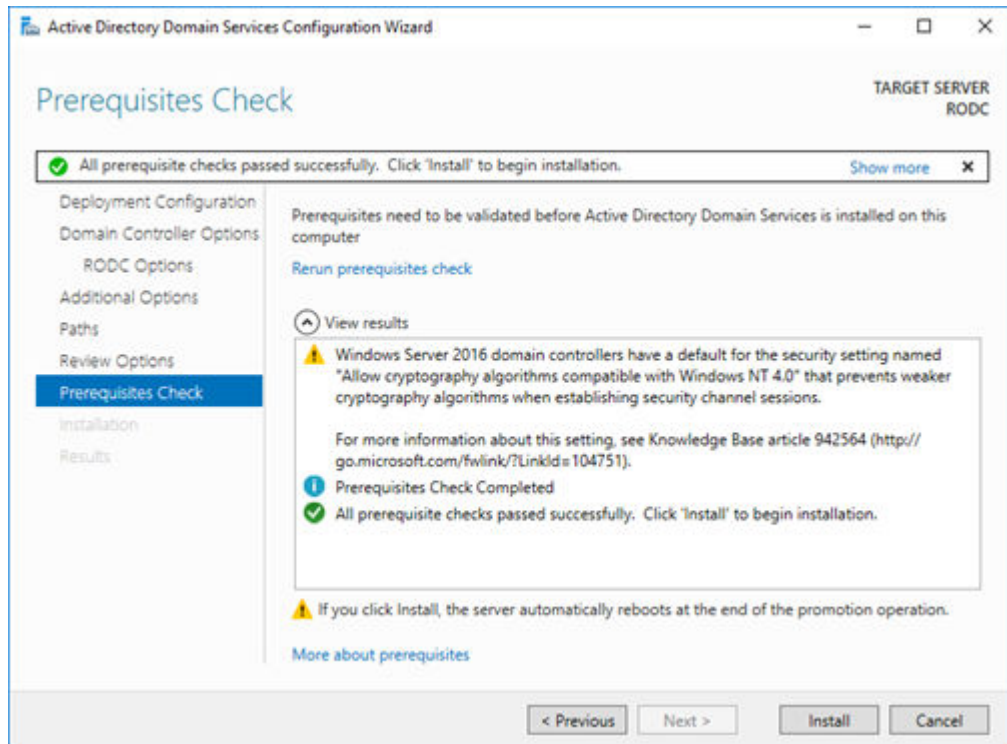
[sc_Selecting Additional Options Paths, 1, en_US]

Figure 4-39 Selecting Additional Options Paths



[sc_Review Option RODC, 1, en_US]

Figure 4-40 Review Options RODC



[sc_Prerequisite Check RODC, 1, en_US]

Figure 4-41 Prerequisite Check RODC

After the installation, the system reboots.

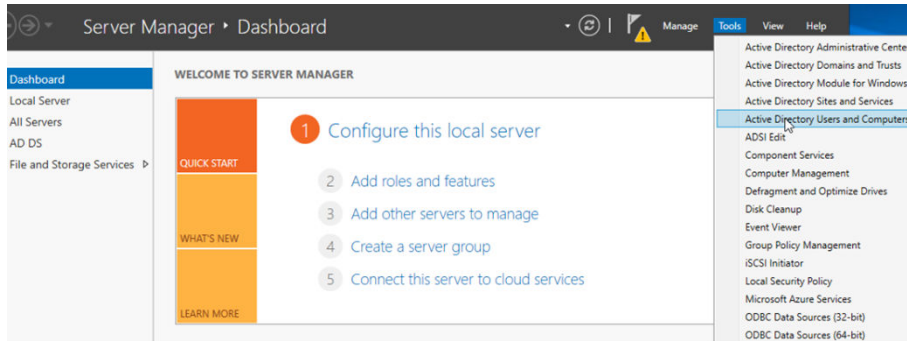
4.2.4.2 Force Replication Manually

- ✧ Start your command prompt with administrative privileges and execute:
repadmin /replicate RODC SERVERDC1 DC=EMDGSYS,DC=com /readonly
Where
RODC: destination server
SERVERDC1: source server
DC=EMDGSYS,DC=com: the naming context for the EMDGSYS.com forest
- ✧ For replication of all Domain Controllers:
repadmin /syncall /AeD

4.2.4.3 Password Replication Policy (PRP)

In Windows Server to configure, we can use 2 security groups it creates with RODC setup. According to Microsoft, it is as following:

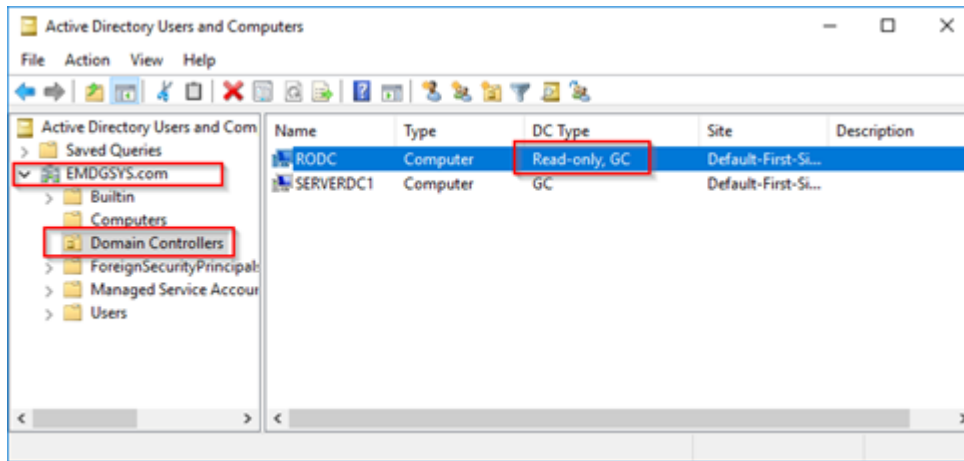
- **Allowed RODC Password Replication Group:**
Members of this group are placed in the **Allow** list of the Password Replication Policies of all RODCs by default.
 - **Denied RODC Password Replication Group:**
Members of this group are placed in the **Deny** list of the Password Replication Policies of all RODCs by default. Some of the groups include administrators, server operators, backup operators, account operators, and Denied RODC Password Replication Group.
- ✧ Log in to a writable domain controller with domain administrator account.
 - ✧ Go to **Server Manager** → **Tools** → **Active Directory Users and Computers**.



[sc_Configuring RODC Deny List, 1, en_US]

Figure 4-42 Configuring RODC Deny List

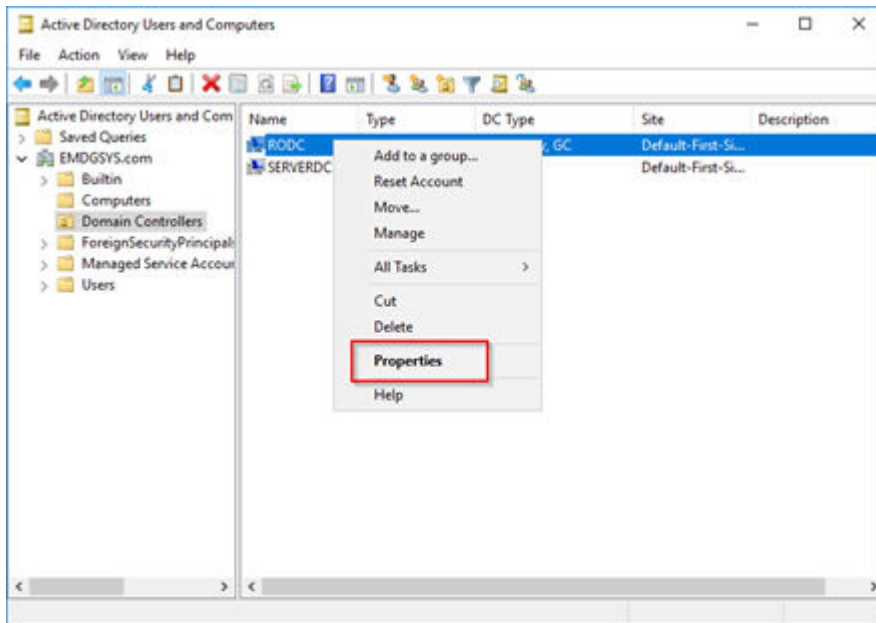
- ✧ Go to **Domain Controllers** or click to select the RODC you need to configure PRP.



[sc_Domain Controller, 1, en_US]

Figure 4-43 Domain Controller

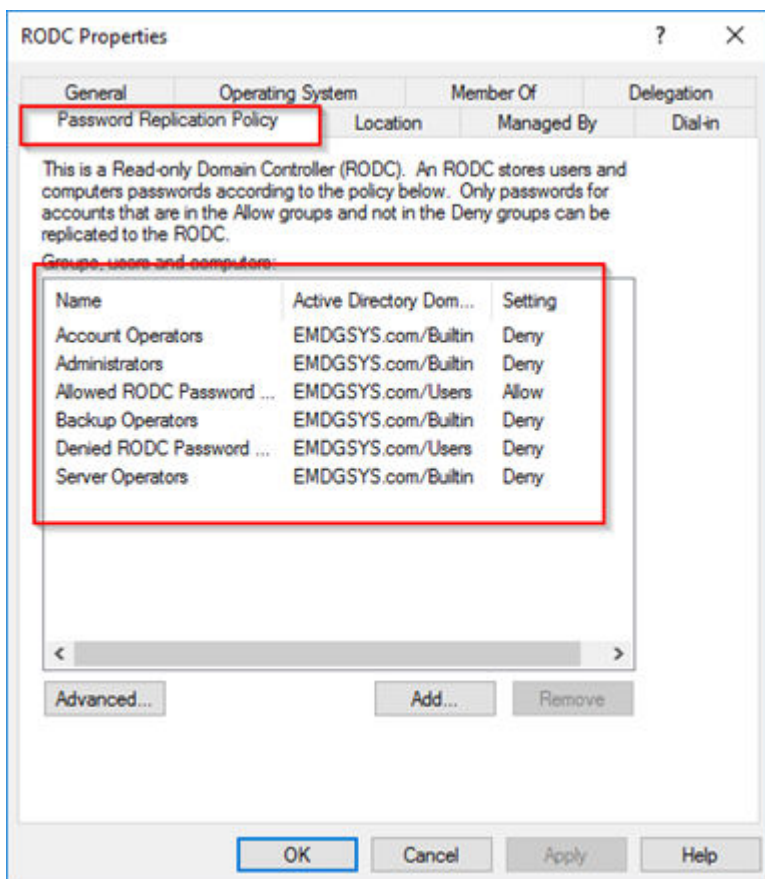
- ✧ Right-click and select **Properties**.



[sc_RODC properties, 1, en_US]

Figure 4-44 RODC Properties

- ✧ In **Properties**, go to the **Password Replication Policy** tab. There are the 2 groups mentioned.



[sc_RODC Password Replication Policy, 1, en_US]

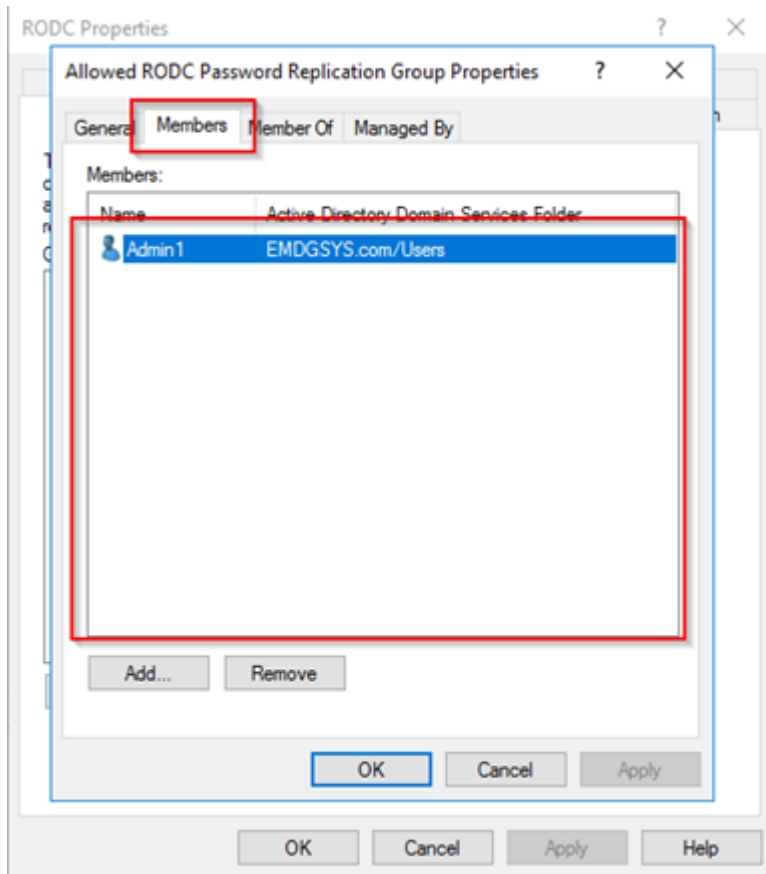
Figure 4-45 RODC Password Replication Policy



NOTE

By default, there are more groups than the 2 shown. Make sure that you add only the groups which are really needed. Remember that **Deny** goes over **Allow**.

- ✧ To add users/computers to those groups, double-click the group and select the **Members** tab.
- ✧ Click **Add** and **OK** to confirm changes.



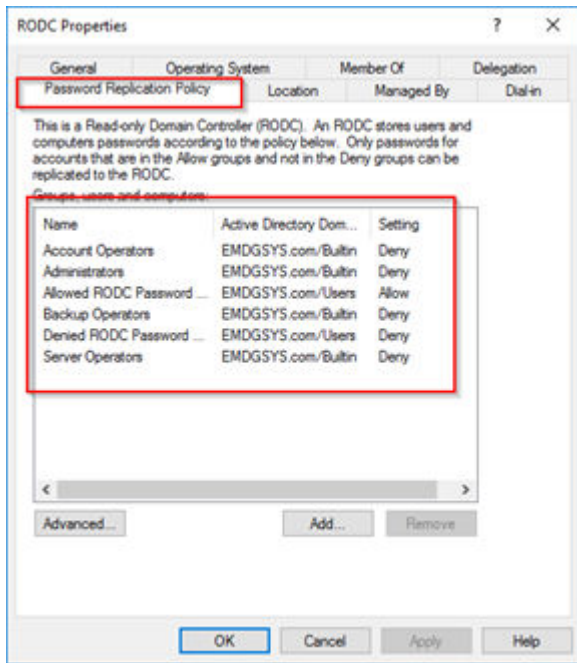
[sc_RODC Members. 1, en_US]

Figure 4-46 RODC Members

Policy Usage Reports and Prepopulate Credential Caching

Microsoft provided an easy method of reporting where we can check the status of password replication. To use this facility, follow the following steps.

- ✧ Log in to a writable domain controller with the domain administrator account.
- ✧ Go to **Server Manager** → **Tools** → **Active Directory Users and Computers**.
- ✧ Go to **Domain Controllers** OU and select the RODC you need to configure PRP.
- ✧ Right-click and select **Properties**.



[sc_Password Replication Policy Setting, 1, en_US]

Figure 4-47 Password Replication Policy Setting

✧ In **Properties**, go to the **Password Replication Policy** tab and click **Advanced**.

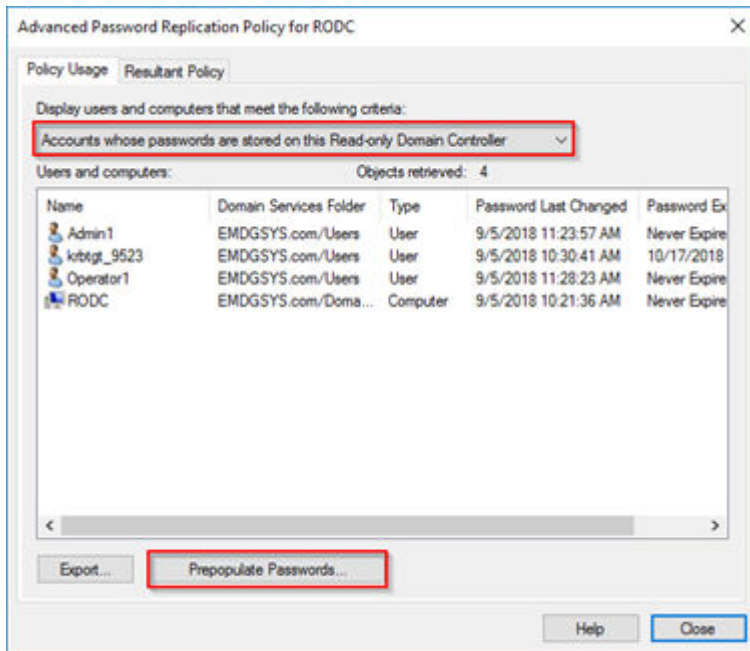
In the drop-down list, there are 2 options listed under the **Policy Usage** tab:

Accounts whose passwords are stored on this Read-Only Domain Controller:

This option will list all the user accounts/computer accounts which are currently cached password on RODC.

Accounts that have been authenticated to this Read-Only Domain Controller:

This option will list the user accounts/computer accounts which were forwarded to writable domain controller for authentication and service tickets process. This is a good place to identify the user accounts/computer accounts which will still need to be added to the **Allow** list for password caching.



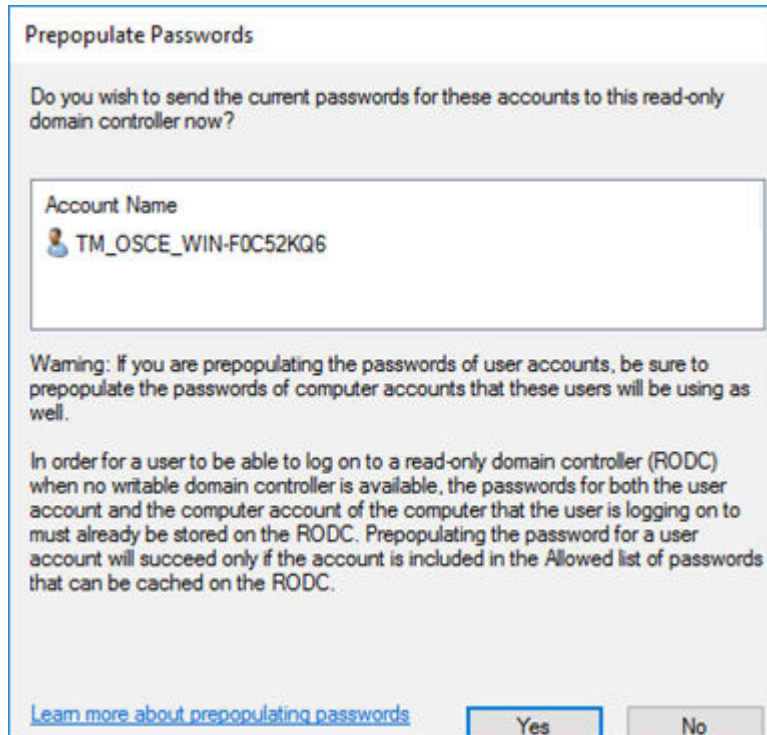
[sc_Prepopulate Passwords, 1, en_US]

Figure 4-48 Prepopulate Passwords

Remember, the RODC will cache credentials once you have made the first authentication request to the RODC. But Microsoft gives an opportunity where we can prepopulate the caching. So, when you log in for the first time, your password is already cached on RODC.

- ✧ To use this feature, click **Pre-Populate Passwords...**
- ✧ Select the accounts you need.
- ✧ Click **Yes** to accept the changes in the following dialog box.

Before doing this, make sure you have already allowed that user/computer account in the **Allow** list of the password caching.



[sc_Accepting Changes, 1, en_US]

Figure 4-49 Accepting Changes



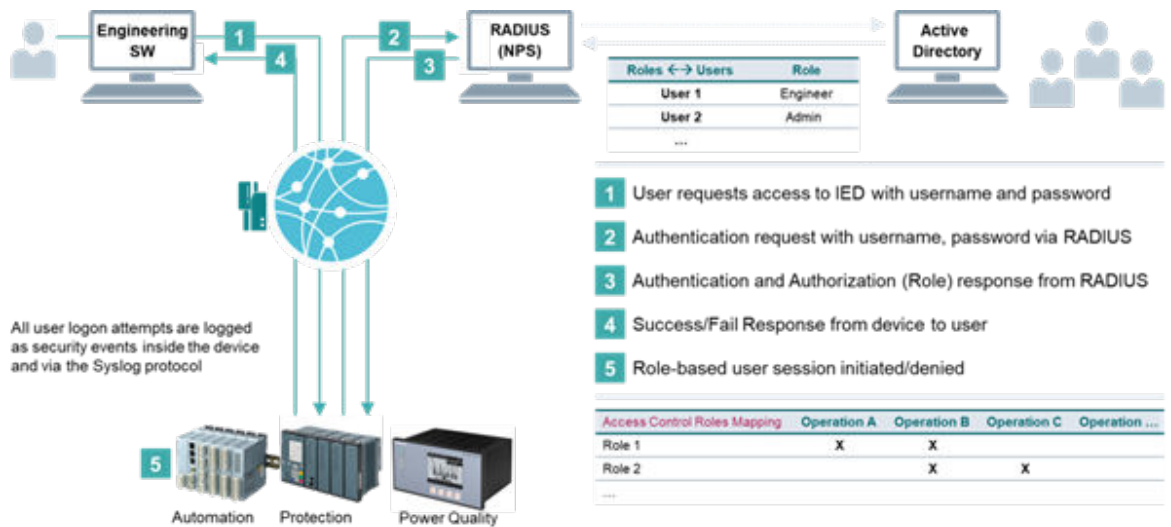
NOTE

Remember the **Allowed RODC Password Replication Group** needs to contain users/groups and computers of the site to where the RODC belongs.

If you have more than one site where a RODC is installed, it is recommended that you create an **Allowed RODC Password Replication Group** as many as sites you have with an initial of the site in the name of the group.

4.3 Role-Based Access Control for Field-Level Devices

The substation products SIPROTEC 5 and SICAM A8000 support role-based access control (RBAC) with central user management using the RADIUS/Active Directory. This role-based access control must be enabled in the SIPROTEC 5 or the SICAM A8000 device to authenticate and authorize user actions such as the access to information or to perform actions on the device. RADIUS is a standardized client/server protocol and the client implementation is integrated in the SIPROTEC 5 and SICAM A8000 device firmware. The following figure depicts the workflow of a RADIUS/Active Directory-Based Authentication/Authorization.



[sc_Role-Based Access Control to Field level Devices, 1, en_US]

Figure 4-50 Role-Based Access Control to Field Level Devices

Siemens has implemented the RADIUS protocol according to the IEC 62351-8 Ed.2 standard which includes the RADIUS implementation of role-based access control (RBAC).

To get more information, see [IEC Webstore](#) for Smart Grid Security.

4.3.1 Network Policy Server (NPS)

4.3.1.1 Network Policy Server for RADIUS

Network Policy Server (NPS) is the Microsoft implementation of a Remote Authentication Dial-In User Service (RADIUS) server. It is a client/server protocol that enables remote-access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service.

RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point. Having a central service also means that it is easier to track the usage for billing and for keeping network statistics. Created by Livingston (now owned by Lucent), RADIUS is a de facto industry standard used by several network product companies and is a proposed IETF standard.

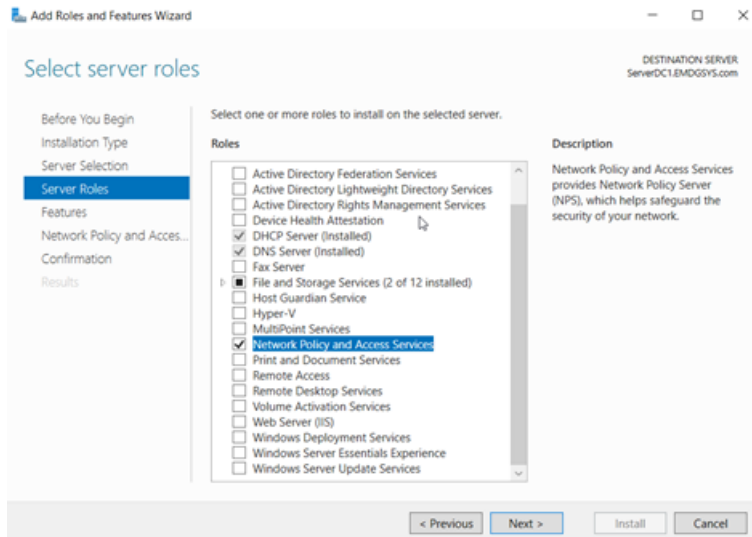
Table 4-1 Differences between Datacenter and Standard Edition from of Windows Server 2016

Feature	Standard Edition	Datacenter Edition
Network Access Connections (NPS)	50	Unlimited

4.3.1.2 Installation of Network Policy Server

Add the **Network Policy and Access Services** role to your domain controller:

- ✧ Go to **Server Manager** → **Manage** → **Add Roles and Features**.
- ✧ Select **Network Policy and Access Services** and click **Next**.



[sc_Network Policy Access Configuration, 1, en_US]

Figure 4-51 Network Policy Access Configuration

✧ Use the default settings and click **Install** in the last step.

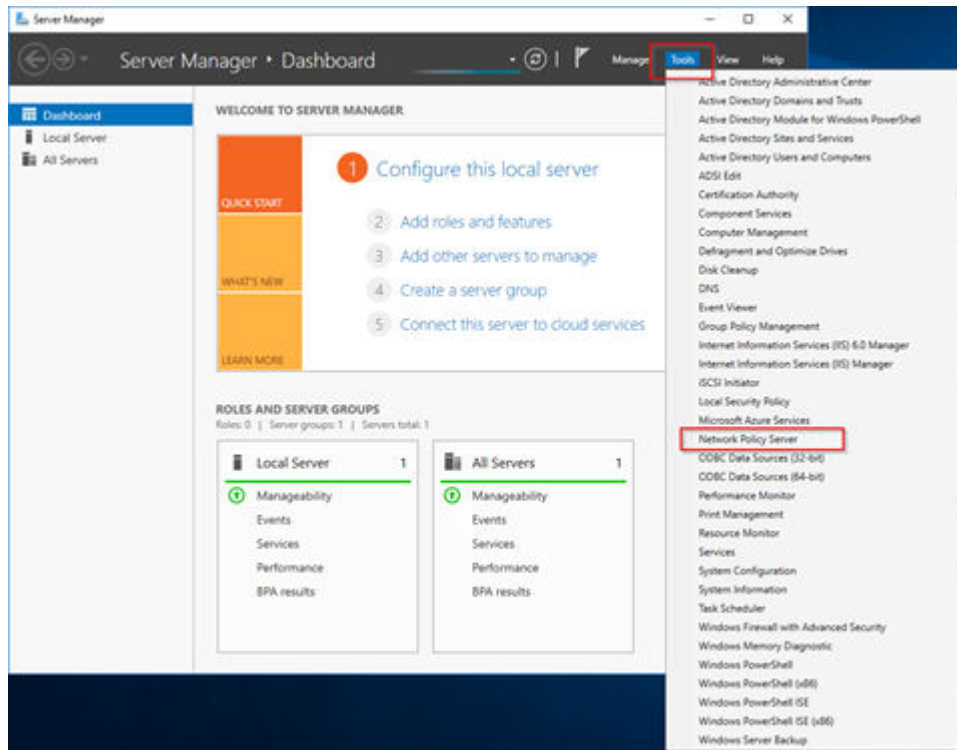
4.3.2 NPS Setup and Verification of Server Settings

4.3.2.1 Registering Network Policy Server in the Active Directory

It is necessary to register the Network Policy Server in the Active Directory. To do this, follow the steps below.

Register in Default Domain (Recommended)

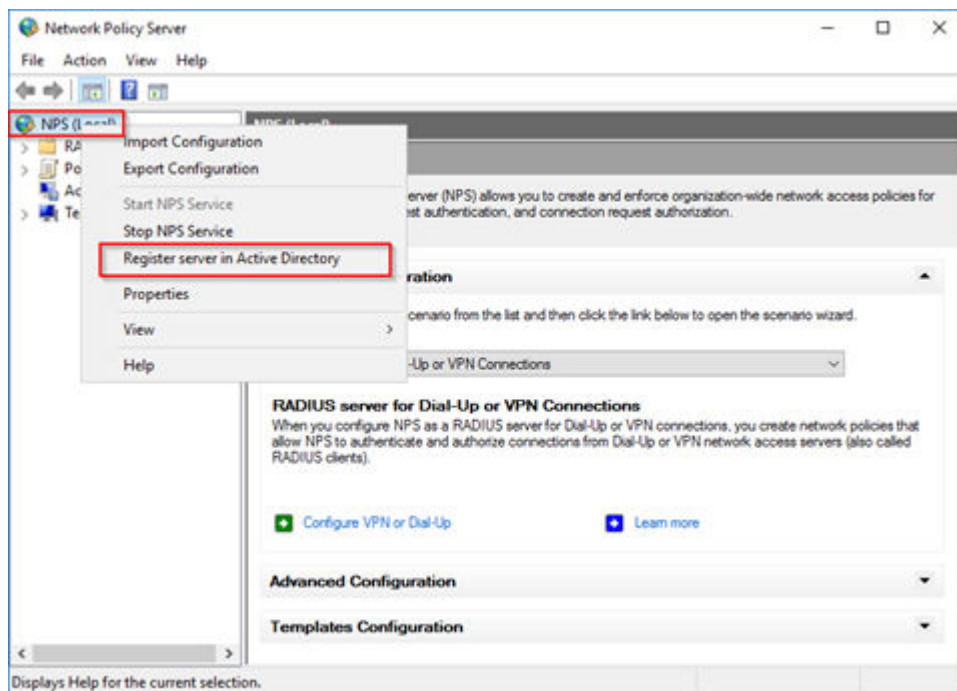
✧ Go to **Server Manager** → **Tools** → **Network Policy Server**.



[sc_Adding tasks, 1, en_US]

Figure 4-52 Adding Tasks

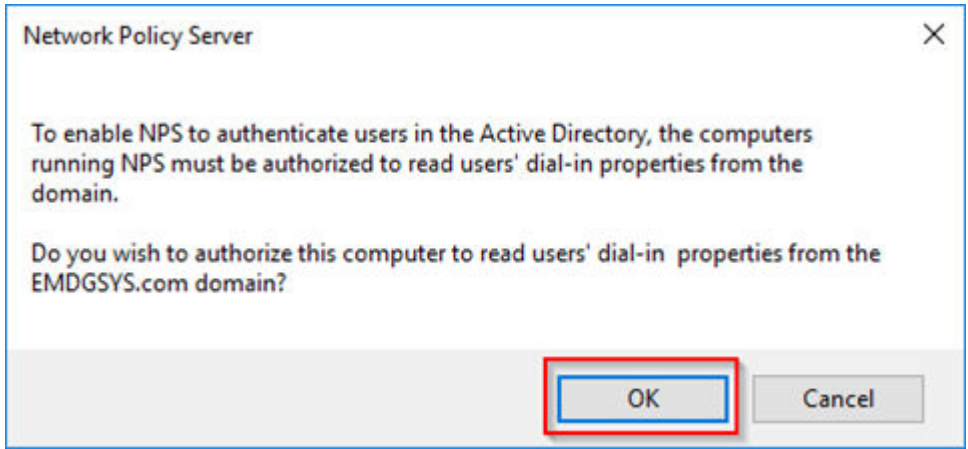
✧ Right-click in **NPS (Local)** → **Register server in Active Directory**.



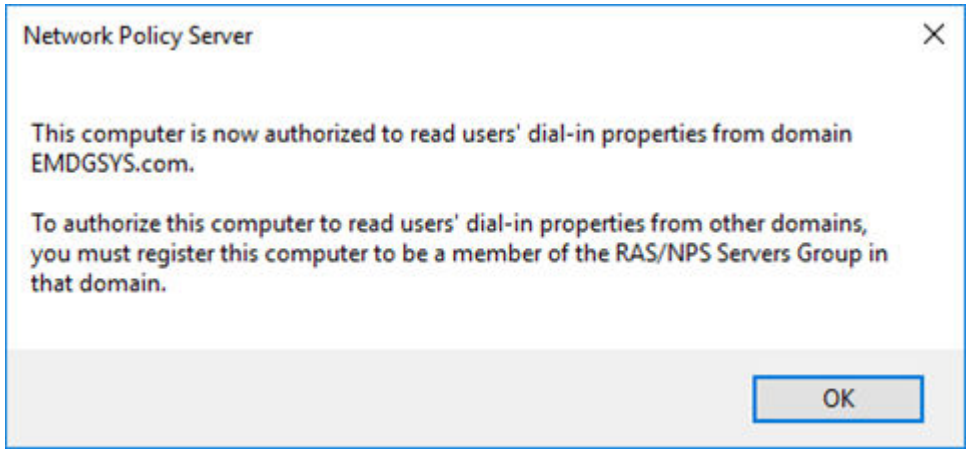
[sc_Registering Server in Active Directory, 1, en_US]

Figure 4-53 Registering Server in Active Directory

✧ In the dialog box that opens, finish the configuration by confirming the changes (OK).



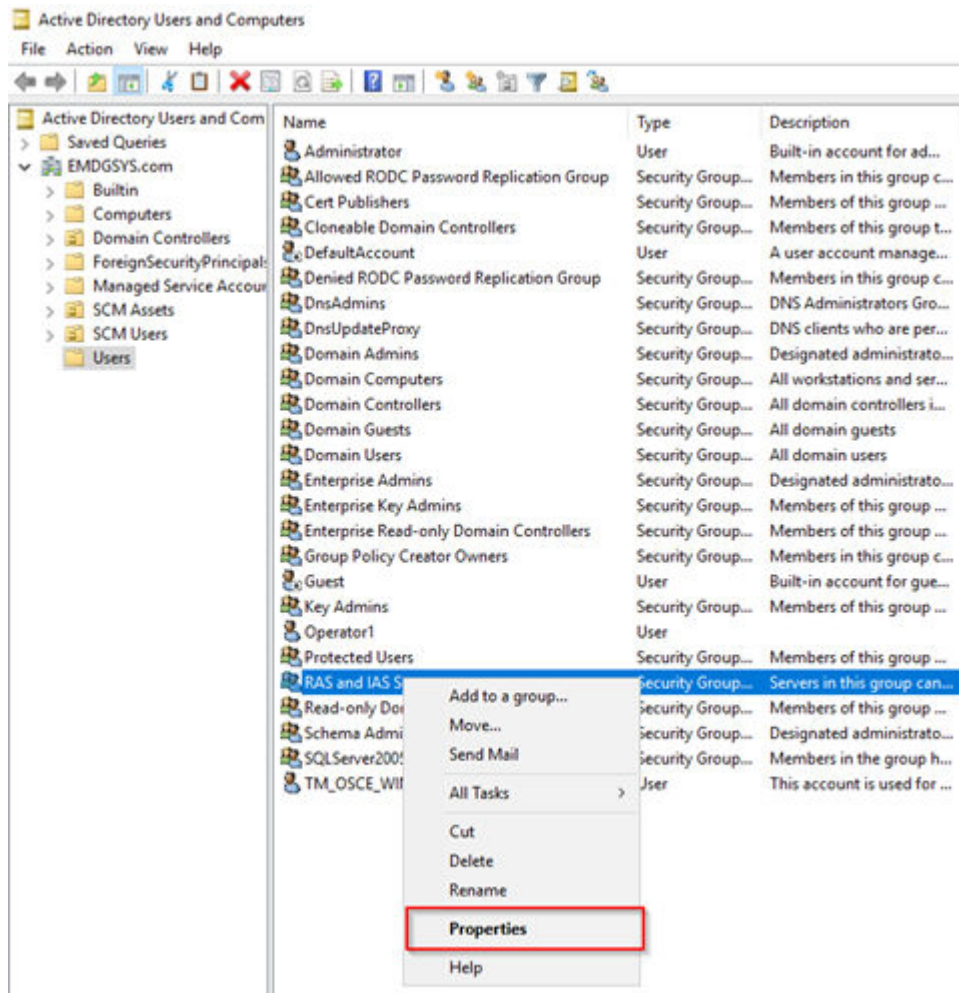
[sc_Confirming NPS Authorization, 1, en_US]
Figure 4-54 Confirming NPS Authorization



[sc_Enabling Network Policy Server Settings, 1, en_US]
Figure 4-55 Enabling Network Policy Server Settings

Register in Another Domain

- ✧ Go to **Server Manager** → **Tools** → **Active Directory Users and Computers**.
- ✧ Navigate to the domain where you want the NPS server to read user-account information and then click the **Users** folder.
- ✧ In details pane, right-click **RAS and IAS Servers** and select **Properties**.



[sc_Registering in Other Domain, 1, en_US]

Figure 4-56 Registering in Other Domain

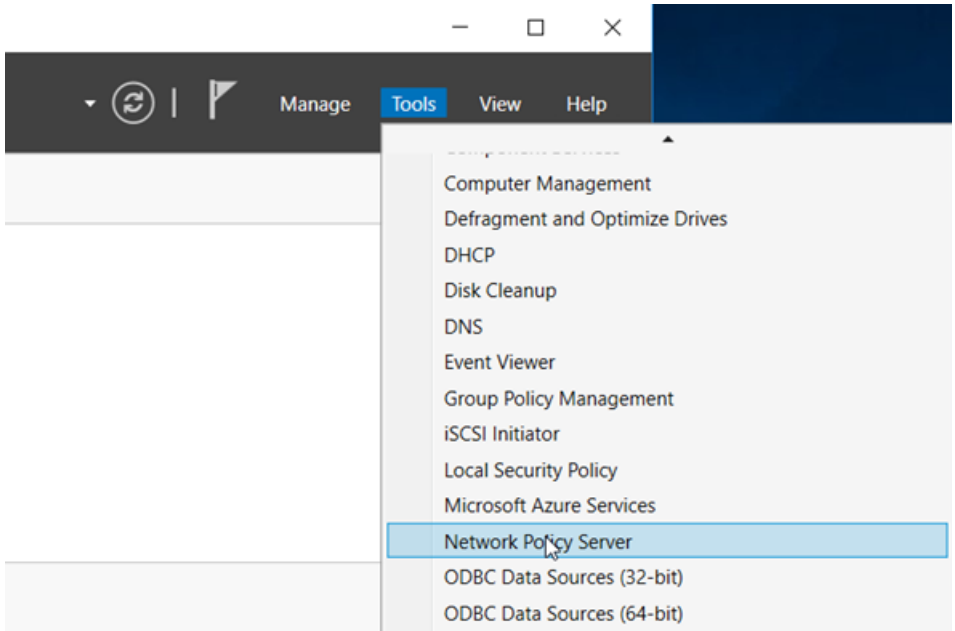
- ✧ In the dialog box, click the **Members** tab, add each of the NPS you want to register in the domain, and confirm the changes (**OK**).

Register using a Command Line

- ✧ `netsh nps add registeredserver [DNS_domain_name] [name_NPS_server]`

4.3.2.2 Port Numbers

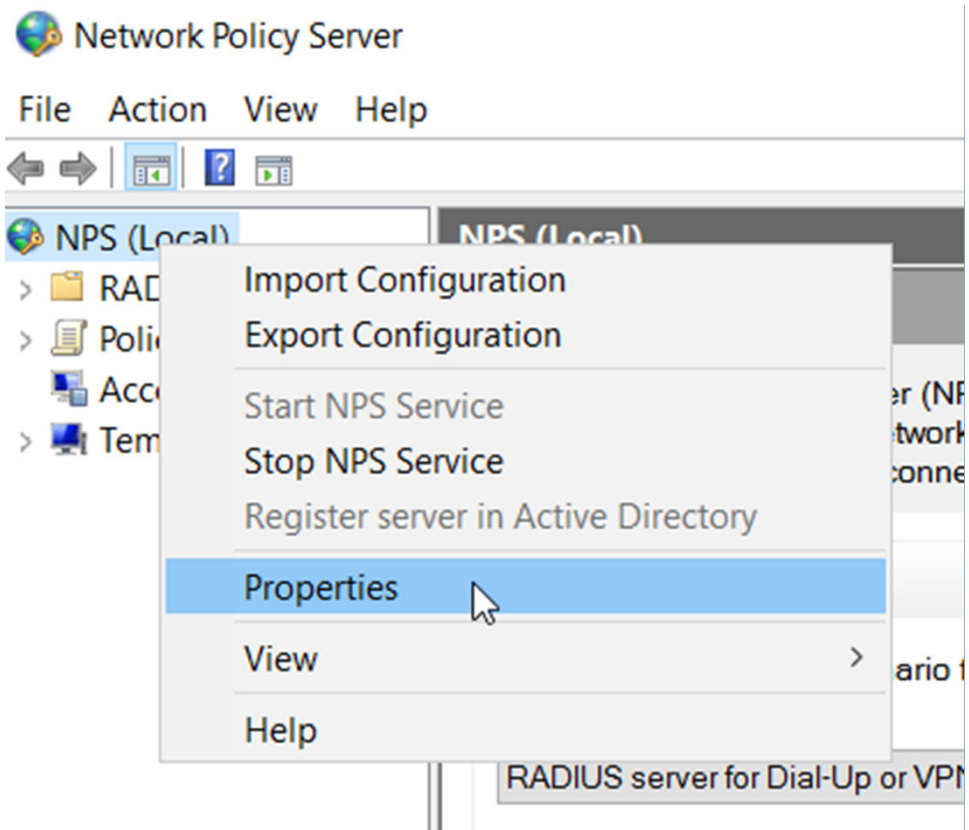
- ✧ Go to **Server Manager** → **Tools** → **Network Policy Server**.



[sc_Configuring Ports, 1, en_US]

Figure 4-57 Configuring Ports

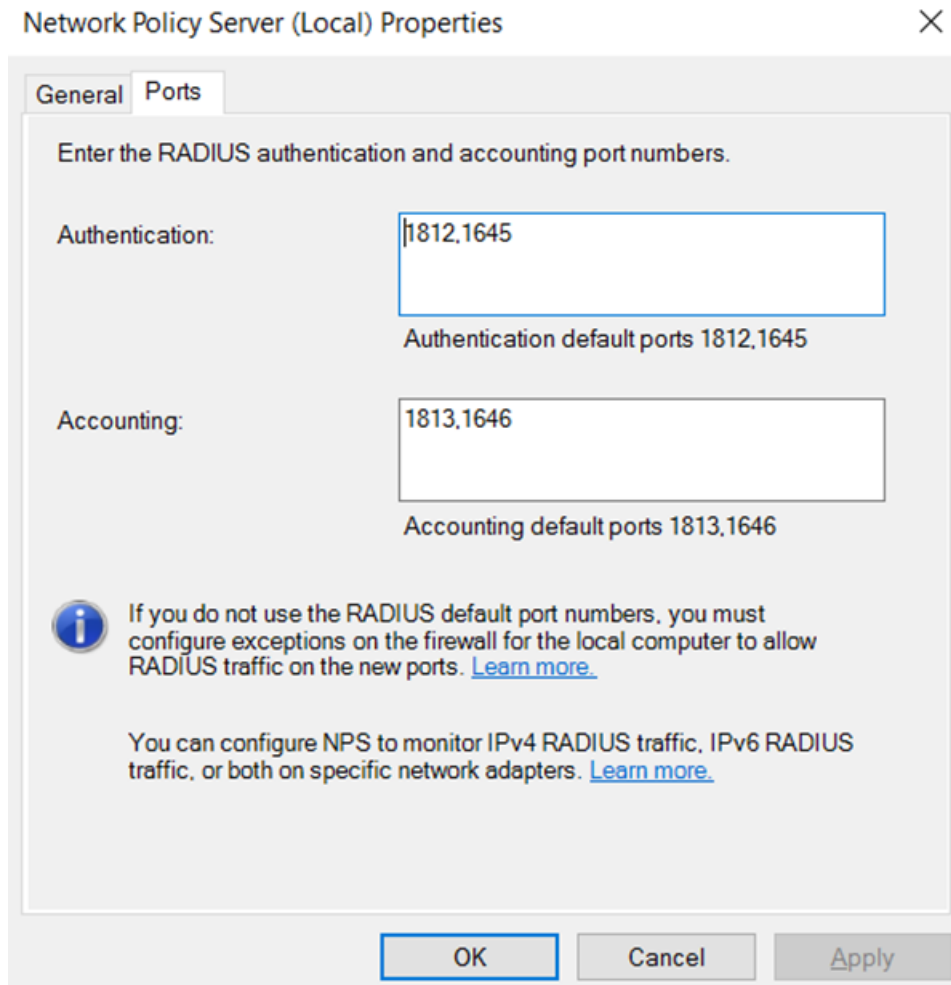
- ✦ Right-click in **NPS (Local)**, select **Properties** and go to the **Ports** tab.



[sc_NPS Properties, 1, en_US]

Figure 4-58 NPS Properties

- ✧ Verify the defaults for:
Authentication: 1812 and 1645 (optional)
Accounting: 1813 and 1646



[sc_NPS Properties Ports, 1, en_US]

Figure 4-59 NPS Properties Ports

4.3.2.3 Policies

2 sets of policies need to be configured:

- **Connection request policies** are sets of conditions and settings that allow network administrators to designate which Remote Authentication Dial-In User Service (RADIUS) servers perform the authentication and authorization of connection requests that the server running Network Policy Server (NPS) receives from RADIUS clients.
If this match it will jump to:
- **Network policies** can be viewed as rules. Each rule has a set of conditions and settings. NPS compares the conditions of the rule to the properties of connection requests. If a match occurs between the rule and the connection request, the settings defined in the rule are applied to the connection.

4.3.3 User Management of the SIPROTEC/SICAM Device

The Network Policy Server (NPS) is the prerequisite for using the centralized user management for SIPROTEC and SICAM devices. The following section describes an example for the SIPROTEC/SICAM user management.

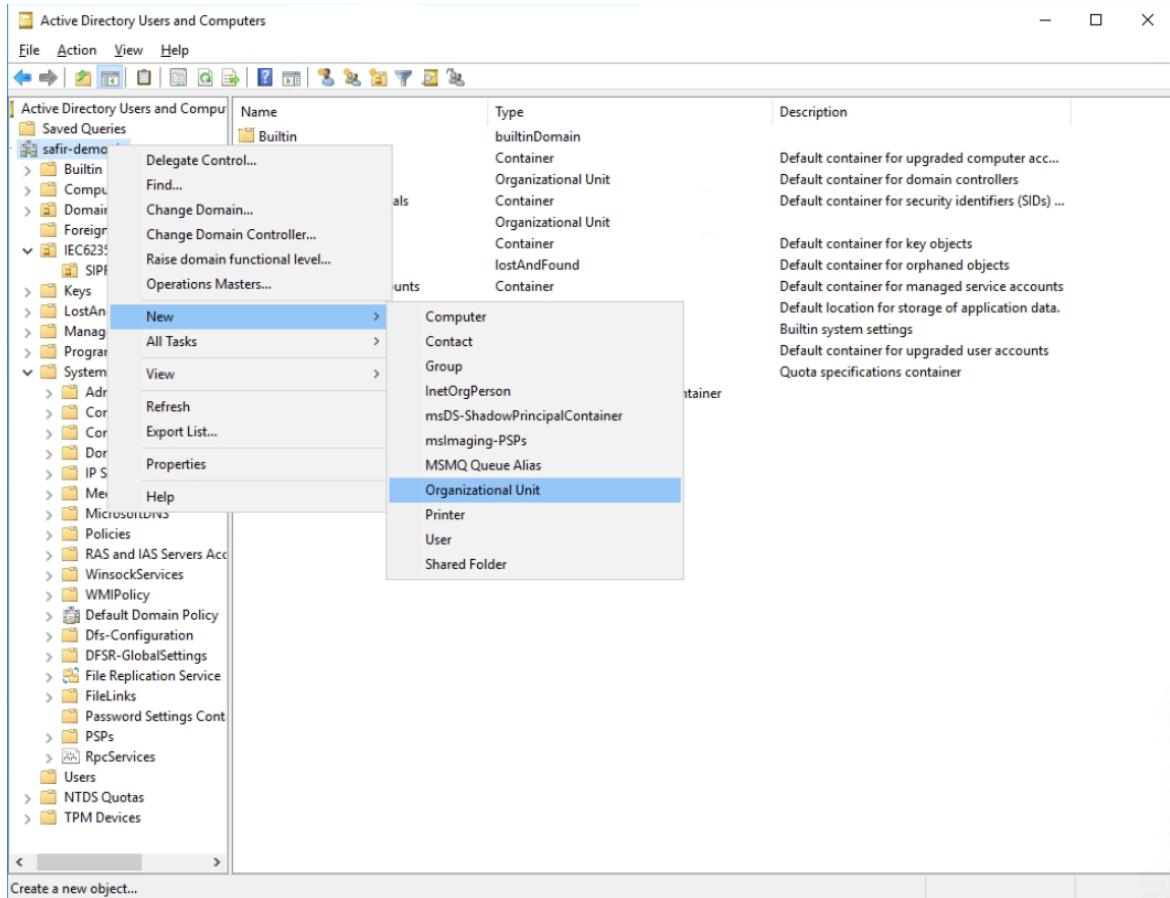
The use case is based on IEC 62351 requirements and the Organizational Unit (OU) IEC62351 is created. The Windows Security Group is assigned IEC 62351-standardized and Siemens-specific roles. For the local HMI users, the passcode-based authentication is being used.

Prerequisites:

- Installation of Windows Server 2016 or later

4.3.3.1 Windows User Groups and User Settings

- ✧ Go to **Server Manager** → **Tools** → **Active Directory Users and Computers**.
- ✧ Right-click the domain level and create the new **OU IEC 62351** group (or any other name).



[sc_Assigning Organizational Unit, 1, en_US]

Figure 4-60 Assigning Organizational Unit

4.3.3.2 Add Global Security Groups

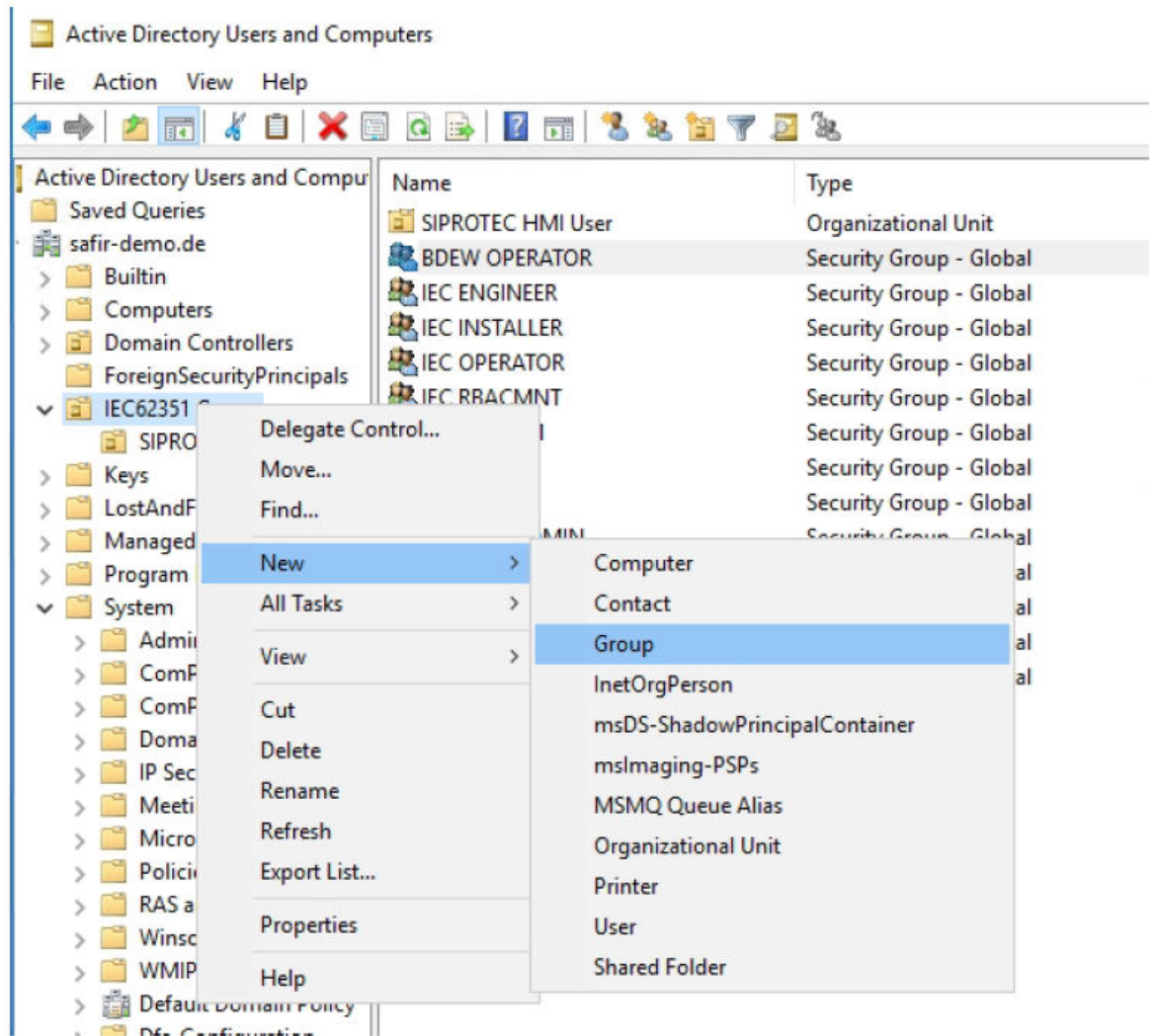
- ✧ On the Organizational Unit level, create all necessary IEC 62351 and Siemens roles as Global Security Groups as shown below.



NOTE

The group name is not essential for proper functionality; thus, any name can be chosen.

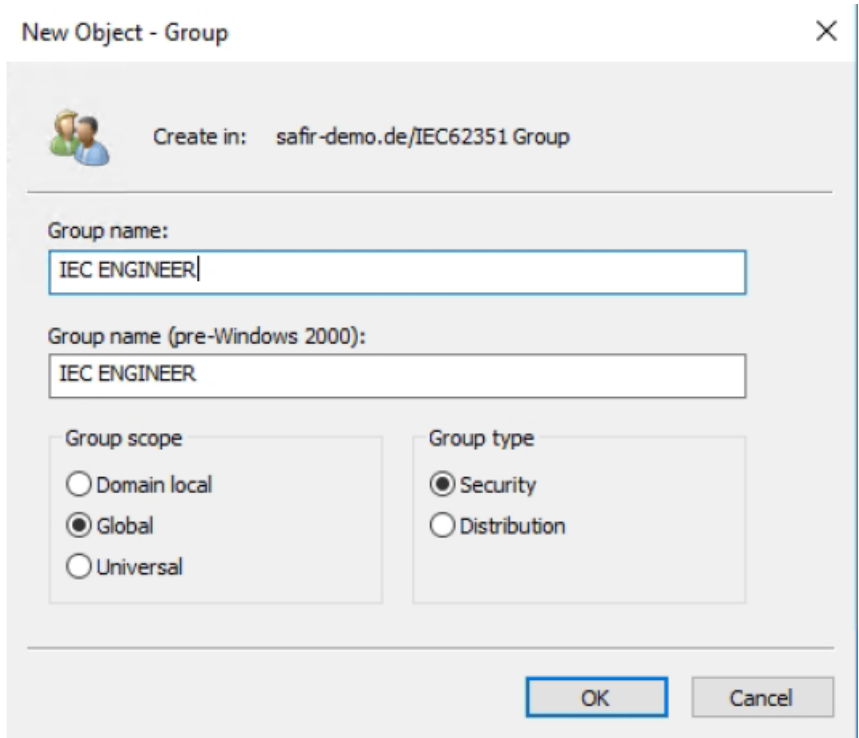
- ✧ Configure a Windows Active Directory and NPS.



[sc_Assigning Group to IEC 62351, 1, en_US]

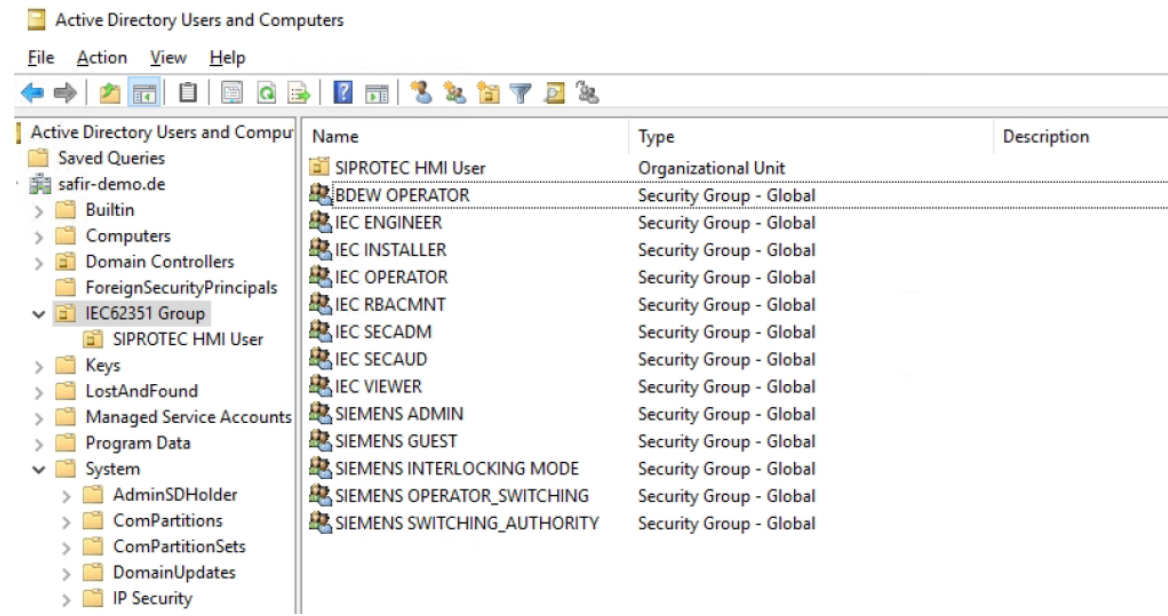
Figure 4-61 Assigning Group to IEC 62351

- ◇ Create new roles with a right-click on the **IEC 62351** group and select **New → Group**.



[sc_Creating new IEC Group, 1, en_US]
 Figure 4-62 Creating New IEC Group

- ✧ Enter the IEC 62351 or Siemens (role) group name and click **OK**. Repeat the procedure until all groups exists as shown in the following figure:



[sc_Creating new IEC Group users, 1, en_US]
 Figure 4-63 Creating New IEC Group Users

4.3.3.3 Local Users for SIPROTEC 5 Devices

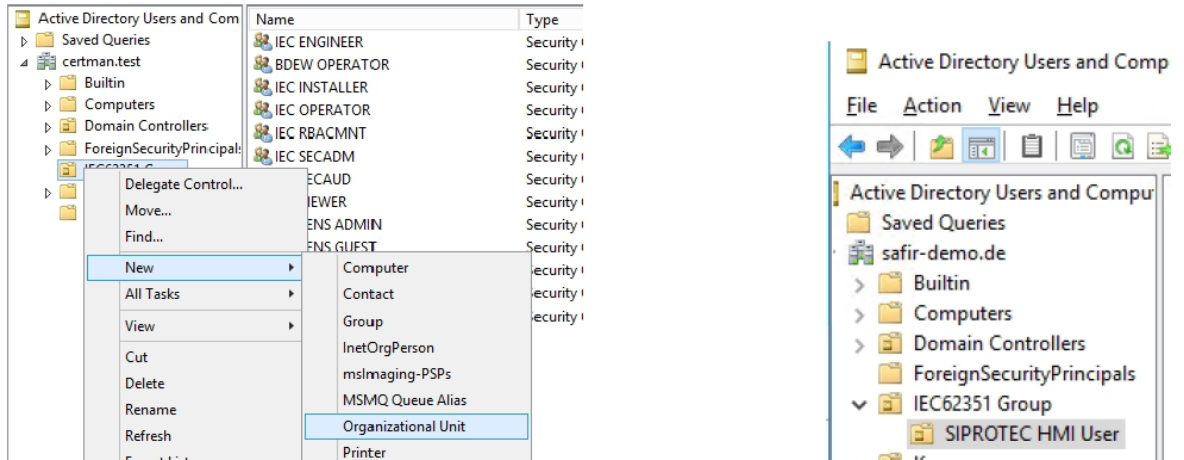
- ✧ Add an additional Organizational Unit (OU) as **SIPROTEC HMI User**.



NOTE

The group name is not essential for proper functionality; thus, any name can be chosen.

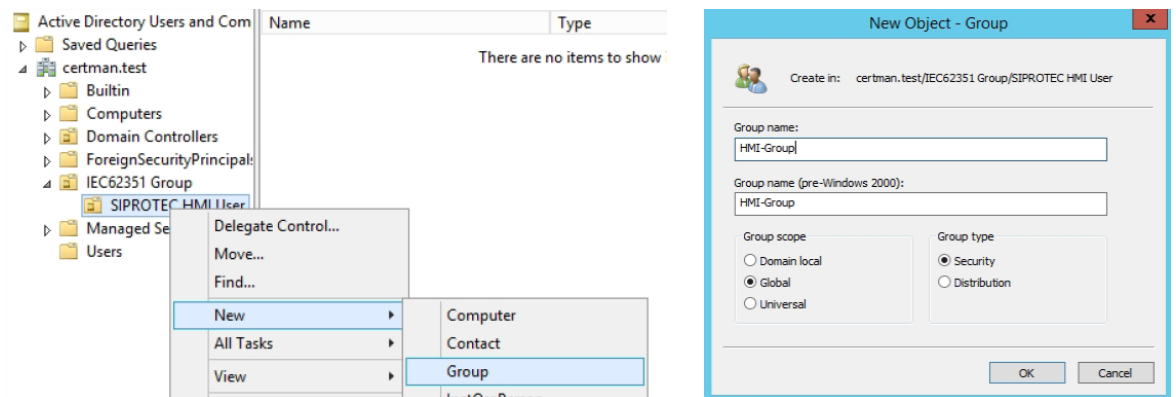
- ✧ For the local HMI user, add the additional OU **SIPROTEC HMI User** under the OU **IEC 62351 Group**.



[sc_Assigning Organizational Unit to IEC Group, 1, en_US]

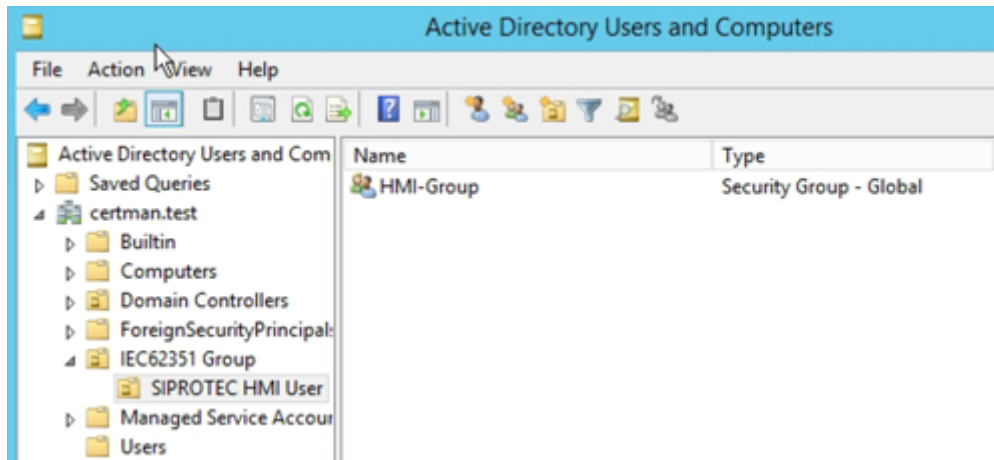
Figure 4-64 Assigning Organizational Unit to IEC Group

- ✧ Under the OU **SIPROTEC HMI User**, add a global security group as **HMI Group**.



[sc_Adding HMI group, 1, en_US]

Figure 4-65 Adding HMI Group



[sc_Adding HMI group members, 1, en_US]

Figure 4-66 Adding HMI Group Members

SIPROTEC 5 (local) does not support complex passwords. Therefore, for HMI users, use weak passwords with numeric passcodes.



NOTE

This guide is based on Windows Server 2016 or later.

4.3.3.4 Creation of Password Policy Objects

- ✧ Under the **Server Manager** → **Tools** menu of the Windows Server, start **ADSI Edit** and connect it to a domain and Domain Controller for which password policy is required.
- ✧ Double-click **CN=DomainName**, then double-click **CN=System**, and then double-click **CN=Password Settings Container**.
- ✧ Right-click **CN=Password Settings Container** and click **New**, then **Object...**
- ✧ Click **Next**.
- ✧ Type the name **HMI Users** of the Password Settings Object (PSO) in the **Value** field and then click **Next**.
- ✧ Type in a number that will be the precedence for this Password Policy, then click **Next**.
- ✧ Type **FALSE** in the **Value** field and click **Next**.
- ✧ Type **0** in the **Value** field and click **Next**.
- ✧ Type **FALSE** in the **Value** field and click **Next**.
- ✧ Type **5** in the **Value** field and click **Next**.
- ✧ Type **1:00:00:00** in the **Value** field and click **Next**.
- ✧ Type **42:00:00:00** in the **Value** field and click **Next**.
- ✧ Type **10** in the **Value** field and click **Next**.
- ✧ Type **0:00:30:00** in the **Value** field and click **Next**.
- ✧ Type **0:00:30:00** in the **Value** field and click **Next**.
- ✧ Click **Finish**. This would create a Password Policy Object.

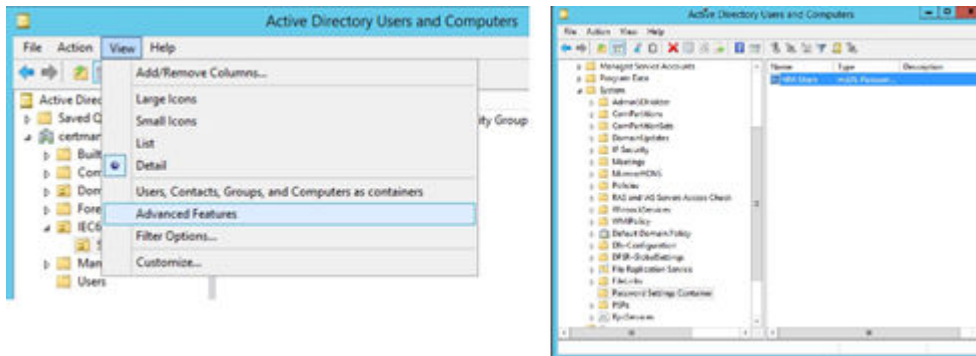
Name	Class	Distinguished Name
CN=HMI Users	msDS-Passw...	CN=HMI Users,CN=Passwo

[sc_Creating password policy for HMI Users, 1, en_US]

Figure 4-67 Creating Password Policy for HMI Users

4.3.3.5 Assigning a Password Settings Object (PSO) to a User Group or a User

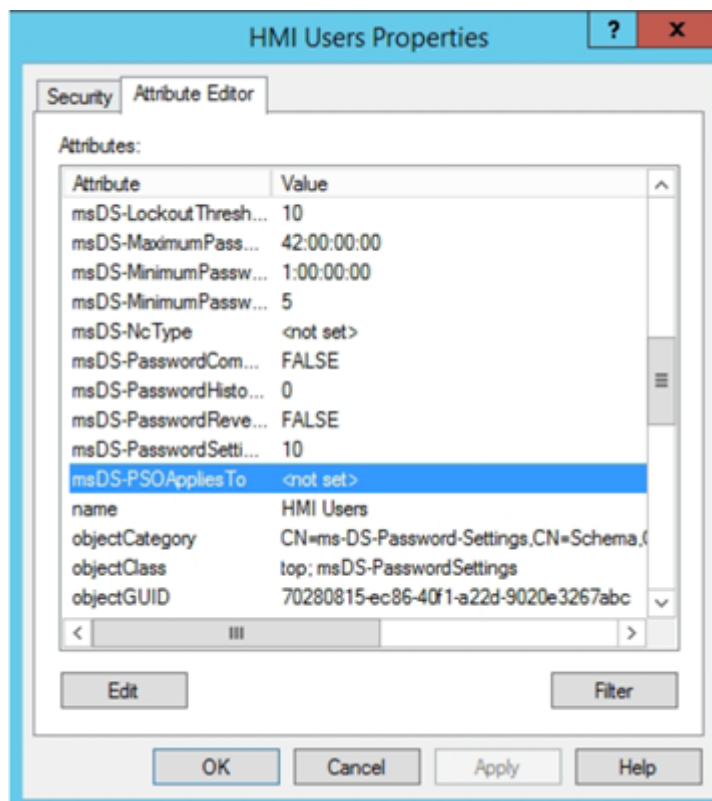
- ✧ Open Active Directory Users and Computers and navigate to System → Password Settings Container.



[sc_Assigning PSO to a User Group or a User, 1, en_US]

Figure 4-68 Assigning PSO to a User Group or a User

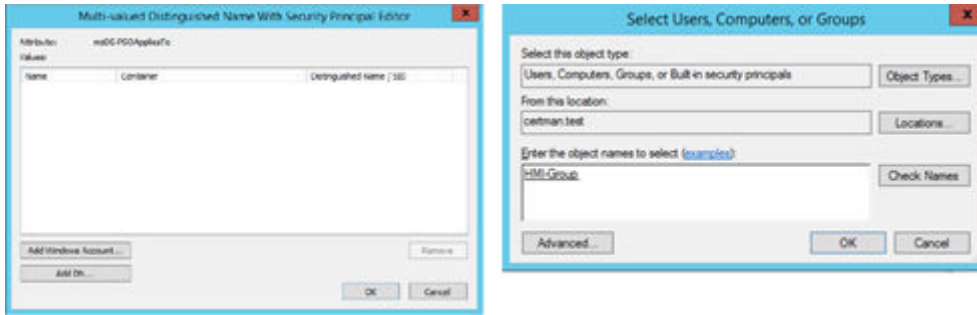
- ✧ Double-click the PSO you created, then click the **Attribute Editor** tab.
- ✧ Select the **msDS-PSOAppliesTo** attribute and click **Edit**.



[sc_Assigning attribute to PSO group, 1, en_US]

Figure 4-69 Assigning Attribute to PSO Group

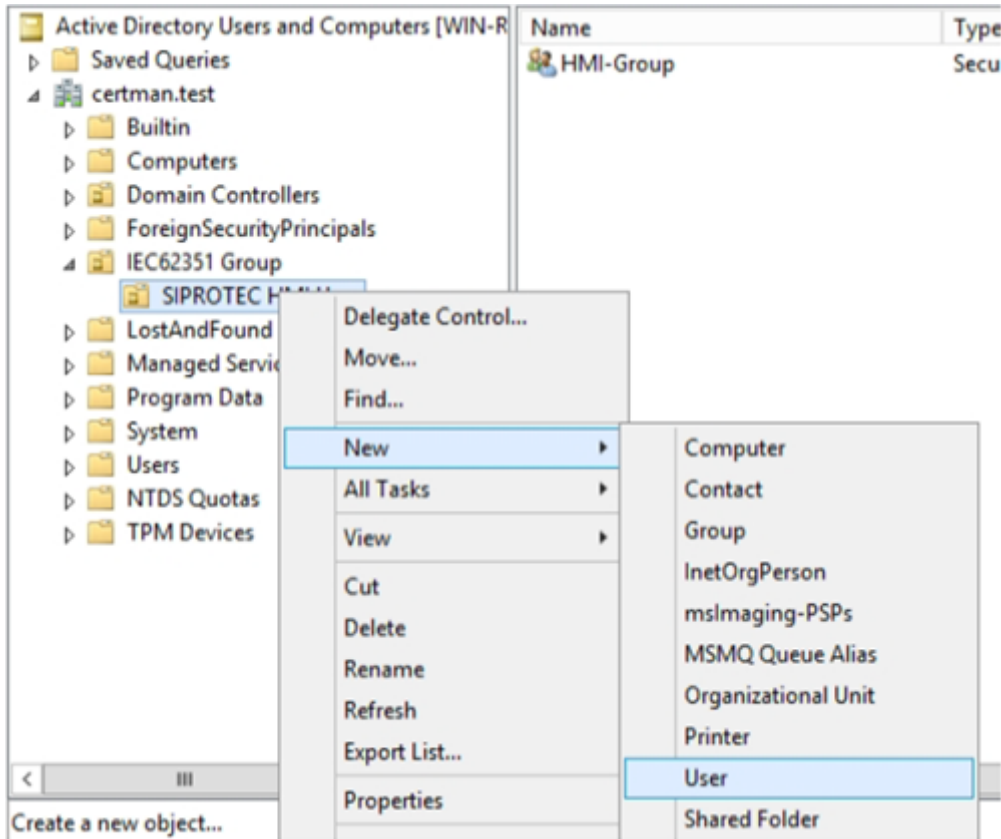
✦ Click **Add Windows Accounts...**



[sc_Adding Windows Account, 1, en_US]

Figure 4-70 Adding Windows Account

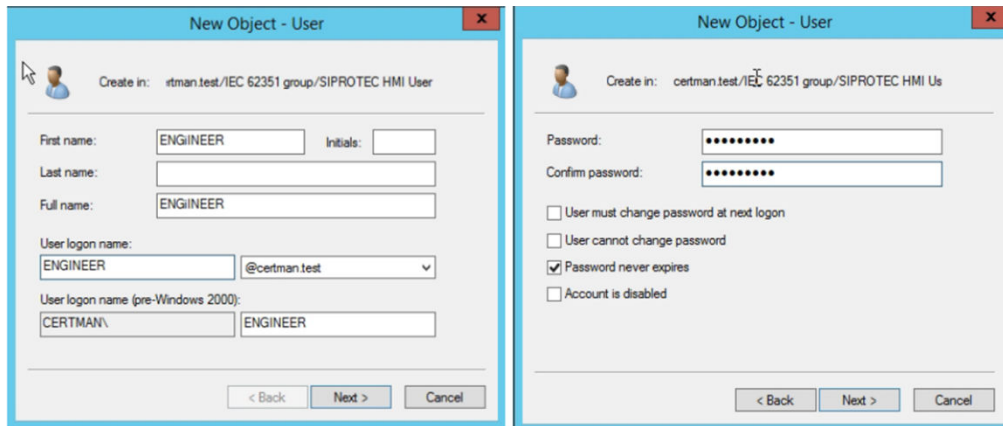
- ✦ Select the group **HMI-Group** to apply this PSO and click **OK**.
- ✦ Now, add all HMI users under **SIPROTEC HMI User** in a first step with a strong password.



[sc_Assigning User to HMI group, 1, en_US]

Figure 4-71 Assigning User to HMI Group

- ✦ The **User logon name** should be identical to the **Full name**. The following users shall be created the same way: ADMIN, ENGINEER, VIEWER, INSTALLER, OPERATOR, SECADM, SECAUD, Operator_Switching, Switching_Authority, Interlocking_Mode.



[sc_Creating User and Password in HMI group, 1, en_US]

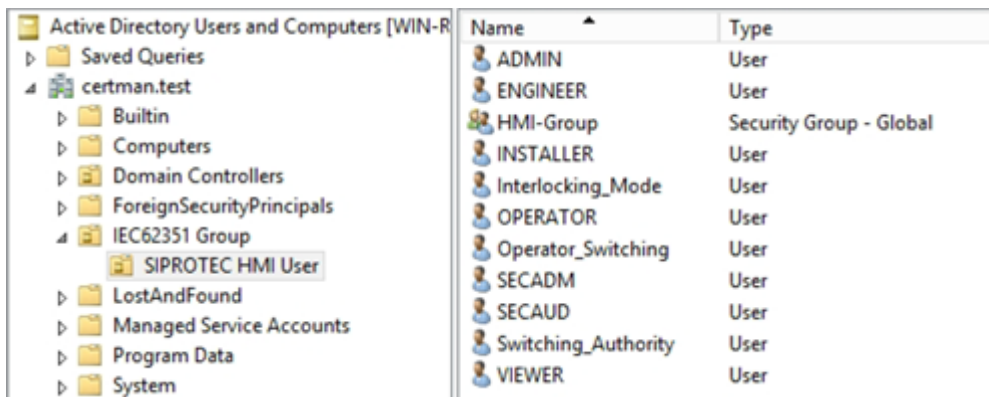
Figure 4-72 Creating User & Password in HMI Group



NOTE

These are HMI users which are hard-wired inside the SIPROTEC 5 devices for HMI local login. The names cannot be adjusted or changed; these are not groups or roles but have to be mapped to the corresponding group in later steps.

- ✧ Enter a strong password, a weak password during user creation stage may lead to a Weak Password Policy.



[sc_Adding users to HMI group, 1, en_US]

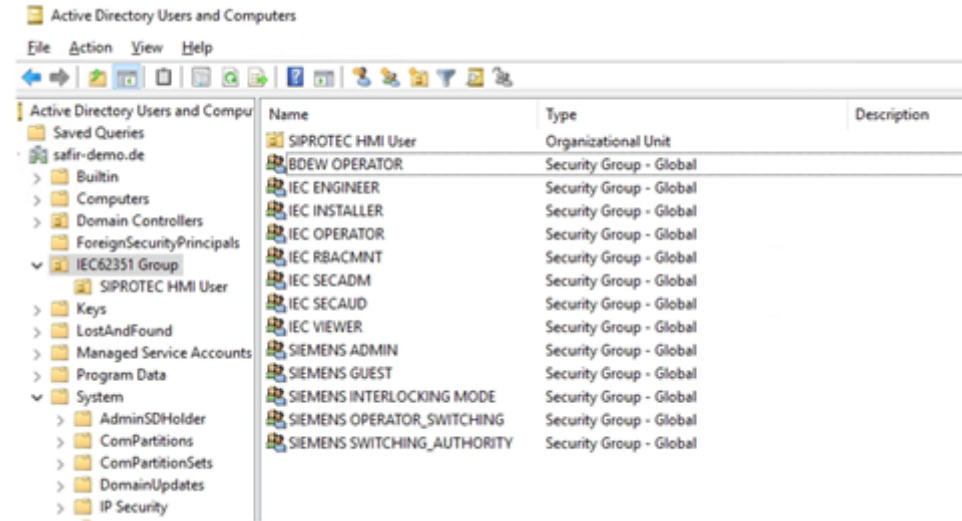
Figure 4-73 Adding Users to HMI Group

- ✧ Add the users to a member of the HMI-Group (for weak password policy) and to their specific IEC 62351 or Siemens Group:

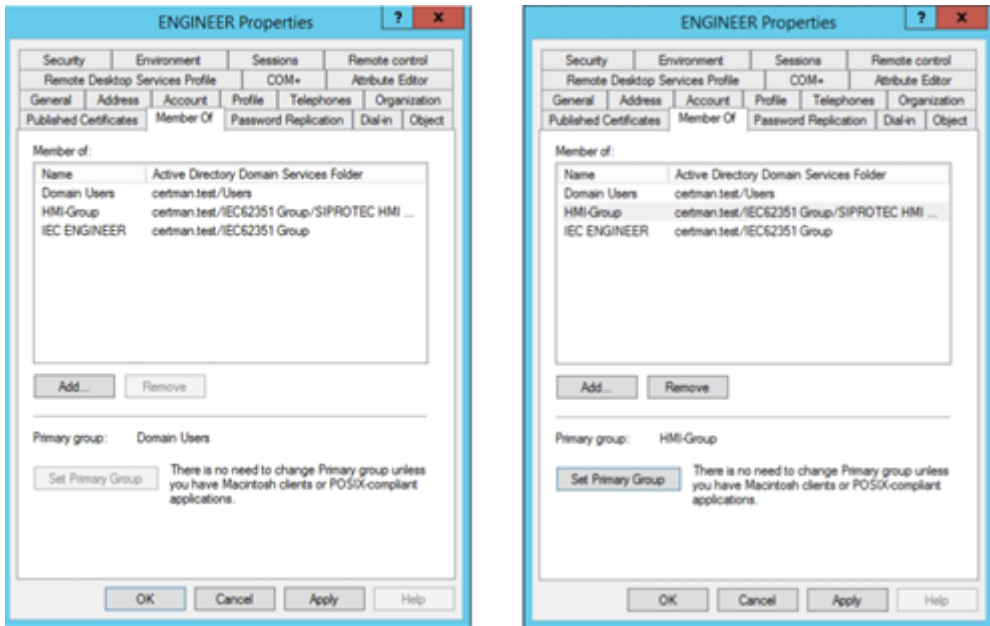
Table 4-2 HMI Groups

Users of HMI Group	IEC or Siemens Group
ADMIN	SIEMENS ADMIN
VIEWER	IEC VIEWER
OPERATOR	IEC OPERATOR
ENGINEER	IEC ENGINEER
INSTALLER	IEC INSTALLER
SECADM	IEC SECADM
SECAUD	IEC SECAUD
RBACMNT	IEC RBACMNT

Users of HMI Group	IEC or Siemens Group
Operator_Switching	SIEMENS OPERATOR_SWITCHING
Switching_Authority	SIEMENS SWITCHING_AUTHORITY
Interlocking_Mode	SIEMENS INTERLOCKING MODE

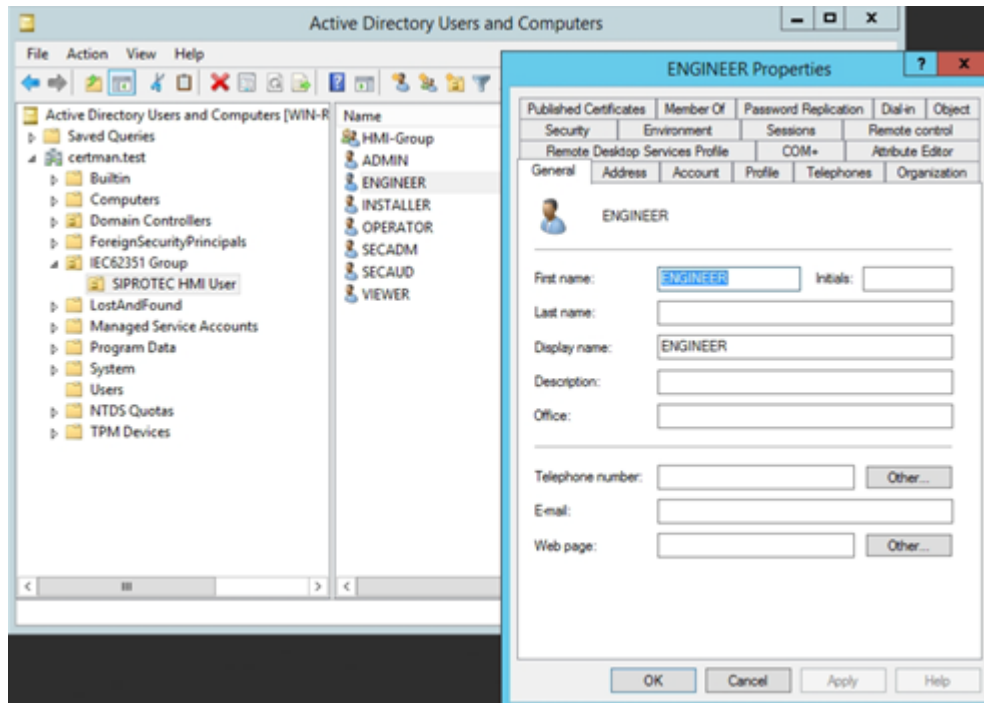


[sc_IEC 62351 Group Users, 1, en_US]
 Figure 4-74 IEC 62351 Group Users



[sc_IEC 62351 Group User properties, 1, en_US]
 Figure 4-75 IEC 62351 Group User Properties

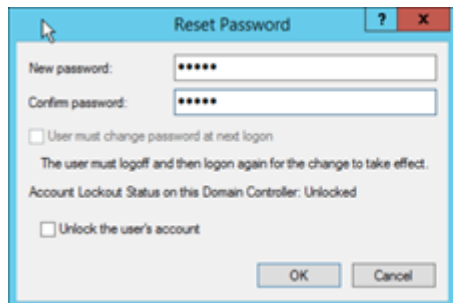
- ✧ Set HMI Group as Primary Group and remove **Domain Users** default group.



[sc_Removing domain users, 1, en_US]

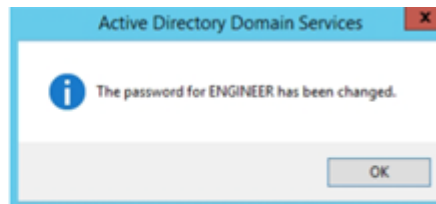
Figure 4-76 Removing Domain Users

- ✧ Set the HMI passwords now. It can be a simple numeric passcode, for example, 56923 (recommended minimum length is 5 digits).

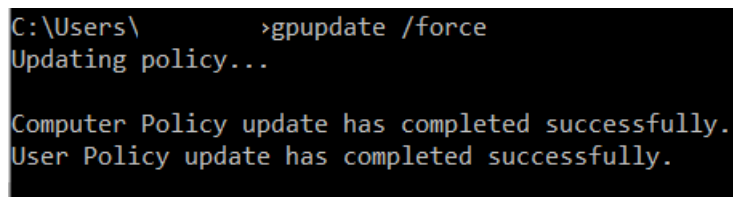


[sc_Setting HMI Password, 1, en_US]

Figure 4-77 Setting HMI Password



- ✧ Update the computer and user policy before starting the NPS using the command shell as follows:
gpupdate /force

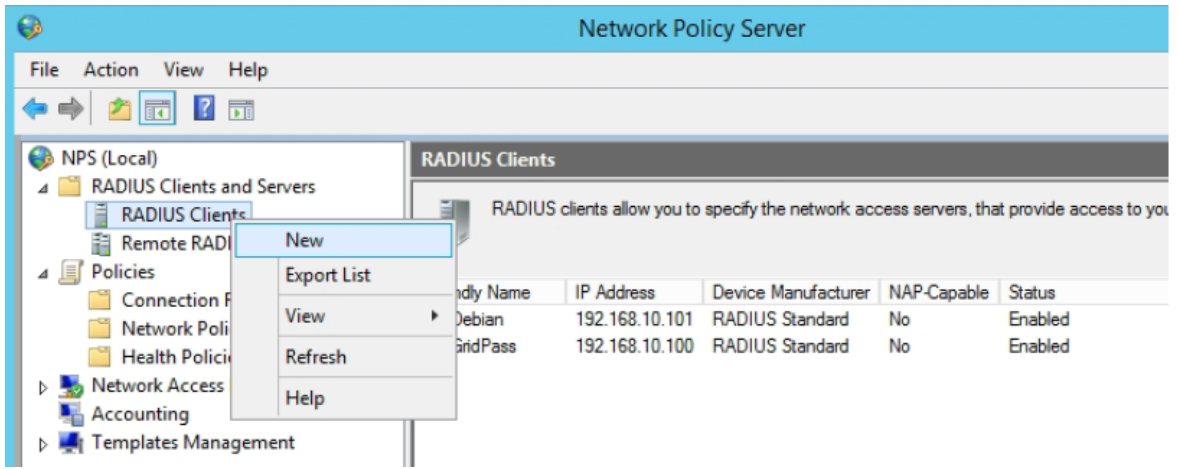


[sc_Pushing GPU update through Command Line, 1, en_US]

Figure 4-78 Pushing GPU update through Command Line

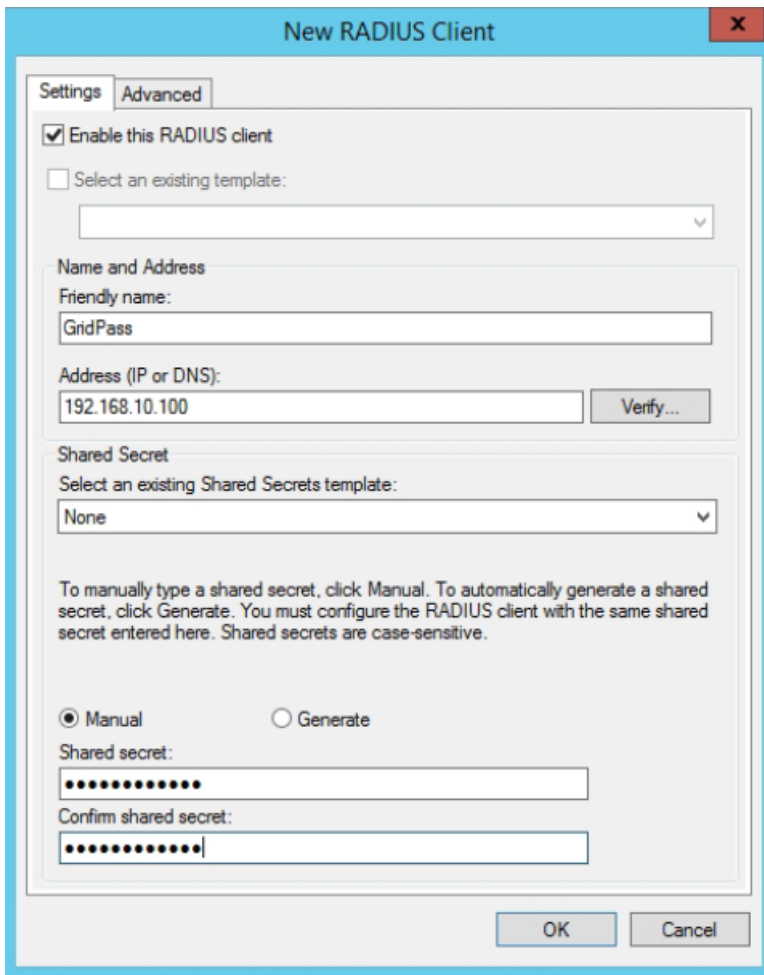
4.3.3.6 Configuration of a Network Policy Server (NPS)

- Start the Network Policy Server via the **Server Manager** → **Tools** and add all RADIUS Clients with known name and the IP which comes with the requested UDP packet to the NPS and choose a shared secret. This would be required to be entered in the client system.



[sc_Configuring NPS, 1, en_US]

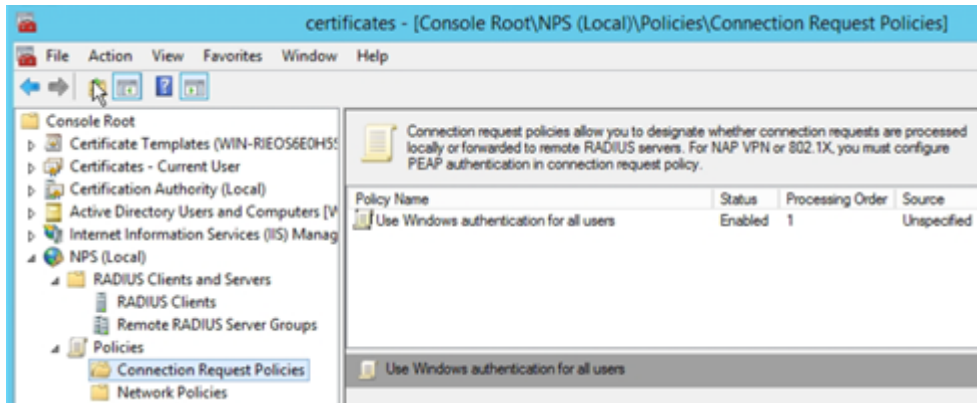
Figure 4-79 Configuring NPS



[sc_New RADIUS Client, 1, en_US]

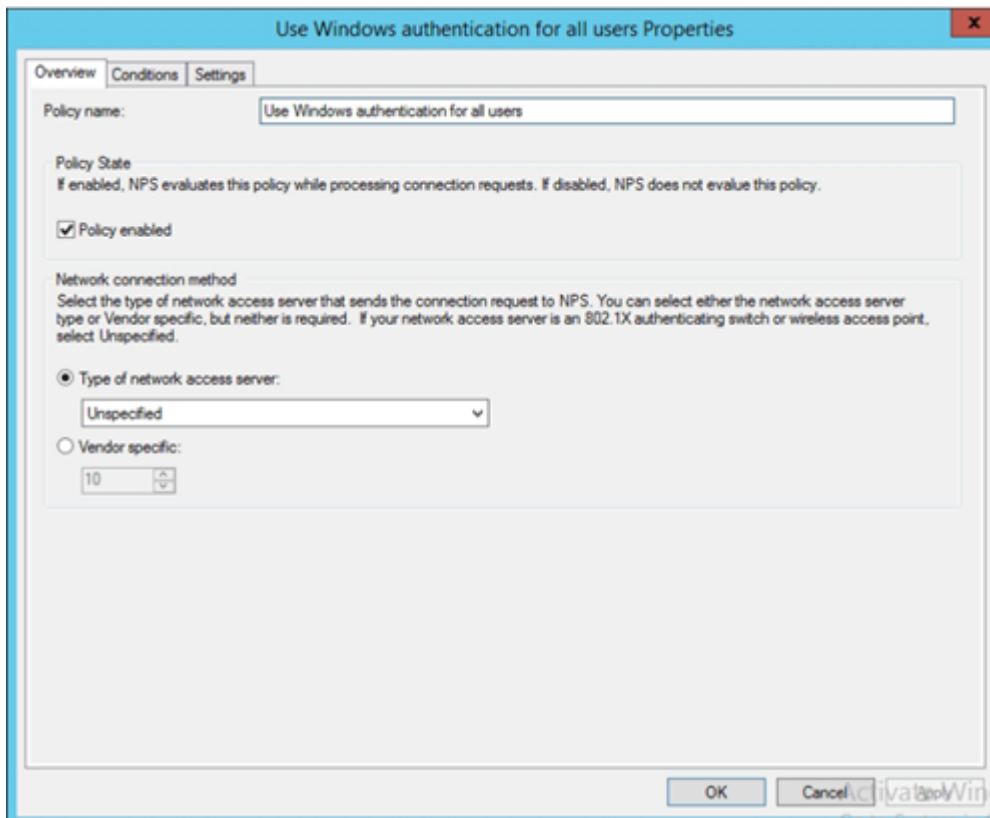
Figure 4-80 New RADIUS Client

- ✧ Add one allowing connection policy.
This can be more than one based on the day and time restrictions.



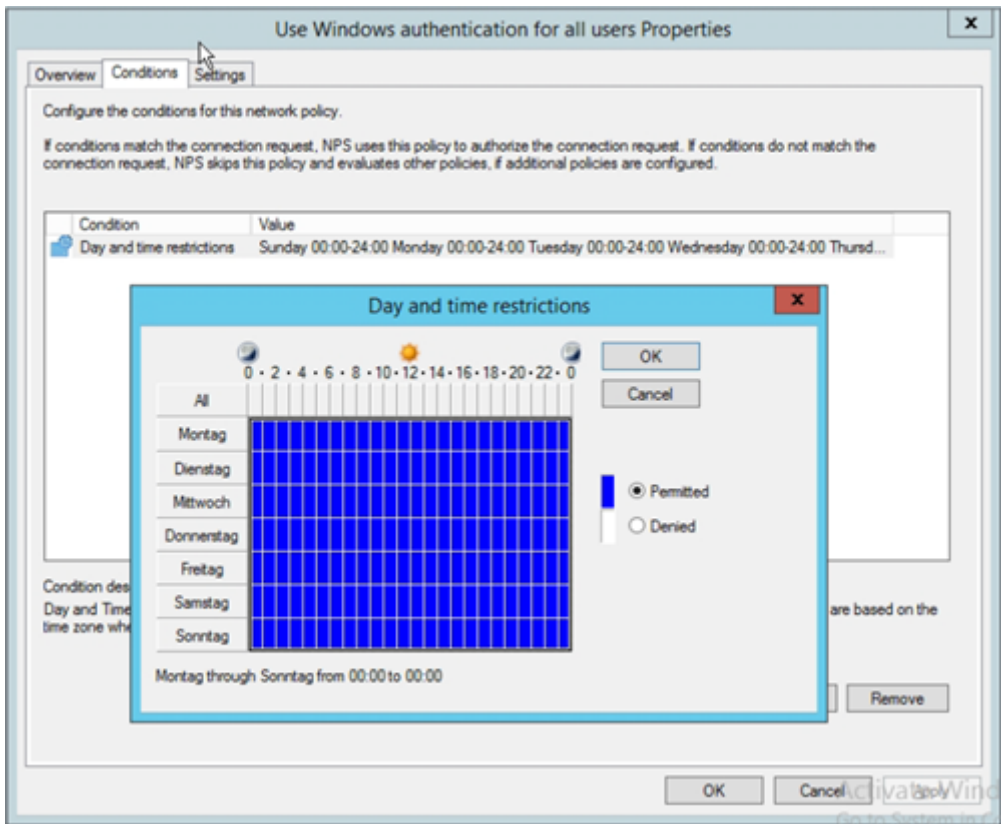
[sc_Certificate Console, 1, en_US]

Figure 4-81 Certificate Console



[sc_Using windows authentication in RADIUS, 1, en_US]

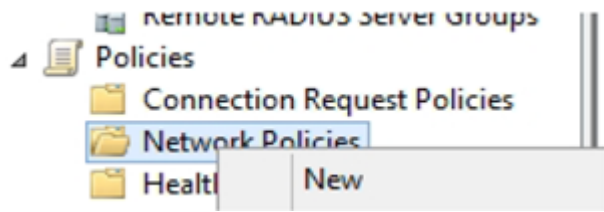
Figure 4-82 Using Windows Authentication in RADIUS



[sc_Assigning Access Attributes, 1, en_US]

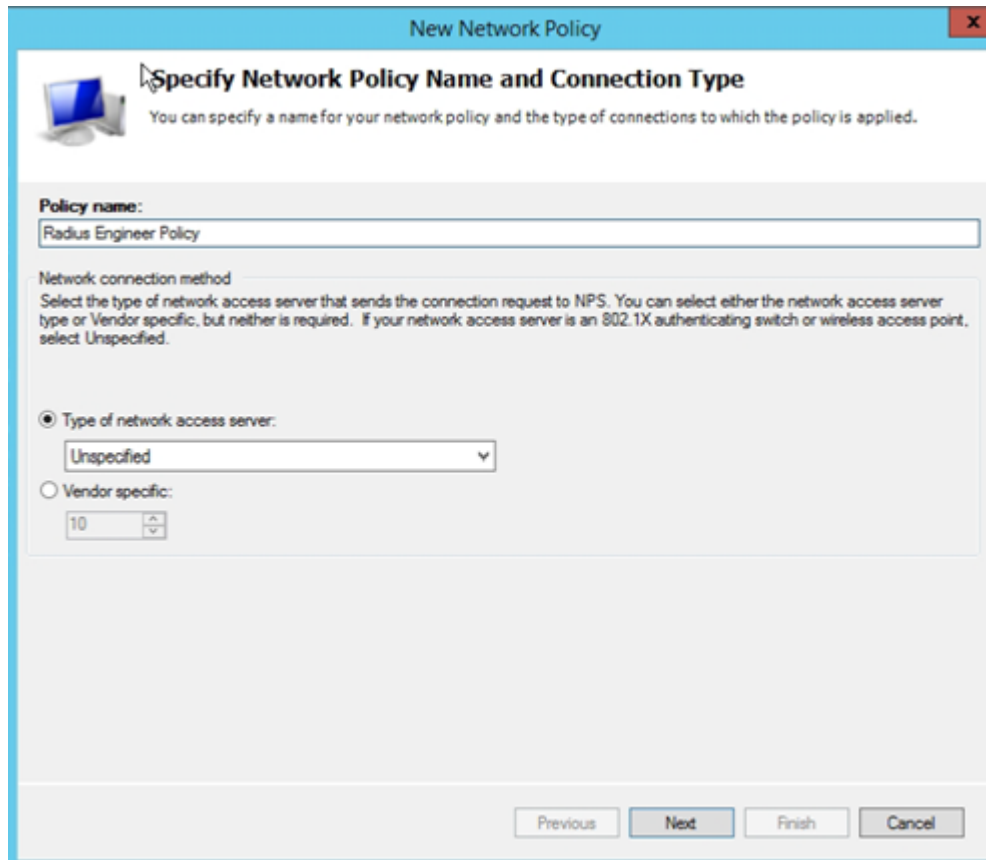
Figure 4-83 Assigning Access Attributes

- ◇ Create the Network policies with the context menu and select **New**.



[sc_Creating new Network policy, 1, en_US]

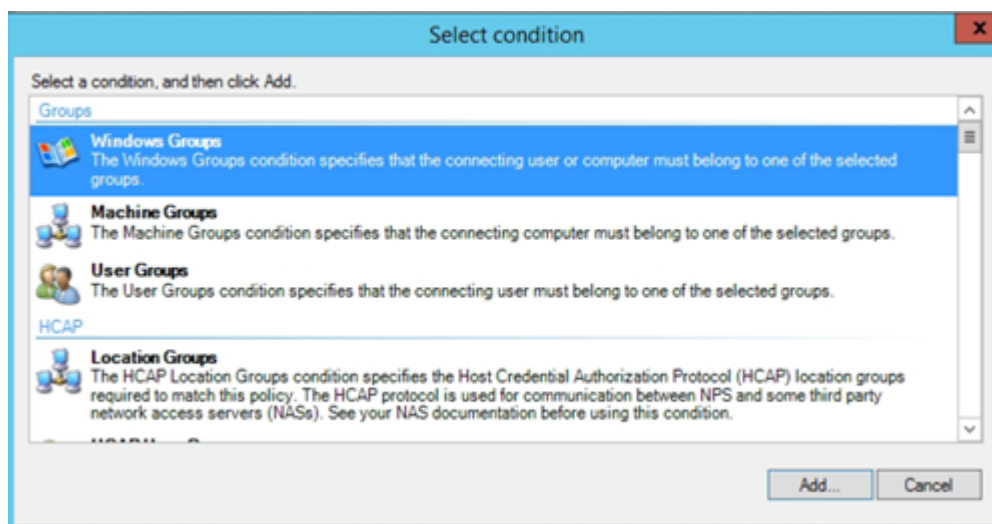
Figure 4-84 Creating New Network Policy



[sc_Creating new Network policy name, 1, en_US]

Figure 4-85 Creating New Network Policy Name

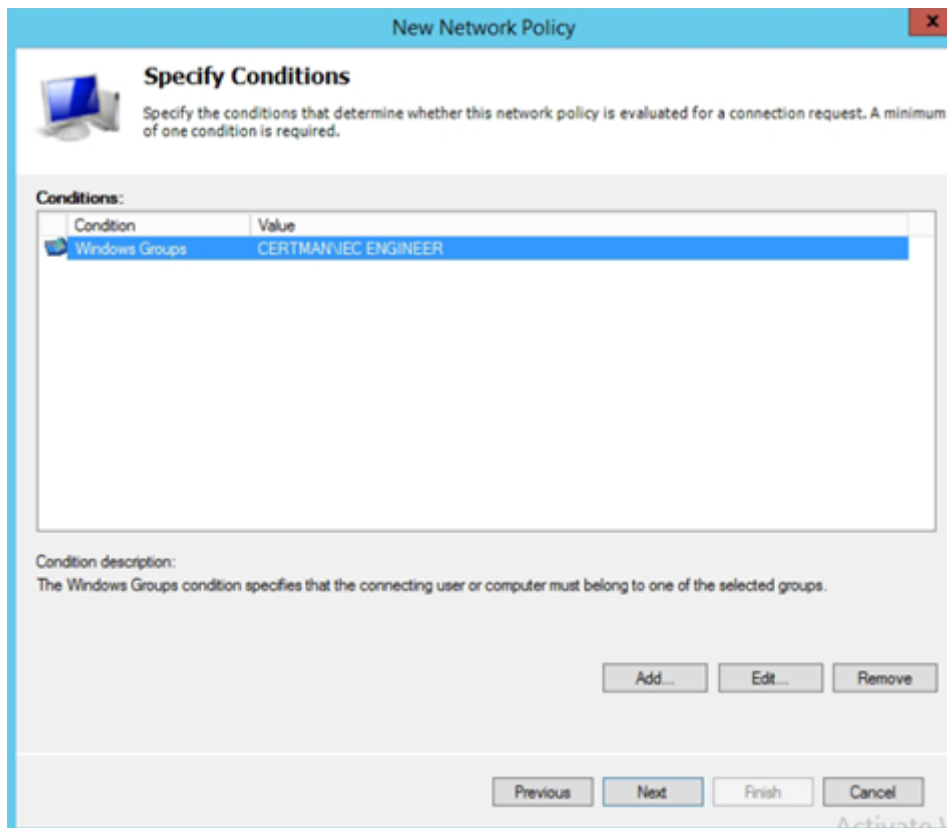
- ✧ Specify the policy name as **Radius Engineer Policy** (or something else) and click **Next**.
- ✧ In the **Select Condition** window, choose **Windows Groups**.



[sc_Assigning Windows group to NPS, 1, en_US]

Figure 4-86 Assigning Windows group to NPS

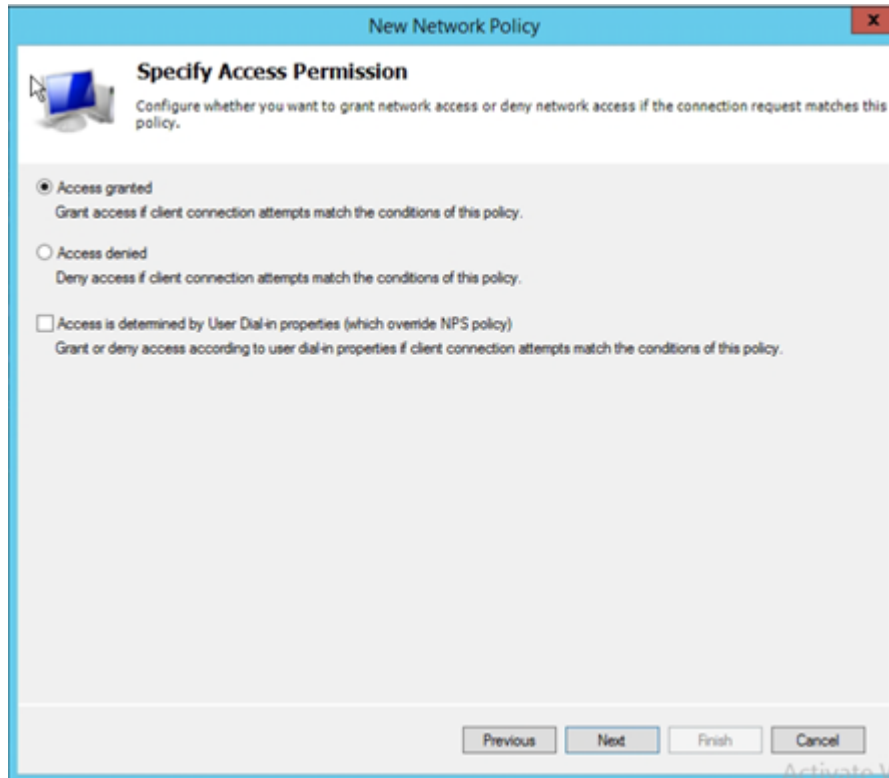
- ✧ Select the corresponding IEC or Siemens group for the created policy.



[sc_Assigning Windows group to NPS user, 1, en_US]

Figure 4-87 Assigning Windows Group to NPS User

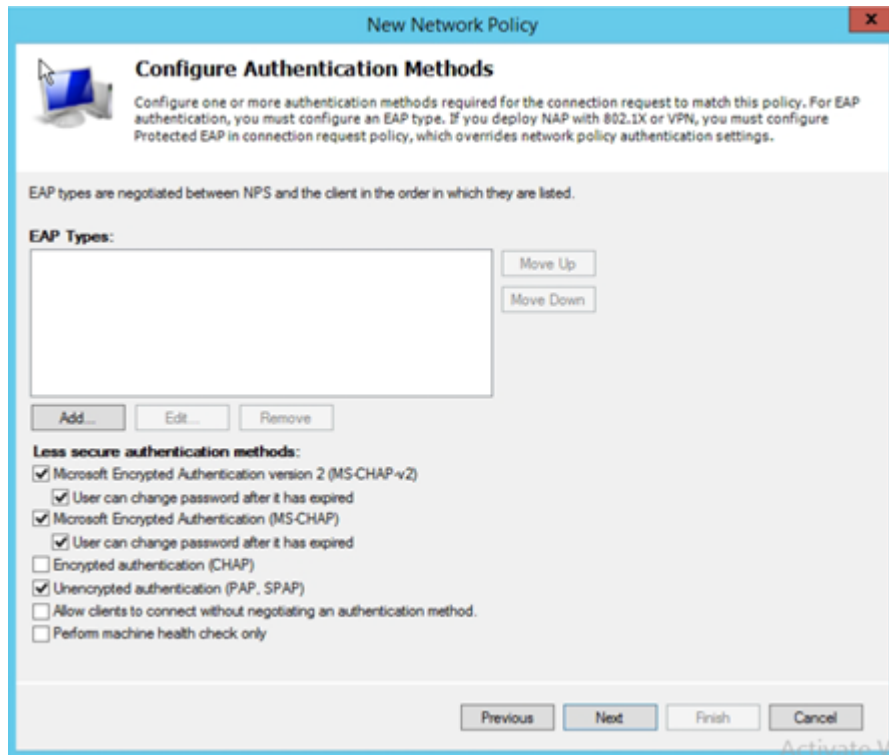
- ✧ Select **Access granted** and click **Next**.



[sc_Granteeing Access, 1, en_US]

Figure 4-88 Granting Access

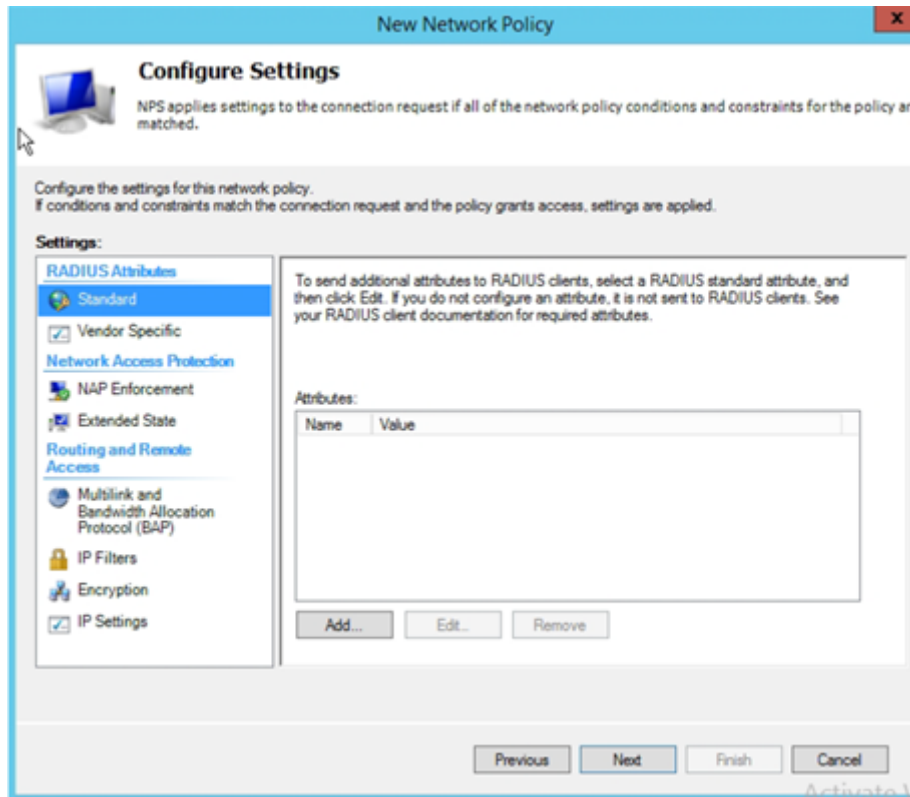
✧ Select the additional authentication method as PAP and click **Next** twice.



[sc_Configuring Authentication Method, 1, en_US]

Figure 4-89 Configuring Authentication Method

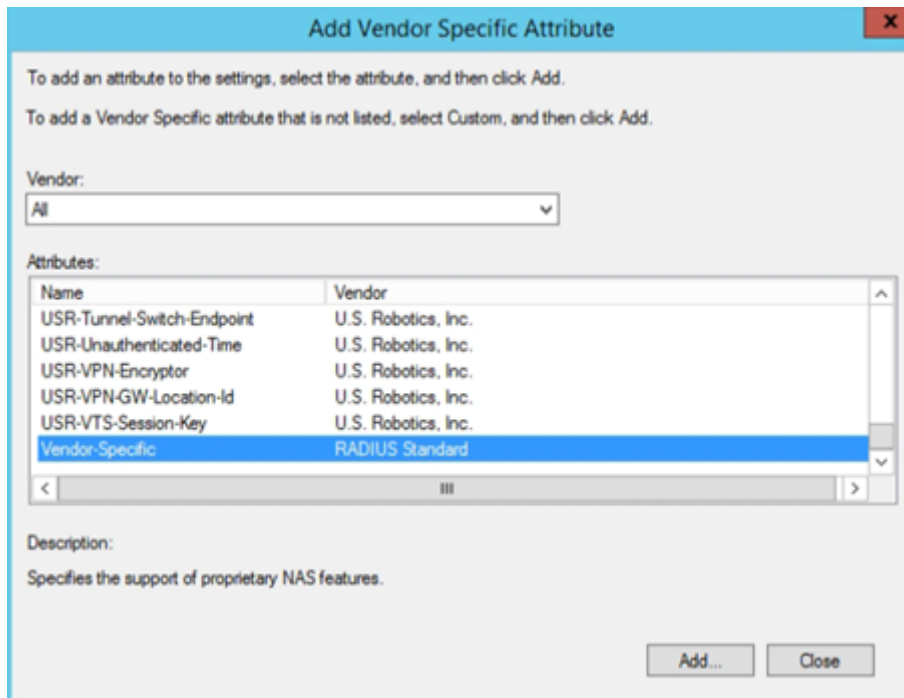
- ✧ Remove the standard attributes.



[sc_RADIUS Attributes, 1, en_US]

Figure 4-90 RADIUS Attributes

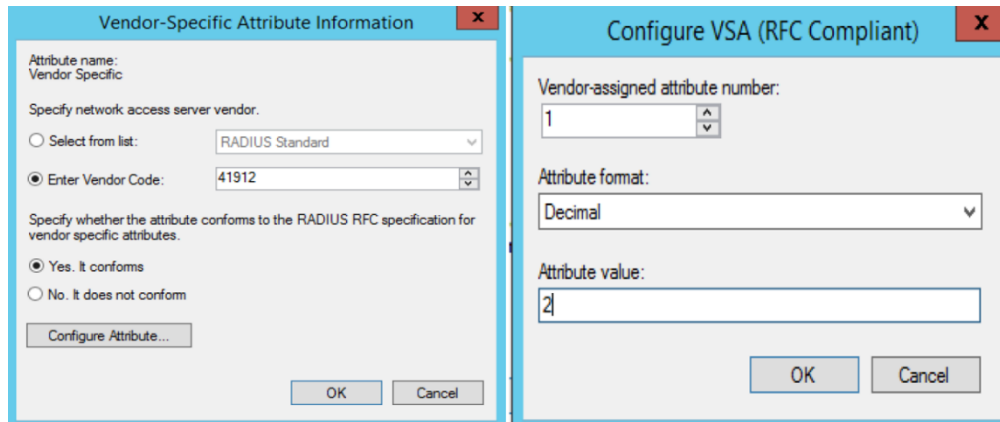
- ✧ Now, add Vendor-Specific attributes.



[sc_Adding Vendor Specific Attributes, 1, en_US]

Figure 4-91 Adding Vendor Specific Attributes

✧ Add the IEC 62351-Specific Attribute to the Policy.

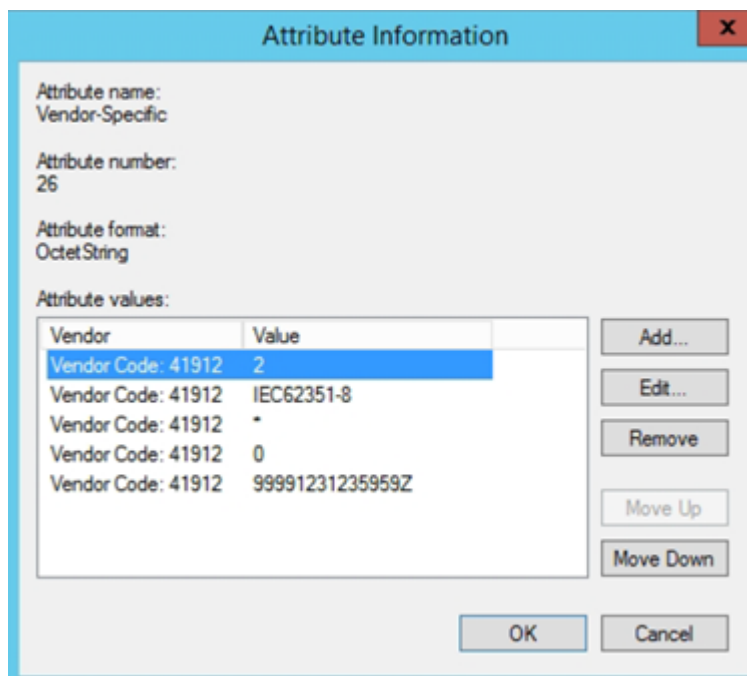


[sc_Configuring Vendor Specific Attributes, 1, en_US]

Figure 4-92 Configuring Vendor Specific Attributes

The Attribute format is

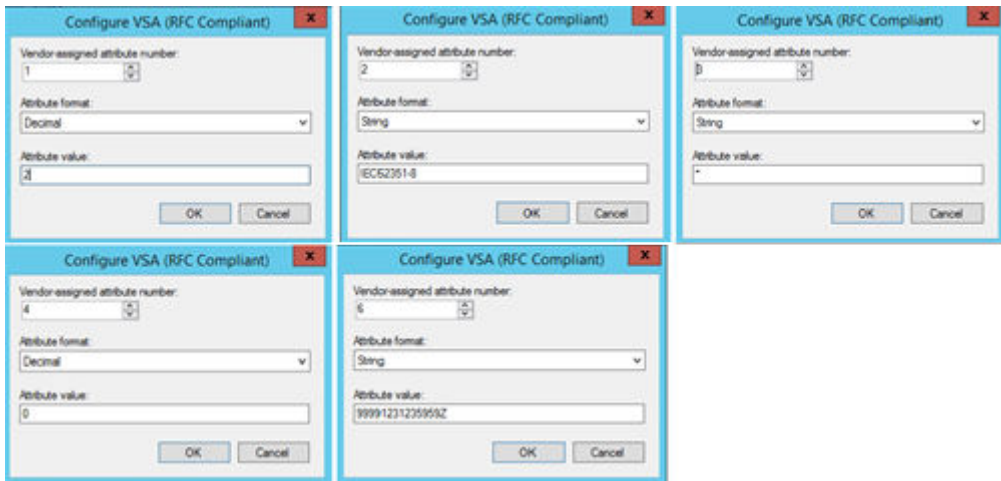
- ATTRIBUTE IEC62351-8-RoleID-0 1 integer
 - Vendor-assigned attribute, number “1” means IEC6235-8-RoleID-0
 - Using signed integer with NPS use the hexadecimal format
 - Range for signed int32: from -2.147.483.648 to 2.147.483.647
 - Range for unsigned in32: from 0 to 4.294.967.295
 - For example – 101 decimal results to FFFFFFF9B hex
- ✧ Add all attributes and values to the Policy. For example, for the role IEC ENGINEER.



[sc_Configuring Attribute Information, 1, en_US]

Figure 4-93 Configuring Attribute Information

Example for the Engineer policy/role:



[sc_Engineer Policy Rules, 1, en_US]

Figure 4-94 Engineer Policy Rules



NOTE

For IEC roles, use **IEC62351-8** (optional) string value for ID 2 (roleDefinition) and for Siemens roles **SiemensGridSecurity** string value for ID 2 (roleDefinition)
 for revision use always "0" as decimal value for ID 4
 for ValidTo and ValidFrom strings use the format YYYYMMDDHHMMSSZ (Year, Month, Day, Hour, Minutes, Seconds, Zulu time zone)

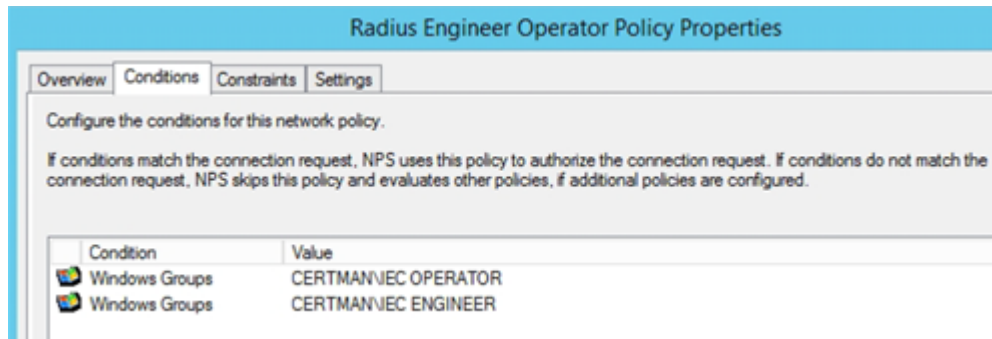
The Combined roles would have more than one Windows group:

Policy Name	Status	Processing Order
Radius Engineer Operator Policy	Enabled	1
Radius SECADM Policy	Enabled	2
Radius Operator Policy	Enabled	3
Radius Engineer Policy	Enabled	4
Radius Installer Policy	Enabled	5
Radius Viewer Policy	Enabled	6
Radius BDEW Operator Policy	Enabled	7
Radius Operator_Switching Policy	Enabled	8
Radius Switching Authority Policy	Enabled	9
Radius Interlocking_Mode Policy	Enabled	10
Radius SECAUD Policy	Enabled	11
Radius RBACMNT Policy	Enabled	12
Radius Siemens Admin Policy	Enabled	13
Radius Siemens Guest Policy	Enabled	14

[sc_Sample Radius policies, 1, en_US]

Figure 4-95 Sample Radius Policies

✧ The Combined roles should be placed in the beginning as Windows handles policy rules like a firewall.



[sc_Radius Engineer Operator Policy properties, 1, en_US]

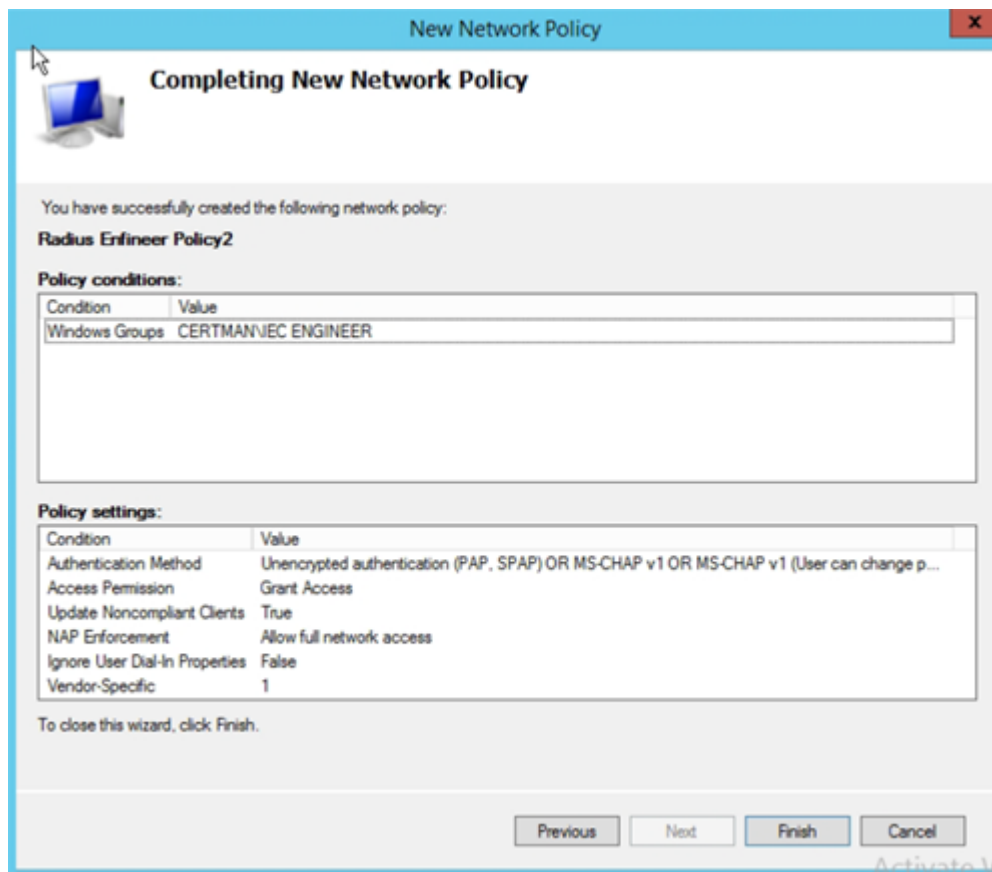
Figure 4-96 Radius Engineer Operator Policy Properties



NOTE

When more than one role is added to a policy, the values must be unique.

✧ Finish the Wizard.



[sc_Completing New Network Policy, 1, en_US]

Figure 4-97 Completing New Network Policy

4.4 Public Key Infrastructure (PKI)

A public key infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.

The Certification Authorities (CA) are part of PKI which are entities issuing digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate. In accordance with the provisions under IEC 62351-9, cybersecurity key management is required for power system equipment. PKI solutions comply with this requirement where infrastructure is supported through various components of PKI. A use case of PKI using Siemens SICAM GridPass to generate a certificate and device authentication is explained in [4.4.4 Using SICAM GridPass to Create Key Material](#).

Other uses include:

- Network access control
- Web access
- Config upload
- Process communication
- Remote desktop/RDP

4.4.1 Digital Certificates

A digital certificate is a data structure that binds a public key value to a subject. A binding is achieved by a trusted certification authority (CA) verifying the identity of the subject and digitally signing the certificate. The digital certificate has a limited lifetime that is checked by the relying party along with the signature.

```

Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 12 (0xc)
    Signature Algorithm: sha256WithRSAEncryption
    ① Issuer: C=DE, O=Siemens, OU=EM DG PRO, ST=Bavaria, L=NBG, CN=SiemensEMDGPROCA
    Validity
      Not Before: Feb 15 01:00:00 2018 GMT
      Not After : Feb 15 01:00:00 2019 GMT
    ② Subject: C=DE, O=Siemens, OU=EM DG PRO, ST=Bavaria, L=NBG, CN=localhost.siemens.de
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (2048 bit)
      Modulus:
    ③ 00:b4:59:f0:41:7b:df:60:c7:aa:bb:c5:8f:19:3e:
      08:e5:dc:b9:31...
      Exponent: 65537 (0x10001)
    ④ X509v3 extensions:
      X509v3 Basic Constraints: critical
      CA:FALSE
      X509v3 Key Usage: critical
      Digital Signature, Key Encipherment
      X509v3 Extended Key Usage:
      TLS Web Server Authentication
      X509v3 Subject Alternative Name:
      DNS:localhost.siemens.de
      X509v3 CRL Distribution Points:

      Full Name:
    ⑤ URI:localhost.siemens.de

      Signature Algorithm: sha256WithRSAEncryption
    ⑥ 1b:9e:2f:d7:9e:20:0b:f7:ba:c0:6c:ef:21:29:ac:d6:ee:55:
      5f:ba:11:32:fe:2e:...
    
```

[file: digital-certificate_1_de_DE]

Figure 4-98 Digital Certificate

Legend	Description
(1)	CA which issued the user/device certificate
(2)	User/device info
(3)	User/device public key
(4)	Extensions, purpose of certificate
(5)	Certificate revocation list storage location
(6)	CA signature of user/device certificate, including public key and all information shown here

4.4.1.1 Registration Authority

A registration authority (RA) verifies the identity of entities requesting digital certificates and sends the certificate signing request to the CA. CA and RA are often co-located.

4.4.1.2 Certificate Revocation List (CRL)

A certificate revocation list is a list of digital certificates that have been revoked by the issuing certificate authority (CA) before their scheduled expiration date and should no longer be trusted. The CRL distribution point, for example a Web server link, is stored inside the certificate. A CRL has a validity and must be updated from the CA and downloaded from the entity before getting invalid. Often, an interval of 24 hours is used.

```

Certificate Revocation List (CRL):
  Version 2 (0x1)
  Signature Algorithm: sha256WithRSAEncryption
  Issuer: /C=DE/O=Siemens/OU=EM DG PRO/ST=Bavaria/L=NBG/CN=SiemensCertMan
  Last Update: Mar  1 08:51:06 2018 GMT
  Next Update: Mar  2 08:51:06 2018 GMT
Revoked Certificates:
  Serial Number: 03
  Revocation Date: Mar  1 09:48:00 2018 GMT
  CRL entry extensions:
    X509v3 CRL Reason Code:
      Key Compromise
  Signature Algorithm: sha256WithRSAEncryption
  b5:d2:42:fa:d3:ef:ed:34:06:af:2f:7c:f3:7c:28:30:f1:33:
  99:8e:b2:ec:f8:...
  
```

[sc_Certificate Revocation List, 1, en_US]

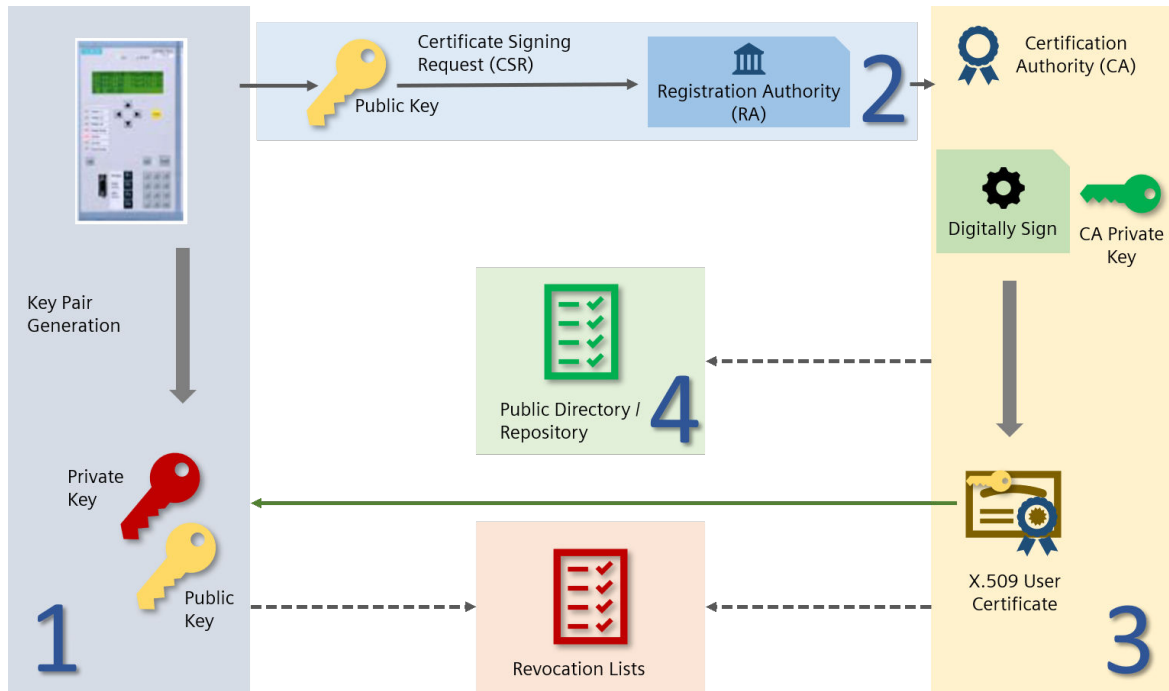
Figure 4-99 Certificate Revocation List

4.4.2 PKI Workflow

In the following figure, the PKI workflow with Enrollment over Secure Transport (EST) in the Siemens Energy environment is shown.

- The entity creates an asymmetrical key pair to use it later for example as https server certificate.
- The entity creates a Certificate Signing Request (CSR) including the public key and entity information as well as the intended use of the requested certificate and sends it to the RA/CA.
- The RA/CA signs the CSR with the CA private key.
- The RA/CA sends the created certificate back to the entity.

In general, certificates often will be stored in a public repository. Here, it is only mentioned because in our environment, it is not necessary and not used. In case of revoked certificates, this CRL will be stored in a publicly available repository.



[sc_PKI Workflow, 1, en_US]

Figure 4-100 PKI Workflow

4.4.3 Creating Key Material

For a secure TLS communication, it is essential to have a mutual authentication between the communication partners. For TLS in general, X.509 certificates are used.

You have 3 different options to get these certificates:

- You can get these certificates from an external PKI.
- You can get these certificates from your internal PKI, SICAM GridPass
- You can create own certificates with the Open Source Software tool OpenSSL.

Certificates

Certificates are a set of keys and information.

You need the following 2 types of keys:

- **Private key**
The private key is in general an RSA key with a length of 1024 bits (for legacy usage) or better of 2048 bits. The private key stays in your access and will be used for signature and decryption.
- **Public key**
You need a corresponding public key with the same length. The public key can distribute to the public and will be used for verifying the signature or for encrypting a message or file.

X.509 Certificate

An X.509 certificate is more than the public key.

The X.509 certificate includes, besides others, the following data:

- Public key
- Information about the issuer

- Subject
- Validity
- Certificate signature of the Certifying Authority (CA)

This means that the public key with all the additional information is signed by a CA private key to verify the authenticity of the public key and information by the communication partner in a later step.

You can find more information on creating a CA, a private key, a public key, and a certificate with OpenSSL in the following chapters.

TLS Function

In the following, you can find a simplified description of the handshake process.

Both communication partners own their certificate, their private key, and the CA certificate. Starting the communication means starting also the TLS handshake. The first partner sends his certificate to the communication partner. The second partner gets the certificate and can verify the certificate at first with the CA certificate. Now, the second partner knows that the certificate of the first partner is not modified and comes from a trusted CA. This means that the second partner can trust the certificate of the first partner and, hence, the second partner can trust the first partner.

Now, the second partner checks, for example, the validity or if the certificate is placed on a black list etc. if he wants to know to accept the certificate (adjusted by policies etc. This document does not treat certificate handling in such a detailed way). After that, the second partner sends his certificate to the first partner and this partner performs the same checks.

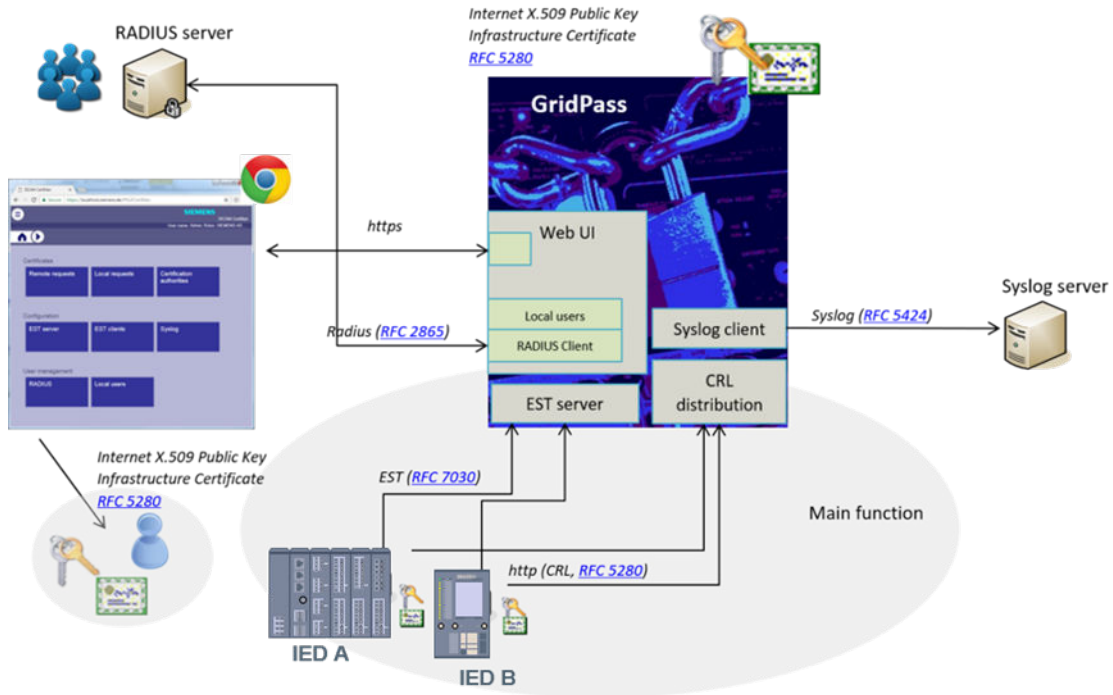
Now both partners know and trust each other. Additionally, both partners have the public key of the other partner to encrypt messages or files. In TLS, the encryption of all TCP packages with this RSA key (called asymmetrical keys) would be too slow. Therefore, one partner creates a symmetrical key, for example, AES, for encryption and sends the key encrypted with the public key of the other partner to the other partner. The other partner can now decrypt the symmetrical key with his private key. In this way, both partners have the same symmetrical key for encryption and decryption of messages. Things like renegotiation, resumption, or Diffie-Hellman key-exchange mechanisms improve the performance and security of a TLS connection as readable in the corresponding RFCs.

In the following chapters, you will find a description of how to create useful X.509 key material.

4.4.4 Using SICAM GridPass to Create Key Material

4.4.4.1 Overview

To support the customer environment with functionalities mentioned above the Siemens SICAM GridPass offers a RA/CA together with an EST server and CRL distribution point. The CA offers the possibility to sign CSRs coming from entities using the EST protocol and the possibility to create local certificates based on X.509.



[sc_SICAM GridPass Workflow, 1, en, en_US]
 Figure 4-101 SICAM GridPass Workflow

4.4.4.2 Workflow

SICAM GridPass can create own (Sub-)CA key material or can import a (Sub-)CA key material from a customer PKI. The EST server is used with a configured X.509 key material issued from a CA which is part of SICAM GridPass. SICAM GridPass can support an arbitrary number of CAs created by SICAM GridPass or imported in SICAM GridPass. Imported and created CAs will be defined as trusted. An EST request from an entity that wants to be authenticated with a certificate issued by an imported or created CA will be always trusted except if it is listed in the CRL. Each authenticated and validated entity can send a CSR to the EST server. The EST server will exhibit a configured server certificate issued by an imported or created CA to the EST client (entity). The EST server uses the configured operational CA to sign the certificate signing request. It is not intended to use different CAs to sign a CSR.

Summary of a CSR Handling

- The EST server trusts any EST client certificate issued by any CA imported or created in SICAM GridPass.
- The EST server checks the offered EST client certificate against the CRL if used.
- The EST server itself uses a server certificate issued by an imported or created CA in SICAM GridPass.
- The EST server uses exactly 1 CA to sign a CSR.
- SICAM GridPass signs any CSR with any content (except the X509v3 extensions for CA usage; these will be set to the basic constraints: critical, CA: FALSE) to convey the signed CSR (the certificate) to the entity.
- SICAM GridPass can revoke an issued certificate for any reasons and will distribute a CRL after revoking to an internal running plain text Web server.
- In general, the CRL has a validity of 24 h and will be distributed every 12 h in case of no new revoked certificates.

4.4.4.3 Integration

A possibility is to create a SICAM GridPass instance or any other customer CA at the Control Center (CC) level and to create the CA certificates for each substation. The CA in the CC environment can be used to support

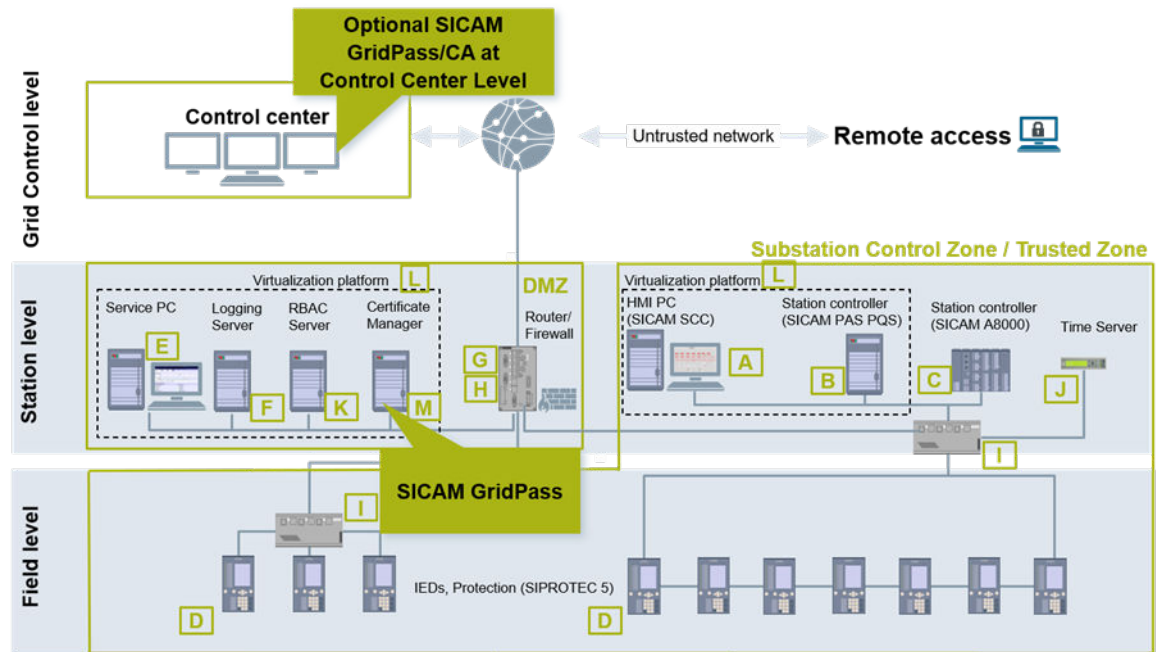
devices at a CC level via EST with certificates. All CAs based at a substation level can support the devices within the substation via EST with certificates.



NOTE

The substation level CA can be derived from a root CA or can also be a root CA. This depends on the company policy.

In the following figure, the design of the CAs for the control center and substation is shown. If more substations are used, the substation control zone can be mirrored.



[sc_EST Integration, 1, en_US]

Figure 4-102 EST Integration

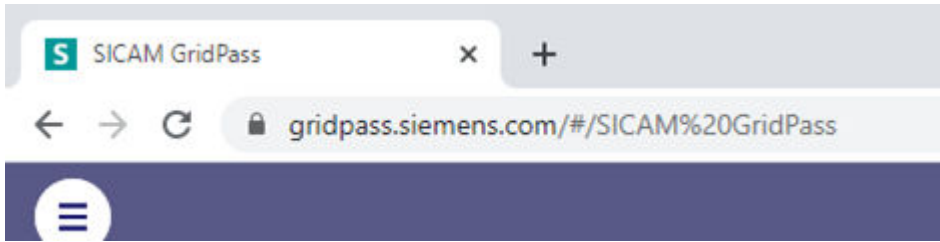
4.4.4.4 Operating Overview

SICAM GridPass offers 3 different TCP-based services:

- **Web UI access SICAM GridPass operation** with https listening per default on standardized TCP port 443
- **CRL server** (CRL distribution point) based on http listening per default on standardized TCP port 80
- **EST server** based on TLS/https listening on a configurable TCP port (not standardized, but TCP 8085 is selected by default)

4.4.4.5 Web UI Access

After the installation of SICAM GridPass, a Web interface for operation listening on each external interface is offered. Therefore, it is possible to manage the certificates, CRL, and entities via a Web browser in a secure way over https. During the installation and configuration phase, the self-signed certificate should be changed by a trusted certificate from SICAM GridPass to get a trusted connection with a browser:

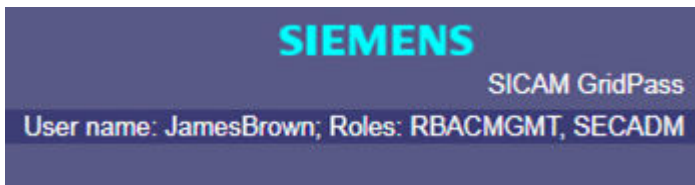


[sc_Web UI Access Link, 1, en_US]

Figure 4-103 Web UI Access Link

Depending on the firewall settings and routings, a substation CA can be managed from the CC or locally within the substation.

SICAM GridPass provides both local and repository-based user management with different roles. SICAM GridPass provides the option to change the local user management to a repository-based user management. LDAP and RADIUS access are supported. This allows to use a RADIUS repository located in the substation or CC to manage SICAM GridPass users.



[sc_Web UI Access User, 1, en_US]

Figure 4-104 Web UI Access User

4.4.4.6 CRL Server

To support the entities within the different zones, a CRL distribution point is provided by SICAM GridPass listening per default on port 80 as a Web server. The CRL support will be configured within the SICAM GridPass Web-based access.

This CRL distribution point is placed inside each created or signed certificate of SICAM GridPass. SICAM GridPass generates for each CA a CRL at least every 12 h. The next update field within the CRL is set to 24 h.

The possibility to provide on the same machine the EST server and the CRL distribution point (CDP) Web server is an advantage for the network configuration because each machine with access to the EST server has also access to the Web server. In general, the CDP is listening on TCP port 80 and is accessible without authentication via http. In general, the substation CRL server will be contacted from the entities inside the same substation.

4.4.4.7 EST Server

SICAM GridPass provides an EST server to handle the EST client entity request for signing the entity CSRs with the configured CA private key. EST support will be configured within the SICAM GridPass Web-based access. Here the trusting between entities and EST server will be configured. The EST server signs all CSR requests coming from an entity authenticated by a trusted CA. In general, the substation EST server will be contacted from the entities inside the same substation.

Entities (Products)

The only way for an entity to authenticate itself to the EST server is using the preinstalled X.509 key material. It depends on the device if it is imprinted by default from the factory or imported during engineering. Also the EST server certificate issued by the CA used for the EST server has to be trusted by the entity. If the mutual trust is engineered, the entity can always obtain a CA-signed certificate by sending a CSR to the EST server. Also for renewal reasons, a CSR can be sent to the EST server. The EST server CA signs all certificates with all X.509 extensions without any validation, except when a CA flag is set in the CSR. An entity cannot obtain a certificate useable as CA. This is the only exception.

4.5 OpenLDAP

4.5.1 Overview

In the IEC 62351-8, RBAC is defined - beside others - with X.509 certificates stored in an LDAP repository. Although Microsoft Active Directory supports LDAP, Siemens recommends OpenLDAP in case a standard LDAP repository is needed. It can be easily installed in any Linux distribution.

4.5.2 Installing OpenLDAP Debian Buster (11)

For more information, refer to the Debian documentation (<https://wiki.debian.org/LDAP/OpenLDAPSetup>).

- ✧ Check the used Linux operating system:

```
lsb_release -a
Distributor ID: Raspbian
Description: Raspbian GNU/Linux 11 (bullseye)
Release: 11
Codename: bullseye
```
- ✧ Update your system:

```
sudo su
aptitude update
aptitude upgrade
```
- ✧ Install the OpenLDAP packages:

```
aptitude install slapd ldap-utils
```
- ✧ Check the initial installation:

```
slapcat
```
- ✧ Check and the hostname of the computer.

```
hostnamectl status
hostnamectl set-hostname TestRaspi.myhome.local
hostnamectl set-icon-name RaspberryPiTest
hostnamectl status
```
- ✧ In case of a static IP address, configure the file **/etc/hosts**:

```
nano /etc/hosts
```
- ✧ In the file, add the line:

```
<static_IP-Address>TestRaspi.myhome.local TestRaspi
```
- ✧ Start the reconfiguration of the OpenLDAP package **slapd**:

```
dpkg-reconfigure slapd
```
- ✧ Select **No** and skip the existing OpenLDAP configuration. This keeps the existing configuration available.
- ✧ Enter the DNS local domain name for your OpenLDAP server and select **OK**.
- ✧ Enter the LDAP administrator password.
- ✧ Decide if you want to remove your configuration in case of removing **slapd**.
- ✧ Select **Yes** and create a new database with new entries:

```
slapcat
```
- ✧ Restart and check the **slapd** running state:

```
systemctl restart slapd
systemctl status slapd
```

- ✧ Download the program **LDAP Admin** (refer to <https://sourceforge.net/projects/ldapadmin/files/ldapadmin/>).
For more information, refer to the official LDAP Admin documentation (refer to <http://www.ldapadmin.org/docs/index.html>).

Adding a User

- ✧ Create a new user under the root tree of LDAP:

```
nano GivenNameSurname.ldif
```



```
dn: cn=GivenNameSurname,dc=TestRaspi,dc=myhome,dc=local
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
cn: GivenNameSurname
sn: Surname
givenName: GivenName
uid: gsurname
mail: givenName.surname@siemens.com
```
- ✧ Add the user to the LDAP repository:

```
ldapadd -D "cn=admin,dc=TestRaspi,dc=myhome,dc=local" -W -H
ldapi:/// -f GivenNameSurname.ldif
```
- ✧ Check the user to the LDAP repository:

```
ldapsearch -x -b "dc=TestRaspi,dc=myhome,dc=local" cn
```

Preparing the OpenLDAP System for TLS and StartTLS

- ✧ Open SICAM GridPass.
For more information, refer to the SICAM GridPass documentation.
- ✧ Create a TLS server certificate and export it as a .p12 file.
- ✧ Export the root CA certificate as a .pem file.
- ✧ Copy the root CA certificate and the .p12 server key material to your OpenLDAP system with SCP or WinSCP (refer to <https://winscp.net/eng/index.php>) in your home directory.
- ✧ Use OpenSSL to generate the key and certificate from the .p12 file:

```
cd /home/pi
openssl pkcs12 -in OpenLDAPServer.p12 -nodes | openssl ec -inform PEM
-outform PEM -out
OpenLDAPServer_key.pem
openssl pkcs12 -in OpenLDAPServer.p12 -out OpenLDAPServer_cert.pem -nokeys
```



NOTE

In case of RSA key material, use `rsa` instead of `ec`.

Setting Up OpenLDAP with TLS and StartTLS

- ✧ Create 2 new folders:

```
mkdir -p /etc/ssl/openldap/{private,certs}
```


- ✧ Copy the key material to the new folders:

```
cp /home/pi/OpenLDAPServer_cert.pem /etc/ssl/openldap/certs/  
cp /home/pi/AndreasPICA.pem /etc/ssl/openldap/certs/  
cp /home/pi/OpenLDAPServer_key.pem /etc/ssl/openldap/private/
```
- ✧ Change the ownership of the folders and files:

```
chown -R openldap: /etc/ssl/openldap/
```

Updating OpenLDAP Database with Server TLS Certificate

- ✧ Create a new ldif file, for example, with nano:

```
nano ldap-tls.ldif
```
- ✧ Create the following entries:

```
dn: cn=config  
changetype: modify  
add: olcTLSCACertificateFile  
olcTLSCACertificateFile: /etc/ssl/openldap/certs/AndreasPICA.pem  
-  
replace: olcTLSCertificateFile  
olcTLSCertificateFile: /etc/ssl/openldap/certs/OpenLDAPServer_cert.pem  
-  
replace: olcTLSCertificateKeyFile  
olcTLSCertificateKeyFile: /etc/ssl/openldap/private/OpenLDAPServer_key.pem
```
- ✧ Import the ldif file to the OpenLDAP database:

```
ldapmodify -Y EXTERNAL -H ldapi:/// -f ldap-tls.ldif
```
- ✧ Check the import:

```
ldapsearch -Y EXTERNAL -H ldapi:/// -b cn=config | grep olcTLS
```
- ✧ Check the configuration:

```
slaptest -u  
config file testing succeeded
```
- ✧ Restart OpenLDAP:

```
systemctl restart slapd
```

Adding TLS Listening on TCP/636

- ✧ Update the slapd configuration as shown in the file and restart the OpenLDAP service:

```
nano /etc/default/slapd
```
- ✧ Search for `SLAPD-SERVICES` and add `ldaps:///` to the line.
- ✧ Restart OpenLDAP:

```
systemctl restart slapd
```
- ✧ Check the listening port for `tcp:389` and `tcp:636`:

```
netstat -tulpen
```

Configuring TLS in LDAP Admin

- ✧ In LDAP Admin, open the connection properties.
- ✧ For TLS, select **SSL** and enter the following parameter:

```
Port: 636  
Base: dc=TestRaspi,dc=myhome,dc=local
```

- ✧ For StartTLS, select **TLS** and enter the following parameter:
Port: 389
Base: dc=TestRaspi,dc=myhome,dc=local
- ✧ Log on to LDAP with your administrator account.
- ✧ Import the certificate and place it in the folder for the trusted root certification authorities.

Setting Up OpenLDAP (Optional)

- ✧ Create a new ldif file, for example, with nano:
nano disable-anon.ldif
- ✧ Create the following entries:
dn: cn=config
changetype: modify
add: olcDisallows
olcDisallows: bind_anon

dn: cn=config
changetype: modify
add: olcRequires
olcRequires: authc

dn: olcDatabase={-1}frontend,cn=config
changetype: modify
add: olcRequires
olcRequires: authc
- ✧ Import the ldif file to the OpenLDAP database:
ldapadd -Y EXTERNAL -H ldapi:/// -f disable-anon.ldif

Creating an Entry

- ✧ In LDAP Admin, create a new user.
- ✧ Import the <name>.ldif file.

Creating Additional Administrator Accounts

- ✧ Display current access rights:
ldapsearch -H ldapi:// -Y EXTERNAL -b "cn=config" olcAccess

- ✧ Create a new entry via Ldif for a user allowed to manage all entries (for example, the subtree **people**):


```
nano LDAPAdmin_olcAccess.ldif
dn: olcDatabase={1}mdb,cn=config
changetype:modify
add: olcAccess
olcAccess: {0}to attrs=userPassword by self =xw by anonymous auth by
dn.base="uid=AdminLDAP01,ou=LDAPAdmin,dc=TestRaspi,dc=myhome,dc=local" =w by * none
-
add: olcAccess
olcAccess: {1}to dn.subtree="ou=people,dc=TestRaspi,dc=myhome,dc=local" by
dn.base="uid=AdminLDAP01,ou=LDAPAdmin,dc=TestRaspi,dc=myhome,dc=local"
write by self read by * none
-
add: olcAccess
olcAccess: {2}to dn.children="ou=LDAPAdmin,dc=TestRaspi,dc=myhome,dc=local"
by self read by * none
```
- ✧ Modify the olcAccess in the cn=config repository:


```
ldapmodify -Y EXTERNAL -H ldapi:/// -f LDAPAdmin_olcAccess.ldif
ldapsearch -H ldapi:// -Y EXTERNAL -b "cn=config" olcAccess
```

Exporting Certificate to LDAP

- ✧ In SICAM GridPass, export the certificate as a directory service (LDAP).
- ✧ Enter the LDAP user and the LDAP password.

Importing an X.509 Certificate

- ✧ Create a new user Ldif file, for example, with nano:


```
nano GivenNameSurname.ldif
```
- ✧ Create the following entries (according to the RFC 4523):


```
dn: cn=GivenNameSurname,dc=TestRaspi,dc=myhome,dc=local
changetype: modify
add: userCertificate;binary
userCertificate;binary:< file:///home/siemens/GivenNameSurname.der
```
- ✧ Import the Ldif file to the OpenLDAP database:


```
ldapmodify -D "cn=admin,dc=TestRaspi,dc=myhome,dc=local"
-W -H ldapi:/// -f GivenNameSurname.ldif
```
- ✧ If necessary, convert PEM to DER:


```
openssl x509 -inform pem -in GivenNameSurname.pem
-outform der -out GivenNameSurname.der
```
- ✧ Create a new user Ldif file, for example, with nano:


```
nano GivenNameSurname.ldif
```
- ✧ Create the following entries:


```
dn: cn=GivenNameSurname,dc=TestRaspi,dc=myhome,dc=local
changetype: modify
add: userCertificate;binary
userCertificate;binary::MIIDKzCCAtGgAwIBAgIUfTfm <base64>
+q49vvSpdPN0gKcRjG89yac1EkHa3BcwC5y1Zo+bpw=
```

- ✧ Import the ldif file to the OpenLDAP database:

```
ldapmodify -D "cn=admin,dc=TestRaspi,dc=myhome,dc=local"  
-W -H ldapi:/// -f GivenNameSurname.ldif
```
- ✧ In LDAP Admin, check the certificate.



NOTE

Access Rights

The default access rules of Debian allow only the system root user to change the configuration by connection with the SASL EXTERNAL authentication:

```
ldapsearch -Y EXTERNAL -H ldapi:/// -b "cn=config"
```

The directory can be searched by every user without any authentication:

```
ldapsearch -x -b "dc=TestRaspi,dc=myhome,dc=local"
```

The database administrator has unrestricted access. To connect as the database administrator, use the simple authentication and enter the password configured during the installation.

```
ldapsearch -x -D "cn=admin,dc=TestRaspi,dc=myhome,dc=local" -W -b  
"dc=TestRaspi,dc=myhome,dc=local"
```

```
ldapsearch -x -D "cn=admin,dc=TestRaspi,dc=myhome,dc=local" -w <password> -b  
"dc=TestRaspi,dc=myhome,dc=local"
```

4.5.3 OpenLDAP Attribute Certificates

An userCertificate attribute is normally part of the following objectClass for a standard LDAP repository:

- inetOrgPerson (Oid: 2.16.840.1.113730.3.2.2 registered by IETF (RFC 2798))
- pkiUser (Oid: 2.5.6.21 registered by ITU)

or for the Microsoft Active Directory Service:

- inetOrgPerson (Oid: 2.16.840.1.113730.3.2.2 registered by IETF (RFC 2798))
- user (Oid: 1.2.840.113556.1.5.9 registered by Microsoft)

OpenLDAP

In general, OpenLDAP does not support attribute certificates. This is because - according to the RFC 4523 - the supported syntax of a certificate is defined as an X.509 certificate only. An attribute certificate is defined in clause 14 of the X.509 specification. Therefore, it is currently not defined for the usage in an LDAP directory service.

Microsoft Active Directory Service

In an Microsoft Active Directory service, an attribute certificate can be imported although the userCertificate is also used with the OID 2.5.4.36 as in a standardized LDAP repository. But, Microsoft uses the syntax ID 1.3.6.1.4.1.1466.115.121.1.40.

Using a defined syntax, all types of data artifacts - therefore also attribute certificates - can be stored even if the definition and standard view contradicts this.

4.5.4 Using Active Directory in an OpenLDAP Environment

If LDAP has not yet defined an attribute similar to the attribute userCertificate and if no objectClass exists where the new attribute should be used, a workaround for LDAP-based systems is possible. During this workaround, the userCertificate syntax is changed.

- ✧ Log on directly to device with the system on which OpenLDAP is installed or log on via SSH access.

- ✧ Change to the root account.

**NOTE**

If you already imported certificates before changing the schema, you can no longer see the old certificates. In addition, it is not possible to import new certificates if users already had certificates before.

- ✧ Remove all certificates. Otherwise, no import of new certificates is possible.
- ✧ Open the file `cn={0}core.ldif` containing the core schema. Depending on your Linux distribution, you find the file in a different location. For Ubuntu, for example:


```
root@ubuntu:/etc/ldap/slapd.d/cn=config/cn=schema#
-rw----- 1 openldap openldap 15578 Mär 27 18:43 cn={0}core.ldif
```

 Besides other attributes and objectClasses, you can find the attribute `userCertificate` as an `olcAttributeType` in this file:


```
olcAttributeTypes: {30}( 2.5.4.36 NAME 'userCertificate' DESC 'RFC2256: X.509 user certificate, use ;binary' EQUALITY certificateExactMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.8 )
```
- ✧ Log on as the root user.
- ✧ Create a ldif file to change the configuration, for example, a `newUserCertificateSyntax.ldif` in the home directory:


```
dn: cn={0}core,cn=schema,cn=config
changetype: modify
delete: olcAttributeTypes
olcAttributeTypes: ( 2.5.4.36 NAME 'userCertificate' DESC 'RFC2256: X.509 user certificate, use ;binary' EQUALITY certificateExactMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.8 )
-
add: olcAttributeTypes
olcAttributeTypes: ( 2.5.4.36 NAME 'userCertificate' DESC 'Octet String' EQUALITY octetStringMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.40 )`
```

 Siemens recommends not to change the file directly.
- ✧ Add an empty line at the end of the file.
- ✧ Copy the original file as a backup to your home directory:


```
cp /etc/ldap/slapd.d/cn=config/cn=schema/cn={0}core.ldif
/home/siemens/cn={0}core.ldif.org
```
- ✧ Execute the new configuration on the system on which OpenLDAP is installed:


```
ldapmodify -Y EXTERNAL -H ldapi:/// -f /home/siemens/newUserCertificateSyntax.ldif
```

The attribute `userCertificate` is deleted and added again with the new SYNTAX(-ID), a new EQUALITY and a new DESC.

- ✧ Restart your LDAP server:


```
root@ubuntu:/etc/ldap/slapd.d/cn=config/cn=schema# /etc/init.d/slapd restart
[ ok ] Restarting slapd (via systemctl): slapd.service.
```

The new schema with the changed `userCertificate` syntax is identical to the Microsoft Active Directory Service.

Using LDAP Commands

- ✧ To show the content of a user including imported certificates:


```
ldapsearch -D "cn=admin,dc=localhost,dc=siemens,dc=de" -w <password>
-p 389 -h 127.0.0.1 -b "cn=Manfred Schmidt,dc=localhost,dc=siemens,dc=de"
```

- ✧ To import an attribute value to a user, for example, a X.509 base64 encoded certificate:


```
ldapmodify -x -W -D "cn=admin,dc=localhost,dc=siemens,dc=de"
            -f /home/siemens/ManfredSchmdit.ldif
```

 when the Ldif file includes the following entry:


```
dn: cn=Manfred Schmdit,dc=localhost,dc=siemens,dc=de
            changetype: modify
            add: userCertificate
            userCertificate:< file:///home/siemens/AndreasGuettinger.pem
```
- ✧ To directly change a configuration on the system:


```
ldapmodify -Y EXTERNAL -H ldapi:///
            -f /home/siemens/newUserCertificateSyntax.ldif
```

4.5.5 LDAP and Microsoft Active Directory

LDAP and Microsoft Active Directory have some differences. The most significant difference is the class user which is only available in Microsoft Active Directory. The class includes the attribute userPrincipalName which is named **User logon name** in Microsoft and has the value name@domain.

This attribute is used for the logon in Microsoft Active Directory. It cannot be used for LDAP as the class user and therefore also the attribute userPrincipalName (for example, tomjones@certman.test) are not available in an LDAP repository.

The default way for both repositories is to use the complete DN (bindDN) of a user, for example, cn=Tom Jones,CN=Users,DC=certman,DC=test.

The screenshot shows the Microsoft Active Directory console with a tree view on the left and a detailed attribute list on the right. The tree view shows the hierarchy: DC=certman,DC=test [192.168.56.101] > OU=Domain Controllers > CN=Users > CN=John Smith. The right pane displays the following attributes and values:

Attribute	Value	Type	Size
objectClass	top	Text	3
objectClass	person	Text	6
objectClass	organizationalPerson	Text	20
objectClass	user	Text	4
objectClass	inetOrgPerson	Text	13
cn	John Smith	Text	10
sn	Smith	Text	5
userCertificate	30 82 04 91 30 82 04 37 A0 03 02 01 02 02 14 0E 7A 80 DE 67 77 CE EE 6E 0F AF...	Certi...	1174
givenName	John	Text	4
distinguishedName	CN=John Smith,CN=Users,DC=certman,DC=test	Text	41
instanceType	4	Text	1
whenCreated	20200203163404.0Z	Text	17
whenChanged	20220830094231.0Z	Text	17
displayName	John Smith	Text	10
uSNCreated	86110	Text	5
uSNChanged	127049	Text	6
name	John Smith	Text	10
objectGUID	AB C5 22 0D 53 FD CB 41 9C 8D E0 58 74 49 06 5B	Binary	16
userAccountControl	66048	Text	5
badPwdCount	0	Text	1
codePage	0	Text	1
countryCode	0	Text	1
badPasswordTime	0	Text	1
lastLogoff	0	Text	1
lastLogon	0	Text	1
pwdLastSet	132252212444189873	Text	18
primaryGroupID	513	Text	3
objectSid	01 05 00 00 00 00 05 15 00 00 00 08 28 A9 F0 60 94 62 4F CA 10 64 92 7A 0...	Binary	28
accountExpires	9223372036854775807	Text	19
logonCount	0	Text	1
sAMAccountName	johnsmith	Text	9
sAMAccountType	805306368	Text	9
userPrincipalName	johnsmith@certman.test	Text	22
objectCategory	CN=Person,CN=Schema,CN=Configuration,DC=certman,DC=test	Text	55
dSCorePropagation...	20200203163404.0Z	Text	17
dSCorePropagation...	16010101000000.0Z	Text	17

[DN_Active Directory, 1, en_US]

Figure 4-105 Microsoft Active Directory Repository

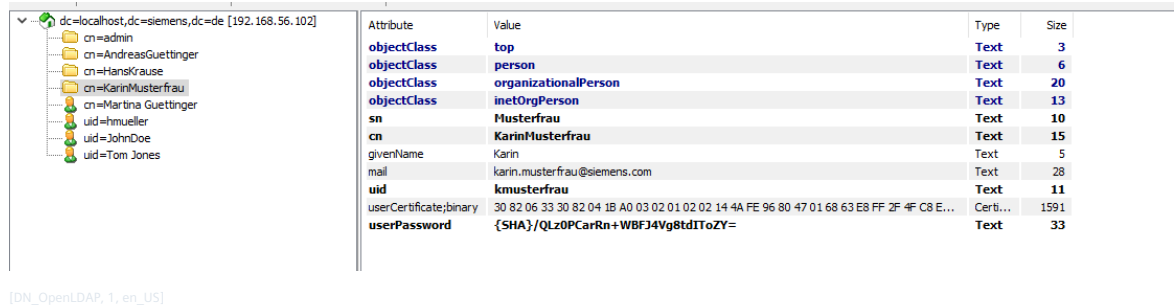


Figure 4-106 LDAP Repository

SIPROTEC 5 Logon Methods

For SIPROTEC 5, you can log on with the DN and the userPrincipalName with Microsoft Active Directory and with the DN with LDAP.

If the checkbox **Bind with Parent DN** is not selected, the conventional approach (person@domain.com) is used. If the checkbox is selected, the DN approach is used by reconstructing the CN (user input) and the parent DN (setting) to bind the user.

The BaseDN (search DN) is explicitly separated from the BindDN as the BaseDN is the recursive search string while the BindDN is the pointer to the LDAP object. In most cases, these 2 are identical. However, for multi-site repositories, they might differ.

4.6 Device-Specific Configuration Notes

4.6.1 SICAM SCC

SICAM SCC (SICAM Station Control Center) represents a powerful, universally applicable process visualization system that offers all features of a sophisticated HMI software. The SIMATIC WinCC is the platform on which SICAM SCC operates. A project is visualized and operated by the SICAM SCC Runtime system.

The SICAM SCC user account management is based on the Windows account management. In addition, SICAM SCC allows for additional application-level account management.

The SIMATIC WinCC Explorer is used by system engineers.

The SICAM SCC runtime is used by system administrators, system engineers, operators, and the special user (that can access Web Navigator over Web Navigator Client) for **Login without password**.

The SICAM SCC runtime engine requires Windows auto-logon to start the SICAM SCC runtime automatically. After Windows has concluded the auto-logon process, SIMATIC WinCC starts the project and the user can have access to SICAM SCC runtime (configuration made in the SIMATIC tool **Autostart**).

4.6.1.1 Setting Up User Authorizations

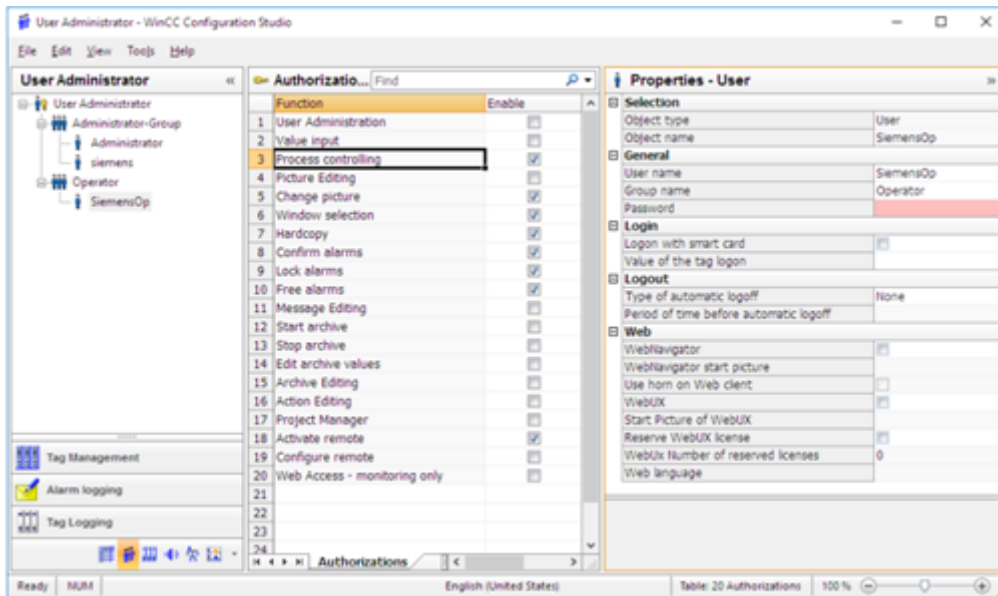
Siemens suggests to create the following users inside the SICAM SCC environment with the authorizations as indicated:

Table 4-3 Authorizations per User in SICAM SCC

Authorization/User	Admin Group	Non-Admin Group	
	Admin	Eng	Oper
User administration	X	X	–
Value input	–	–	X
Process controlling	–	–	X
Picture editing	–	X	–
Picture change	–	X	X
Window selection	X	X	–

Authorization/User	Admin Group		Non-Admin Group	
	Admin	Eng	Oper	
Hard copy	X	X	X	
Confirming messages	–	–	X	
Locking messages	–	–	X	
Unlocking messages x	–	–	X	
Message editing	–	X	–	
Starting archive	–	X	–	
Stopping archive	–	X	–	
Archive value editing	–	X	–	
Archive editing	–	X	–	
Action editing	–	X	–	
Project manager	–	X	–	

✦ Open the WinCC Explorer and double-click the **User Administrator** level.



[sc_Configuring SICAM SCC Access, 1, en_US]

Figure 4-107 Configuring SICAM SCC Access

Creating a Group

- ✦ Select **User** and **Add group**.
- ✦ Enter the name of the new user group.
- ✦ Assign the group rights by double-clicking the desired row in the **Authorization** column.

Creating New Users

After creating the 2 recommended groups, it is time to create new users.

- ✦ Select the group under which you wish to create a new user, select **User** and **Add User**.
- ✦ Enter the user name in the **Login** field.
- ✦ Fill the **Password** fields and complete.

Assigning Authorizations

There is an option to copy group settings that assign the same authorizations as the group to these new users. However, even inside a group it is recommended to split authorizations by user, like in the suggestion table. After creating 3 users under the respective 2 groups, assign the authorizations individually for each one, based on [Table 4-3](#).

- ✧ Double-click the user name and double-click the desired row in the **Authorization** column.

The screenshot shows the 'User Administrator - WinCC Configuration Studio' interface. On the left, a tree view shows the hierarchy: 'User Administrator' > 'Group1' > 'User_1'. Below 'Group1', there are 'Ansehen' and 'Steuern' sub-items. Other groups listed include 'Administrator-Group', 'Logon_Administrator', and several 'SCC-Admin' roles. On the right, the 'Authorizations [User...]' table is displayed. The table has two columns: 'Function' and 'Enable'. Row 2, 'Value input', is highlighted with a black box, and its 'Enable' checkbox is checked. Other rows have their 'Enable' checkboxes either checked or unchecked.

	Function	Enable
1	User Administration	<input type="checkbox"/>
2	Value input	<input checked="" type="checkbox"/>
3	Process controlling	<input checked="" type="checkbox"/>
4	Picture Editing	<input type="checkbox"/>
5	Change picture	<input checked="" type="checkbox"/>
6	Window selection	<input checked="" type="checkbox"/>
7	Hardcopy	<input checked="" type="checkbox"/>
8	Confirm alarms	<input checked="" type="checkbox"/>
9	Lock alarms	<input checked="" type="checkbox"/>
10	Free alarms	<input checked="" type="checkbox"/>
11	Message Editing	<input type="checkbox"/>
12	Start archive	<input type="checkbox"/>
13	Stop archive	<input type="checkbox"/>
14	Edit archive values	<input type="checkbox"/>
15	Archive Editing	<input checked="" type="checkbox"/>
16	Action Editing	<input checked="" type="checkbox"/>
17	Project Manager	<input type="checkbox"/>
18		<input type="checkbox"/>
19		<input type="checkbox"/>
20		<input type="checkbox"/>
21		<input type="checkbox"/>
22		<input type="checkbox"/>
23	Activate remote	<input type="checkbox"/>
24	Configure remote	<input type="checkbox"/>
25	Web Access - monitoring only	<input type="checkbox"/>
26		
27		
28		

[sc_Access User Function, 2, en_US]

Figure 4-108 Access User Function

Assigning Authorizations by Object

- ✧ In the Graphics Design, double-click the object to open the **SICAM Switch Control Properties** dialog.
- ✧ Select the **Advanced** tab and click ... to the right of the **Operator authorization** field.
- ✧ Select the desired authorization.

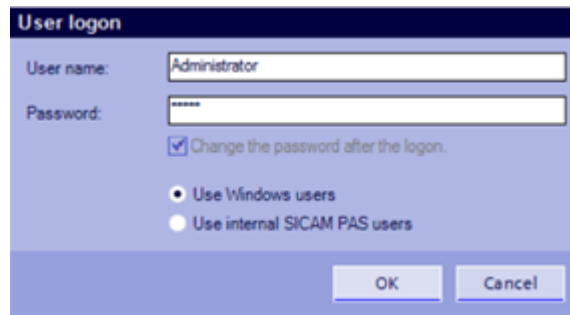
For more details, refer to the *SICAM SCC* manual.

4.6.2 SICAM PAS

SICAM PAS is used by system administrators and system engineers. System engineers need to access SICAM PAS applications (such as UI Configuration and UI Operation).

4.6.2.1 Setting Up User Administration

✧ In Windows, go to **Start** → **All Apps** → **SICAM PAS/PQS** → **User Administration**.



[sc_SICAM PAS Access Configuration, 1, en_US]

Figure 4-109 SICAM PAS Access Configuration

The Default Credentials are:

- Username: Administrator
- Password: Admin

After the first login, choose between **Use Windows users** or **Use internal SICAM PAS users**. This setting can be changed later in the **User Administration** window under **Tools** by selecting **Type of user administration**. For Active Directory Users, the Windows Users shall be selected.



NOTE

Use of AD users may create problems as the Domain SID.

4.6.3 SIPROTEC 5 and DIGSI 5

SIPROTEC 5 devices support role-based access control with a central user management in RADIUS/Active directory among other advanced cybersecurity features. To access information on a SIPROTEC 5 device or to perform actions on the device, optionally the role-based access control (RBAC) can be enabled. After activation, the operator must authenticate and authorize himself as a user before each interaction with the device. All SIPROTEC 5 devices can be connected to a central RADIUS server containing the authentication and authorization configuration. RADIUS is a standardized client/server protocol and the client implementation is integrated in the SIPROTEC 5 device firmware.

When creating a new SIPROTEC 5 device in DIGSI 5, by default, the following set of standard confirmation IDs and connection passwords has to be used:

- Settings/operation: 222222
- Switching (process): 333333
- Switching (unlocked): 444444
- Switching authority: 666666

For details to enable and configure the RBAC feature, refer to [4.3.3 User Management of the SIPROTEC/SICAM Device](#).

4.6.4 SICAM A8000/SICAM Device Manager

The SICAM Device Manager is the engineering software for SICAM A8000. SICAM A8000 CP-8050 performs the role-based access model. The configuration of RBAC is carried out by the IED. In case of engineering SICAM A8000 CP-8000/CP-802x via SICAM Device Manager/SICAM WEB, user authentication and login are carried out separately for each device via the group accounts **Administrator** (read/write: can use all functions of the engineering too) and **Guest** with read-only access.

4.6.5 RuggedCom Switch RSG2100

The switch can be administered via Serial Console, Telnet, SSH, RSH, and a Web-based user interface. Access to the switch is only required for system administrators.

The following 3 user accounts are predefined in the RuggedCom switch:

- **guest**:
can view most settings, but may not change settings or run commands
- **operator**:
cannot change settings, but can reset alarms, clear statistics, and logs
- **admin**:
can change all the settings and run commands

These 3 predefined user accounts cannot be deleted or deactivated. Additional user accounts cannot be created.

The system administrator can use the predefined **admin** user account to perform his tasks. For better security, it is recommended to use as well the other 2 predefined users **operator** and **guest**, if tasks have to be performed at the switch, for which not the complete super user capability is needed.

The passwords of the 3 users need to be changed using the **Passwords** menu.

- 15-character ASCII string is allowed for a password.
- No password expiration capability is available.

4.6.6 RuggedCom RX 1400/RX1500

The router can be administered via Serial Console, SSH, and a Web-based user interface (WebUI). Access to the router is only required for system administrators.

The system administrator can use the predefined **admin** user account with default password of **admin** for the first setup. RuggedCom ROX II can be accessed through a direct serial or Ethernet connection. The MGMT port can be used to connect to RuggedComROX II through the network on default IP **192.168.1.2/24** using a Web browser.

RuggedCom ROX II allows for up to 3 user profiles to be configured locally on the device. Each profile corresponds to one of the following access levels:

- Guest
- Operator
- Admin

The access levels provide or restrict the user's ability to change settings and execute various commands.

Table 4-4 Rights for User Type in ROS

Rights	User Type		
	Guest	Eng	Oper
View Settings	x	x	x
Clear Logs	x	x	x

Rights	User Type		
	Guest	Eng	Oper
Reset Alarms	–	x	x
Clear Statistics	–	x	x
Change Basic Settings	–	x	x
Change Advanced Settings	–	–	x
Run Commands	–	–	x

5 Security Logging and Monitoring

5.1	General	150
5.2	Logging Architecture	151
5.3	Logging Windows System	151
5.4	Logging with Syslog	158
5.5	Logging in Siemens Products	161
5.6	Recommendations	172

5.1 General

Security monitoring is a very important part of cybersecurity as the security is not a one-time event. Threats and vulnerabilities are continuously evolving and this necessitates monitoring and logging events continuously. Most of the security requirement catalogs, like IEC 62443, NERC CIP, and BDEW White Paper, ask for an implementation of a manual or automatic process for monitoring electronic access to the control system. For that purpose, all products provide at least local logging facilities used for logging of security-relevant events like:

- Failed/successful login
- Logout
- Changes in user/password management (user added, deleted, modified, etc.)
- Software/firmware updates

Additional central logging is required for an easy overview and a fast response.

For large systems, it is useful to inspect log files from a centralized point. Due to high volume of log, a manual check is impossible and ineffective thus the automated monitoring using SIEM is recommended. This chapter explains different approaches to implement such a centralized logging.

Network devices like routers and switches are in general syslog-ready and offer various log files with different kinds of log levels. Windows provides several log files, but does not support syslog by default. To make Windows possible to send syslog information to a centralized source, it is required to install 3rd party software with the capability of forwarding Windows event logs as well as 3rd party log files (Windows firewall logs).

Central logging with Microsoft included native programs is not so easy. So it is not possible to log all relevant log data to a central Syslog server. For this, you need third-party software, for example, the Datagram Syslog Agent distributed by Datagram Consulting as **Free software** delivered under the GPLv2 license.

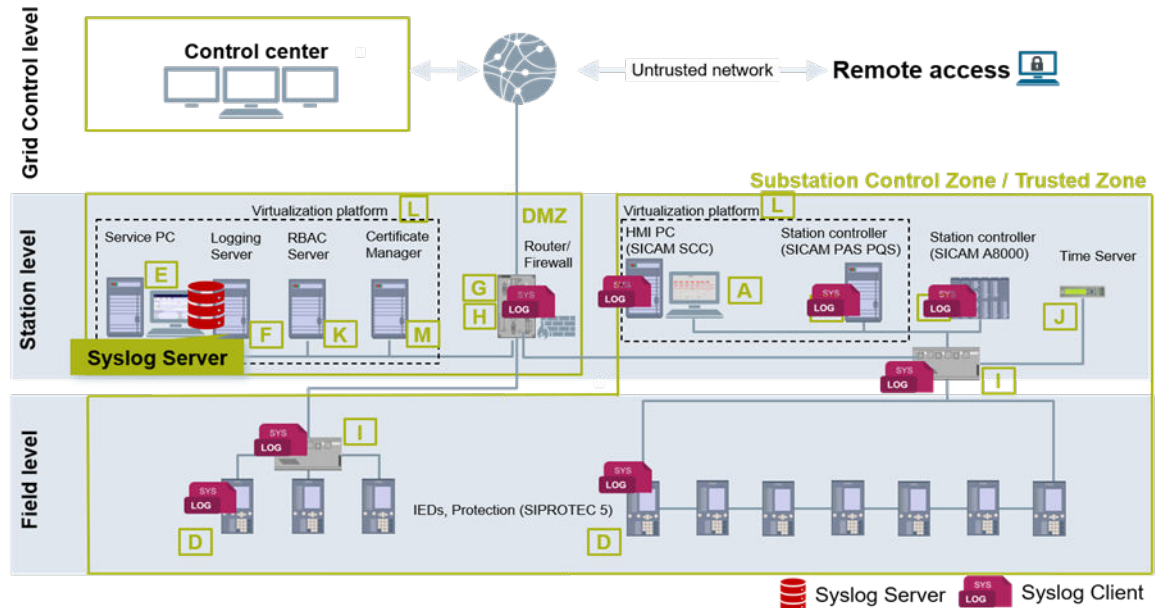
All the components of the Secure Substation support security logging through Syslog. To transfer the logs to a Centralized Syslog server in Windows, a 3rd party application utility may be required.



NOTE

Ensure that all firewalls in the solution allow Syslog protocol traffic.

5.2 Logging Architecture



[sc_Security Logging Architecture, 1, en_US]

Figure 5-1 Security Logging Architecture

The above figure shows architecture of Syslog logging. All the Syslog clients send logs to the Syslog server placed in the station level DMZ. The server can further forward these logs to a centralized SIEM at the control center level as discussed in [5.6.1 SIEM as a Service](#).

5.3 Logging Windows System

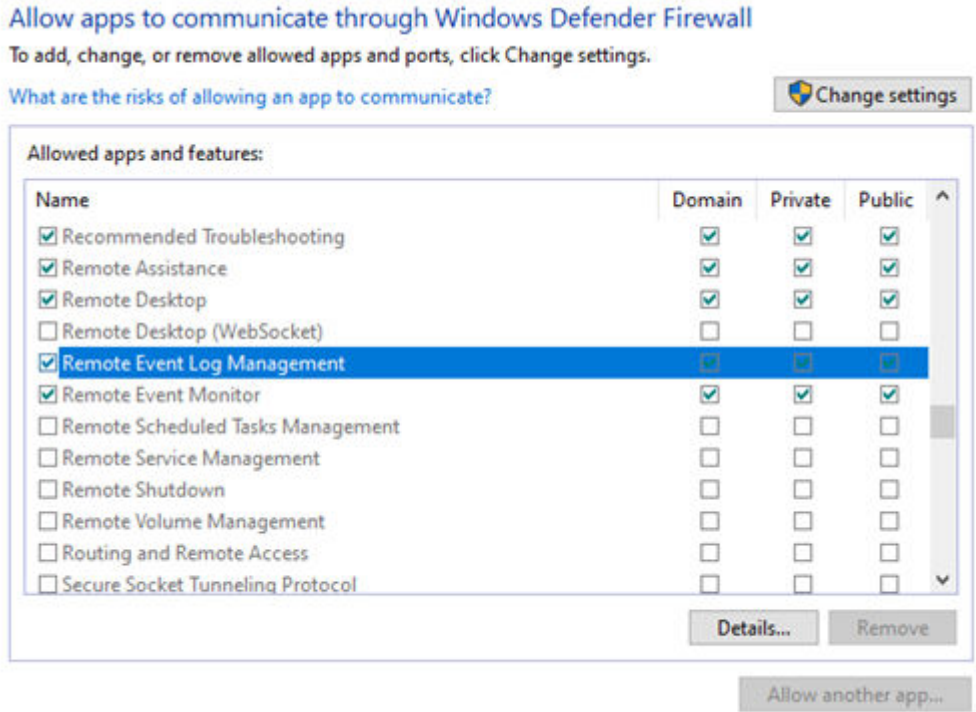
Central logging with the Microsoft native Syslog server is not possible for all the relevant events. For this, third-party software is required:

<https://nxlog.co/products/nxlog-enterprise-edition/download>

Windows also supports remote event log access via the included Event viewer. To view the remote log files, you have to observe a few boundary conditions. If you have any troubles, see also the **Event Viewer Troubleshooting** from Microsoft.

(<http://technet.microsoft.com/en-us/library/cc738322%28WS.10%29.aspx>)

- To read the log files, you need administrator rights on the remote machine. This user must also be created on the local machine with the same password. As a security best practice, consider using **Run as** to perform this procedure. Siemens recommends creating an audit-administrator on the remote and the local machine with administrator rights.
- Next, on diverse Windows operating systems, the Remote Registry Service must be started for you to be able to see the Description or Category fields in the property page for an event log.
- If the firewall is activated as recommended, open the incoming traffic for remote event logging.



[sc_general_logging, 2, en_US]

Figure 5-2 Enable Remote Event Log in Windows Server

5.3.1 Viewing Remote Logs in the Windows Event Viewer

Windows machines can be configured centrally to remote access of logs via Group Policy objects:

Secpol.msc → **Security Settings** → **Local Policies** → **Security Options**

→ **Edit security** setting to for

Force audit policy subcategory settings = Enabled

Secpol.msc → **Security Settings** → **Advanced Audit Policies – Local Group Policy Object**

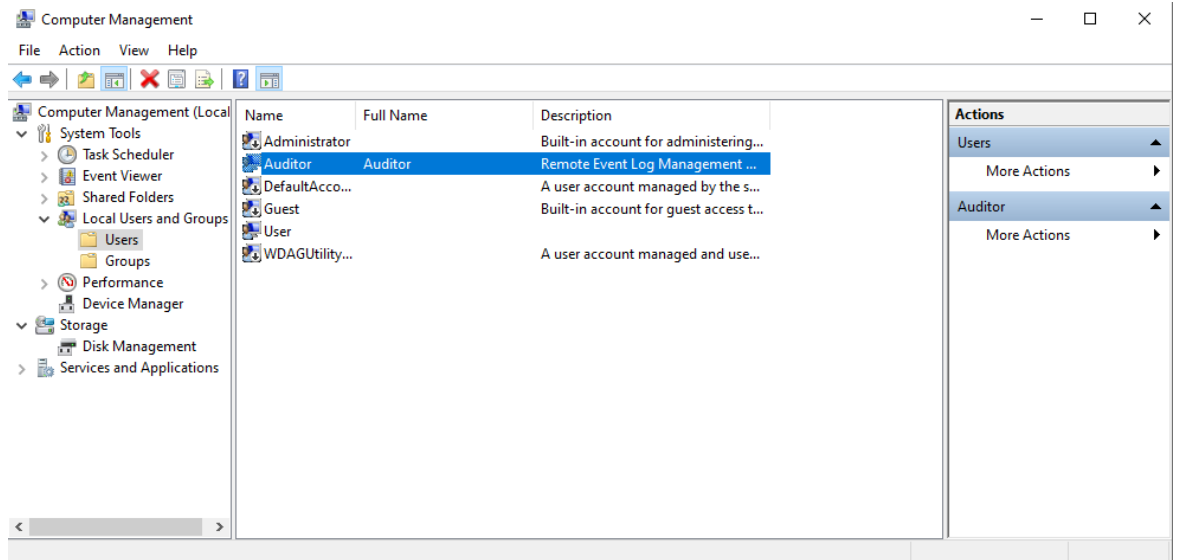
The following section is a step-by-step manual for Windows 10 (Local Site) and Windows Server 2016/2019 (Remote Site).

- ✧ Create a user **Auditor** in the remote machine (Windows 10).



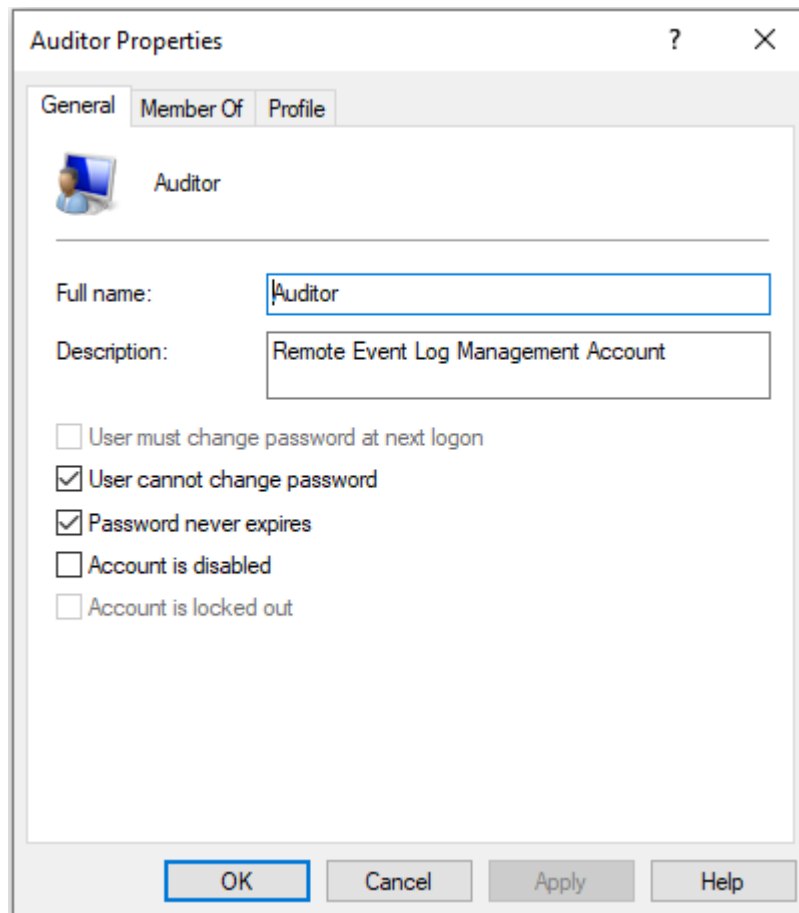
NOTE

For consistence on local and remote site, you always need the same logon and password. For this, a Domain Controller concept is better.



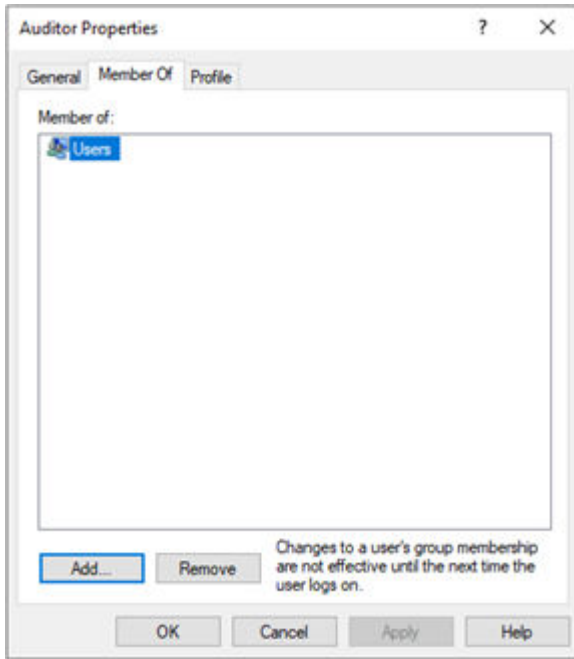
[sc_user_auditor, 2, en_US]

Figure 5-3 Creating an Auditor User



[sc_Windows 1020162019 User Auditor, 1, en_US]

Figure 5-4 Windows 10/2016/2019 User Auditor



[sc_Selecting Auditor Group, 1, en_US]

Figure 5-5 Selecting Auditor Group

- ✧ Activate the Remote Event Log Management on remote site.

Allow apps to communicate through Windows Defender Firewall

To add, change, or remove allowed apps and ports, click Change settings.

What are the risks of allowing an app to communicate?

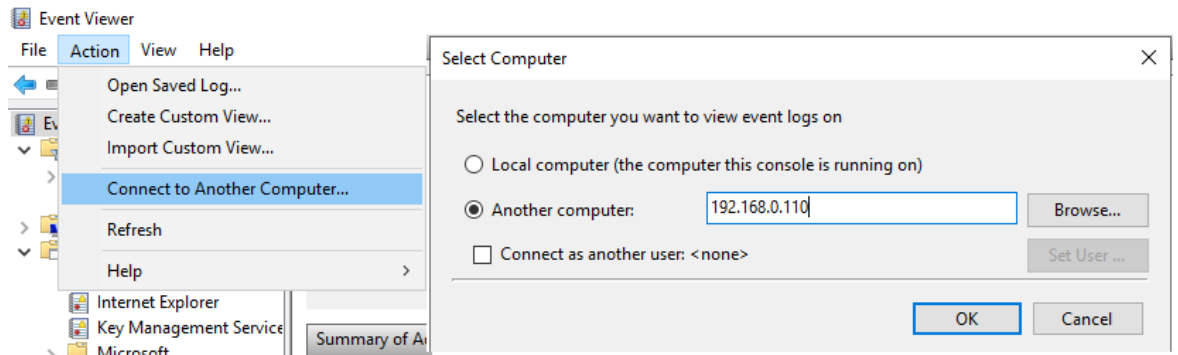
Allowed apps and features:

Name	Domain	Private	Public
<input checked="" type="checkbox"/> Recommended Troubleshooting	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Remote Assistance	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Remote Desktop	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Remote Desktop (WebSocket)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Remote Event Log Management	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Remote Event Monitor	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Remote Scheduled Tasks Management	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Remote Service Management	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Remote Shutdown	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Remote Volume Management	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Routing and Remote Access	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Secure Socket Tunneling Protocol	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

[sc_enable_remote_event_log, 2, en_US]

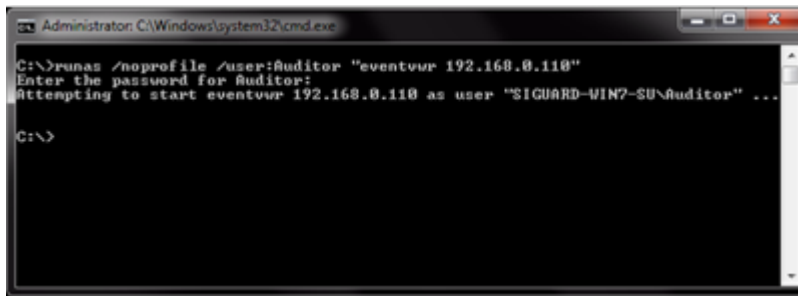
Figure 5-6 Enable Remote Event Log

- ✧ On local site, start the remote Event Viewer via user interface or command shell.



[sc_user_interface, 2, en_US]

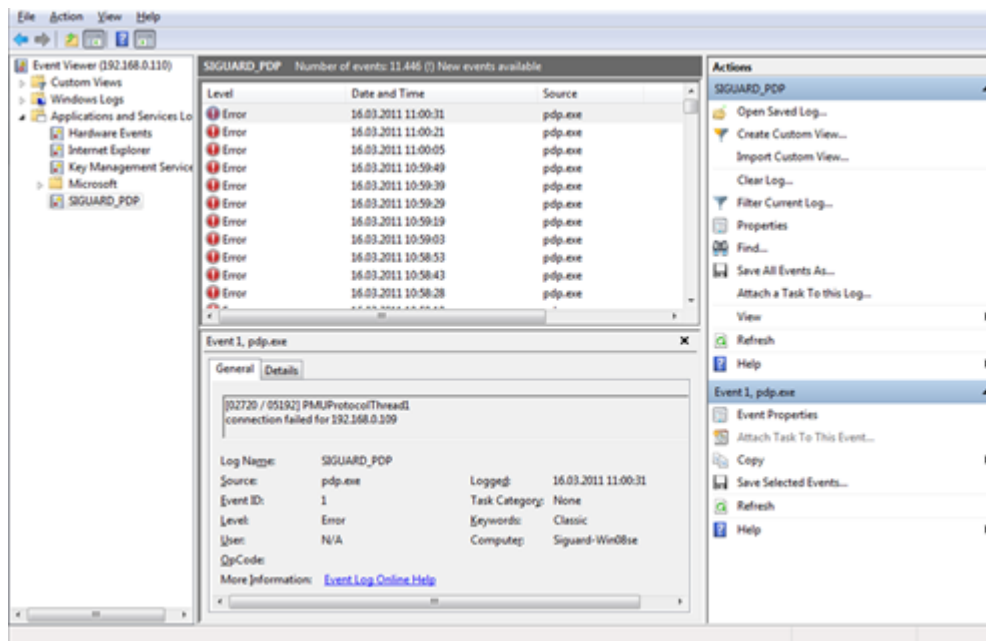
Figure 5-7 User Interface



[sc_start_remote_event_viewer, 2, en_US]

Figure 5-8 Start Remote Event Viewer>

Now, you are connected to server logs:

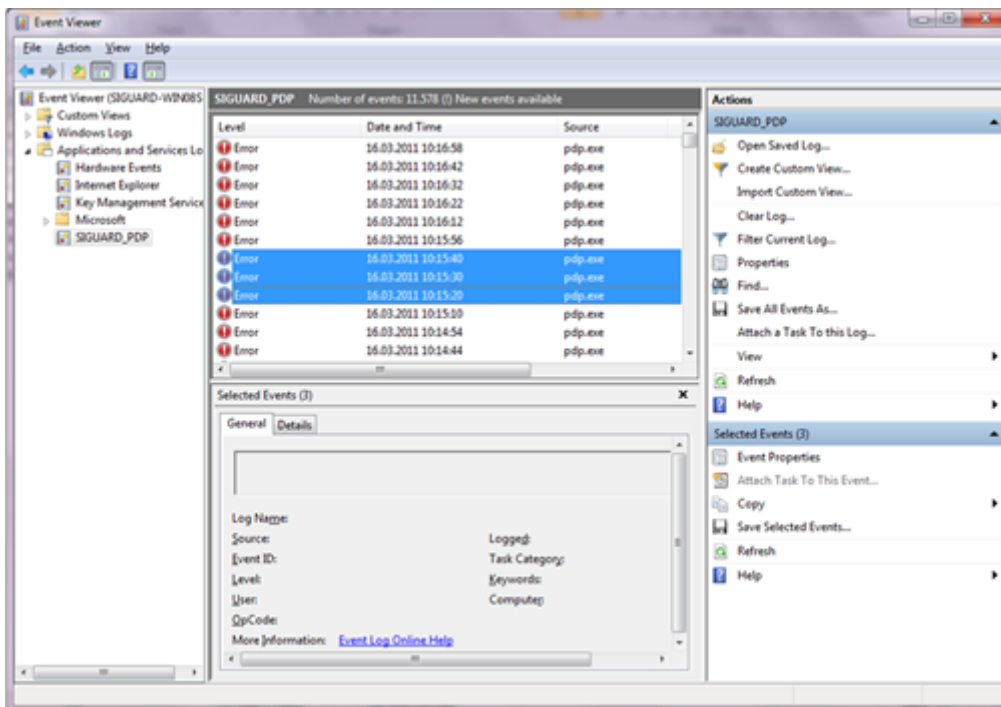


[sc_remote_event_viewer, 2, en_US]

Figure 5-9 Remote Event Viewer

After that, you can store log events you want.

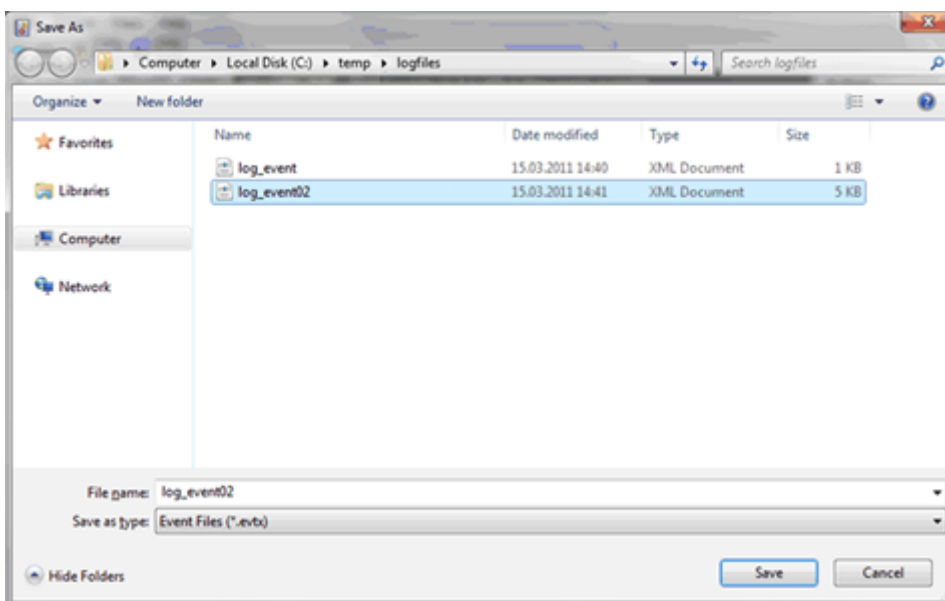
- ✧ Select events you want to store and select the **Save Selected Events...** menu on the right.



[sc_select_events_save, 2, en_US]

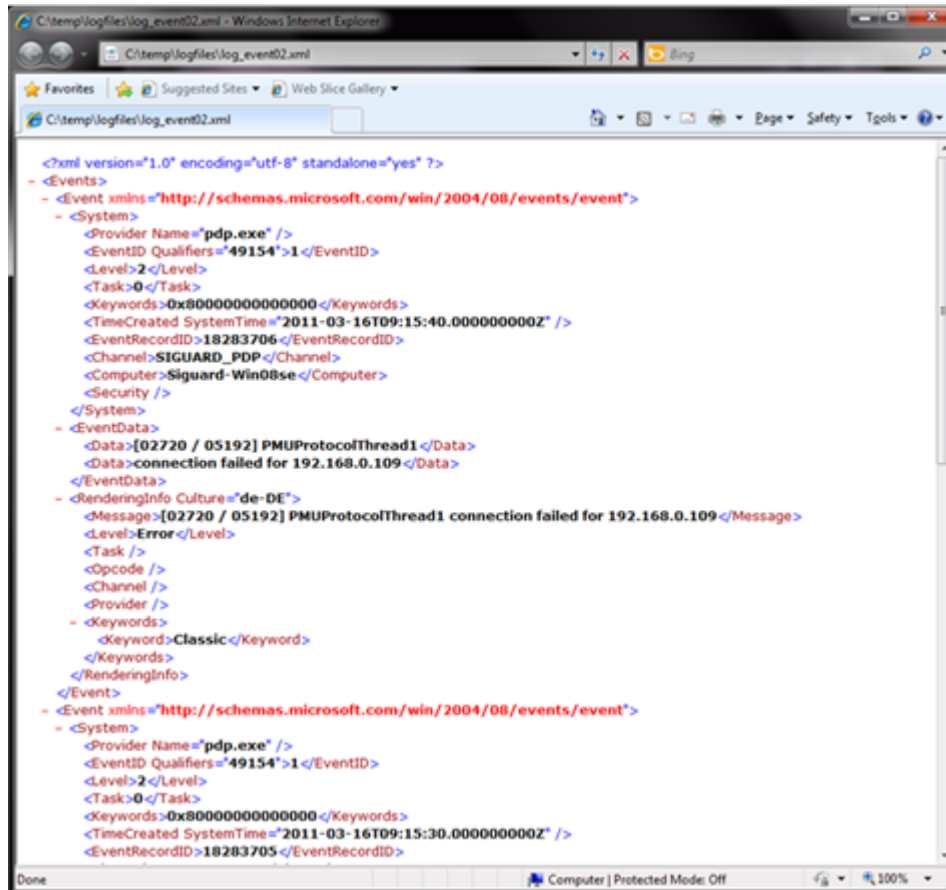
Figure 5-10 Select Events

Now, you can store the files as .txt or .xml file for further action:



[sc_select_events_format, 2, en_US]

Figure 5-11 Eventlog



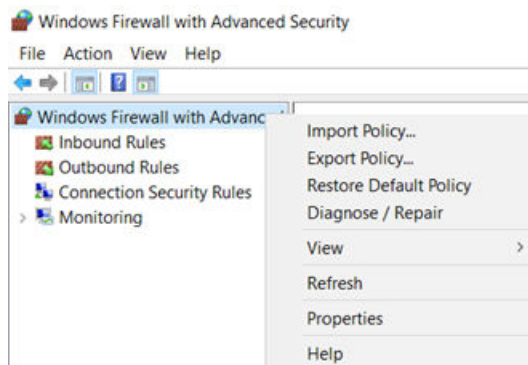
[sc_event_log_xml, 2, en_US]

Figure 5-12 Event Log Export as XML

5.3.2 Firewall Logs

It is possible to configure the firewall to generate a log file in text format, it could be done following the steps below. But the real recommendation is to enable in the Windows Event Log the acquisition of the log files and to use this tool to manage the logs.

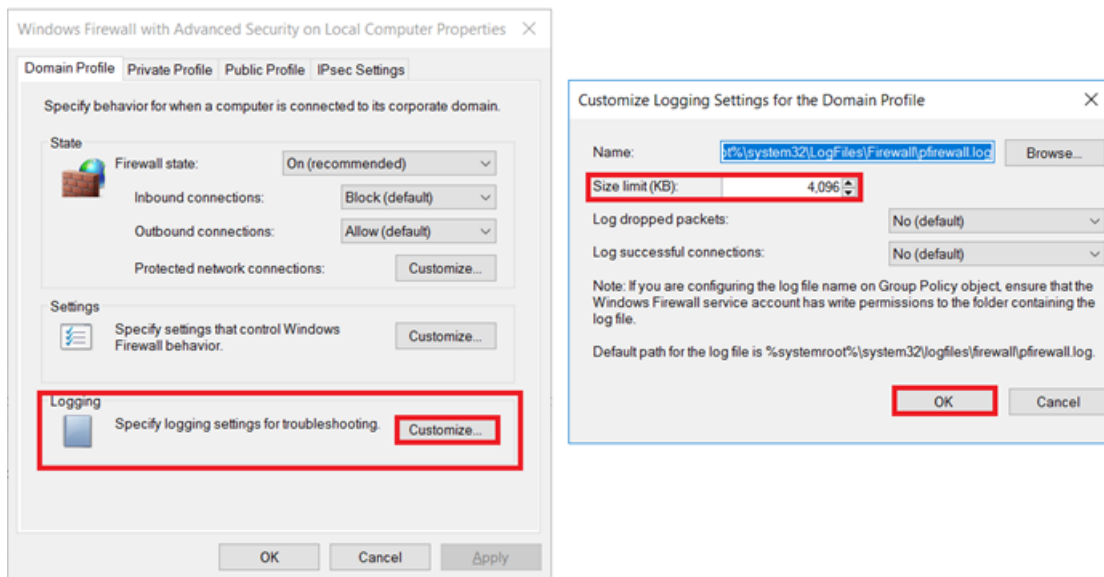
- ✧ To configure the size of firewall logs, go to the Windows **Start** menu, search for the **Windows Firewall with Advanced Security**, and open it.
- ✧ Right-click **Windows Firewall with Advanced Security** and select **Properties**.



[sc_Firewall Logs, 1, en_US]

Figure 5-13 Firewall Logs

- ✧ Look for Logging settings and set the **Size limit (KB)** to 1GB (1000000KB).



[sc_Firewall Log Size Configuration, 1, en_US]

Figure 5-14 Firewall Log Size Configuration

5.3.3 PowerShell Logs

The Windows PowerShell logging can be enabled using the **Group Policy Editor**.

- ✧ To enable this, navigate to:
Computer configuration → **Administrative Templates** → **Windows Components** → **Windows PowerShell**
- ✧ To configure Windows PowerShell Logging remotely, open the **Windows Event Viewer** again and under **Applications and Services Logs**, select **Windows PowerShell**.
- ✧ Right-click **Windows PowerShell** and select **Properties**.
- ✧ Customize the log size to 1 GB.
- ✧ Also, navigate under **Application and Services Logs** → **Microsoft** → **Windows** → **PowerShell** to select **Operational**.
- ✧ Right-click **Operational** and select **Properties**.
- ✧ Customize the log size to 1 GB.
- ✧ Finally, under **Application and Services Logs**, navigate under **Microsoft** → **Windows** to select **Windows Remote Management**.
- ✧ Customize this log size to store it for at least one year.

5.4 Logging with Syslog

5.4.1 Logging with Syslog

Normally, Windows programs do not support the syslog protocol. To enable logging to a central syslog server, the capabilities of the regular Microsoft Windows logging system, needs to be extended, syslog protocol is supported by most of the applications. The easiest way is to convert Windows Event log messages to syslog

messages with a local wrapper. The NXLog Enterprises Edition may be used for this (<https://nxlog.co/products/nxlog-enterprise-edition/download>).

In concept NXLog is like syslog-ng or rsyslog but it is not limited to Unix and syslog only. It supports different platforms, log sources and formats. Thus, nxlog can be an ideal choice to implement a centralized logging system. It can collect logs from files in various formats, receive logs from the network remotely over UDP, TCP or TLS/SSL on all supported platforms. It supports platform-specific sources such as the Windows Eventlog, Linux kernel logs, Android device logs, local syslog etc. Writing and reading logs to/from databases is also supported for many database servers. The collected logs can be stored into files, databases or forwarded to a remote log server using various protocols.



NOTE

You can use NXLog as syslog server and as a syslog client that is reading the events from the MS event viewer, converting to syslog format and forward to a centralized syslog server. For help see <https://nxlog.co/docs/nxlog-ce/nxlog-reference-manual.html>.

5.4.2 syslog Client

The 3rd party Software NXLog in the community version supports the reading of Microsoft event logging and the converting to the syslog format defined in the RFC 5424. Filter can be used as it is from the Microsoft event viewer filter in XML format. The converting happens automatically but can also be adjusted if necessary (see the NXLog documentation for more information).

The following example shows the configuration for logging the above shown event log entries stored in a file and transmitted via UDP syslog protocol, both formatted according to RFC 5426.

```
### This is a sample configuration file. See the nxlog reference manual
## https://nxlog.co/docs/nxlog-ce/nxlog-reference-manual.html about the
## configuration options.

## Please set the ROOT to the folder your nxlog was installed into,
## otherwise it will not start.
## Running the executable with the -f command line argument will run it
## in foreground if you don't want to run it as a service.

#define ROOT C:\Program Files\nxlog
define ROOT C:\Program Files (x86)\nxlog
define SYSLOGFILE %ROOT%\data\syslog.log

Moduledir %ROOT%\modules
CacheDir %ROOT%\data
Pidfile %ROOT%\data\nxlog.pid
SpoolDir %ROOT%\data
LogFile %ROOT%\data\nxlog.log

<Extension _syslog>
  Module xm_syslog
</Extension>

<Input in>
  # input from the MS event log
  Module im_msvistalog
  ReadFromLast True
  # copied from event viewer XML query
  <QueryXML>
    <QueryList>
      <Query Id="0" Path="Security">
        <Select Path="Security">*[System[(Level=1 or Level=2)]]</Select>
      </Query>
    </QueryList>
  </QueryXML>
```

```
</QueryList>
</QueryXML>
</Input>

<Output file>
  Module    om_file
  File      '%SYSLOGFILE%'
  # Output in IETF syslog format as defined by RFC 5424
  Exec      to_syslog_ietf();
</Output>

<Output syslogudp>
  Module    om_udp
  Host      172.17.17.245
  Port      514
  Exec      to_syslog_ietf();
</Output>

<Route 1>
  Path      in => file, syslogudp
  # output to the local syslog file and to the remote syslog server
</Route>
```

The typical configuration example to read a SICAM PAS entry can be configured in the following way:

```
<QueryXML>
  <QueryList>
    <Query Id="0">
      <Select Path="PASecurity">*</Select>
    </Query>
  </QueryList>
</QueryXML>
```

5.4.3 syslog Server

5.4.3.1 General

This chapter shows how to use a syslog server in Substation Automation. A syslog server is required to collect logs from all the devices in the substation and forward the logs to a central (Security Information and Event Management).

5.4.3.2 Syslog Server with NXLog

As described in the chapter before NXLog can also be used as a syslog server. In this case the NXLog server is listening on the dedicated UDP port as defined in the RFC 5426.

Enclosed an example of a NXLog server listening on UDP port 514 and writing all inputs to a local file. Additional the logfile is rotating and storing the older one:

```
define ROOT C:\Program Files (x86)\nxlog
define SYSLOGFILE %ROOT%\data\syslog.log
```

```
Moduledir %ROOT%\modules
CacheDir %ROOT%\data
Pidfile %ROOT%\data\nxlog.pid
SpoolDir %ROOT%\data
LogFile %ROOT%\data\nxlog.log
```

```
<Extension _syslog>
  Module    xm_syslog
</Extension>
```



```

<Input in>
  Module      im_udp
  Host        167.87.41.10
  Port        514
</Input>

Output out>
  Module      om_file
  File        '%SYSLOGFILE%'
</Output>

<Route 1>
  Path        in => out
</Route>

#check the size of the Syslog file periodically (e.g. every hour) and rotate it
#if it is larger than e.g. 1Mb.
#I.e. 'file' will be moved to "'file'.1".
#If "'file'.1" already exists it will be moved to "'file'.2" and so on,
#until e.g. 5 files reached, then oldest file will be removed.
<Extension fileop>
  Module xm_fileop

  <Schedule>
    Every 1 hour
    Exec if (file_size('%SYSLOGFILE%') >= 1M) file_cycle('%SYSLOGFILE%', 5);
  </Schedule>
</Extension>

```

The NXLog can also be used as an intermediate syslog server and can forward the syslog messages additional to an external (central) syslog server.

```

<Output file>
  Module      om_file
  File        "%SYSLOGFILE%"
</Output>

<Output centralsyslog>
  Module      om_udp
  Host        172.17.17.245
  Port        514
</Output>

<Route 1>
  Path        in => file, centralsyslog
</Route>

```

5.5 Logging in Siemens Products

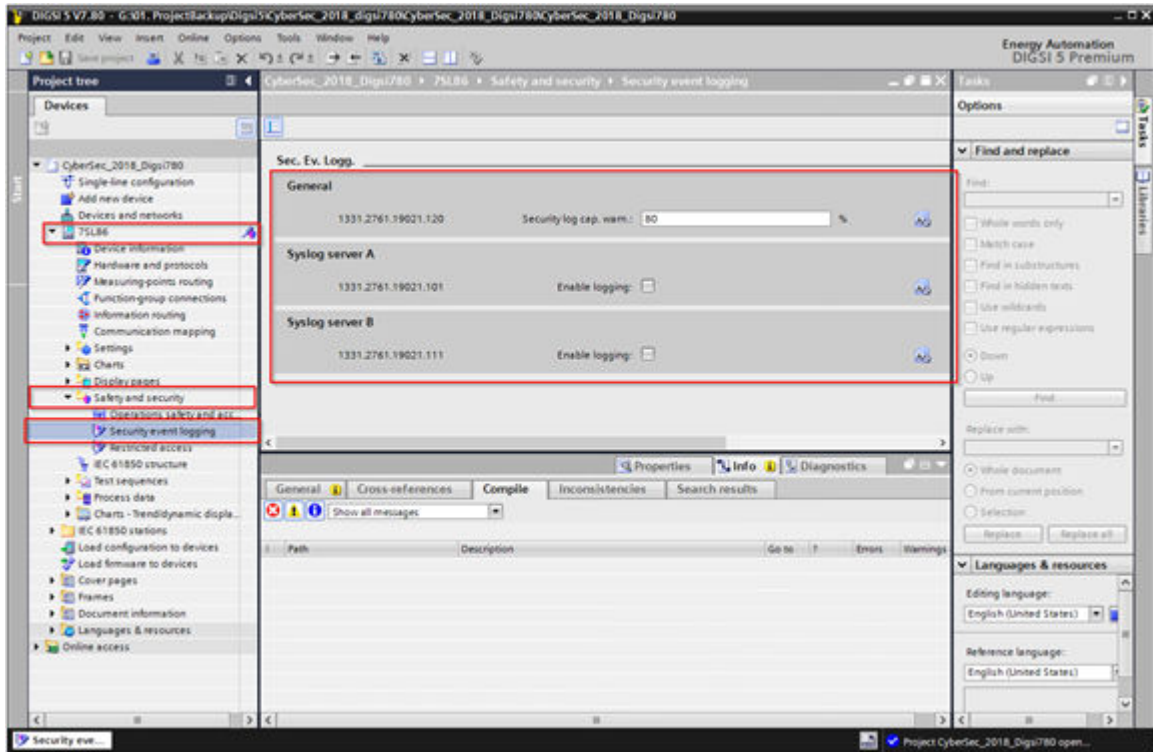
5.5.1 SIPROTEC 5

For SIPROTEC 5 devices, starting from firmware version 7.50 and above, recordings are automatically created for cybersecurity events during the operation of the IEDs. All security-related events and alarms recorded in the internal log can also be transmitted simultaneously to a central syslog server. Logging is started centrally on 1 or 2 self-selected syslog servers.

5.5.1.1 Configuring the Central Syslog Server

To configure the syslog Server in the SIPROTEC 5 devices, open DIGSI 5 and select the desired device.

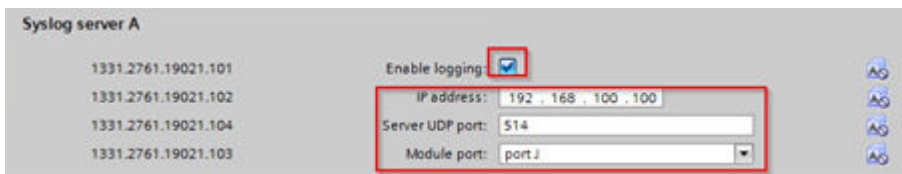
- ✧ Navigate to **Safety and security** and double-click **Security event logging**.



[sc_Central Logging in SIPROTECS DIGSIS, 1, en_US]

Figure 5-15 Central Logging in SIPROTEC 5/DIGSI 5

- ✧ In the **Sec. Ev. Logg.**, up to 2 syslog servers can be activated. In the **General** area, the capacity warning level of the device-internal security log can be defined, where when enabling logging for Syslog server A or B, the settings for **IP address**, **Server UDP port**, and **Module port** can be configured.



[sc_Adding Syslog Server IP, 1, en_US]

Figure 5-16 Adding Syslog Server IP

With the adjustable setting: **Security log cap. warn.** threshold, it can be determined from which utilization of the security log on a warning indication is issued. A warning threshold of 80 % means that the set capacity limit has been reached after approx. 1600 entries in the security log. Further warning indications are issued when the capacity limits of 85 %, 90 %, 95 %, and 98 % are reached.

If the log organized as a ring buffer exceeds the 100 % capacity limit, the oldest entries are automatically overwritten, and the capacity utilization is reset to 0 %. When the security log is read using DIGSI 5, the capacity utilization is reset to 0 %. The indications remain in the device. All settings must be applied with DIGSI 5.

5.5.2 SICAM PAS

For SICAM PAS, there are 2 methods of collecting the Syslog events:

- Using the Syslog functionality implemented in the User Administration
- Transmitting the PAS Security events generated and displayed in the Windows event viewer using a Syslog collector, such as NXLog

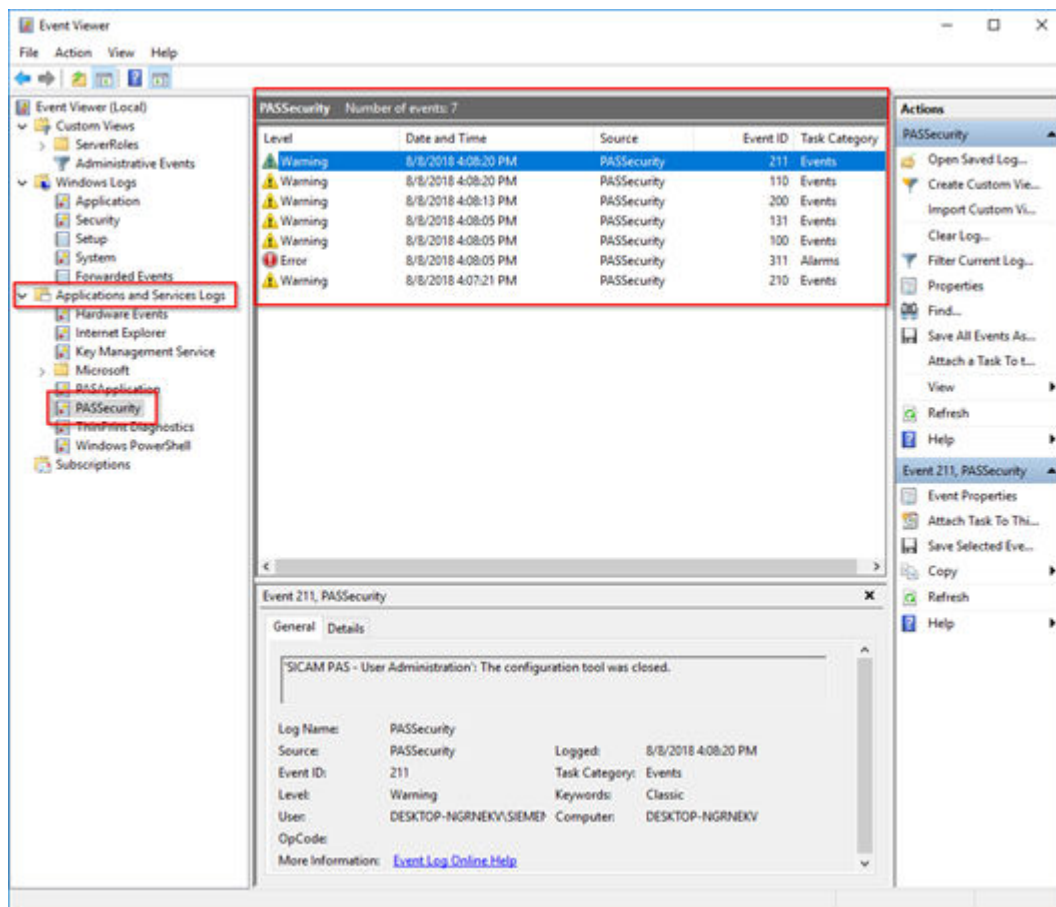
The following section shows logging using User Administration Method.

5.5.2.1 SICAM PAS Security Log Events

During the installation of SICAM PAS v8.10 and above, the security log events are available and displayed in the Windows Event Viewer.

✧ To access it, simply logged on as **Administrator**, open **Start** → **Search Bar**, type **Event Viewer**, and click **Enter**.

SICAM PAS Events will be available in **Applications and Services Logs** → **PASSecurity**.

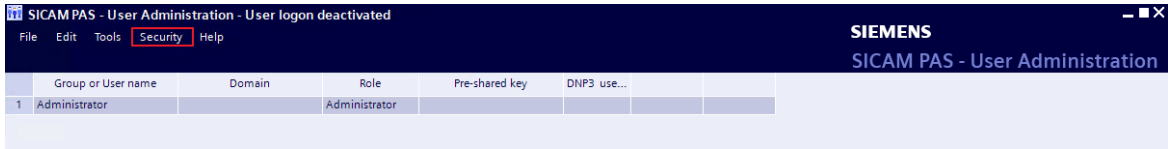


[sc_Enabling logging in SICAM PAS, 1, en_US]

Figure 5-17 Enabling Logging in SICAM PAS

5.5.2.2 Configuring Syslog

In this section, the method used for User Administration is demonstrated. For this case, only the Administrator and Security Administrators can view the **Security** menu.

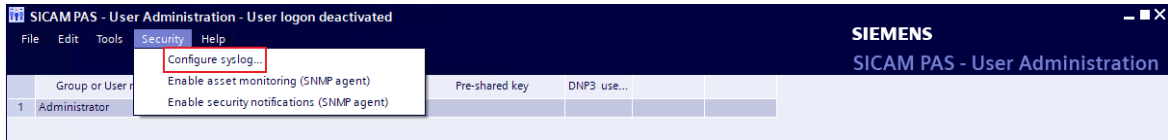


[sc_Enabling Syslog in SICAM PAS, 1, en_US]

Figure 5-18 Enabling Syslog in SICAM PAS

To configure Syslog, proceed as follows:

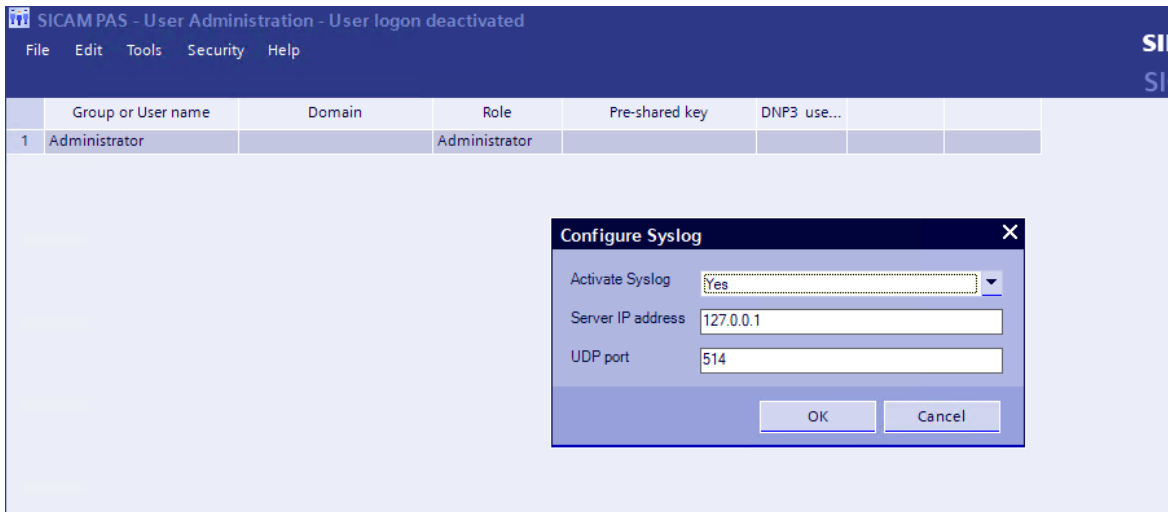
- ✦ Select **Security** → **Configure Syslog...**



[sc_Configuring Syslog logging in SICAM PAS, 1, en_US]

Figure 5-19 Configuring Syslog Logging in SICAM PAS

- ✦ Activate Syslog selecting **Yes**, then type the **Server IP address** and **UDP port**.



[sc_Adding Syslog Server IP in SICAM PAS, 1, en_US]

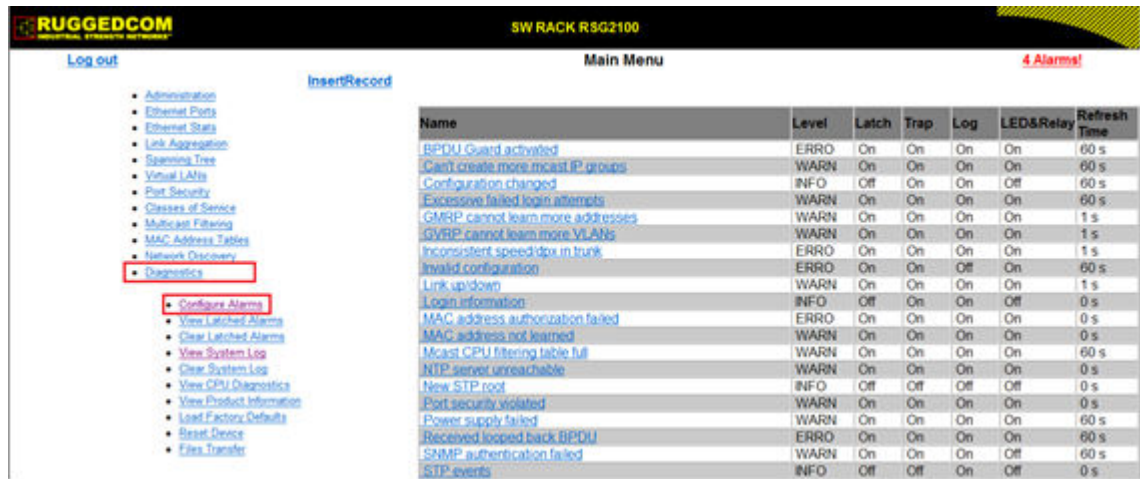
Figure 5-20 Adding Syslog Server IP in SICAM PAS

- ✦ Click **OK**.
- ✦ After the Syslog is configured, update the system in SICAM PAS/PQS UI – Operation.

5.5.3 RuggedCom Switch RSG2100

5.5.3.1 Alarm Configuration for Syslog

- ✦ Log in to the switch as admin user.
- ✦ Navigate in the main tree to **Diagnostics** → **Configure Alarms** and choose which of the preconfigured alarms should go in the Syslog.

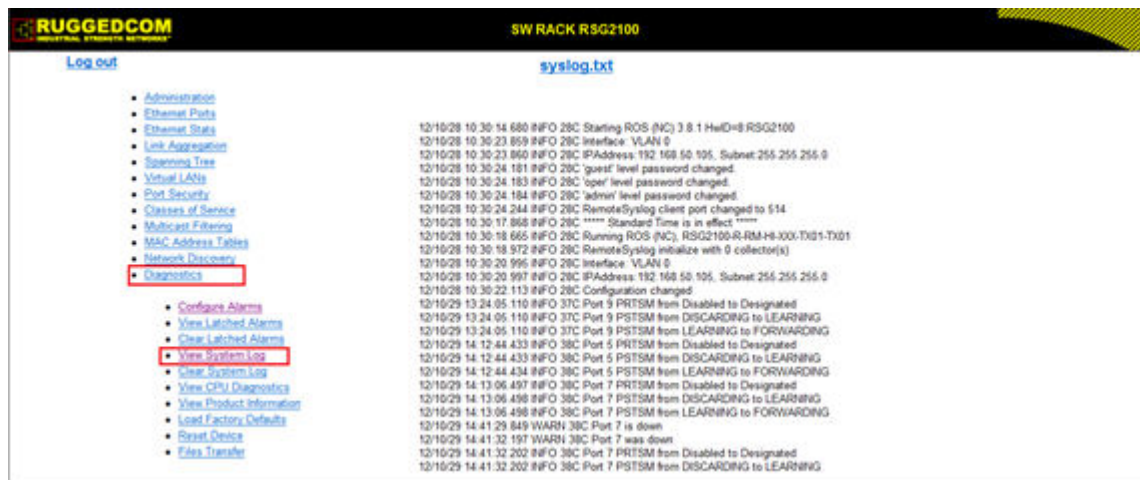


[sc_Configuring Syslog logging in Ruggedcom Router, 1, en_US]

Figure 5-21 Configuring Syslog logging in Ruggedcom Router

5.5.3.2 Display Syslog Information

- ✦ To check the logs on the switch, you must navigate to **Diagnostics** → **View System Log**.



[sc_Display Syslog logging in Ruggedcom Router, 1, en_US]

Figure 5-22 Display Syslog Logging in Ruggedcom Router

5.5.3.3 Syslog Server Connection

- ✦ Log in to the RSG2100 as admin user.
- ✦ First, you must configure the local syslog level. Navigate in the right tree to **Administration** → **Configure Syslog** → **Configure Local Syslog** and set it to **INFORMATIONAL**.



[sc_Configuring Syslog Server Connection in Ruggedcom Router, 1, en_US]

Figure 5-23 Configuring Syslog Server Connection in Ruggedcom Router

It represents the severity of the message that has been generated. Note that the severity level selected is considered the minimum severity level for the system. For example, if ERROR is selected, the system sends any syslog messages generated by Error, Critical, Alert, and Emergency.

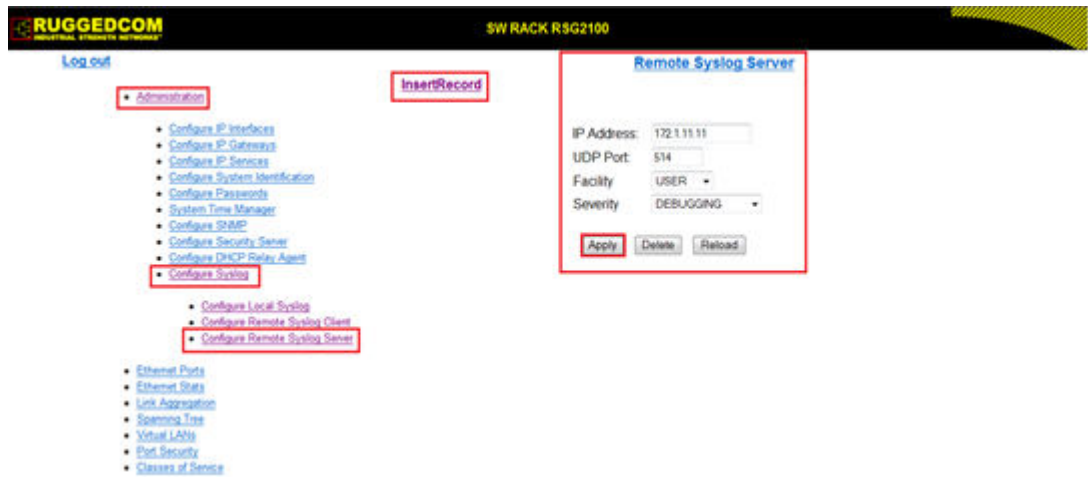
- ✧ Now, you have to go to **Configure Remote Syslog Client** and set the **Port** through which the client sends information to the server(s) to e.g. 514 (standard Syslog Port).



[sc_Configuring Remote Syslog Client, 1, en_US]

Figure 5-24 Configuring Remote Syslog Client

- ✧ And at the end, go to **Configure Remote Syslog Server** → **Insert a new Server** and put in the information of your server where the monitoring software is installed e.g. 172.1.11.11.



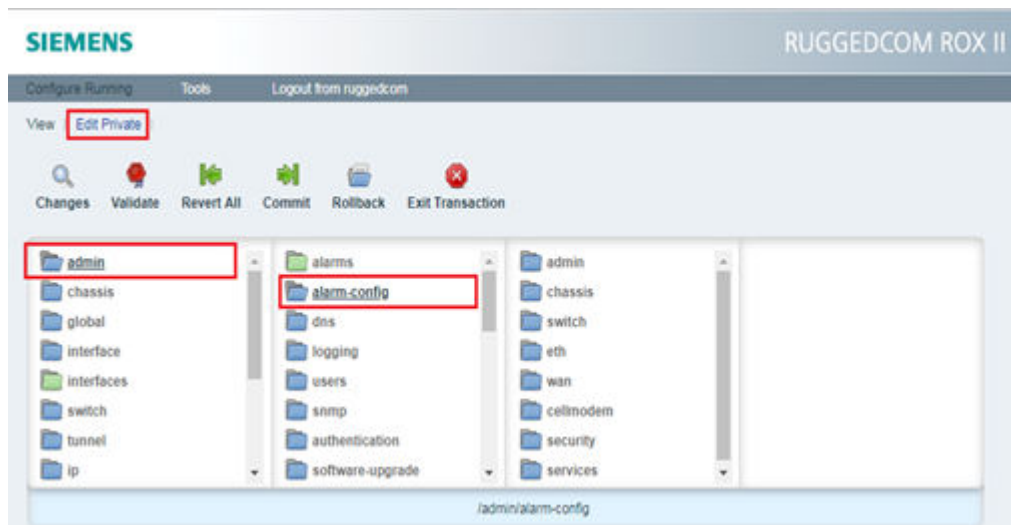
[sc_Configuring Syslog Server Ip in Ruggedcom, 1, en_US]

Figure 5-25 Configuring Syslog Server Ip in Ruggedcom

5.5.4 RuggedCom Router RX1500

5.5.4.1 Alarm Configuration for Syslog: Event Configuration

- ✧ Log in as admin user.
- ✧ Change to the **Edit Private** or **Edit Exclusive** mode and navigate to **admin** → **alarm-config**.



[sc_Syslog Configuration for Alarm Events, 1, en_US]

Figure 5-26 Syslog Configuration for Alarm Events

Preconfigured alarms are available which could be adapted as required.

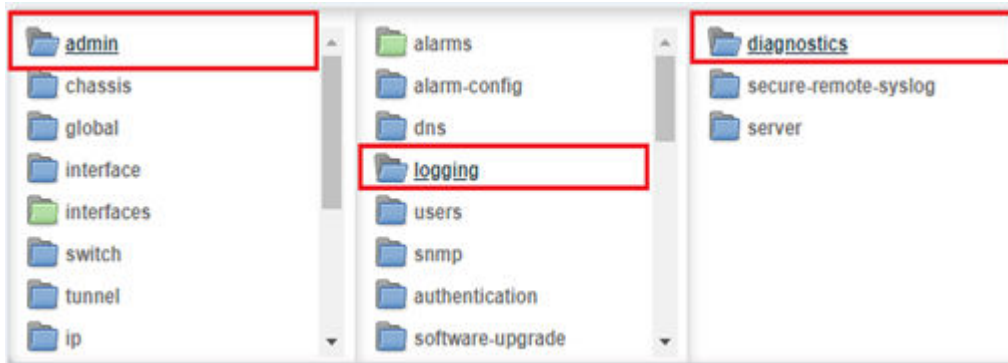
Most of the alarms are already preconfigured events and fall into one of the following log types:

<p>Security Event Logs</p>	<p>Information related to the following security events are logged by RUGGEDCOM ROX II:</p> <div style="border: 1px solid gray; padding: 5px; margin-bottom: 10px;"> <p>NOTE <i>Passwords can be retried up to 3 times before the login attempt is considered a security event.</i></p> </div> <ul style="list-style-type: none"> • Successful and unsuccessful login attempts • Local and remote (RADIUS) authentication • Security-sensitive commands (whether successful or unsuccessful) • An optionally configurable SNMP Authentication Failure Trap (disabled by default) in accordance with SNMPv2-MIB <p>All security event logs are recorded in <code>var/log/auth.log</code> and can be viewed in the Authlog Viewer. For more information about viewing logs, refer to Section 3.9.1, "Viewing Logs".</p>
<p>Syslogs</p>	<p>Syslog allows users to configure local and remote syslog connections to record important, non-security event information. The remote Syslog protocol, defined in RFC 3164 [http://tools.ietf.org/html/rfc3164], is a UDP/IP-based transport that enables a device to send event notification messages across IP networks to event message collectors, also known as Syslog servers. The protocol is designed to simply transport these event messages from the generating device to the collector.</p> <p>All log files are organized in the log directory (<code>/var/log</code>) according to the facility and priority at which they have been logged. Remote Syslog sends the requested logs to the remote server(s) at whichever facility and priority they were initially logged, after filtering the logs based on the selectors configured for the server.</p> <p>The following log files are setup with the following default selectors:</p> <ul style="list-style-type: none"> • <code>syslog</code> catches all logs except <code>daemon.debug</code>, <code>auth</code> or <code>authpriv</code> logs • <code>daemon.log</code> catches all <code>err</code> level (and above) logs written to the <code>daemon</code> facility • <code>messages</code> catches all <code>info</code>, <code>notice</code> and <code>warn</code> level logs for all facilities except <code>auth</code>, <code>authpriv</code>, <code>cron</code>, <code>daemon</code>, <code>mail</code> and <code>news</code> <p>A selector setup using the following facilities at level <code>info</code> and up is recommended:</p> <ul style="list-style-type: none"> • <code>daemon</code> • <code>user</code> • <code>kern</code> • <code>syslog</code>
<p>Diagnostic Logs</p>	<p>Diagnostic logs record system information for the purposes of troubleshooting.</p>

[sc_Security Log Information, 1, en_US]

Figure 5-27 Security Log Information

✧ Additional diagnostic information can be enabled under **logging** → **diagnostics**.

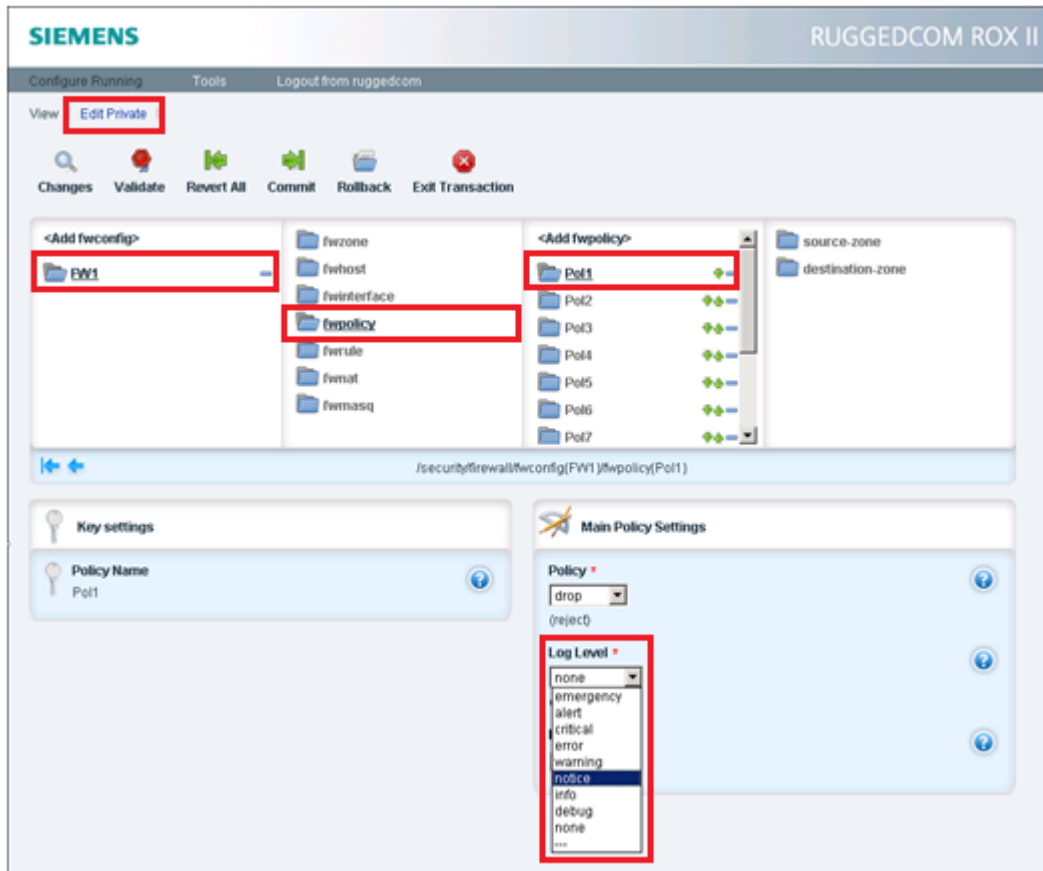


[sc_Diagnostic Information in Ruggedcom, 1, en_US]

Figure 5-28 Diagnostic Information in Ruggedcom

5.5.4.2 Firewall Log Setup

- ✧ To enable Logging information of dropped traffic for the Firewall, go to the Firewall default policy and adapt the log level accordingly.
- ✧ Login as Administrator and go to the **Edit Private** or **Edit Exclusive** mode and navigate to **security** → **firewall** → **fwconfig** → **FW1** → **fwpolicy** → **Pol1** and change the log level to **notice** for all your relevant policies.
- ✧ Commit the change by clicking at commit at top menu.



[sc_Setting Firewall Logs, 1, en_US]

Figure 5-29 Setting Firewall Logs

5.5.4.3 Display Syslog Information

Selected logs can be viewed directly within the Web interface or can be downloaded from the device and viewed in a text editor/viewer.

The following Log files can be displayed:

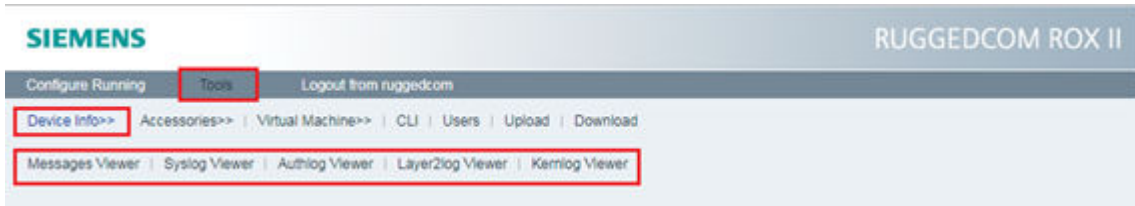
Messages Viewer	Displays all events from <code>/var/log/messages</code>
Syslog Viewer	Displays syslog events from <code>/var/log/syslog</code>
Authlog Viewer	Displays authentication events from <code>/var/log/auth.log</code>
Layer2log Viewer	Displays Layer 2 events from <code>/var/log/layer2</code>
Kernlog Viewer	Displays kernel events from <code>/var/log/kern.log</code>

[sc_Logfiles path, 1, en_US]

Figure 5-30 Logfiles Path

Web Interface

- ✧ In the main bar, navigate to **Tools** → **Device Info**.

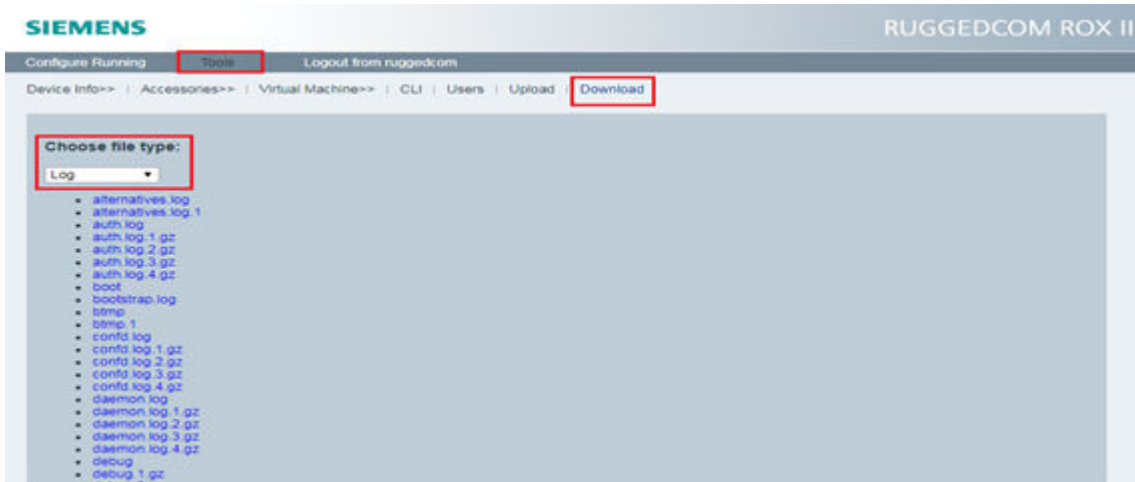


[sc_Web interface of Ruggedcom Log View, 1, en_US]

Figure 5-31 Web Interface of Ruggedcom Log View

Log Download

- ✧ In the main bar, navigate to **Tools** → **Download** and select **Log** and search for the relevant files. Right-click the file and select **Save Target As...** to store the file to a location on your PC.

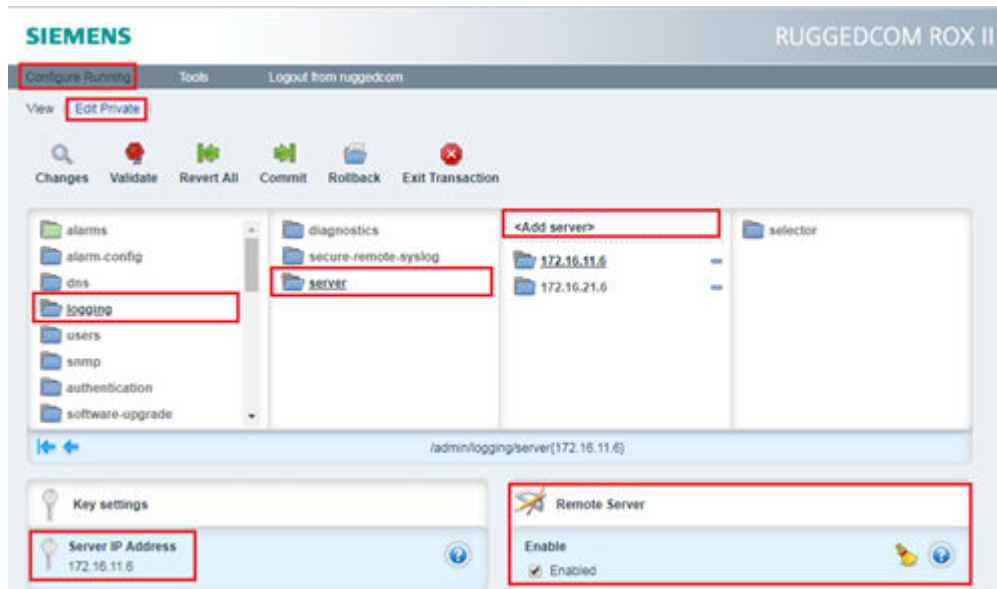


[sc_Downloading Logs in Ruggedcom, 1, en_US]

Figure 5-32 Downloading Logs in Ruggedcom

5.5.4.4 Syslog Server Connection

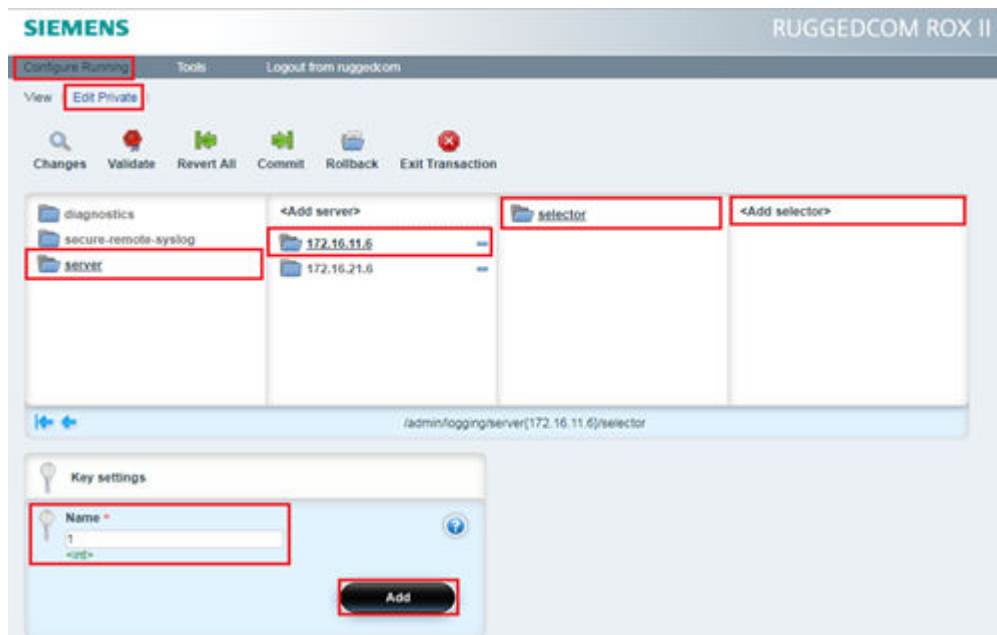
- ✧ Log in as Administrator.
- ✧ Change to the **Edit Private** or **Edit Exclusive** mode and navigate to **admin** → **logging** → **server** and add the server IP e.g the IP of the Engineering Workstation 172.16.11.6 and enable the **Remote Server**.



[sc_Connecting to Syslog Server, 1, en_US]

Figure 5-33 Connecting to Syslog Server

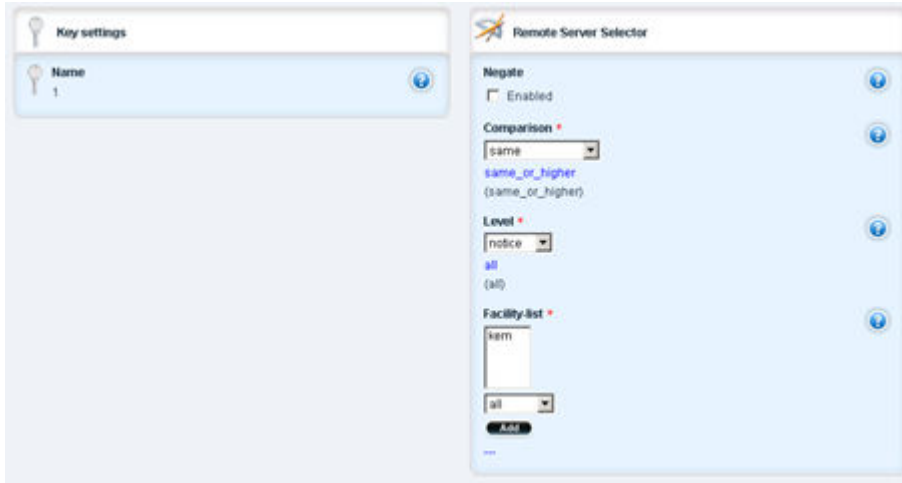
- ✧ Click **Add selector(s)** with proper naming e.g. 1.



[sc_Adding Server Selector, 1, en_US]

Figure 5-34 Adding Server Selector

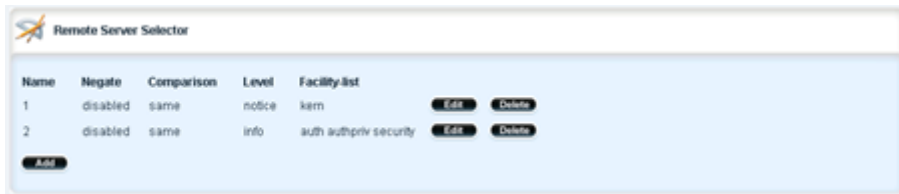
- ✧ Add facility kern from the drop-down menu Facility-list, set the **Comparison** field to **same** and the **Level** as **notice**, in order to limit syslog traffic:



[sc_Adding Facility kern, 1, en_US]

Figure 5-35 Adding Facility Kern

The following 2 example selectors are created, no. 1 for dropped packages and no. 2 for authority, committed jobs, etc.



[sc_Remote Server Selector, 1, en_US]

Figure 5-36 Remote Server Selector

5.6 Recommendations

The protection of an energy automation system alone is not enough. Attempts to attack the systems must be recognized as early as possible so that appropriate measures can be taken before the functions of the systems are adversely affected by the attack. The solution for this is a SIEM (Security Information and Event Management) system.

In a modern-day energy automation system, the manual evaluation of security information is not possible due to plethora of devices and complex system. Also, the security-related information varies based on the device and component. In general, login attempts, changes of configuration, detection of malware protection are reported. For example, a firewall logs in addition the blocked traffic. To fulfill this requirement, a SIEM solution is required which automatically evaluates and alerts the System Operators (e.g. via email).

A SIEM collects all security-related logs from all components of the system. The logs are sent via the syslog protocol to a syslog server. The syslog server on substation level acts as a buffer. With some disadvantages regarding availability, it is possible to send the syslog information from the components direct to a SIEM system.

The syslog information is stored in the SIEM so that it can be used for a forensic analysis after a cyber incident. The SIEM can generate reports that cover a specific malfunction or a period.

International standards such as IEC 27001, IEC 62443, and industry recommendations such as the BDEW white paper (Federal Association of Energy and Water Management) also address the topics of **logging and logging and monitoring**.

Boundary conditions

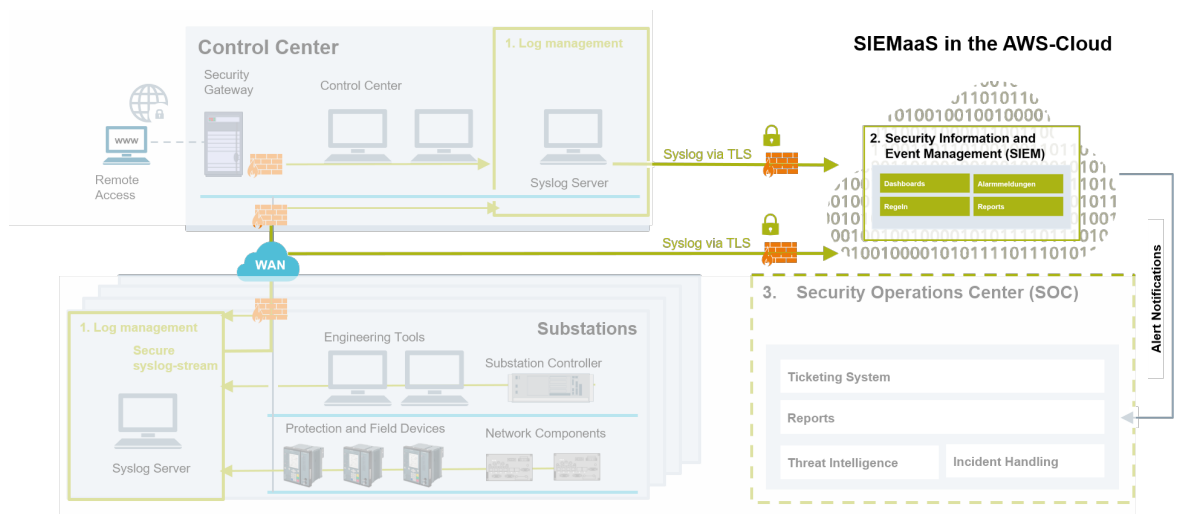
The essential components of the energy automation system must collect the security-related information and make them available via the syslog protocol. The Siemens components for energy automation and communication such as SIPROTEC 5, SICAM A8000, and RuggedCom meet these requirements.

5.6.1 SIEM as a Service

A SIEM solution can be deployed either on-premises or in the cloud. In addition to a SIEM solution on premise, Siemens offers a SIEM as a Service solution. The only difference between an on-premises and cloud-based SIEM is the location, instead of installing the SIEM in the data center of the operator, the SIEM is installed in a cloud environment.

The main advantages of a SIEM as a Service are:

- No efforts for the administration of the SIEM on operator side
- High availability
- Scalable
- Patches and updates are managed by Siemens



[sc_SIEM as a Service Architecture, 1, en_US]

Figure 5-37 SIEM as a Service Architecture

A cloud solution must fulfill the same security requirements as a solution on premise.

A state-of-the-art security is essential for the SIEM as a service solution. The foundation is given by AWS (Amazon Web Services) cloud infrastructure as a base that is in line with the CSA (Cloud Security Alliance) recommendations. A secure communication from the OT systems to the cloud infrastructure complements the overall security.

Siemens SIEM service includes:

- SIEM with analysis and alarming functionalities provided as a cloud service
- SIEM-ready upgrade of your systems
- Implementation of alarm rules in the SIEM system
- Regular updating and adaptation of the alarm rules to current threats
- Training for your employees

Contact your local Siemens partner for more information.

6 Security Patching

6.1	General Instruction	175
6.2	Updating Windows Operating System	175
6.3	Automated Patching	178
6.4	Update Instructions for Siemens Products	187

6.1 General Instruction

Patching is the elimination of security gaps in software products, applications, and IEDs. Microsoft regularly releases patches to their customers. There are many different patch classifications (<http://support.microsoft.com/kb/824684/EN-US/>), but only security patches and critical patches are necessary for the secure and stable behavior of a product.

Once a month, Siemens publishes a **Security Patch Compatibility Report** for substation products. This report is the result of application software tests which were done with the latest released Windows security update patches. The list can be downloaded from the Siemens SIOS portal (see <https://support.industry.siemens.com/cs/document/109808612/security-patch-management?dti=0&dl=en&lc=en-US>). The usage of the updates mentioned above is generally allowed for the following operating systems and components:

- Microsoft Windows and Microsoft Windows Server operating systems
- Microsoft SQL Server
- Microsoft Internet Explorer

In rare cases, a patch can have a negative impact on the Siemens software. These patches are listed in the **Non-Approved List** sheet of the **Security Patch Compatibility Report**.

If contraindications appear during Siemens tests, these indications are communicated immediately via newsletter. This process does not apply for new Microsoft Service Packs. The usage of these packs still requires an explicit release.

You can find information concerning patches on the following Microsoft internet page:

- Microsoft Security Bulletins
<https://technet.microsoft.com/en-us/security/default.aspx>

6.2 Updating Windows Operating System

The Windows operating system shall be updated with the latest available security patches. Siemens recommends doing the update manually.

6.2.1 Downloading the Latest Security Patch

- ✧ Navigate to the list of the **Security Patch Compatibility Reports** in the Siemens SIOS portal (see <https://support.industry.siemens.com/cs/document/109808612/security-patch-management?dti=0&dl=en&lc=en-US>).
- ✧ Download and open the respective report for your application, for example, SICAM PAS.

The relevant Microsoft security updates for the operating systems that are released for your application are listed, for example, Win10 LTSC 2021 and Win Server 2019 for SICAM PAS.

Microsoft Security Updates

The following Microsoft Security Updates have been tested for compatibility with SICAM software:

-Microsoft "patch update" Dec-2022

<https://msrc.microsoft.com/update-guide/en-us/releaseNote/2022-Dec>

For following operating systems patches has been installed from <https://www.catalog.update.microsoft.com/Home.aspx>

- Windows 10 Ltsc 2021

[2022-12 Cumulative Update for Windows 10 Version 21H2 for x64-based Systems \(KB5021233\)](#)

[2022-12 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 21H2 for x64 \(KB5021088\)](#)

- Windows Server 2019 Standard 64 bit

[2022-12 Cumulative Update for Windows Server 2019 for x64-based Systems \(KB5021237\)](#)

[2022-12 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows Server 2019 for x64 \(KB5021085\)](#)

- Windows 11 22H2 64 bit

[2022-12 Cumulative Update for Windows 11 Version 22H2 for x64-based Systems \(KB5021255\)](#)

[2022-12 Cumulative Update for .NET Framework 3.5 and 4.8.1 for Windows 11, version 22H2 for x64 \(KB5020880\)](#)

- Windows Server 2022

[2022-12 Cumulative Update for Microsoft server operating system version 21H2 for x64-based Systems \(KB5021249\)](#)

[2022-12 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Microsoft server operating system version 21H2 for x64 \(KB5021095\)](#)

Following SICAM software products have been tested with the approved 3rd-party security updates:

SICAM PAS PQS V08.20.49

SICAM PQ Analyzer V03.20

SICAM SCC 9.12 (incl. WinCC WinCC V7.5 SP2 Upd11)

Update: 21.12.2022

Recently tested pattern version: Windows Defender security intelligence update 1.381.404.0

Which Microsoft Security Patches are tested at SICAM software on compatibility?

Instructions

[Readme](#) | [History link collection](#) | [Non-Approved List](#) | [Previously Non-Approved List](#) | [+](#)

[sc_Security Patches Compatibility Report, 1, en_US]

In the figure, it would be necessary to update Win Server 2019 with the cumulative update KB5021237.

**NOTE**

Possible negative impacts from a Windows security update on the application's functionality are listed in the sheet **Non-Approved List**.

The sheet **History link collection** lists all released and approved Windows security updates of the last months.

✧ Click the respective security patch.

You are directed to the Microsoft Update Catalog.

✧ Download the security patch.

✧ Save the downloaded installation file of the security patch on an external storage media like a virus-protected USB stick.

6.2.2 Downloading the Latest Security Patch for Legacy Systems

The Siemens **Security Patch Compatibility Report** includes only the latest released operating systems. Security patches for legacy operating systems have to be downloaded in a different way.

- ✧ Open **Programs and Features** in the control panel of the machine on which you want to install the security patch.
- ✧ Click **Installed Updates**.

All installed updates are displayed.

- ✧ Note down the KB number of the latest **Security Update for Microsoft Windows**, for example, KB5018419.
- ✧ Go to the Microsoft Update Catalog (<https://www.catalog.update.microsoft.com/Home.aspx>).
- ✧ Enter the KB number in the search bar.
- ✧ In the title row, click the update for the correct architecture, for example, x64-based Systems.

Update details are displayed in a separate window.

- ✧ In the package details tab, search for the latest cumulative update and write down its KB number, for example, KB5021237.

- ✧ Close the update details.
- ✧ Enter the KB number of the latest cumulative update in the search bar.
- ✧ Open the update details of the cumulative update.
- ✧ To check if you need an SSU, open the link under **More information**.

If applicable, information regarding a possibly needed SSU are displayed.

- ✧ If an SSU is necessary, install it on your machine.
- ✧ Close the update details.
- ✧ Download the respective cumulative update.



NOTE

As an alternative, you can also directly search the title of your legacy operating system in the Microsoft Update Catalog, for example, Windows 10 LTSB 1809.

6.2.3 Installing the Patches

- ✧ Connect the media storage containing the update to the machine on which you want to install it.
- ✧ Execute the .msu installation file.

**NOTE**

Several restarts may be required.

- ✧ Go through the installation wizard.
- ✧ To check the successful installation, go to **Programs and Features** in the control panel.
- ✧ Click **Installed Updates** and check the update.

6.2.4 Checking the Patches with SICAM SDM

The Siemens SICAM SDM Collector Tool shall be used for managed service for substation asset documentation and monitoring. It works as a local collector of data in substation systems, bringing information provided by usual protocols like SNMP, IEC 61850, or through WMIC requests on PCs. SICAM SDM can generate reports based on inventory lists of assets, reducing documentation time and efforts on information gathering, facilitating evaluation of patch management procedures.

SICAM SDM may be used to scan and generate the list of software detailed with the current version installed. If the software is not in the latest patch version, it should be updated.

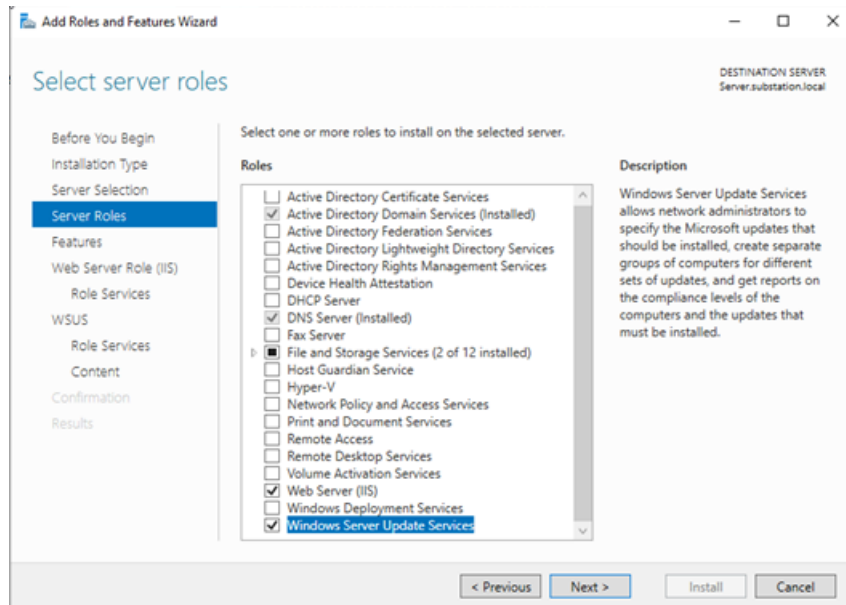
6.3 Automated Patching

The Windows Operating System can also be updated automatically in the **offline-environment** using a WSUS (Windows Server Update Services) export and import server. The update procedure shall be repeated after every patch release by Microsoft or based on patch cycle of the substation. The process is intended for environments without Internet connection. The updates are required to be downloaded on the patch server placed externally at the control center level. The WSUS export server is used for this procedure. The updates must be transferred to an external device and must be imported on the WSUS import server in the **offline-environment**. On the WSUS import server, the updates can be approved for the different client groups. However, the update compatibility list shall be checked on the Siemens Website before pushing the updates to client machines (<https://new.siemens.com/global/en/products/energy/energy-automation-and-smart-grid/grid-security/product-security.html>). To patch the clients automatically after importing the updates, group policies can be used.

6.3.1 Installation and Setup

6.3.1.1 Installation and Setup

For automatic WSUS updates the Web Server (IIS) and Microsoft Report Viewer are required.



[sc_Adding WSUS using centralized Server, 1, en_US]

Figure 6-1 Adding WSUS Using Centralized Server

6.3.1.2 WSUS and IIS Installation

The installation of WSUS and IIS is described in the Microsoft TechNet step by step:

<https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/deploy/1-install-the-wsus-server-role>

6.3.1.3 Installation of the WSUS Server Role

- ✧ Log on to the server on which you plan to install the WSUS server role by using an account that is a member of the Local Administrators group.
- ✧ In **Server Manager**, click **Manage** → **Add Roles and Features**.
- ✧ In the **Before you begin** page, click **Next**.
- ✧ In the **Select installation type** page, confirm that Role-based or feature-based installation option is selected and click **Next**.
- ✧ In the **Select destination server** page, choose where the server is located (from a server pool or from a virtual hard disk).
After you select the location, choose the server on which you want to install the WSUS server role, and then click **Next**.
- ✧ In the **Select server roles** page, select **Windows Server Update Services**.
Add features that are required for Windows Server Update Services opens. Click **Add Features**, and then click **Next**.
- ✧ In the **Select features** page, retain the default selections and then click **Next**.



NOTE

WSUS only requires the default Web Server role configuration. If you are prompted for additional Web Server role configuration while setting up WSUS, you can safely accept the default values and continue setting up WSUS.

- ✧ In the **Windows Server Update Services** page, click **Next**.
- ✧ In the **Select Role Services** page, leave the default selections, and then click **Next**.



NOTE

Select at least one Database type. If the database options are all cleared (not selected), post installation tasks will fail.

- ✧ In the **Content location selection** page, type a valid location to store the updates. For example, you can create a folder named **WSUSupdates** at the root of drive C specifically for this purpose, and type **c:\wsusupdates** as the valid location.
- ✧ Click **Next**.

The Web Server Role (IIS) page opens.

- ✧ Review the information, and then click **Next**.
- ✧ In **Select the role services to install for Web Server (IIS)**, retain the defaults, and then click **Next**.
- ✧ In the **Confirm installation selections** page, review the selected options, and then click **Install**.

The WSUS installation wizard runs. This might take several minutes to complete.

- ✧ Once the WSUS installation is complete, in the summary window on the **Installation progress** page, click **Launch Post-Installation tasks**.

The text changes, requesting: **Please wait while your server is configured**.

When the task has finished, the text changes to: **Configuration successfully completed**.

- ✧ Click **Close**.
- ✧ In **Server Manager**, verify if a notification appears to inform you that a restart is required. This can vary according to the installed server role. If it requires a restart, make sure to restart the server to complete the installation.

6.3.1.4 Report Viewer

For Microsoft Windows Server 2016 and 2019 WSUS reporting, the following versions must be installed:

- SQL Server System CLR types for SQL Server 2012:
<https://www.microsoft.com/en-us/download/details.aspx?id=49999>
- Report Viewer 2012:
<https://www.microsoft.com/en-US/download/details.aspx?id=35747>

Integrating WSUS Solution to Substation Environment

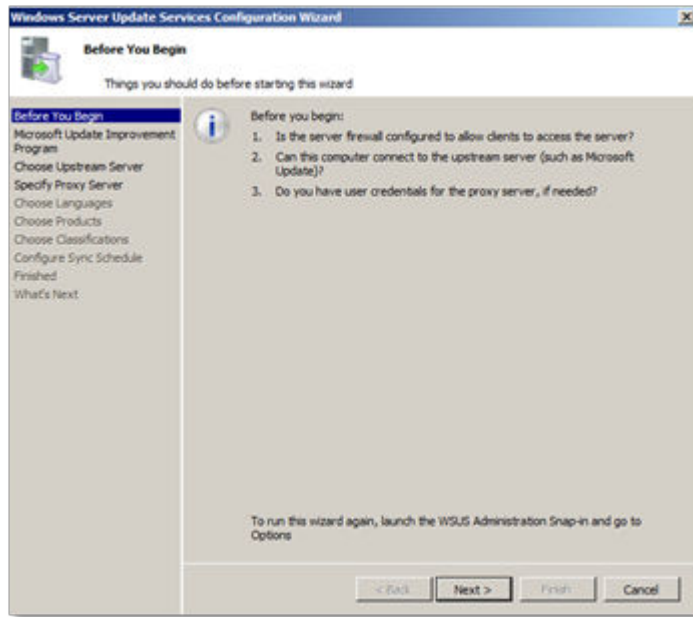
The following steps must be performed to integrate the WSUS solution into a substation environment:

- ✧ Install WSUS on a Microsoft Windows Server connected to the Internet. This will be the WSUS export server.
- ✧ Install WSUS also on a Microsoft Window Server inside your separated network where you want to distribute the updates. This will be the WSUS import server.
- ✧ Firewall settings:
Default: WSUS uses the port 80 (http) or 443 (https) if installed on the default Web site.
For Microsoft Window Server 2016 and higher: WSUS uses port 8530 (http) and 8531 (https).
- ✧ Enable SSL for secure communication between the import server and the clients: <https://technet.microsoft.com/en-us/library/hh852346.aspx>

6.3.1.5 Setup of the WSUS Export Server

To set up the WSUS export server, use the Server Configuration Wizard:

- ✧ Connect the server to the internet (required for the wizard).
- ✧ Open the WSUS snap-in via the **Server Manager**.
- ✧ Go to **Options** → **Start the WSUS Server Configuration Wizard**.

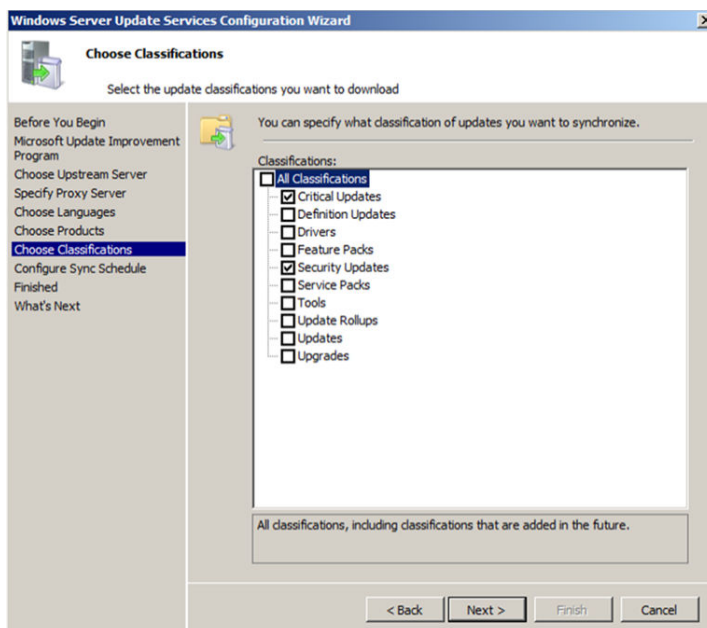


[sc_WSUS Configuration Wizard, 1, en_US]

Figure 6-2 WSUS Configuration Wizard

Use the wizard to set up your WSUS export server with following settings:

- ✧ In **Specify Proxy Server**, enter a proxy server and user credentials if you need to.
- ✧ Click **Next** and **Start Connecting** (This can take several minutes).
- ✧ In **Choose Languages**, select the languages you need.
- ✧ Click **Next** and specify the products that you use in your environment (Windows Server, Windows 10 etc.).
- ✧ In **classifications**, choose the update classifications **Security Updates** and **Critical Updates**.



[sc_Select Update type, 1, en_US]

Figure 6-3 Select Update Type

- ✧ Choose **Synchronize manually**.
- ✧ If you want to, you can begin the initial synchronization.

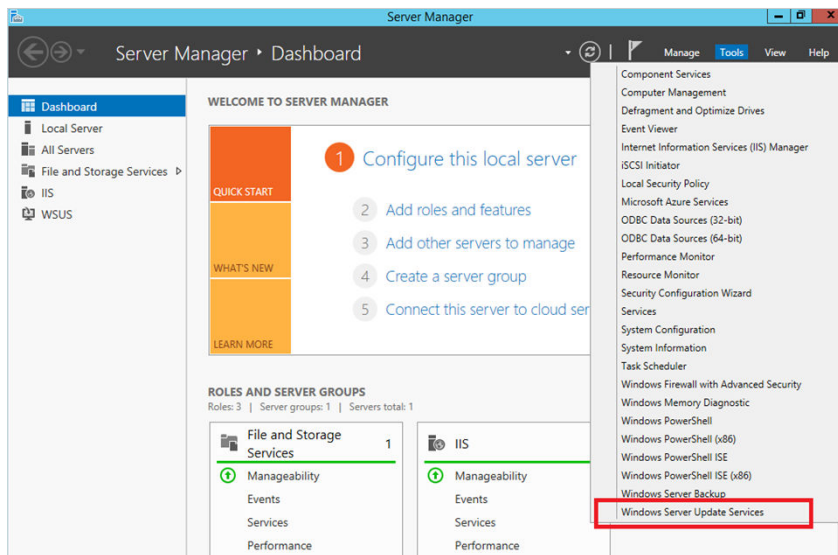
This will initiate a connection to Microsoft Update.

- ✧ Finish the Configuration Wizard.

6.3.1.6 Setup of the WSUS Import Server

You do not have to run the Configuration Wizard on the import server.

- ✧ Open the WSUS snap-in via the **Server Manager**.



[sc_Enabling WSUS snap-in, 1, en_US]

Figure 6-4 Enabling WSUS Snap-In

- ✧ Go to **Options** → **Updates Files and Languages**.
The settings for Update Files must be the same as on the export server!
- ✧ Go to **Update Languages** and choose the same languages as on the export server. (English)

Creating Computer Groups

- ✧ Go to **Computers** → **All Computers**.
- ✧ Right-click **All Computers** → **Add computer group**.
- ✧ Create computer groups for the different clients (SICAM PAS, SICAM SCC etc.) to manage computers with same settings or the same software configuration that need the same patches.
- ✧ To create subgroups, right-click a specific group. You can use them for further division of the clients (e.g. testing groups).

Adding Clients to the WSUS Server

- ✧ To add the clients to WSUS server, you must set up group policies on each client computer.
The required settings are described in [6.3.1.7 Setup of the WSUS Clients – Connecting Clients to the WSUS Import Server](#).

After setting up the clients, the clients will appear in the group **Unassigned Computers**.

- ✧ Select one or more computer(s), right-click a **computer** → **Change Membership** to add them to another group.
- ✧ If it is not installed yet, install the Nxlog Syslog Software and start it.

6.3.1.7 Setup of the WSUS Clients – Connecting Clients to the WSUS Import Server

On each client, you need to define the update source. In this case, the update source is the WSUS import server.

The following steps must be performed on each client computer that shall be updated from the WSUS import server. The settings can be done either locally on each client or on a central domain controller.

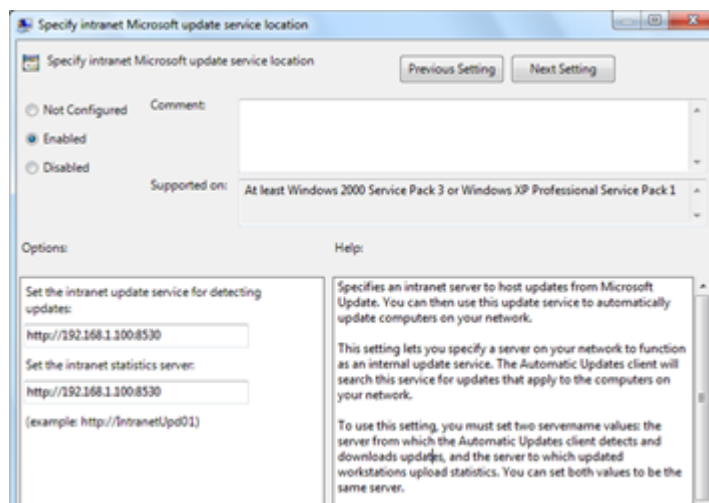
Setting up Group Policies for the Clients

- ✧ Open gpedit.msc, go to **Computer Configuration** → **Administrative Templates** → **Windows Components** → **Windows Update** and set up the following policies:
 - Specify Intranet Microsoft Update Service Location:
Enter the IP and port of your WSUS import server into both text fields in the following format:
[http://\[IP-ADDRESS\]:\[PORT\]](http://[IP-ADDRESS]:[PORT])
 - Default ports:
Windows Server 2016 and newer: 8530 (http) or 8531 (https)



NOTE

Do not forget to configure the required firewall rules for firewall appliances or host-based firewalls in the communication path.

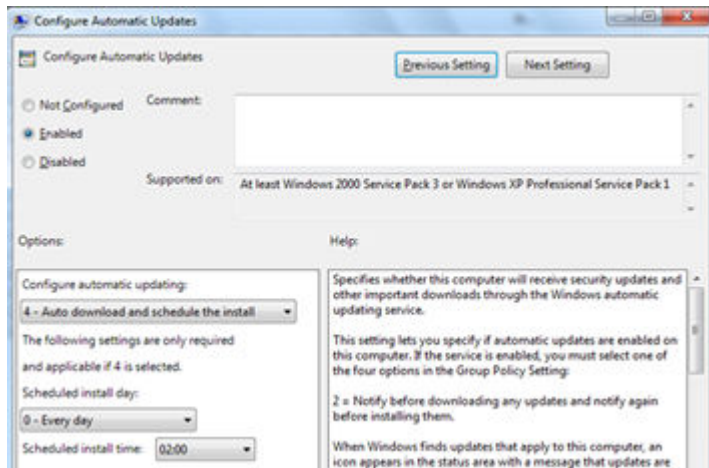


[sc. Specifying server IP, 1, en. US]

Figure 6-5 Specifying Server IP

The clients will connect to the WSUS server and appear in the group **Unassigned Computers**.

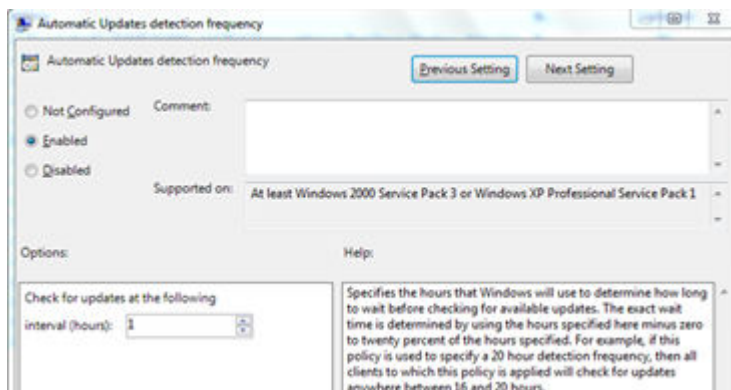
- ✧ Configure automatic updates:
Set to **4 – Auto download and schedule the install** and choose you day and time of installation.



[sc_Selecting automated download, 1, en_US]

Figure 6-6 Selecting Automated Download

- ✧ Automatic Updates detection frequency: Set to every hour (1)



[sc_Selecting Interval Hours, 1, en_US]

Figure 6-7 Selecting Interval Hours

- ✧ To update the group policies immediately: `cmd` → `gpupdate /force`



NOTE

You can force the client to contact the WSUS server by clicking **Check for Updates** in the **Update & Security** on Windows Settings.

6.3.2 Update Procedure

This section describes the procedure necessary to distribute updates to the clients. It is relevant every time new updates are being installed. The steps 1 to 4 are mandatory for the update installation.

6.3.2.1 Download all Updates on the WSUS Export Server

- ✧ Open the WSUS snap-in and go to **Synchronizations**.
- ✧ Click **Synchronize Now** on the right to synchronize WSUS with the Microsoft update servers (WSUS downloads metadata/information for the updates).
- ✧ Go to **Updates** and approve all updates for installation you need (e.g. updates of last patch day) for all computers. You can sort the updates by date of publication.

WSUS will now download the approved updates.

- ✧ Wait for all downloads to complete (small icon on the left of a list entry indicates the status of an update).

Title	Installed...	Release Date	Approval
March, 2017 Security Only Quality Update for Windows 7 for x64-based Systems (KB4012212)	0%	3/28/2017	Install
March, 2017 Security Monthly Quality Rollup for Windows 7 for x64-based Systems (KB4012215)	0%	3/14/2017	Install
Cumulative Security Update for Internet Explorer 11 for Windows 7 for x64-based Systems (KB4...	0%	3/14/2017	Install
March, 2017 Security Monthly Quality Rollup for Windows 7 (KB4012215)	0%	3/14/2017	Install
Cumulative Security Update for Internet Explorer 11 for Windows 7 (KB4012204)	0%	3/14/2017	Install
March, 2017 Security Only Quality Update for Windows 7 (KB4012212)	0%	3/28/2017	Install
December, 2016 Security Only Update for .NET Framework 4.6.2 on Windows 7 (KB3205406)	0%	12/13/2016	Install
December, 2016 Security and Quality Rollup for .NET Framework 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2 ...	0%	12/14/2016	Install
December, 2016 Security and Quality Rollup for .NET Framework 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2 ...	0%	12/14/2016	Install

[sc_Selecting update, 1, en_US]

Figure 6-8 Selecting Update

This update supersedes another update. Before you decline any superseded update, we recommend that you verify it is no longer needed by any computers. To do so, approve the superseding update first.

The files for this update have not yet been downloaded. The update can be approved but will not be available to computers until the download is complete.

Status:

- Computers with errors: 0
- Computers needing this update: 0
- Computers installed/not applicable: 0
- Computers with no status: 0

MSRC severity: Critical
MSRC number: MS17-006
Release date: Tuesday, March 14, 2017
KB article numbers: 4012215

[sc_Update detail, 1, en_US]

Figure 6-9 Update Detail

6.3.2.2 Export the Updates and Meta Data

The next step is to copy the patch binaries and metadata from the export WSUS to the USB key.

- ✧ The update files can be copied via the Windows Explorer.
Copy the `\YOUR_WSUS_FOLDER\WSUSContent\` folder to a USB key.

Exporting Meta Data

The metadata must be exported with the `wsutil.exe` tool.

- ✧ Open a command prompt (`cmd.exe`) and navigate to: `c:\program files\update services\tools`
- ✧ Run the command: `wsutil.exe export packagename.cab logfile.log`

You can change names `packagename` and `LogFile` to whatever you want. The files will be created directly in the folder `c:\program files\update services\tools` in case no other folder is specified.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd c:\program files\update services\tools
C:\Program Files\Update Services\Tools>wsutil.exe export packagename.cab logfile.log
```

[sc_Exporting Updates and Metadata using CMD, 1, en_US]

Figure 6-10 Exporting Updates and Metadata Using CMD

- ✧ Transfer the file `packagename.cab` to the USB key.

6.3.2.3 Import the Updates and Meta Data on the WSUS Import Server

- ✧ Copy the update files to the `\YOUR_WSUS_FOLDER\WSUSContent\` folder. The folder has been defined during WSUS Role installation (copy only the content of the `WSUSContent` folder).
Overwrite all existing files and folders.

Importing the Meta Data

Import the metadata to the import server with the WSUSutil tool.

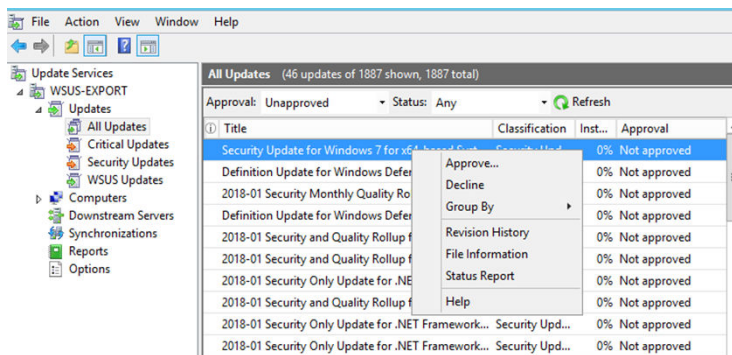
- ✧ a. Run the WSUSutil tool on the import server:
cmd.exe
\\program files\update services\tools\wsusutil.exe import packagename.cab logfile.log
- ✧ You must specify the location of the **packagename.cab** file.

For more detailed instructions of the import and export process: <https://technet.microsoft.com/en-us/library/dd939873.aspx>

You must always import the update files to the WSUS import server before you import the update metadata. If WSUS finds meta data for an update that does not have corresponding update files, WSUS considers the update to be a failed download. To resolve this issue, copy the update to a directory on the WSUS import server and redeploy the update.

6.3.2.4 Approving Updates for the Different Client/Computer Groups on the WSUS Import Server

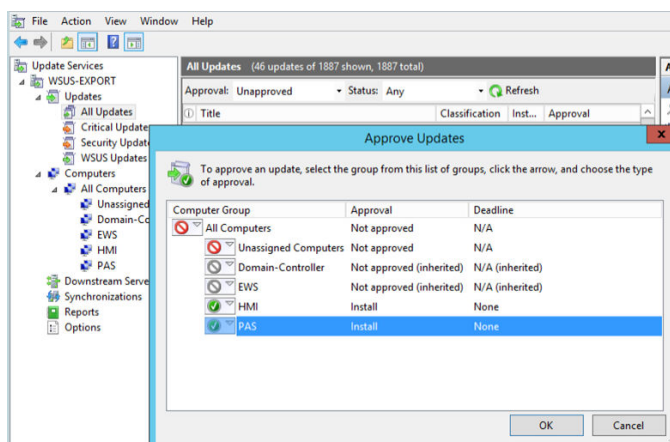
- ✧ Open: <https://support.industry.siemens.com/cs/document/109808612/security-patch-management?dti=0&lc=en-US>
- ✧ In the reports you can find the patches in the **Non-Approved List**.
- ✧ Open the WSUS snap-in, go to **Updates**.
- ✧ Right-click the concerned update and click **Approve**.



[sc_Approving Update in WSUS, 1, en_US]

Figure 6-11 Approving Update in WSUS

- ✧ Select the computer groups where you want to install the update and click **OK**.



[sc_Approving update for a computer group, 1, en_US]

Figure 6-12 Approving Update for a Computer Group

The clients will search for the updates and install them at the scheduled time in the group policies. The clients will reboot after few minutes and will log the status of the required service and send the log to the syslog server. The update process can also be triggered immediately.

6.3.3 Event Logs

The following event logs can be used to monitor the status of the WSUS Server and the WSUS clients.

On the Server

- ✧ Click **Start** → **Run**, and then type **eventvwr** to start the **Event Viewer**.
- ✧ In the left pane, click **Application**.
- ✧ Find the events whose source is Windows Server Update Services.

Additional log files: C:\Program Files\Update Services\LogFiles\ ...

On the Clients

- ✧ Click **Start** → **Run**, and then type **eventvwr** to start the **Event Viewer**.
- ✧ In the left pane, click **Applications and Services Logs**.
- ✧ Click **Microsoft** → **Windows** → **WindowsUpdateClient** → **Operational**.

Additional log files:

- C:\Windows\SoftwareDistribution\ReportingEvents.log
- C:\Windows\WindowsUpdate.log
- Health Monitoring in WSUS 3.0:
<https://technet.microsoft.com/en-us/library/cc720478.aspx>

6.4 Update Instructions for Siemens Products

This section summarizes patching instructions for the Siemens products covered by this document. Detailed instructions can be found in the official manuals for the respective documentation. The below instructions are summarized to provide an overview in a single place.

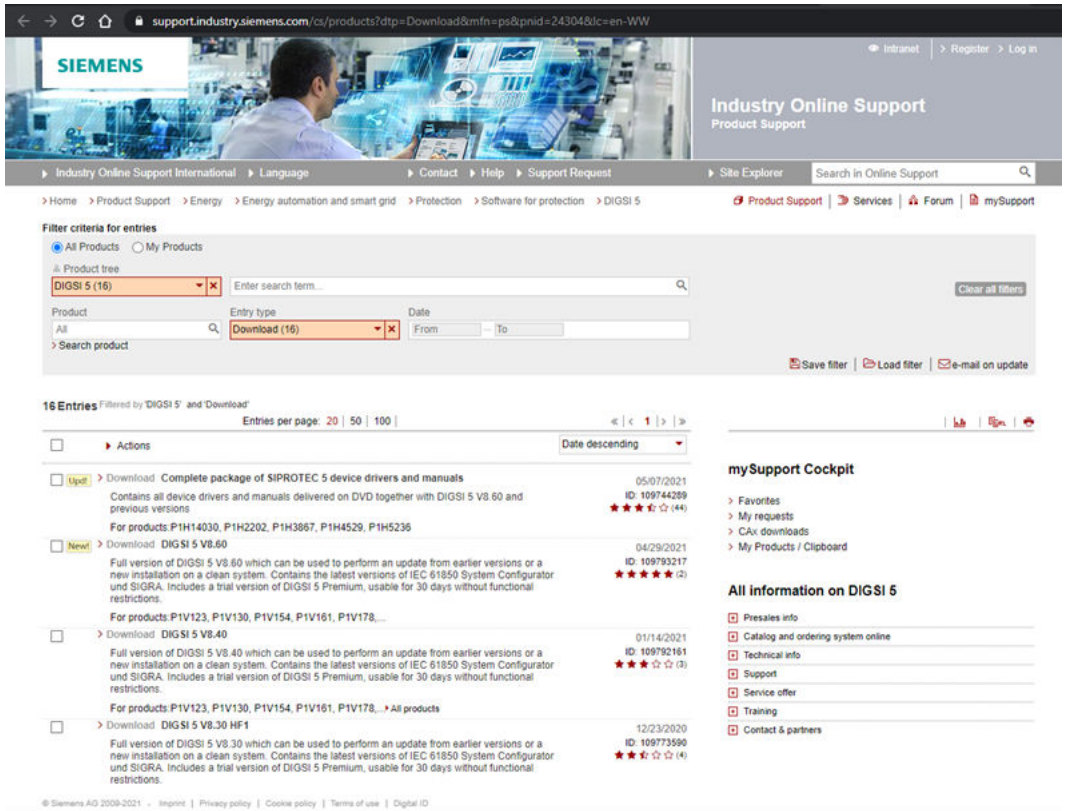
As a rule, for any update activity, the installed updates are recorded in an update protocol that includes:

- Updates of own or 3rd party application software
- Updates of firmware versions

Use the iSDM to scan the devices and check the patch versions of software and firmware, if needed you should download the latest versions and update.

6.4.1 DIGSI 5 Engineering Software

- ✧ Download the latest updates and corresponding readme files from:
<https://support.industry.siemens.com/cs/products?dtp=Download&mfnc=ps&pnid=24304&lc=en-US>



[sc_Downloading Latest tested update from Siemens web, 1, en_US]

Figure 6-13 Downloading Latest Tested Update from Siemens Internet

You can find detailed installation instructions in the readme file. Follow these instructions for installing the update.

6.4.2 SIPROTEC 5

Firmware updates for SIPROTEC devices are installed from the engineering PC in the system. The general installation procedure for DIGSI Updates is described in SIPROTEC 5 manual.

https://support.industry.siemens.com/cs/attachments/109742461/DIGSI5_Onlinehelp_enUS.pdf

6.4.3 SICAM A8000 Series/SICAM RTUs

Every system element of the SICAM A8000 series/SICAM RTUs has its own loadable firmware that is managed centrally by the SICAM TOOLBOX II/SICAM Device Manager. With the SICAM TOOLBOX II/SICAM Device Manager, all the firmware can be reloaded and updated individually. New firmware is first saved in the SICAM TOOLBOX II/SICAM Device Manager and then distributed to SICAM A8000 series/SICAM RTUs.

6.4.3.1 SICAM TOOLBOX

The distribution of the firmware to the SICAM RTUs is carried out with the tool Load Firmware (TOOLBOX II → Service Program/OPM → Load Firmware).

6.4.3.2 SICAM Device Manager

The distribution of the firmware to the SICAM RTUs is carried out via menu item Update devices → Firmware....

6.4.4 RuggedCom Switch RSG2100

Use the following link to download the firmware via the Siemens SIOS portal: <https://support.industry.siemens.com/cs/document/109806156/firmware-download-for-ruggedcom-ros-5-6-0?dti=0&lc=de-DE>.

To upgrade the firmware, you can use the tool SINEC PNI (<https://support.industry.siemens.com/cs/products?mfn=ps&pnid=26672&lc=en-US>).



NOTE

The switches with older hardware (less than 32 MB of RAM) should not receive firmware versions up to V4.3.5. Although switches with new hardware specifications could receive firmware versions like V5.2.0, with new features like an MRP protocol, IPv6 capabilities.

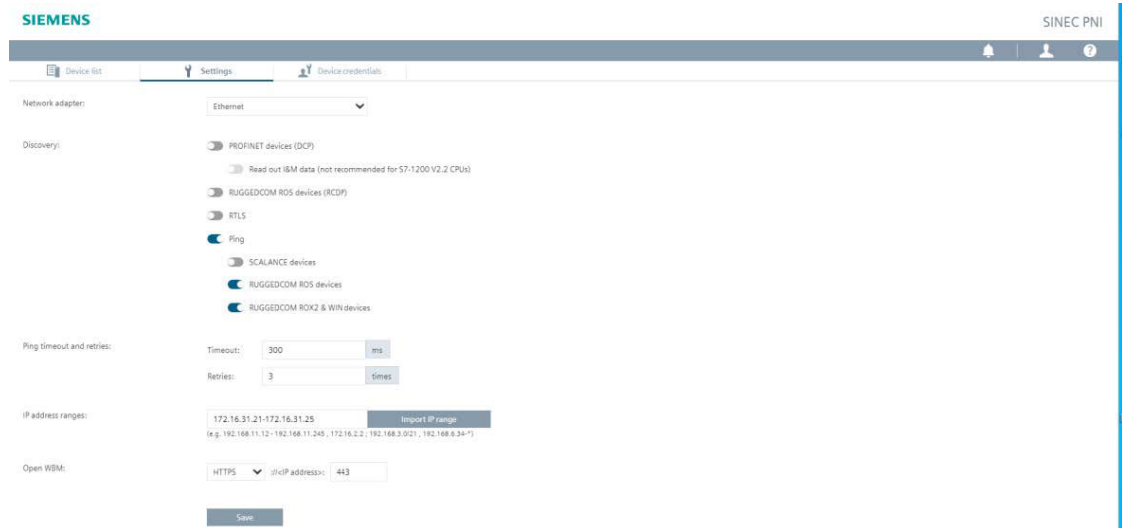
To check the RAM specification, access the Web UI, navigate to **Diagnostics** and **View CPU Diagnostics**, under the **Total RAM** box. You should see an 8-character number, representing the amount of RAM in MB (see following figure).



[!e_Total RAM box, 1, --]

- (1) 3 characters of Mbytes
- (2) 3 characters of kbytes
- (3) 3 characters of bytes

- ✧ Ensure that the switch is reachable via SSH.
- ✧ Open the SINEC PNI tool on the engineering workstation.
- ✧ Open the **Settings** tab.
- ✧ Enable **Ping** and the Ruggedcom ROS devices.



- ✧ Enter the IP address of the switch.
- ✧ Click **Save**.
- ✧ Open the **Device credentials** tab.
- ✧ Enter a username and password with administrator privileges on the switch.
- ✧ Open the **Device list** tab.
- ✧ Click **Start network scan**.

When the scan is finished, the found devices are displayed.

- ✧ Select the devices you want to update.
- ✧ From the **Device Management** list box, click **Firmware Update**.
- ✧ Select the boot.bin and main.bin firmware files.
- ✧ Click **Firmware Update**.
- ✧ Click **OK**.

When the update is finished, the status **Restart pending** is displayed for the updated devices.

- ✧ From the **Device Management** list box, click **Restart Device**.

When the restart is finished, the new firmware version is displayed.

6.4.5 RuggedCom Router RX1500

You can download the firmware via the Siemens SIOS portal: <https://support.industry.siemens.com/cs/products?search=RX1500&ntp=Download&mfno=DefaultRankingDesc&lc=de-DE>

Once the file is available, there are 2 possible approaches:

- Using the SINEC PNI tool
- Using a USB drive

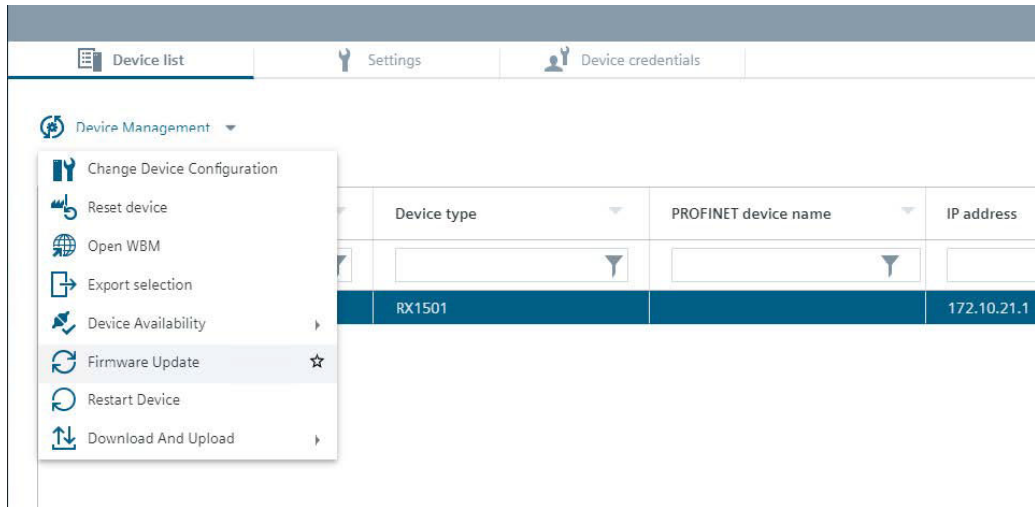
SINEC PNI

- ✧ Open the SINEC PNI tool on the engineering workstation.
- ✧ Open the **Settings** tab.
- ✧ Enable **Ping** and the Ruggedcom ROX2 & WIN devices.
- ✧ Enter the IP addresses of the routers.
- ✧ Click **Save**.
- ✧ Open the **Device credentials** tab.
- ✧ Enter a username and password with administrator privileges on the router.
- ✧ Open the **Device list** tab.
- ✧ Click **Start network scan**.

When the scan is finished, the found devices are displayed.

- ✧ Select the devices you want to update.
- ✧ From the **Device Management** list box, click **Firmware Update**.
- ✧ Under **Firmware file path**, upload the .zip firmware file.
- ✧ Select the network interface card.
- ✧ Select the internal HTTP server with the default port 80.

- ✦ Click **Firmware Update**.



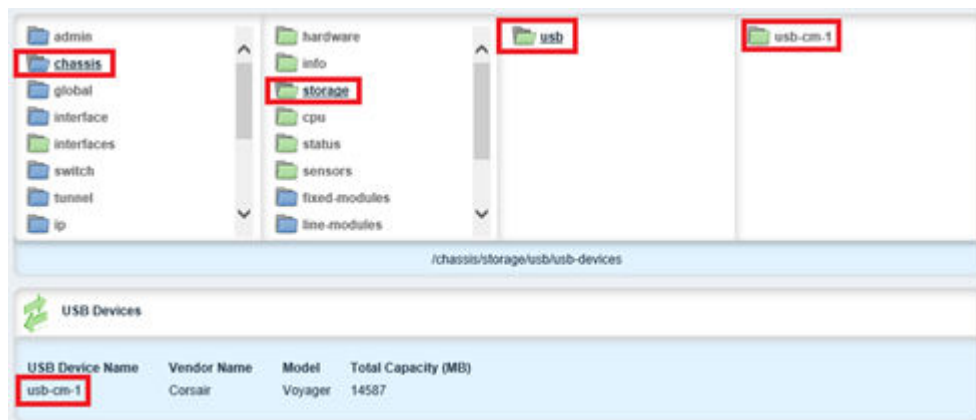
- ✦ Click **OK**.

When the update is finished, the new firmware version is displayed.

USB Update

Alternatively, the update can be performed by plugging in a USB to the router which contains the update file.

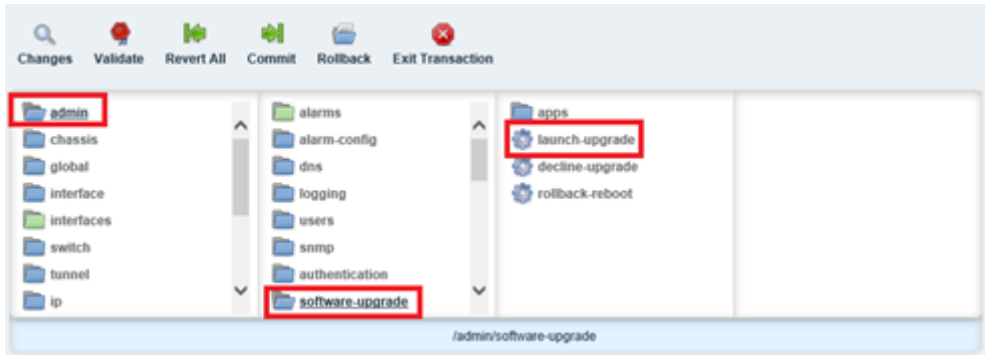
- ✦ Navigate to **chassis** → **storage** → **usb**.
- ✦ Click USB and copy the **USB Device Name**.



[sc_Updating Ruggedcom through USB Drive, 1, en_US]

Figure 6-14 Updating RuggedCom Through USB Drive

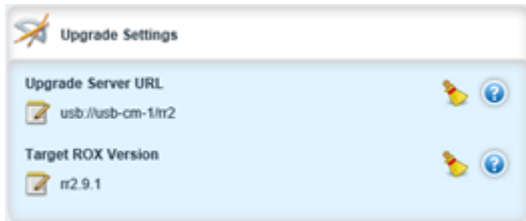
- ✦ Navigate to the update settings with **admin** → **software-upgrade** (as below), but do not process **launch-upgrade** yet. A configuration is required prior to launching the upgrade.



[sc_Creating an update Folder, 1, en_US]

Figure 6-15 Creating an Update Folder

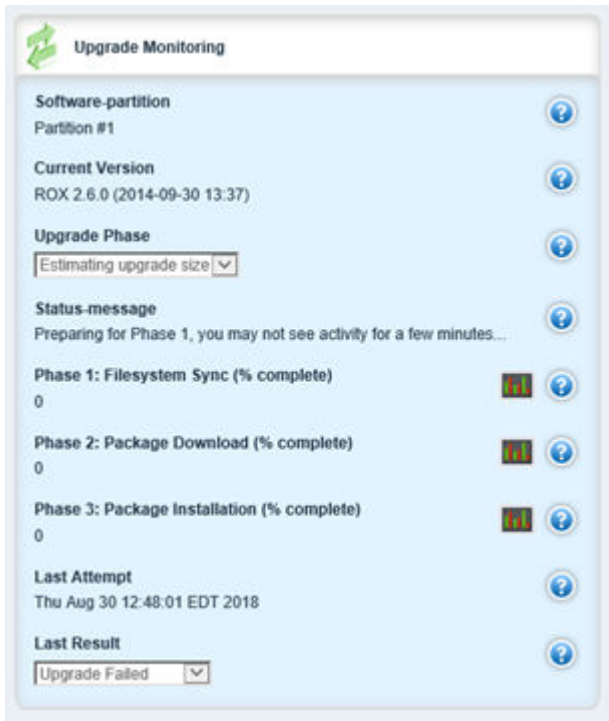
- ✧ Configure the server URL and the target ROX version according to the downloaded one and according to the USB name copied previously.



[sc_Configuring Update Server URL, 1, en_US]

Figure 6-16 Configuring Update Server URL

- ✧ Now, **launch-upgrade**. Use the **Upgrade Monitoring** area under **admin** → **software-upgrade** to look if everything worked.



[sc_Upgrade Monitoring, 1, en_US]

Figure 6-17 Upgrade Monitoring

- ✧ Wait until the upgrade finish and reboot the system under **admin** → **reboot**.

7 Malware Protection/Prevention

7.1	Motivation	194
7.2	Windows Defender	194
7.3	Malware Protection for Siemens Products	222
7.4	Recommendations	223

7.1 Motivation

Malware protection encompasses all technologies that provide protection of infection of a system with malware, e.g. by special configuration as deactivation of USB ports, and also the detection of malware by dedicated software products.

Protection against malware infection is essential for all IT systems including those used in process networks and controls systems.

The concepts for anti-virus tools known from office environments are also applicable to process networks and control systems but need to be adapted due to the different requirements. Updates to malware software may impact the control-system behavior or process-network performance. A direct connection to the Internet for downloading the updates is generally not allowed from within a secure zone in an industrial environment. Furthermore, automatic detection and removal of system components identified as malware poses a not acceptable risk to these environments. If components belonging to the system are wrongly identified as malware and deactivated, the control system or process-network component may not work anymore – affecting availability. In contrast, most malware infections do not lead to immediate system unavailability.

This chapter describes 3 approaches to prevent from malware:

- Windows-specific malware protection
- Malware protection for Siemens products
- Other malware protection measures

7.2 Windows Defender

The latest version of Windows provides a range of inbuilt tools to increase the security of the system. These tools are part of the Windows Defender Family. In the recent years, the Windows 10 built-in security capabilities have increased tremendously. This is the reason why in new projects, 3rd party Malware Protection tools can be replaced by these inbuilt windows tools.

Malware protection can be achieved by 2 different means namely:

- Blacklisting of unnecessary application and processes
- Whitelisting of necessary applications

The **Windows Defender Antivirus** shall be used to achieve blacklisting which is inbuilt with Windows 10 or Server 2016/2019. For Whitelisting Windows Defender Application Control (WDAC) and Windows Defender Exploit Protection shall be used in conjunction which prevents against known exploit techniques. The components of Windows Defender with different OS are as follows:

Table 7-1 Windows Defender Features

	Windows Defender Application Control	Windows Defender Exploit Protection	Windows Defender Antivirus
Windows 10 Enterprise LTSC 2016	Yes (code integrity policies)	No	Yes
Windows 10 Enterprise LTSC 2019	Yes	Yes	Yes
Windows Server 2016	Yes (code integrity policies)	No	Yes
Windows Server 2019	Yes	Yes	Yes

7.2.1 Blacklisting Solution with Windows Defender

Windows Defender Antivirus is part of Windows Defender and a Windows built-in malware protection. No additional software installation is required. The Windows Defender Security Center and Windows Defender Antivirus have been continuously improved with updates to Windows 10.

The following section describes how to set up the Windows Defender Antivirus using group policies and how to update it using WSUS. It also shows the log management and use of the Defender Antivirus on Windows Server 2016/2019.

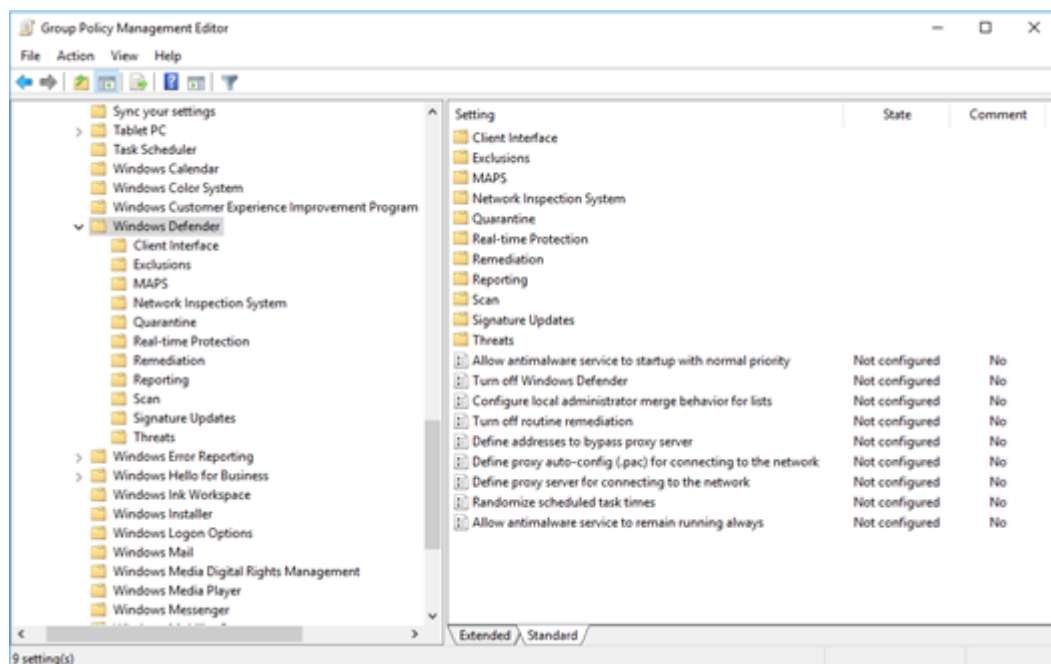
Windows 10 Defender Antivirus: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-antivirus/windows-defender-antivirus-in-windows-10>

7.2.1.1 Setting up/Configuring Windows Defender Antivirus

The Windows Defender is installed by default in Windows operating system. It can only be used if there is no other malware protection installed. It requires to enable and configure the client on endpoints using group policies. This can be done either using the local group policy editor or in the Domain Controller (in Active Directory environments).

To configure and manage Windows Defender Antivirus using group policies via the domain controller (Windows Server), proceed as follows:

- ✧ On your Group Policy management machine, open the **Group Policy Management Console**, right-click the **Group Policy Object (GPO)** you want to configure, and click **Edit**.
- ✧ In the **Group Policy Management Editor**, go to **Computer configuration**.
- ✧ Click **Policies**.
- ✧ Click **Administrative templates**.
- ✧ Expand the tree to **Windows components > Windows Defender Antivirus**.
- ✧ Expand the section (referred to as Location in the table in this topic) that contains the setting you want to configure, double-click the setting to open it, and make configuration changes.
- ✧ Deploy the updated GPO as you normally do.



[sc_Editing Group Policy for Windows Defender, 1, en_US]

Figure 7-1 Editing Group Policy for Windows Defender

A description of the Group Policy management settings can be found on the Microsoft website:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-antivirus/use-group-policy-windows-defender-antivirus>

It is possible to configure certain parts of Windows Defender Antivirus via command line. E.g. removing the signatures of the previous version in case of compatibility issues. A description of all commands can be found on the Microsoft website:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-antivirus/command-line-arguments-windows-defender-antivirus>

7.2.1.2 Configuring Windows Defender Antivirus via Local GUI

Windows Defender Antivirus provides limited configuration possibilities via the local GUI.

- ✧ To start the interface, click the **Windows** and start the **Windows Security Center**.

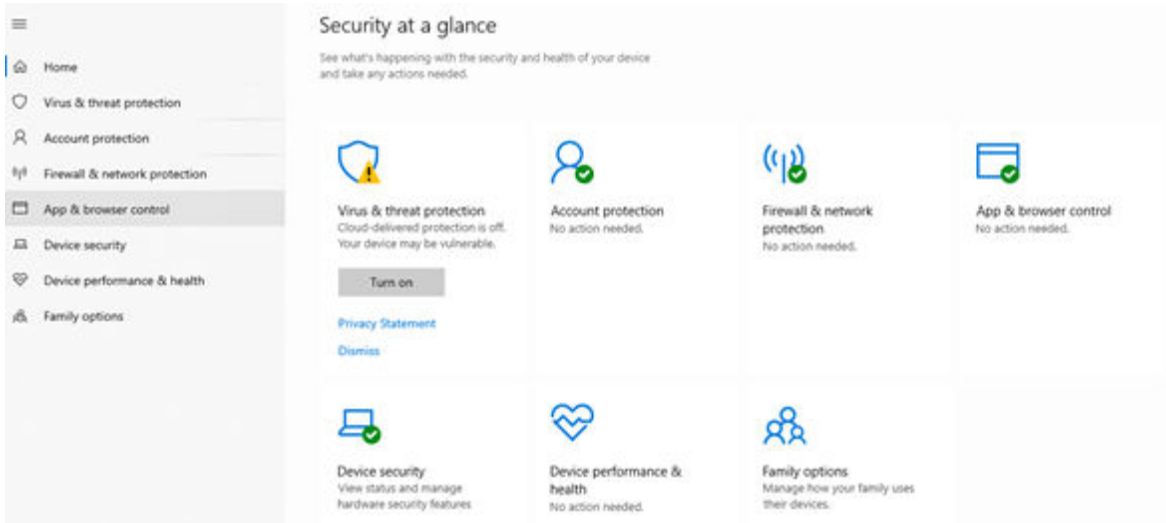


[sc_Selecting Windows Security in Start Menu, 1, en_US]

Figure 7-2 Selecting Windows Security in Start Menu

The **Windows Security Center** provides an overview on different security-related features.

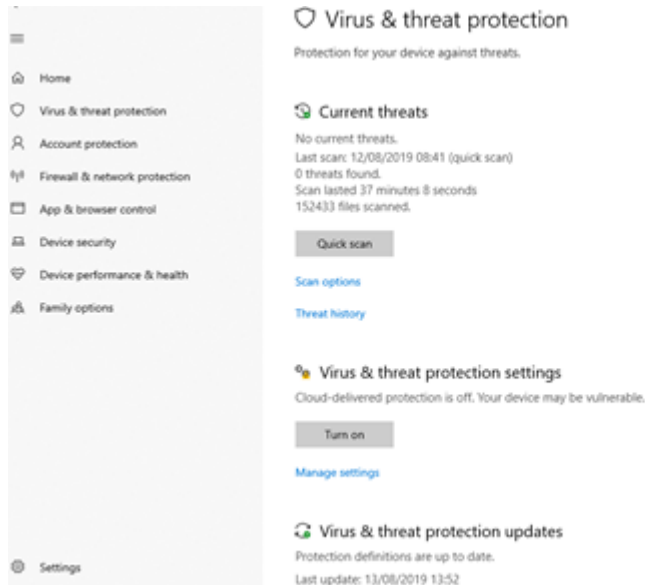
- ✧ To open the Windows Defender Antivirus configuration interface, click **Virus and threat protection**.



[sc_Selecting Virus and Threat Protection in Security Settings, 1, en_US]

Figure 7-3 Selecting Virus and Threat Protection in Security Settings

- ✧ The **Scan of Local PC** and **Check for Updates** can be accessed from here.



[sc_Enabling Virus and Threat Protection, 1, en_US]

Figure 7-4 Enabling Virus and Threat Protection

7.2.1.3 Updates for Windows Defender Antivirus

2 types of updates are available for Windows Defender:

- **Definition updates:**
Definition updates are updates to malware detection signatures.
- **Product updates:**
The product updates are updates to features and settings of the Windows Defender Antivirus.

The Windows 10 LTSB (Long-Term Service Branch) can only get the definition updates.

The recommended way of updating the Windows Defender Antivirus is the usage of WSUS (Windows Server Update Services). The definition updates will be distributed the same way as other Windows patches and updates via WSUS.

It is also possible to download the definition updates for the Windows Defender Antivirus from the Microsoft Malware Protection Center (MMPC) definitions page: <https://www.microsoft.com/en-us/wdsi/definitions>. These are called **Security intelligence updates**.

- ✧ Click the version of operating system used (e.g. 64bit, next to Windows Defender Antivirus for Windows 10). For Windows Server 2016 or 2019, the same updates as for Windows 10 is used.

You need to download different security intelligence files for different products and platforms. Select the version that matches your [Windows operating system](#) or the environment where you will apply the update.

Note: Starting on Monday October 21, 2019, the Security intelligence update packages will be SHA2 signed. Please make sure you have the necessary update installed to support SHA2 signing, see [2019 SHA-2 Code Signing Support requirement for Windows and WSUS](#).

Antimalware solution	Definition version
Microsoft Defender Antivirus for Windows 10 and Windows 8.1	32-bit 64-bit ARM
Microsoft Security Essentials	32-bit 64-bit
Windows Defender in Windows 7 and Windows Vista	32-bit 64-bit
Microsoft Diagnostics and Recovery Toolset (DaRT)	32-bit 64-bit
System Center 2012 Configuration Manager	32-bit 64-bit
System Center 2012 Endpoint Protection	32-bit 64-bit
Windows Intune	32-bit 64-bit

The links point to an executable file named *mpam-fe.exe*, *mpam-feX64.exe*, or *mpas-fe.exe* (used by older antispysware solutions). Simply launch the file to manually install the latest security intelligence.

[sc_Downloading latest update of Windows Defender, 1, en_US]

Figure 7-5 Downloading Latest Update of Windows Defender

This will download all the released patterns as one file (called mpam-fe.exe). This downloaded file can either be executed locally in each client machine or distributed centrally.

7.2.1.4 Feature Updates of Windows Defender Antivirus Platform

Feature updates for the Windows Defender Antivirus platform periodically can be installed separately. These updates can be downloaded manually from the Microsoft Update Catalogue or via a WSUS Server. It is recommended to install the updates whenever Windows Updates are installed. The updates contain feature updates and bug fixes. In Windows Defender, this patch will update the Antimalware Client Version. The updates are provided via the KB4052623.

<https://support.microsoft.com/en-us/help/4052623/update-for-windows-defender-antimalware-platform>

The screenshot shows the Microsoft Update Catalog search results for "windows defender". The search bar contains "windows defender" and the search button is labeled "Search". Below the search bar, there are links for "FAQ" and "help". The search results are displayed in a table with columns: Title, Products, Classification, Last Updated, Version, Size, and Download. The table lists several updates, including "Update for Windows Defender Antivirus antimalware platform - KB4052623 (Version 4.18.2001.10)" and "Update for Windows 8 for x64-based Systems (KB3025417)".

Title	Products	Classification	Last Updated	Version	Size	Download
Update for Windows Defender Antivirus antimalware platform - KB4052623 (Version 4.18.2001.10)	Windows Defender	Updates	4/30/2020	n/a	13.1 MB	Download
Update for Windows Defender Antivirus antimalware platform - KB4052623 (Version 4.18.2001.10)	Windows Defender	Updates	3/4/2020	n/a	13.1 MB	Download
Update for Windows Defender Antivirus antimalware platform - KB4052623 (Version 4.18.2001.10)	Windows Defender	Updates	2/27/2020	n/a	13.1 MB	Download
Update for Windows 8 for x64-based Systems (KB3025417)	Windows 8	Update Rollups	3/9/2015	n/a	6.3 MB	Download
Update for Windows Vista for x64-based Systems (KB931099)	Windows Vista	Updates	4/10/2007	n/a	3.3 MB	Download
Update for Windows Vista (KB931099)	Windows Vista	Updates	4/10/2007	n/a	2.6 MB	Download

[sc_Feature update of Windows Defender, 1, en_US]

Figure 7-6 Feature Update of Windows Defender

7.2.1.5 Update File Location

The signature update files of Windows Defender Antivirus are stored locally in the following folder:
C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{GUID}

his PC > (C:) SYSTEM > ProgramData > Microsoft > Windows Defender > Definition Updates > {F45B8177-FDB4-458F-A048-EE828CEC788A}

Name	Date modified	Type	Size
mpasbase.vdm	8/11/2020 11:18 AM	VDM File	48,233 KB
mpasdlta.vdm	8/11/2020 11:18 AM	VDM File	3,640 KB
mpavbase.vdm	8/11/2020 11:19 AM	VDM File	43,400 KB
mpavdlta.vdm	8/11/2020 11:18 AM	VDM File	8,856 KB
mpengine.dll	8/11/2020 6:04 AM	Application extens...	14,188 KB

[sc_Defender update file location, 1, en_US]

Figure 7-7 Defender Update File Location

The following files are part of the Security Intelligence Updates:

- Antispyware (mpasbase.vdm + mpasdlta.vdm)
- Antivirus (mpavbase.vdm + mpavdlta.vdm)
- Engine (mpengine.dll)

The previous versions of these files are stored in the following folder:

C:\ProgramData\Microsoft\Windows Defender\Definition Updates\Backup

7.2.1.6 Logging of Windows Defender Antivirus

The Windows Defender Antivirus records events with IDs in the Windows event log. The event logs can be viewed either directly or using third-party tools for central security log collection.

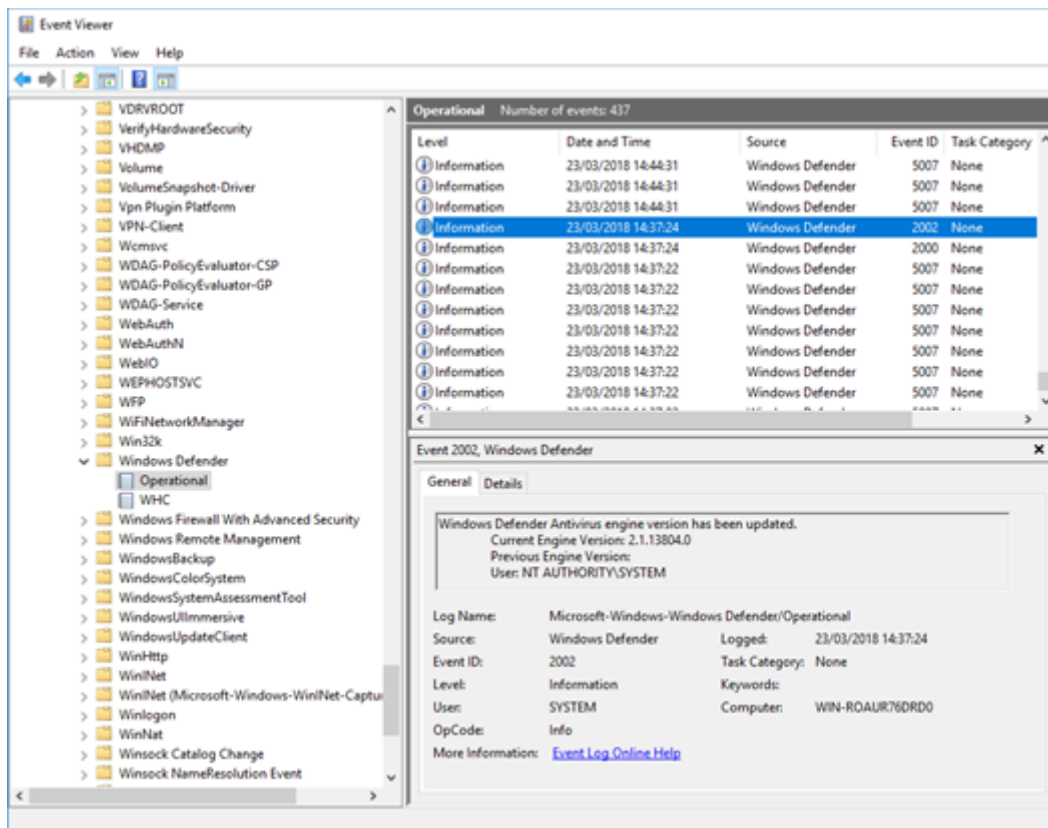
Viewing Events in the Windows Event Log

To view the events of Defender Antivirus in the Windows event log, proceed as follows:

- ✧ Open the Event Viewer.
- ✧ In the console tree, expand **Applications and Services Logs** → **Microsoft** → **Windows** → **Windows Defender Antivirus**.
- ✧ Double-click **Operational**.
- ✧ In the details pane, view the list of individual events to find your event.
- ✧ Click the event to see specific details about an event in the lower pane, under the **General and Details** tabs.

Seeing all Event IDs and Descriptions

- ✧ To see all events IDs and their description go to:
<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-antivirus/troubleshoot-windows-defender-antivirus>
- ✧ Report on Windows Defender Antivirus protection:
<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-antivirus/report-monitor-windows-defender-antivirus>



[sc_Defender Antivirus event log, 1, en_US]

Figure 7-8 Defender Antivirus Event Log

7.2.1.7 Microsoft Windows Defender Antivirus on Microsoft Windows Server 2016

Microsoft Windows Defender Antivirus is available by default on the Microsoft Windows Server 2016. The user interface is also installed by default on some Microsoft Windows Server editions. If it is not installed it can be added using the **Add Roles and Features** wizard at the **Features** step, under **Windows Defender Features** by selecting the option **GUI for Windows Defender**.

The difference between the Microsoft Windows Defender Antivirus on Microsoft Windows 10 and Microsoft Windows Server 2016 is the application of automatic exclusions based on the defined server role(s).

To verify that Microsoft Windows Defender Antivirus is running on the server, run the following command from a command prompt:

```
>> sc query Windefend
```

The sc query command returns information about the Microsoft Windows Defender service. If Microsoft Windows Defender is running, the **STATE** value displays **RUNNING**.

Microsoft Windows Defender Antivirus on Windows Server 2016:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-antivirus-windows?view=o365-worldwide>

7.2.2 Whitelisting Solution with Windows Defender

The application whitelisting is a protection mechanism that allows only trusted programs and applications to run on a system. Therefore, it blocks unknown/malicious code. Whitelisting software is installed after installing necessary system applications on a virus-free machine. A whitelist of programs, applications, and services will be generated by the whitelisting solution. All applications/programs/services on the list will be signed or secured by a checksum. This ensures that only approved software will be executed. The downloaded software or viruses that might potentially infect the system after activation of the whitelisting protection

will be prevented from executing. Newly installed software from reliable sources should be signed. The main benefit is the reduced frequency of installing pattern files. A patch-management process is still required. For substation automation projects where antivirus/antimalware solutions are not applicable or additional security is required, or where the regular update of signature files of a regular antivirus solution is not feasible, the use of application whitelisting is recommended.

The whitelisting solution will be realized with Windows Defender Application Control (WDAC). The Windows Defender Exploit Protection will provide memory protection features that 3rd-party whitelisting programs include.

7.2.2.1 Windows Defender Application Control (WDAC)

Windows Defender Application Control (WDAC) will create the whitelist of trusted executable files on a PC. When enforced, it will only allow files to run that are part of the whitelist. Every other application will be blocked. WDAC policies also block unsigned scripts and MSIs, and Windows PowerShell runs in Constrained Language Mode.



NOTE

The whitelist can only be created on Windows 10 Enterprise/Professional editions or Windows Server 2016 and newer.

7.2.2.2 Windows Defender Exploit Protection

The exploit protection feature of Windows helps to protect against memory-based attacks, where malware or other code manipulates memory to gain control of a system for example, malware that attempts to use buffer overruns to inject malicious executable code into memory. This feature is considered here because 3rd-party whitelisting applications provide similar functionalities.

The exploit protection is the successor of the Enhanced Mitigation Experience Toolkit (EMET) and includes its features. The exploit protection is supported beginning with Windows 10, version 1709 and Windows Server 2016, version 1803.

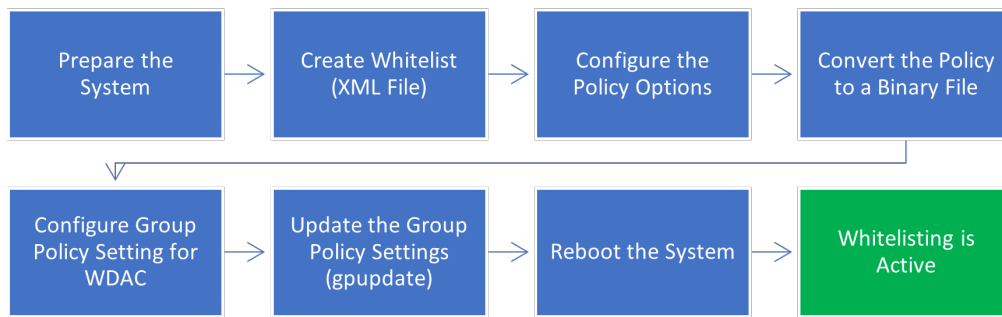


NOTE

Depending on a project-specific security analysis, application whitelisting may be used as alternative to regular antivirus protection software, to protect system components from malware. It is not recommended to use application whitelisting as a replacement for the timely qualification and installation of security patches, as application whitelisting is not considered capable of addressing all vulnerabilities and attack scenarios that are addressed by security patches for the installed software versions.

7.2.2.3 Configuration Process for WDAC

This section describes the process, how to initially configure WDAC on a Windows-based system.



[sc_Configuration process of WDAC, 1, en_US]

Figure 7-9 Configuration Process of WDAC

Preparing the System

Before starting the whitelisting process, the following tasks should be finished:

- ✧ Install all required applications.
- ✧ Install all required updates/patches.
- ✧ Close all running applications.
- ✧ Remove all unneeded files from the PC.
- ✧ Perform a malware scan with Windows Defender Antivirus (Full Scan).

Configuration Process

- ✧ Create the whitelist (.xml file):
The system is scanned for all executable files on the system and will create an xml file that contains the whitelist. The xml file contains Hash-values of the executables or the certificate that has been used to sign the executable.
- ✧ Configure the policy options:
The xml policy contains several settings. The options must be configured for the policy.
- ✧ Convert the policy to a binary file.
Windows can only apply the WDAC policy if it is available in a binary format. Accordingly, the xml whitelist file must be converted into a binary format.
- ✧ Configure the Group policy setting for WDAC.
WDAC must be enabled via a group policy setting that specifies the path to the binary whitelisting policy.
- ✧ Reboot the system.
Whitelisting will be activated after a reboot of the system. The **SIPolicy.P7B** whitelisting policy will be applied.

7.2.2.4 Creating and Deploying a Policy

The configuration of Windows Defender Application Control is done via PowerShell. The required steps are described in this section. To enable WDAC, you must execute the PowerShell commands in this section.

Prerequisites

Before creating the whitelisting, make sure the following steps are finished:

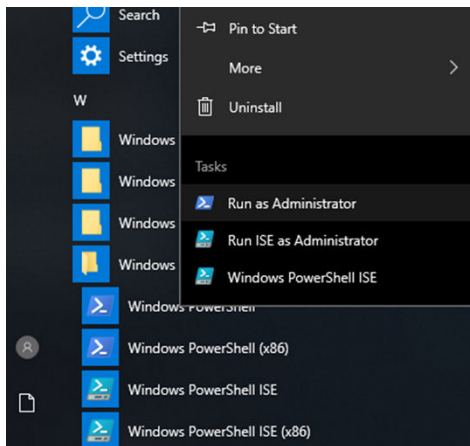
- ✧ Install all required applications.

- ✧ Install all required updates/patches for operating system and applications.
- ✧ Close all running applications.
- ✧ Remove all unneeded files from the PC.
- ✧ Perform a malware scan with Windows Defender Antivirus (Full Scan).

Enabling WDAC

To enable WDAC, the first step is to create an initial policy (the whitelist). The policy must be created via PowerShell. After that you can convert the policy to binary and deploy it via group policies. To simplify the engineering, you can copy the PowerShell code from [7.2.2.8 PowerShell Command Summary](#).

- ✧ Open the PowerShell or the PowerShell ISE with administrative privileges. Right-click the **Windows PowerShell** in the **Start** menu and click **Run as Administrator**.



[sc_Starting Power shell as Administrator, 1, en_US]

Figure 7-10 Starting Power Shell as Administrator

- ✧ Run the cmdlet **New-CIPolicy**.
This cmdlet will initiate a scan for all executable files on the system and create an xml with the whitelist. The xml file contains Hash-values of the executables or the certificate that has been used to sign the executable.

PowerShell command:

```
New-CIPolicy -Level Publisher -Fallback Hash -Filepath C:\Windows\System32\Codeintegrity\ExamplePolicy.xml
-UserPEs 3> CIPolicyLog.txt
```

The following parameters are part of this command:

- **Level:**
Defines the parameter of each file that is contained in the whitelist (e.g. Publisher or Hash value)
- **Fallback (optional):**
Defines a Fallback level in case the usage of the initial **level** is not possible (e.g. if a file is not digitally signed)
- **ScanPath (optional):**
Defines the paths that will be scanned (otherwise it scans the entire system)
- **Filepath:**
Defines the output policy file
- **UserPEs:**
This is required to enable whitelisting for applications.
- **3> CIPolicylog.txt:**
This will write WDAC logs into a textfile.

Depending on the system size and system performance, the scan can take more than one hour to finish.

- ✧ Remove the Audit Mode option.

The audit mode is enabled by default in the policy. To enforce the whitelisting, you must remove the option. If you want to run the policy in audit mode skip this step!

Remove the audit option using PowerShell:

- 1 # Remove the audit node option
- 2 Set-RuleOption -FilePath C:\Windows\System32\CodeIntegrity\ExamplePolicy.xml -option 3 -delete

PowerShell command:

The execution of this command will take a while. You can also edit the policies manually to add or remove rule options. The policies are in the XML format.

- ✧ Set recommended options for the policy:

Microsoft strongly recommends enabling rule options 9 (F8 reboot menu) and 10 (Enable Boot on Audit Failure) before running any enforced policy for the first time. Doing so allows Windows to start with the code integrity policy in audit mode if the code integrity policy blocks a kernel-mode driver from running and provides administrators with a reboot command prompt.

Set the rule options 9 and 10:

Setting recommended security rules

PowerShell commands:

```
Set-RuleOption -FilePath C:\Windows\System32\CodeIntegrity\ExamplePolicy.xml -Option 9
```

```
Set-RuleOption -FilePath C:\Windows\System32\CodeIntegrity\ExamplePolicy.xml -Option 10
```

- ✧ Optionally: Merge the policy with the Microsoft Recommended Block rules.

- ✧ Convert the xml policy to a binary policy:

WDAC can only use binary whitelisting files. Convert the .xml policy to a binary with the (ConvertFrom-CIPolicy <<xml>><<bin>>) Cmdlet.

Keep the original .xml file for merging or updating the policy later!

PowerShell commands:

```
1 # Convert policy to binary
```

```
2 ConvertFrom-CIPolicy C:\Windows\System32\CodeIntegrity\ExamplePolicy.xml  
C:\Windows\System32\CodeIntegrity\ExamplePolicy.bin
```

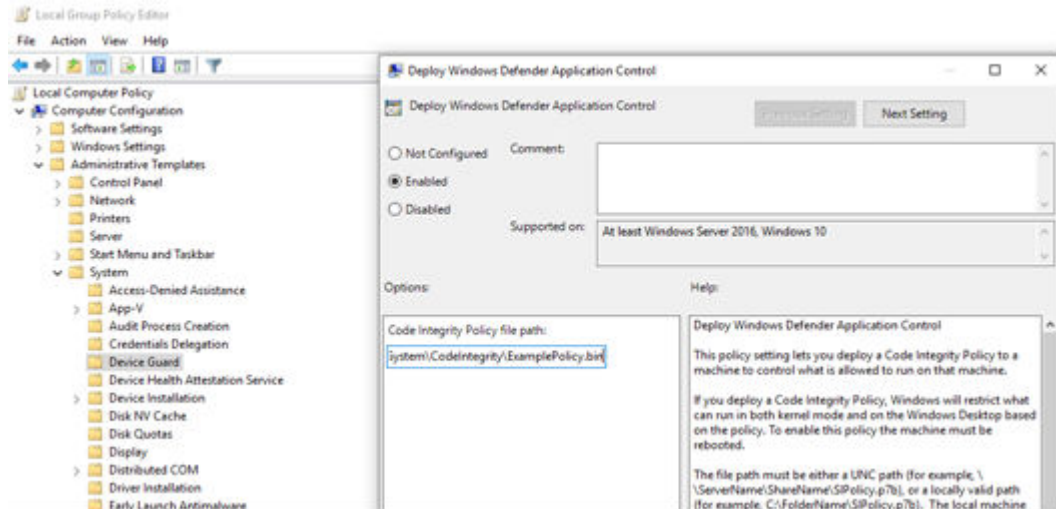
- ✧ Deploy the policy using group policies.

To enable WDAC, a group policy setting is required.

- ✧ Copy the binary policy to C:\Windows\System32\CodeIntegrity.

- ✧ Group policy editor:

Computer Configuration\Administrative Templates\System\Device Guard. Go to **Deploy Windows Defender Application Control**, set it **Enabled**, and enter the path of the binary policy (e.g. C:\Windows\System32\CodeIntegrity\ExamplePolicy.bin).



[sc: Enabling WDAC in group Policy Editor, 1_en_US]

Figure 7-11 Enabling WDAC in Group Policy Editor

- ✧ Open a command prompt and execute **gpupdate /force**.
- ✧ Restart the computer (the feature will be enabled only after a reboot).



NOTE

Important:

Each PC can have only one code-integrity policy. If you want to add new files to the whitelist, you will have to merge policies or create a new whitelist.

If you create a WDAC policy on a different PC than where it will be applied, it is important that you first audit the code-integrity policy on every model of machine to which you will deploy the policy. If you do not, the policy could block the operating system from loading at all, caused by different content of the KMCI policy (e.g. different device drivers).

7.2.2.5 Installation of Updates

During the operation phase, it will be necessary to install different types of updates on the PCs:

- Windows updates:
To install Windows updates, no change in the whitelisting policy is necessary.
- Application updates/hotfixes:
To install updates of applications, it may be necessary to update the WDAC policy.

If the publisher rule for the policy is used and the applications are signed by default, there is no need to update the policy when an application will be updated, because the publisher (and therefore the update) is trusted. New application from a trusted publisher can always be installed (depends on the level e.g. FilePublisher or SignedVersion).

The whitelisting policy must be updated in the following cases:

- The update is not digitally signed.
- The publisher is not trusted in the whitelisting policy.

The recommended way to update the whitelisting policy is to merge the existing policy with a new policy that contains the rules for the update.

Option 1: Merging of Policies

It is possible to merge different .xml policies into a single .xml policy. This can be necessary, e.g. after an update has been installed or to add new applications to the policy. A prerequisite for this option is, that the initial .xml policy is still available!

Steps to create a new policy (for new or updated applications) to update your latest policy:

- ✧ Turn off WDAC.
Refer to [7.2.2.7 Disabling WDAC](#).
- ✧ Install all the required applications and application updates.
- ✧ Create a new policy including only the files of the installed software. Use the Scanpath parameter to scan only a certain folder:
Create one new xml policy for each folder that includes updated files. The following example includes updates for SICAM PAS (Core Components and Systems Services are installed in different directories):
#Create a new Policy based on a limited Scan
New-CIPolicy -Level Publisher -Fallback Hash -Scanpath C:\Program Files (x86)\Siemens Energy\ -Filepath C:\Windows\System32\Codeintegrity\UpdatePolicy.xml -UserPEs > CIPolicyLog.txt

Powershell commands:

```
New-CIPolicy -Level Publisher -Fallback Hash -Scanpath C:\Program Files (x86)\Siemens Energy\ -Filepath C:\Windows\System32\Codeintegrity\UpdatePolicy1.xml -UserPEs 3> CIPolicyLog.txt  
New-CIPolicy -Level Publisher -Fallback Hash -Scanpath C:\Siemens\ -Filepath C:\Windows\System32\Codeintegrity\UpdatePolicy2.xml -UserPEs 3> CIPolicyLog.txt
```

- ✧ Merge your initial policy or latest policy (xml) with the new created policy (xml). The Merge-CIPolicy command is used to merge 2 or more policies into a single file:

```
Merge-CIPolicy -PolicyPaths <policy1.xml>,<policy2.xml> -OutputFilePath <mergedpolicy.xml>
```

Below is an example, how the initial policy can be merged with the two update policies.

```
1 # Declare Initial (old) Policy Variable  
2 $InitialCIPolicy="C:\Windows\System32\CodeIntegrity\ExamplePolicy.xml"  
3  
4 # Declare New Policy with updated files (1) Variable  
5 $UpdateCIPolicy1="C:\Windows\System32\CodeIntegrity\UpdatePolicy1.xml"  
6  
7 # Declare New Policy with updated files (2) Variable  
8 $UpdateCIPolicy2=" C:\Windows\System32\CodeIntegrity\UpdatePolicy2.xml"  
9  
10 # Declare Merged Policy (xml) Variable  
11 $MergedCIPolicy=" C:\Windows\System32\CodeIntegrity\MergedPolicy.xml"  
12  
13 # Merge the two xml policies  
14 Merge-CIPolicy -PolicyPaths $InitialCIPolicy,$UpdateCIPolicy1,$UpdateCIPolicy2 -OutputFilePath $Merged-  
CIPolicy  
15  
16 # Delete the Audit Option  
17 Set-RuleOption -FilePath C:\Windows\System32\CodeIntegrity\MergedPolicy.xml -option 3 -delete  
18  
19 # Declare Merged Policy (Binary) Variable  
20 $CIPolicyBin=" C:\Windows\System32\CodeIntegrity\Mergedpolicy.bin"  
21  
22 # Convert Merged Policy to binary - Check options in the xml file before doing this  
23 ConvertFrom-CIPolicy $MergedCIPolicy $CIPolicyBin
```

When creating a new policy after an update, the following default folders must be scanned for updates of specific Applications:

To be scanned folders	Paths
SICAM PAS	C:\ProgramFiles (x86)\Siemens Energy\ C:\Siemens\
SICAM SCC	C:\ProgramFiles (x86)\Siemens Energy\ C:\ProgramFiles (x86)\Siemens\ C:\ProgramFiles (x86)\Common Files\Siemens\
DIGSI 5	C:\ProgramFiles\Siemens Energy\ C:\ProgramFiles (x86)\Siemens Energy\
Automation License Manager	C:\Program Files\Siemens\
.NET Framework	C:\Windows\assembly C:\Windows\Microsoft.NET\



NOTE

In some cases, it is necessary to include additional files/folders in the updated whitelist. E.g. when files in the Windows folder have been changed.
Some parts of the above-mentioned applications create unsigned .dll files with a random name when the application is executed (e.g. for PASoperateclient). This means that application whitelisting should be set in audit mode after installing an update.

Option 2: Create a Completely New Policy

Another way is to create a completely new policy each time an application is updated, or a new application needs to be installed. The advantage of this option is, that it is easier and faster to implement. The disadvantage is that potentially unwanted applications may be included in the whitelist.

Steps to create a completely new policy for updates:

- ✧ Turn off WDAC.
Refer to [7.2.2.7 Disabling WDAC](#).
- ✧ Install all the required applications and application updates.
- ✧ Create a new policy.

Option 3: Installation of Updates via Catalog File

To use additional unsigned LOB applications, Microsoft recommends the use of catalog files. They can be used to update or extend an application control policy without the need to regenerate the xml policy file.

The catalog files must be signed and you need to configure your WDAC policies to trust the signer or signing certificate (if not already configured). This requires an internal certification authority (CA) code signing certificate or purchased code signing certificate.

The catalog files need to be updated each time an application is updated!

For the creation of the catalog files, the tool **Package Inspector** will be used, that monitors the installation binaries so that they can be trusted. Then, you create the catalog file, identifying the discovered binaries, and sign it.

Steps to create, sign, and deploy a catalog file:

- ✧ Refer to <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/deploy-catalog-files-to-support-windows-defender-application-control>.

7.2.2.6 WDAC Event Logs

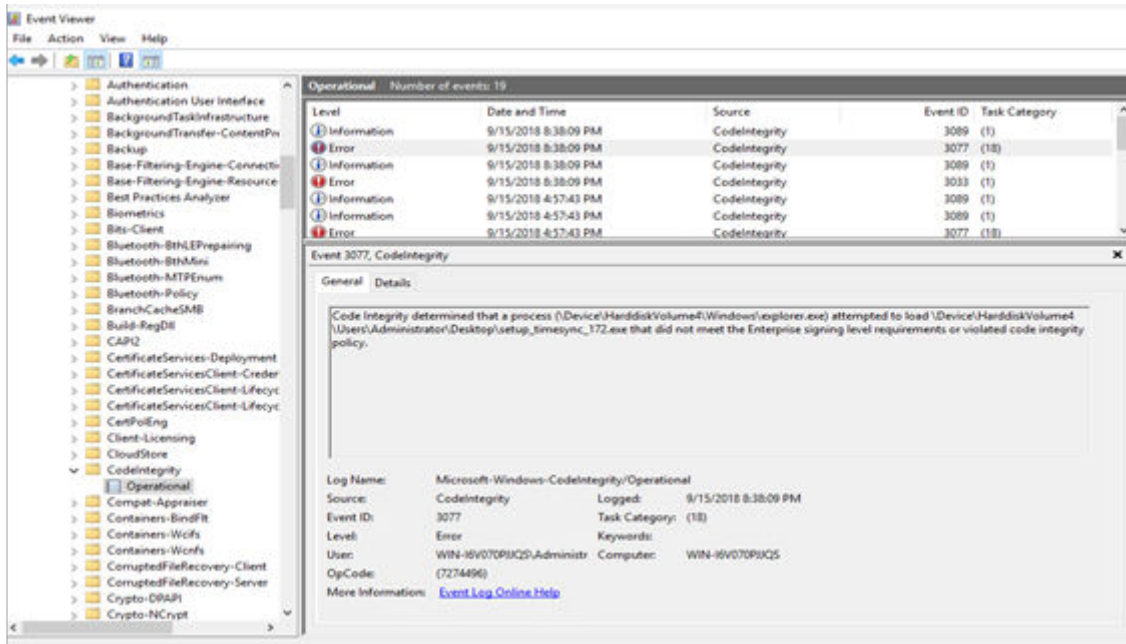
Logs of WDAC can be found in the Windows Event Viewer.

The logs during operation (e.g. blocked execution of files) are stored in the following subfolder:

- Applications and Services Logs\Microsoft\Windows\CodeIntegrity\Operational

The logs regarding activation and deactivation of WDAC are stored in the following subfolder:

- Applications and Services Logs\Microsoft\Windows\DeviceGuard\Operational

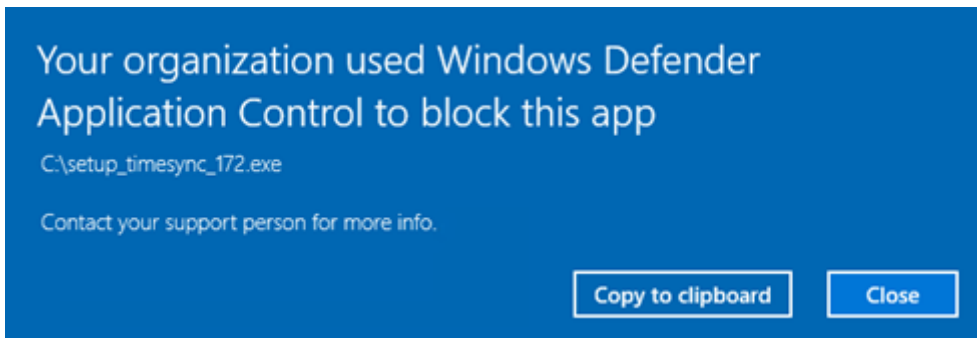


[sc_Device Guard Logs in Event Viewer, 1, en_US]

Figure 7-12 Device Guard Logs in Event Viewer

If the policy is in audit mode, all programs can run, but will still create a log entry, in case they are not whitelisted.

If the policy is in non-audit mode, the program will not run, and will create a log entry (Event ID 3077). In addition, a pop-up window will appear. The pop-up may look different, depending on the OS version and executed type of application.



[sc_Pop up on unauthorized application blocking, 1, en_US]

Figure 7-13 Pop-Up on Unauthorized Application Blocking

7.2.2.7 Disabling WDAC

To disable WDAC, you must follow the following steps. Only disabling WDAC via group policy is not enough:

- ✦ Disable WDAC via the **Group Policy Setting**.
- ✦ Run the command **gpupdate /force**.
- ✦ Delete the File C:\\Windows\\System32\\CodeIntegrity\\SIPolicy.p7b.
- ✦ Restart the PC.

7.2.2.8 PowerShell Command Summary

This section contains only PowerShell code that has been described in the previous chapters. An overview of all PowerShell cmdlets for WDAC can be found on the Microsoft Website:

<https://docs.microsoft.com/en-us/powershell/module/configcil?view=win10-ps>

7.2.2.9 Whitelist Creation

```
New-CIPolicy -Level Publisher -Fallback Hash -Filepath C:\Windows\System32\CodeIntegrity\ExamplePolicy.xml
-UserPEs 3> CIPolicyLog.txt
Set-RuleOption -FilePath C:\Windows\System32\CodeIntegrity\ExamplePolicy.xml -option 3 -delete
Set-RuleOption -FilePath C:\Windows\System32\CodeIntegrity\ExamplePolicy.xml -Option 9
Set-RuleOption -FilePath C:\Windows\System32\CodeIntegrity\ExamplePolicy.xml -Option 10
ConvertFrom-CIPolicy C:\Windows\System32\CodeIntegrity\ExamplePolicy.xml C:\Windows\System32\CodeIntegrity\ExamplePolicy.bin
```

7.2.2.10 Whitelist Merging Test

It is recommended to test all applications and subcomponents on the PCs that have been whitelisted. The event log should be monitored for WDAC events.

To add blocked files to the whitelist, a new policy based on the event log entries can be created. The **-Audit** option parses the log events of WDAC and automatically creates a policy file. An example looks as follows:

```
New-CIPolicy -Audit -Level Hash -Filepath c:\windows\system32\CodeIntegrity\Auditpolicy.xml -UserPEs 3>
CIPolicylog.txt
```

Afterwards, the new policy must be merged with the original xml policy and then converted into a binary file.

```
New-CIPolicy -Level Publisher -Fallback Hash -Scanpath C:\Program Files (x86)\Siemens Energy\ -Filepath
C:\Windows\System32\CodeIntegrity\UpdatePolicy1.xml -UserPEs 3> CIPolicyLog.txt
New-CIPolicy -Level Publisher -Fallback Hash -Scanpath C:\Siemens\ -Filepath C:\Windows\System32\Codein-
tegrity\UpdatePolicy2.xml -UserPEs 3> CIPolicyLog.txt
$CIPolicyPath="C:\Windows\System32\CodeIntegrity\"
$InitialCIPolicy=$CIPolicyPath+"ExamplePolicy.xml"
$updateCIPolicy1=$CIPolicyPath+"UpdatePolicy1.xml"
$updateCIPolicy2=$CIPolicyPath+"UpdatePolicy2.xml"
$MergedCIPolicy=$CIPolicyPath+"MergedPolicy.xml"
$CIPolicyBin=$CIPolicyPaht+"Mergedpolicy.bin"
Merge-CIPolicy -PolicyPaths $InitialCIPolicy,$updateCIPolicy1,$updateCIPolicy2-OutputFilePath $MergedCIPo-
licy
Set-RuleOption -FilePath C:\Windows\System32\CodeIntegrity\MergedPolicy.xml -option 3 -delete
ConvertFrom-CIPolicy $MergedCIPolicy $CIPolicyBin
```



NOTE

The application whitelisting would work only if WDAC runs in Windows user mode. Also, the PowerShell constrained Language mode shall be used to limit unconstrained code execution on a locked-down system.

7.2.2.11 Configuration Details of Policies

Rule Options

There are many rule options for code integrity policies. The rule options are the basic settings for a policy.

Table 7-2 Configuration Details of Policies

Rule Option	Description
0 Enabled:UMCI	WDAC policies restrict both kernel-mode and user-mode binaries. By default, only kernel-mode binaries are restricted. Enabling this rule option validates user-mode executables and scripts.
1 Enabled:Boot Menu Protection	This option is currently not supported.

Rule Option		Description
2	Required:WHQL	By default, legacy drivers that are not Windows Hardware Quality Labs (WHQL) signed can execute. Enabling this rule requires that every executed driver is WHQL signed and removes legacy driver support. Going forward, every new Windows 10-compatible driver must be WHQL certified.
3	Enabled:Audit Mode (Default)	Enables the execution of binaries outside of the WDAC policy but logs each occurrence in the CodeIntegrity event log, which can be used to update the existing policy before enforcement. To begin enforcing a WDAC policy, delete this option.
4	Disabled:Flight Signing	If enabled, WDAC policies will not trust flightroot-signed binaries. This would be used in the scenario in which organizations only want to run released binaries, not flighted builds.
5	Enabled:Inherit Default Policy	This option is currently not supported.
6	Enabled:Unsigned System Integrity Policy (Default)	Allows the policy to remain unsigned. When this option is removed, the policy must be signed and have UpdatePolicySigners added to the policy to enable future policy modifications.
7	Allowed:Debug Policy Augmented	This option is currently not supported.
8	Required:EV Signers	In addition to being WHQL signed, this rule requires that drivers must have been submitted by a partner that has an Extended Verification (EV) certificate. All future Windows 10 and later drivers will meet this requirement.
9	Enabled:Advanced Boot Options Menu	The F8 preboot menu is disabled by default for all WDAC policies. Setting this rule option allows the F8 menu to appear to physically present users.
10	Enabled:Boot Audit on Failure	Used when the WDAC policy is in enforcement mode. When a driver fails during startup, the WDAC policy will be placed in audit mode so that Windows will load. Administrators can validate the reason for the failure in the CodeIntegrity event log.
11	Disabled:Script Enforcement	This option is currently not supported.
12	Required:Enforce Store Applications	If this rule option is enabled, WDAC policies will also apply to Universal Windows applications.
13	Enabled:Managed Installer	Use this option to automatically allow applications installed by a software distribution solution, such as System Center Configuration Manager, that has been defined as a managed installer.
14	Enabled:Intelligent Security Graph Authorization	Use this option to automatically allow applications with known good reputation as defined by Microsoft's Intelligent Security Graph (ISG).
15	Enabled:Invalidate EAs on Reboot	When the Intelligent Security Graph option (14) is used, WDAC sets an extended file attribute that indicates that the file was authorized to run. This option will cause WDAC to periodically revalidate the reputation for files that were authorized by the ISG.
16	Enabled:Update Policy No Reboot	Use this option to allow future WDAC policy updates to apply without requiring a system reboot.

File Rules

The granularity with which binaries are discovered is based on the file-rule level specified when the policy is created.

Table 7-3 File Rules

Rule Level	Description
Hash	Specifies individual hash values for each discovered binary. Although this level is specific, it can cause additional administrative overhead to maintain the current product versions' hash values. Each time a binary is updated, the hash value changes, therefore requiring a policy update.
FileName	Specifies individual binary file names. Although the hash values for an application are modified when updated, the file names are typically not. This offers less specific security than the hash level but does not typically require a policy update when any binary is modified.
SignedVersion	This combines the publisher rule with a version number. This option allows anything from the specified publisher, with a version at or above the specified version number, to run.
Publisher	This is a combination of the PcaCertificate level (typically one certificate below the root) and the common name (CN) of the leaf certificate. This rule level allows organizations to trust a certificate from a major CA (such as Symantec), but only if the leaf certificate is from a specific company (such as Intel, for device drivers).
FilePublisher	This is a combination of the FileName attribute of the signed file, plus Publisher (PCA certificate with CN of leaf), plus a minimum version number. This option trusts specific files from the specified publisher, with a version at or above the specified version number.
LeafCertificate	Adds trusted signers at the individual signing certificate level. The benefit of using this level versus the individual hash level is that new versions of the product will have different hash values but typically the same signing certificate. Using this level, no policy update would be needed to run the new version of the application. However, leaf certificates have much shorter validity periods than CA certificates, so additional administrative overhead is associated with updating the WDAC policy when these certificates expire.
PcaCertificate	Adds the highest available certificate in the provided certificate chain to signers. This is typically one certificate below the root certificate, because the scan does not validate anything beyond the certificates included in the provided signature (it does not go online or check local root stores).
RootCertificate	Currently unsupported.
WHQL	Trusts binaries if they have been validated and signed by WHQL. This is primarily for kernel binaries.
WHQLPublisher	This is a combination of the WHQL and the CN on the leaf certificate and is primarily for kernel binaries.
WHQLFilePublisher	Specifies that the binaries are validated and signed by WHQL, with a specific publisher (WHQLPublisher), and that the binary is the specified version or newer. This is primarily for kernel binaries.



NOTE

Recommendation for file rules:

Use the **Publisher** rule as default and the **Hash** rule as backup, so that updates of applications with known publishers are allowed (files need to be signed by publisher e.g. Siemens).

Files using the **Hash** rule cannot be updated without using catalog file or updating the policy.

7.2.2.12 WDAC Audit Mode

The WDAC audit mode enables the discovery of policy issues. It allows administrators to discover applications that were missed during initial policy scan and to identify new applications that have been installed and run after the original policy was created. While a WDAC policy is running in audit mode, any binary that runs and would have been denied had the policy been enforced is logged in the Applications and Services Logs\Microsoft\Windows\CodeIntegrity\Operational event log. When these logged binaries have been validated, they can easily be added to a new WDAC policy. When the new exception (audit) policy is created, it can be merged with existing WDAC policies. The process of auditing and merging policies is recommended by Microsoft to be done at least twice to ensure that all the exceptions to the policy are captured.

- ✧ Create a new WDAC policy based on the event logs with the following PowerShell command:
New-CIPolicy -Audit -Level Hash -FilePath c:\windows\system32\CodeIntegrity\Auditpolicy.xml -UserPEs 3> CIPolicylog.txt
- ✧ Review the WDAC audit policy xml file just created and look for the following:
Any applications that were caught as exceptions but should be allowed to run. These are applications that should be in the .xml file. Leave these as-is in the file.
Any applications that should not be allowed to run. Delete these from the .xml file.
- ✧ Merge initial policy or latest policy (xml) with the new audit policy (xml).

7.2.2.13 Signing of a WDAC Policy – Protection Against Tampering (Optional)

Signed code integrity policies give organizations the highest level of malware protection available in Windows 10. In addition to their enforced policy rules, no user or administrator on the machine can modify or delete signed policies. These policies are designed to prevent administrative tampering and kernel mode exploit access. It is much more difficult to remove signed code integrity policies than unsigned policies.

7.2.2.14 Prerequisites

To sign a WDAC policy with SignTool.exe, the following components are needed:

- SignTool.exe, found in the Windows SDK
- The binary format of the WDAC policy
- An internal CA code signing certificate or a purchased code signing certificate

To sign catalog files or code integrity policies internally, either a publicly issued code signing certificate or an internal certification authority (CA) are needed.

Steps to sign a policy:

- ✧ 1 # Initialize the variables that will be used
2 \$CIPolicyPath="C:\Windows\System\CodeIntegrity\
3 \$InitialCIPolicy=\$CIPolicyPath+"ExamplePolicy.xml"
4 \$CIPolicyBin=\$CIPolicyPath+" ExamplePolicy.bin"
- ✧ Import the .pfx code signing certificate. Import the code signing certificate to sign the WDAC policy into the signing user's personal store on the computer that will be signing it.
- ✧ Export the .cer code signing certificate. After the code signing certificate has been imported, export the .cer version to desktop. This version will be added to the policy so that it can be updated later.
- ✧ Navigate to working directory:
cd C:\Windows\System\CodeIntegrity\
✧ Use the Add-SignerRule to add an update signer certificate to the WDAC policy:
1 # Add an update signer certificate to policy
2 Add-SignerRule -FilePath \$InitialCIPolicy -CertificatePath <Path to exported .cer certificate> -Kernel -User -Update
- ✧ Use Set-RuleOption to remove the unsigned policy rule option:
1 # Remove unsigned policy rule option
2 Set-RuleOption -FilePath \$InitialCIPolicy -Option 6 -Delete

- ✧ Use ConvertFrom-CIPolicy to convert the policy to binary format:
 - 1 # Convert policy
 - 2 ConvertFrom-CIPolicy \$InitialCIPolicy \$CIPolicyBin
- ✧ Sign the WDAC policy by using SignTool.exe:
 - 1 # Sign the policy
 - 2 <Path to signtool.exe> sign -v /n "CERT_SUBJECT_NAME" -p7 . -p7co 1.3.6.1.4.1.311.79.1 -fd sha256 \$CIPolicyBin



NOTE

The <Path to signtool.exe> variable should be the full path to the SignTool.exe utility.

- ✧ Validate the signed file. When complete, the commands should output a signed policy file called DeviceGuardPolicy.bin.p7 to your desktop. You can deploy this file the same way you deploy an enforced or non-enforced policy.

7.2.2.15 Known Issues

Unsigned Files Are Created By Applications

Some parts in applications create unsigned .dll files when the application is executed (e.g. the PASOperations client application which is part of SICAM PAS and some subsets of SICAM SCC). To resolve this issue, all parts of the application should be executed once, before creating a new whitelist. Alternatively, WDAC can be set to the audit mode after an application update before enforcing the policy.

Files That Cannot Be Added to the Whitelist

In some cases, when the whitelist is created via the New-Cipolicy command, an error message might appear that not all files are added to the whitelist. The error message will look as follows. The concerned files are listed in the indicated .tmp file. So far, no files that are critical for operation have been concerned.

```
"Unable to generate rules for all scanned files at the requested level. A list of files not covered by the current policy can be found at C:\Users\admin1\AppData\Local\Temp\tmpA470.tmp. If it is safe to not include these files, no action needs to be taken, otherwise a more complete policy may be created using the -fallback switch"
```

[sc_Error for file that cannot be added to whitelist, 1, en_US]

Figure 7-14 Error for File That Cannot be Added to Whitelist

Erroneous Behavior of WDAC if Windows Updates Are Not Installed

On Windows Systems running SICAM SCC on a fresh installation of Windows 10 LTSC 2019 without the latest Windows patches, erroneous behavior has been recognized (e.g. blocking applications without creating an event log entry). After installing the latest cumulative Windows Update, this problem is resolved.

7.2.3 Windows Defender Exploit Protection

The exploit protection feature of Windows helps to protect against memory-based attacks, where malware or other code manipulates memory to gain control of a system (for example, malware that attempts to use buffer overruns to inject malicious executable code into memory).

The exploit protection is part of Windows Defender Exploit Guard and helps to protect devices from malware that use exploits to spread and infect. It consists of several mitigations that can be applied at either the operating system level or at the individual application level.

It is the successor of the Enhanced Mitigation Experience Toolkit (EMET) and includes its features. EMET does not run on Windows 10, version 1709 or higher.

The following table describes the memory protection features of Windows 10. All of them are enabled by default.

Table 7-4 Memory Protection Feature in Windows 10 Defender

Mitigation and Corresponding Threat	Description
Data Execution Prevention (DEP) helps prevent exploitation of buffer overruns	Data Execution Prevention (DEP) is a system-level memory protection feature available in Windows operating systems. DEP enables the operating system to mark one or more pages of memory as non-executable, which prevents code from being run from that region of memory, to help prevent exploitation of buffer overruns. DEP helps prevent code from being run from data pages such as the default heap, stacks, and memory pools. Although some applications have compatibility problems with DEP, most applications do not. More information: Data Execution Prevention.
SEHOP helps prevent overwrites of the Structured Exception Handler	Structured Exception Handling Overwrite Protection (SEHOP) is designed to help block exploits that use the Structured Exception Handler (SEH) overwrite technique. Because this protection mechanism is provided at runtime, it helps to protect apps regardless of whether they have been compiled with the latest improvements. A few applications have compatibility problems with SEHOP, so be sure to test for your environment. More information: Structured Exception Handling Overwrite Protection.
ASLR helps mitigate malware attacks based on expected memory locations	Address Space Layout Randomization (ASLR) loads DLLs into random memory addresses at boot time. This helps mitigate malware that is designed to attack specific memory locations, where specific DLLs are expected to be loaded. More information: Address Space Layout Randomization.

The following mitigations shall be at least set to the operating system default values on system level:

- **Control flow guard (CFG):**
Ensures control flow integrity for indirect calls.
- **Data Execution Prevention (DEP):**
Prevents code from being run from data-only memory pages such as the heap and stacks.
- **Force randomization for images (Mandatory ASLR):**
Force relocation of images not compiled with /DYNAMICBASE.
- **Randomize memory allocations (Bottom-Up ASLR):**
Randomizes locations for virtual memory allocations including those for system structures heaps, stacks, TEBs, and PEBs.
- **High-entropy ASLR:**
Increase variability when using Randomize memory allocations (Bottom-up ASLR).
- **Validate exception chains (SEHOP):**
Ensures the integrity of an exception chain during exception dispatch.
- **Validate heap integrity:**
Terminates a process when heap corruption is detected.
- All settings above, except of **Mandatory ASLR** are turned on by default.

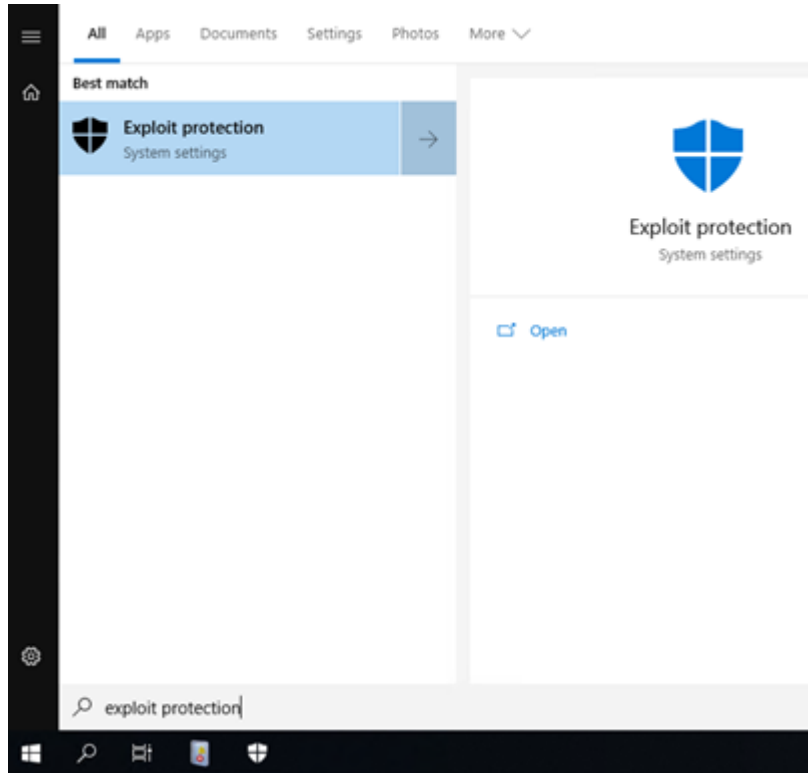
7.2.3.1 Exploit Protection Configuration

Local Configuration

- ✧ To open the settings for the Windows Defender Exploit Protection, click the **Windows** and type **exploit protection**. Then, click the **Exploit protection**.

- or -

✧ Navigate to **Windows Security** → **App and browser control** → **Exploit Protection settings**.



[sc_Selecting Exploit Protection, 1, en_US]

Figure 7-15 Selecting Exploit Protection

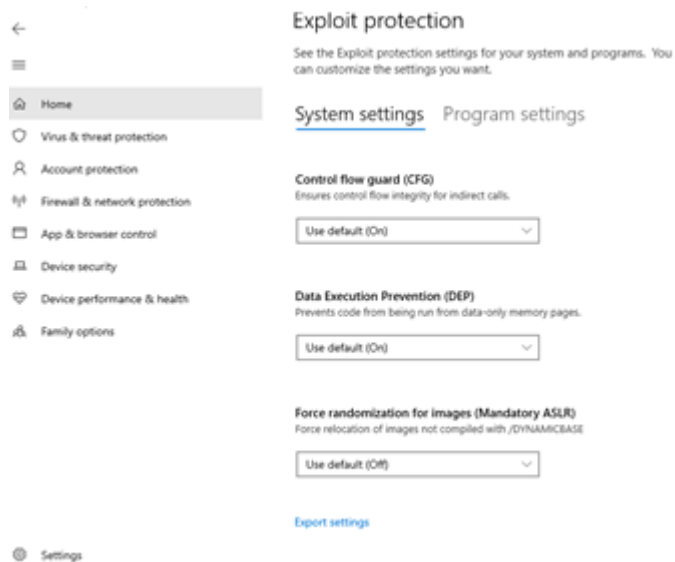
The **Exploit protection** interface contains 2 main sections:

- **System settings:**

Here the different protection mechanism can be turned on and off on a system-wide basis.

For the different mitigations, the GUI offers the values **On by default**, **Off by default**, and **Use default (<On>)** or **Use default (<Off>)** to be chosen. It is important that the meanings of **On by default** and **Use default (<On>)** are different. **On by default** has the meaning and effect of an **Always On** state in the OS, while **Use default (<On>)** has the meaning and effect of an **Application can OptOut of mitigation** state in the OS.

The **Exploit Protection** settings can also be exported into an .xml file.

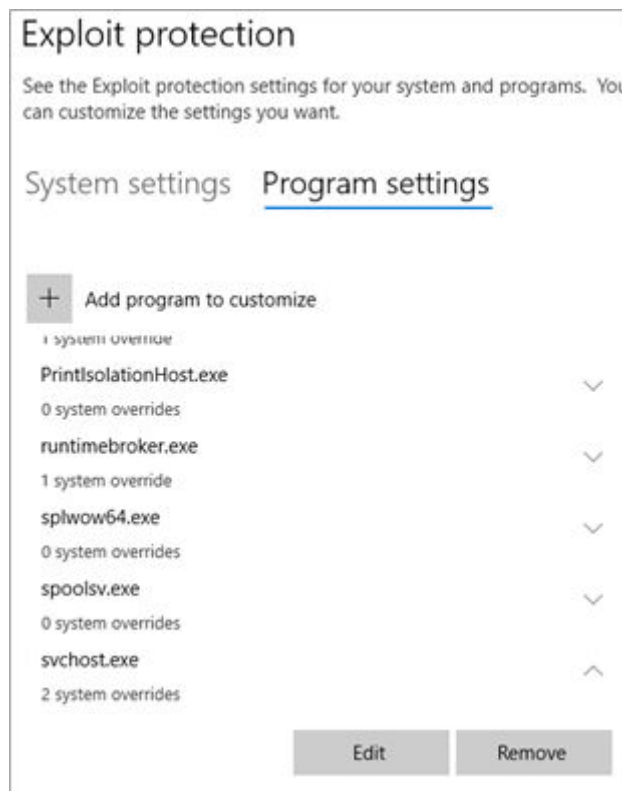


[sc_Exploit protection Settings, 1, en_US]

Figure 7-16 Exploit protection Settings

- **Program settings:**

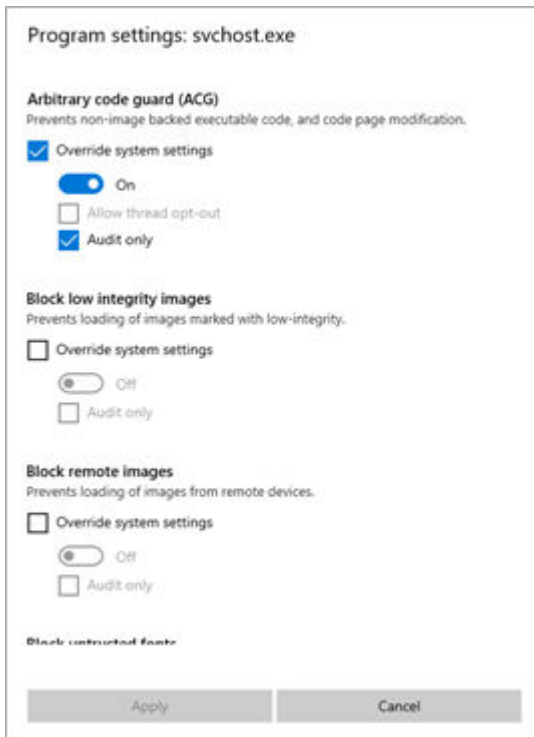
Here the exceptions are defined for certain executables. This may be necessary in case there are incompatibilities with the default settings. Some system files already have exceptions predefined in the default settings.



[sc_Exploit Protection program Settings, 1, en_US]

Figure 7-17 Exploit Protection Program Settings

A new executable can be added/edited to the program settings via the **Edit**. Certain protection mechanism can be turned on or off for each executable. This should only be done in case an incompatibility has been detected.



[sc_Program Settings svchost, 1, en_US]

Figure 7-18 Program Settings svchost

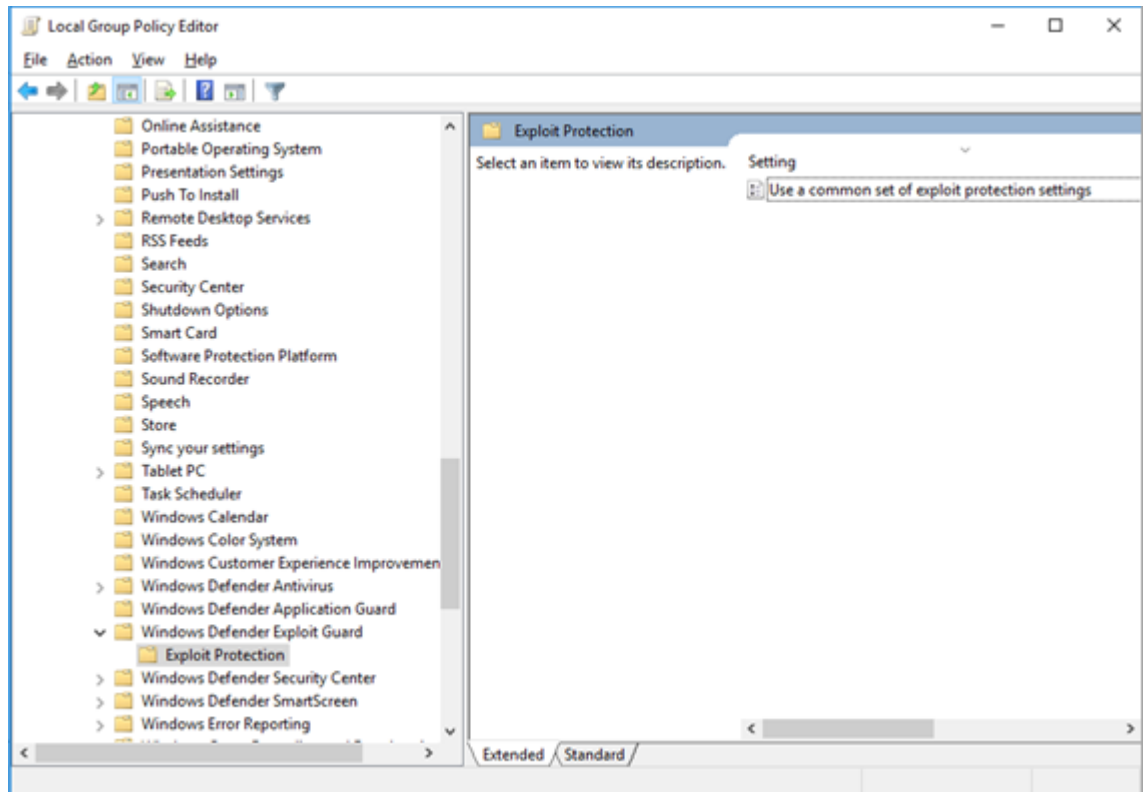
To reset the default all values of Windows Defender Exploit Protection on the PC, use the following PowerShell command:

```
Set-ProcessMitigation -System -Remove -Disable CFG,DEP,ForceRelocateImages,BottomUp,HighEntropy,SEHOP,TerminateOnError
```

Central Configuration

The configuration of the **Exploit Protection** settings via GPO may be required when the default settings are not used. An XML file must be used for this purpose. To get an xml file with the default settings, export the settings via the local dashboard.

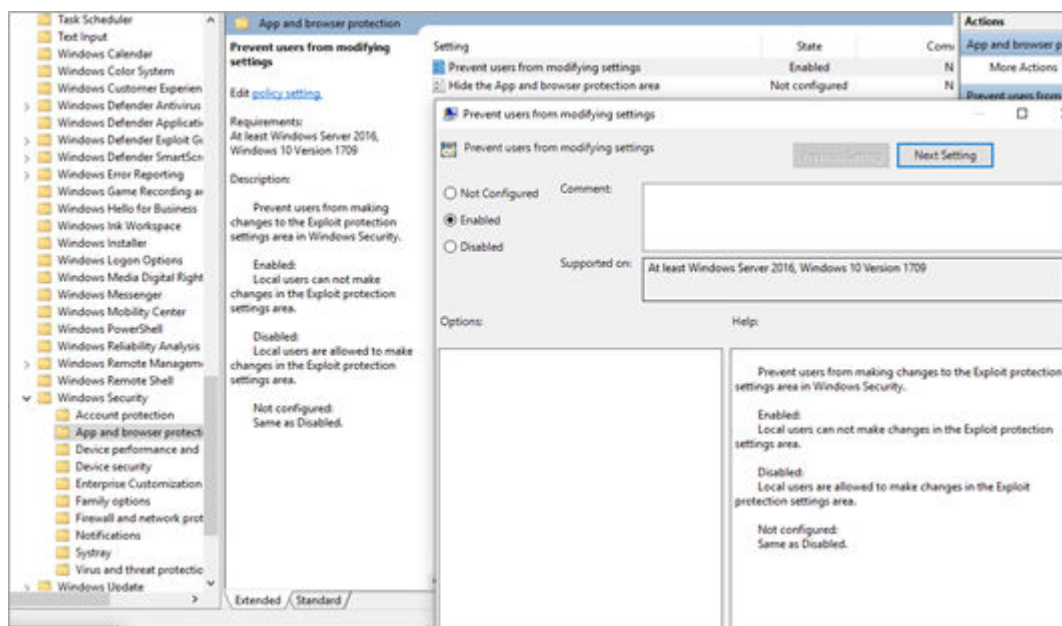
- ✧ In the **Group Policy Management Editor**, go to **Computer configuration** → **Administrative Templates** → **Windows Components** → **Windows Defender Exploit Guard** → **Exploit protection**.
- ✧ Enable the settings **Use a common set of exploit protection settings**.
- ✧ In the **Options** section, enter the location and filename of the xml configuration file that you want to use. (e.g. C:\MitigationSettings\Config.XML or \\Server\Share\Config.xml)



[sc_Central Configuration of Exploit Protection, 1, en_US]

Figure 7-19 Central Configuration of Exploit Protection

- ✧ To prevent local users to modify the exploit protection settings, set the following Group Policy setting to **Enabled**:
Computer Configuration\Administrative Templates\Windows Components\Windows Security\App and browser protection\Prevent users from modifying settings



[sc_Preventing Users from modifying Settings, 1, en_US]

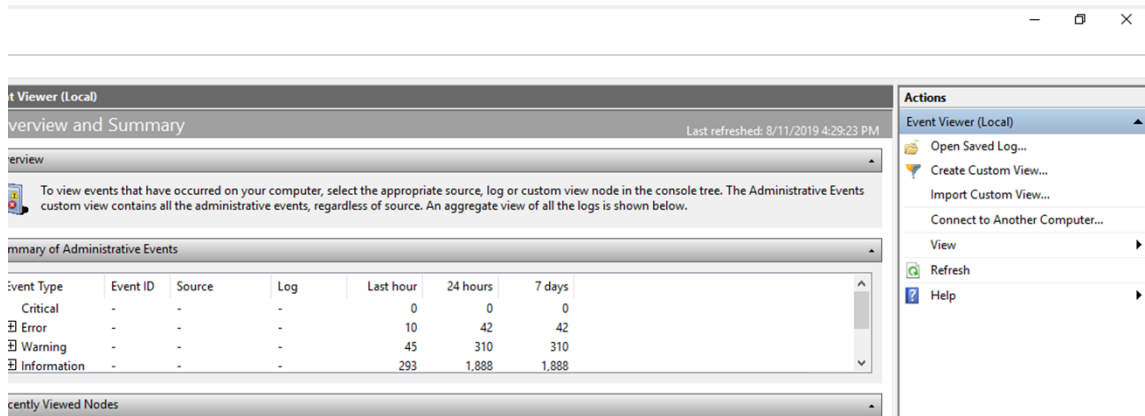
Figure 7-20 Preventing Users from Modifying Settings

This will enforce the default settings and prevent the modification by users.

Exploit Protection Event Logs

The Exploit Protection events are not located in a dedicated section in the Windows Event viewer. It is necessary to create custom view.

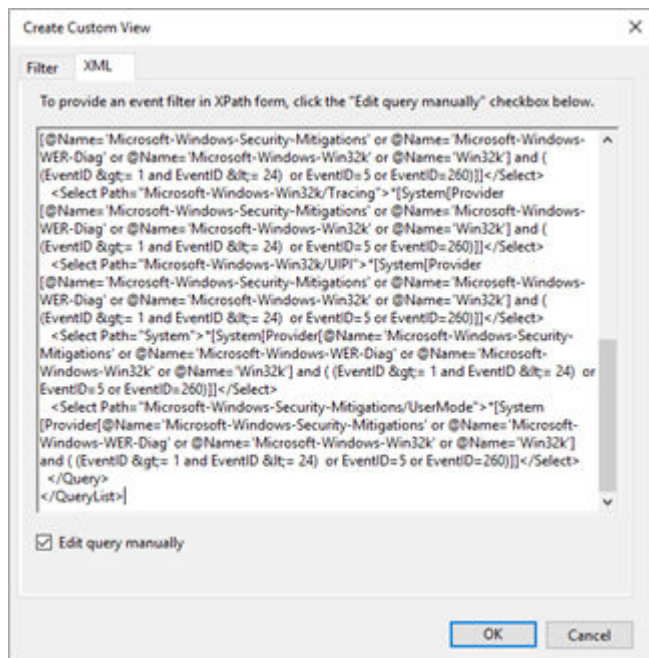
- ✦ Click **Action** → **Create Custom View**.



[sc_Exploit Protection Event Logs, 1, en_US]

Figure 7-21 Exploit Protection Event Logs

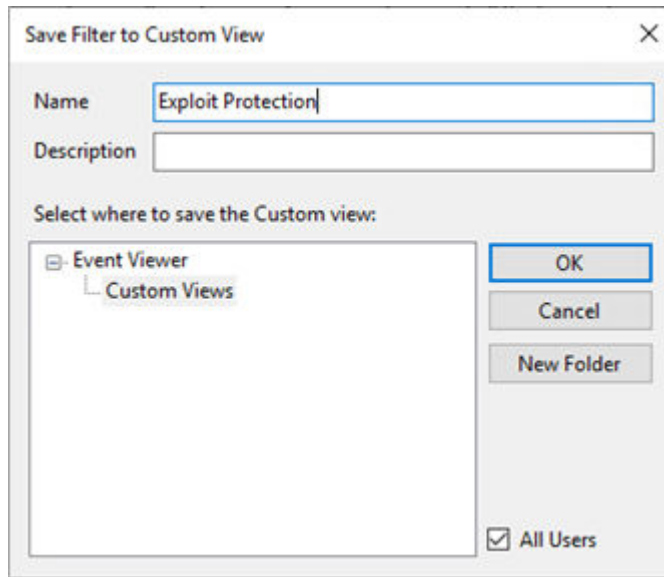
- ✦ Navigate to the **XML** tab, activate the checkbox **Edit query manually**, and copy the xml content from the textbox on the next side into the field:



[sc_XML for custom view, 1, en_US]

Figure 7-22 XML for Custom View

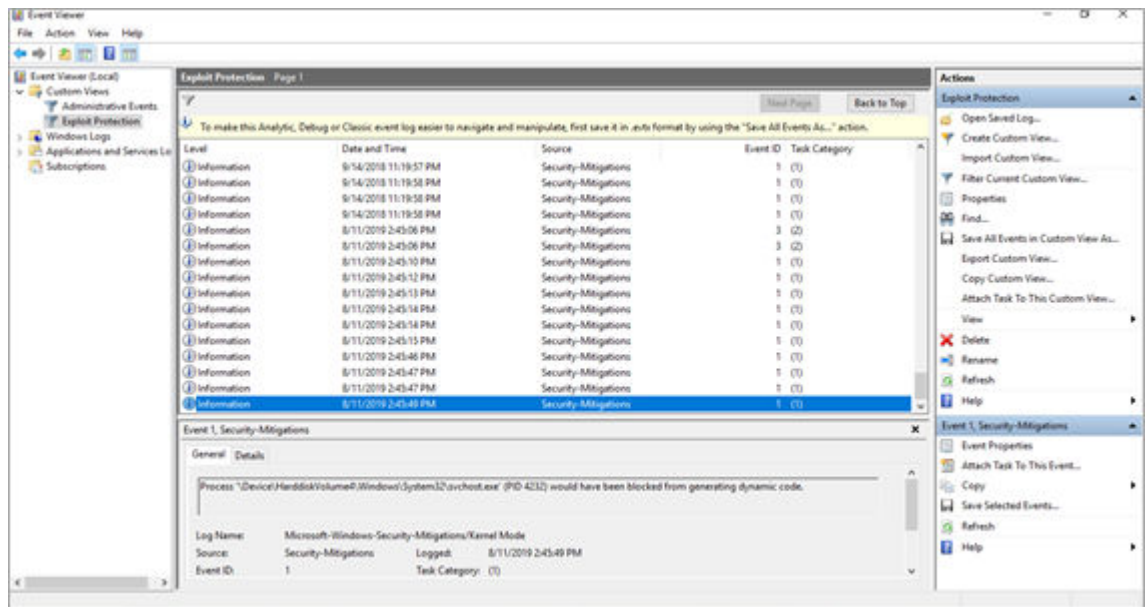
- ✦ Click **OK**.
- ✦ Save the new view with the Name **Exploit Protection**.



[sc_Saving Custom View in XML, 1, en_US]

Figure 7-23 Saving Custom View in XML

- ✧ If a warning is shown that you will not be able to edit the query using the **Filter** tab if you use the XML option, click **Yes**.



[sc_Resulting view of event viewer, 1, en_US]

Figure 7-24 Resulting View of Event Viewer

7.2.3.2 HW Requirements

Several hardware, software, and firmware features are required for the Exploit Protection feature. The state-of-the-art hardware will support the following features:

- Secure boot
- Secure boot configuration and management
- Secure firmware update process
- Trusted Platform Module (TPM)

- United Extensible Firmware Interface (UEFI)
- Virtualization-based security (VBS)

A detailed description of the requirements can be found here:

<https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-device-guard>

7.3 Malware Protection for Siemens Products

7.3.1 SICAM PAS Station Controller

The station controller is considered a highly critical component that must meet very strict availability and real-time requirements. Malware protection for such components is important. However, frequent software updates as required for common virus-scanner software may conflict with the availability and real-time requirements.

Hence, for SICAM PAS station controllers as fixed-function devices, the use of whitelisting software instead of virus-scanner software should be considered. The Windows Defender Application Control Whitelisting solution has been tested for SICAM PAS running on standard Windows OS.

However, Siemens has tested the use of Windows Defender Antivirus in conjunction with Windows Defender Application Control for SICAM PAS installed systems. Siemens also provides tested antivirus pattern for Windows Defender Antivirus.

7.3.2 SICAM SCC HMI PC

The same consideration as for SICAM PAS applies for SICAM SCC. Also, as a fixed-function device, the use of whitelisting is recommended for SICAM SCC. The tested whitelisting for Siemens Automation products is Windows Defender Application Control.

Siemens has tested the use of Windows Defender Antivirus in conjunction with the Windows Defender Application Control for SICAM SCC installed systems. Siemens also provides tested antivirus pattern for Windows Defender Antivirus

7.3.3 SICAM A8000 Series/SICAM RTUs

The SICAM A8000 series/SICAM RTUs components are self-developed Embedded Systems, for which no known viruses exist. The products are developed with self-signed firmware. Therefore, no protection software is available for these systems. In addition, the components are hardened before commissioning, to achieve increased protection against possible malicious software.

Also, it is recommended that only Siemens signed firmware sourced from Siemens directly shall be used for updating and patching.

7.3.4 SIPROTEC 5/DIGSI 5 Devices

The SIPROTEC 5 devices are equipped with an internal firewall for protection against attacks over the network. To enhance the standard level of protection, the firewall is enabled by default and only digitally signed firmware files can be uploaded into SIPROTEC 5 devices. Secure signing is applied at Siemens production facilities with Siemens's internal PKI for products.

The PC-based engineering software application for SIPROTEC relays – DIGSI 5 – is installed using a signed installer to protect its integrity. Siemens regularly tests and reports the compatibility of new antivirus patterns with the latest DIGSI versions. These reports, which also include the results of the Microsoft Windows patch-compatibility verification, are available in the Internet monthly. Furthermore, every release of DIGSI 5 is tested against a multitude of antivirus scanners before delivery. The Windows Defender Application Control Whitelisting solution has been tested for DG engineering tools that run on the Service PC (e.g. DIGSI).

7.3.5 Service PC

Windows Defender (Windows 10) is recommended. Due to the non-critical nature of these machines and to the varying set of installed applications, explicit testing or approval of pattern updates does not generally apply (with exception of DG applications where tests are regularly executed to ensure functionality). If, based on the project-specific risk assessment, or based on customer request, such explicit testing is required, the recommended approach is to set up a second redundant system and perform rollout and testing of updates on the second system prior to rollout on the main systems.

The Windows Defender Application Control Whitelisting solution has been tested for DG engineering tools that run on the service PC (e.g. DIGSI).

7.4 Recommendations

File-Integrity Checks

Another preventive measure for malware protection is the implantation of integrity checks for software and firmware files. You can also verify the integrity of all SIPROTEC firmware and software files which are available for download on the Siemens-supported portal. For each downloadable firmware and software file, the corresponding SHA-256 fingerprint is published in the Internet.

Tools such as Certutil in Microsoft Windows can be used for the following purposes:

- Generate the SHA-256 fingerprint for the file you download.
- Check if the SHA-256 fingerprint is identical to the published fingerprint, that is verifying the file integrity.

8 Backup and Restore

8.1	General	225
8.2	Concept	226
8.3	Disaster Recovery	229
8.4	Backup Procedure for Siemens Products	235
8.5	SICAM SCC	239
8.6	Archiving of Engineering Tools	245

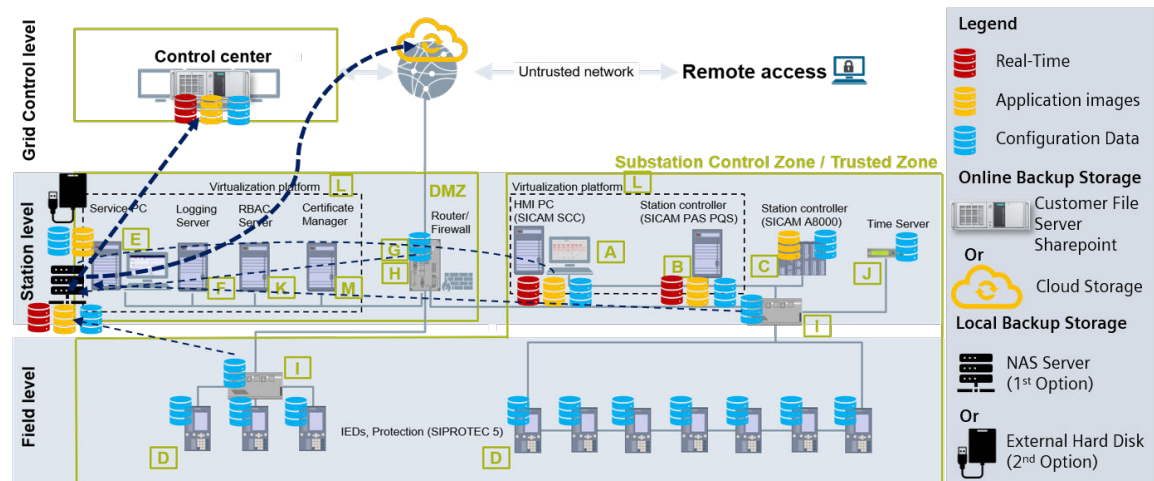
8.1 General

Backup and archiving serve different purposes. The goal of backup is reliable recovery, while the goal of archiving is data preservation. Backup solutions protect data by making a copy of the most recent volume and any incremental changes on secondary storage; this copy can later be recovered in the event of a planned or unplanned outage. Archiving helps reduce the backup burden by moving aged or infrequently accessed data from primary storage media to less expensive storage media, thus removing it from the backup stream.

The goal of this Backup & Restore manual for Digital Grid System is to describe:

- The activities (what and when backup) in the delivery and maintenance process (see [8.2 Concept](#))
- How to do backup application programs for PC systems (images)
- How to do backup configuration data for several products:
 - SICAM PAS
 - SICAM SCC
 - SIPROTEC
 - Switch/Router

8.1.1 Illustrated Concept



[sc_sas_backup_and_restore_1_en_US]

Figure 8-1 SAS Backup and Restore

8.1.2 Introductory Notes

Backup and restore is the process of copying data preemptively for the specific purpose of restoring that same data following an event that results in a loss of either hardware storing that data, or the loss of only the data itself. This process, also known as data backup and restore, can be used to restore entire volumes of electronic files and media, or restore discrete smaller numbers of files for a variety of purposes, including:

- Accidental deletion or corruption of data
- Hardware failure
- Facilities damage due to natural disasters, fire, or flooding
- Damage caused by cyber-attacks



NOTE

Backup and restore is not the same as data archival. Data archival refers to the process of storing primary copies of inactive or otherwise non-critical data, generally for longer-term storage.

Backup and restore is performed by transferring designated backup data to some type of storage media, including magnetic tape backup, disk-to-disk backup, or with a variety of removable media like USB drives. Disk-to-disk backup can be performed locally, called **local backup** (e.g. using a removable media or a NAS Server), or via IP-WAN called **online backup** (using operator's own infrastructure or some commercial of-the-shelf solutions like AWS S3 cloud storage). Modern disk-to-disk backup systems are increasingly fault-tolerant and while initially costing more than tape backup or removable media, offer higher restore success rates, dramatically reduced administration, improved data backup granularity, and other benefits.

Additionally, disk-to-disk backup and restore performed via IP-WAN allows an offsite data storage provider to ship drives containing recent backup data to customers in the event of a data loss event for a local restore, which can transfer data to new or existing hardware at LAN speeds without being restricted by IP-WAN bandwidth.

More and more businesses are making the switch from standalone local backup solutions to online backup to manage their entire backup and restore processes, as value emphasis shifts from storage media costs to scalable savings achieved through streamlined administration and automation of backup and restore processes.

8.2 Concept

8.2.1 Overview

The backup depends on data types (what), backup schedule during the project phases (when) and must be performed to backup media (where). The document describes best practice recommendations and should be aligned with customer data restore recovery objectives.

8.2.2 Data Types (What)

Data types that must be considered for the backup and restore procedures are:

- Application programs itself (e.g.: firmware and operating system, installation files)
- Configuration data of the equipment (HMI drawings, substation controller logics, protection settings, Ethernet switch/router settings)
- Real-time/process data (e.g. event list, measurement, fault record files in HMI – workstation)

The following table illustrates the relation between the data types and the existing components from a substation automation system.

Table 8-1 Data Types and Backup Method

Data Type	Method of back-up	HMI (SICAM SCC)	Station Controller (SICAM PAS/ SICAM RTU)	IEDs (SIPROTEC)	Third Party (Switch/Router)
Application	Image for PC-based systems Firmware for dedicated Hardware Installation Files for engineering tools	Images	SICAM PAS → Images SICAM RTU → Firmware	Firmware managed with DIGSI	Dedicated hardware with firmware
Configuration	Dedicated engineering tools performing the backup of the configuration data	Based on SICAM SCC (Simatic WinCC Explorer)	Based on SICAM PAS UI config.	Based on DIGSI	Dedicated tools
Real-time	Storage media must be always available on HMI PCs	SICAM SCC archiving functionalities	N/A	N/A (real-time data and local fault-record files are stored in internal buffer but not for backup).	N/A

8.2.2.1 Archiving Real-Time Data

Only SICAM SCC has real-time data. The storage cycles of the real-time data are usually provided by the customer according to the information criticality and available space to keep it.

8.2.2.2 Archiving Firmware

For PC-based application in general, installation media are provided. These installation media could be used for restoring the installed version of an application or OS.

But, for embedded devices often the firmware is delivered only installed in the embedded devices without delivery of installation media. The upload of the firmware from the device is often not possible. So, it is part of the backup process to check the availability of the used firmware versions of embedded devices and make sure it is kept secure and will be available in case it is needed. For instance, in case of using a spare part of a device after a device failure, the same original firmware must be used. It must be guaranteed that the needed firmware version is available at this time.

8.2.3 Backup Schedule (When)

For all types of backup, the recommended locations are removable media and/or online storage.

Table 8-2 Backup Schedule for Different Products

Product	Data Type	Schedule/Milestone
SICAM PAS/SICAM SCC and Service PC	Application data Full backup Image for PC-based systems	At important milestones: Before and after FAT, SAT, and important software updates During commissioning, operation & maintenance: monthly
Switches/Routers/NTP Server and SIPROTEC	Application data Firmware for dedicated hardware	At important milestones: Before and after FAT, SAT, and important software updates During commissioning, operation & maintenance: monthly
SICAM PAS (UI Configuration)/SICAM SCC (Editor)/Toolbox/ DIGSI and RuggedExplorer	Application data Archiving of tools	After commissioning
SICAM PAS/SICAM SCC/ DIGSI/Toolbox Switches/ Routers/NTP Server	Configuration data Project databases	During FAT, SAT, configuration & commissioning: daily
SICAM SCC	Real-time data	During FAT, SAT, configuration & commissioning: For archives with spontaneous and event-controlled scan, the storage cycle is set to 2 hours.

8.2.4 Backup Media (Where)

Images (application programs), approved configurations data, and real-time data should be stored on **external hard disks** or NAS Servers using a local storage concept. The next step for a more reliable backup solution is to implement in parallel an offsite online backup storage using the customers own file-server infrastructure or some online service.

8.2.4.1 Local Backup Storage Recommendation 1: Removable Media (External Hard Disks)

- An external hard drive can easily be attached to your computer using a USB port.
- External hard drives can hold lots of information. We recommend that you use an external hard drive that holds at least 1 terabyte (TB).
- Attention: The external hard drive needs to be plugged into your computer and available when a backup is scheduled to occur. If you store your hard drive somewhere else for safekeeping, you will need to remember to get it out and attach it to your computer before your backup is scheduled.
- Attention: Procedures for the control and management of removable backup media must be defined together with the customer on a project base.
 - Siemens recommends keeping more than one current copy of the backup media.
 - Store one copy at an off-site location in a properly controlled, secure environment.

NOTICE

The risk of virus infection is very high when you attach a removable media to your computer.

Nonconformance with the measures can result in property damage.

- ✧ Check some hardening configurations and recommendations for the operating system where the external hard drive will be attached.

8.2.4.2 Local Backup Storage Recommendation 2: NAS (Network-Attached Storage) Server

A NAS unit is a computer connected to a network that provides only file-based data storage services to other devices on the network which contains one or more hard disk drives, often arranged into logical, redundant storage containers or RAID.

- NAS provides access to files using network file sharing protocols such as:
 - NFS (popular on UNIX systems)
 - SMB/CIFS (Server Message Block/Common Internet File System)
 - AFP (used with Apple Macintosh computers)
- NAS is a convenient method of sharing files among multiple computers.
- Some benefits include:
 - Faster data access
 - Easier administration
 - Simple configuration
 - Vibration tolerance
 - Reliable data-blocks recovery and redundancy using RAID arrays

8.2.4.3 Online Backup Storage Recommendation 1: File System on Operate SharePoint

- Can hold lots of information
- Can be shared securely with the operator
- Inherent stored in a location that is separate from your computer, which can help protect your backup in a second place
- Attention: in the substation control room environment, access to the SharePoint is required (Internet/ Intranet connection point).

8.2.4.4 Online Backup Storage Recommendation 2: Online Cloud Services

- Can hold lots of information and have broad network access (Network available and access through standards mechanisms are guaranteed) and rapid elasticity (Computing capabilities can be elastically provisioned and released according to demand, this way companies only need to pay for the storage they use, being possible to expand anytime).
- The well-known online cloud storages solutions can be used as natural disaster proof backup, as normally there are 2 or 3 different backup servers located in different places around the globe.
- Storage availability, housekeeping (maintenance tasks), and data protection is intrinsic to object storage architecture, so depending on the application, the additional technology, effort, and cost to add availability and protection can be eliminated.
- It increases the number of networks over which the data travels, potentially increasing the attack surface area. Instead of just a local area network (LAN) or storage area network (SAN), data stored on a cloud requires a WAN (wide area network) to connect them both. The risk of having data read during transmission can be mitigated through encryption technology.
- Performance for outsourced storage is likely to be lower than local storage, depending on how much a customer is willing to spend for WAN bandwidth.

8.3 Disaster Recovery

Disaster recovery is the ability of the information and communication technology (ICT) elements of an organization to support its critical business functions to an acceptable level within a predetermined period following a disruption. [ISO/IEC 27031]

The following examples are part of a substation automation system:

- Protection relays/IEDs
- RTUs
- Substation Controller
- Local HMI
- Network equipment (e.g. switch, router)

The duties of the automation system are in general protection, monitoring, and control. In energy automation substations, the primary process is generally not actively controlled by the automation system. The primary process runs also in case the automation system is off.

A Disaster Recovery Plan (DRP) is part of the Business Continuity Planning (BCP) of the operator. A Business Continuity Planning is a proactive planning process that ensures critical services or products are delivered during a disruption.

A Business Continuity Plan includes:

- Plans, measures, and arrangements to ensure the continuous delivery of critical services and products, which permits the organization to recover its facility, data, and assets.
- Identification of necessary resources to support business continuity, including personnel, information, equipment, and infrastructure protection.

The objective of a DRP is to minimize downtime and data loss after a disruption. Disruptions are handled in 3 steps:

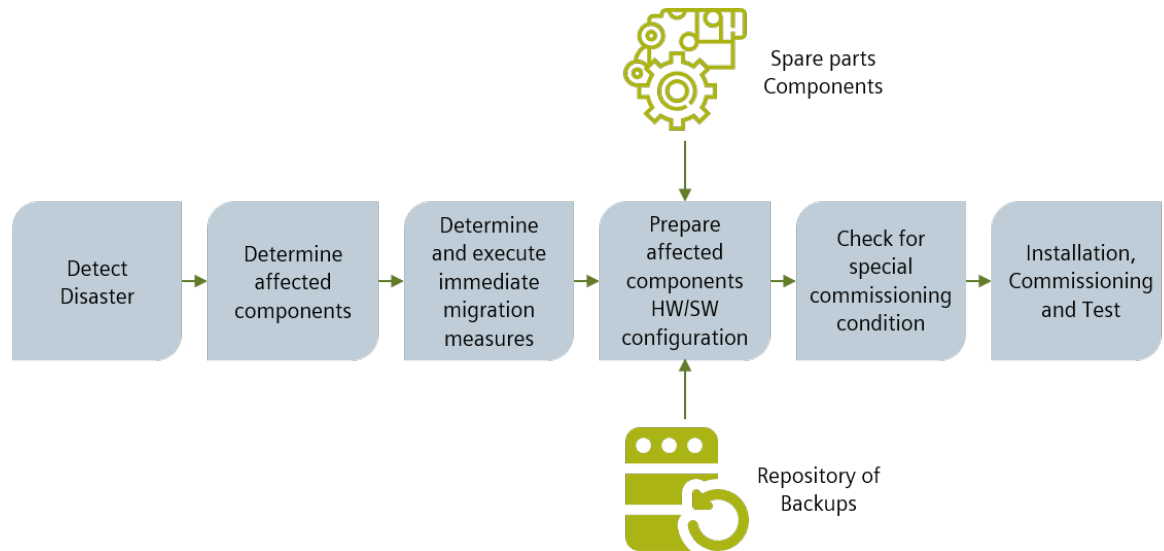
- Response
- Continuation of critical services
- Recovery and restoration

Incident response involves the deployment of teams, plans, measures, and arrangements to identify the range and scope of damage and rapidly assume control of the situation. It helps to ensure that all time-sensitive critical services or products are continuously delivered or not disrupted for longer than is permissible.

The dedicated disaster recovery plan is part of a dedicated project contract with the operator.

8.3.1 Recovery Process

The recovery process starts with the detection of a disaster. A disaster in general is one or more failed elements. An overview over the main process steps for the recovery is shown in the following figure.



[sc_Overview Recovery Process, 1, en_US]

Figure 8-2 Overview Recovery Process

The process starts with the detection of a disaster. Then follows the analysis of which components are affected. This process step includes the investigation of the reason of the disaster, which is an important input for the process step **Determine and execute immediate mitigation measures**.

For example, in case of a malware infection the isolation of the component could be an appropriate immediate mitigation measure. The next step **Prepare affected components** consists in the preparation of hardware and software of the affected components. The goal is to prepare a 100 % identical copy of the affected assets. That means the hardware, software, and configuration should be identical including the software-patch level.

For this purpose, the repository of backups is used. The **Check of special commissioning conditions** includes the investigation of impacts of the primary process or of the secondary process in case of the hot swap of each affected component. In general, the primary process runs independently from the secondary automation equipment. In general, also the automation process is robust in direction of the sequence of startup of single elements. In exceptional cases, those special conditions must be considered during **installation and commissioning**.

The process ends with a test of the complete system. The scope of the test depends on the type and number of replaced components.

8.3.2 Disaster Recovery Strategy

The disaster recovery strategy depends on the type of component and the type of failure. The following table contains typical disasters about the dedicated components. Other use cases can derive from this.

Table 8-3 Disaster Recovery Strategies Examples

Critical System	Threat	Response Strategy	Response Actions Steps	Recovery Strategy	Recovery Actions Steps
HMI with hardware redundancy (SICAM SCC)	Loss of hardware	Switch over to secondary HMI	Verify if primary HMI is down or isolated. Verify data has been backed up and is safe. Test secondary HMI. Start switch over to alternate HMI.	Fix/replace primary HMI. Fail back to primary HMI.	Verify cause of HMI outage. Contact repair resources. Fix HMI or use the preconfigured HMI spare part. Test new primary HMI. Fail systems back to primary HMI
HMI without hardware redundancy (SICAM SCC)	Loss of hardware	Operate the field equipment through IED	Temporarily adopt the procedure for local operation to the field equipment through IED.	Use the spare part to substitute the HMI	Use spare part HMI. Restore the last complete and trusted system backup. Connect the HMI to the network. Return to operate through HMI;

Critical System	Threat	Response Strategy	Response Actions Steps	Recovery Strategy	Recovery Actions Steps
Service PC	Malware	Isolate the infected system	Verify PC is isolated from network to stop the infection from spreading to other system;	Repair the infected system and reconnect it to the network.	<p>Ensure the latest virus definitions from antivirus software are installed.</p> <p>Ensure that anti-virus systems are configured to scan all files.</p> <p>Run a full system scan.</p> <p>Restore missing or corrupt data.</p> <p>Remove/clean infected files.</p> <p>If the malware was not found, restore the last complete and trusted system backup.</p> <p>Confirm that the computer systems are free of malware.</p> <p>Reconnect the cleaned computer systems to the network</p>
IED	Loss/defect of hardware	Isolate the IED from field equipment	<p>Verify that the IED is shut down. Ensure that IED is isolated and will have no influence on the field equipment.</p> <p>For the control IED, verify that is possible to operate the field equipment directly.</p> <p>For the protection IED, ensure that alternate protection is functional.</p>	Use the spare part to substitute the IED	<p>Use spare part IED (consider updating the hardware revision).</p> <p>Install the firmware, patches, and restore the configuration identical to the lost IED.</p> <p>Schedule a programmed intervention in the system to replace the defect IED.</p>

Critical System	Threat	Response Strategy	Response Actions Steps	Recovery Strategy	Recovery Actions Steps
Data Concentrator/Gateway (SICAM RTU / SICAM PAS)	Loss/defect of hardware	Isolate the gateway from other equipment, disconnecting all communications interfaces.	Verify that the Gateway is shut down. Ensure that the gateway is isolated and will have no influence on another equipment.	Use the spare part to substitute the hardware and use backup to restore to original configuration	Use spare part hardware and restore the configuration identical to the lost gateway using backup. Schedule a programmed intervention in the system to replace the defect gateway.
Network equipment (Switches, routers, NTP server)	Loss/defect of hardware	Isolate the device	Verify device is down or isolated	Use the spare part to substitute the device	Use spare part device (consider updating the hardware revision). Install the firmware, patches, and restore the configuration identical to the lost device. Schedule a programmed intervention in the system to replace the defect device.

As shown in the examples, having a critical-spare inventory is essential to handle the most of the smaller scale interruptions.

Up-to-date backups must be available to restore the last condition of each system component damaged. These backups should be kept in a secure location where they can be quickly obtained by authorized individuals when needed. It is a good practice to keep backups locally and in a shared external source.

It is suggested verifying and testing the backups when they are produced to ensure the data are usable and accurate.

A proactive approach that helps to handle disaster recovery situations is to use an architecture with redundant systems, avoiding single points-of-failure. In this way, it is possible to have a stable situation even in a degraded scenario with a reduced amount of healthy equipment.

Depending upon the magnitude of the damage inflicted by a particular incident, cybersecurity forensic specialists may need to be consulted for the following:

- To determine the root cause of the incident
- To evaluate the effectiveness of the response(s) taken
- In case of an intentional loss: to preserve the chain of evidence to support efforts to prosecute the perpetrator

It is very important that the damage be repaired as quickly as possible to restore the initial condition of redundancy to the system. And after the recovery phases are complete, response and update policies should be thoroughly reviewed and improved according to lessons learned.

8.3.3 Test Procedure

Prerequisite for a successful recovery is the use of the same hardware as for the backup. A spare PC should be available for every system (SICAM PAS, SICAM SCC, and Engineering PC) and the operator should have spare parts also for PLCs and IEDs.



NOTE

Virtualization can provide significant benefits for disaster recovery planning. Generally, it helps save money, time, and effort, and make the often-daunting task of designing and implementing a disaster recovery plan easier.

- Fewer physical servers needed at a disaster recovery site reduce one-time and ongoing costs, and results in less idle hardware.
- Hardware independence allows for more hardware options without compatibility issues.
- Encapsulation turns a VM into a single portable file for easier transport and deployment.
- Snapshots provide an effective method for backup and save reliable states of virtual machines.
- Automated failover and easier testing
- Easier server deployment: scripting can be used to help automate many configuration and operational tasks.

8.4 Backup Procedure for Siemens Products

8.4.1 IED SIPROTEC (with DIGSI)

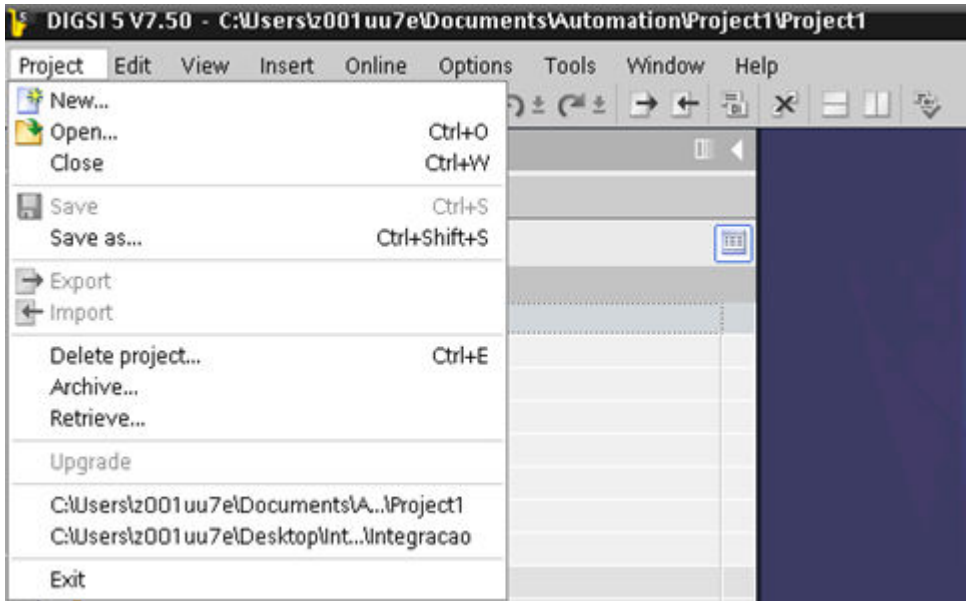
DIGSI 5 manages the components of a system and all the data associated with it in relation to the project. Projects are structured as folders in Windows. You can find the project folders under **My Files\Automation**. A folder with the name of the project is created for each project.

8.4.1.1 Archiving/Retrieving a Project

To save a project as a backup file and retrieve it later, you can archive the project created in DIGSI with the same name or any another name in the desired location. Further, after archiving any current opened project in DIGSI, you can continue working on the project without closing it. At any point of time, you can always retrieve the archived version of the project and start working on it, if required.

Archiving a Project

- ◇ In the **Project** menu, click **Archive**.

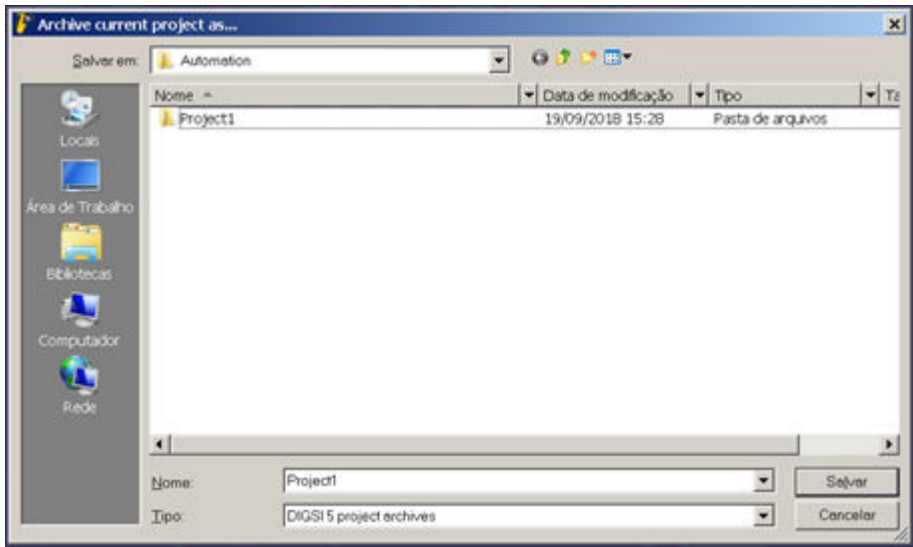


[sc_Archiving a project in DIGSI5, 1, en_US]

Figure 8-3 Archiving a Project in DIGSI 5

The **Archive current project as...** dialog opens with the default **File name**.

- ✧ Select the desired project folder from the **Save in** list box.
- ✧ Enter the new project name in the **File name** text box, if required.
- ✧ Click **Save**.



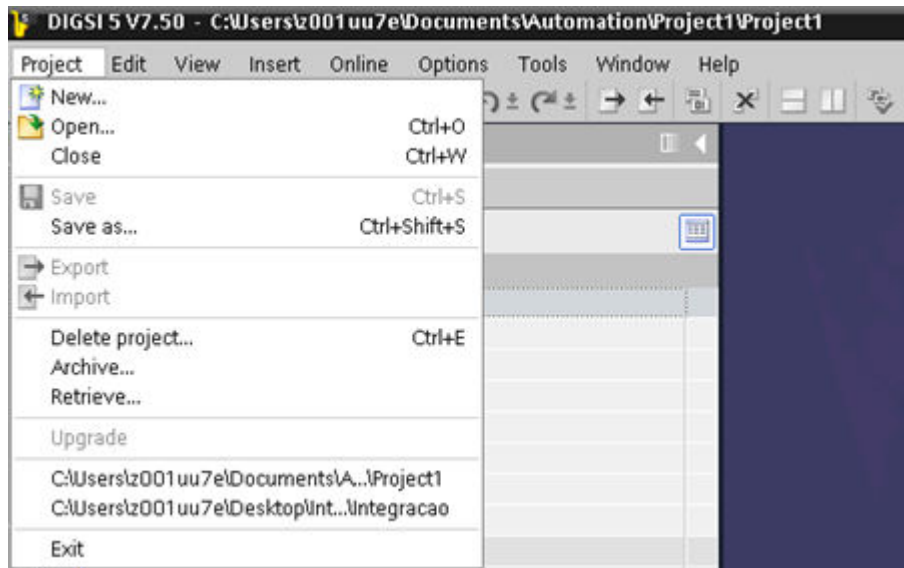
[sc_Selecting a project to archive, 1, en_US]

Figure 8-4 Selecting a Project to Archive

A progress dialog appears displaying the archive status and the archived project file is saved in the desired location with the file extension .dz5.

Retrieving an Archived Project

- ✧ In the **Project** menu, click **Retrieve**.



[sc_Retrieving an archived project, 1, en_US]

Figure 8-5 Retrieving an Archived Project

A confirmation prompt appears to confirm the retrieval.

✧ Click **Yes**.

The **Retrieve archived project** dialog opens.

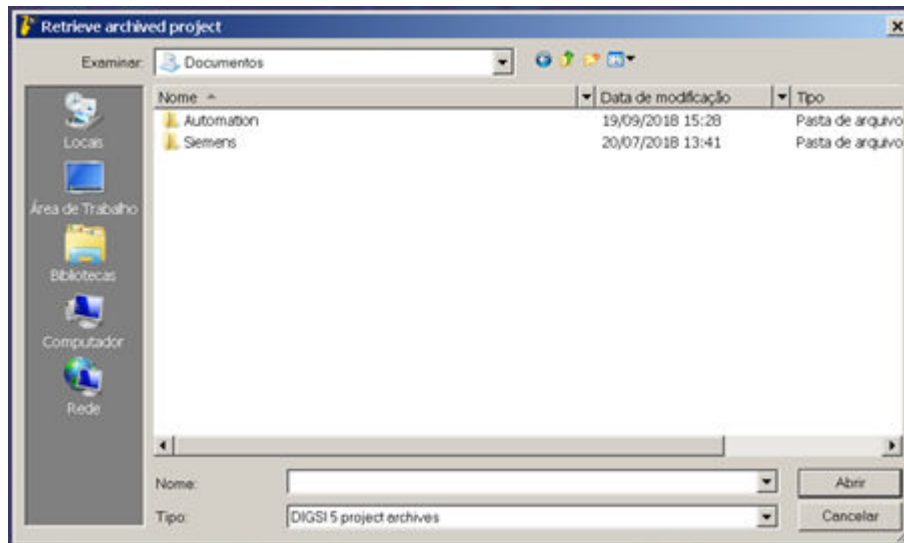
✧ Enter the new project name in the **File name** text box.

✧ Select the archived project with the file extension **.dz5** from the respective folder.

The file name is displayed in the **File name** text box.

✧ Click **Open**.

The **Browse for Folder** dialog opens.



[sc_Selecting target directory, 1, en_US]

Figure 8-6 Selecting Target Directory

✧ Select the target directory.

✧ Click **OK**.

A progress dialog appears displaying the project retrieval status and the retrieved project is displayed in the project tree.

8.4.2 SICAM PAS

8.4.2.1 Local Backup Storage Recommendation 2: NAS (Network-Attached Storage) Server

SICAM PAS/PQS saves your project's configuration data in a relational database in the (%PAS_APPDATA%\Data-base\pas.db) installation directory.

This project database is loaded and displayed by default. Any change in the current station configuration is automatically saved in this database.

Additionally, you can archive and load back your station's configuration. This creates the backup copies of your station configuration, e.g., before performing changes. If you configure a station offline on another computer, you can transfer this configuration to your station and unarchive and customize it afterwards. In a redundant system, you can archive and unarchive the configuration on a redundancy computer to transfer it.

On the project level, you can:

- Archive project data
- Unarchive project data
- Create a new database
- Create a new database from a template
- Compress a database

8.4.2.2 Archiving Project Data

Archive your database in the **Configuration** view. This menu item is disabled in all other views.

Proceed as follows:

- ✧ Select the **Configuration** view.
- ✧ Click **File** → **Archive** and select the directory in which you want to save the backup copy.
- ✧ Click **Save** to confirm.

The data is compressed as a *.ZIP file and saved in the selected directory. The ZIP file includes the database and log files and the ARCHIVES subdirectory.

8.4.2.3 Dearchiving Project Data



NOTE

When copying an archived project database, all communication links are interrupted and restarted automatically afterwards. SICAM PAS/PQS UI – Operation is exited.

When loading an archived project database, the current project is overwritten. You are prompted to confirm this step. Siemens recommends saving a backup copy of your current database before loading another project (**File** → **Archive...**).

When dearchiving the previously archived project database after an update of SICAM PAS/PQS, the database is also converted.

Proceed as follows:

- ✧ Click **File** → **Dearchive...** and navigate to the directory with the project database which you want to restore.
- ✧ Select the zipped project database and confirm with **Open**.

Some items of information stored in the unarchived configuration database must be customized for the new system, e.g., the IP addresses of the computer.

8.4.2.4 Dearchiving Large Project

For projects with a large data volume, you have the option to transfer the archived project data directly under Windows.

Proceed as follows:

- ✧ Stop the SICAM PAS/PQS runtime environment. To do this, click **Start** → **Run** → **cmd.exe** to open a console window and enter the net stop ssr command.
- ✧ In a Windows Explorer, open the %PAS_APPDATA%\Database folder of the SICAM PAS/PQS database. Delete or move the **Archives** folder and the **pas.db** and **pas.log** files.
- ✧ Unzip the zip file of the archived project to the SICAM PAS/PQS database folder.

The database folder must now contain the **pas.db** and **pas.log** files and, if required, the **Archives** folder again.

- ✧ Start the SICAM PAS/PQS runtime environment. Enter the net start ssr command in the console window.
- ✧ Enter the cd %PAS_BIN% and Changeloggenerator.exe commands in the console window.

The SICAM PAS/PQS runtime environment restarts with the dearchived project.

Alternatively, you can click **Update system** to restart the runtime environment in SICAM PAS/PQS UI – Operation.

8.5 SICAM SCC

8.5.1 Backup the SICAM SCC Database



NOTE

When archiving a database, all communication links are interrupted. The restart must be done manually. In case of a redundant system, the partner is still communicating to the process level.

Proceed as follows:

- ✧ Go to the SICAM SCC and stop the WinCC Runtime.
- ✧ Close the WinCC project and Explorer if open.
- ✧ Go to **Start** → **Run** and write **reset_wincc.vbs** and click **OK**.
- ✧ After you get a message box, confirm and open the Windows explorer and zip WinCC project folder, e.g., D:/WinCC.
- ✧ Save all backups on a centralized drive to avoid discrepancy problems.
- ✧ After archiving, restart the PC. If autostart for WinCC is not activated, start the WinCC explorer and activate the project manually.

8.5.2 Restore the SICAM SCC Database



NOTE

When archiving a database, all communication links are interrupted. The restart must be done manually. In case of a redundant system, the partner is still communicating to the process level.

Proceed as follows:

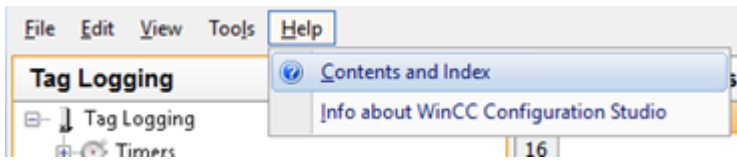
- ✧ Go to the SICAM SCC and stop the WinCC Runtime.
- ✧ Close the WinCC project and Explorer if open.
- ✧ Go to **Start** → **Run** and write **reset_wincc.vbs** and click **OK**.

- ✧ After you get a message box, confirm and open the Windows explorer.
- ✧ Move the folder where you have your project folder, e.g., D:\WinCC to D:\temp\WinCC.
- ✧ Unzip the new backup in the place where project is normally located, e.g., D:\.
- ✧ After unarchiving, restart the PC. If autostart for WinCC is not activated, start the WinCC explorer and activate the project manually.

8.5.3 Backup SICAM SCC Real-Time Data

SIMATIC WinCC, the basis platform for SICAM SCC, uses SQL segments to store and archive the alarm logging and tag logging data. These 2 services need to be configured to export the data automatically to a Windows directory.

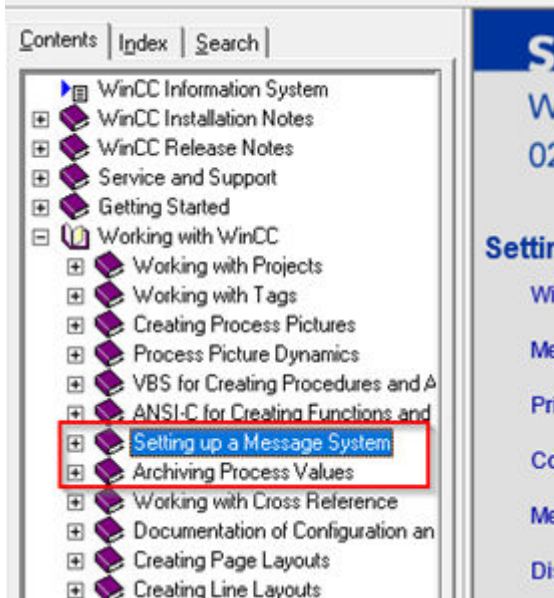
The process of creating individual messages or individual tags to be stored according to a specific cycle or event will not be demonstrated in the document, as well as the criteria on how to set up an archive. Therefore, for more information regarding on how to set up alarm logging or tag logging and how to set up archives, refer to **SIMATIC WinCC Help → Contents and Index**.



[sc_Backup up SICAM SCC data, 1, en_US]

Figure 8-7 Backing Up SICAM SCC Data

In the **Help** window under the **Contents** tab, refer to **Working with WinCC → Archiving Process Values** or **Working with WinCC → Setting up a Message System**.



[sc_Selecting Setting up a Message System, 1, en_US]

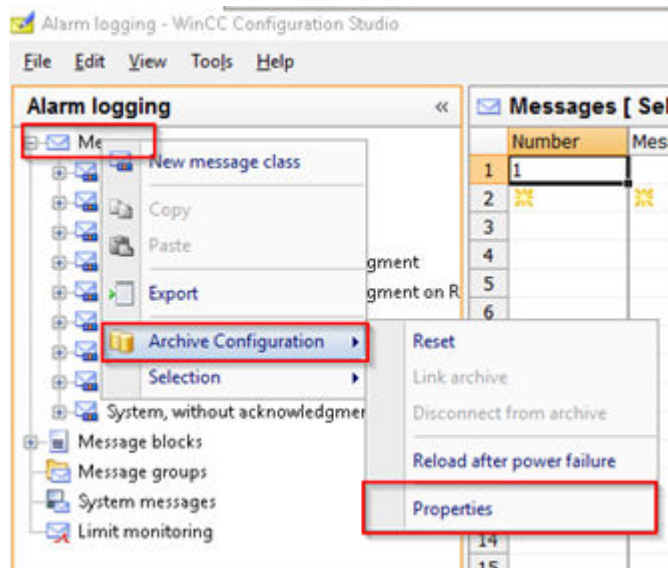
Figure 8-8 Selecting Setting up a Message System

8.5.4 Alarm Logging Archive Backup

To enable the Alarm Logging Archive Backup, proceed as follows:

- ✧ Go to **Alarm Logging**.

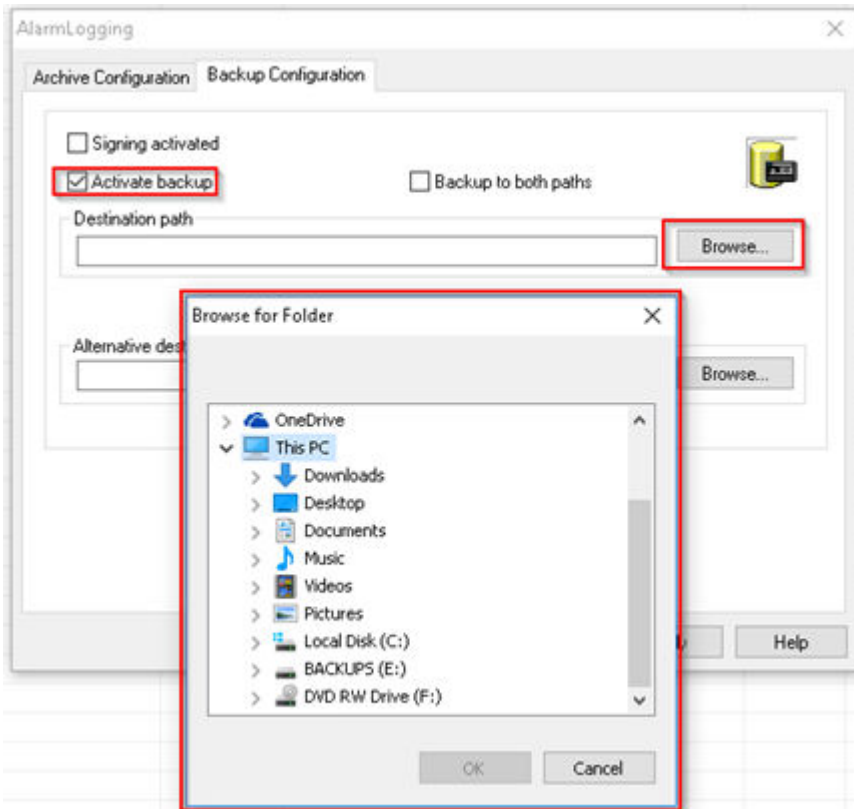
- ◇ Right-click **Messages** and select **Archive Configuration** → **Properties**.



[sc: Archive Configuration Properties, 1, en_US]

Figure 8-9 Archive Configuration Properties

- ◇ In the **Backup Configuration** tab, check the **Activate Backup** option.
- ◇ Click **Browse...**
- ◇ Choose the desired destination directory in the **Browse for Folder** window.
- ◇ If a backup destination path is needed, the option **Backup to both paths** needs to be checked.
- ◇ After selecting the destination folder, click **OK**.



[sc_Selecting Archive Backup Location, 1, en_US]

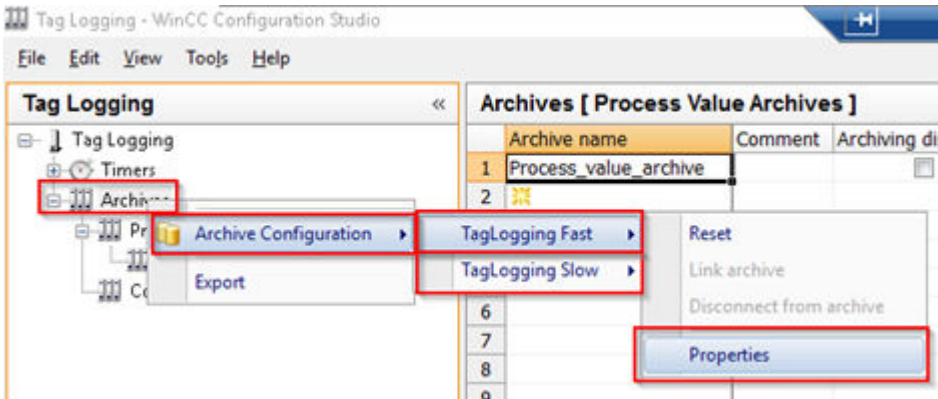
Figure 8-10 Selecting Archive Backup Location

- ✧ Restart the project runtime.

8.5.5 Tag Logging Archive Backup

To enable the Tag Logging Archive Backup, proceed as follows:

- ✧ Go to **Tag Logging**.
- ✧ Right-click **Archives** and select **Tag Logging Fast** or **Tag Logging Slow** → **Properties**.

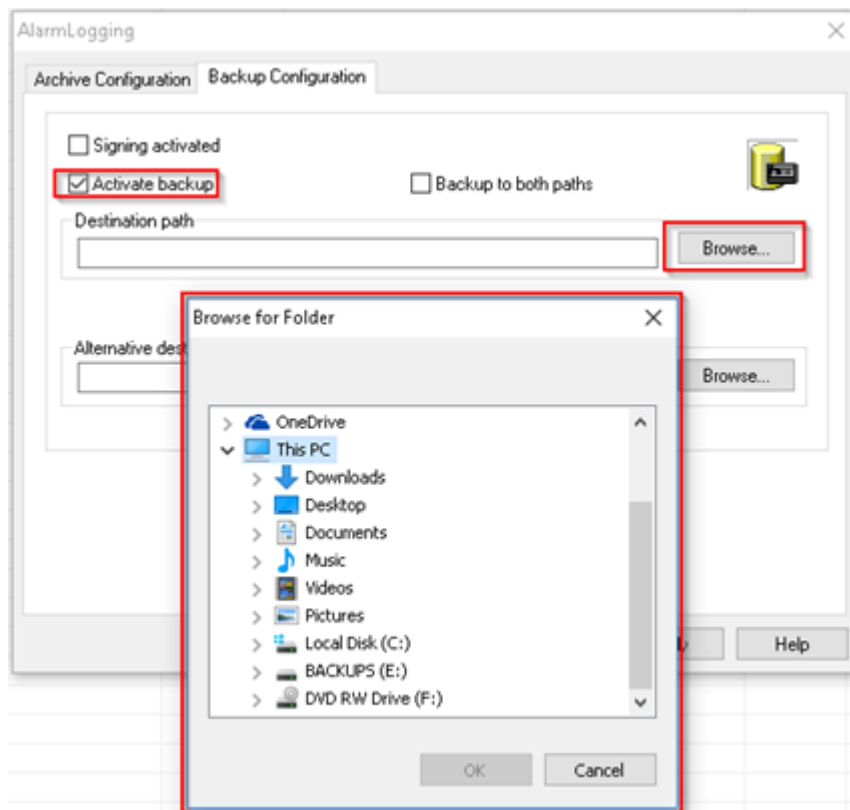


[sc_Tag Logging, 1, en_US]

Figure 8-11 Tag Logging

- ✧ In the **Backup Configuration** tab, check the **Activate Backup** option.
- ✧ Click **Browse....**

- ✧ Choose the desired destination directory in the **Browse for Folder** window.
- ✧ If a backup destination path is needed, the option **Backup to both paths** needs to be checked.
- ✧ After selecting the destination folder, click **OK**.



[sc_Selecting Location for Tag Logging, 1, en_US]

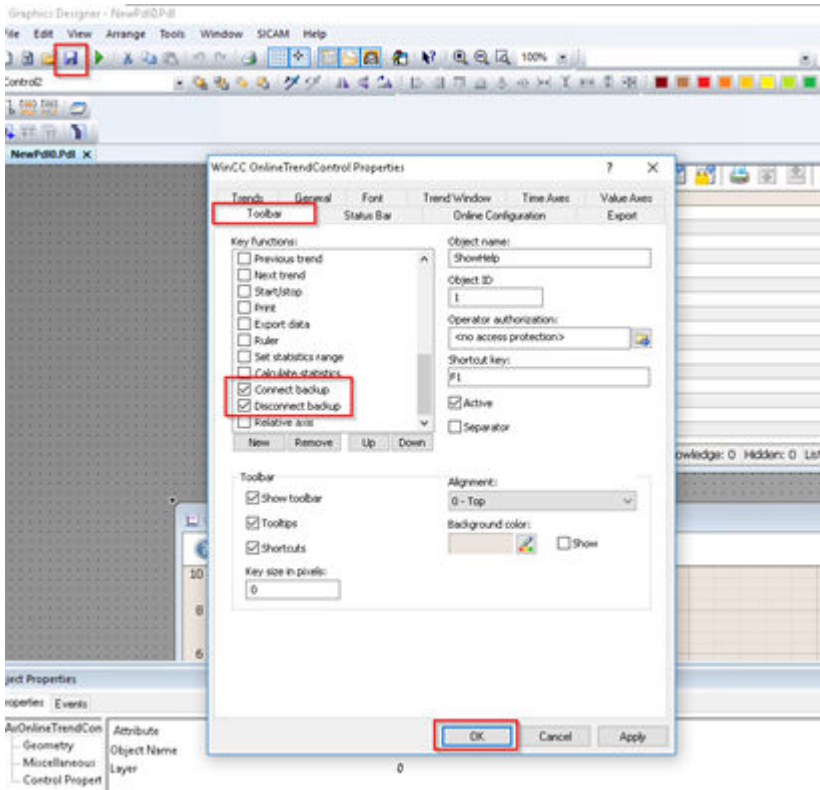
Figure 8-12 Selecting Location for Tag Logging

- ✧ Restart the project runtime.

8.5.6 Restore Archive Backup


For SIMATIC WinCC, all backed-up archive data can be only connected at the active running server and for fast display of the archived data, it can be connected via WinCC AlarmControl and OnlineTrendControl objects by using the **Connect Backup** and **Disconnect Backup** located in the toolbar of each object. To do so, proceed as follows:

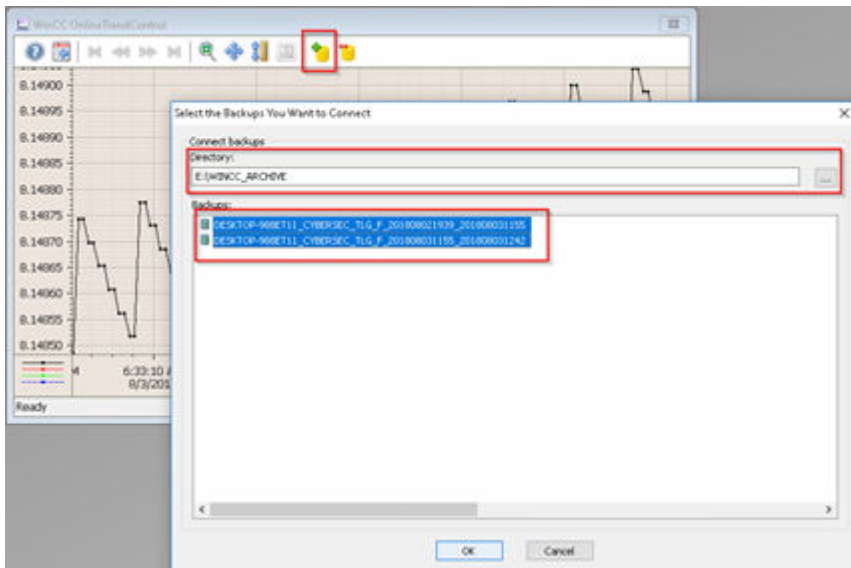
- ✧ The **Connect Backup** and **Disconnect Backup** need to be enabled in the toolbar of each object that is being used to display the data. To display these buttons, simply edit the properties of the object and check the options in the **Graphics Designer**. Save the pdl picture file and reload the picture in the Runtime.



[sc_Restoring Archive Backup, 1, en_US]

Figure 8-13 Restoring Archive Backup

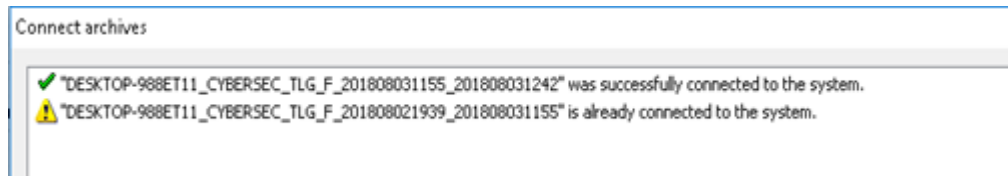
- ✧ To **Connect Backup**, in runtime click the  (Connect Backup) either in the **Alarm Control** or **Online Trend Control**, select the path, and one or more segments can be selected.



[sc_Connecting Backup in Runtime, 1, en_US]

Figure 8-14 Connecting Backup in Runtime

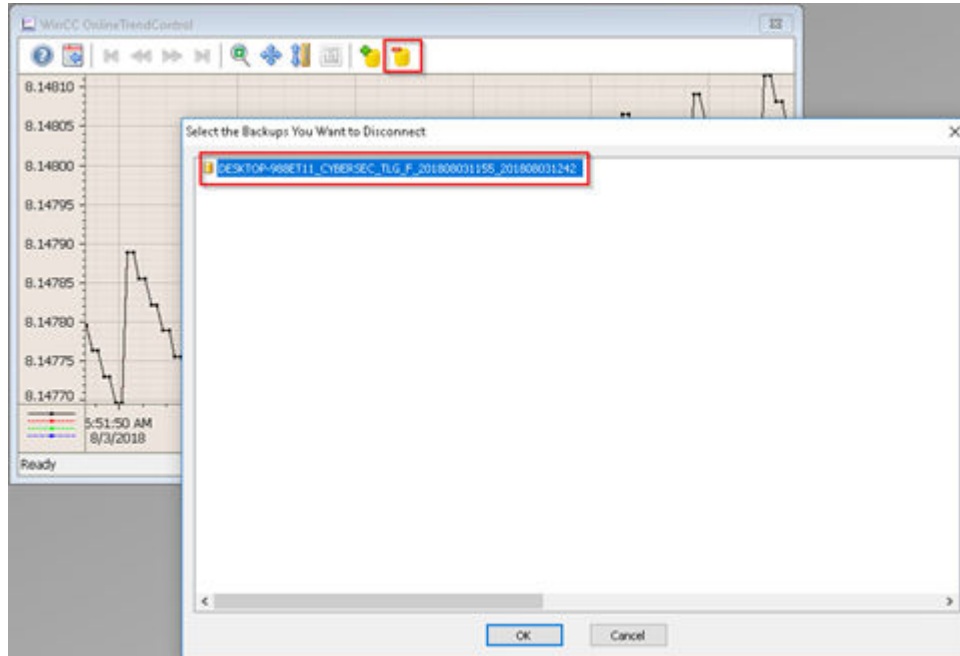
The Windows Connect Archives will display the confirmation of the connected archives.



[sc_Archive Connect Confirmation, 1, en_US]

Figure 8-15 Archive Connect Confirmation

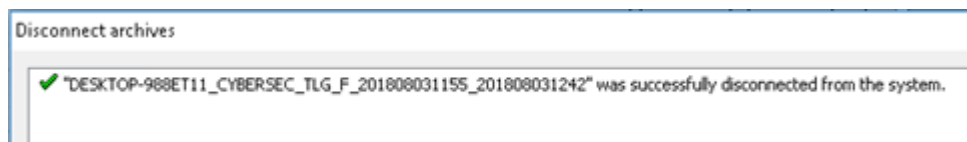
- ✧ To **Disconnect Backup**, in runtime click the  (Disconnect Backup) either in the **Alarm Control** or **Online Trend Control**, select one or more segments to be disconnected.



[sc_Disconnecting backup in Runtime, 1, en_US]

Figure 8-16 Disconnecting Backup in Runtime

The Windows Disconnect Archives will display the confirmation of the connected archives.



[sc_Backup Disconnect Confirmation, 1, en_US]

Figure 8-17 Backup Disconnect Confirmation

8.6 Archiving of Engineering Tools

All engineering tools and respective versions (also hotfixes) used in the project must be saved after commissioning and delivered to customer. It includes, for instance, the following:

- SICAM PAS (UI Configuration)
- SICAM SCC (Simatic WinCC Explorer)
- Toolbox

- DIGSI
- RuggedExplorer

9 Secure Remote Access

9.1	cRSP (common Remote Service Platform)	248
-----	---------------------------------------	-----

9.1 cRSP (common Remote Service Platform)

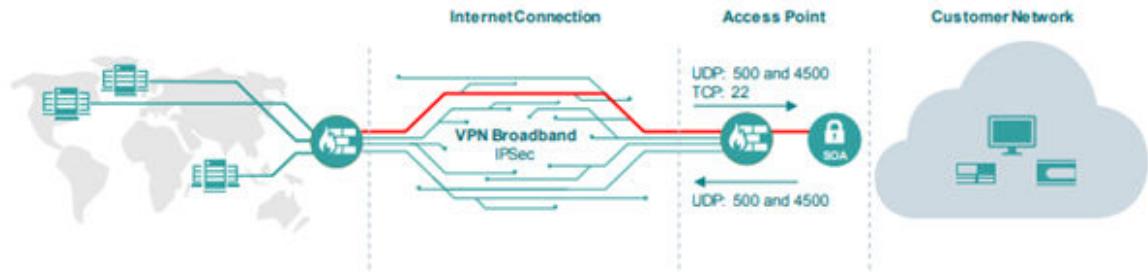
Remote Access to Substation Systems provides huge operation benefits but at the same time, secure connectivity is very important. Siemens provide a secure, cost-effective, faster, and flexible service over the Internet or by mobile wireless communication.

It is important to consider that to make a system available to users beyond the walls of trusted environment should be a balance between ease of use and security considerations.

cRSP provides several options for remote access based on the purpose of the access and type of systems. In some cases, the installation of extra software may be required on the target system. This would enable to access the systems anywhere in the world to competent energy automation experts, and to introduce the necessary maintenance measures. The system makes it possible for internal experts or external partners like system integrators to be involved in the remote access in addition to the skilled personnel from Siemens. There could be 2 different setup architecture for cRSP

9.1.1 Siemens-Owned Access

The connection between the cRSP infrastructure and the customer network is performed through a router provided by Siemens.

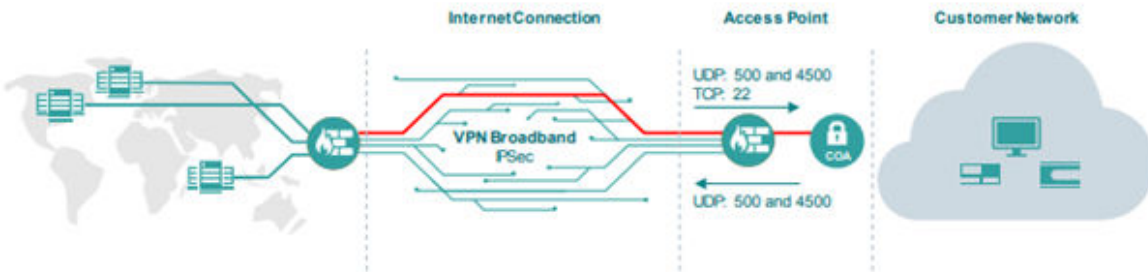


[sc_Siemens owned cRSP Access, 1, en_US]

Figure 9-1 Siemens-Owned cRSP Access

9.1.2 Customer-Owned Access

The connection between the cRSP infrastructure and the customer network is performed through a customer router or it ends at the customer's firewall.

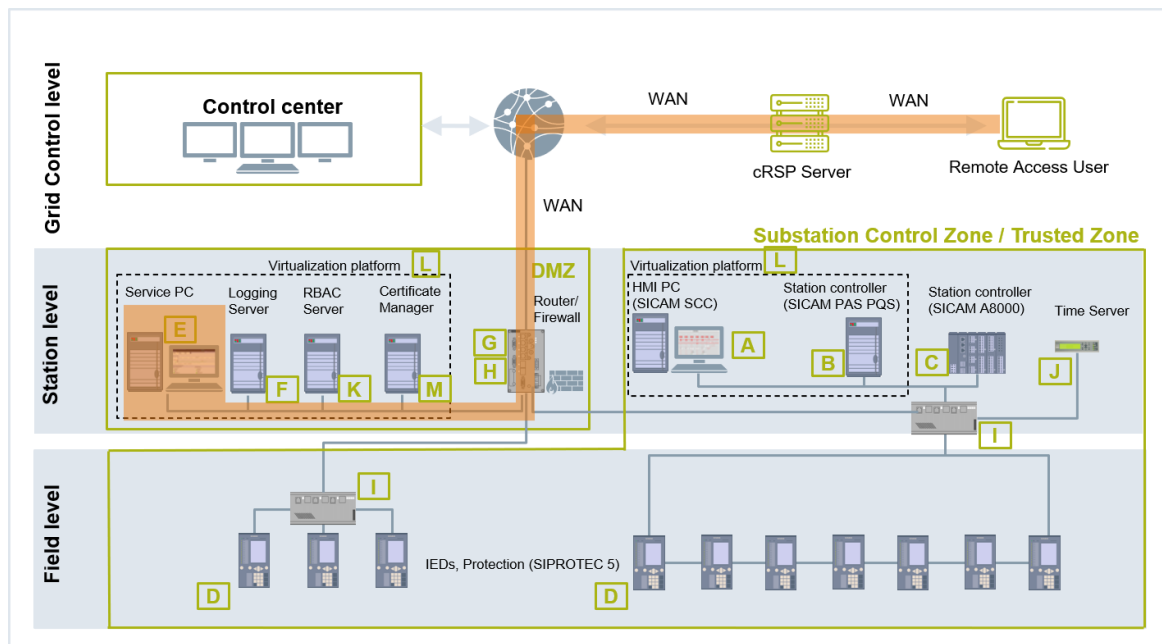


[sc_Customer owned cRSP Access, 1, en_US]

Figure 9-2 Customer-Owned cRSP Access

This chapter describes the configuration and usage of the common Remote Service Platform (cRSP), which is used to connect to the substation automation and protection systems. cRSP is owned by Siemens.

The general setup is shown in the following figure:



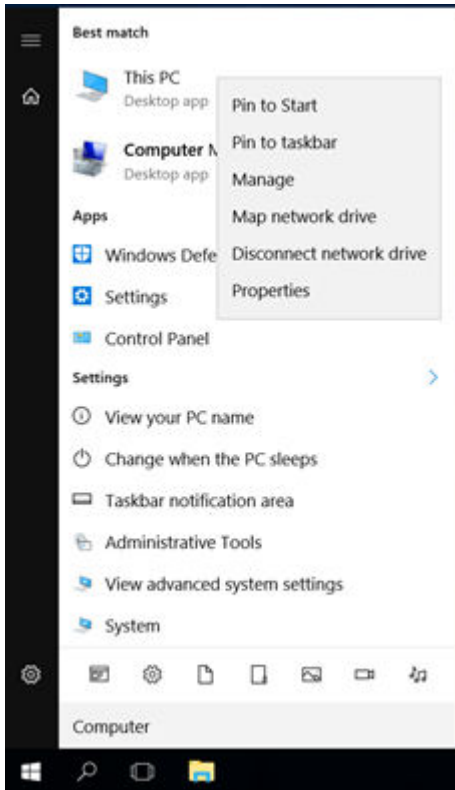
[sc_Remote Access through cRSP, 1, en_US]

Figure 9-3 Remote Access Through cRSP

9.1.3 Activate Windows RDP

The remote access allows an authorized user to perform similar engineering and configuration tasks as from a dedicated PC on the substation itself. The required permissions in the OS depend on the service tasks of the authorized user and will be configured via the account management locally or via Active Directory.

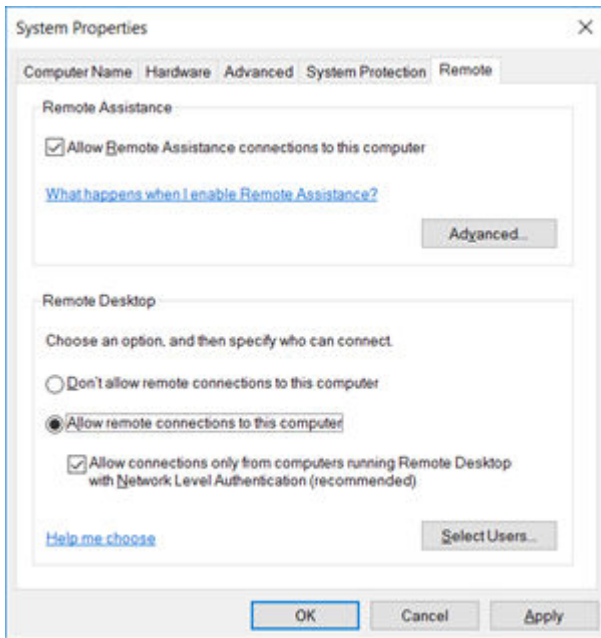
- ✧ Click **Start**, search for **Computer**, and go to **Properties**.



[sc_Enabling Remote Access in Windows, 1, en_US]

Figure 9-4 Enabling Remote Access in Microsoft Windows

- ✧ Select **Advanced system settings** and open the remote strap on the top bar and tick **Allow connections only from computers running Remote Desktop with Network Level Authentication**.

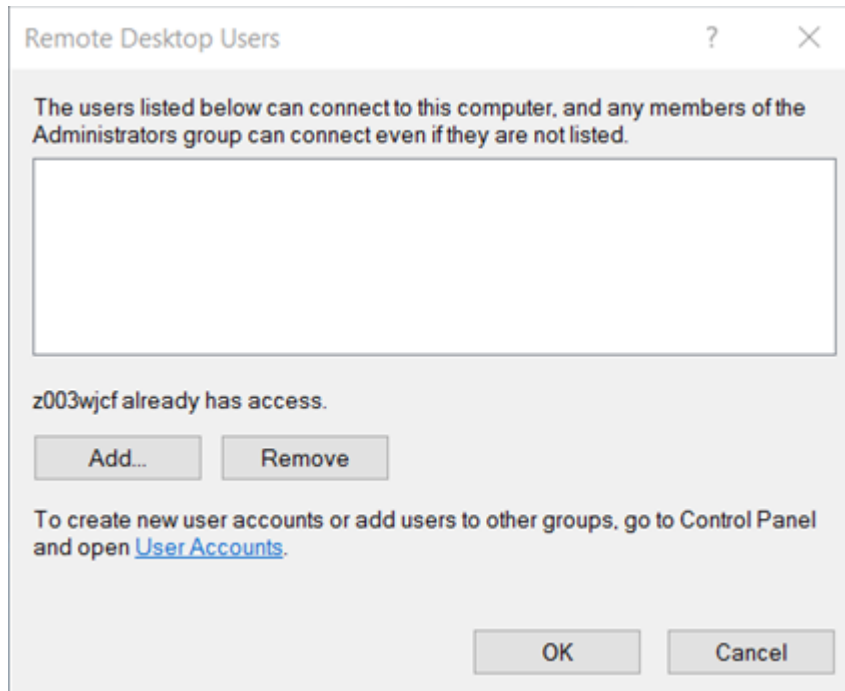


[sc_Allowing Remote Access in System Properties, 1, en_US]

Figure 9-5 Allowing Remote Access in System Properties

The system administrator used should already be part of the remote access group. If a special user needs to be added, select the **System Properties** window:

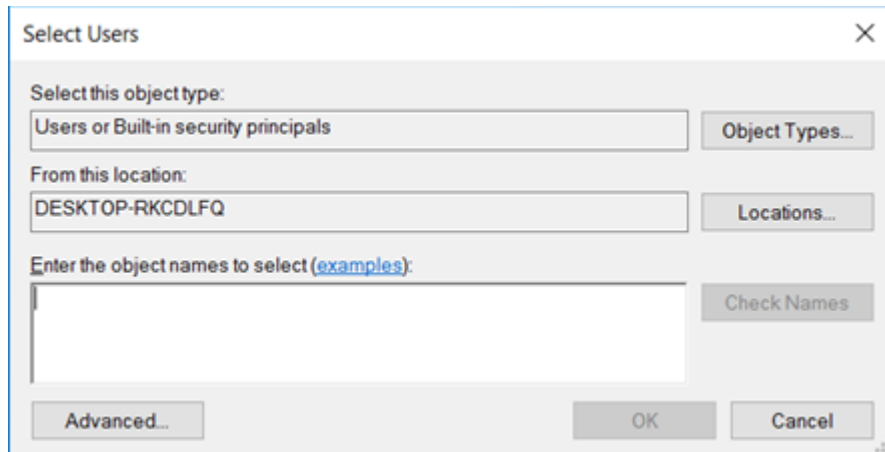
- ✧ Select **User...** and **Add...**, go to **Advanced** and **Find Now**.



[sc_Adding New User for Remote Access, 1, en_US]

Figure 9-6 Adding New User for Remote Access

- ✧ Select the user you want to add and click **OK** until all dialogs are closed.



[sc_Selecting User for Remote Access, 1, en_US]

Figure 9-7 Selecting User for Remote Access

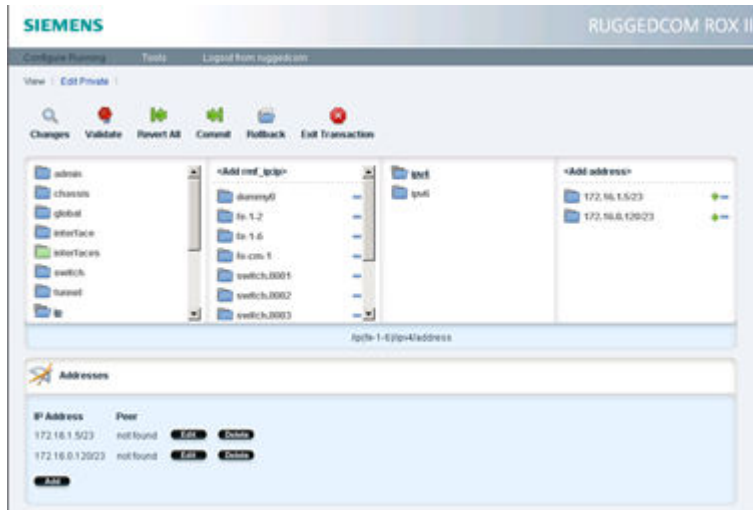
9.1.4 Network Setup – Firewall/NAT

The following description is based on a use case where the cRSP router is in a different zone than the PC which will provide the remote Terminal Access Service. The cRSP router is configured with certain fixed IPs. It is required to set up the network in a way to get the dedicated remote access PC available within the remote access zone.

Remote DMZ	IP → 172.16.0.120	(preconfigured in the cRSP)	Interface → RDMZ
Internal Workstation	IP → 172.16.11.6	(Service Workstation in the DMZ)	Interface → DMZ

9.1.4.1 Interface Settings

Set up a new RJ45 Interface with the following IP addresses as shown in the following figure:



[sc_Setting New Interface for Remote Access in Ruggedcom, 1, en_US]

Figure 9-8 Setting New Interface for Remote Access in Ruggedcom



NOTE

Set up a default gateway as static route with the gateway (GW) address 172.16.1.1.

9.1.4.2 Firewall Policy/Rule Settings

A new zone needs to be created in the firewall for allowing remote access in this example. It is considered as Remote DMZ (RDMZ). For detailed instructions, refer to [2.4 Firewall](#).

- ✦ Create a new zone called **RDMZ**.
- ✦ Add the new interface fe-1-6 and connect it with the RDMZ.
- ✦ Add a new set of default policies to block access between the new zone and the already existing zones.
- ✦ Create a rule which contains the following:

The IP addresses are used by the cRSP server service platform which represents the source of any service which requires access to your relevant equipment (for example your remote desktop session):

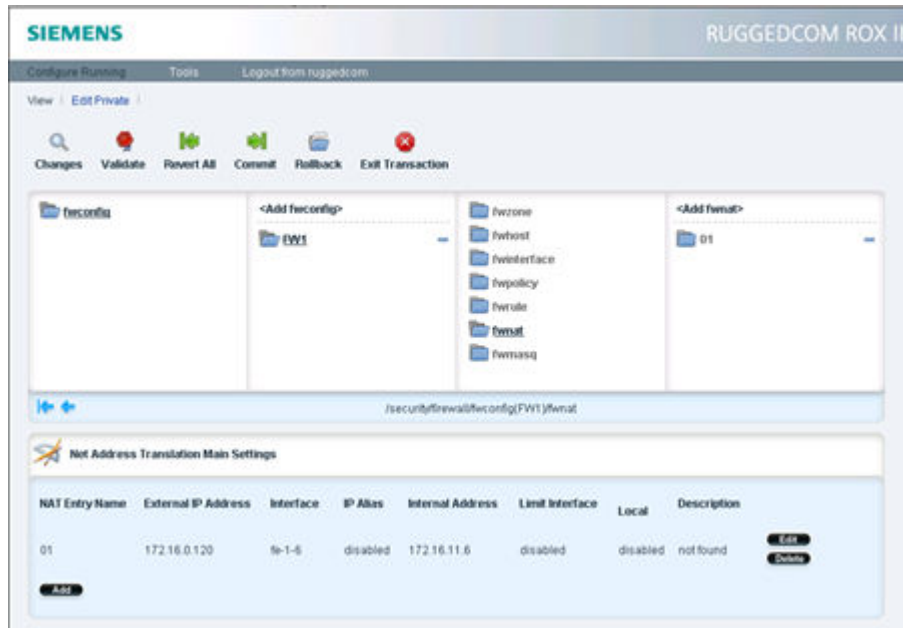
Source IP	cRSP Server <ul style="list-style-type: none"> • 194.138.39.24 • 129.73.116.83 • 194.138.243.184
Endpoint IP	Engineering Workstation <ul style="list-style-type: none"> • 172.16.11.6
Rule 1	Protocol: TCP Port: 3389
Rule 2	Protocol: ICMP

9.1.4.3 NAT – Network Address Translation

NAT is generally used in substations. One of the use cases is keeping the remote access interface in the predefined IP address range so that it does not interact with the substation IP addresses.

- ✦ Log in to the WebUI of the ROX and change to the **Edit** mode.

- ✧ Navigate to **security** → **firewall** → **fwconfig** → **FW1** → **fwnat**.
- ✧ Click **Add fwnat**.
- ✧ Fill the parameters: name or number, external IP, interface, and Internal IP (to where the request should get routed).
- ✧ Commit the change.



[sc_Enabling NAT in firewall, 1, en_US]

Figure 9-9 Enabling NAT in Firewall

It is important to enable NAT in the firewall to make it work. If the firewall is switched off, all interfaces will not be accessible from the Shell network.

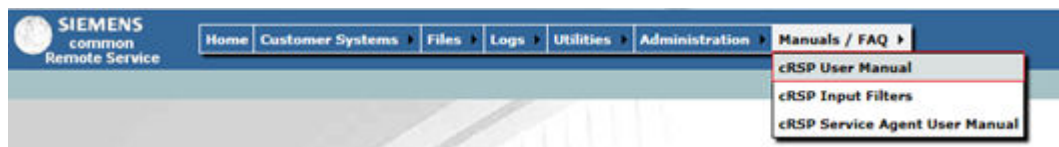
9.1.5 Test the cRSP Access

Access the cRSP Web page.

9.1.5.1 cRSP Settings

Generally, the change of settings is disabled for users. This can only be done by the Siemens Support team. For more information, refer to the *cRSP manual* available at the website

- ✧ Go to **Manuals / FAQ** → **cRSP User Manual**.



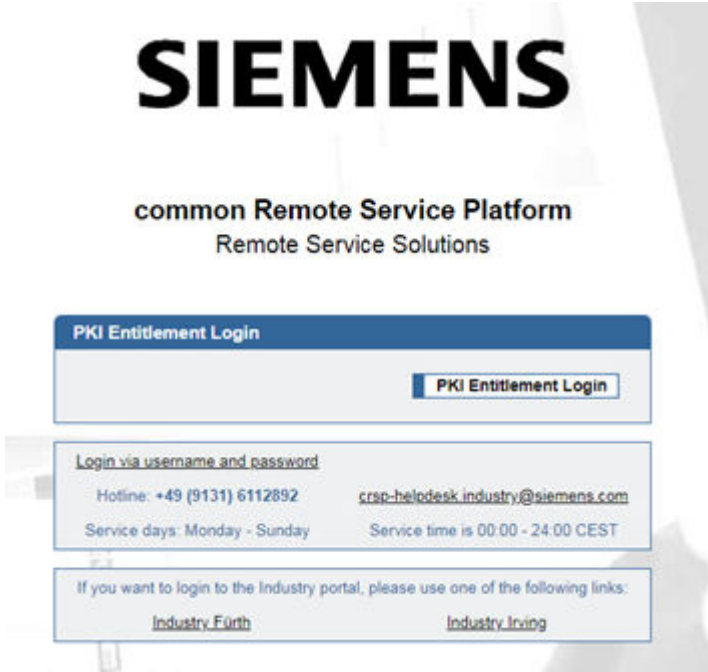
[sc_Accessing cRSP manual from cRSP Website, 1, en_US]

Figure 9-10 Accessing cRSP Manual from cRSP Website

9.1.5.2 Logon to the cRSP

The user that needs to login via cRSP should be part of the cRSP User group.

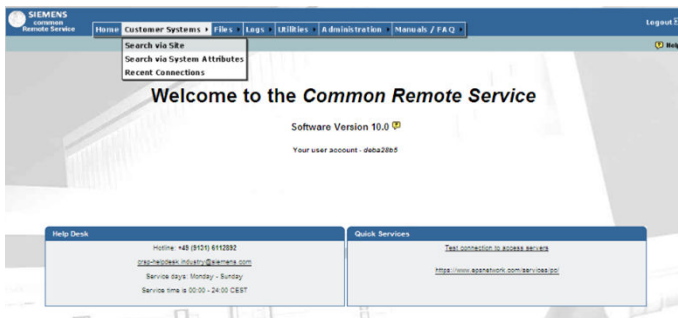
- cRSP Portal; Siemens internal (Intranet):
 - <https://crsp1.siemens.com/ic/login.do> (I&C)
 - <https://crsp1.siemens.com/industry/login.do> (Industry)
 - cRSP Portal; Siemens external CWP (Internet):
 - https://crsp-fth.siemens.com/dana-na/auth/url_4/welcome.cgi
- ✧ Open <https://crsp1.siemens.com/ic/login.do> with the Internet Explorer and login via PKI or unique user-name provided by the cRSP Helpdesk and the password chosen.



[sc_Logging in to cRSP, 1, en_US]

Figure 9-11 Logging in to cRSP

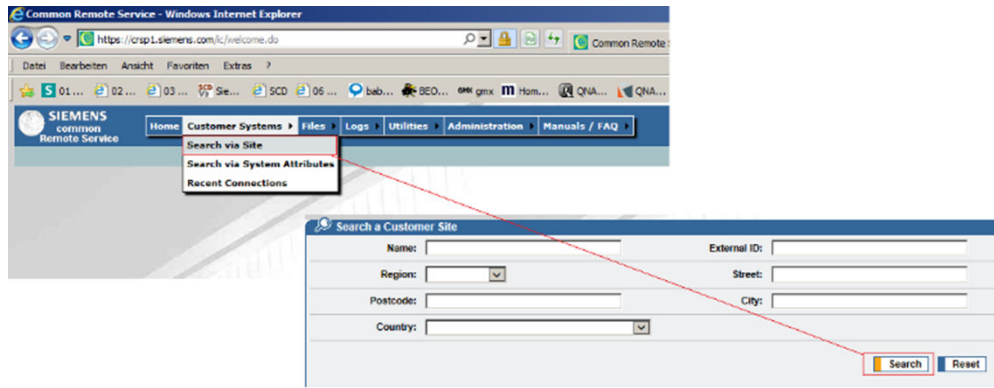
- ✧ Beside other navigation options, the site assigned to the user’s personal account can be accessed as shown in the following figure.



[sc_cRSP landing page, 1, en_US]

Figure 9-12 cRSP Landing Page

- ✧ Navigate via **Customer System** → **Search via Site** and click **Search** without any further filtering to get a list of all sites assigned to the user. It is possible to type the name or other search criteria of the site to filter the results.



[sc_Search via Site, 1, en_US]
Figure 9-13 Search via Site

Host Name [1]	Alert Status [1]	System Type [1]	Customer Site [1]	Product [1]	IP Address (Site View) [1]	Real Host IP Address [1]	Operational State [1]
Confly_PC1		SICAM PAS	Siemens AG, E D EA S1S	IC S3 Products / Dgpl / OPMI	10.65.142.224	172.16.0.121	Complete
Confly_PC2		DIGS	Siemens AG, E D EA S1S	IC S3 Products / Dgpl / OPMI	10.65.142.225	172.16.0.122	Complete
Enginering		DIGS_L3	Siemens AG, E D EA S1S	IC S3 Products / Dgpl / OPMI	10.65.142.226	172.16.0.120	Complete
FAK-Fullst1		SICAM PAS	Siemens AG, E D EA S1S	IC S3 Products / Dgpl / OPMI	10.65.142.227	172.16.0.19	Complete
FAK-Fullst2		SICAM PAS	Siemens AG, E D EA S1S	IC S3 Products / Dgpl / OPMI	10.65.142.228	172.16.0.11	Complete
PA3CC-Sew1		SICAM PAS/CC	Siemens AG, E D EA S1S	IC S3 Products / Dgpl / OPMI	10.65.142.229	172.16.0.15	Complete
PA3CC-Sew2		SICAM PAS/CC	Siemens AG, E D EA S1S	IC S3 Products / Dgpl / OPMI	10.65.142.230	172.16.0.16	Complete
RS02100_1		Switch	Siemens AG, E D EA S1S	IC S3 Products / Dgpl / OPMI	10.65.142.231	172.16.0.99	Complete
RS02100_2		Switch	Siemens AG, E D EA S1S	IC S3 Products / Dgpl / OPMI	10.65.142.232	172.16.0.100	Complete
SIPROTEC4		Protection	Siemens AG, E D EA S1S	IC S3 Products / Dgpl / OPMI	10.65.142.233	172.16.0.20	Complete

[sc_Search via site results, 1, en_US]
Figure 9-14 Search via Site Results

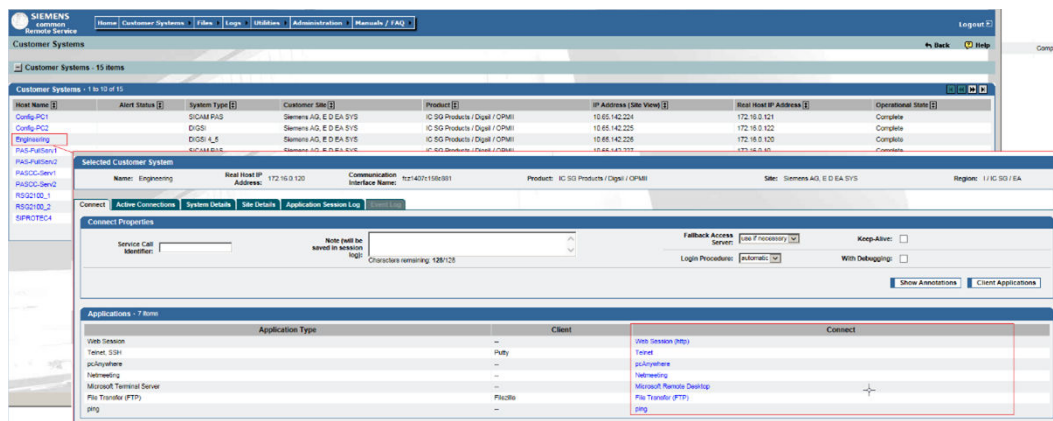
All available addresses can be seen under **Real Host IPs** which are preconfigured in the Cisco router. The IP assigned to the NAT configuration in the router should be one of those.

IP Address (Site View) [1]	Real Host IP Address [1]
10.65.142.224	172.16.0.121
10.65.142.225	172.16.0.122
10.65.142.226	172.16.0.120
10.65.142.227	172.16.0.10
10.65.142.228	172.16.0.11
10.65.142.229	172.16.0.15
10.65.142.230	172.16.0.16
10.65.142.231	172.16.0.99
10.65.142.232	172.16.0.100
10.65.142.233	172.16.0.20

[sc_IPs Assigned for NAT, 1, en_US]
Figure 9-15 IPs Assigned for NAT

✧ Click the device with IP configured for the equipment.

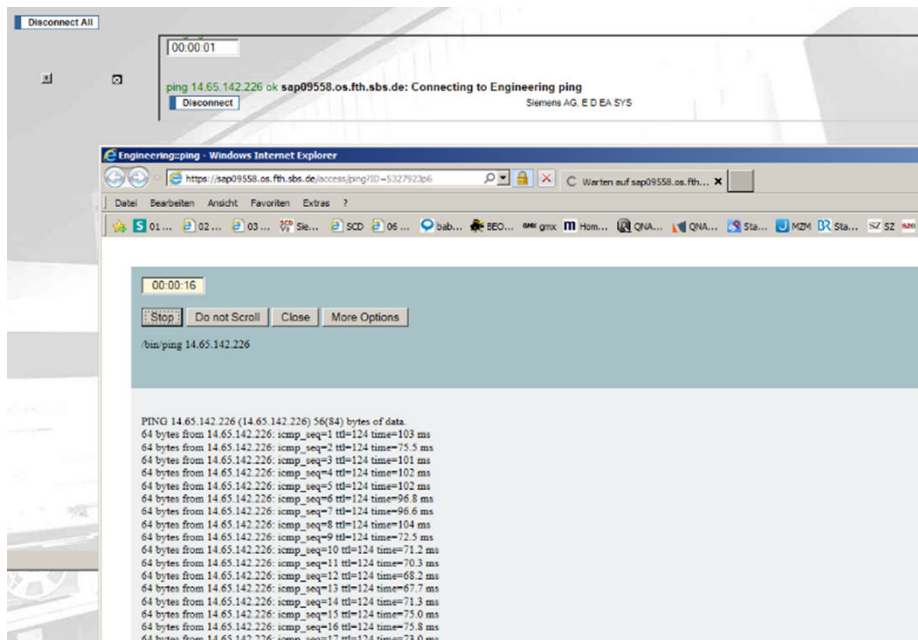
It will open a new page with the available services and applications that will start for this host:



[sc_Selecting a Device in cRSP, 1, en_US]
Figure 9-16 Selecting a Device in cRSP

Connect to a system only if its operational state has the value **Complete**. If the system's operational state has a different value (e.g. **Under Construction**), only administrators may establish connections to the system (for connection tests).

- **Name:**
The name of the customer system as used internally by the cRSP (unique within all systems of a tenant).
 - **Real Host IP Address:**
The customer system's IP address as defined in the system itself.
 - **Product:**
The product type of the customer system.
 - **Site:**
The administrative site to which the customer system is assigned.
 - **Region:**
The administrative region to which the customer system is assigned.
- ✧ Try to ping the device. When the **Ping** is pressed, 2 new windows will be opened and the feedback time can be seen like ping in the Windows Command Prompt.



[sc_Pinging a Device in cRSP, 1, en_US]

Figure 9-17 Pinging a Device in cRSP

If the device is reachable, close the window and start any other service available.

9.1.6 Applications for Remote Monitoring and Control

9.1.6.1 Remote Desktop (RDP)

Remote desktop software enables to operate a computer as if being accessed physically, from a remote, internet-enabled computer. The term **remote desktop** refers to a software or an operating system feature allowing applications, either command line programs or graphical applications, to be run remotely on a server, while being displayed locally.



NOTE

The user on the target PC logs off as soon as the remote-desktop connection has been established. For SICAM PAS Station Units without screen, the remote-desktop application must be used.

- ✧ For selecting the remote-desktop application, click **Microsoft Terminal Server**.

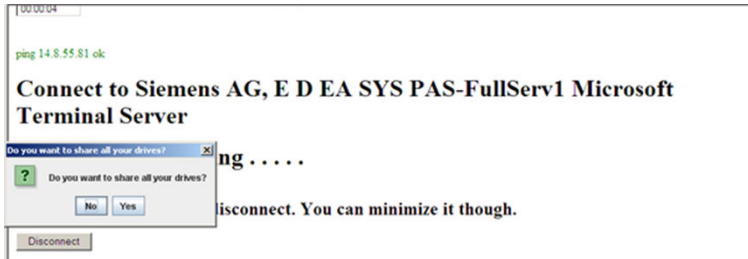
Application Type	Client	Connect
Web Session	--	Web Session
Telnet Session	Putty	Telnet
pcAnywhere	--	pcAnywhere
Netmeeting	--	Netmeeting
Microsoft Terminal Server	--	Microsoft Terminal Server
File Transfer (FTP)	Filezilla	File Transfer (FTP)

[sc_Selecting Remote Desktop Application, 1, en_US]

Figure 9-18 Selecting Remote Desktop Application

cRSP will connect to the selected PC and a pop up will occur asking if you want to share all your drives of your local PC.

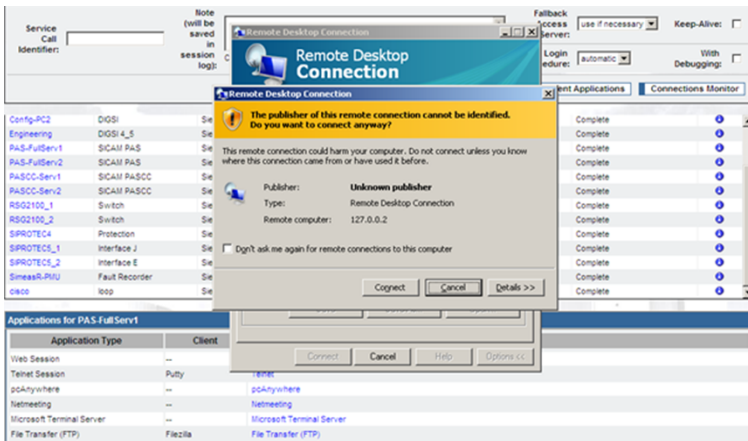
- ✧ Confirm the message with **Yes**. This will allow to share files in the explorer view of the target PC selected.



[sc_Starting Remote Desktop, 1, en_US]

Figure 9-19 Starting Remote Desktop

- ✧ Now, log on with the user configured in the Windows PC. In the pop-up window **Remote Desktop Connection**, click **Connect**. This will give access to the target PC.



[sc_Accessing Target PC, 1, en_US]

Figure 9-20 Accessing Target PC

As mentioned above, the file can now be shared and the user has full access to all applications and functions of the target PC.

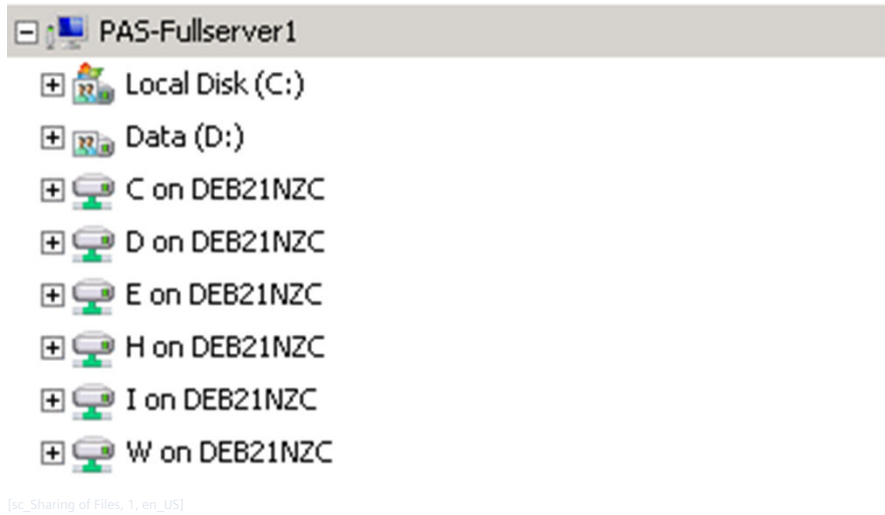


Figure 9-21 Sharing of Files

9.1.6.2 Applications for the Transfer of Files

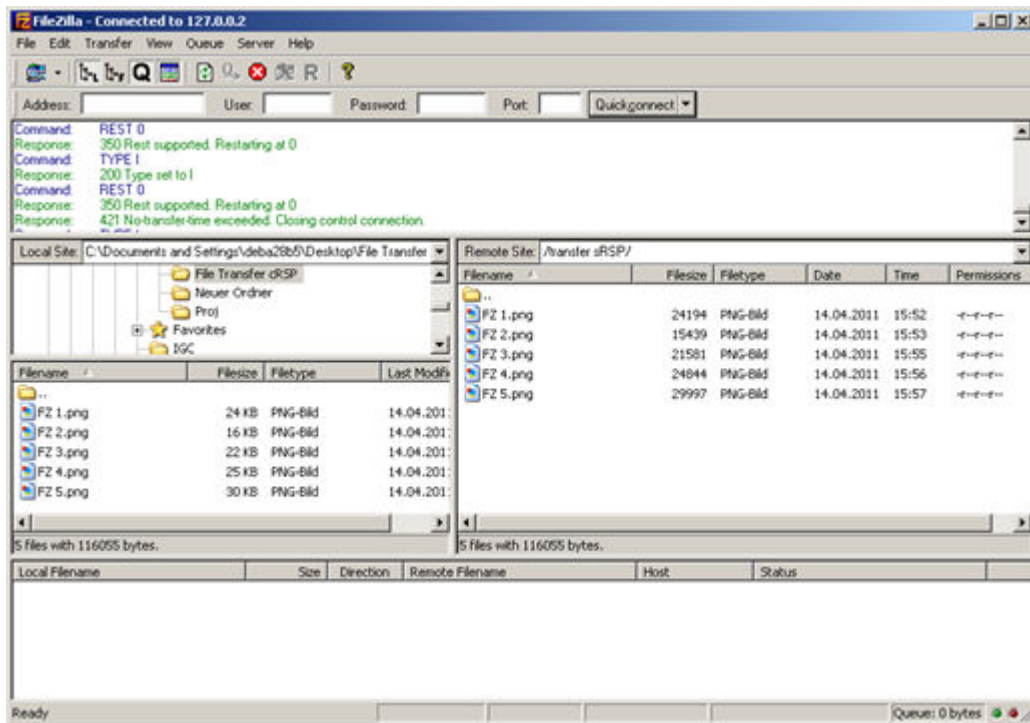
FileZilla (File Transfer with Logging Function)

FileZilla is a free and cross-platform FTP software, consisting of FileZilla Client and FileZilla Server.

A FileZilla client is a fast and reliable cross-platform FTP, FTPS, and SFTP client with lots of useful features and an intuitive graphical user interface featuring:

- Supports FTP, FTP over SSL/TLS (FTPS), and SSH File Transfer Protocol (SFTP)
- Cross-platform. Runs on Windows, Linux, *BSD, Mac OS X, and more
- IPv6 support
- Available in many languages
- Supports resume and transfer of large files > 4 GB
- Tabbed user interface
- Powerful site manager and transfer queue
- Bookmarks
- Drag & drop support
- Configurable transfer speed limits
- File-name filters
- Directory comparison
- Network configuration wizard
- Remote file editing
- Keep-alive
- HTTP/1.1, SOCKS5, and FTP-Proxy support
- Logging to file
- Synchronized directory browsing
- Remote file search

Users can exchange file using FileZilla user interface.



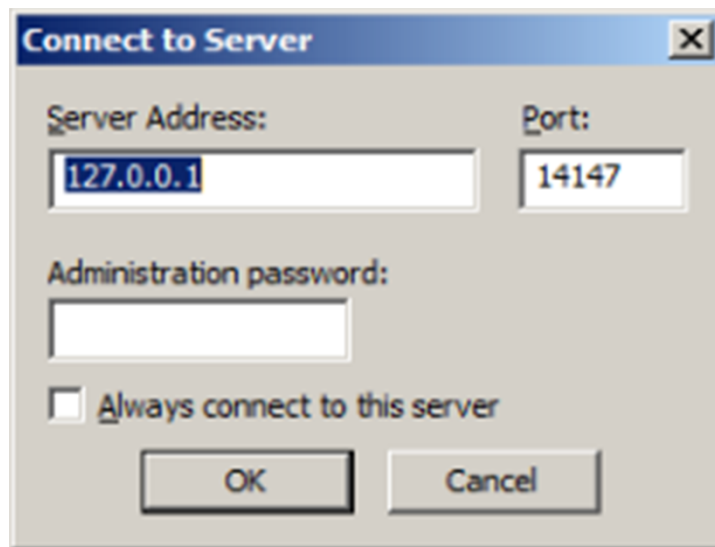
[sc_FileZilla User Interface, 1, en_US]

Figure 9-22 FileZilla User Interface

9.1.6.3 File Transfer on Remote Site

FileZilla Server needs to be installed on the target system (e.g., Engineering PC), a user password must be defined, and a folder needs to be shared. Therefore, proceed as follows:

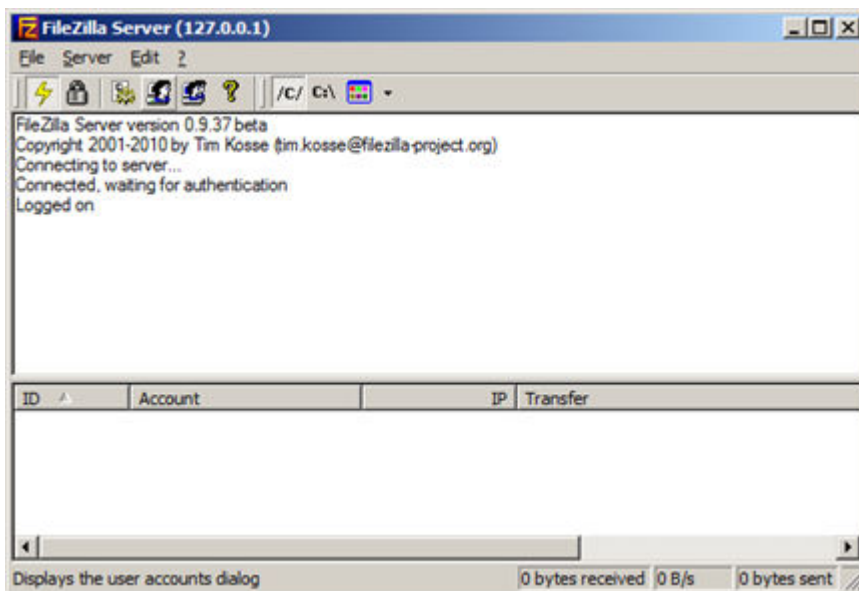
- ✧ Double-click the desktop link of the FileZilla Server and keep the settings like the **Server Address** as shown.



[sc_Connecting to Server in FileZilla, 1, en_US]

Figure 9-23 Connecting to Server in FileZilla

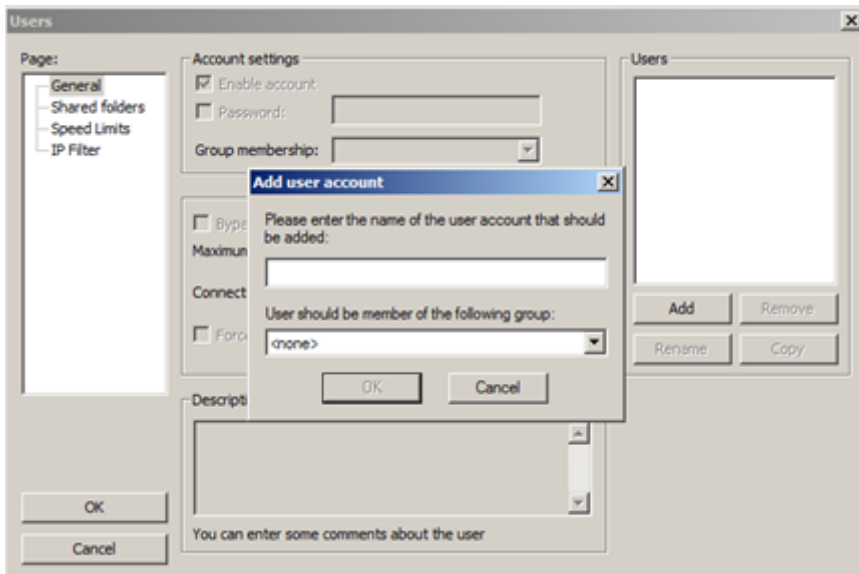
- ✧ Click the user symbol to open the **Users** dialog.



[sc_Selecting User, 1, en_US]

Figure 9-24 Selecting User

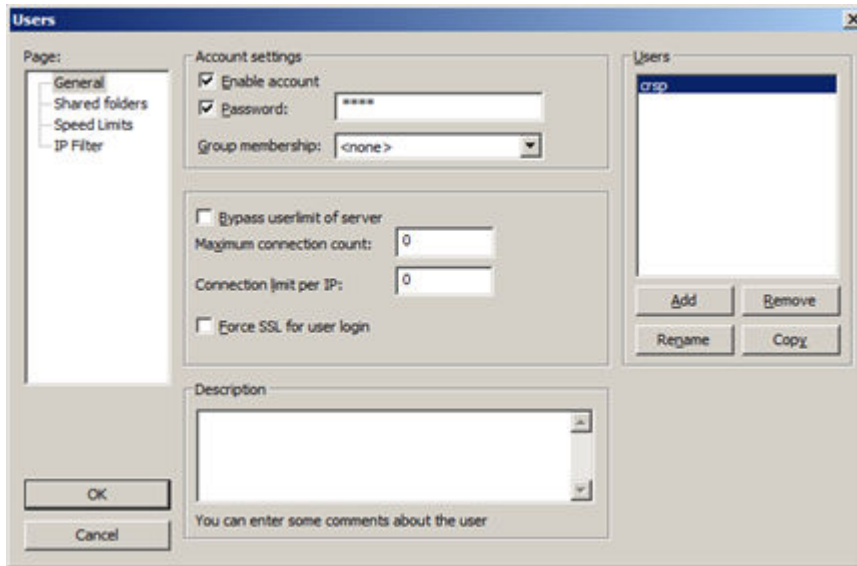
✧ Now, define a user account.



[sc_Defining a User, 1, en_US]

Figure 9-25 Defining a User

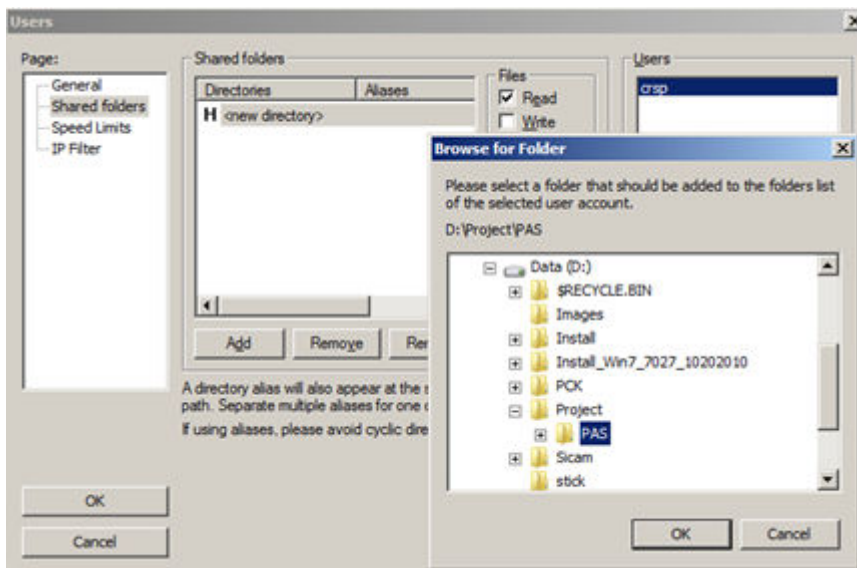
✧ Enter a password (as shown in the following figure).



[sc_User Authentication using Password, 1, en_US]

Figure 9-26 User Authentication Using Password

- ✧ Select a folder to be shared for data exchange and give proper user rights (read, write, delete). As soon as the configuration of FileZilla is finished, minimize the application but do not close it.



[sc_Select folder to be shared, 1, en_US]

Figure 9-27 Select Folder to be Shared

- ✧ File transfer on user site.
- ✧ During a remote service, the FileZilla client is started on the user PC via cRSP by clicking **File Transfer (FTP)** and appears as Java Applet.

Applications for PAS-FullServ1		
Application Type	Client	Connect
Web Session	--	Web Session
Telnet Session	Putty	Telnet
pcAnywhere	--	pcAnywhere
Netmeeting	--	Netmeeting
Microsoft Terminal Server	--	Microsoft Terminal Server
File Transfer (FTP)	Filezilla	File Transfer (FTP)

[sc_cRSP Java Applet, 1, en_US]

Figure 9-28 cRSP Java Applet

A Appendix

A.1	Abbreviations	264
-----	---------------	-----

A.1 Abbreviations

For general abbreviations used in the Management Manual, process, and work instructions, see <https://blog.insresearch.com/acronym-quick-reference> (PLM Process Glossary).

List of **project/document specific** abbreviations:

AC	Application Control
AD	Active Directory
AD DS	Active Directory Domain Services
CC	Change Control
CLI	Command-Line Interface
CSR	Certificate Signing Request
DDC	Desktop Delivery Controller
DMZ	Demilitarized Zone
EA	Energy Automation
ESP	Encapsulating Security Payload
HIDS	Host-Based Intrusion Detection System
HMI	Human Machine Interface
IC	Integrity Control
ICA	Citrix XenApp Independent Computing Architectures
IDS	Intrusion Detection System
IED	Intelligent Electronic Device
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
LTS	Long-Time Support
MD5	Message-Digest Algorithm
NIDS	Network-Based Intrusion Detection System
Nmap	Network Manager
OpenSSL	Open Source Secure Sockets Layer
OSI	Open Systems Interconnection
PFS	Perfect Forward Secrecy
PRP	Parallel Redundancy Protocol
PSK	Pre-Shared Key
RSA	Rivest, Shamir, and Adelman - an algorithm for public-key encryption
SaaS	Software-as-a-Service
SCT	Security Configuration Tool
SHA	Secure Hash Algorithm
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
VM	Virtual Machine
VPN	Virtual Private Network
WOU	WSUS Offline Update
WSUS	Windows Server Update Services

B List of Required Open Ports

The following table lists are excerpts of the Security Manuals of each individual product:

B.1	SICAM PAS/PQS, SICAM SCC	266
B.2	SIPROTEC 5/DIGSI 5	268

B.1 SICAM PAS/PQS, SICAM SCC

The following table lists the programs and services that communicate between members of the network. If 2 members are in different subnetworks, the ports and protocols must be opened in the firewalls between the subnetworks.

Service	Layer 4 Protocol	Layer 7 Protocol	From (Client)		To (Server)	
			Host	Port	Host	Port
BTIServer	TCP	BTI protocol	SICAM PAS/PQS Full Server/DIP	–	SICAM PAS/PQS Full Server/DIP	10025
CRLDP Client	TCP	http	SICAM PAS/PQS Full Server/DIP	(>1024)	SICAM GridPass	80
DNP3i Master	TCP	DNP3i	SICAM PAS/PQS Full Server/DIP	(>1024)	IED	20000
DNP3i Slave	TCP	DNP3i	Control center	(>1024)	SICAM PAS/PQS Full Server/DIP	20000
DSIServer	TCP	DSI protocol	SICAM PAS/PQS DIP	–	SICAM PAS/PQS Full Server/DIP	10500
EST Client	TCP	EST	SICAM PAS/PQS Full Server/DIP	(>1024)	SICAM GridPass	8085
IEC 60870-5-104 Master	TCP	IEC 60870-5-104	SICAM PAS/PQS Full Server/DIP	(>1024)	IED	2404
IEC 60870-5-104 Slave	TCP	IEC 60870-5-104	Control center	(>1024)	SICAM PAS/PQS Full Server/DIP	2404
IEC 61850 Client	TCP	IEC 61850	SICAM PAS/PQS Full Server/DIP	10036	IED	102
IEC 61850 Server	TCP	IEC 61850	Control center	(>1024)	SICAM PAS/PQS Full Server/DIP	102
Modbus Master	TCP	Modbus	SICAM PAS/PQS Full Server/DIP	(>1024)	IED	502
Modbus Slave	TCP	Modbus	Control center	(>1024)	SICAM PAS/PQS Full Server/DIP	502
OPC DA Client	TCP	OPC DA	SICAM PAS/PQS Full Server/DIP	(>1024)	IED	135
OPC DA Server	TCP	OPC DA	Control center	(>1024)	SICAM PAS/PQS Full Server/DIP	135
OPC XML DA Server	TCP	OPC XML DA	Control center	(>1024)	SICAM PAS/PQS Full Server/DIP	8081
PQ Analyzer backup	TCP	Proprietary	PQ Analyzer	(>1024)	Local	4845
PQ Analyzer demo	TCP	Proprietary	PQ Analyzer	(>1024)	Local	4846
PQS Automatic Notification	TCP	Proprietary	PQ Analyzer	(>1024)	SICAM PAS/PQS Full Server /PQ Collector	4847
PQ Analyzer runtime PQS Automatic Notification	TCP	SMTP	SICAM PAS/PQS Full Server/DIP	(>1024)	SMTP server	25
SCC Proxy	TCP	Proprietary	WinCC Server	(>1024)	SICAM PAS/PQS Full Server/DIP	10501
Sentinel LDK License Manager	TCP	Proprietary	Local	1947	Local	1947
	UDP	Proprietary	Broadcast	1947	n/a	n/a
SICAM PAS/PQS UI – Operation Client	TCP	HTTP	Computer with Web browser	(>1024)	SICAM PAS/PQS Full Server/DIP	80
	TCP	HTTPS	Computer with Web browser	(>1024)	SICAM PAS/PQS Full Server/DIP	443

Service	Layer 4 Protocol	Layer 7 Protocol	From (Client)		To (Server)	
			Host	Port	Host	Port
SICAM Q80	TCP	FTP	SICAM PAS/PQS Full Server/DIP	(>1024)	IED	1200 to 1202
SIMEAS R / PMU	TCP	Proprietary	SICAM PAS/PQS Full Server/DIP	(>1024)	IED	2010
SIPROTEC 4 DIGSI protocol	UDP	Proprietary	DIGSI computer	50000	SIPROTEC 4	50000
SIPROTEC 4 Web Monitor	UDP	JAVA	Computer with Web browser	(>1024)	SIPROTEC 4	56797
SIPROTEC 4 Web Monitor & Communication Module Website	TCP	HTTP	Computer with Web browser	(>1024)	SIPROTEC 4	80
SIPROTEC 5 ¹ DIGSI 5	TCP	HTTPS	DIGSI computer	(>1024)	SIPROTEC 5	443
SoftPLC language switch	TCP	Proprietary	SICAM PAS/PQS Full Server/DIP	(>1024)	SICAM PAS/PQS Full Server/DIP	8089
SQL Anywhere 17 - Pas	TCP	ODBC	SICAM PAS/PQS DIP / SICAM PAS/PQS UI – Configuration	(>1024)	SICAM PAS/PQS Full Server	2638
Supervision via SNMP	UDP	SNMP	DIGSI computer	(>1024)	SIPROTEC 4	161
	UDP	SNMP	Computer with SNMP browser	(>1024)	SIPROTEC 4	161
	UDP	SNMP	Computer with SNMP browser	(>1024)	SICAM PAS/PQS Full Server/DIP	162
	UDP	SNMP	SICAM PAS/PQS Full Server/DIP	(>1024)	SIPROTEC 4	161
syslog Server	UDP	syslog	SICAM PAS/PQS Full Server/DIP	(>1024)	syslog Server	514
Time Synchronization	UDP	NTP	SICAM PAS/PQS Full Server/DIP	(>1024)	NTP Server	123
	UDP	NTP	SIPROTEC 4	(>1024)	NTP Server	123
Time Synchronization SICAM PAS/PQS - NTP Service	UDP	NTP	SIPROTEC 4	(>1024)	SICAM PAS/PQS Full Server/DIP	123
WinCC Web Client	TCP	HTTPS	WinCC Web Client	(>1024)	WinCC WebNavigator Server	443
WinCC, Simatic Communication Service SCS	TCP	Proprietary via RPC	WinCC WebNavigator Server	(>1024)	WinCC Server	135
WinCC, Simatic Communication Service SCS ²	TCP	Proprietary via RPC	WinCC Client	(>1024)	WinCC Server	135
Windows – Remote Desktop	TCP	RDP	Windows	–	Windows	3389
IEC 60870-5-104 Master	TCP	IEC 60870-5-104	SICAM SCC	(>1024)	IED	2404
Supervision via SNMP	UDP	SNMP	SICAM SCC	(>1024)	IED	161
IEC 61850 Client	TCP	IEC 61850	SICAM SCC	(>1024)	IED	102

¹ The DIGSI5 application itself needs no special open port, because there are no incoming connections.

² Depending on used WinCC functions, more ports could be in use. For details, see SIMATIC HMI WinCC V7 System Description. For RPC communication, ports are temporarily used and dynamically assigned (1024 through 65635) by the RPC endpoint mapper.

B.2 SIPROTEC 5/DIGSI 5

Service	Layer 4 Protocol	Layer 7 Protocol	Typical Client	Client Port	Typical Server	Server Port
DIGSI 5 protocol to Automation License Manager	TCP	DIGSI 5 protocol to Automation License Manager	DIGSI 5 PC	4410 (default value)	Automation License Manager on a possible separate server, i.e. local host	4410 (default value)
DIGSI 5 communication protocol to SIPROTEC 5	TCP	HTTPS	DIGSI 5 PC	>1024	SIPROTEC 5	443
Reporting / IEC 61850 / MMS	TCP	IEC 61850	IEC 61850 client (e.g. SICAM PAS, SICAM A8000)	>1024	SIPROTEC 5	102
Time Synchronization / SNTP	UDP	SNTP	SIPROTEC 5	123	SNTP Server	123
Monitoring via Simple Network Management Protocol (SNMPv3)	UDP	SNMPv3	PC with SNMP client (e.g. SICAM PAS, 1703, DIGSI 5 PC/ Remote DIGSI 5 PC)	>1024	SIPROTEC 5	161
DNP3i	TCP	DNP3 TCP	SICAM PAS	20000 or next free port	SIPROTEC 5	20000
IEC 60870-5-104	TCP	IEC 104	SICAM PAS	>1024	SIPROTEC 5	2404
Synchrophasor	TCP	–	Phasor data concentrator	>1024	SIPROTEC 5	4712
	UDP	–	Phasor data concentrator	>1024	SIPROTEC 5	4713
MODBUS on TCP	TCP	MODBUS	Substation controller	>1024	SIPROTEC 5	502
Temperature box	UDP	RTD	Temperature box	>1024	SIPROTEC 5	can be configured
syslog Client	UDP	–	SIPROTEC 5	*	syslog Server	514
Homepage	TCP	HTTP	PC	>1024	EN100	8080 to 8083
RADIUS Client	UDP	–	SIPROTEC 5	–	RADIUS Server	1812
OPC UA	TCP	MQTT	SIPROTEC 5	–	Broker	8883

Literature

- /1/ Description of Powershell cmdlets for WDAC: <https://docs.microsoft.com/en-us/powershell/module/configci/?view=win10-ps>
- /2/ The DG-Readiness-Tool can be used to check whether the computer is capable to run Device Guard: <https://www.microsoft.com/en-us/download/details.aspx?id=53337>
- /3/ Microsoft Self-paced Labs: Search for "Deploy Device Guard": <https://www.microsoft.com/hands-on-labs/self-paced-labs>
- /4/ Microsoft Docs for Device Guard: https://blogs.msdn.microsoft.com/windows_hardware_certification/2015/05/22/driver-compatibility-with-device-guard-in-windows-10/
- /5/ WDAC main page on Microsoft Docs: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/windows-defender-application-control>
- /6/ WDAC Policy Rule
Options: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/select-types-of-rules-to-create#windows-defender-application-control-policy-rules>
- /7/ WDAC Policy Rules: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/select-types-of-rules-to-create#windows-defender-application-control-file-rule-levels>
- /8/ WDAC - Merging of policies: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/merge-windows-defender-application-control-policies>
- /9/ WDAC can also control specific plug-ins, add-ins, and modules: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/use-windows-defender-application-control-policy-to-control-specific-plug-ins-add-ins-and-modules>
- /10/ Description of the PowerShell constrained language mode: <https://devblogs.microsoft.com/powershell/powershell-constrained-language-mode/>