SIPROTEC 5 Compact Cybersecurity Functionality

APN – C.007

siemens.de/siprotec

SIPROTEC 5 Compact Application

Cybersecurity Functionality

APN-C.007, Edition 1

Content:

1 Cybersecurity Functionality

1.1 introduction

In the past, computers were islands of functionality with little interconnectivity, if any at all. Nowadays computer servers, Desktop PCs, and automation units are linked with each other.

On one hand, the current mode creates new business opportunities. On the other hand, these interconnected components, for example, applications that are not designed for use in heavily networked environments, can be attacked.

This APN application note serves as a recommendation for the secure commissioning and operations of the SIPROTEC 5 / SIPROTEC 5 Compact devices in networked environments.

Siemens offers products and technologies, which consider the leading cybersecurity standards. The major drivers for secure infrastructures are the standards and guidelines, such as IEC 62443, IEC 62351, BDEW White Paper, IEEE 1686, and NERC CIP (Critical Infrastructure Protection).

The most important security requirements are the following:

- Authentication and authorization of the users
- Assurance of the integrity of the transmitted data
- Protections against virus, trojans, and other malware
- Collection and saving of log files
- Operation of the system in a protected environment (physical security)
- Every user is given the only those rights that are necessary to fulfill the corresponding work.
- Assurance, that in case of a system failure, a restoration is possible without or only with marginal data loss
- Only activate required services and ports
- Network load of critical systems are limited to the extent to make the systems continue to work under maximum load. For example, limit the number of broadcasts in the power-system components.

The described security aspect may not always yet prescribed or according user philosophy mandatory used, but maybe needed in the future due to new regulations or adaptation of the user philosophy and therefore it is recommended to consider already now when buying new protection devices that the security function are implemented and can be activated at any time needed. That ensures that a Todays investment is sustainable also for the future.

This APN application note will give a good overview about the possibilities related to Cybersecurity functions what can be activated at any time the need may arise and how to set them up. More detailed instructions and information can be found in the referred documents listed in chapter 6.

1.2 Securely Resetting the Device Configuration

The described measures in this APN application note are meant to ensure the security of the devices concerning their interactions with external components. There is however always a risk to lock the access for themselves in a way that the only way to un-lock this access can be done in the Siemens factory. Possible root-causes are mistakes during set-up of the Cybersecurity functionality, failure of an external component like RADIUS Server needed for role-based access control (RBAC), data for the access like passwords were lost or the Security administrator in charge to manage these data is no longer available.

In the first chapter the counter measures (Security Credentials and Configuration Reset and Secure Factory Reset) are described to ensure that the access to the devices can be re-established in case the above-mentioned problems happen. This functionality is available in SIPROTEC 5 since version V7.90.

Additionally, the user should always consider the rules for „operational cybersecurity ", meaning sticking to the security processes like keeping security relevant data save in order to avoid that nobody without clearance can use them.

1.2.1 General

Latest during commissioning but better already during set up of project parameterization the process of storing back-up files for resetting of the credentials needed for accessing the SIPROTEC 5 / SIPROTEC 5 Compact devices should be started. This ensures that the access can be restored at any time in case some problems may occur.

Following files can be stored for this purpose:

- **S**ecure **C**redential and Configuration **R**eset **F**ile = SCRF
  - File for resetting the Credentials and Configuration
  - Only the user accounts which are assigned with the role SECADM or Administrator have the authority to download the SCRF from a device
- **S**ecure **F**actory **R**eset **F**ile = SFRF
  - SFRF file: file for a secure reset to the Factory settings
  - The security administrator role is required for configuring the factory default state

The **reset** via the mentioned files is independent from the user role defined in RBAC and can be done from everyone with access to the files, therefore it mandatory to keep these files in a secure location and ensure that if needed can be accessed from a project member.

Before resetting, you need to consider the following points:

- Each device has a unique SCRF- and SFRS- file, it is therefore necessary to make a back-up via SCRF- and SFRS- files for all devices of the project.
  - An SCRF and SFRS file can only be used to reset the settings of the device from which the files have been down-loaded: to recognize the correct device a clear and unique naming convention of the files should be used.
- You must always exercise utmost care in handling the SCRF and prevent unauthorized access to these files.
  - Because regardless the assigned role(s), everyone can reset the settings of a device by uploading the SCRF or SFRS file into the device. For this reason, the SCRF and SFRS files must be effectively deleted from the PC after resetting
  - The SCRF can always be used to reset the security settings
  - The SFRF can always be used to reset the SIPROTEC 5 device to its factory default state

Attention: This functionality is supported for SIPROTEC 5 / SIPROTEC 5 Compact devices with Firmware V7.90 or higher. Devices delivered since release of V7.90 have these SCRF- and SFRC files loaded inside. In case you want to use this function with devices manufactured earlier our hotline must be contacted to check if that is possible.

1.2.2 Saving and restoring Secure Credentials

Following steps are necessary for downloading the SCRF file:

Downloading of the SCRF-file:

- Connect the SIPROTEC 5 device to a PC using a network cable
- Start DIGSI 5
- Logon as ***Security Administrator*** or ***Administrator (RBAC must be enabled therefore)***
- Select the device
- Open the ***Online*** menu item
- Select ***Security -> Download credentials reset file...***
- Select a storage location on the PC, such as D:\DIGSI5\Projekt-xy\SCRF_SecurityData
- Confirm the action with OK

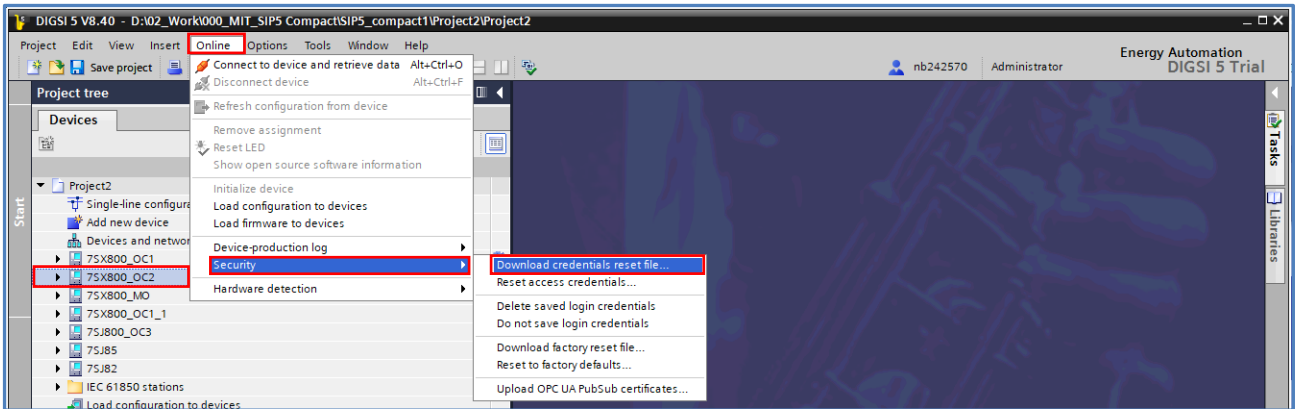


Figure 2.1: Downloading the SCRF-file

Resetting of the Security Settings:

If the connection to the RADIUS server is broken or the emergency access has not been configured, you can reset the device security settings to regain interactive access to the devices where RBAC is activated.

- Save the SCRF on the PC.
- Connect the SIPROTEC 5 device to a PC using a network cable.
- Start DIGSI 5
- Select the device and open the ***Online*** menu item.
- Select ***Security -> Reset access credentials....***
- Transfer the SCRF file to the device.

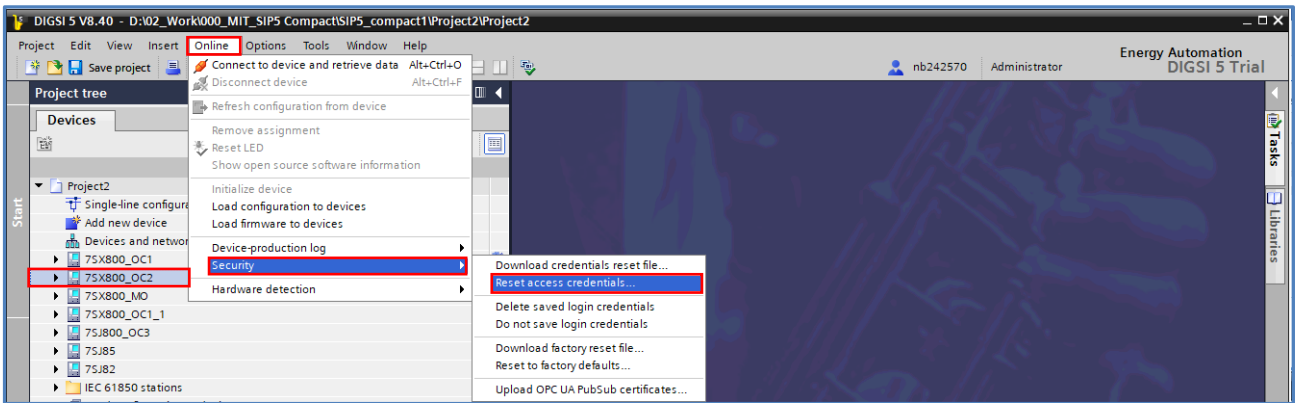


Figure 2.2: Resetting the security settings

When successful, DIGSI shows an information and all security settings are inactive in the SIPROTEC 5 device.

Remark: On the device operation panel and the browser-based user interface, the security settings will not be refreshed after the SCRF is successfully uploaded. To refresh the settings, a reboot is needed. But to avoid impacting the protection functions, the device does not restart automatically. You can select to restart the device according to the actual situation.

1.2.3 Secure Factory Reset

To return a SIPROTEC 5 device to its factory default state, you must first download the signed SFRF file from the device. Following steps are necessary for downloading the SFRF file:

Downloading the SFRF File:

- Connect the SIPROTEC 5 device to a PC using a network cable
- Start DIGSI 5
- Logon as ***Security Administrator (RBAC must be enabled therefore)***
- Select the device
- Select the device and open the ***Online*** menu item
- Select ***Security -> Download factory reset file....***
- Select a storage location on the PC, such as D:\DIGSI5\Projekt-xy\SFRF_SecurityData
- Confirm the action with OK

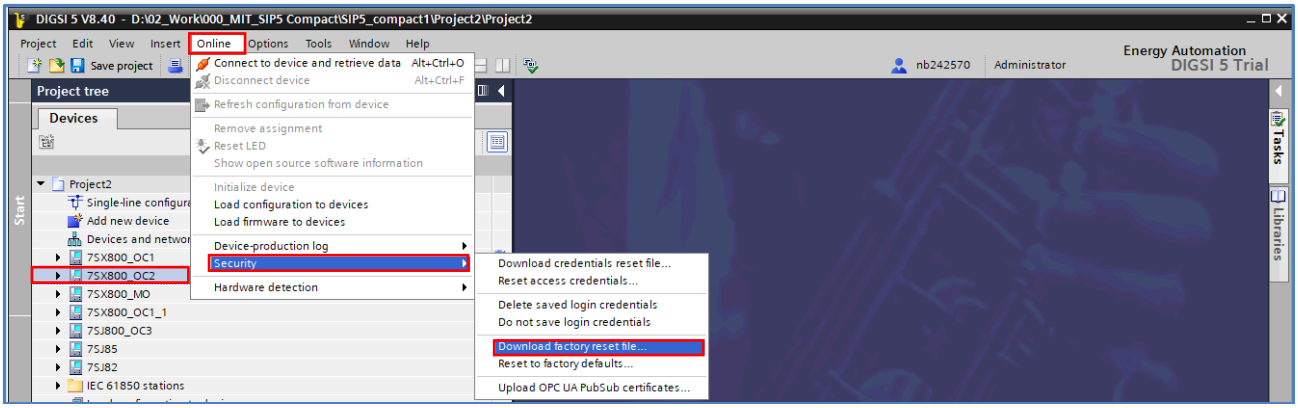


Figure 2.3: Downloading the der SFRF-file

Resetting to the Factory Default State:

- Save the SFRF on the PC.
- Connect the SIPROTEC 5 device to a PC using a network cable.
- Start DIGSI 5
- Select the device and open the ***Online*** menu item.
- Select ***Security -> Reset to factory default....***
- Transfer the SFRF file to the device.

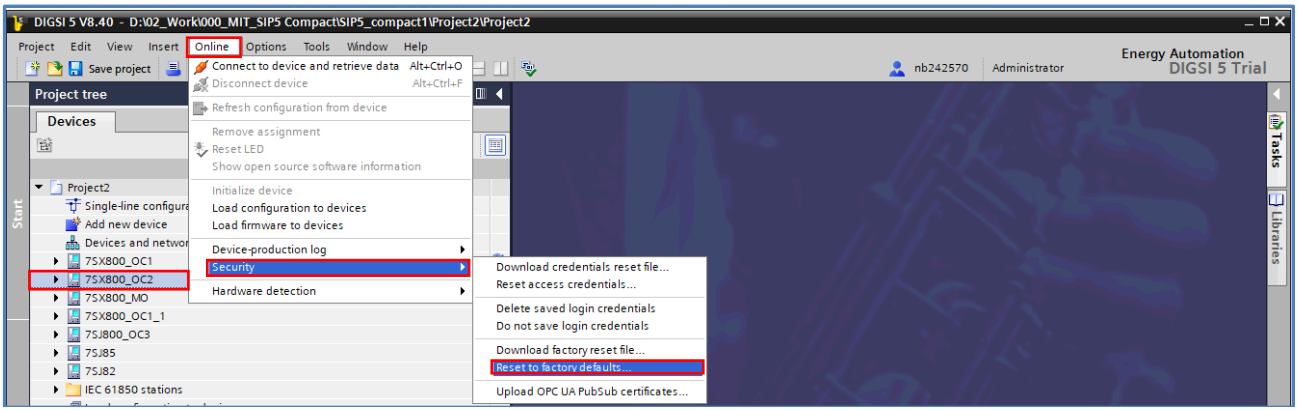


Figure 2.4: Reset to factory default

After restarting the device, the factory default settings are restored.

Remark: All data on the device as well as the security and protection settings are cleared upon loading the SFRF file.

1.3 Access Control

SIPROTEC 5 devices support user authentication and operations for protecting access to the security-relevant operations and functions. You can select between the centralized Role-Based Access Control (RBAC) option and the device-specific DIGSI 5 connection password option.

If you do not intend to use the RBAC feature, set up the devices to conduct a user authentication using the connection password.

Furthermore, if RBAC is disabled, to prevent you from executing safety-critical actions on the device unintentionally, you can set up confirmation IDs.

Further Information can be found:

- Access Control and Connection Password:
  [4] SIPROTEC 5 Security – Manual in chapter 3.1
  [6] DIGSI 5 Software Description Help – Manual in chapter 17.8.1
- Role-Based Access Control (RBAC)
  [4] SIPROTEC 5 Security – Manual in chapter 3.2
  [6] DIGSI 5 Software Description Help – Manual in chapter 17.8.2

The see and/or change of the default settings for Access Control you must select in the **Project navigation** of the device the menu point **Safety and Security -> Operations safety and access control**.

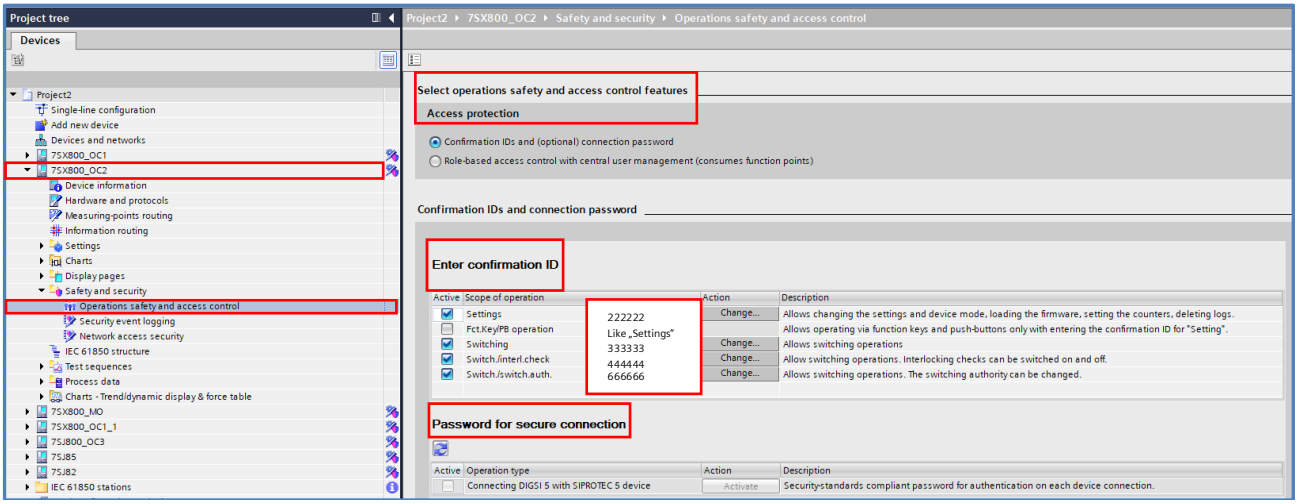


Figure 3.1: Access protection

In the default settings only the configuration IDs are pre-selected, the pre-set codes are listed in [6] DIGSI 5 Software Description Help – Manual in chapter 17.8.1. Our recommendation is to leave the confirmation IDs always active, exceptionally you can deactivate them during tests and commissioning for faster working

Figure 3.1 shows the „Default values", changing them is recommended and always possible.

The use of a Password for secure connection or the Role-Based Access Control (RBAC) are optional and can be activated at any time. Our recommendation it to use at least a Password for secure connection.

1.3.1 Password for secure connection

The connection password follows the NERC-CIP-standard (North American Electric Reliability Critical Infrastructure Protection) and consists of the following parts:

- Lower-case letters
- Upper-case letters
- Digits
- Special characters, for example, %, &, $

The length of the connection password ranges from 8 characters to 24 characters. DIGSI 5 verifies the length during entry.

The connection password is empty by default. To enter a new connection password, the existing characters are concealed by asterisks. To confirm the connection password, enter it twice. This confirmation prevents erroneous entries.

Note:
The deactivation of the connection password results in providing everyone unauthenticated and unrestricted access to the device through DIGSI 5 or through the browser-based user interface. If you wish to hinder this, set the connection password in the device.

The Activation / Modification of the connection password can only be done when the device has an online connection and active communication with the DIGSI 5 PC.

Once you enter a new connection password, DIGSI 5 transfers it to the device automatically. Initialization of the connection password is possible only via the front USB interface or via an Ethernet interface of the device.

In both cases, the entered connection password is securely transferred to the device via the TLS protocol. The connection password is not stored in the DIGSI 5 project or anywhere on the Windows PC. It is stored as a salted hash in the device.

If you have initialized the connection password, further access to the device (via DIGSI 5 or via the browser-based user interface) is possible only if you enter the correct connection password in the DIGSI 5 dialog while establishing a connection to the device. This procedure prevents unauthenticated access. Siemens recommends checking the connection password after initialization.

By pressing the „button“ (Figure 3.2) when online and active connected to the device the actual status of the connection password (password set/not set) can be checked and will be transferred from the device to DIGSI 5. If the connection password is activated the access is only possible after entering the correct password.

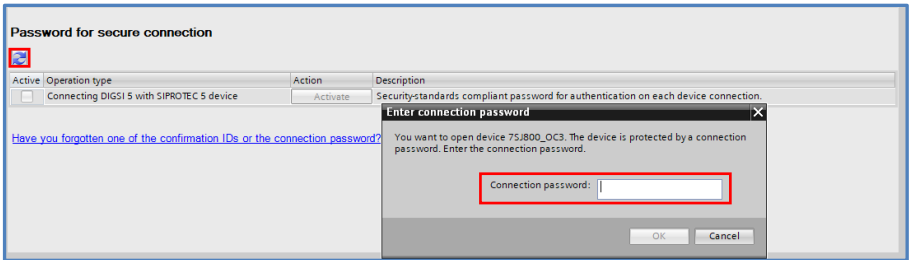


Figure 3.2: Checking status of the connection password

After entree of the password the checkbox for „active“ is set and it is possible to change this and also the password itself (Figure 3.3)

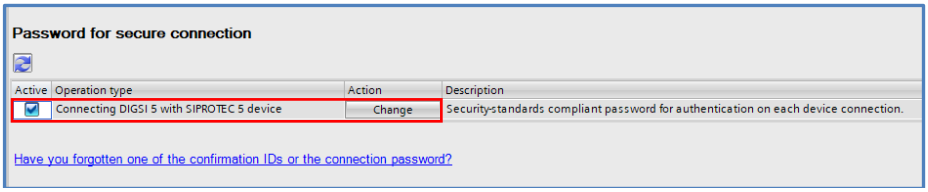


Figure 3.3: Online connection active and Password activated

The default setting is that the connection password is not activated as shown in Figure 3.4. With an active online connection the connection password can now be entered after pressing the button „activate".

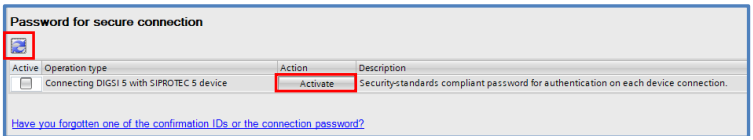


Figure 3.4: Active connection to the device and password not yet activated

After pressing the button „activate" a new dialog-box is opened for entering the connection password and confirmation of the password. Finalization via pressing the „OK" button will start the transmission of the setting to the device. After successful transmission a dialog box will indicate the success and confirm the activation of the connection password.

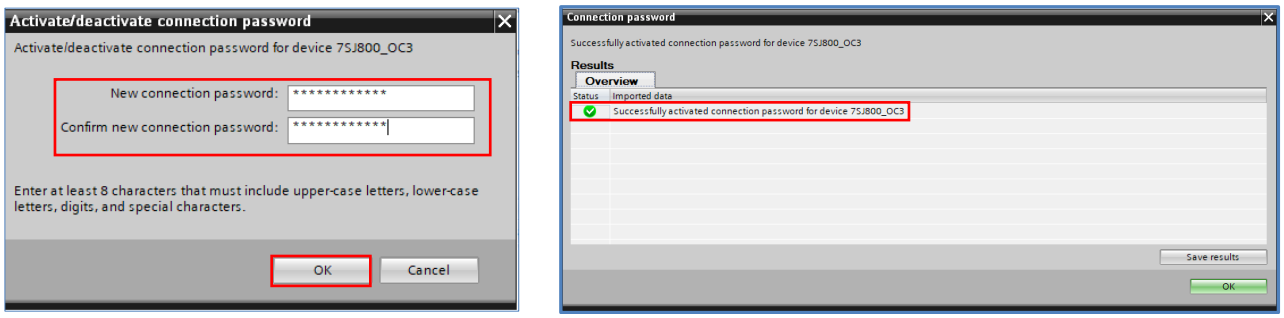


Figure 3.5: Entering the connection password and transmission in the device

The 1st sequence between DIGSI 5 and the device is an authentication procedure based on the TLS protocol in which digital certificates are exchanged between DIGSI 5 and the device. This procedure ensures that only DIGSI 5 can have full engineering access to a SIPROTEC 5 device. If other applications try to gain access, they are blocked.

Following the TLS authentication, the SIPROTEC 5 device queries the connection password if you have set a connection password in the device.

To gain access to the device, you need to enter the correct connection password. If you enter a wrong connection password, device records this action in the security log. If you enter wrong connection password for 5 times, access to the device is blocked for 5 minutes. These operations are recorded in the security log of the device as well.

The activation of a connection password is a very simple but powerful measure for protecting the access from a DIGSI 5 PC (from 3rd party user) to your SIPROTEC 5 device.

If you forget the set connection-password, before deactivating it, you can reset it. How to do this is described in [4] SIPROTEC 5 Security – Manual chapter 3.1.4 or in [6] DIGSI 5 Software Description Help – Manual chapter 17.8.9.

In the next chapter an higher protection method will be described; resetting is with this method not easily possible; how that can be done is described in chapter 2 and is very important to be considered together with the Role-based Access control (RBAC) in case the passwords are "lost".

1.3.2 Role-Based Access Control (RBAC)

This application note shows the necessary settings in DIGSI 5 and for the SIROTEC 5 compact devices. Precondition is that all **necessary preparations, like settings in the RADIUS Server, what will used for the connection and communication with the DIGSI-PC and the SIROTEC 5 compact devices, already has been done and tested and the connection to the RADIUS server is active running and a communication between the partners is possible**. How to set up a RADIUS Server for our purpose is described in [1] „Setting up RBAC for Siemens Digital Grid Products".

To protect access to a SIPROTEC 5 device for performing security-relevant operations and functions, you can activate the RBAC feature. After activation, all users will be uniquely authenticated and authorized with their centrally managed user accounts as for each access attempt.

You can connect all SIPROTEC 5 devices to a RADIUS server (**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice) where the user accounts and authorization information are centrally managed. RADIUS is a client/server protocol; the client implementation is integrated in the SIPROTEC 5 device firmware.

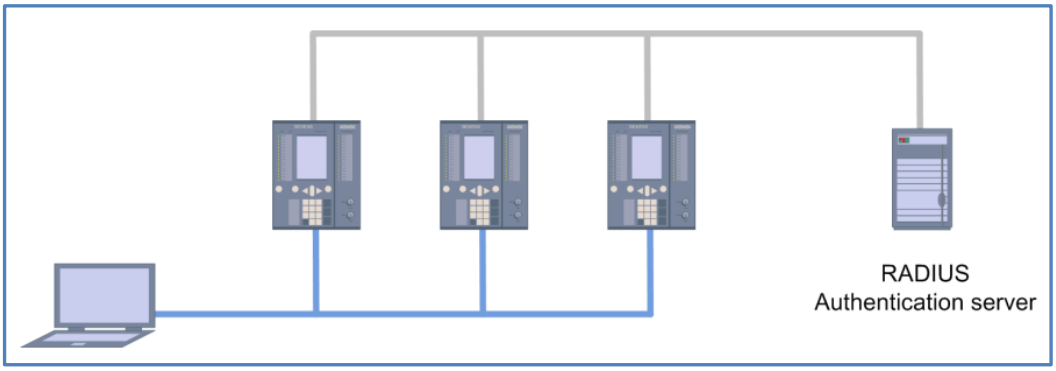


Figure 3.6: RADIUS Authentication-Server

During a user login, the SIPROTEC 5 device sends the username and password to a RADIUS server. This RADIUS server checks the user credentials and, in case of successful authentication, sends the assigned roles of the specific user back to the SIPROTEC 5 device.

SIPROTEC 5 devices support RBAC with predefined standards-based roles. User accounts are assigned roles; roles receive rights according to their functions. The assignment between users and roles is defined in the configuration for a RADIUS server. The assignment of rights to roles is predefined in the security configuration of the SIPROTEC 5 devices.

SIPROTEC 5 devices support the following requirements:

- Standard roles and roles-to-rights assignments from the IEC 62351-8 and IEEE 1686 standards
- Standard roles and rights recommended in the BDEW white paper
- Centralized management of user accounts, roles, and areas of responsibilities (**A**rea **o**f **R**esponsibility, AoR) in a RADIUS server
- Offline/emergency user account access when the RADIUS server is unreachable

The main tasks of the RADIUS server are user authentication and control of user access rights. During authentication, with unique usernames and passwords, the RADIUS server checks if the connecting users are correctly claimed.

If the user is clearly identified, the authorization handles the assignment of the access rights. The user receives specific access rights to data or services of the SIPROTEC 5 device. Furthermore, the access-attempt events are recorded for later analysis (audit trail).

The following information is recorded:

- Connection attempts
- Username and role information
- Time of login

The process chain for establishing a communication connection from the DIGSI 5 PC to a SIPROTEC 5 device with RADIUS Server (and additionally involvement of an „Active Directory" Server for central management of the users / user groups is of course also possible) is shown in Figure 3.7

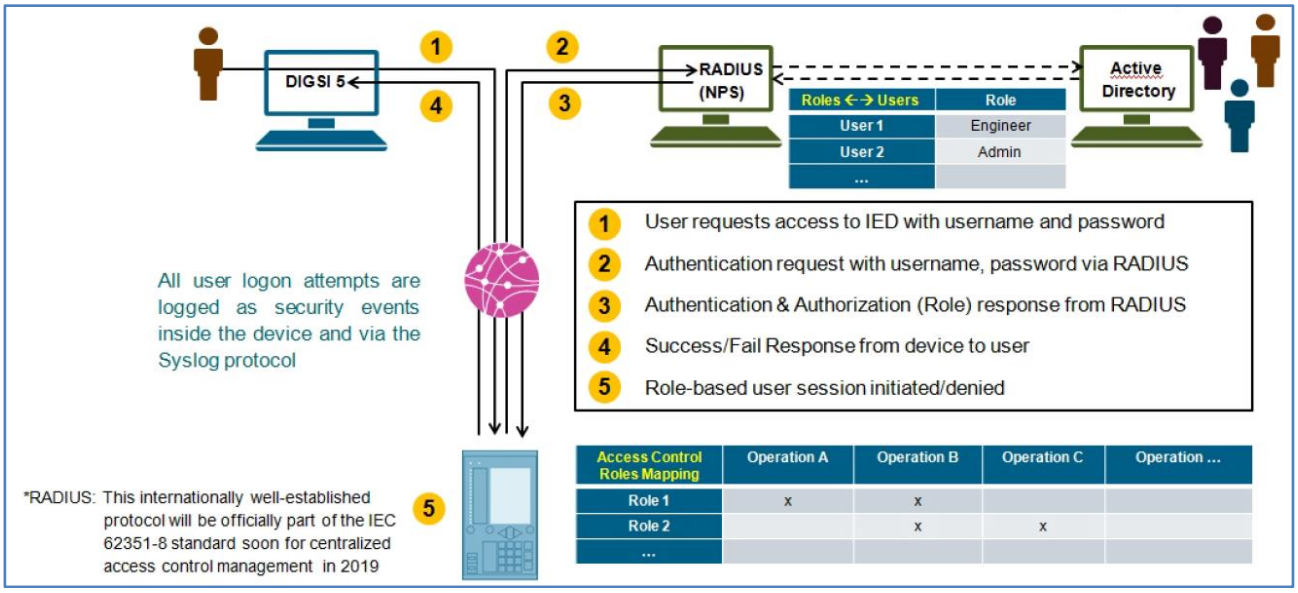


Figure 3.7: Process with RADIUS Authentication-Server

The following steps are necessary before an access to a SIPROTEC 5 device according to the defined role of a user is released:

1. The User requests the access to the device (e.g. to load parameter or establish an online connection). With activated RBAC function a dialog-box will open, and the user must enter his credentials (username and password)
2. The SIPROTEC 5 device will forward this request including username and password to the RADIUS Server
3. In the RADIUS Server the credentials are checked if they are known and correct (check via the „Active Directory" connection if additionally there in case this is also set up) and what role and rights are assigned to the user. The result of the check is transmitted back form the RADIUS Server to the SIPROTEC 5 device.
4. Depending on the result of the check in the RADIUS Server, the access is granted to the user with his assigned rights or the access is rejected.
5. The session between DIGSI and the SIPROTEC 5 device is started when the check was ok, and the user can do the action only what are allowed for his assigned role.

A role is a combination of rights defined for the SIPROTEC 5 device. You can assign a role to users in various contexts. The roles a user has in specific contexts determines what the user is or is not allowed to do in the SIPROTEC 5 device.

The following tables show the overview of the basics of rights and supported roles according to:

- IEEE 1686
- BDEW white paper
- IEC 62351-8 standard
- SIPROTEC 5 operational requirement

Details are described in [4] SIPROTEC 5 Security – Manual Chapter 3.2.8 and 3.2.9 (user roles for direct access from the SIPROTEC 5 device display).

1.3.2.1 RADIUS Server Settings

To activate RBAC, you first must make the following settings via DIGSI 5. You can activate up to 2 RADIUS Servers.

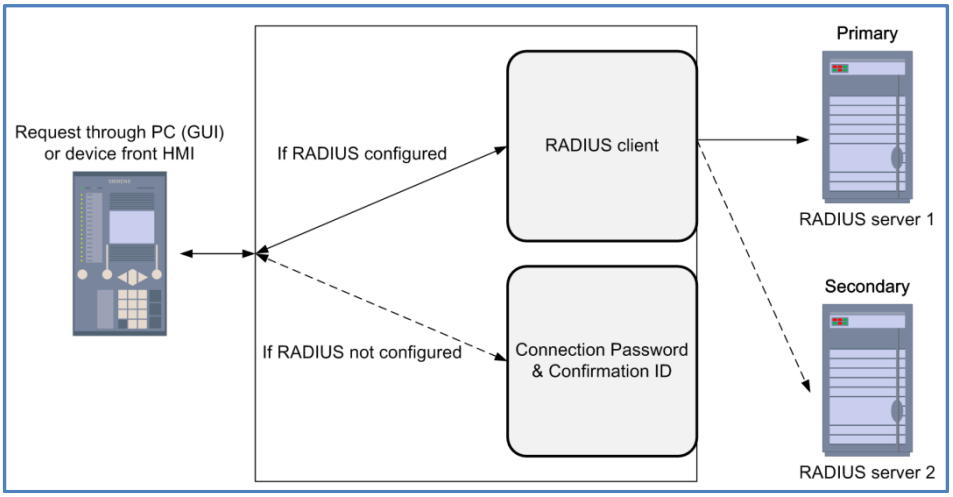


Figure 3.8: Connection between DIGSI PC / SIPROTEC 5 device and RADIUS Authentication-Server

To activate RBAC, you first must make the following settings via DIGSI 5. You can activate up to 2 RADIUS Servers:

- Open a project in DIGSI 5.
- Open the Safety and security menu item in the project tree.
- Double-click the Operations safety and access control menu item.

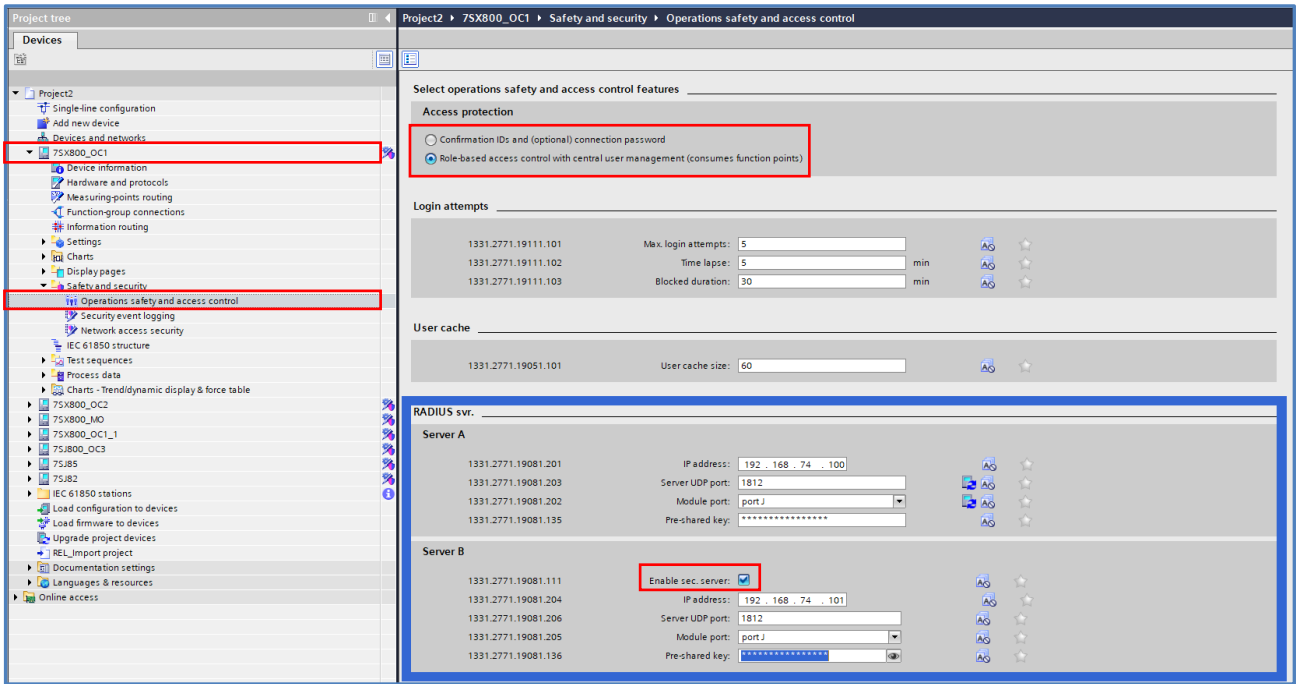


Figure 3.9: Activation of the RBAC function and settings

- If the connection password is activated in the Confirmation IDs and connection password section, deactivate it (see chapter 3.1; Figure 3.3 unhook in case the “active” was set)
- Activate the RBAC feature under ***Access Protection*** in the DIGSI Main working area

After activation the settings for the connection to the RADIUS server and additional settings will be visible. These settings will normally be provided from the security expert who set up the RADIUS Server because it must be assured that:

- All components are in the same Ethernet subnet. The settings for the IP-Addresses for the Radius Server and of the Ethernet access points of the DIGSI PC and the Ethernet modules of the SIPROTEC devices must fit to each (Parameter: IP-address / Module port)
- That the configured port set in the RADIUS client (SIPROTEC 5) for the connection to the PADIUS Server is identical to the settings in the RADIUS Server (Parameter: Server UDP-Port)
- The connection is secure and encrypted; that is done via a „**P**re-**S**hared **K**ey, what has been set and defined on the side of the RADIUS Server and this key must be entered here (Parameter: Pre-shared key)

In a concept with redundant RADIUS Server like shown in Figure 3.8 and 3.9 it is necessary to activate and set up also the second RADIUS Server.

You can configure the following parameters to handle incorrect login attempts:

- **Max.login_attempts:**
  With this parameter, you set the maximum number of sequential login attempts for a user.
- **Time_lapse:**
  With this parameter, you set the time range after which the number of login attempts is set back to 0 after the last unsuccessful attempt
- **Blocked_duration:**
  With this parameter, you set the time duration for which the device remains blocked after the maximum number of login attempts is reached. If you log on with wrong credentials, the login attempts are counted. Once the maximum number of login attempts has been reached, logging on is not possible for the set Blocked duration. If this Blocked duration has elapsed, login can be attempted again.
- **User_Cache_Size:**
  With the RBAC user-cache feature enabled, the device caches user credentials that have been successfully authenticated by the RADIUS server. When the RADIUS server connectivity is interrupted, such users can log on to the device with their cached user credentials and operate the device with their cached roles. Each time a user logs on successfully, the device updates the corresponding user-cache entry with the latest credentials (the username and the hashed password) and the role(s). With the parameter User cache size, you define the maximum number of cached user accounts. To disable the user-cache feature, set the size to 0.

Remark:

- The device time is not synchronized with a central time server and is earlier than the total of the login-blocked time and the Blocked duration; therefore Siemens strongly recommends to use a time synchronization of the SIPROTEC devices from a time server (e.g. SNTP Server, IRIG B time server, IEEE1588)
- Consider that no emergency account exists after RBAC is activated. (chapter 3.3)

Please consider that after finishing the settings the Security setting must be downloaded into the device; security settings are not downloaded together with the configuration settings but separate. This considers that role-based access control maybe used (only with the role SECADM or Administrator have the right to do this).

Important: There must be an active and running communication to the RADIUS Server because already during loading the new Security Settings a check of username, password and assigned role is done, if no RADIUS Server is connected the action will be rejected..

Even in case no RBAC functionality is set the downloading of the Security settings into the SIPROTEC 5 device must be done, in this case either the default settings are transferred to the device or modification related to the connection password or to the confirmation IDs or to the network access security.

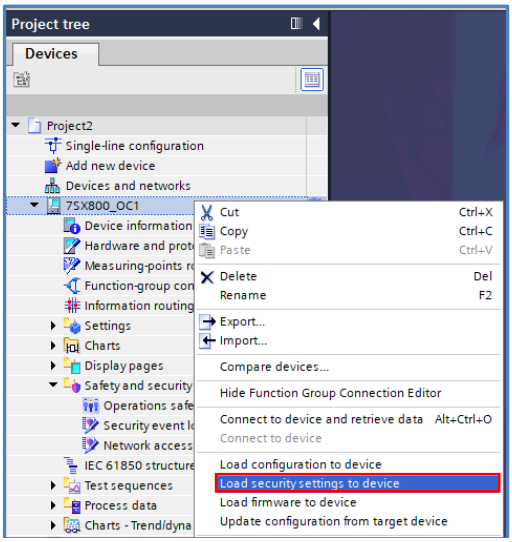


Figure 3.10: Menu item Load security settings to device

1.3.2.2 RBAC access via the Device Operation Panel

The role-based access control has not only to be assured in case the connection is established for the DIGSI setting-PC but also for direct access via the SIPROTEC 5 operation panel. How that is done is described in [1] „Setting up RBAC for Siemens Digital Grid Products“.

The roles are according to the standard IEC 62351-8 and additionally for the operation of SIPROTEC 5 devices necessary defined roles. User authentication and authorization start with the SIPROTEC 5 device. In this case, the device is the RADIUS client and sends an access request to the RADIUS server. This request contains the user credentials.

Figure 3.11: Login to the SIPROTEC 5 device with RBAC

Log on to the Device

Proceed as follows:

- Press the **Login** softkey on the device
  => A user-name selection appears in the lower area of the device display.
- Use the up and down navigation keys to select your intended username or enter a user ID.
- Confirm the selection by pressing the **OK** softkey
  => The prompt for entering the passcode appears
- Enter the numerical passcode
- Complete the input with the Enter **Softkey**

1.3.2.3 Role-Based Views in DIGSI 5

The Administrator role is automatically active in DIGSI 5 in case no role-based access control is activated to ensure that the user has the rights for all possible activities.

With activated RBAC function after opening DIGSI 5, the UI display adapts to the respective roles with which the user has logged in to the Windows session. When you launch DIGSI 5, your username as per the Windows login session and your supported role(s) are displayed on the top right side of the DIGSI 5 UI.

If you still want to restrict your access to DIGSI 5 functionalities to prevent unintended changes to the project, you may do so by manually selecting a specific role for your current DIGSI 5 session. You can click the **username or the supported role** (in figure 3.12: **nb242570 / Administrator**) to open the Select role(s) dialog and select the required role. The permissions associated with each role are mentioned in the Select role(s) dialog.

In the Project tree it is visible that a user with Administrator role / rights is having access to all settings

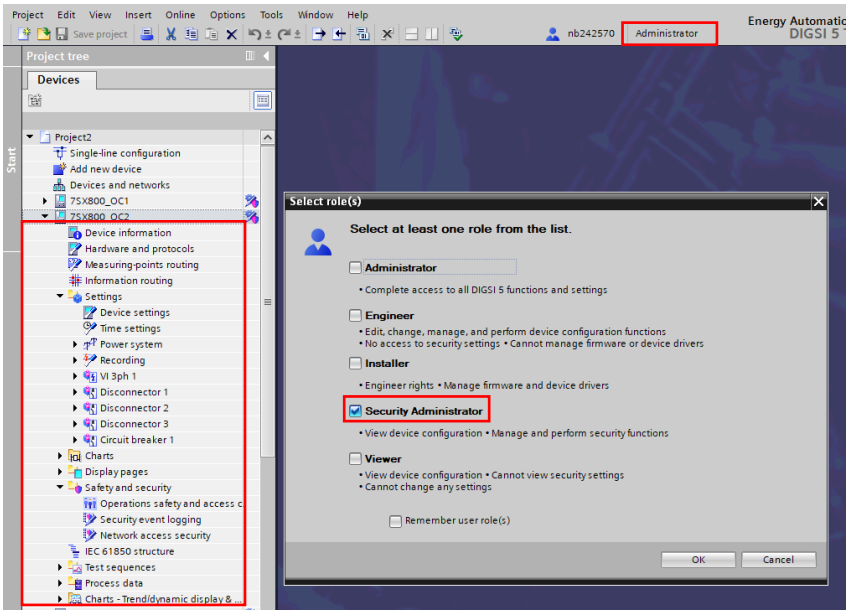


Figure 3.12: Menu tree of Administrator user

After the view has been changed from Administrator -> Security Administrator the menu structure will also change (Figure 3.13), and the limited access points of this role are visible only. Some menu items contain settings what needs to be accessible as well for the protection engineer and also for the Security Administrator; therefore, the menu item Hardware and protocols is visible. Settings related to the IP-settings fitting to the network structure and enabling services like webserver or module homepage is related with the role of the Security Administrator and can be modified from him. Other settings like the selection of the communication protocol is only visible for him but cannot be modified.

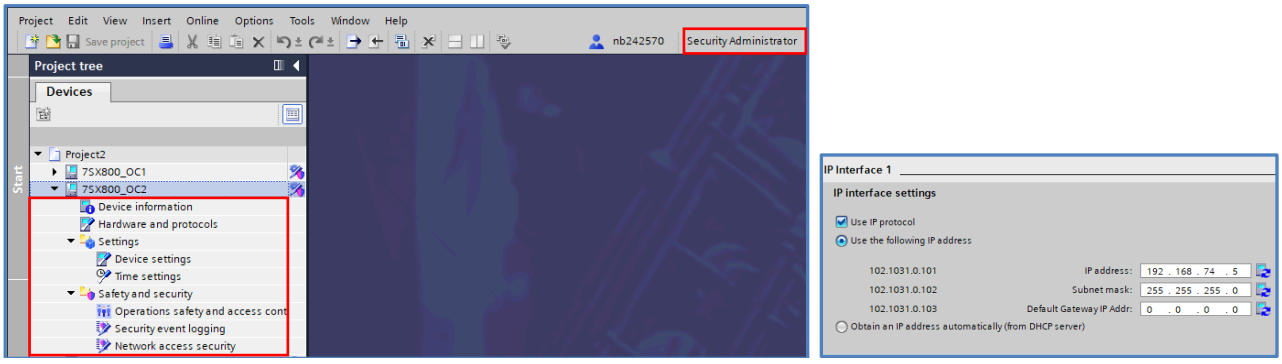


Figure 3.13: Menu tree of Security Administrator user

1.3.3 Emergency Access

If the RADIUS server cannot be reached when logging on to the device and you cannot log on as a user, you can log on to the device using the emergency access.

It is recommended configuring the emergency access for DIGSI 5 and the on-site operation during the device commissioning or during the configuration of the cyber-security parameters.

Before activating the emergency account, consider the following points:

- You use the emergency access only if you do not have access to the configured RADIUS server(s) and an active communication between the devices (SIPROTEC 5 and DIGSI 5 -PC) and the RADIUS Server is established. and the RBAC configuration already has been downloaded into the SIPROTEC 5 devices.
- The SIPROTEC 5 device needs to have an active connection and communication to the RADIUS server
- After setup of the emergency access this access is only working for the use case that the RADIUS servers are not reachable.
  In der dialog-box (e.g. during loading changes into the device) both access options are visible, but:
  - If the RADIUS Server is accessible, an access via emergency access will be rejected
  - If the RADIUS Server is **not** accessible, an access via emergency access will be granted
- The configuration of emergency access requires the security-administrator role.

Activating the Emergency Account

- Start DIGSI 5
- Open the project in DIGSI 5
- Switch to the **Safety and security** menu item in the project tree
- Double-click the **Operations safety and access control** menu item
- Under **Emergency Account Settings**, click **Configure**

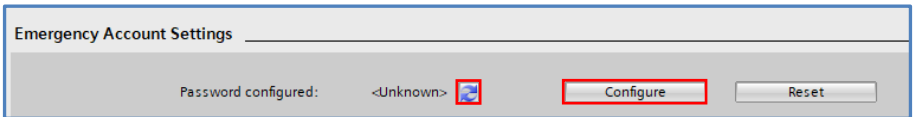


Figure 3.14: Emergency-Account Settings in DIGSI

With the refresh button , you can check the status of the emergency account in the device:

- **Yes:** the emergency password is configured.
- **No:** the emergency password is not configured.
- **Unknown: RBAC** is not active in the device.

For on-site operation of the device, enter an emergency password that is at least 6 numbers long. The emergency password for on-site operation can be entered only directly on the device operation panel.

For operation via DIGSI 5, enter an emergency password with at least 8 characters, which must consist of upper-case letters, lower-case letters, numbers, and special characters. The emergency password for DIGSI access can be entered only via DIGSI 5.

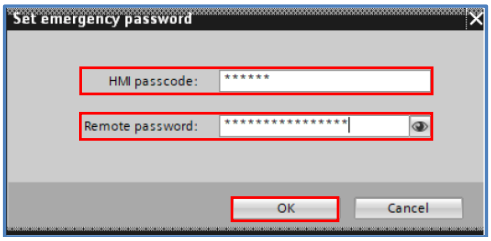


Figure 3.15: Dialog for Entering the Emergency Passwords

Confirm the input with **OK**. Now, the emergency access with the same rights as the role Administrator is granted.

1.3.4 Access via own user certificates

The access from the DIGSI PC to the SIPROTEC 5 devices is always protected via certificates. The certificates are installed during installation of the DIGSI program and are loaded into the SIPROTEC 5 devices during manufacturing. These certificates are Siemens manufacturer certificates. An enhanced protection can be reached by replacing the Siemens manufacturer certificates with own ones. When using own certificates only user with these certificates installed into their DIGSI PC and their SIPROTEC 5 devices can have access. How this is done is described in the next chapter.

1.4 Communication Security

Additional to the measures and methods described in the last chapter focusing on access control allowing only access to a SIPROTEC 5 devices via password (connection password or the „credential" stored on a RADIUS Server namely username, password and assigned role for this credentials) the focus in this chapter are additional measures concerning securing the communication. These measures can be used as well instead of the measures described in the last chapter or additionally and parallel to them.

1.4.1 Ethernet Access Restrictions

Via the security settings, you can restrict the access rights of a DIGSI 5 connection for each Ethernet interface.

You can set the security settings in DIGSI 5 in the Project tree under Safety and security **-> Network access security**.

You can set the following access rights:

- **No access**
  No DIGSI communication is possible via this interface.
- **Read-only access**
  You only have read access to the device via this interface.
- **Read and write access**
  Read and write access to the device is possible via this interface.

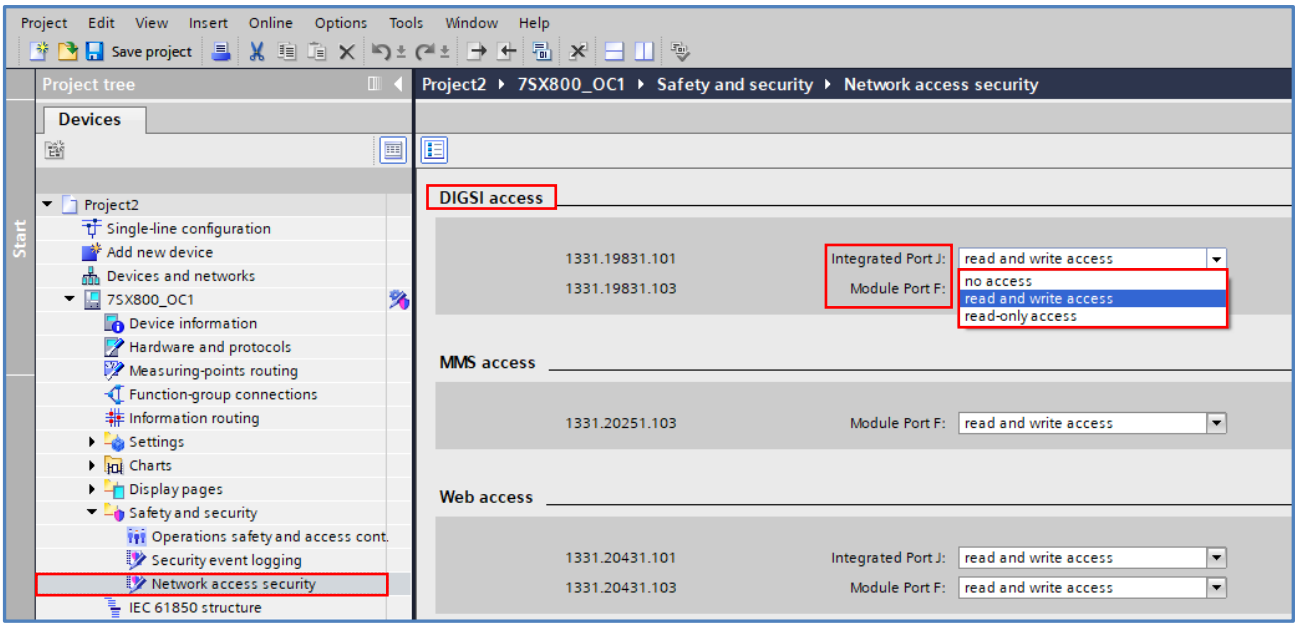


Figure 4.1: Define access right for DIGSI

1.4.2 DIGSI 5 access right with Certificates

With the new feature DIGSI Client authentication, you can use your own digital certificates in the DIGSI 5 program for the secure communication between DIGSI 5 and the SIPROTEC 5 device.
Once this feature is configured, a connection to a device using a standard DIGSI 5 version with the embedded default Siemens client certificate is not possible anymore. This prevents unauthorized Windows users with DIGSI 5 installations from accessing operational SIPROTEC 5 devices.

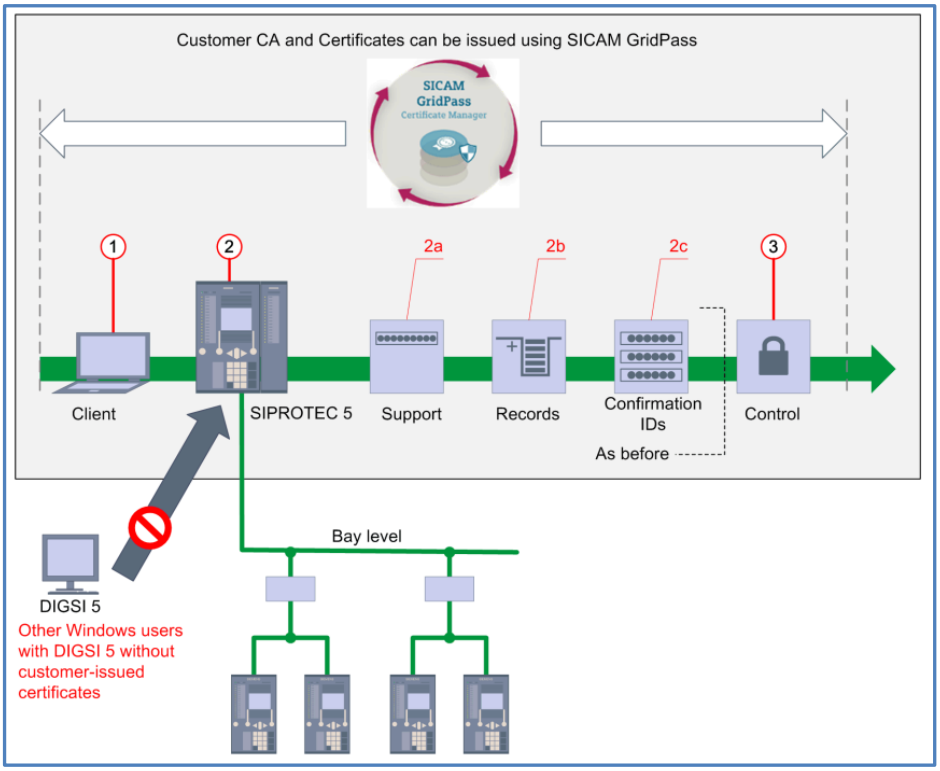


Figure 4.2: Schematic Representation of the Security Feature

1 Installation of customer-issued client certificate in the Windows user account (client authorization).

2 Installation of the customer CA used to sign the DIGSI 5 client certificates in the device

2a Device-side support for role-based access control including central user management and emergency access

2b Recording of security-relevant events and alarms via Syslog and recording in non-volatile security logs in the device

2c Confirmation IDs for safety-critical operations

3 Mutually authenticated and encrypted communication between DIGSI 5 and the SIPROTEC 5 device.

The security measures 2a to 2c are independent from the here described functionality and can either be set up and used and are running than additionally and parallel or in case they are not set and used are not influencing the access control via certificates.

While establishing the connection with a SIPROTEC 5 device, DIGSI 5 presents its client digital certificate (hereafter called **client certificate**) to the device for authentication purposes. If you want your DIGSI 5 installation to use your own client certificates instead of Siemens default certificates, then you need a Public Key Infrastructure (PKI) with an operational Certificate Authority (CA) that you can use to issue or digitally sign such client certificates.

Necessary steps – preparational tasks:

When own certificates are used for securing the access from the DIGSI 5 PC some preparational tasks must done first for creating and manage the certificates. This preparation is normally done from the Security Expert and the certificates are then handed over to the Engineer. Some activities are needed once per DIGSI 5 PC / User and others are needed per SIPROTEC 5 device. According to the recommendation and regulations for the validity duration for certificates (1 year) it is necessary to repeat most of the task cyclically.

These tasks can be automated when using a **central Certificate Management** Tool like **SICAM GridPass**, what are take care about singing and renewal of the used and needed certificated before they expire. This is done via EST protocol (**E**nrollment over **S**ecure **T**ransport protocol). Detailed information are available in [7] „SICAM GridPass – Manual".

The needed necessary steps will be described in the following chapters; indicating what steps could be handled automatically when using a **central Certificate Management** Tool supporting EST protocol.

While establishing the connection with a SIPROTEC 5 device, DIGSI 5 presents its client digital certificate (hereafter called **client certificate**) to the device for authentication purposes. If you want your DIGSI 5 installation to use your own client certificates instead of Siemens default certificates, then you need a Public Key Infrastructure (PKI) with an operational Certificate Authority (CA) that you can use to issue or digitally sign such client certificates.

Two or three (when following the recommendation to use a central Certificate Management Tool supporting EST protocol) „partners" are involved in the process:

1. **DIGSI PC / DIGSI user**
2. **SIPROTEC 5 protection devices**
3. **Certificate Management Tools (recommended, but not mandatory)**

1. DIGSI PC / DIGSI user - preparational tasks:

To configure the new feature DIGSI Client authentication, proceed as follows:

a. Setup a DIGSI 5 CA store (CA = Certificate Authority)
b. Configure the DIGSI 5 Client authentication security feature
c. Import of the user certificate

To ensure that only user with operational access right to establish a connection from their DIGSI PC to the SIPROTEC 5 devices, it is necessary to issue a client certificate for these users and import this personalized client certificate to his DIGSI-5 PC. The issuer of this client certificate, called Certificate Authority (CA), needs to be known on the DIGSI 5 PC and can be trusted; an import of the CA public certificate must be therefore imported and placed into the DIGSI 5 CA store.

SICAM GridPass can be used to create and sign all needed certificates (figures below) and handed over after export to the user for installing them. Details are described in [7] SICAM GridPass – Manual.

Precondition for the following steps is, that the CA = Certificate Authority is already created in SICAM GridPass. Open SIOCAM GridPass and select under „Certificates" the tile „Certification Authorities" (figure 4.3)

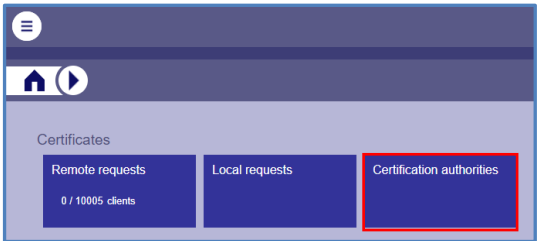


Figure 4.3: UI of SICAM GridPass central Certificate Management Tool

After opening the work-space of „Certification Authorities" search the CA what must be exported (Figure 4.4 SICAM_GridPass_CA") and extent the information area.

To export the Certificate, press the button.

An Export Dialog-box opens; select DER File Format for the Export; this format is expected in DIGSI and does contain only the public key (the private key is not needed) and therefore the export is not protected via PIN (transport key). Start the export by pressing the o.k. button. Store the exported certificate in a save location, it is needed in further steps.

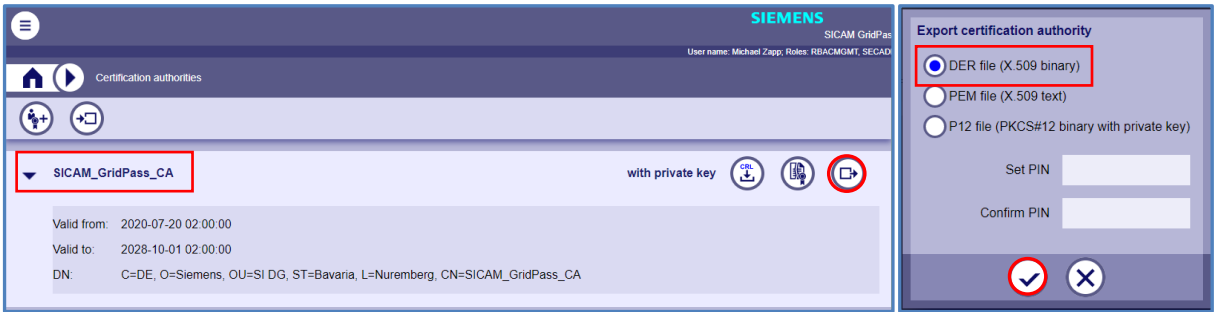


Figure 4.4: Export of CA public certificate from SICAM_GridPass

Remark: When using a central Certificate Management Tool with EST functionality this step is only once necessary, renewal of the certificate is automatically done

In the following steps it is assumed that the certificates are already issued and handed over and the installation steps will be explained.

For **1a. Setup a DIGSI 5 CA store**, please select in the DIGSI main menu (see figure 4.5):
Tools -> Manage certificate authorities (CA)

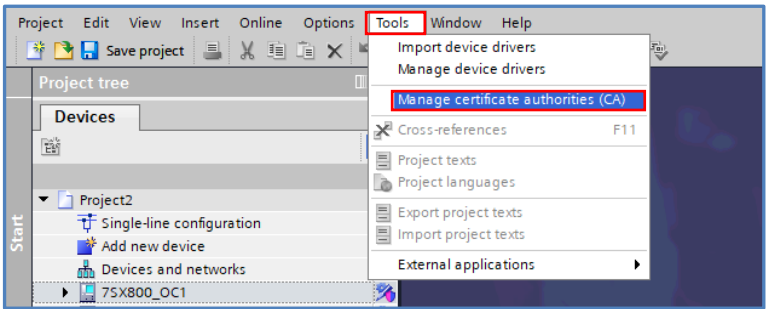


Figure 4.5: Setup DIGSI 5 CA-Store step 1

The certificate of the Certificate Authority (CA) what issued and signed all other needed certificates can be imported in the newly opened main working area (Figure 4.6). This CA present its identification with the "public key", therefore no transport key is needed for the import.

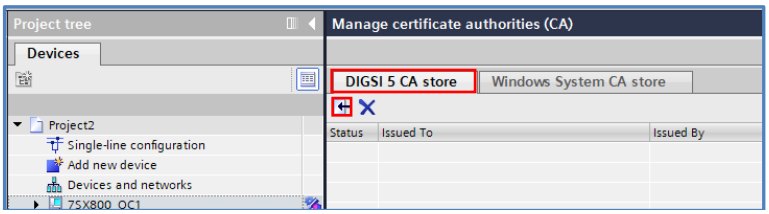


Figure 4.6: Setup DIGSI 5 CA-Store step 2

After pressing the import button  a new Dialog-box (Figure 4.7) opens for selecting the storage location and selection of the certificate to be imported (SICAM_GridPass_CA.der in this example); Remark: *.cer format is expected, either the file extension has already been modified (*.der and *.cer are identical and exchangeable) or enter * for the file name in the dialog box for showing all files.

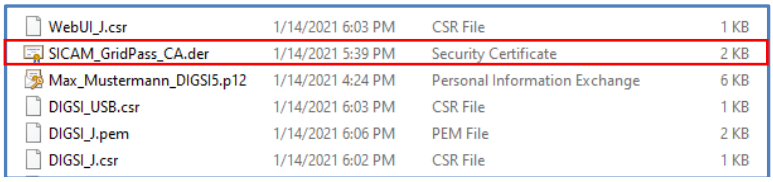


Figure 4.7: Setup DIGSI 5 CA-Store step 3

After pressing „open" the certificate will be imported into the DIGSI 5 CA-Store and can be seen there with its state an expiry date (Figure 4.8).

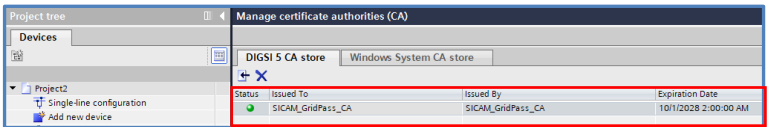


Figure 4.8: DIGSI 5 CA-Store after Import

In case the certificate of the CA Certificate Authority has been already imported to the Windows System CA under trusted CA, you can open the tile Windows System CA-store, search for the certificate and copy it via the button shown in figure 4.9 into the DIGSI 5 CA-store.

The process for importing the CA certificate into the Windows System CA store is identical to the later described import of the User Client certificate; different is only the storage location what must be "trusted Certificate Authorities" (to be visible in DIGSI 5 Windows CA-store) and that no transport key (PIN) is necessary and no passwords needs to be set.

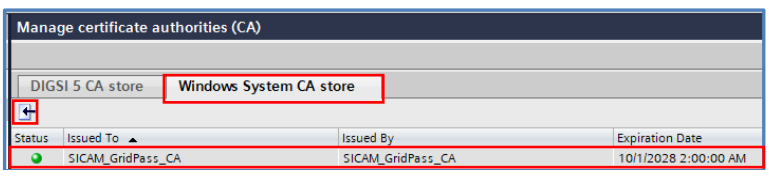


Figure 4.9: Copy from Windows CA store into DIGSI 5 CA-Store

After that done the first part of preparational tasks for the DIGSI PC are nearly done. The certificate authority (CA) what will be used has been imported with its public key and can be selected and used from now on.

The next step is **1b. Configure the DIGSI 5 Client authentication security feature** for informing the SIPROTEC 5 devices what CA must be presented as issuer of the Client certificate from the DIGSI PC / user to the device when trying to establish a connection. This is done in selecting (see Figure 4.10) the trusted CA under: SIPROTEC 5 Device -> Network access security -> Client Auth

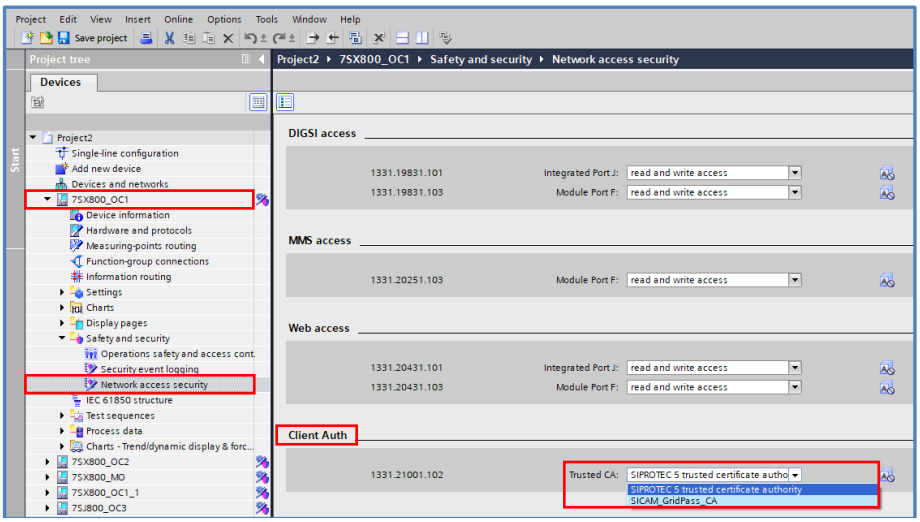


Figure 4.10: Selection of Trusted CA for the Client Authentication

This setting must now be loaded into the SIPROTEC 5 device; To do this (see Figure 4.11) select the device in the project tree and right-click in the context menu -> Load security settings to device.

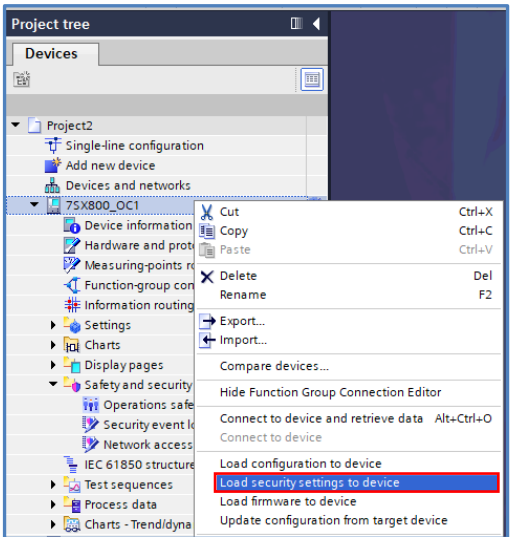


Figure 4.11: Load the setting of the CA to be used into the SIPROTEC 5 device

A check, after loading the security settings, whether the CA to be used in the future really has been transferred into the device, can be checked on the device via the web server.

After access via the web server, select the tiles in the user interface (Figure 4.12):
Certificates -> Certificate authorities
Settings -> Security -> Client Auth

There you can see which certification authority must present its client certificate during checking the DIGSI access to the device for permitting this access (in our example SICAM_GridPass_CA)

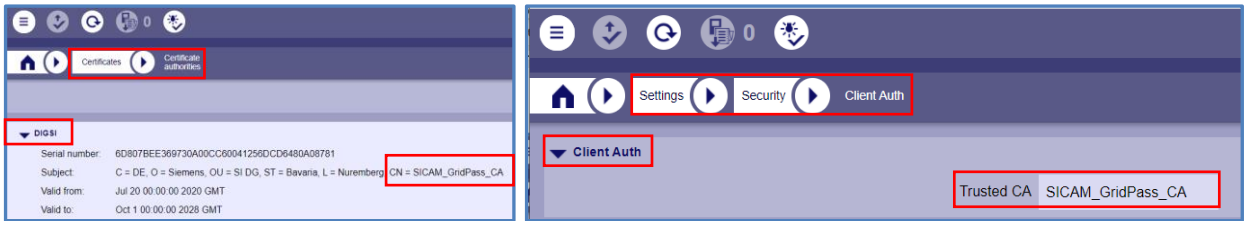


Figure 4.12: Check the CA to be used with the web UI

As next step the client which was created and signed by this CA certificate can be installed on the DIGSI computer **1c. Import of the user certificate** (client certificate).

The necessary certificates can e.g. be created with SICAM GridPass (following figures) and handed over to the user for installation. Details can be found in [7] SICAM GridPass - Manual.

It is assumed that the certification authority to be used has already been created; select the “Local requests” tile under “Certificates” (Figure 4.3).

There (Figure 4.13) add a new certificate by pressing the button.

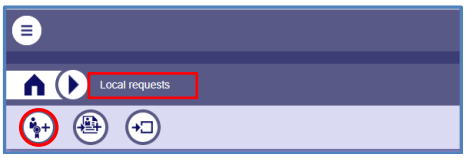


Figure 4.13: Add a new user certificate

The menu for creating a new certificate (Figure 4.14) opens. A TLS client user certificate must be created; Important settings under step 2 are the selection of the correct certification authority (SICAM_GridPass_CA) and the assignment of the user identification for which the certificate is to be issued (Max_Mustermann_DIGSI5). For the creation of a TLS client certificate, all other settings can be left at the default values (validity: recommended max. 365 days, key type: RSA 2048)

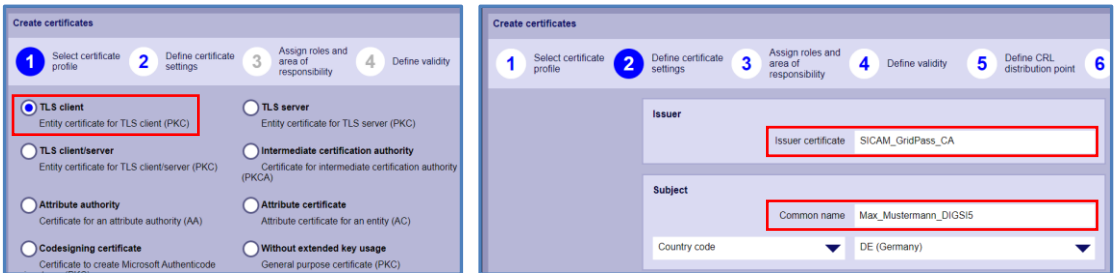


Figure 4.14: Create TLS client user certificate

After completion, the newly created certificate is visible under "Local Requests" and can be exported using the button (Figure 4.15): In the export dialog the p12 file must be selected as file type, since the private key of the certificate is only contained in this format; the purpose of the **user certificate** (client certificate) is to grant only authorized users access from the DIGSI PC to the SIPROTEC Devices and this must be verified,. A transport key (PIN) must therefore be entered when exporting to ensure that this "secret" is protected; the transport PIN is required to install the **user certificate** (client certificate) in the "Certificate vault" on the DIGSI PC.

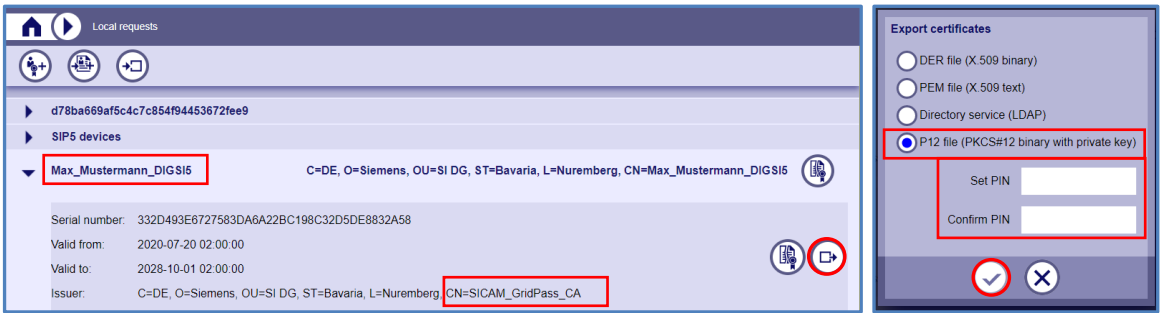


Figure 4.15: Export TLS client user certificate

In the following it is assumed that the user certificate has been created and transferred (Figure 4.16) and it is shown how it is to be installed.

To install the **user certificate**, simply start the process with a double click (or better right mouse and -> run as administrator).

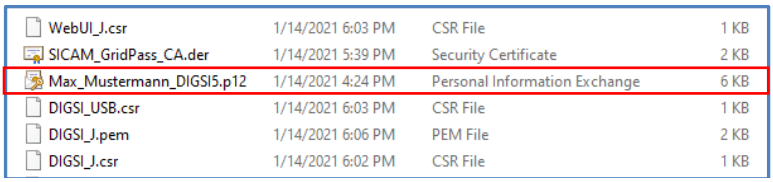


Figure 4.16: Import user certificate

The first dialog box opens (step sequence see Figure 4.17). Since the user certificate should be user-related, the certificate should be imported into the certificate vault of the "current user" (step 1).

In the next step, the file name and the folder is displayed from which the certificate should be imported => confirm with "continue".

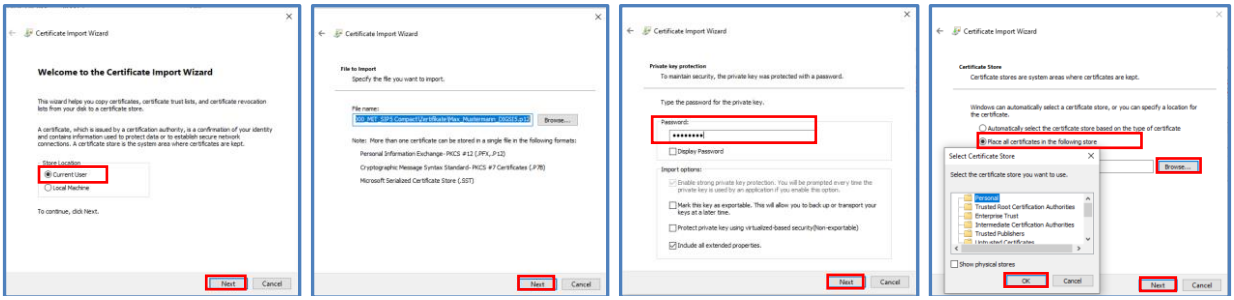
In the next step, the transport PIN must be entered (Figure 4.15), which was used when exporting from SICAM GridPass (or was transferred with the certificate by the Security Administrator). Continue with "next".

The next step is to select the storage location within the “vault” under “Save all certificates in the following storage” and “Search” -> in the new dialog box select “Own certificates”. Then continue with the import with "ok" and "continue".

Now the certificate can be imported, a summary of the settings will be displayed in the next dialog box, if everything is correct, confirm with "Finish".

Since it is a *.p12 certificate with a private key, "Security level" must be selected in the next step. **Attention:** The password that we assign here must be remembered (and eventually stored in a save place), as this password will be needed in the future to establish a connection between the DIGSI PC and the device.

After entering and repeating the password, press “Finish” and in the next window (not shown in Figure 4.17) complete the import with “ok”



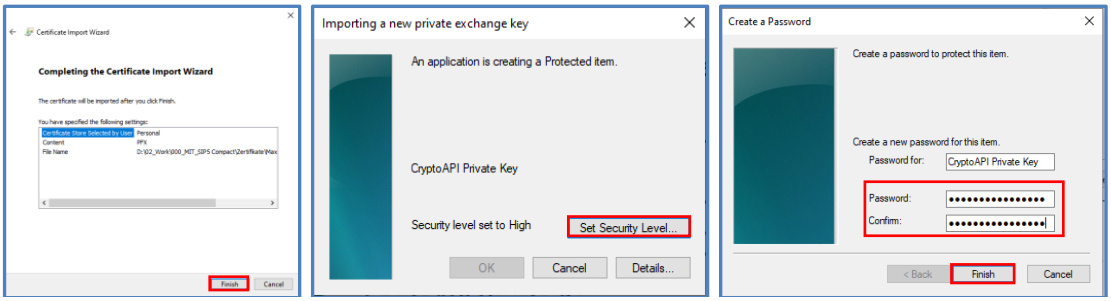


Figure 4.17: Steps for importing the user certificate

To check whether the certificate has actually been imported and is also stored in the correct location in the certificate "safe", the "Microsoft Management Console" can be displayed and started by entering  mmc in the "magnifying glass" next to the Windows symbol. After starting the console, select "File" -> "Add / Remove Snap-in" in the main menu and select "Certificates" in the dialog that opens, press the "Add" button and the following standard settings with "Finish" and "OK" to confirm. Then, as shown in Figure 4.18, select "Certificates - Current User -> Personal -> Certificates" and check in the main window whether the user certificate (in our example: Max_Mustermann_DIGSI5 "is included and the correct CA is displayed as the issuer (SICAM_GridPass_CA))

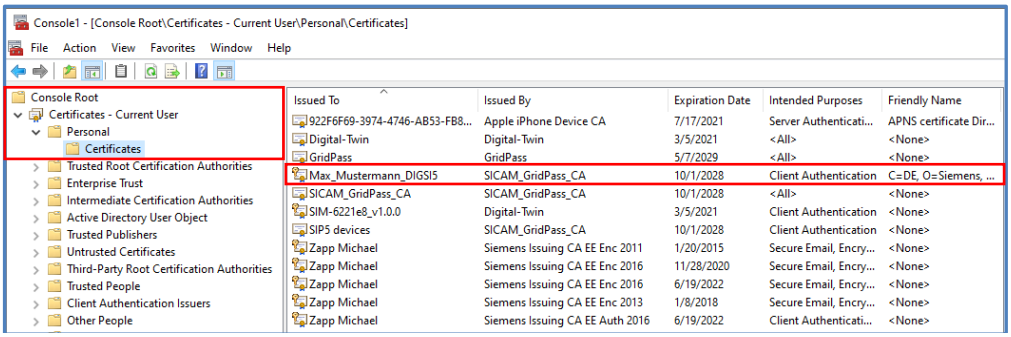


Figure 4.18: Check user certificate import

The preparatory tasks for **DIGSI PC / DIGSI users** are now complete.

Here, too, it should be noted that the imported user certificate has an expiry date (according to Cyber Security recommendation, the validity should be max. 1 year) and must be manually renewed timely, when not using a central certificate management tool, so that the user still will be able connecting to the device . It is therefore advisable to use a central TOOL such as SICAM GridPass with EST functionality so that the certificate is automatically extended before it expires.

SIPROTEC 5 protection devices - preparatory tasks:

The first necessary step for the SIPROTEC 5 protection devices has already been carried out (Figure 4.11). The protection device now knows how the check must take place, i.e. which CA is required when "showing" the user certificate when trying to establish a connection. It is checked whether the stored CA is also the issuer of the user certificate and whether this certificate is still valid.

However, a review must also take place in the other direction; the device must also identify itself to the DIGSI PC with a certificate (in this case a server certificate). This server certificate must be issued and signed by the same certification authority CA.

In a first step, this certificate is **requested** by the SIPROTEC 5 Compact device for each physical interface via which access can be possible (if the Siemens manufacturer certificates are used on both sides, this is not visible and required). The steps that have to be carried out manually for each SIPROTEC 5 Compact device and for each interface, in case that a central certificate management tool with EST functionality is not used, will be explained. If you think about it. Since the certificates also have to be renewed cyclically, it becomes quite clear that such a **tool like SICAM GridPass** is extremely helpful and useful, as all steps there run automatically, and certificates are renewed cyclically before they expire.

The requested certificates can be seen via the web UI interface under "Certificates" -> "Requested certificates" -> DIGSI: * port * (Figure 4.19). This "Signing request" can now be exported using the export button.

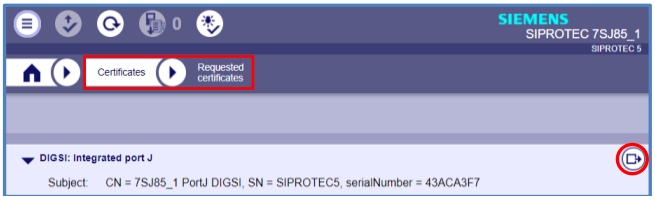


Figure 4.19: Web-UI Requested certificates

Without a central certificate management tool with EST, the next step is to import this “signing request” into the certificate management tool (see Figure 4.20). In SICAM GridPass under "Local Request", the import is started via the "Import Signing Requests" button and the exported file (DIGSI_J.csr) is to be selected in the dialog box.

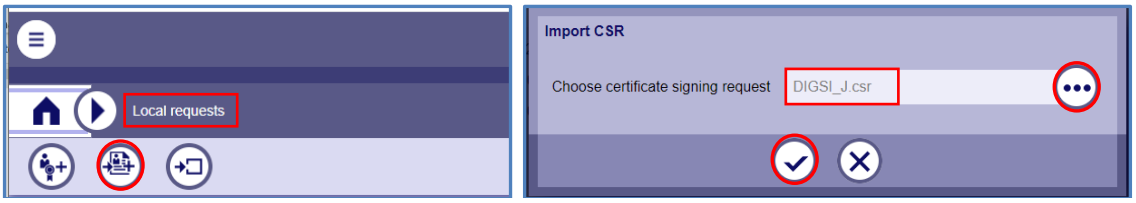


Figure 4.20: Import of the “Signing Request” into SICAM GridPass

After the import has been completed, a menu for creating and signing the server certificate opens (Figure 4.21). Only a few settings need to be made here; It is important that the certification authority CA is selected correctly (here SICAM_Grid_Pass_CA) and a period of validity is set. With the "next" button the second page of the settings is opened: since all information is already contained in the "request", no further settings need to be made here, exception if required: setting where the list of certificates that are no longer trustworthy is located (This happens automatically when using EST protocol).

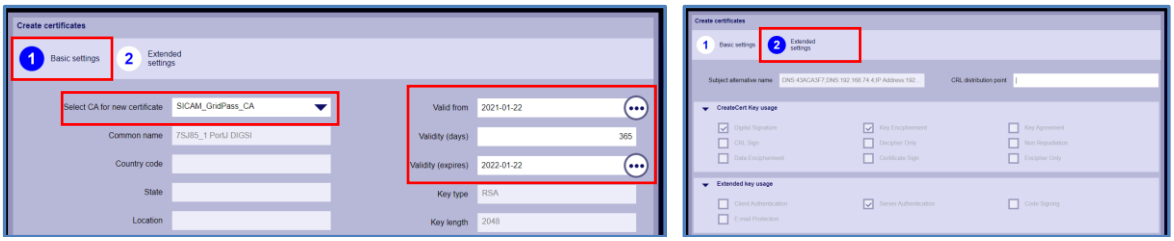


Figure 4.21: Generating the server certificate with SICAM GridPass

After pressing the "Finish" button, the server certificate is signed and created; a dialog box opens to select the storage location of the newly created, signed certificate. The newly created certificate is also saved in SICAM GridPass and its properties are visible there.

The server certificate can also be exported from SICAM GridPass at any time later (Figure 4.22); To do this, select the certificate, open the properties, and click the "Export" button to start the export. The *.pem format is to be selected in the dialog box; no PIN must be entered there as there is no private key in this format.

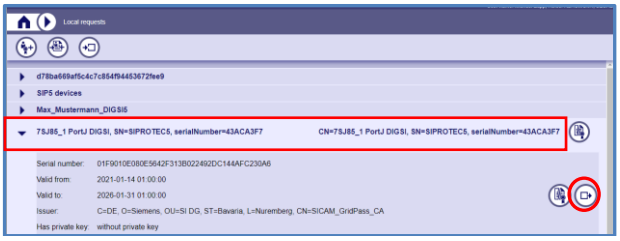


Figure 4.22: Export of the server certificate from SICAM GridPass

Loading the server certificate into the device via the web UI user interface (Figure 4.23) is the final step. To do this, select in the Web UI the tiles “Certificates” -> “Certificates in use” and click the “Upload Certificate” button. Now select the

storage location and the server certificate file (DIGSI_J.pem) in the dialog box and complete the import with the "Finish" button.

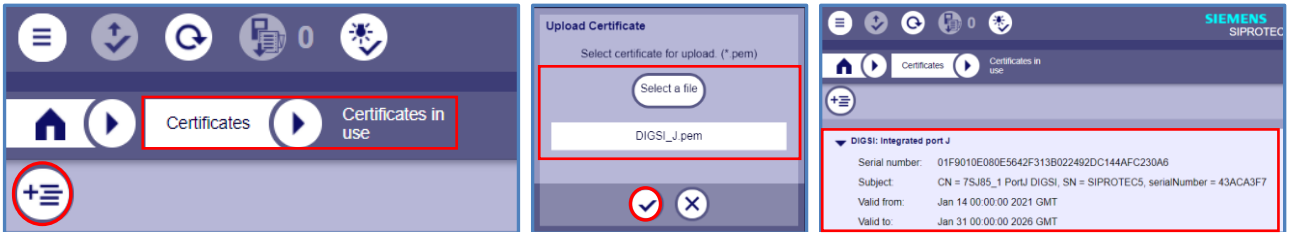


Figure 4.23: Load the server certificate into the device via Web UI

Done; Both on the computer side (client certificate) and on the device side (server certificate) the tools necessary for mutual identification and authentication (such as an ID card) are now available, both were issued and signed by the same certification authority. Only if both partners can use their certificates to prove that they are valid and have been issued by the correct CA (SICAM_GridPass_CA), both sides (PC and device) will accept a connection establishment.

When establishing a connection from the PC, the password of the user certificate (client certificate) must be entered (Figure 4.24), the connection will only be established and an action (e.g. loading parameters) is only permitted if the password and the certificate match. This is also reported back in a dialog box (Figure 4.25); If one of these fails, this is also reported back with an indication of the reason (here: invalid client certificate) and the connection will be rejected.

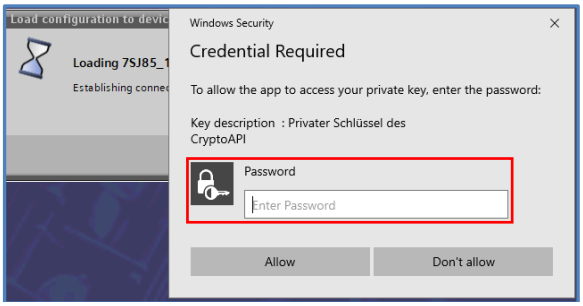


Figure 4.24: Connection establishment with client certificate and password

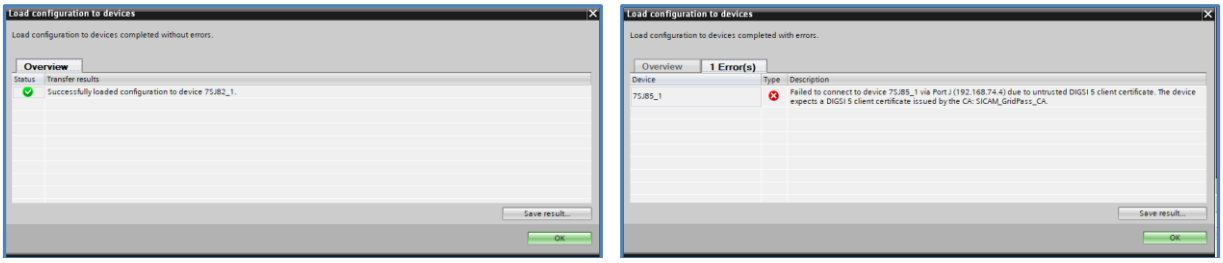


Figure 4.25: Positive / negative feedback dialog

1.4.3 Access rights from the Web UI via certificates

Apart from the use of the engineering tool DIGSI 5 for configuration and maintenance, SIPROTEC 5 devices provide a Web front end that can be used with a standard Web browser:

To protect the access, the settings for each interface via which web access is possible should be adapted in DIGSI under network access security and loaded into the device (Figure 4.26):

- no access
- read and write access
- read-only access

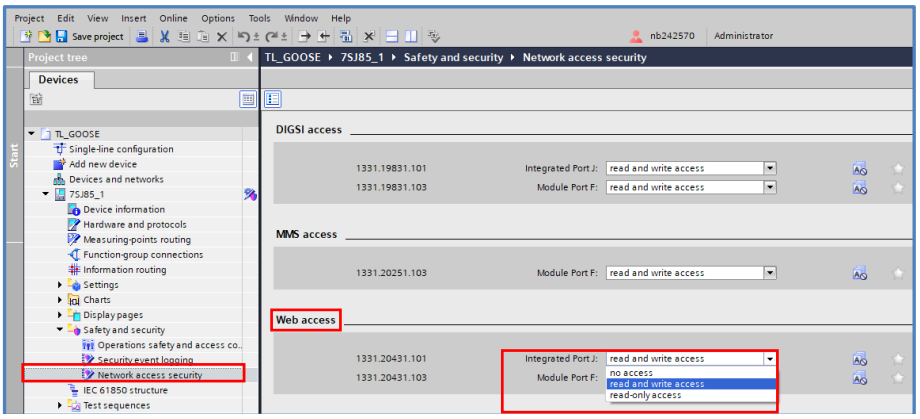


Figure 4.26: Setting of the access rights for web access

The SIPROTEC 5 Compact device must have a physical Ethernet connection to the computer. Start the web browser on your PC. Enter the IP address of the device in the address line of the web browser, followed by the port number 4443, e.g. https://172.16.60.60:4443, and confirm the entry with the Enter key.

The following login dialogs are available, depending on the security configuration of the SIPROTEC 5 device:

- **Variant1:**
  If you have entered a connection password in DIGSI 5 under Operations safety and access control, the login dialog starts with the username **Siprotec 5**. This username cannot be changed. You must use the connection password configured in DIGSI.
- **Variant 2:**
  If you have configured the role-based access control (RBAC) in DIGSI 5 under Operations safety and access control, the login dialog starts with the request of the user name and password that you have configured on the RADIUS server.
- **Variant 3:**
  If you have not configured the role-based access control (RBAC) or the connection password, the login dialog starts with the username **Siprotec 5**. This username cannot be changed. The entry field for the password must be left empty.

The connection between the web server on the SIPROTEC 5 device and the web browser on the PC is based on the secure https protocol and is secured by certificates. The authentication scheme of a web browser prevents a manufacturer certificate from being loaded into the device, because either the DNS name or the IP address of the interface must be part of the issued and signed certificate and both are only finally set during the parameterization. Therefore the device issues a so-called "self-signed certificate" after the IP address settings have been established. This certificate can now be trusted.

More information on this can be found in the description [8] "Trusting self-signed certificates browsers".

1.4.4 Access rights according to IEEE 802.1X via certificates

SIPROTEC 5 devices support thanks to the certificate authentication feature according to IEEE 802.1X a port-based network access control via Ethernet communication modules.

If this feature is activated, working with a 802.1X authenticator such as a router or a switch, a SIPROTEC 5 device takes the role of 802.1X supplicant. This feature provides a secure, certificate-based access control of your network access. It permits or denies network connection to SIPROTEC 5 devices based on the certificate-based mutual authentication. It only allows authenticated devices access your network and prevents illegal devices or clients from accessing and hacking your network (Principle: see Figure 4.27).

Before configuring this feature, make sure that the following prerequisites are met:

- Set the network redundancy protocol of the port to Line Mode, because the IEEE 802.1X standard does not define redundancy protocols such as PRP, HSR or RSTP and no ring structures
- Available certification authorities have been imported into the DIGSI 5 CA store; only then this function will be activated and visible in the parameterization workspace

Note: If RBAC is enabled, only users in the role of a SECADM or an Administrator can configure the IEEE 802.1X certificate authentication feature.

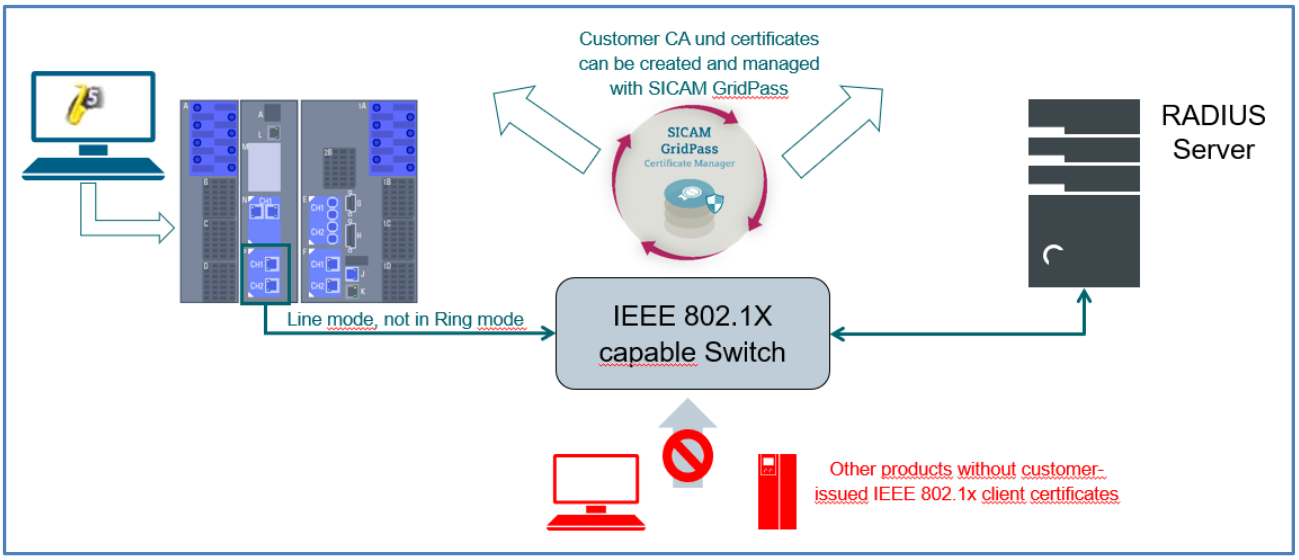


Figure 4.27: Network access authentication of switches / routers

If the requirements ("line mode" for the interface / port are set and CA is available in the DIGSI CA store) is given, in the settings of the SIPROTEC 5 device under "Network access security" -> IEEE 802.1X for all interfaces for which a protected connection to a switch / router is required, the CA (see Figure 4.28 here SICAM_GridPass_CA) must be selected. When that is done: save the project and load the security settings into the device.

After loading the new security settings, the SIPROTEC 5 device recognizes that a client certificate from the selected CA must be presented to establish network access via a switch / router. However, this **client certificate** must first be created and loaded into the device, which is why the device automatically creates a "certificate signing request".

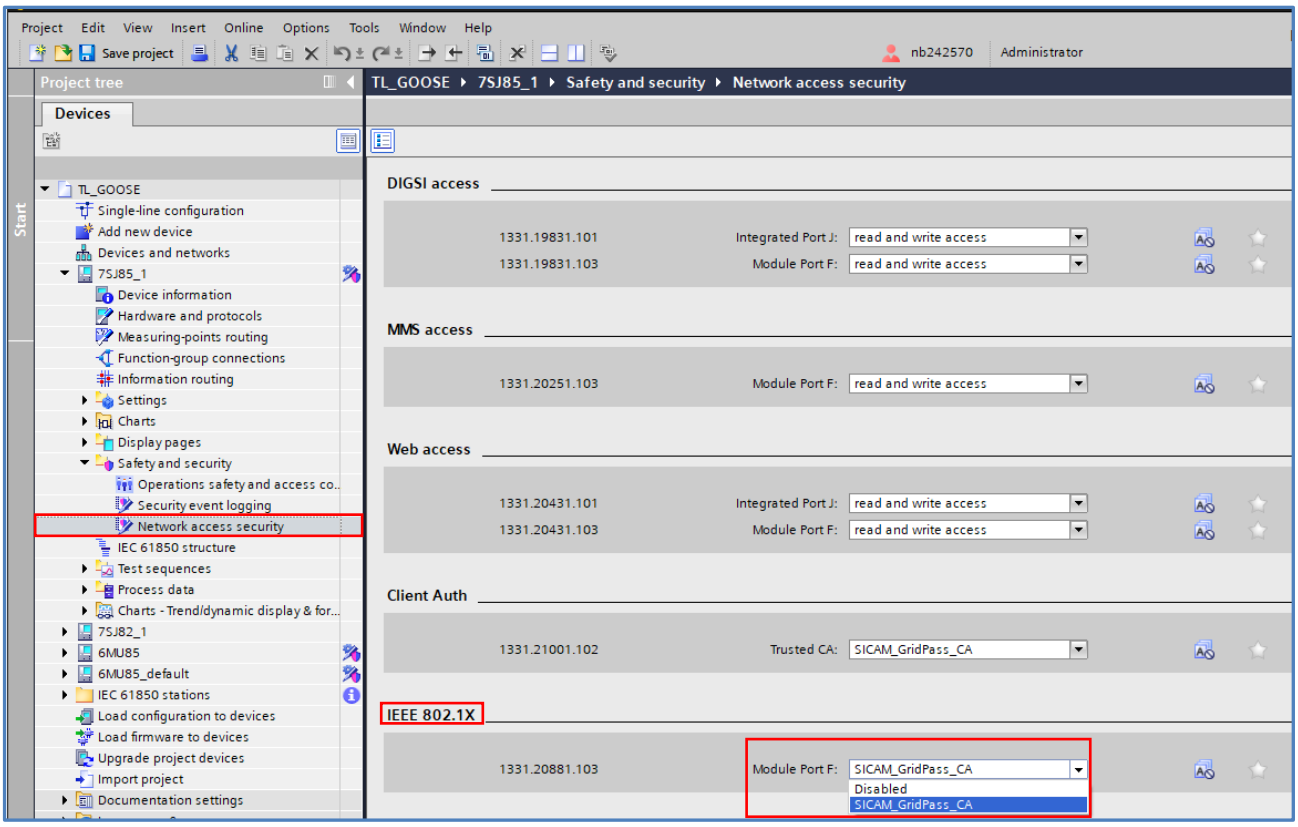


Figure 4.28: Network access authentication for switches / routers

In the following, the steps are explained which, in the event that a central certificate management tool with EST functionality is not used, must be carried out manually for each SIPROTEC 5 Compact device and for each interface via which a secure network access should take place. If you think about it. Since the certificates also have to be renewed cyclically, it becomes quite clear that such a **tool like SICAM GridPass** is extremely helpful and useful, as all steps there run automatically, and certificates are renewed cyclically before they expire.

The requested certificates can be seen in the Web UI interface under "Certificates" -> "Requested certificates" -> IEEE 802.1X: Communication module port * (Figure 4.29). This "Signing request" can now be exported using the export button.

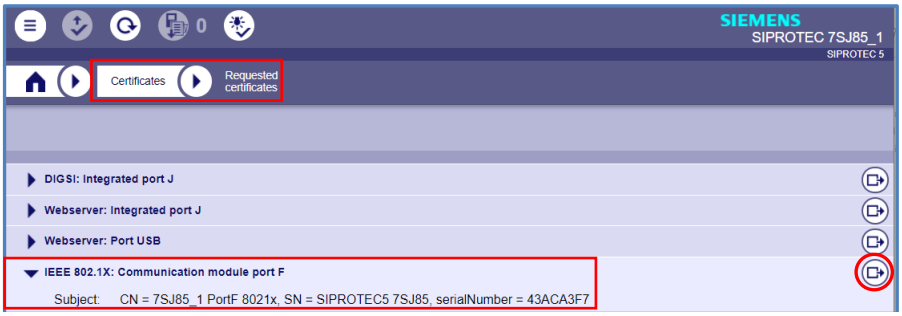


Figure 4.29: Web-UI Requested certificates

Without a central certificate management tool with EST, the next step is to import this “signing request” into the certificate management tool (see Figure 4.20). In SICAM GridPass under "Local Request", the import is to be started via the "Import Signing Requests" button and the file (8021x_F.csr) is to be selected in the new dialog box.

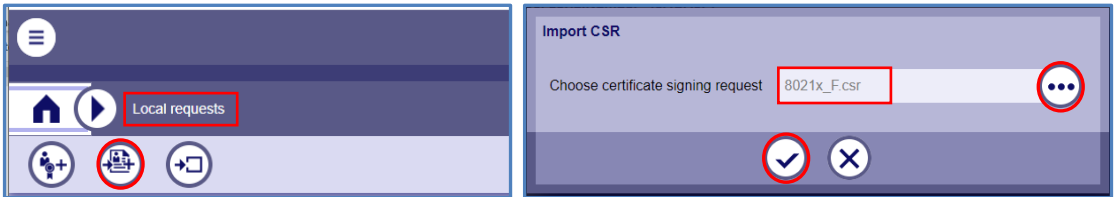


Figure 4.30: Import of the “Signing requests” into SICAM GridPass

After the import has been carried out, a menu for generating and signing the client certificate opens (Figure 4.21). Only a few settings need to be made here; It is important that the certification authority CA is selected correctly (here SICAM_Grid_Pass_CA) and a period of validity is set. With the "next" button the second page of the settings is opened: since all information are already contained in the "request", no further settings need to be made here, exception if required: setting where the list of certificates that are no longer trustworthy is located (This also happens automatically at this point with the help of EST settings).

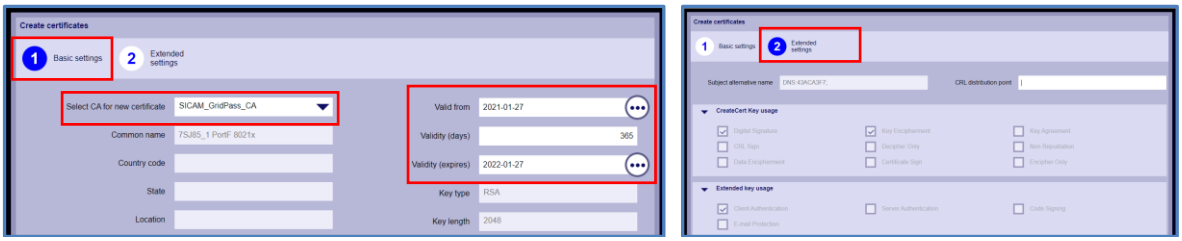


Figure 4.31: Creation of the IEEE 802.1X Client certificate with SICAM GridPass

After pressing the "Finish" button, the client certificate is signed and created; a dialog box opens to select the storage location of the newly created, signed certificate. The newly created certificate is also saved in SICAM GridPass and its properties are visible there.

The client certificate can also be exported from SICAM GridPass at any time later (Figure 4.32); To do this, select the certificate, open the properties, and click the "Export" button to start the export. The *.pem format is to be selected in the dialog box; no PIN must be entered as there is no private key in this format.

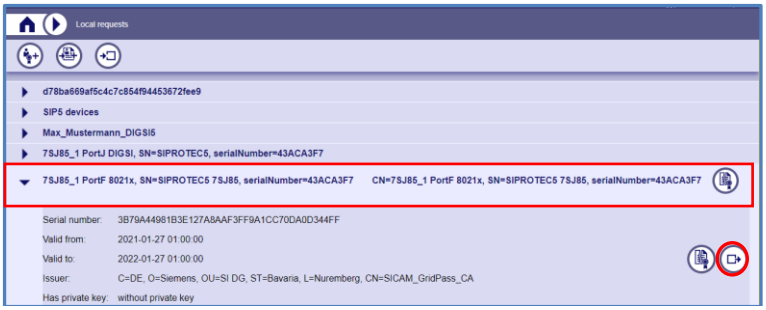


Figure 4.32: Export of the IEEE 802.1X certificate from SICAM GridPass

The final step is now to load the IEEE 802.1X client certificate into the device via the Web UI user interface (Figure 4.33). To do this, select the “Certificates” -> “Certificates in use” tile in the Web UI and then click the “Upload Certificate” button. Now select the storage location and the exported IEEE 802.1X client certificate file name in the dialog box and complete the import with the "Finish" button.

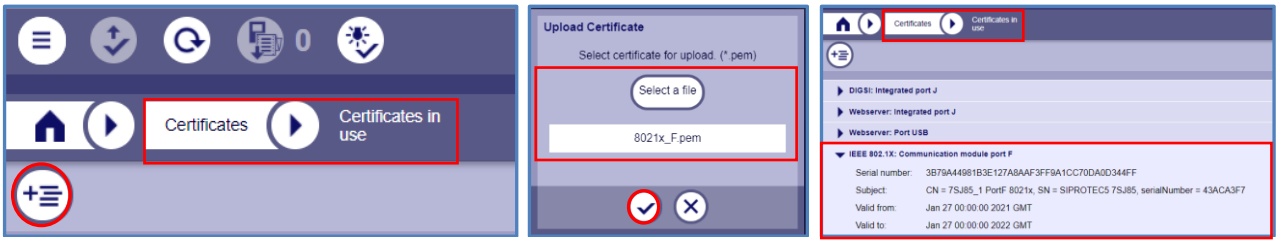


Figure 4.33: Loading of the IEEE 802.1X Client certificate via Web-UI into the device

Everything is now prepared on the SIPROTEC 5 Compact device side (IEEE 802.1X client certificate). The network access switch / router must be IEEE 802.1X capable and have an active connection to the RADIUS server as shown in Figure 4.27. The IEEE 802.1X capable switch forwards the connection request with the IEEE 802.1X client certificate to the RADIUS server, where it is checked whether the interface is allowed to establish a connection or not and the result of the check is returned to the switch by the RADIUS server. Access to interfaces listed in the radius are allowed, requests from interfaces that are not listed there are rejected.

1.4.5 Network separation via VLAN

The Virtual Local Area Network (VLAN) is a data-link layer technology and standardized in IEEE 802.1Q. VLAN allows separation of different communication traffic types (for example, process data, engineering or management, voice calls, and video surveillance) sharing the physical links of the Ethernet network.

Regarding VLAN, SIPROTEC 5 supports the following protocols and technologies:

- Pure layer 2 protocols, for example, GOOSE and SMV.
- IP-based protocols, for example, IEC 61850 MMS, DIGSI 5.

This chapter only describes VLAN regarding IP-based protocols, since the VLAN settings of the pure Layer 2 protocols are not set in DIGSI but in the IEC61850 System Configurator. Details can be found in the manual [5] SIPROTEC 5 communication protocols, so the application and the basic settings are only roughly described here.

The following figure shows an example of the VLAN solution:

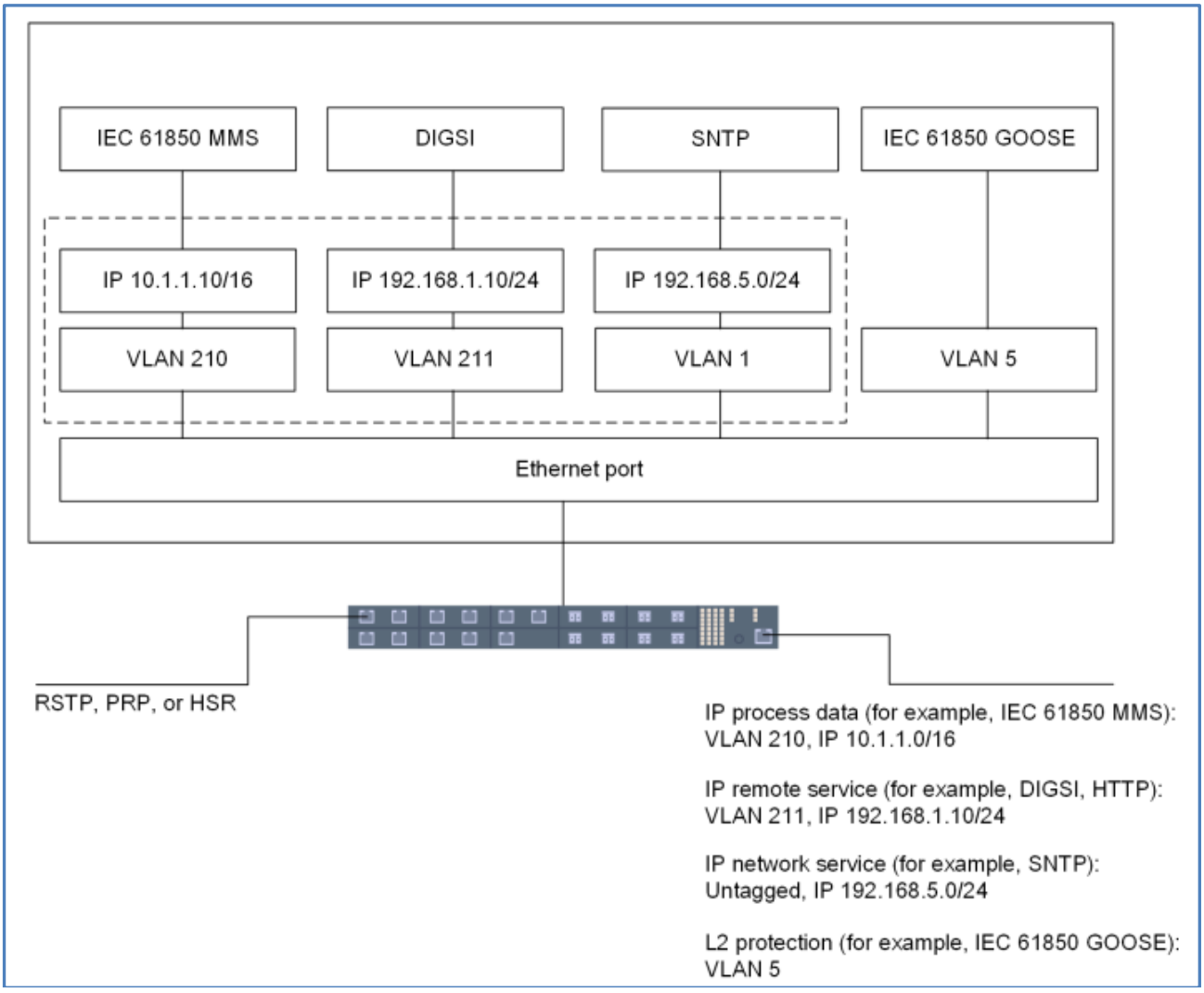


Figure 4.34: Network separation via VLAN

In the SIPROTEC 5 device, VLAN is currently only supported by the ETH-BD-2FO Ethernet module, the FO Ethernet module of the SIPROTEC 5 Compact device also has VLAN setting options.

In the main menu in DIGSI 5 select under the SIPROTEC 5 device “Hardware and Protocols” and open the working space with a double click; Then select the Ethernet interface in the main window and open the properties window. (Figure 4.35)

By default, one IP interface is created and VLAN is deactivated => the VLAN functionality is activated by checking the box next to "Use VLAN tag".

Two more IP interfaces can be added via "Add Interfaces", i.e. a physical Ethernet interface can have 3 different IP addresses and the areas can be segmented and separated from one another via VLAN.

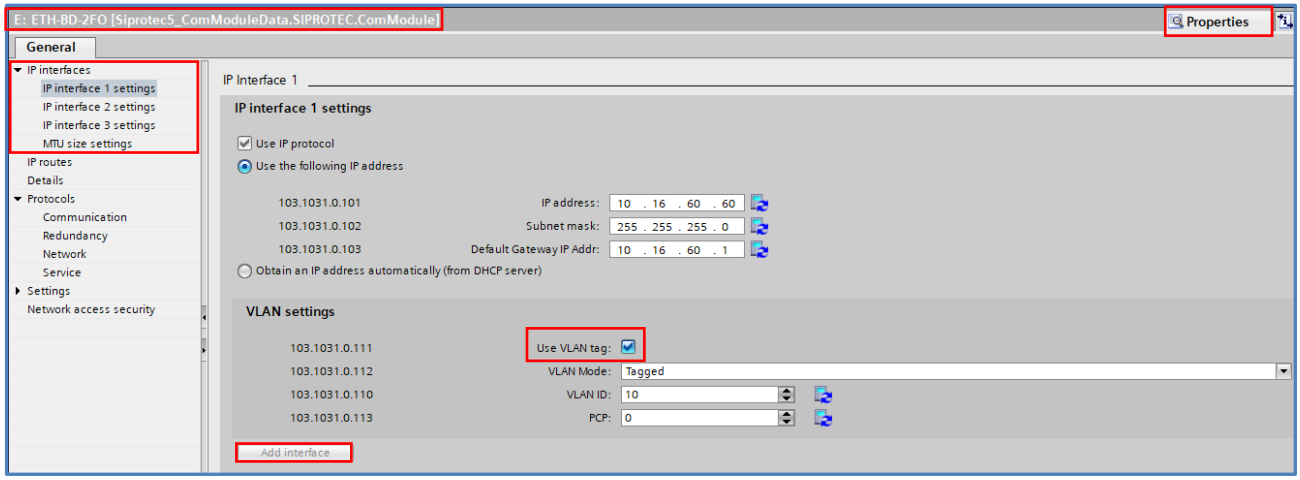


Figure 4.35: Activation of VLAN

The assignment which IP-based protocol (e.g. IEC 61850) / service (e.g. DIGSI / Web-UI access) or network service (e.g. SNMP) shall use which IP address (IP interface) can then be selected under "Properties" -> Protocols (Figure 4.36)

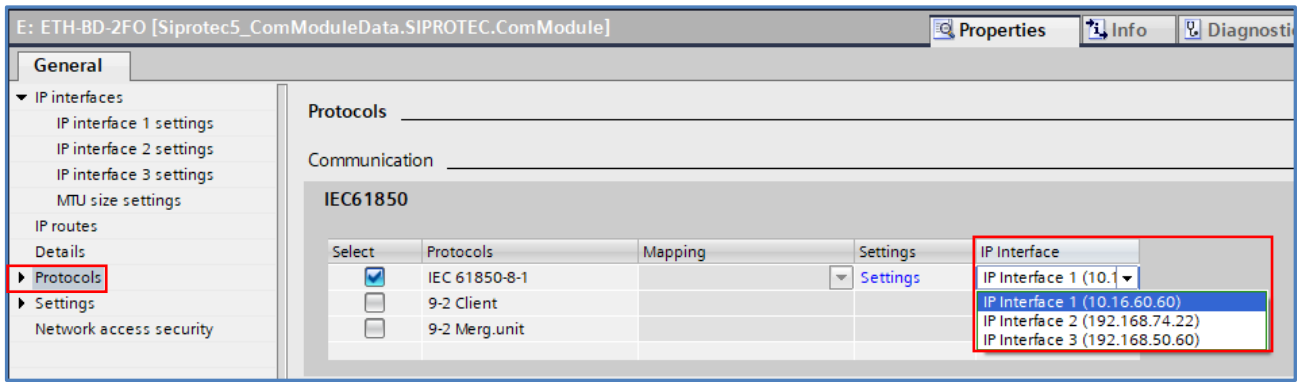


Figure 4.36: Assignment of the IP-based protocol IEC61850 to a VLAN interface

1.5 Security Logging

1.5.1 SYS-Log

The SIPROTEC 5 Compact devices and DIGSI 5 provide a security audit trail which chronologically acquires and categorizes security-relevant events according to the origin and severity.

The SIPROTEC 5 Compact devices automatically send the security-relevant events to an external syslog-server while DIGSI 5 sends such events to the Windows Event Log.

The transmission of the security events to the configured SYS-Log-Server(s) takes place spontaneously and without a conformation via UDP (User Datagram Protocol) when the security event occurs. A later readout of the recorded security-events from the device-local security event buffer is possible. The security events are in English.

To record cybersecurity events during the operation of SIPROTEC 5 Compact devices, recordings are automatically created and data is collected. All security-related events and alarms recorded in the device-internal security log can also be transmitted simultaneously to a central SYS-Log-Server. This action allows safety-relevant events to be recorded from various transformer stations with the requirements of standards and guidelines, such as IEEE 1686, IEC 62443, and the BDEW White Paper. Logging is started centrally on 1 or 2 self-selected SYS-Log-Servers. Combining different protocol data of the devices used gives you a general overview of the device network. You can analyze and monitor this data. This action allows safety-critical events to be logged and related changes to be tracked. You can also track attacks on the operated devices by using the log data.

You can view the collected log data in the security log locally on the device display, irrespective of the current operating mode of the device. The alarm and safety-critical indications are stored chronologically in the security log. You cannot modify or delete these entries.

You can, for example, answer to the following questions:
- How many login attempts have been made?
- When was the device configuration last updated?

Further information regarding:
- Structure of security events
- List of recorded security events
- List of records (actions / potential errors / capacity warning of the safety message buffer)

can be found in Chapter 8 of the [4] SIPROTEC 5 Security Manual.

Configuring the Central Syslog Server (see Figure 5.1)
If you have started DIGSI 5 and connected it to a device, select **“Safety and security” -> “Security event logging”** in the project tree. The **Sec. Ev. Logg**. menu item contains the setting options for a central syslog server. You can activate up to 2 syslog servers via hooking up the “enable logging” checkbox.

In the General area, you define the capacity warning level of the device-internal security log. You can activate logging under syslog server A and/or B. Enter the following data:
- IP address of the central SYS log server (s)
- Server UDP port (UDP is specified in the standard, standard UDP port is 514, but can be adjusted)
- Module port used for the connection from the device to the central SYS log

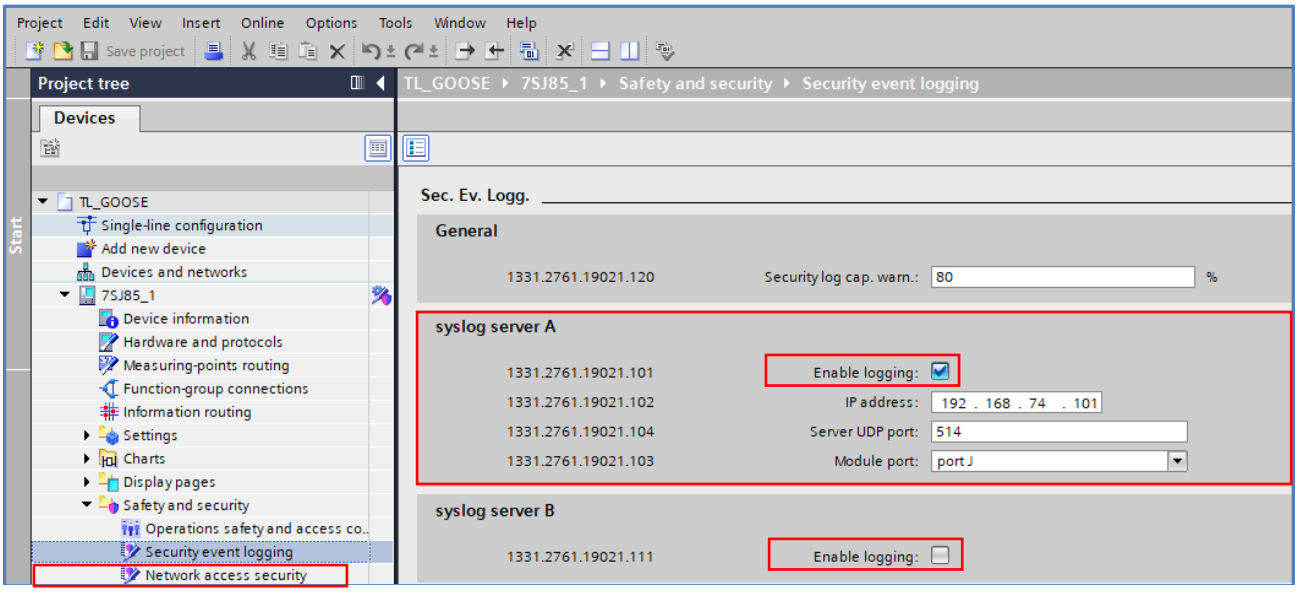


Figure 5.1: Activation and settings of the central SYS log server

With the adjustable Security **log cap. warn.** threshold, you can determine 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 you read the security log using DIGSI 5, the capacity utilization is reset to 0 %. The indications remain in the device. You must apply all settings with DIGSI 5

In addition to access via the central SYS log server, the security message buffers can be viewed on the device display or with an online connection to the device in DIGSI 5.

Note:

- The browser-based user interface does not support to display the security logs.
- On the syslog server(s), Siemens recommends protecting the received security-events from unauthorized read or write access with the role Auditor.

1.6 Link collection to further documents

[1] Setting up RBAC for Siemens Digital Grid Products
https://support.industry.siemens.com/cs/document/109759182/setting-up-rbac-for-siemens-digital-grid-products?dti=0&pnid=24296&lc=en-WW

[2] Certificate trusting in web browsers
https://support.industry.siemens.com/cs/document/109759179/digital-grid-automation-products-certificate-trusting-in-web-browsers?dti=0&pnid=24296&lc=en-WW

[3] SICAM / SIPROTEC System Hardening for Substation Automation and Protection
https://support.industry.siemens.com/cs/document/109759171/sicam-siprotec-system-hardening-for-substation-automation-and-protection?dti=0&pnid=24296&lc=en-WW

https://wse06.siemens.com/content/P0009275/Documents/Products/Manuals/SecureSubStation_SecurityManual_ENG.pdf

[4] SIPROTEC 5 Security – Manual
https://support.industry.siemens.com/cs/document/109768375/siprotec-5-security-manual?dti=0&pnid=24237&lc=en-WW

[4] SIPROTEC 5 Security – Handbuch
https://support.industry.siemens.com/cs/document/109768375/siprotec-5-security-%E2%80%93-handbuch?dti=0&pnid=24237&lc=de-WW

[5] SIPROTEC 5 Communication Protocols – Manual
https://support.industry.siemens.com/cs/document/109742443/siprotec-5-communication-protocols-manual?dti=0&pnid=24237&lc=en-WW

[5] SIPROTEC 5 Kommunikationsprotokolle - Handbuch
https://support.industry.siemens.com/cs/document/109742443/siprotec-5-kommunikationsprotokolle-handbuch?dti=0&pnid=24237&lc=de-WW

[6] DIGSI 5 Software-Beschreibung Hilfe – Handbuch
https://support.industry.siemens.com/cs/document/109742461/digsi-5-software-beschreibung-hilfe-handbuch?dti=0&pnid=24304&lc=de-WW

[6] DIGSI 5 Software Description Help – Manual
https://support.industry.siemens.com/cs/document/109742461/digsi-5-software-description-help-manual?dti=0&pnid=24304&lc=en-WW

[7] SICAM GridPass – Manual
https://support.industry.siemens.com/cs/document/109763384/sicam-gridpass-v1-60-software?dti=0&pnid=25398&lc=en-WW

[8] Trusting self-signed certificates browsers
https://wse06.siemens.com/content/P0009275/Documents/Cyber%20Security%20General/Application%20Note/Trusting_Self-Signed_Certificates_in_Browsers.pdf

1.7 Conclusion

Siemens offers products and technologies, which consider the leading cybersecurity standards. The major drivers for secure infrastructures are the standards and guidelines, such as IEC 62443, IEC 62351, BDEW White Paper, IEEE 1686, and NERC CIP (Critical Infrastructure Protection).

This is illustrated in this clear application and supports safe commissioning and operation of SIPROTEC 5 / SIPROTEC 5 Compact device in a networked environment.

Published by
Siemens AG 2021
Smart Infrastructure
Digital Grid
Automation Products
Humboldtstr. 59
90459 Nuremberg, Germany
www.siemens.com/siprotec
Our Customer Support Center
provides a 24-hour service.
Siemens AG
Smart Infrastructure – Digital Grid
Customer Support Center
E-Mail:
energy.automation@siemens.com