APPLICATION NOTE

Setting Up Role-based Access Control via LDAP

APN-097, Edition 01

SIEMENS

SIEMENS

Secure Substation LDAP

V01.00

Application Notes

APN-097

Table of Contents

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: APN-097.01

Edition: 09.2023

Version of the product described: V01.00

Copyright

Trademarks

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

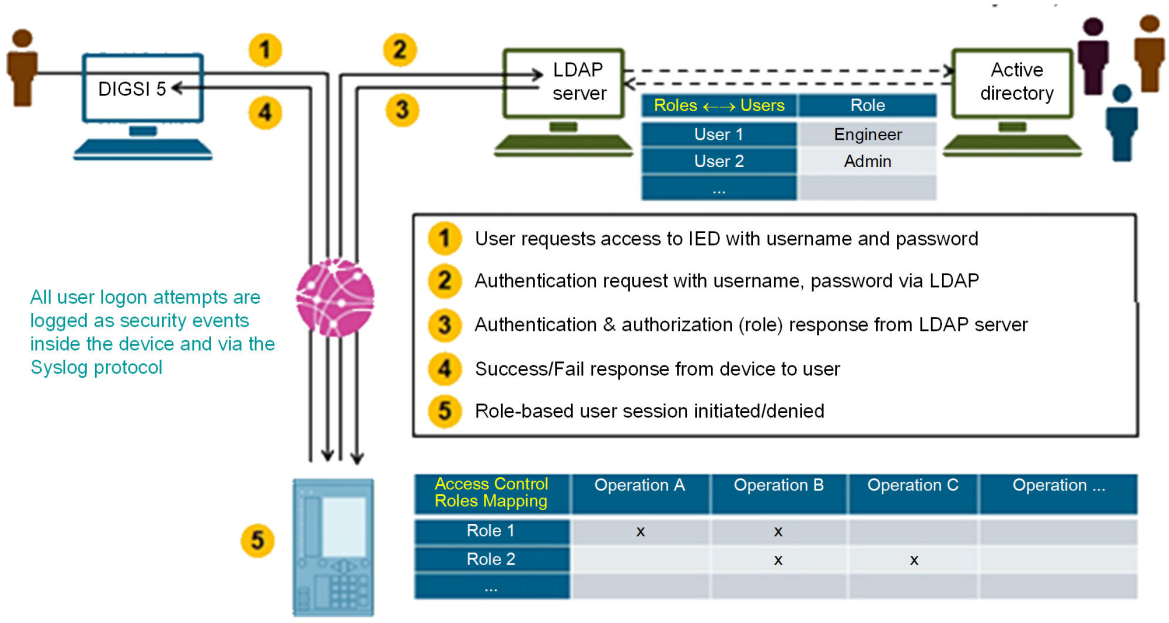
Table of Contents

1 Role-Based Access Control for Digital Grid Products

1.1 Introduction

SIPROTEC 5 and SICAM A8000 devices support role-based access control with central user management in LDAP/Active Directory among other advanced cybersecurity features. To access information on a SIPROTEC 5 or SICAM A8000 device or to perform actions on the device, optionally the role-based access control (RBAC) can be enabled. After activation, the operator has to authenticate and authorize himself as a user before each interaction with the device. In the document APN-051, "Role_Based Access Control", RBAC via Radius is described. In this document, RBAC via LDAP is described.

All SIPROTEC 5 and SICAM A8000 devices can be connected to a central LDAP server containing the authentication and authorization configuration. LDAP (Lightweight Directory Access Protocol) is a standardized client/server protocol, and the client implementation is integrated in the SIPROTEC 5 and SICAM A8000 device firmware.



LDAP: This internationally well-established protocol will be officially part of the IEC 62351-8 standard soon for centralized access control management in 2019.

[sc_introduction_RBAC-with_LDAP, 1, --_--]

This document describes the usage of SIPROTEC 5, SICAM A8000 devices and SICAM GridPass with the LDAP option in an Active Directory of a Windows Server 2022 system. An Active Directory Server (ADS) needs to be installed. Furthermore, for the local user login on a SIPROTEC 5 device over the LDAP protocol, the ADS policy must be adjusted. This specific configuration is part of the APN-051 document.

1.2 Fundamentals

Active Directory (AD)

Active Directory (AD) is a directory service that Microsoft developed for Windows domain networks. It is included in most Windows Server operating systems as a set of processes and services. Initially, Active Directory was only in charge of centralized domain management. Starting with Windows Server 2008, Active Directory became an umbrella title for a broad range of directory-based identity-related services.

Active Directory Domain Service (AD DS)

An Active Directory Server (ADS) is called a domain controller. It authenticates and authorizes all users and computers in a Windows domain type network, assigning and enforcing security policies for all computers and installing or updating software, for example, when a user logs on a computer/device that is part of a Windows domain, Active Directory checks the submitted password and determines whether the user is a

system administrator or normal user. Also, it allows the management and storage of information, provides authentication and authorization mechanisms, and establishes a framework to deploy other related services: Certificate Services.

Active Directory Lightweight Directory Service (AD LDS)

AD LDS is a directory service. Active Directory Lightweight Directory Services (AD LDS) provides only a subset of the capabilities of AD DS. This makes it a leaner and more independent directory service that can be run as a stand-alone directory without integration with an existing AD.

Prior to Windows Server 2008, AD LDS was still called ADAM (Active Directory Application Mode) and was only considered as an extension and not as a server role.

Lightweight Directory Access Protocol (LDAP)

The Lightweight Directory Access Protocol (LDAP) is a directory service protocol that runs on a layer above the TCP/IP stack. It provides a mechanism used to connect to, search, and modify Internet directories. The LDAP directory service is based on a client-server model.

LDAP Client

All SIPROTEC 5 and SICAM A8000 devices support user authentication via LDAPS, LDAP with STARTTLS, which is based on IEC 62351-8 (PULL model with LDAP-profile A). After authentication with user credentials via LDAP, the device downloads the LDAP attribute **inetOrgPerson:userCertificate (cf. RFC 2798)** which contains DER encoded X.509 certificates of the user including user roles. The signature of the user certificate is verified by means of the parameter **User root CA**. The certificate authority configured for connection establishment via LDAP is used if the parameter **User root CA** is not set. This certificate contains the role of a logged-on user and can be generated and pushed into LDAP by means of, for example, SICAM GridPass. To manage permission groups between devices, the Area of Responsibility (AoR) configuration of the device can be used as a distinction. The communication from the device to the LDAP server is TLS encrypted.

IEC 62351-8

Power systems management and associated information exchange – Data and communications security – Part 8: Role-based access control, technical specification. Edition 1 has been released in Sept. 2011.

1.3 Implementation according to IEC 62351-8 Ed.1 Standard

Siemens has implemented the LDAP protocol according to the IEC 62351-8 Ed.1 standard.

2 Configuration

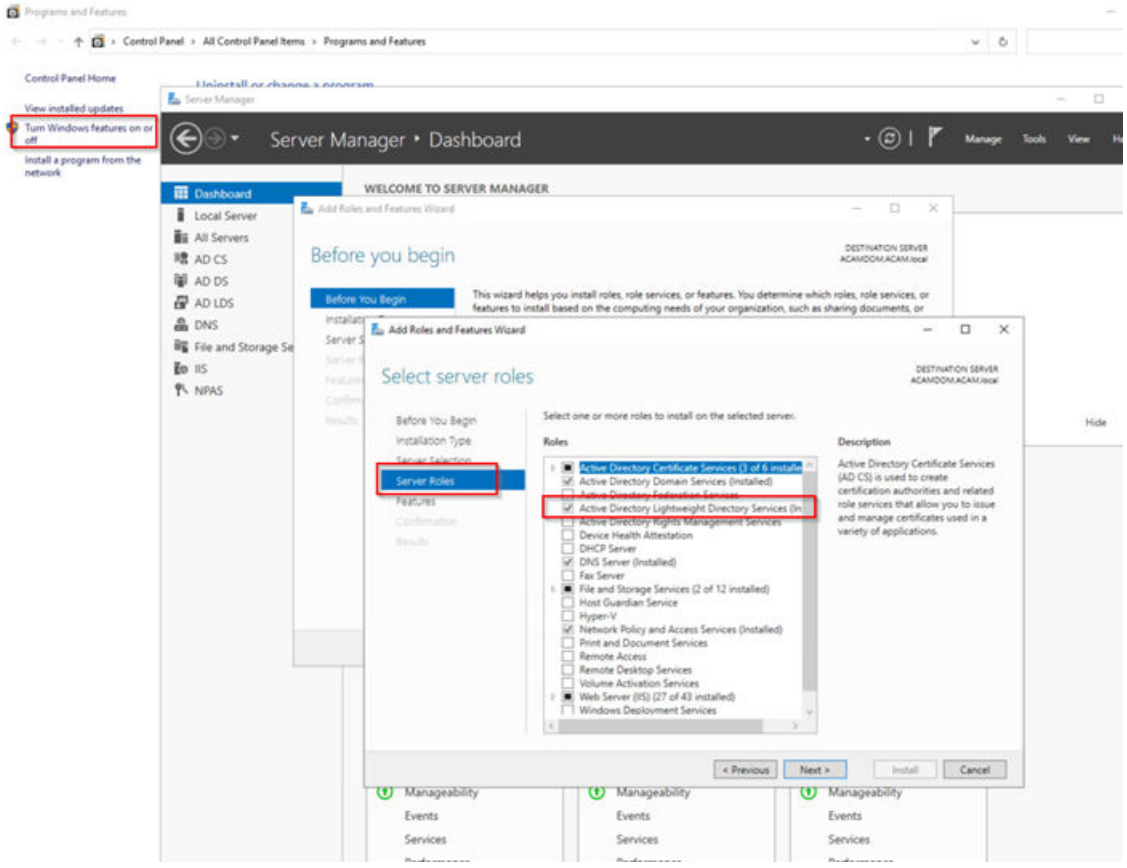
2.1 Installation

✧ To install the Active Directory Lightweight Directory Service (AD LDS) on a Microsoft Windows Server 2022 standard operating system open the dashboard in the control panel.

✧ Select **Add Roles and Features Wizard**.

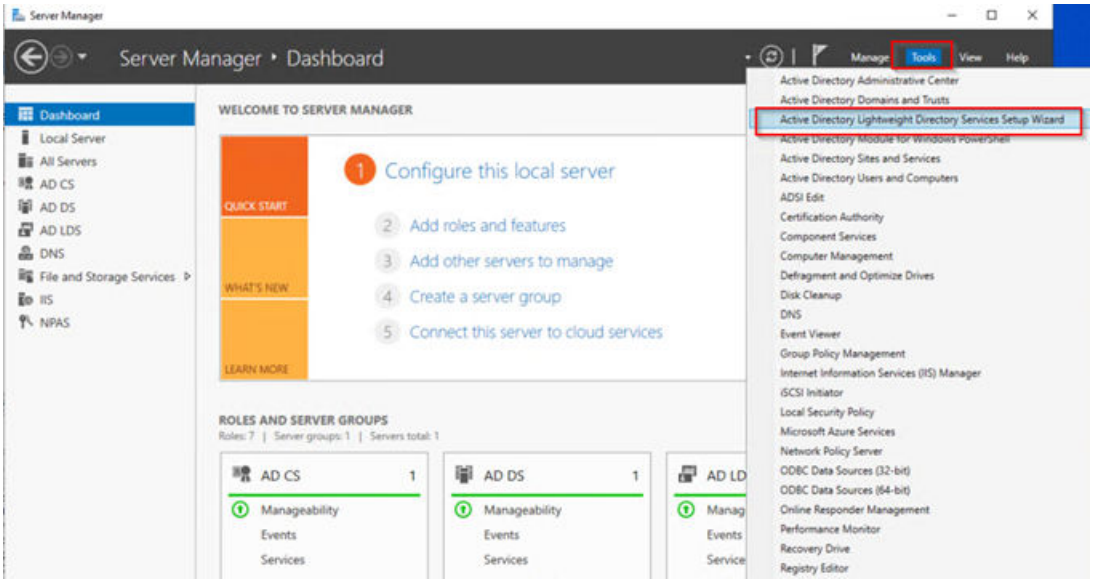
You can find the Active Directory Lightweight Directory Service in the area **Server roles**.

✧ Select server roles.



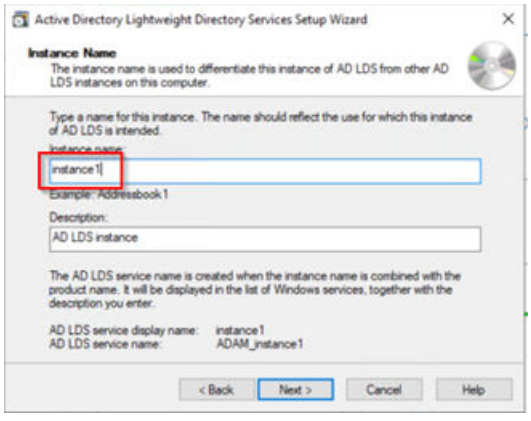
[sc_AD-LDS-installation_add-roles-and-features, 1, en_US]

✧ After the Active Directory Lightweight Directory Service (AD LDS) is installed, execute the Active Directory Lightweight Directory Service for post installation.



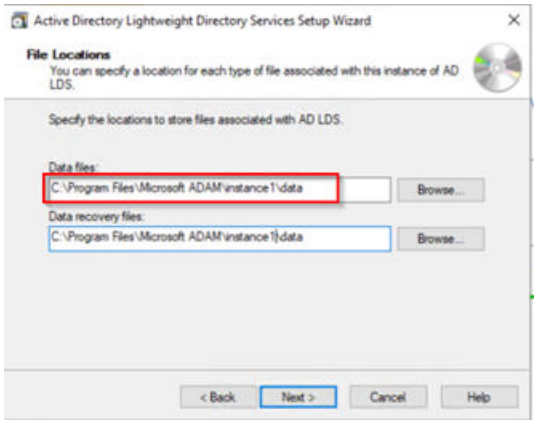
[sc_AD-LDS-installation_post-installation, 1, en_US]

✧ Create an instance.



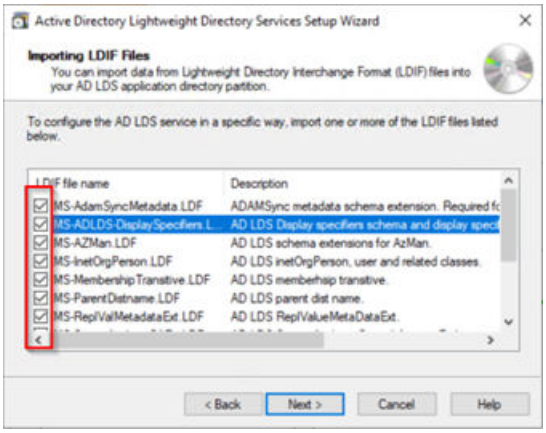
[sc_AD-LDS-installation_create-instance, 1, en_US]

✧ Enter a file location.



[sc_AD-LDS-installation_create-an-instance_file-location, 1, en_US]

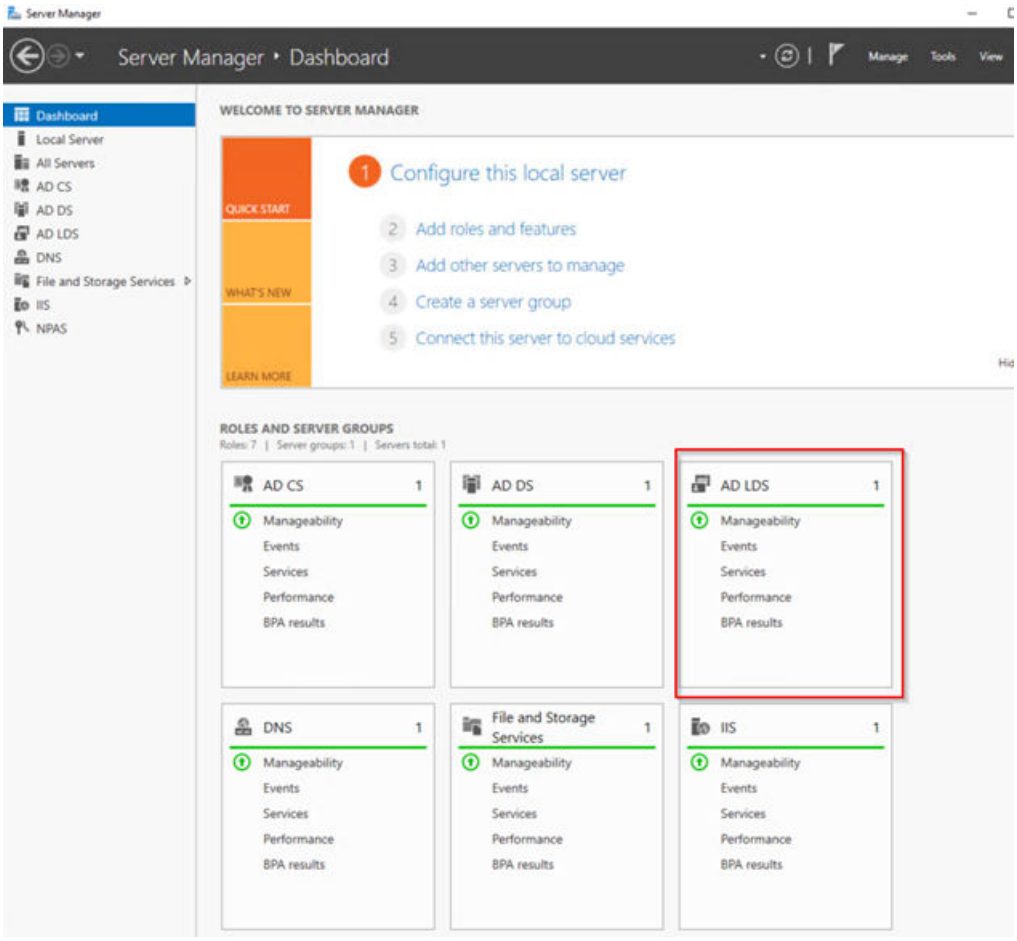
✧ Select all LDIF files.



[sc_AD-LDS-installation_create-an-instance_LDIF-file, 1, en_US]

✧ Run the installation.

The installation is completed.



[sc_AD-LDS-installation_complete, 1, en_US]

NOTE

A detailed step-by-step description of the installation is shown in the AD LDS description of *https://www.youtube.com/watch?v=UFAib3GFtNk*.

2.2 Configuration and Management

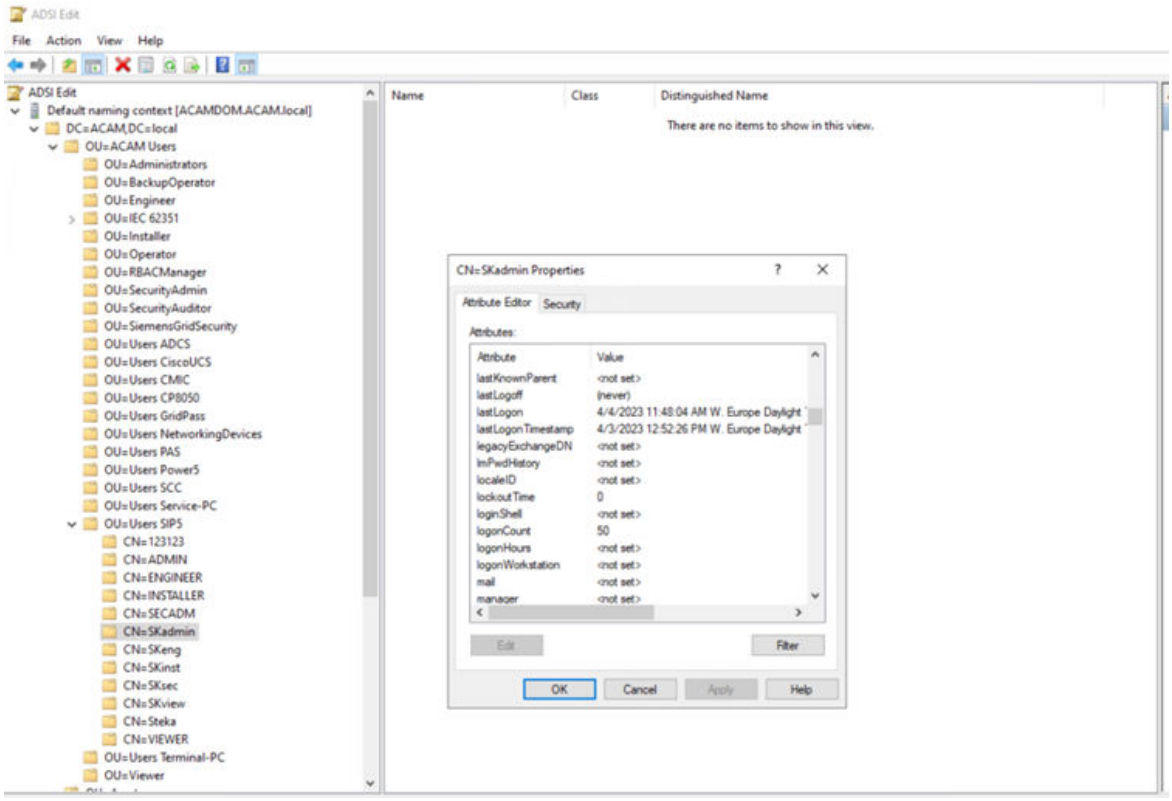
In the Active Directory Lightweight Directory Service (AD LDS), you can see the folder structure of the **Active Directory Users and Computers**. Among others, it includes the user and attribute certificates.
Also LDAP certificates successfully exported with SICAM GridPass can be found here.

Example for Assigned Certificates

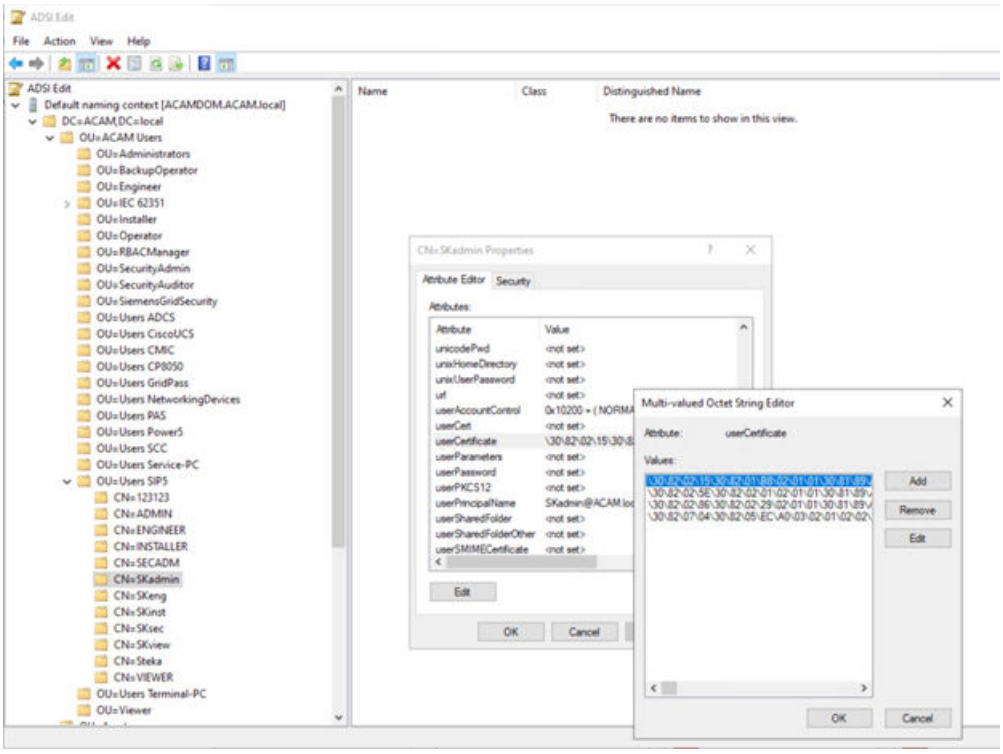
In the following, you can find an example for the user **SKadmin** who has been assigned 4 certificates.

✧ Open ADSI via **run** > **Start C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Administrative Tools\ADSI Edit**.

The structure of the Active Directory is displayed.



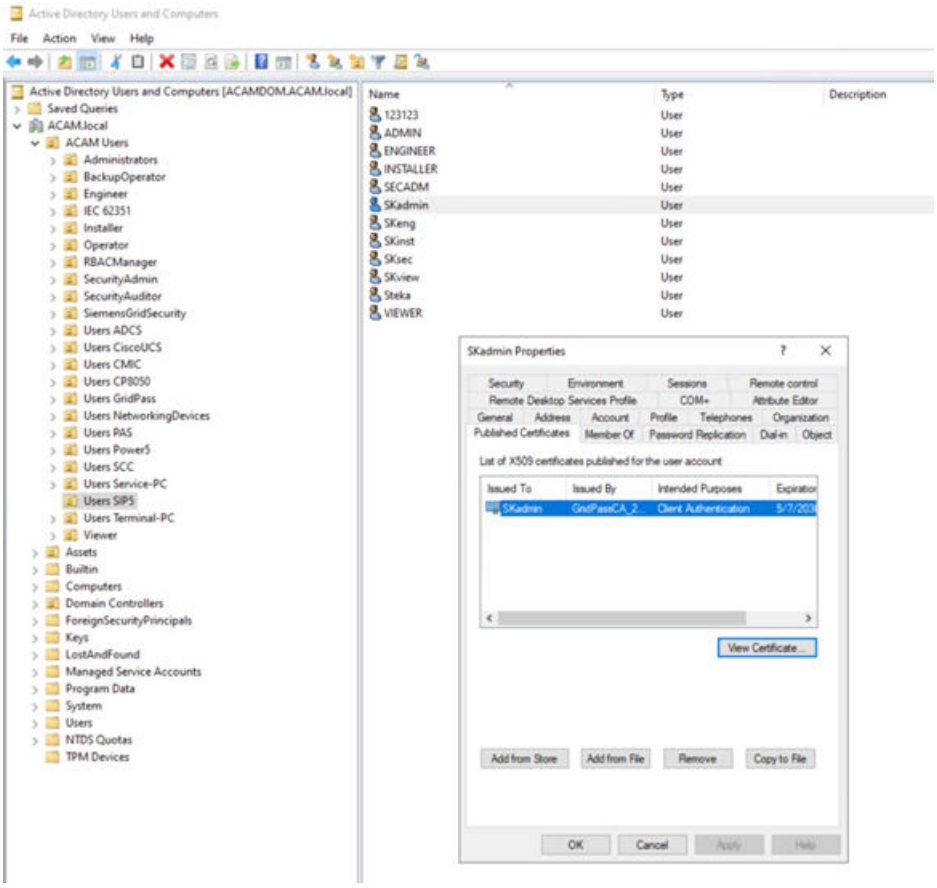
[sc_config_and_management_of_AD-LDS, 1, en_US]



[sc_config_and_managerment_of_AD-LDS_1ID-AD-certificates, 1, en_US]

Active Directory Users and Computers

✧ Only 1 ID or attribute certificate is shown for the user SKadmin.



[sc_config_and_management_of_AD-LDS_only1ID-or-attribute-certificate, 1, en_US]

2.3 LDAP User Certificates

2.3.1 Use Case and Preconditions

Use Case

Creating a new user with the role CP8050 admin who can administrate an A8000 SICAM CP-8050 via Web interface. For authentification LDAP is used. The LDS of a Windows Active Directory is used. The Active Directory is configured on a Primary Domain Controller (Win Server 2022 21H2). The necessary certificates are generated by GridPass.

The following steps are necessary:

- *2.3.2 Creating an LDAP User in the Active Directory*
- *2.3.3 Settings in SICAM GridPass*
- *2.3.4 Creating an LDAP Server Certificate*
- *2.3.5 Generating Client Certificate for the LDAP User CP8050_Admin*
- *2.3.6 Exporting Certificates to LDAP Server*

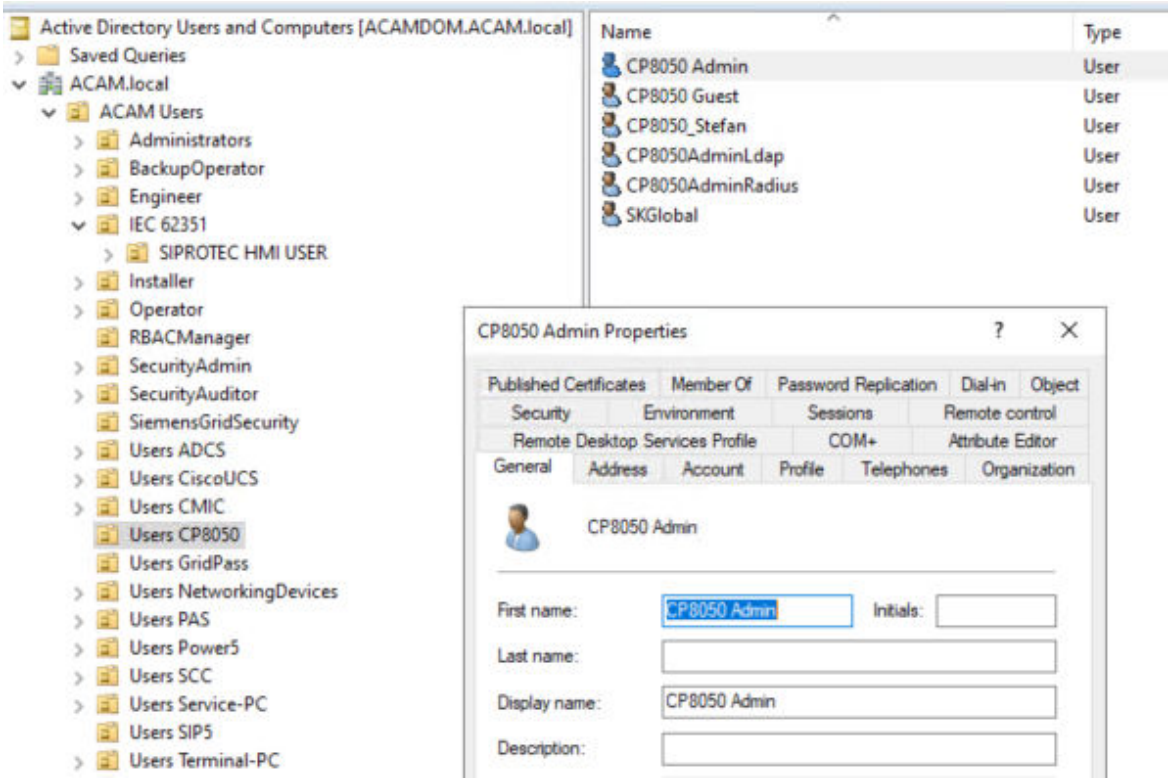
Preconditions

- SICAM PAS V08.20, CP-8050, CPCI85 V05.VH, SICAM GridPass V2.20 are installed.
- The CA certificate **GridPass CA 2022** exists on the SICAM GridPass server and **GridPass CA 2022** is the operational CA.

- SICAM CP-8050 and SICAM PAS received certificates from SICAM GridPass via EST.
- The LDAP server is configured in the active directory of the primary domain controller installed on a Microsoft Windows server 2022, 21H2 system.

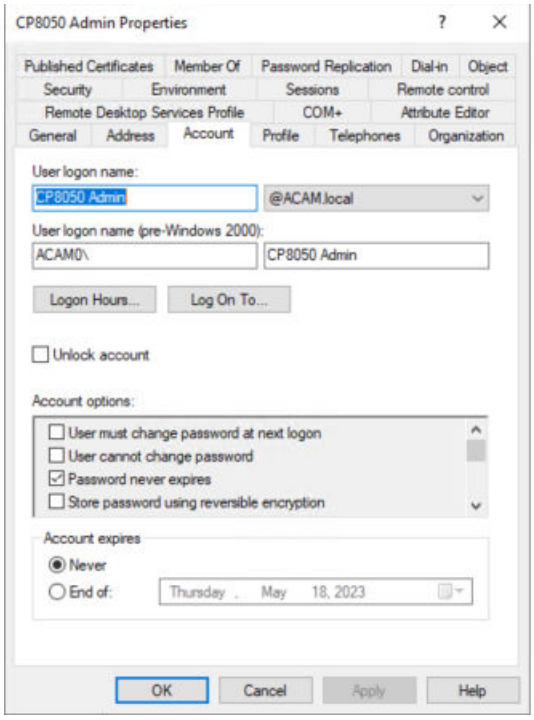
2.3.2 Creating an LDAP User in the Active Directory

✧ In the **General** tab enter a user name.
Use a name that complies with the user role, for example **CP8050 Admin**.



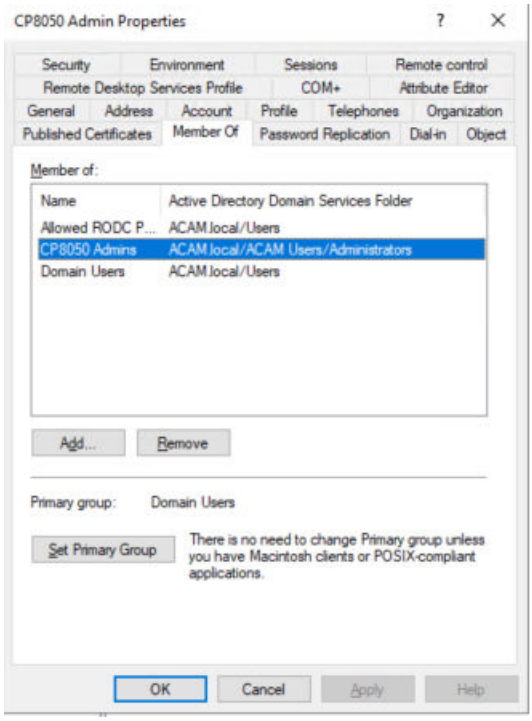
[sc_active-directory_create-a-user_general, 1, en_US]

✧ In the **Account** tab, enter the **User logon name**.



[sc_active-directory_create-a-user_account, 1, en_US]

✧ In the **Member of** tab, assign the user to the group **Admins**.



[sc_active-directory_create-a-user_member-of, 1, en_US]

NOTE

Before assigning the admin role via LDAP certificate, the user must be available in the Active Directory.

2.3.3 Settings in SICAM GridPass

Opening SICAM GridPass – LDAP, you can find the following settings information:

[sc_SicamGridPass_LDAP-configuration, 1, en_US]

IP address

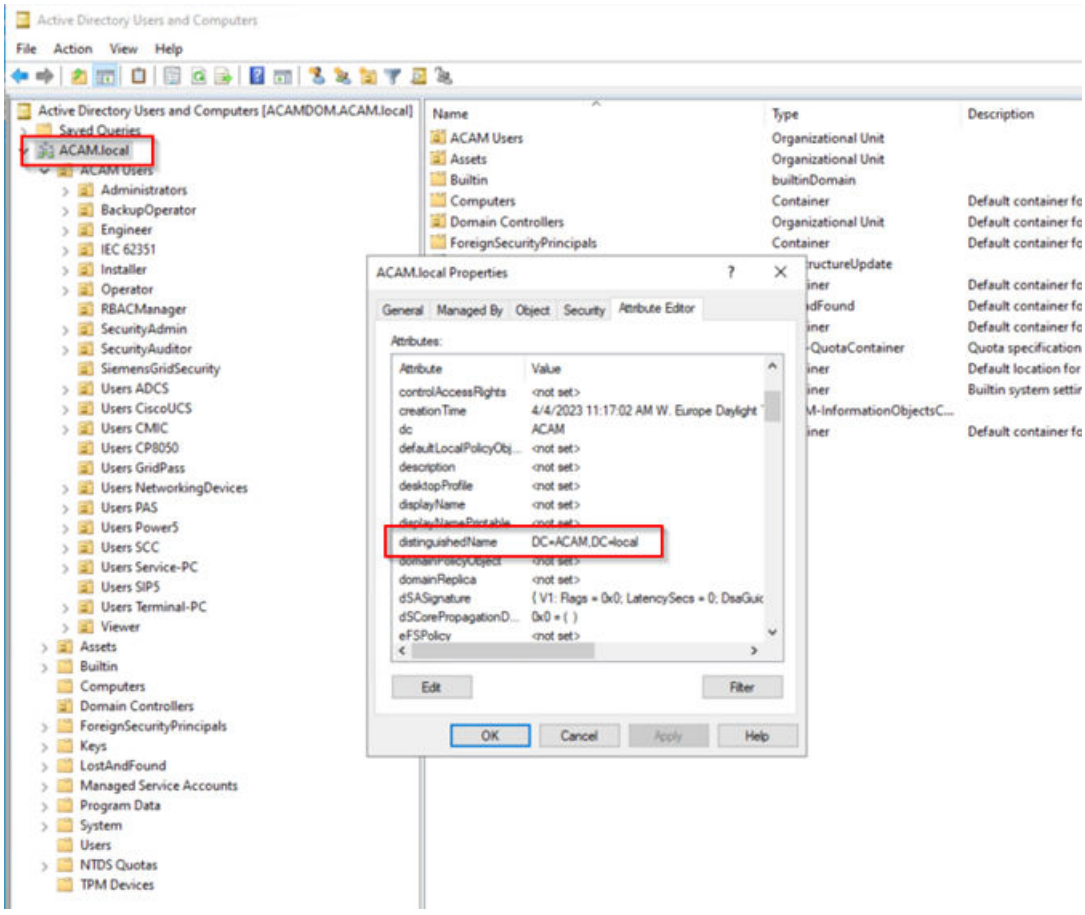
PDC/AD LDS server IP address

Port

389: for StartTLS communication

Search base

You can find the information to be used from the PDC Active Directory.
Therefore take the value from the generated user **CP8050Admin** in the Active Directory.

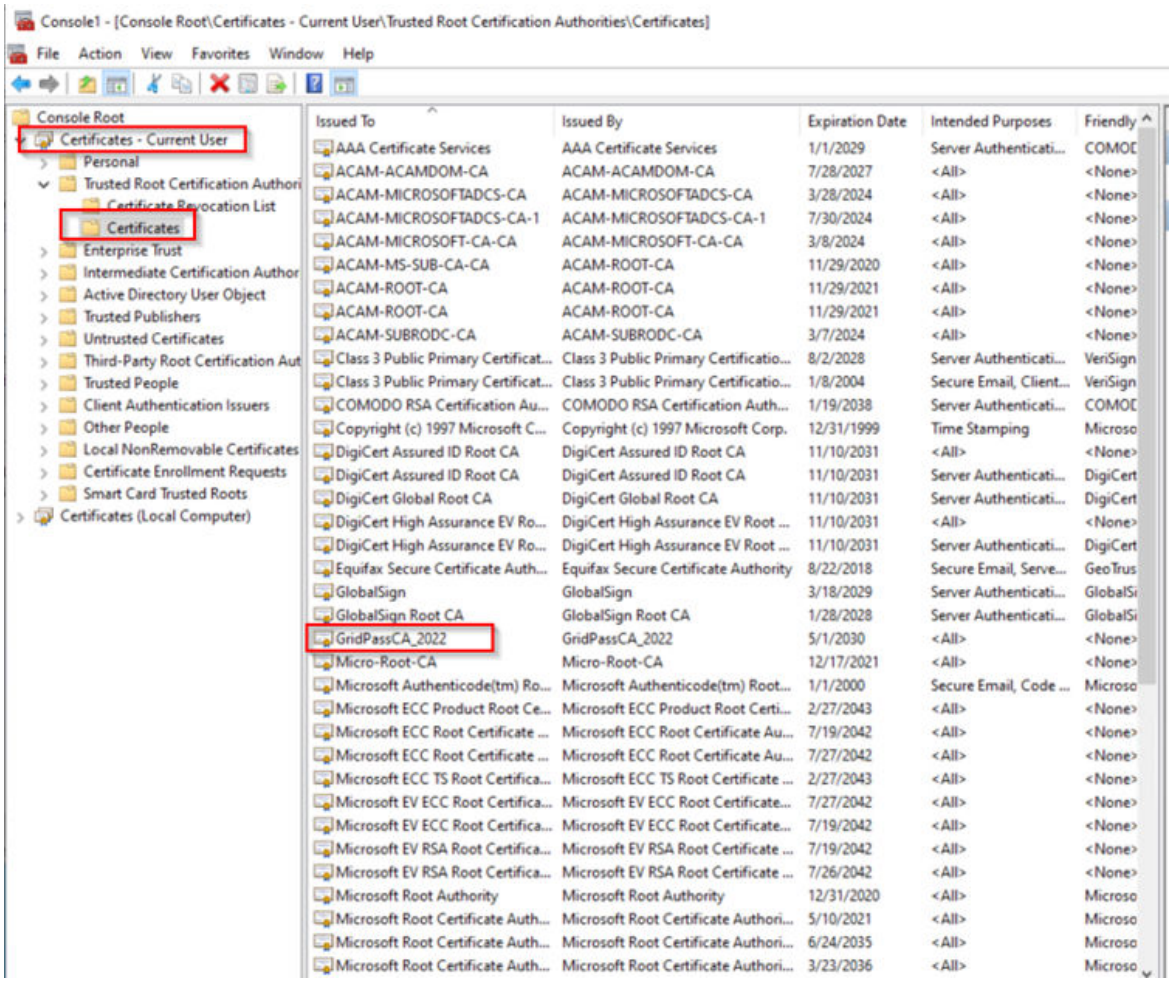


[sc_SicamGridPass_LDAP-configuration_search-base-value, 1, en_US]

Operational certification authority

As the LDAP server must trust the same Certification Authority (CA) as the SICAM GridPass server, you can import the SICAM GridPass CA of the SICAM GridPass server to the LDAP server. Or you can export a CA that already exists on the LDAP server and import it to SICAM GridPass as a CA.

In the following example, the CA **GridPassCA_2022** of the SICAM GridPass server was imported to the LDAP server.



[sc_CA-certificate-in-LDAP-server, 1, en_US]

2.3.4 Creating an LDAP Server Certificate

For generating a **request.csr**, you need to create a **request.inf** file.

NOTE

For detailled information about creating a request.inf file, refer to *Microsoft Learning platform*.

✧ Change the corresponding entries in the **request.inf** file under **Subject** and **[Extensions]**.
In the following example **ACAMDOM.ACAM.local** is used.

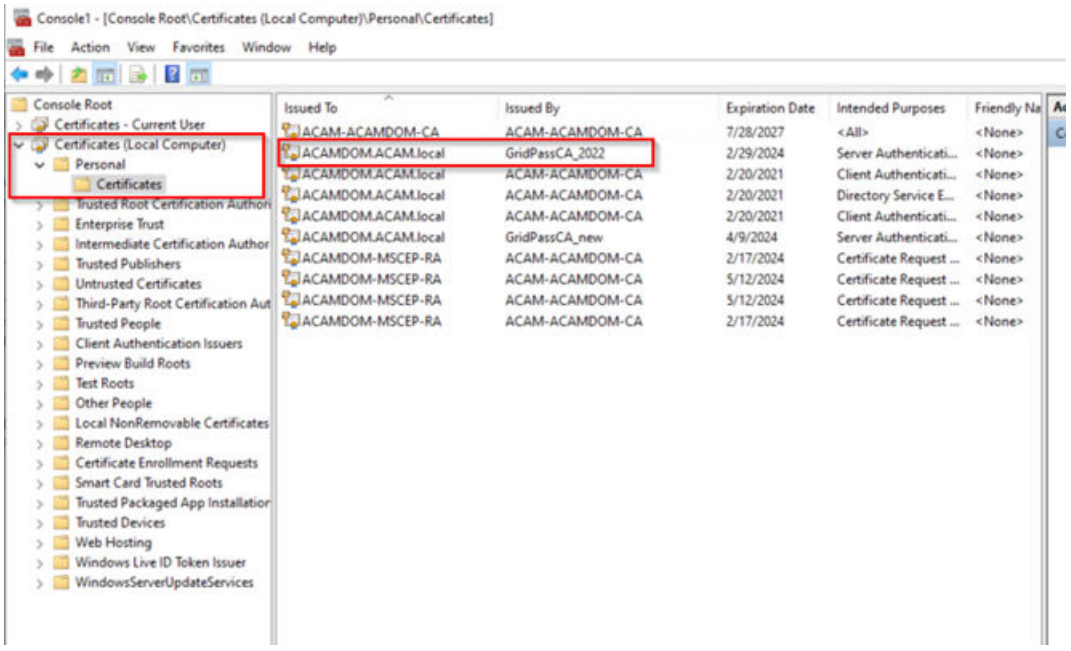
```
;----------------- request.inf-----------------

[Version]
Signature="$Windows NT$
[NewRequest]
Subject = "CN= ACAMDOM.ACAM.local ; replace with FQDN of Domain ControllerC
KeySpec = 1
KeyLength = 1024
; can be 1024, 2048, 4096, 8192 or 16384.
; larger key sizes are more secure however
```

```
; this has consequences to the performance.
export = TRUE
MachineKeySet = TRUE
SMIME = False
PrivateKeyArchive = FALSE
UserProtected = FALSE
UseExistingKeySet = FALSE
ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
ProviderType = 12
RequestType = PKCS10
KeyUsage = 0xa0
[EnhancedKeyUsageExtension]
OID=1.3.6.1.5.5.7.3.1 ; this is for server authentication
2.5.29.17 = "{text}"
_continue_ = "dns=ACAMDOM.ACAM.local&"
[Extensions]
_continue_ = "ipaddress=172.17.18.113&"
```

- ✧ Generate the request file by executing the following command in an administrator command console: certreq -new request.inf request.req
- ✧ Copy the request.req file to the SICAM GridPass system and sign the request in **Certificates** > **Import certificate signing request**.
- ✧ Select **Certificate Signing Request**.
- ✧ Select **All files** to see the **request.req** file.
- ✧ Click **Select CA for new certificate** and **Validity (days)**.
- ✧ In the following dialog, you find the **Subject alternate name** you edited in the request.inf file. You can leave the **CRL distribution point** blank.
- ✧ After confirming the dialog, a request.pem file is generated and can be downloaded.
- ✧ Copy this request.pem file to the LDAP server, rename it to request.cer and execute the following command in **LDAP server** > **Administrator cmd console**: Certreq -accept request.cer

The certificate is displayed in **Certificates** (local computer) > **Personal** > **Certificates**.



[sc_Valid-certificate-in-Certificate-store, 1, en_US]

Figure 2-1 Certificate in Certificate Store

✧ Restart the domain controller (LDAP server).

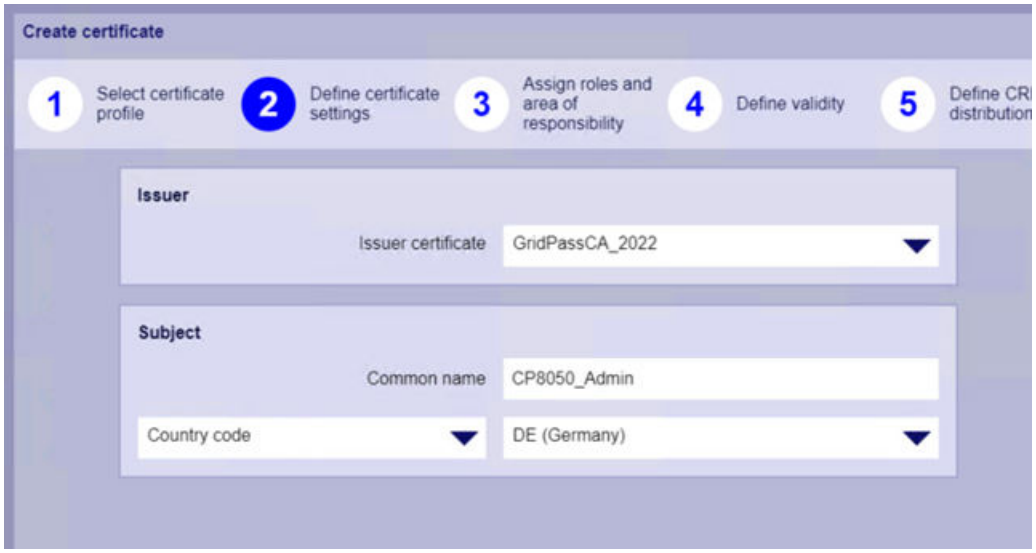
2.3.5 Generating Client Certificate for the LDAP User CP8050_Admin

✧ Open **SICAM GridPass** > **Certificates** > **Add certificate**.

✧ Select **TLS client** in **Select certificate profile**.

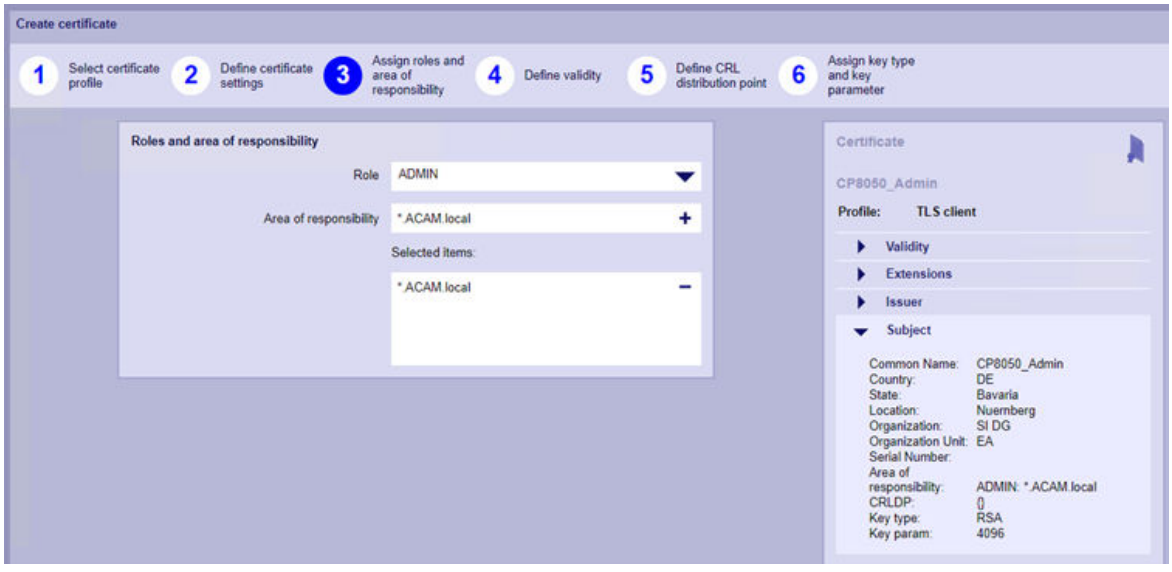
[sc_GenerateClientCertificate_for_LDAP-user, 1, en_US]

✧ Define the certificate settings.



[sc_GenerateClientCertificate_for_LDAP-user_certificate-settings, 1, en_US]

✧ Assign **Roles** and **Area of responsibility**.



[sc_GenerateClientCertificate_for_LDAP-user_AoR, 1, en_US]

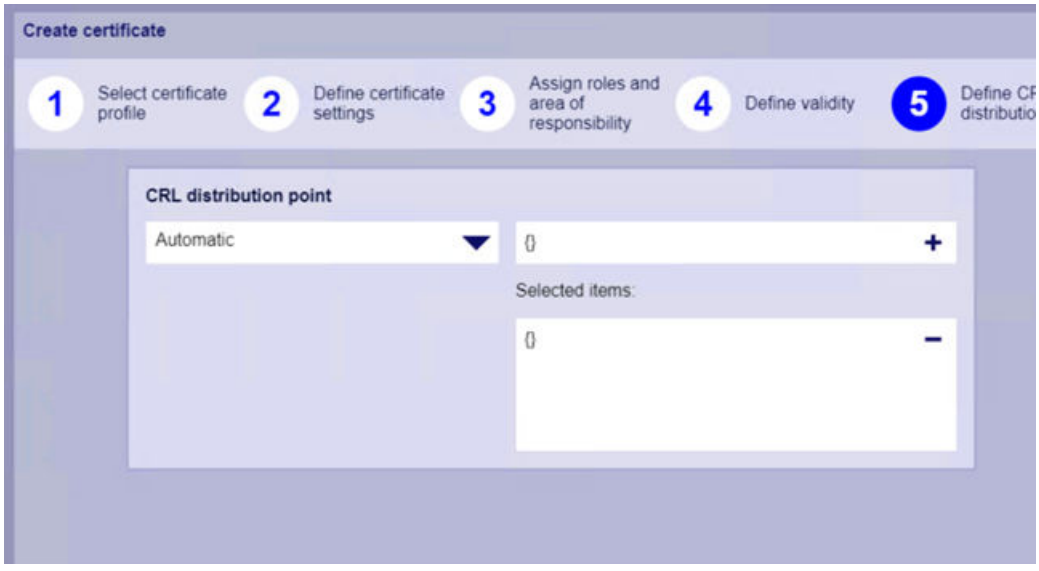
NOTE

- Do not use **Guest** as the role.
- The area of responsibility must fit with the AoR configured in the Toolbox/SICAM Device Manager for SICAM CP-8050 (*.ACAM.local).

✧ Define the validity.

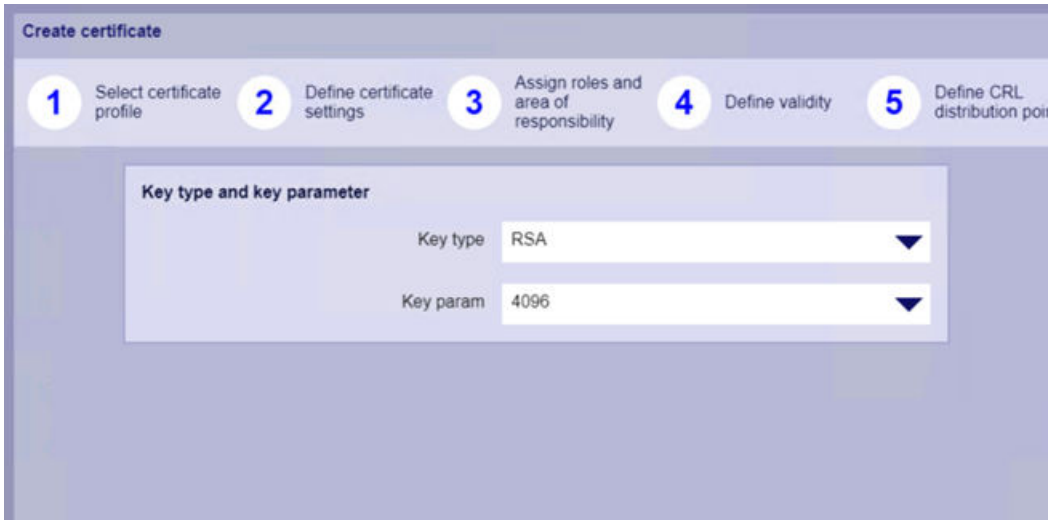
[sc_GenerateClientCertificate_for_LDAP-user_validity, 1, en_US]

✧ Select **Automatic** in the list box. so that the CRL distirbution point is written automatically to the created certificate with all SICAM GridPass system IP addresses and host names.



[sc_GenerateClientCertificate_for_LDAP-user_CRL, 1, en_US]

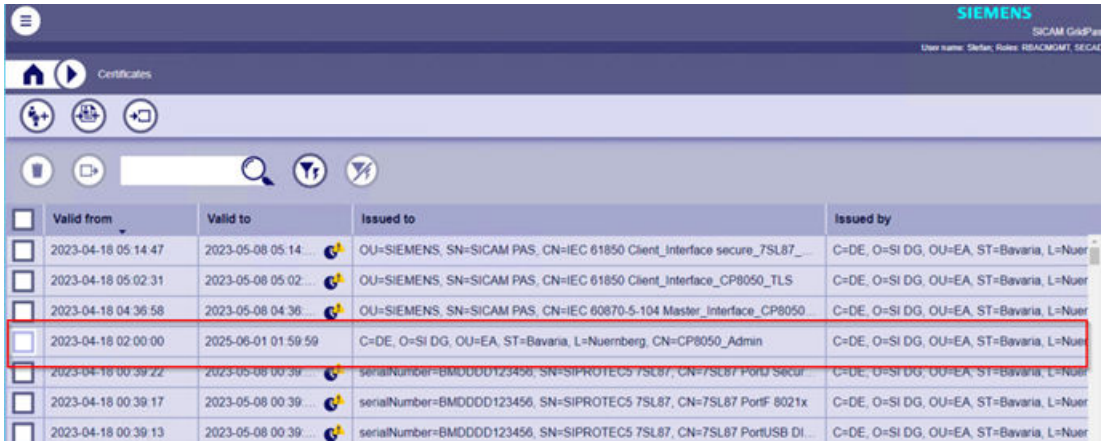
✧ Enter the key type and key parameter according to your encryption requirements, for example RSA and 4096.



[sc_GenerateClientCertificate_for_LDAP-user_Key-type, 1, en_US]

2.3.6 Exporting Certificates to LDAP Server

- ✧ In SICAM GridPass, select **Certificates**.
- ✧ In the certificates list, select **client certificate**, you generated in *2.3.5 Generating Client Certificate for the LDAP User CP8050_Admin*.

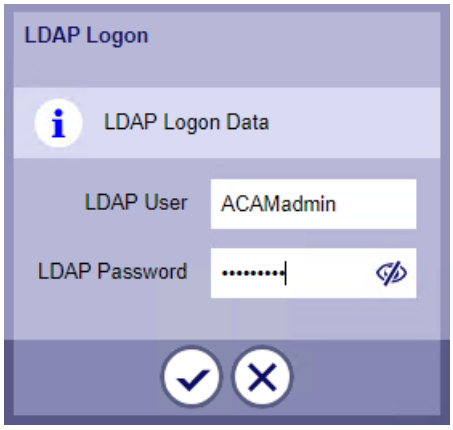


[sc_Export-LDAP-certificate_overview, 1, en_US]

- ✧ Select **Export**.
- ✧ Select **Directory service (LDAP)**.

[sc_Export-LDAP-certificate, 1, en_US]

✧ Enter the name of the LDAP server administrator in the text box **LDAP User**.

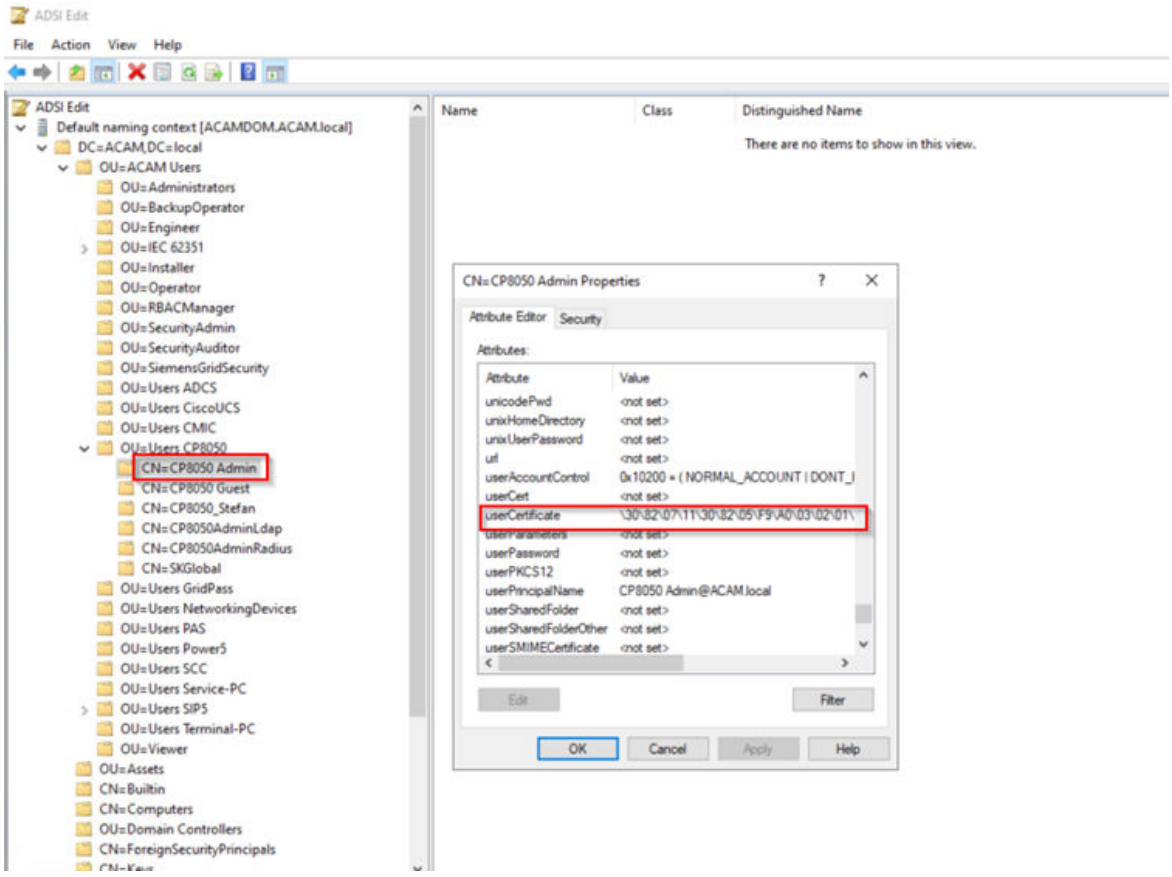


[sc_LDAP-server-user-login, 1, en_US]

✧ Enter the password.

✧ Select **OK**.

The certificate is exported from SICAM GridPass.
Now you can find the published certificate in AD LDS for the user **CP8050_Admin**.

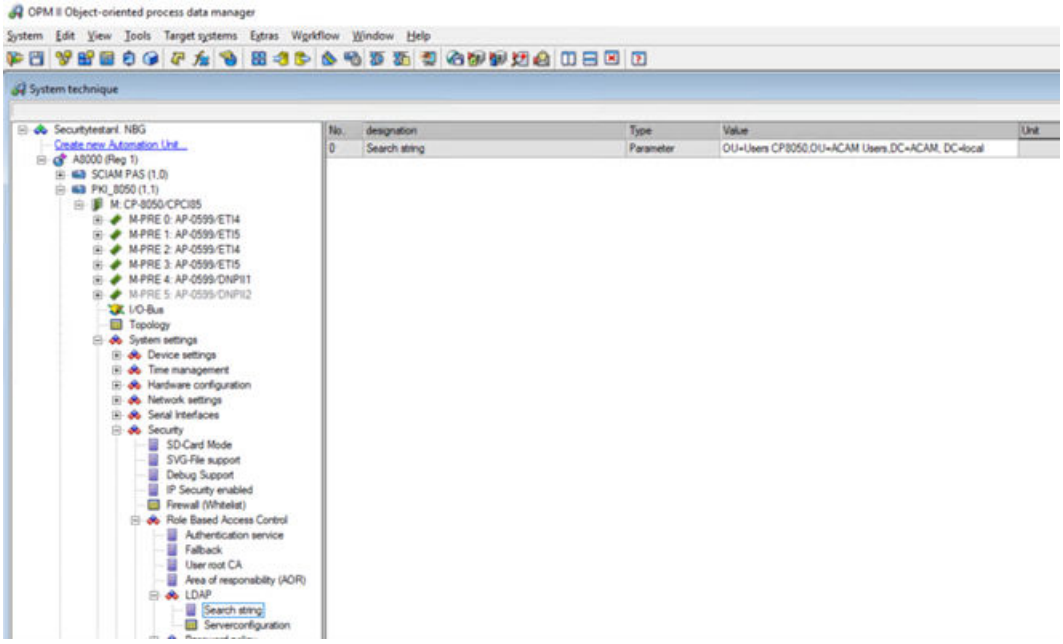


[ID-user-certificate-in AD-LDS, 1, en_US]

Figure 2-2 ID User Certificate in AD LDS

2.4 Configuring SICAM CP-8050 for LDAP Authentication in SICAM Toolbox/Device Manager

To prepare a SICAM CP-8050 device for LDAP authentication, parameters must be configured in: Toolbox > OPM > System Technique > M:CP-8050/CPCI85 > System Settings > Security.



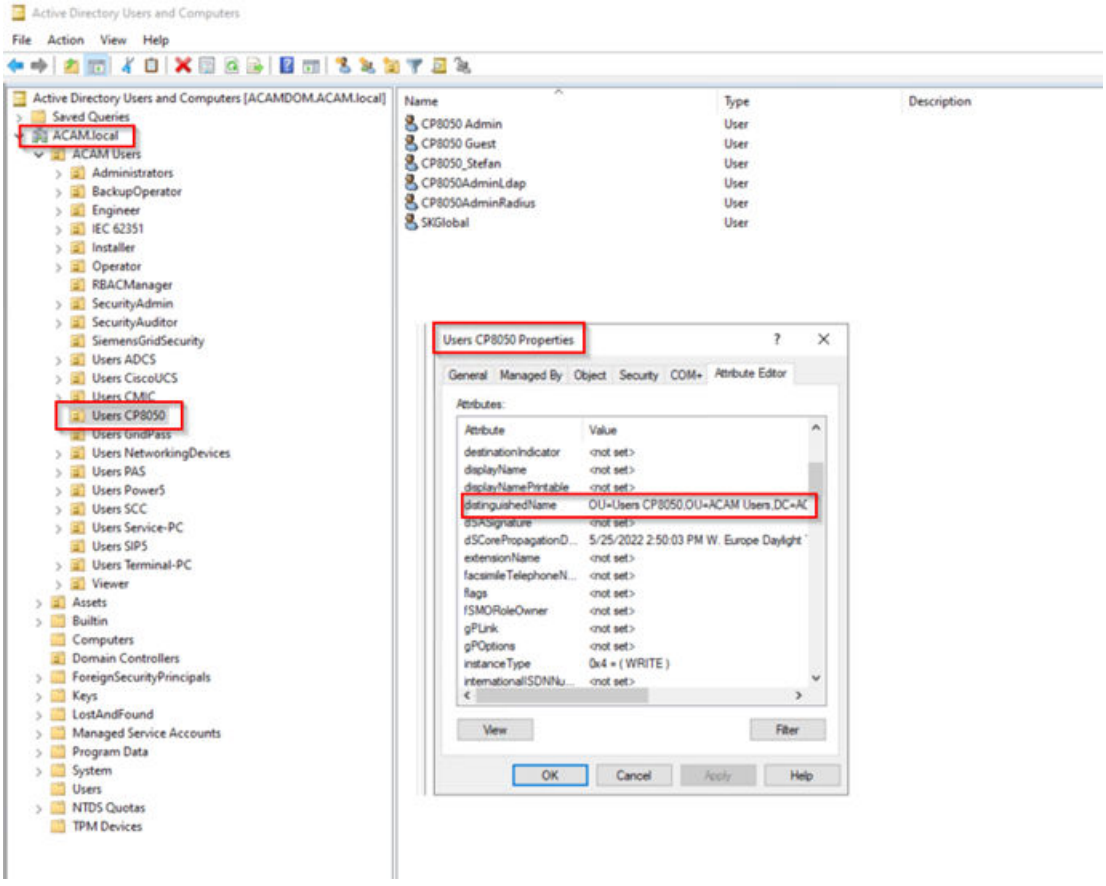
[sc_Toolbox_LDAP-configuration, 1, en_US]

✧ Set the following parameters in **Role-Based Access Control**:

- **Authentication service**:
  LDAP with STARTTLS: port 389 in firewall
  LDAPS: port 636 in firewall for secure communication
- **Fallback**: yes
- **User root CA**: not used
- **Area of responsibility**: domain of the user login.

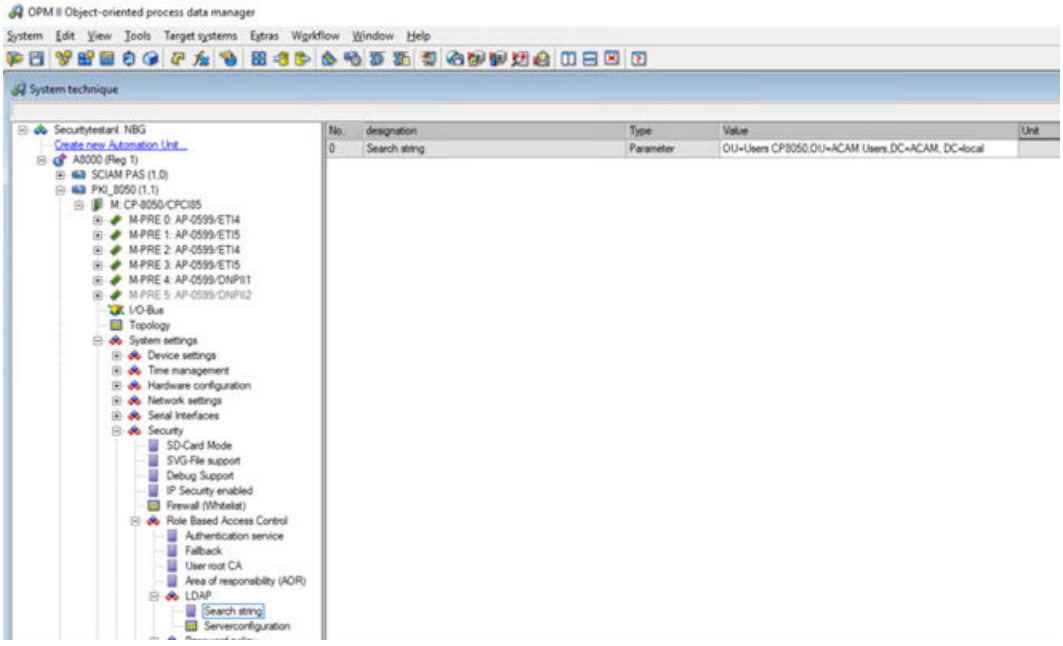
LDAP – Search String

✧ Take the LDAP search string from the LDAP server, active directory, user properties > **distinguished-Name**. It describes where the user will be found in the active directory structure.



[sc_active-directory_of_LDAP-server, 1, en_US]

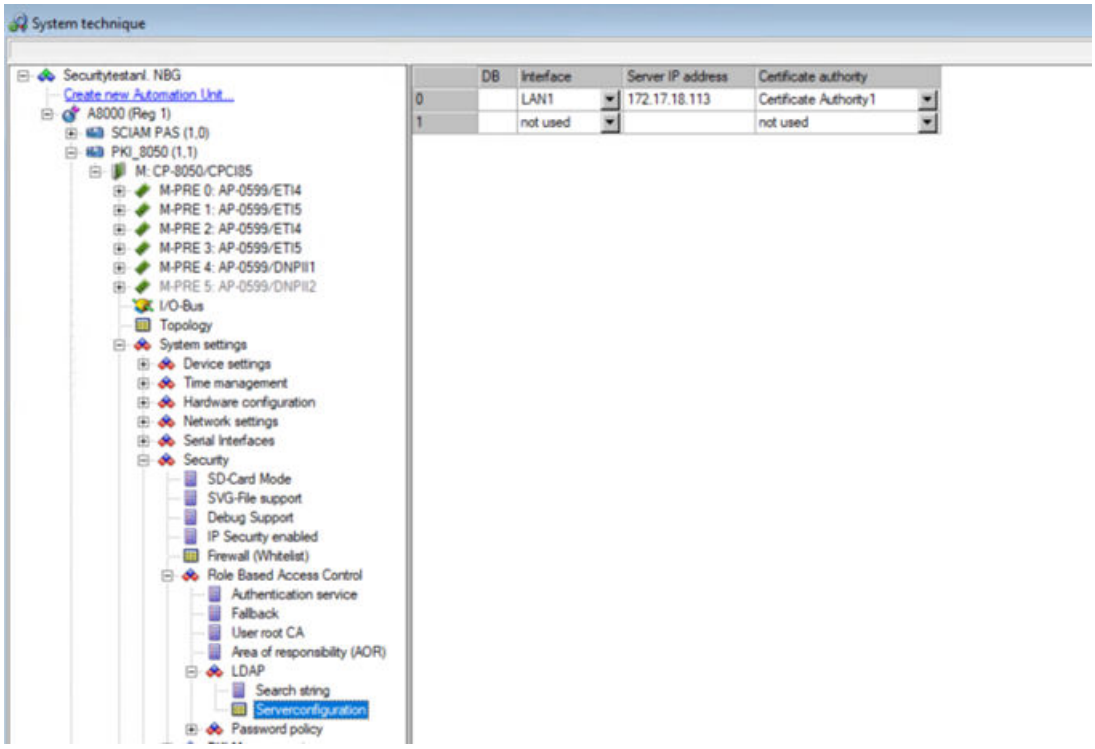
✧ Copy the string and paste it to the search string.



[sc_Toolbox_LDAP-configuration, 1, en_US]

LDAP – Toolbox LDAP Configuration

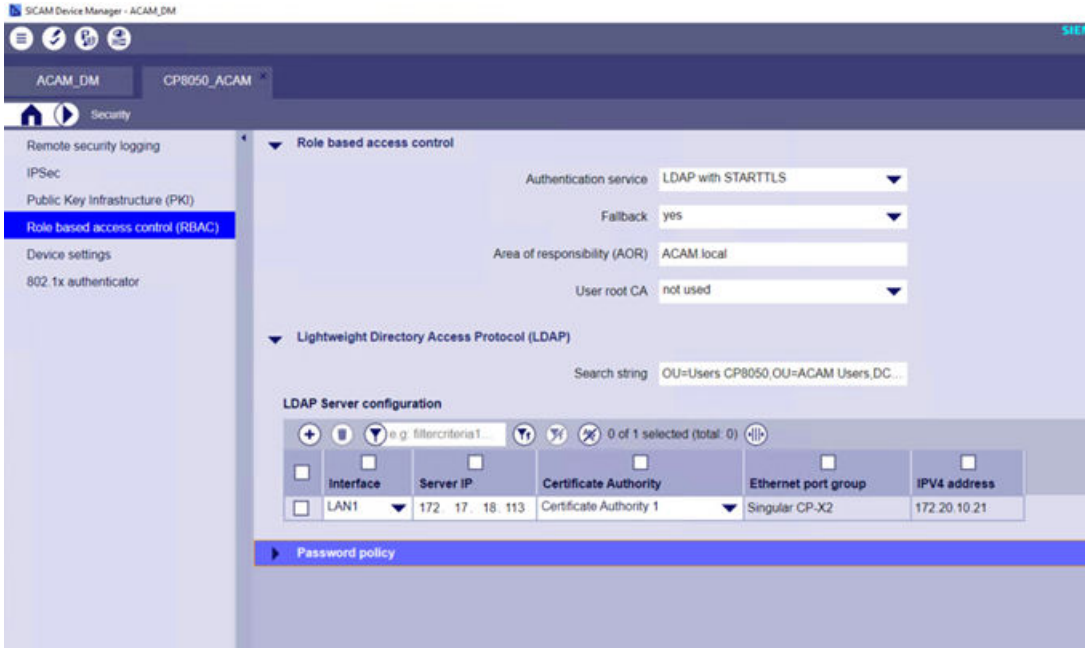
✧ In **LDAP > Serverconfiguration**, determine the container (for example **Certificate Authority 1**) into which you want to load the CA certificate in the Web interface of the SICAM CP-8050 (see also *Figure 2-4*).



[sc_server-configuration_LDAP-server, 1, en_US]

LDAP Configuration – SICAM Device Manager

✧ If you use SICAM Device Manager instead of Toolbox, do the configuration for LDAP authentication in **Security** > **Role Base Access Control (RBAC)**.



[sc_device-manager_LDAP-configuration_complete, 1, en_US]

The certificate **Certificate Authority1** in the LDAP server configuration is the CA certificate (GridPassCA_2022) which was imported to the LDAP server before.

[sc_CA-certificate_in_GridPass, 1, en_US]

Figure 2-3 CA Certificate in SICAM GridPass

This certificate must be imported via the Web interface of the SICAM CP-8050.

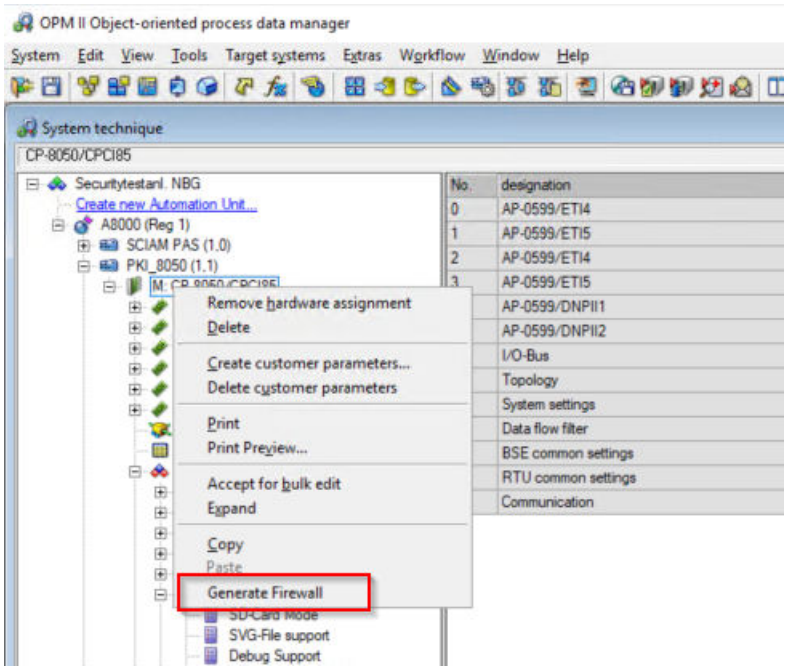
[sc_CA-certificate-import_in_CP8050, 1, en_US]

Figure 2-4 Upload Certificate

Generating the Firewall in the Toolbox

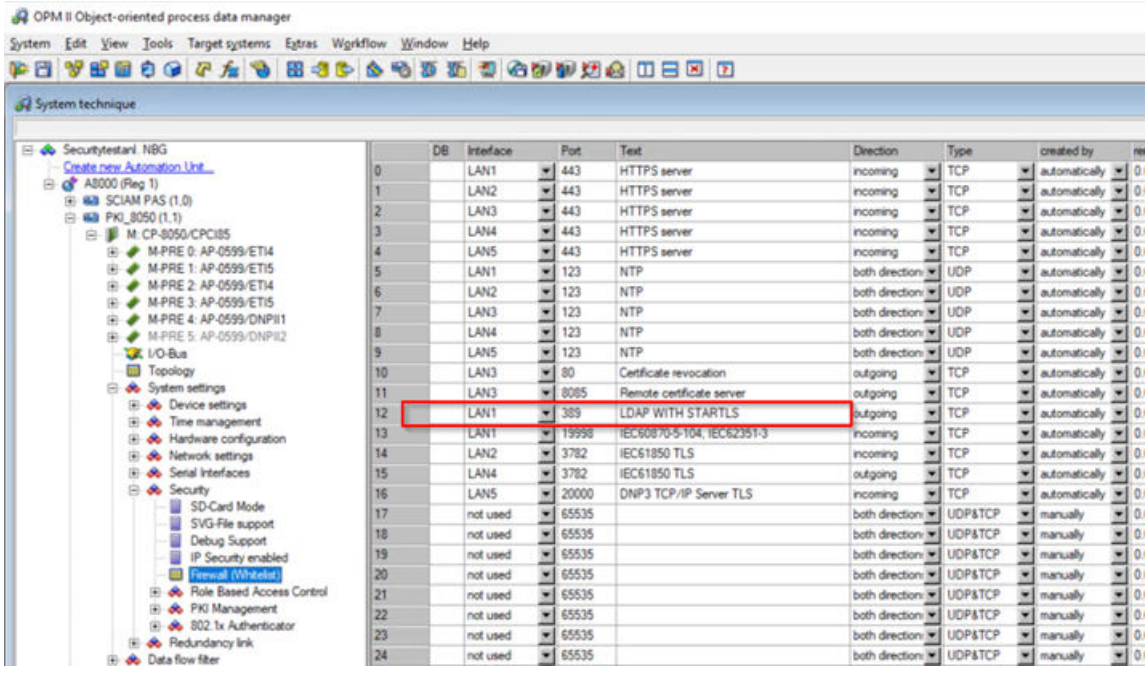
Depending on the setting in **Authentication service**, different ports are used.

- ✧ Open the corresponding ports in the firewall of the SICAM CP-8050:
- ✧ Select **Toolbox** > **M:CP-8050/CPCI85**.
- ✧ Right-click **Generate Firewall**.



[sc_Toolbox_Generate-Firewall, 1, en_US]

The open LDAP ports are shown:



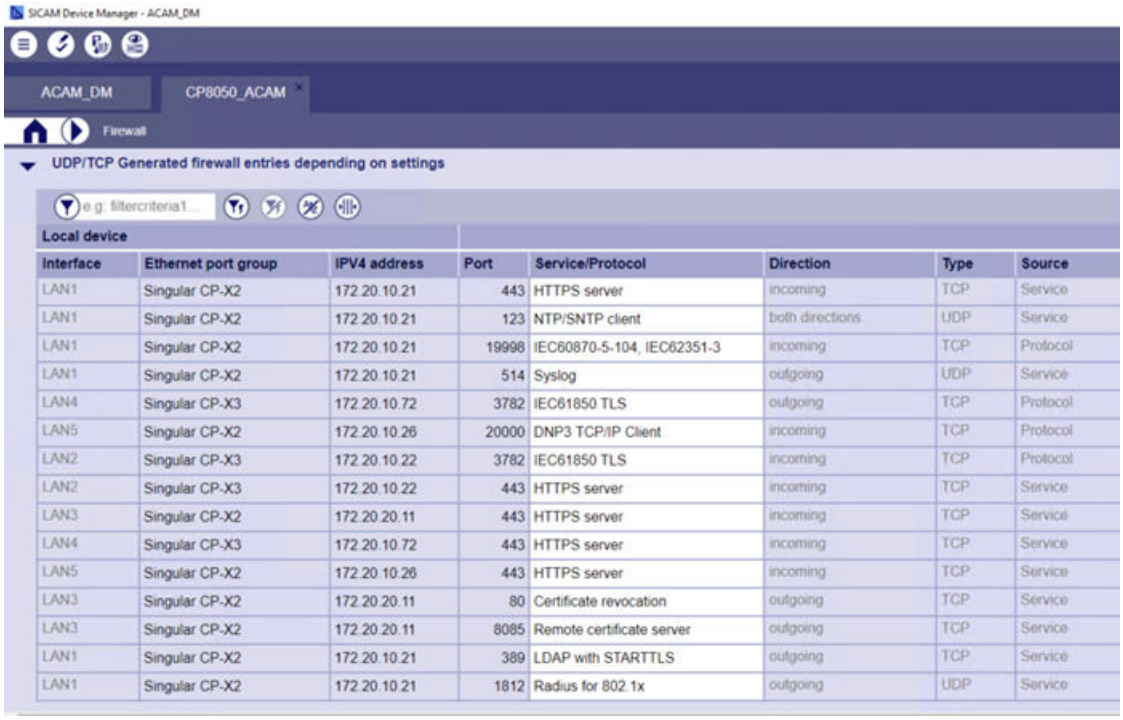
[sc_Toolbox_Generate-Firewall_open_LDAP-port, 1, en_US]

✧ Save and transmit data to the SICAM CP-8050.

Generating the Firewall in the SICAM Device Manager

Unlike to the Toolbox, in the SICAM Device Manager the firewall is generated automatically during the configuration of the parameters.

✧ The following dialog shows the open LDAP ports:

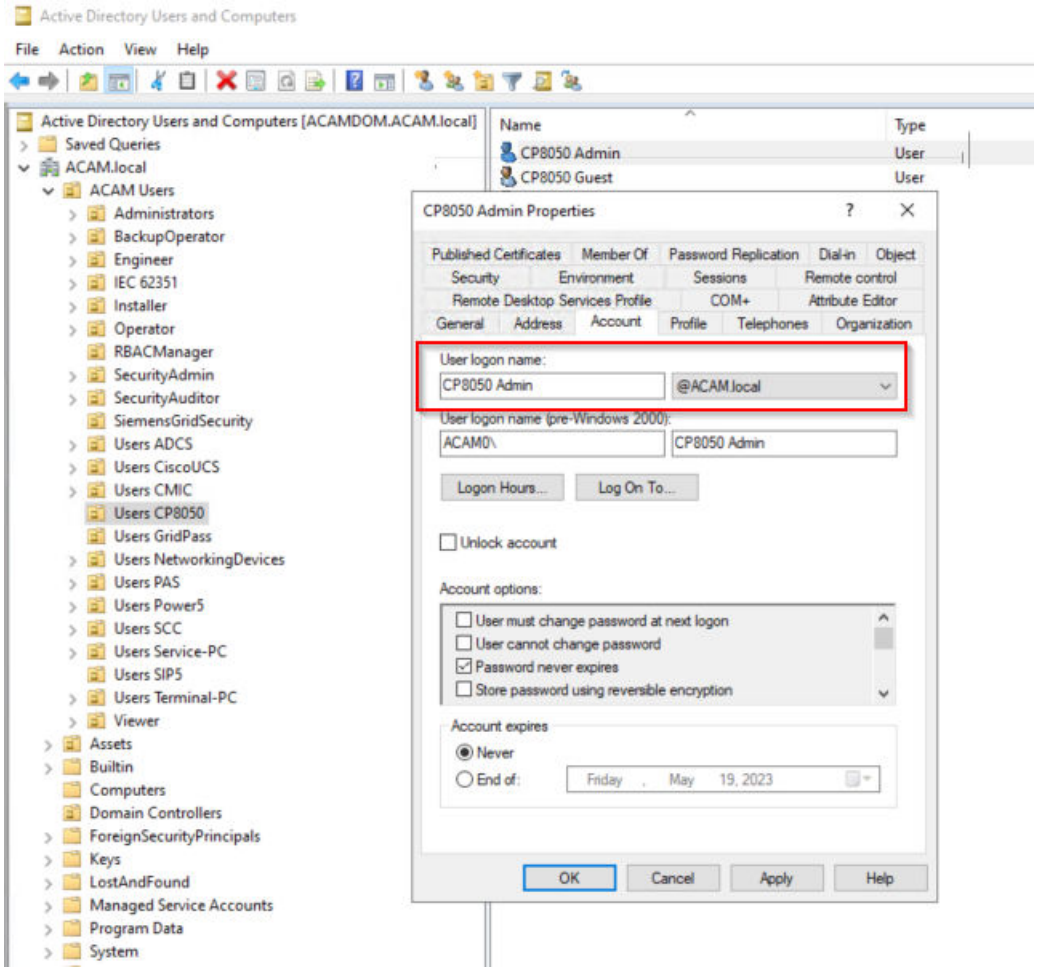


Interface	Ethernet port group	IPV4 address	Port	Service/Protocol	Direction	Type	Source
LAN1	Singular CP-X2	172.20.10.21	443	HTTPS server	incoming	TCP	Service
LAN1	Singular CP-X2	172.20.10.21	123	NTP/SNTP client	both directions	UDP	Service
LAN1	Singular CP-X2	172.20.10.21	19998	IEC60870-5-104, IEC62351-3	incoming	TCP	Protocol
LAN1	Singular CP-X2	172.20.10.21	514	Syslog	outgoing	UDP	Service
LAN4	Singular CP-X3	172.20.10.72	3782	IEC61850 TLS	outgoing	TCP	Protocol
LAN5	Singular CP-X2	172.20.10.26	20000	DNP3 TCP/IP Client	incoming	TCP	Protocol
LAN2	Singular CP-X3	172.20.10.22	3782	IEC61850 TLS	incoming	TCP	Protocol
LAN2	Singular CP-X3	172.20.10.22	443	HTTPS server	incoming	TCP	Service
LAN3	Singular CP-X2	172.20.20.11	443	HTTPS server	incoming	TCP	Service
LAN4	Singular CP-X3	172.20.10.72	443	HTTPS server	incoming	TCP	Service
LAN5	Singular CP-X2	172.20.10.26	443	HTTPS server	incoming	TCP	Service
LAN3	Singular CP-X2	172.20.20.11	80	Certificate revocation	outgoing	TCP	Service
LAN3	Singular CP-X2	172.20.20.11	8085	Remote certificate server	outgoing	TCP	Service
LAN1	Singular CP-X2	172.20.10.21	389	LDAP with STARTTLS	outgoing	TCP	Service
LAN1	Singular CP-X2	172.20.10.21	1812	Radius for 802.1x	outgoing	UDP	Service

[sc_device-manager_overview-firewall_open_LDAP-port, 1, en_US]

Logon to CP-8050 Web User Interface with the LDAP User CP8050Admin

✧ To log on use the fully qualified user account for example **CP8050Admin@ACAM.local**.



[sc_User-Account_LDAP-user_Active-Directory, 1, en_US]

[sc_Log-on_to_CP8050_with_LDAP-user_account, 1, en_US]

NOTE

The fallback logon (for example Administrator) does only work in case the network connection between the SICAM CP-8050 and the LDAP server is disabled/interrupted.

2.5 Creating LDAP Attribute Certificates for SICAM A8000, CP-8050

Preconditions

- SICAM CP-8050, SICAM CPCI85 V05, SICAM GridPass V2.20, AD LDS are installed
- AD LDS (Active Directory Lightweight Directory Service) server is configured in the active directory of the primary domain controller installed on a Microsoft Windows server 2022, 21H2 system
- User **CP8050Admin** is created in the active directory/LDAP server (see also *2.3.2 Creating an LDAP User in the Active Directory*)

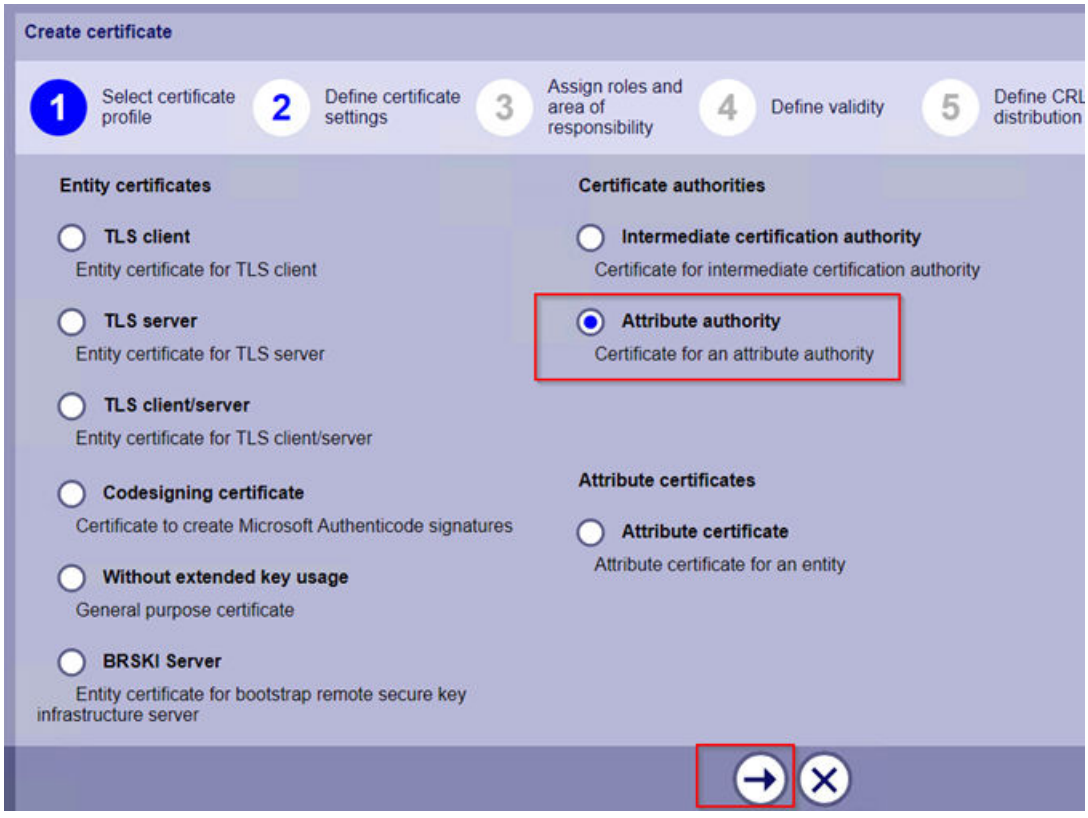
Use Case

The user **CP8050Admin** has the role **DataEngineer**. The user can configure a SICAM A8000 device via the Web interface. Because an OPERATOR colleague of the CP8050Admin user is out of office for a while, CP8050Admin user must deal with the OPERATOR tasks. So, an attribute certificate with the role OPERATOR is generated in SICAM GridPass and exported to the CP8050Admin user. The attribute certificate has a short validity, only for the time the OPERATOR colleague is out of office.

Creating an Attribute Authority

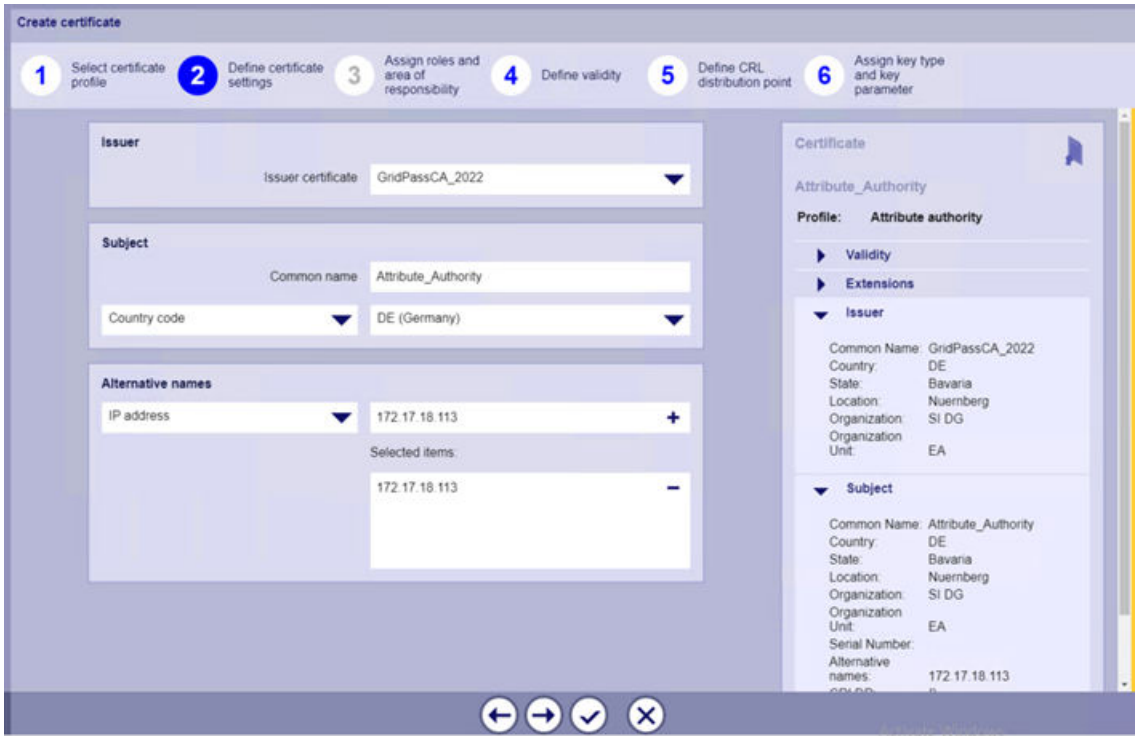
✧ Open **SICAM GridPass** > **Certificates** > **Add certificate**.

✧ Select **Attribute authority**.



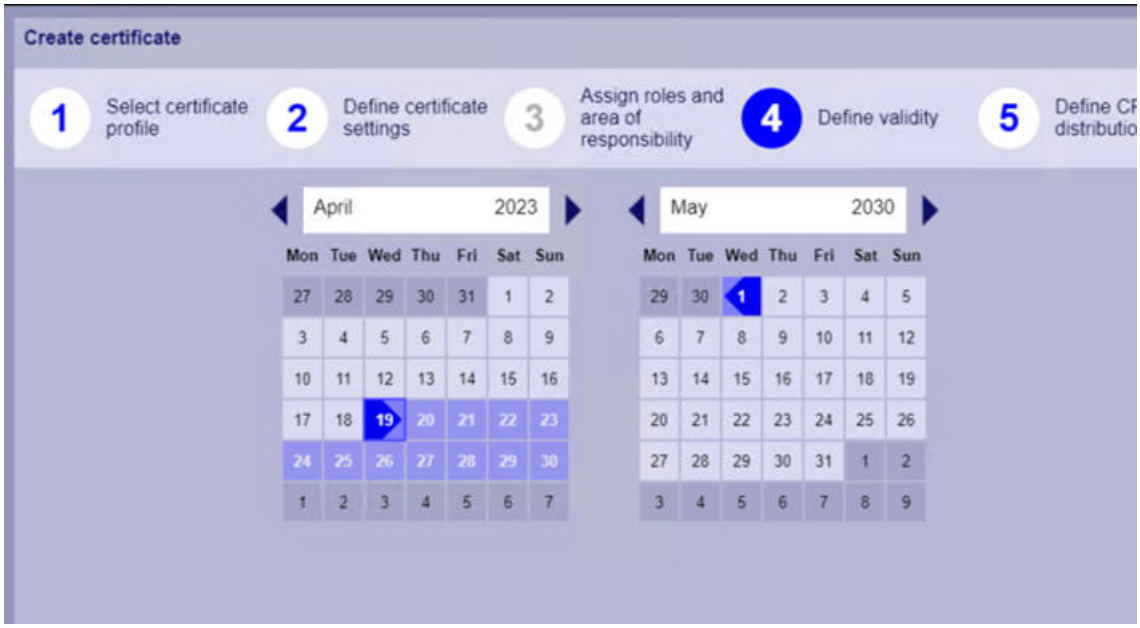
[sc_Sicam GridPass_create-attribute-authority_certificate-profil, 1, en_US]

✧ Define the certificate settings.



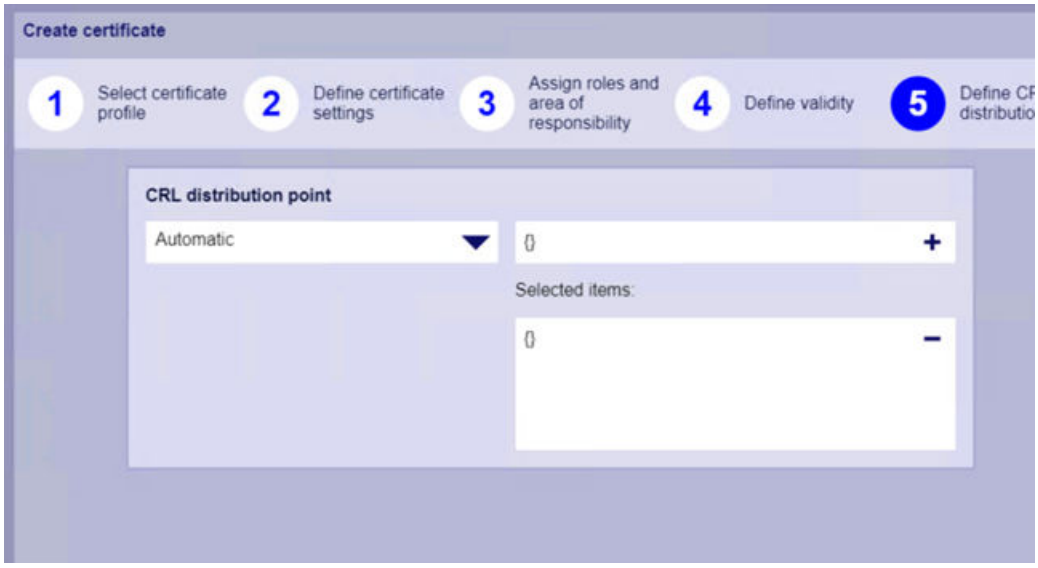
[sc_SicamGridPass_Create-Attribute-Authority_Certificate-settings, 1, en_US]

✧ Define the validity.



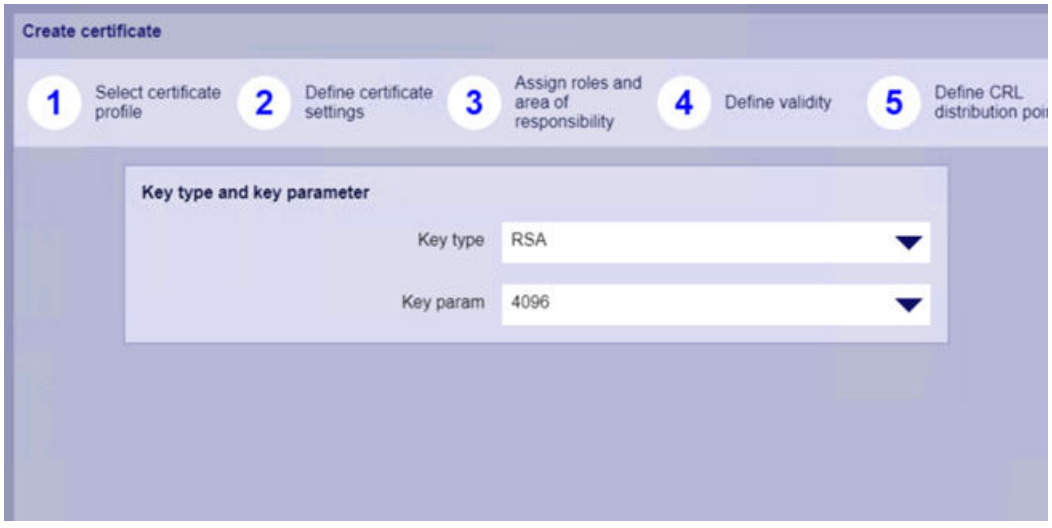
[sc_SicamGridPass_Create-Attribute-Authority_validity, 1, en_US]

✧ Create the CRL distribution point.



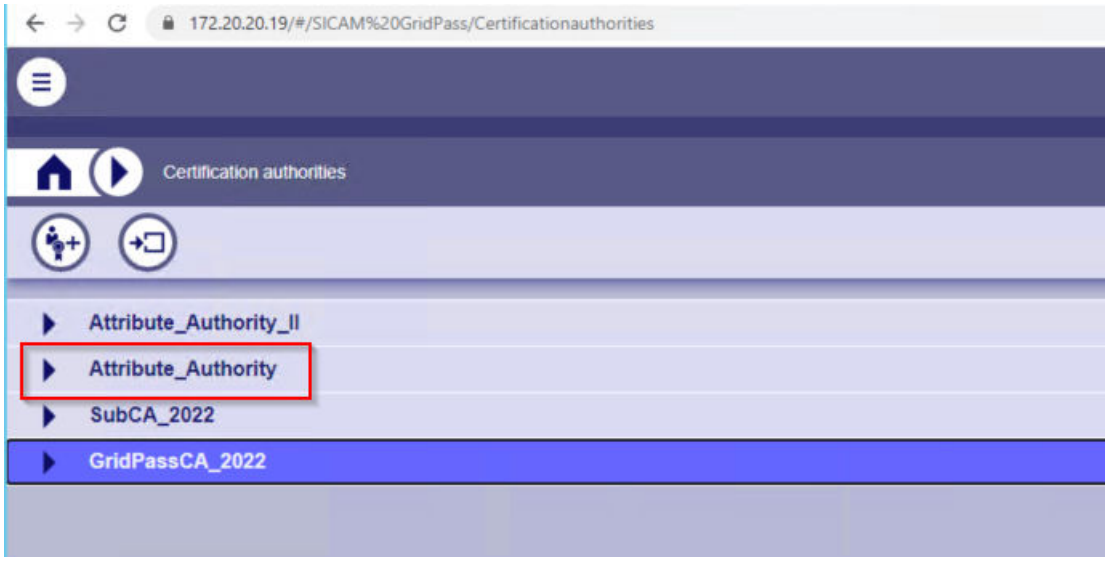
[sc_GenerateClientCertificate_for_LDAP-user_CRL, 1, en_US]

✧ Enter the key type and key parameter.



[sc_GenerateClientCertificate_for_LDAP-user_Key-type, 1, en_US]

An attribute authority is created.



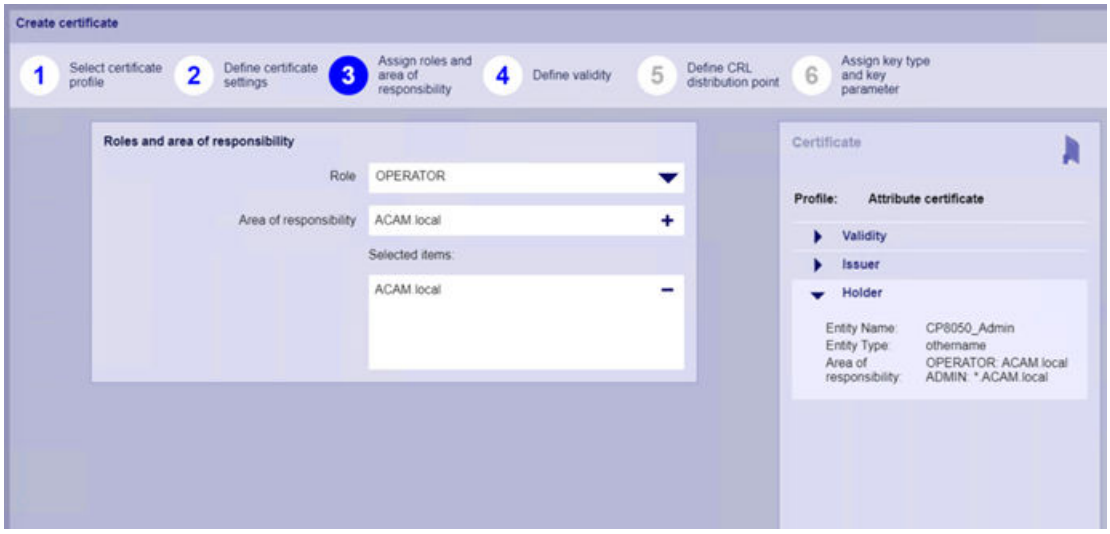
[sc_SicamGridPass_Attribute-Authority, 1, en_US]

Creating the Attribute Certificate for the LDAP User CP8050_Admin with the Role OPERATOR

- ✧ Open **SICAM GridPass** > **Certificates** > **Add certificate**.
- ✧ Select **Attribute certificate**.
- ✧ In **Define certificate settings**, select either the ID certificate of the user **CP5050_Admin** for **Entity certificate** or enter the user name **CP8050_Admin** for **Entity name**.

[sc_SicamGridPass_create_Attribute-Certificate_settings, 1, en_US]

- ✧ In **Assign roles and areas of responsibility**, select the role **OPERATOR** and fill in the area of responsibility **ACAM.local**.



[sc_SicamGridPass_create_ Attribute-Certificate_AoR, 1, en_US]

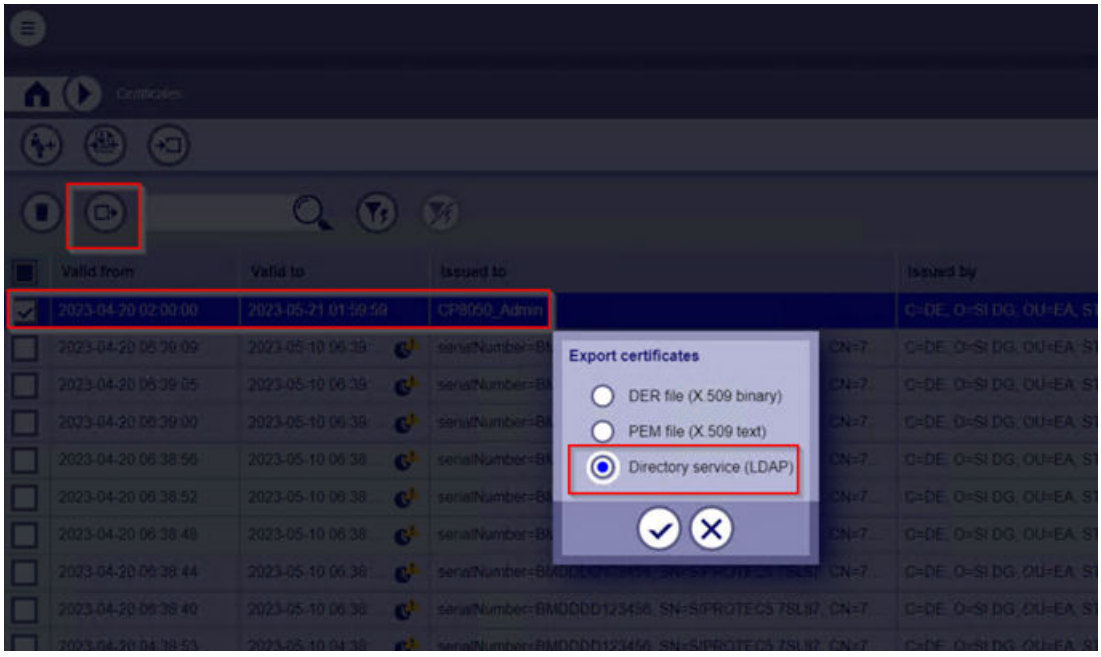
✧ Define the validity.

[sc_SicamGridPass_create_ Attribute-Certificate_validity, 1, en_US]

The attribute certificate is created.

Exporting Attribute to LDAP

✧ In the **Certificates** check the attribute certificate and click **Export certificates**.

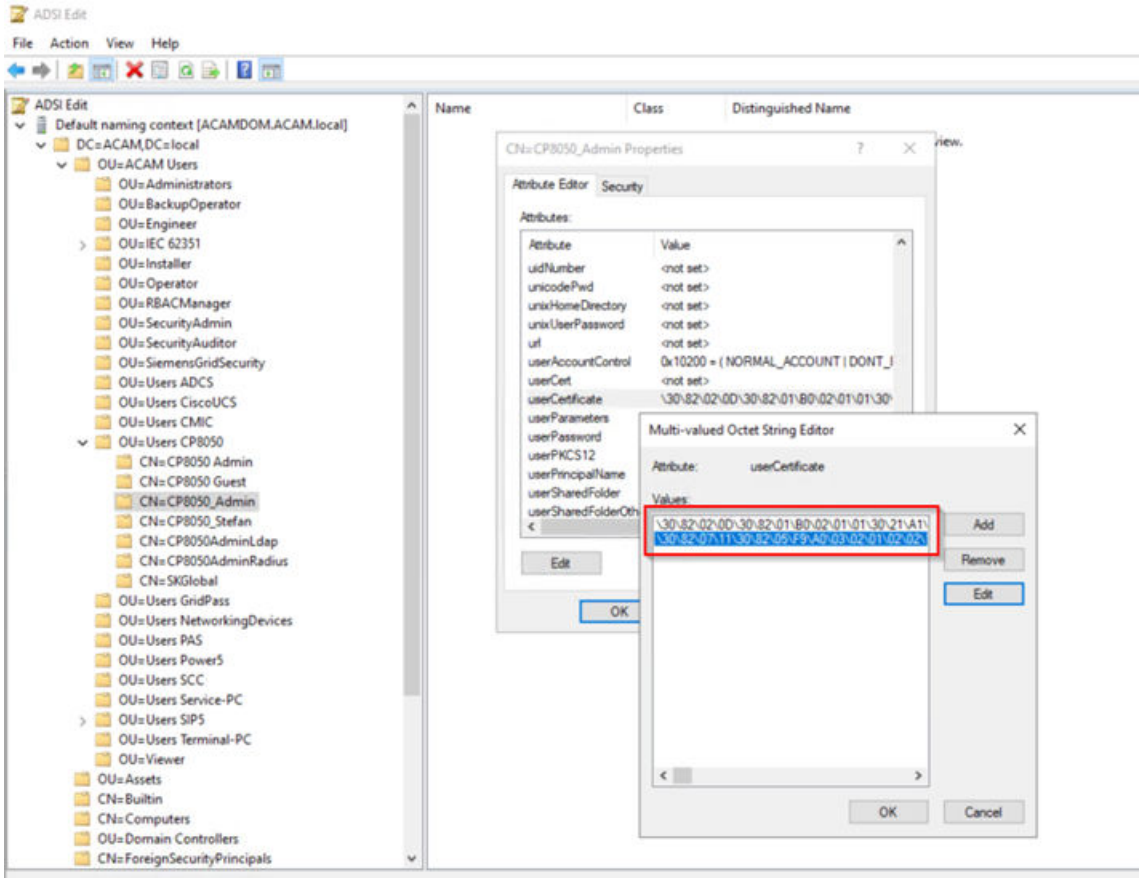


[sc_SicamGridPass_create_ Attribute-Certificate_export, 1, en_US]

✧ To execute the export, enter the credentials of the AD LDS Administrator user.

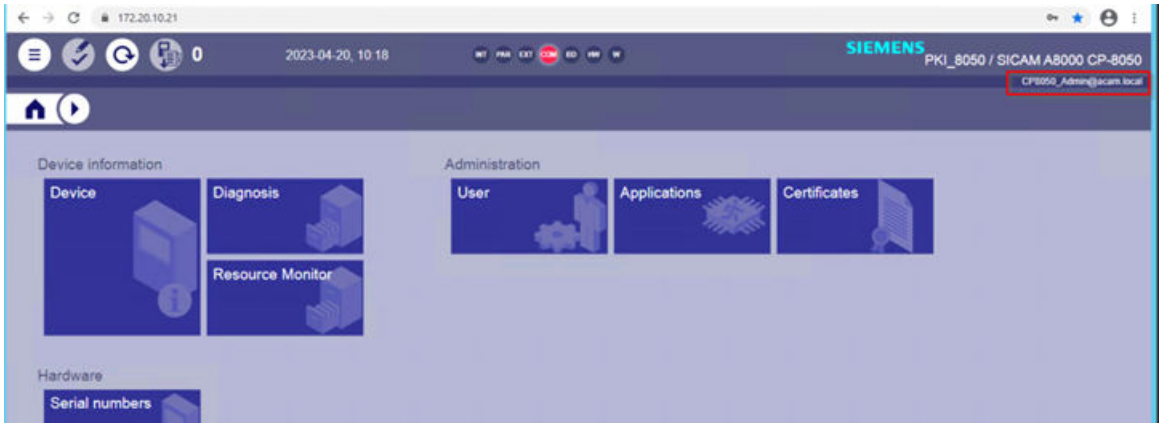
[sc_SicamGridPass_create_ Attribute-Certificate_export_LDAPuser-logon, 1, en_US]

The exported attribute and ID certificates are visible in AD LDS (ADSI Edit).



[sc_Attribute-Certificate_in_AD-LDS, 1, en_US]

After logon and authentification via LDAP the roles that were assigned with the attribute certificates are available.



[sc_CP8050WebUI_Logon_CP8050_Admin, 1, en_US]

2.6 Creating LDAP User Certificates for SIPROTEC 5, DIGSI 5

Preconditions

- DIGSI 5 V09.40, SIPROTEC 5 V09.40, SICAM GridPass V2.20 are installed
- AD LDS (Active Directory Lightweight Directory Service) server is configured in the active directory of the primary domain controller (domain= “ACAM.local”) installed on a Microsoft Windows Server 2022 system

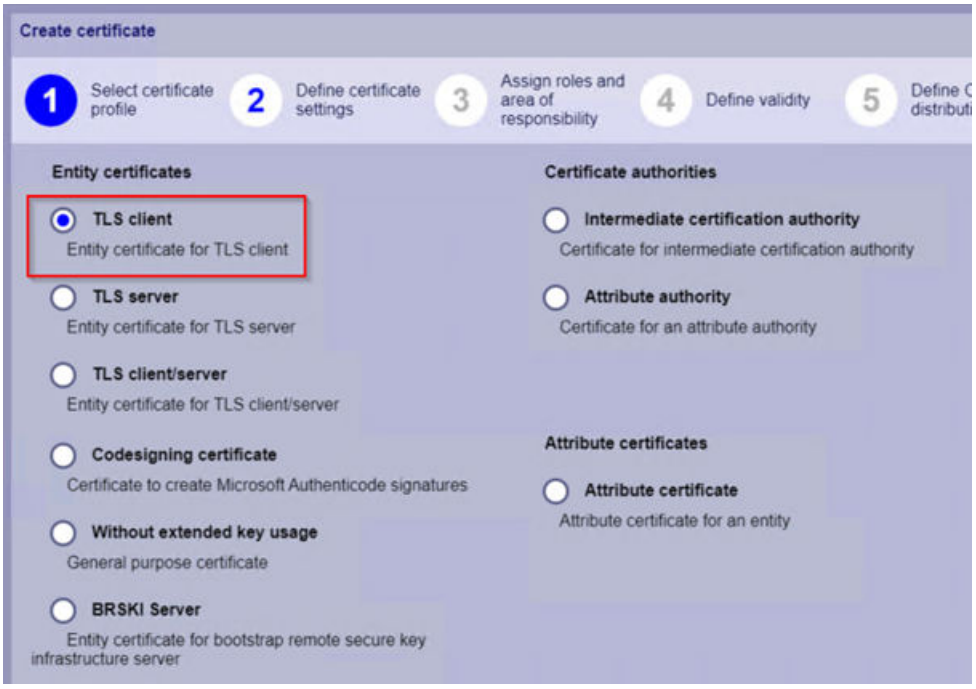
- There is a user defined in the active directory, for example **SKadmin**
- An LDAP server is configured in SICAM GridPass.

Use Case

Different DIGSI 5 users with different roles/access rights are managed by an active directory of a Microsoft Windows server 2022 operating system which is also an LDAP server. According to the specific role, for example **Administrator**, **Security Admin**, **Operator**, the users are allowed to do, for example, configuration changes, security-relevant tasks or only supervisory operations. The relevant certificates are generated with SICAM GridPass.

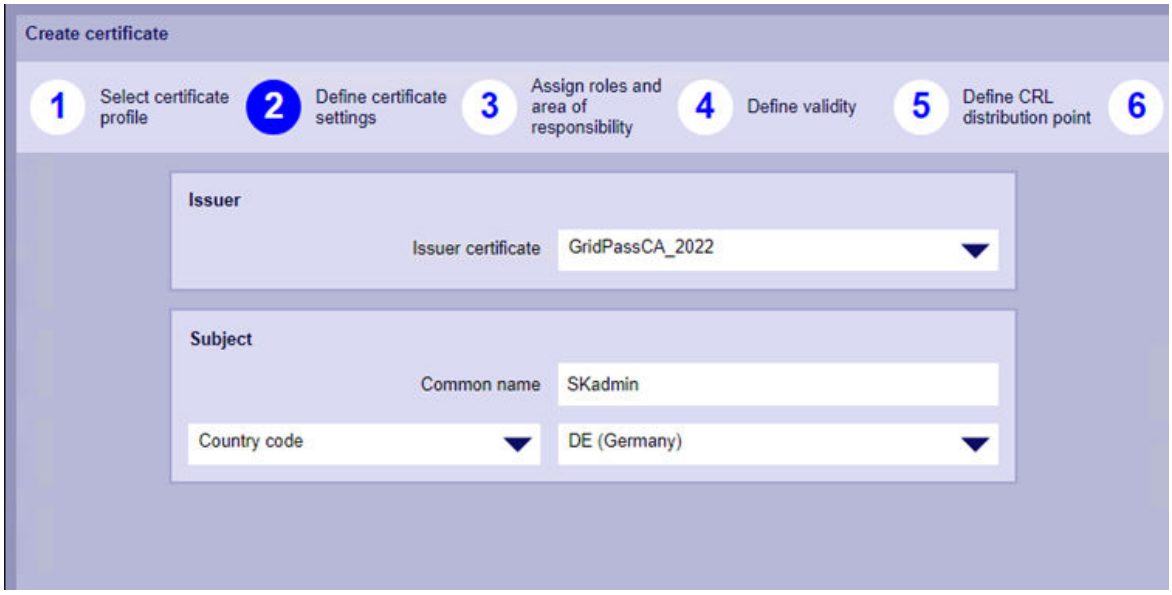
Generating a Client Certificate for the LDAP User SKadmin with the Role Administrator

✧ Open **SICAM GridPass** > **Certificates** > **Add certificate** and select **TLS client**.



[sc_Sicam GridPass_create-TLS-client-certificate, 1, en_US]

✧ Define the certificate settings.
Ensure to enter the user name used in the active directory in the text box **Common name**.

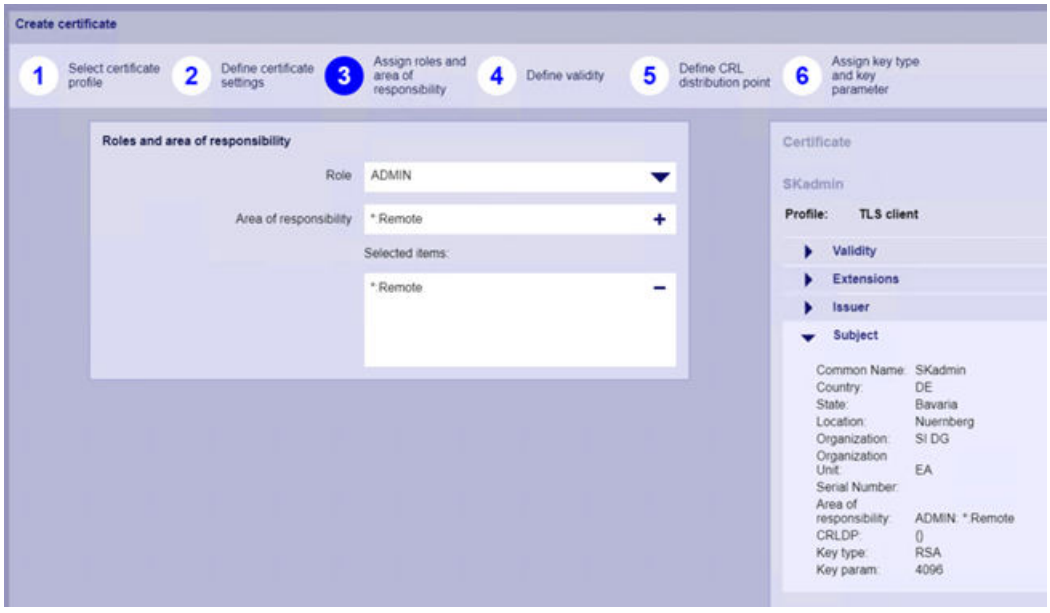


[sc_Sicam GridPass_Client-certificate_settings_AD, 1, en_US]

NOTE

The **Common name** must be identical with the user name in the Active Directory.

✧ Assign roles and the area of responsibility.

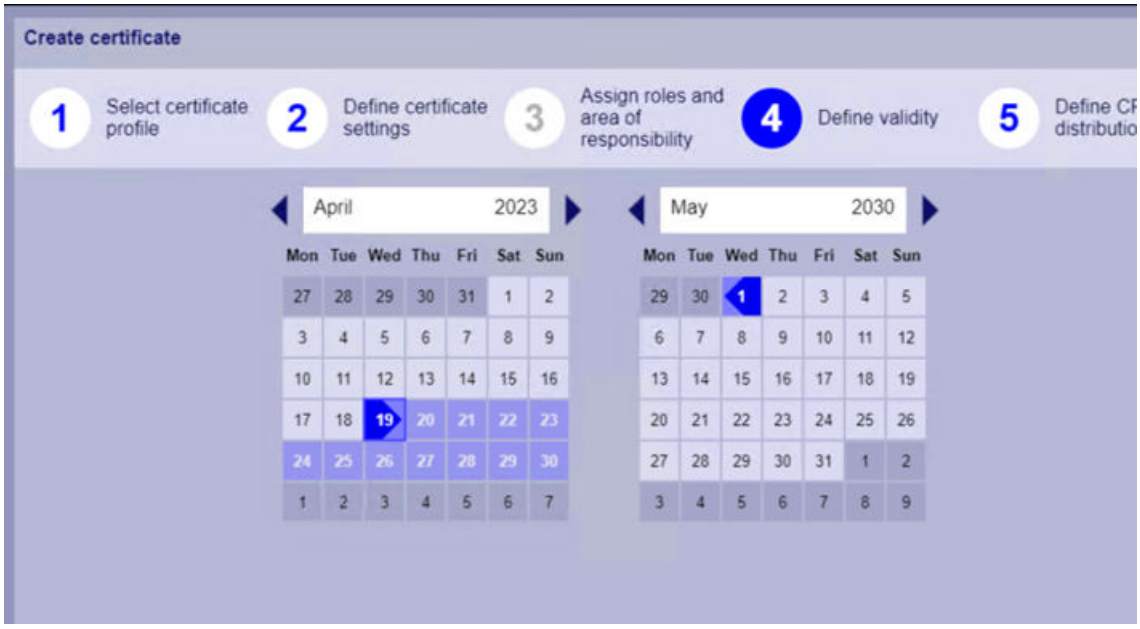


[sc_Sicam GridPass_Client-certificate_AoR, 1, en_US]

NOTE

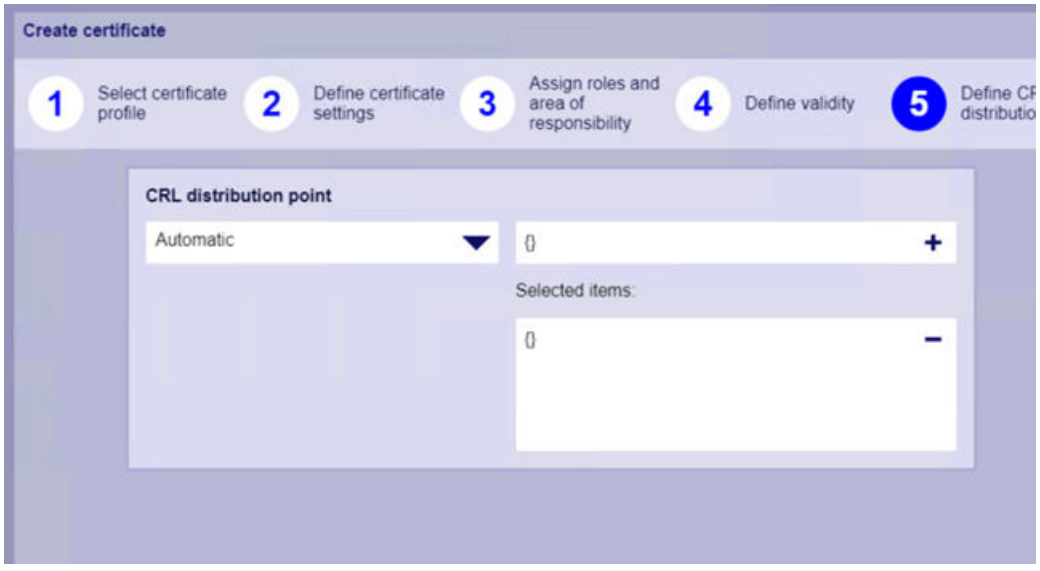
In case the user is a WebUI user, AoR must be “*: Remote”.
In case the user is a HMI user (login at device directly), AoR must be “*: Local”.

✧ Define the validity.



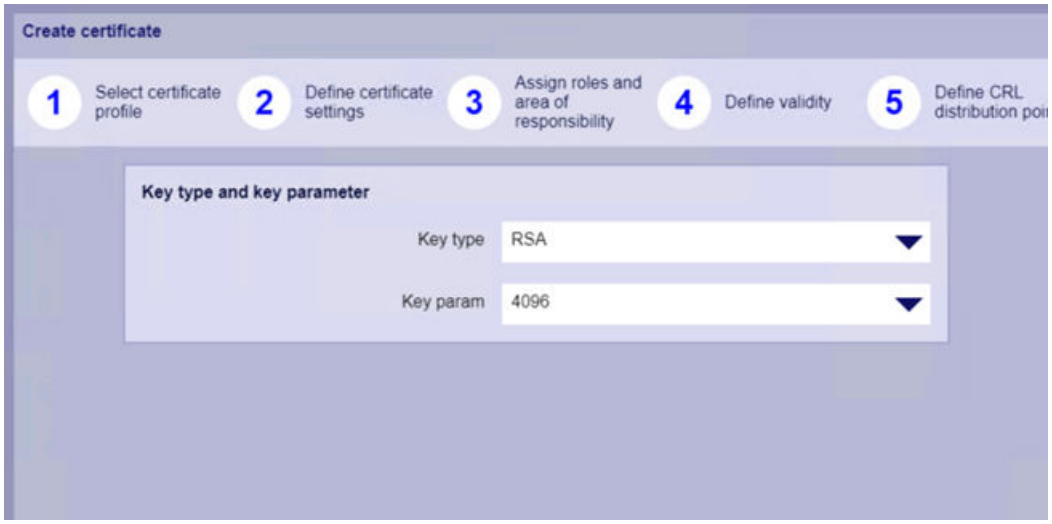
[sc_SicamGridPass_Create-Attribute-Authority_validity, 1, en_US]

✧ Define the CRL and distribution point.



[sc_GenerateClientCertificate_for_LDAP-user_CRL, 1, en_US]

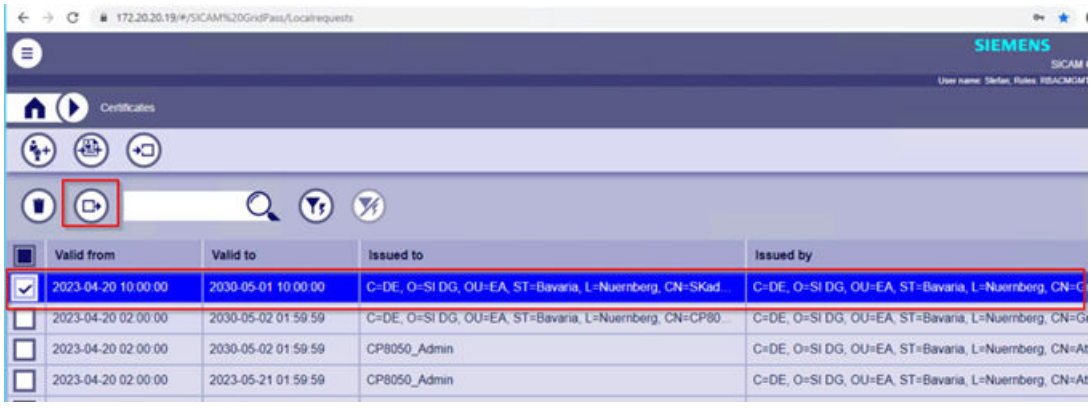
✧ Enter **Key type and key parameter** according to the encryption requirements, for example RSA and 4096.



[sc_GenerateClientCertificate_for_LDAP-user_Key-type, 1, en_US]

Exporting LDAP ID Certificates to the LDAP Server

✧ In **Certificates**, select the certificate you want to export.



[sc_Sicam GridPass_Client-certificate_export-ID, 1, en_US]

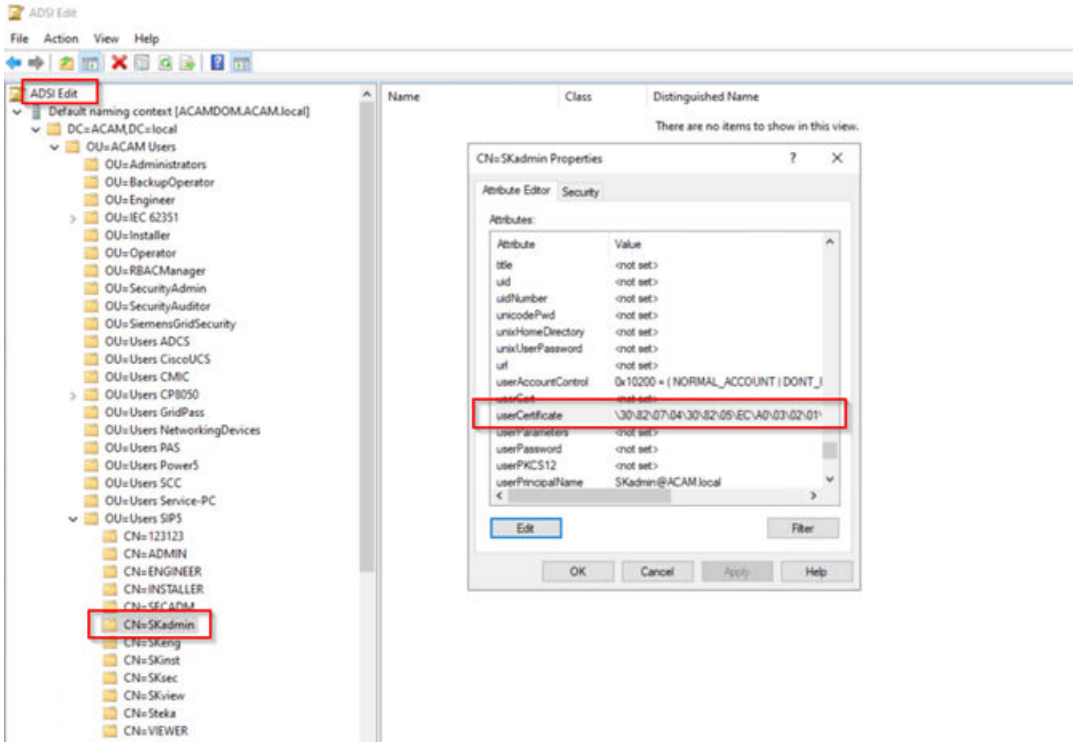
✧ Activate **Directory service (LDAP)** and click OK.

[sc_Export-LDAP-certificate, 1, en_US]

✧ To execute the export, enter the credetials of the AD LDS Administrator user.

[sc_SicamGridPass_create_Attribute-Certificate_export_LDAPuser-logon, 1, en_US]

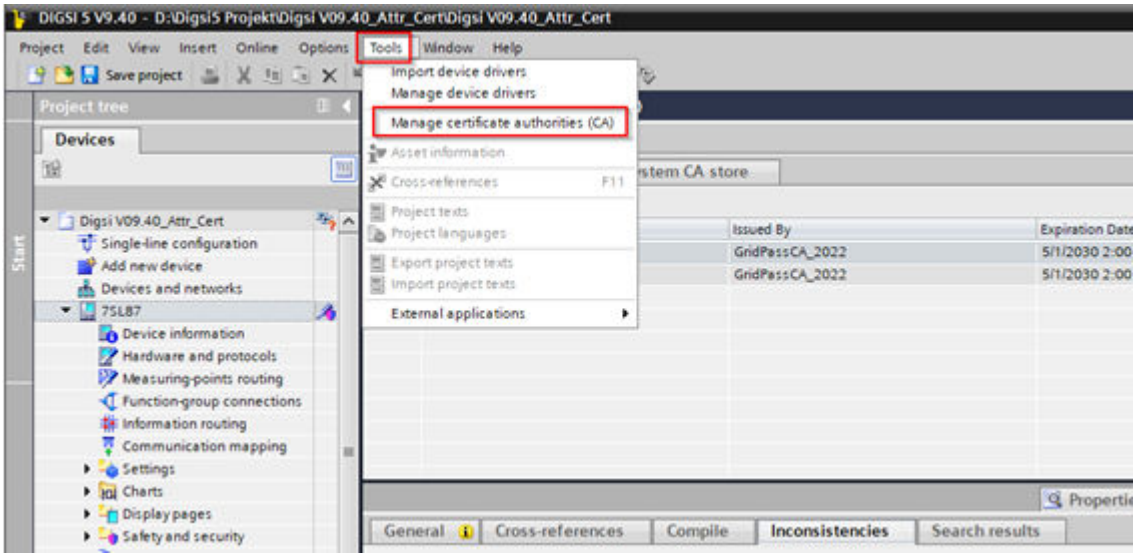
You can find the published certificate in the properties of AD LDS for the user **SKadmin**.



[sc_LDAP-ID-certificate_AD-LDS, 1, en_US]

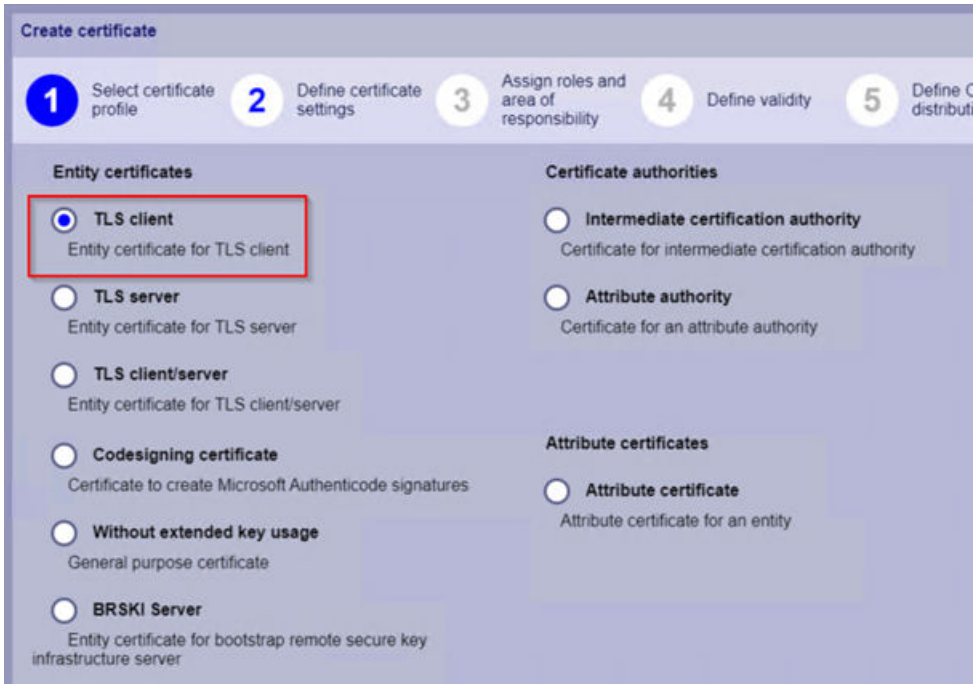
Configuring DIGSI 5 for LDAP Authentication

✧ Import the CA certificate (in this example: GridPassCA_2022) to the DIGSI 5 CA store.



[sc_Digs5_manage-certificate-authorities, 1, en_US]

✧ Open **SICAM GridPass** > **Certificates** > **Add certificate** and select **TLS client** to generate the DIGSI client certificate.

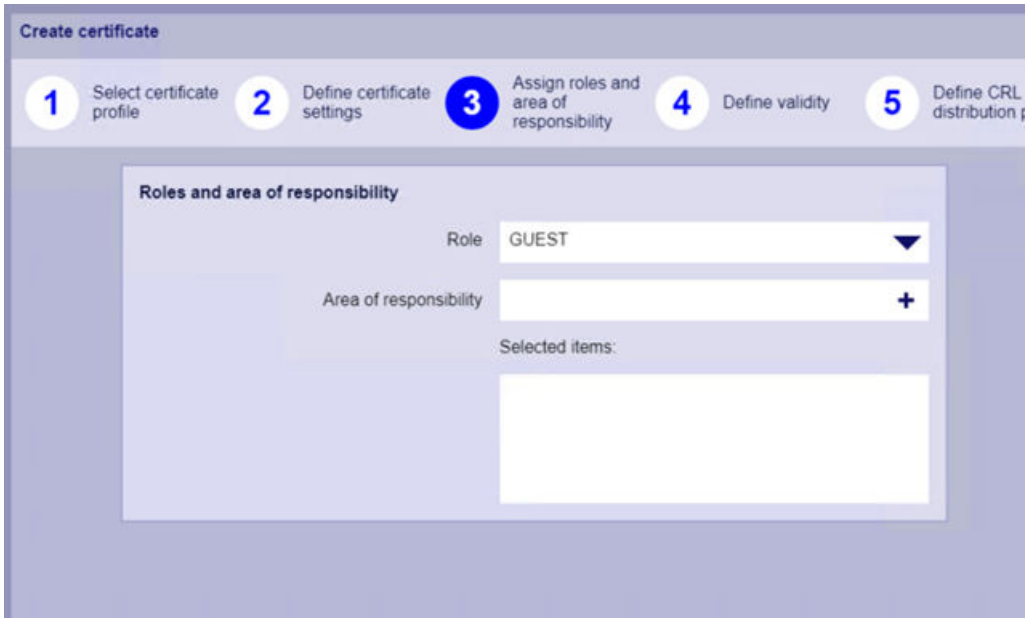


[sc_Sicam GridPass_create-TLS-client-certificate, 1, en_US]

✧ Define the certificate settings.

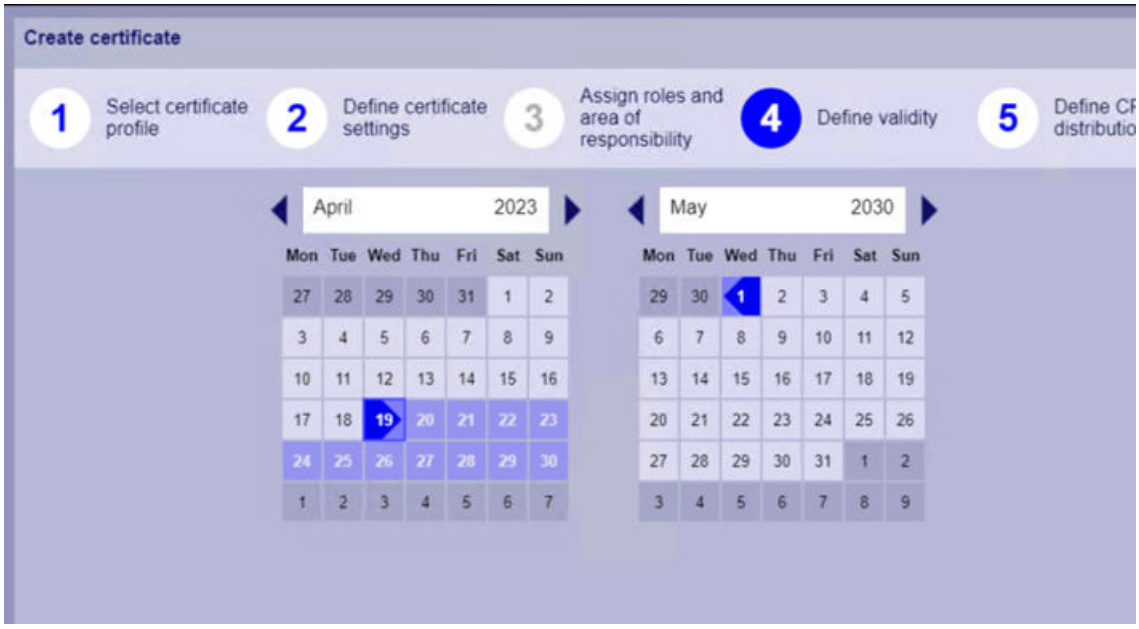
[sc_Sicam GridPass_Client-certificate_settings, 1, en_US]

✧ Assign roles and the area of responsibility.



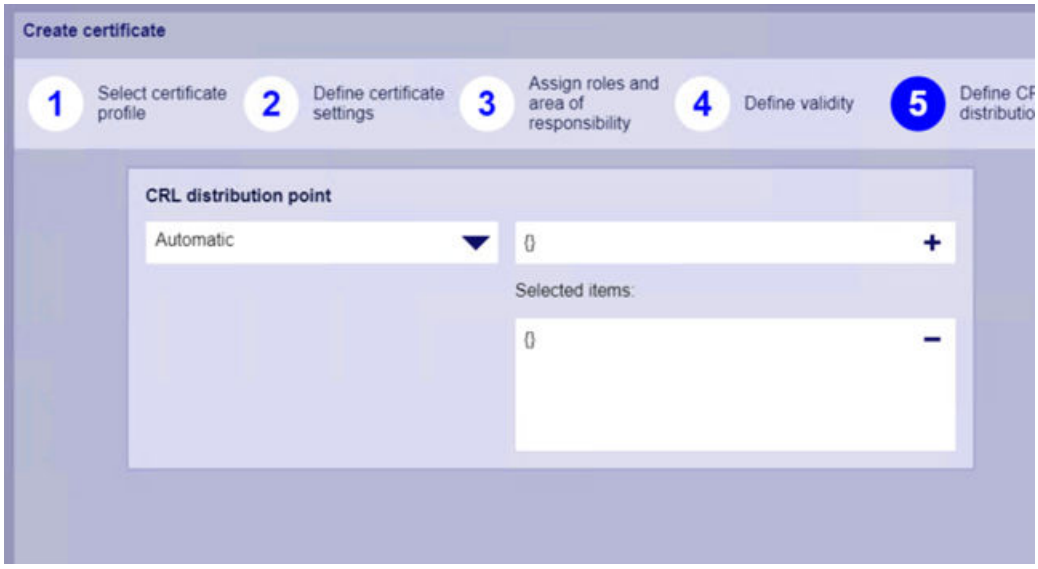
[sc_Sicam GridPass_Create-Digsi-client-certificate_AoR, 1, en_US]

✧ Define the validity.



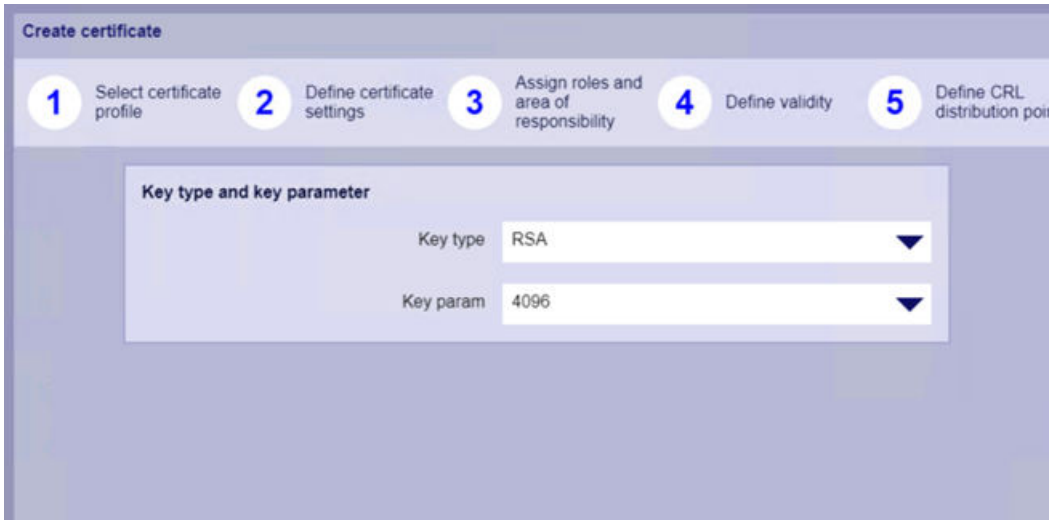
[sc_SicamGridPass_Create-Attribute-Authority_validity, 1, en_US]

✧ Define the CRL and distribution point.



[sc_GenerateClientCertificate_for_LDAP-user_CRL, 1, en_US]

✧ Enter the key type and key parameter.

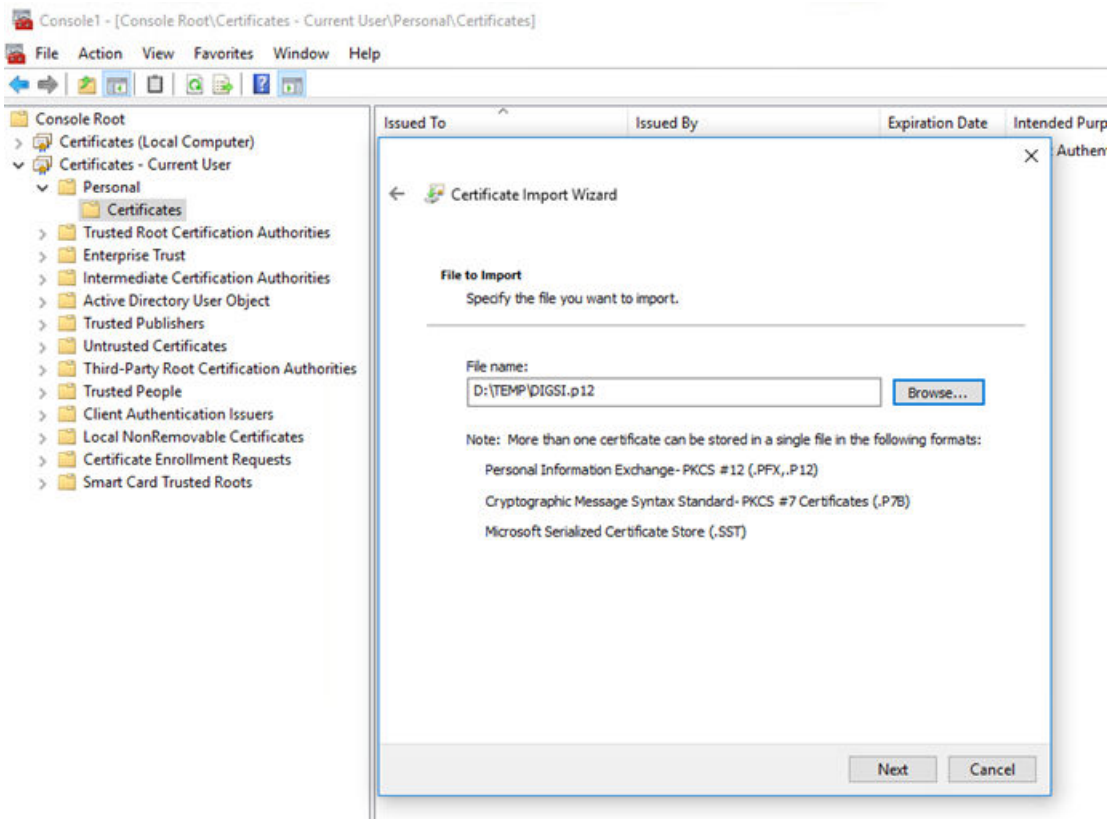


[sc_GenerateClientCertificate_for_LDAP-user_Key-type, 1, en_US]

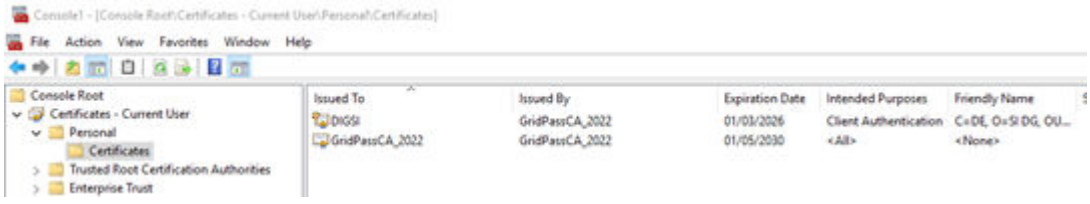
✧ Export this certificate as a P12 file.

[sc_Sicam GridPass_export-DIGSI-client-certificate-12files, 1, en_US]

✧ Import this certificate to a DIGSI 5 system under **Certificates** – **Current User** > **Personal** > **Certificates**.



[sc_import_client-certificate_Digsi5-machine, 1, en_US]

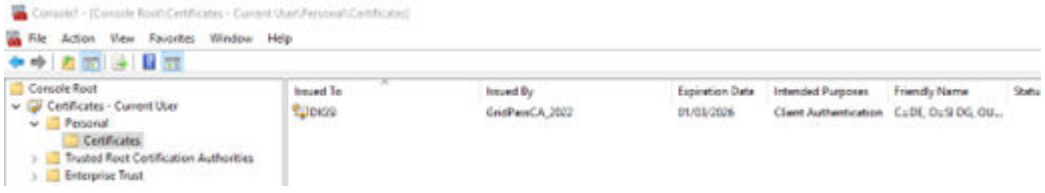


[sc_client-certificate_Digsi5-machine_incl_CA-certificate, 1, en_US]

NOTE

You must import the client certificate to each user certificate store, or you import the certificate to the certificate store of the local computer.

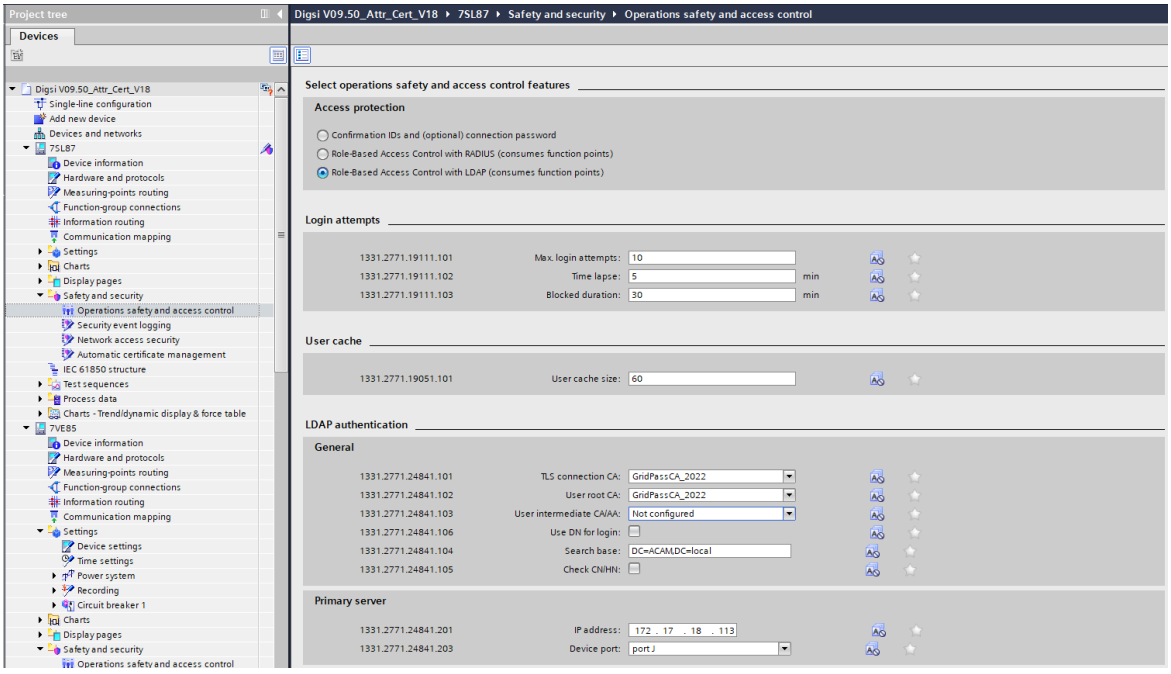
✧ You can remove the root CA certificate (in the example: GridPassCA_2022).



[sc_client-certificate_Digsi5-machine, 1, en_US]

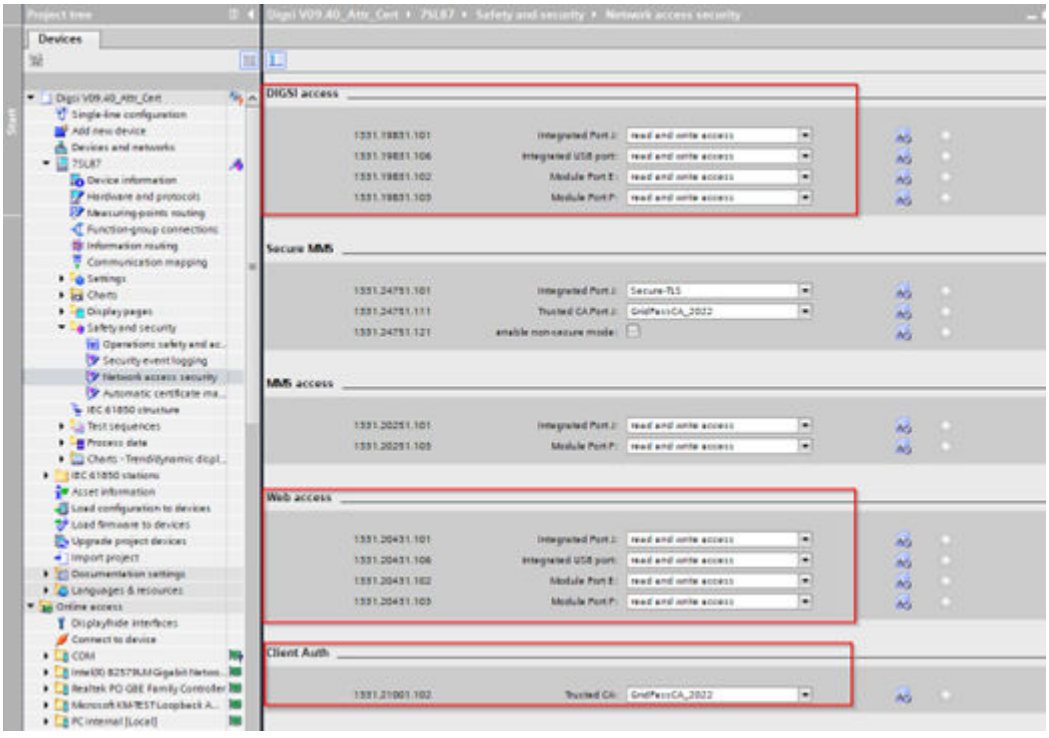
The following settings must be done in DIGSI 5 for the LDAP configuration:

✧ Open **DIGSI 5 project** > **Device** (for example 7SL87) > **Safety and security** > **Operations safety and access**



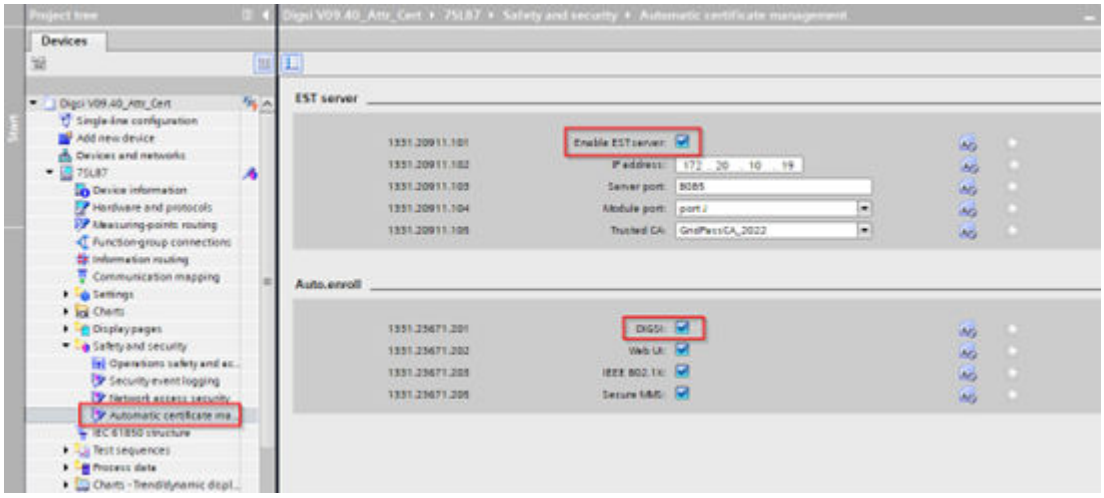
[sc_Digsi5_safety_security-settings, 1, en_US]

✧ Enter all settings for the **Network access security**.



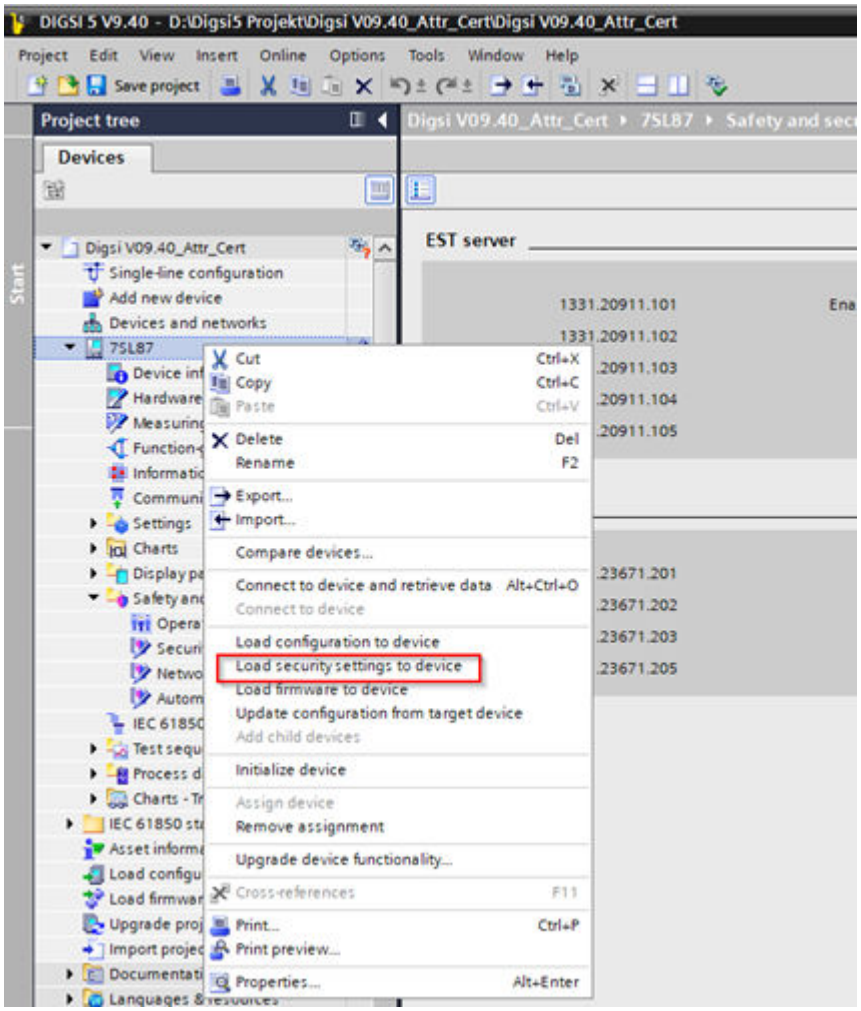
[sc_Digsi5_Network-access-security, 1, en_US]

✧ In case you want to use the auto enrollment with EST, configure **DIGSI 5 project** > **Device** (for example 7SL87) > **Safety and security** > **Automatic certificate management**.



[sc_DigsiS_automatic-certificate-management, 1, en_US]

✧ Right-click the device in the project tree and select **Load security settings to device**.



[sc_DigsiS_load-security-settings, 1, en_US]

2.7 Creating LDAP Attribute Certificates for SIPROTEC 5 and DIGSI 5

Use Case

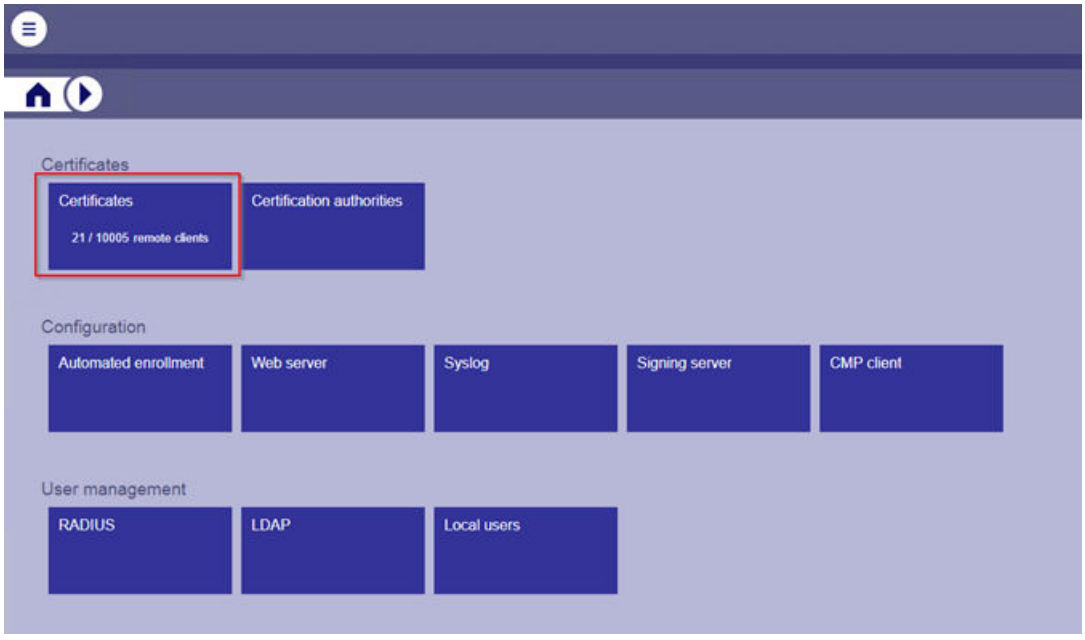
Attribute certificates are used to give users additional roles for a limited period. For example, a user SECADM with the role **Security Administrator** should substitute for a user with the role **OPERATOR**. You create an attribute certificate with the role **OPERATOR** with the validity time of the substitution and add it to the user SECADM. After the validity time, the user SECADM looses the OPERATOR role automatically.

NOTE

In case you want to add one or more roles to a user (as described above), you must create an attribute certificate for each role (for example, **Security Administrator** and **Operator**). It is not possible to mix roles of IDs and attribute certificates.

Generating Attribute Certificates

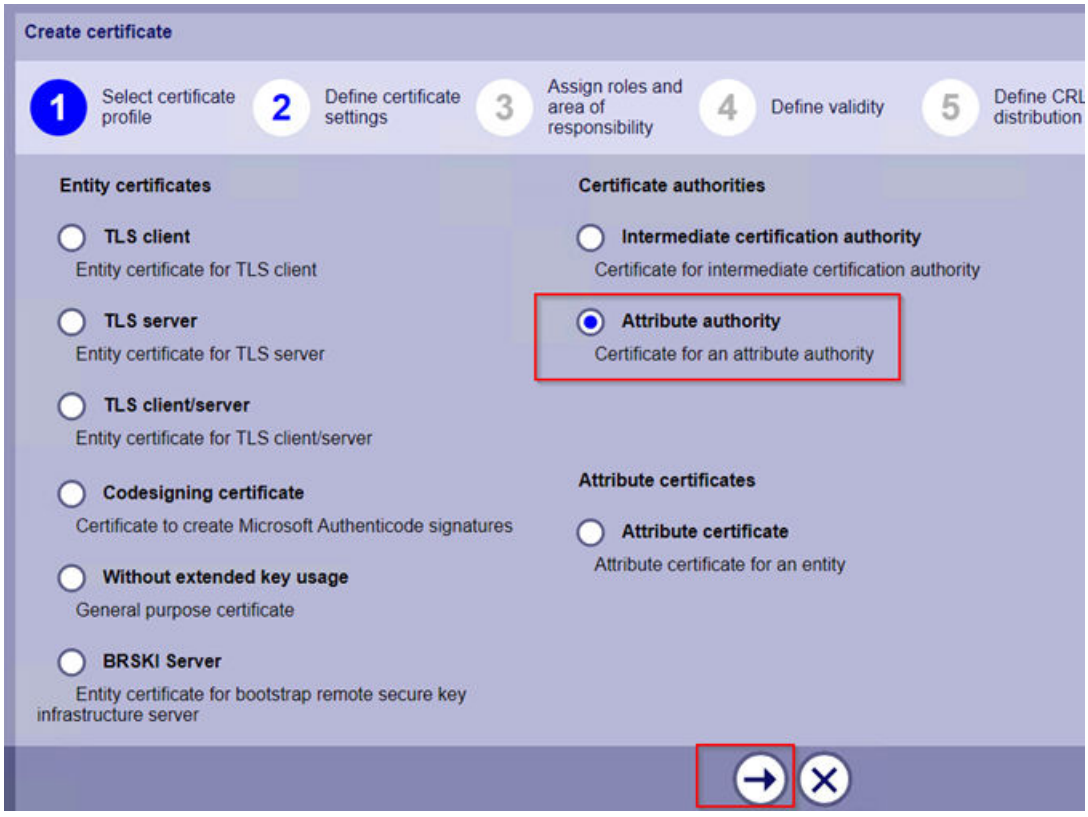
✧ Create an attribute authority (required for generating attribute certificates).



[sc_Sicam GridPass_create-attribute-authority_01, 1, en_US]

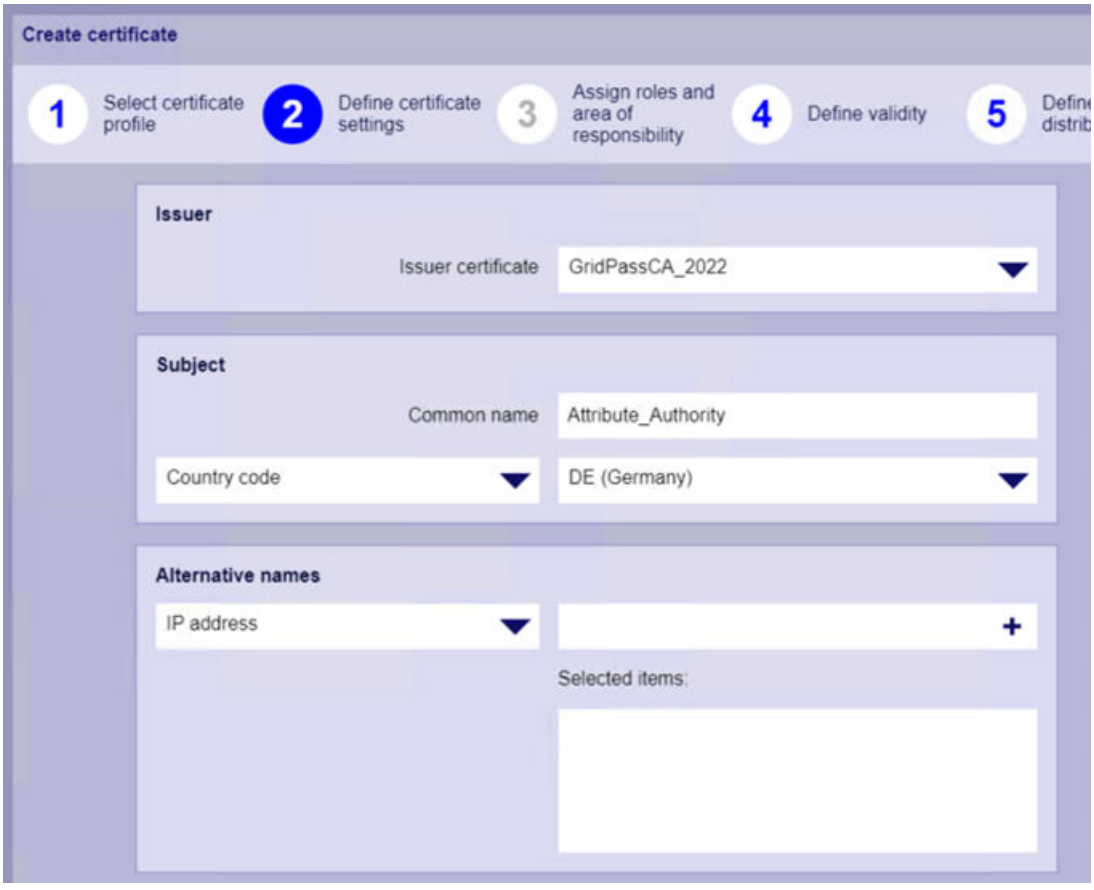
[sc_Sicam GridPass_create-attribute-authority_02, 1, en_US]

✧ Select **Attribute authority** in **Select certificate profile**.



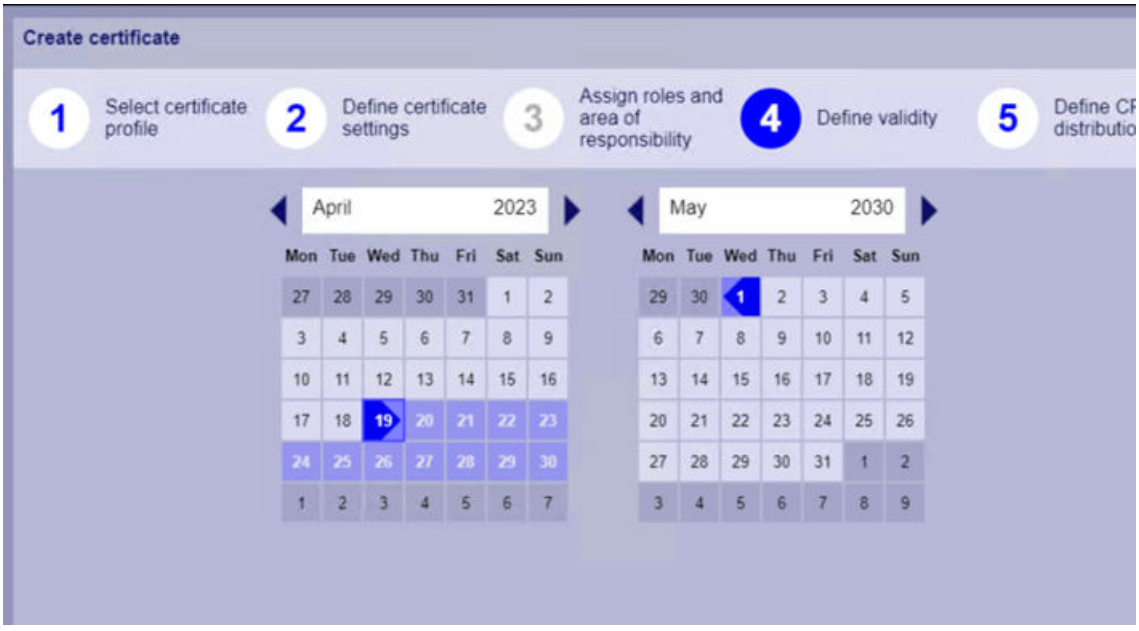
[sc_Sicam GridPass_create-attribute-authority_certificate-profil, 1, en_US]

✧ Define the certificate settings.



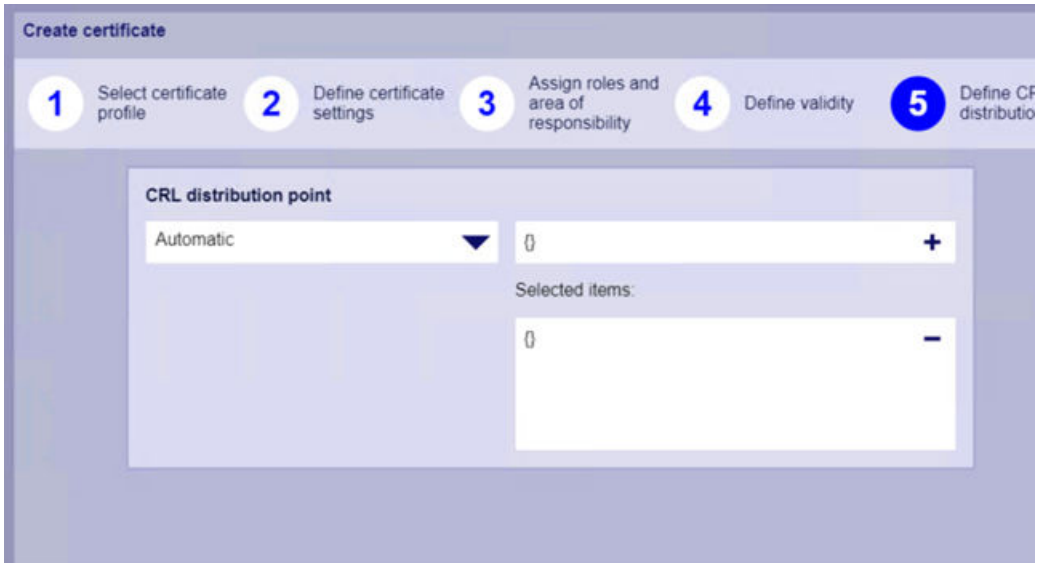
[sc_Sicam GridPass_create-attribute-authority_setting, 1, en_US]

✧ Define the validity.



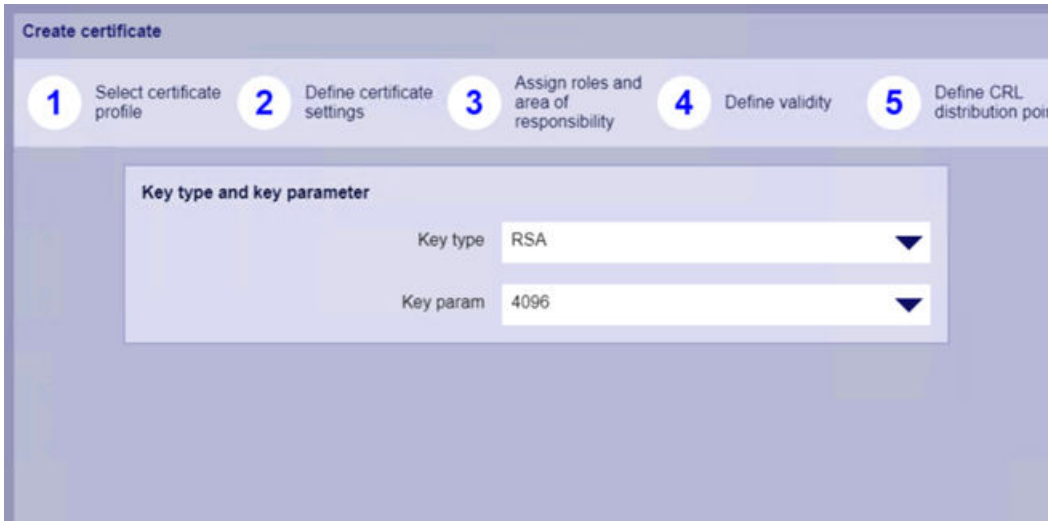
[sc_SicamGridPass_Create-Attribute-Authority_validity, 1, en_US]

✧ Define the CRL and distribution point.



[sc_GenerateClientCertificate_for_LDAP-user_CRL, 1, en_US]

✧ Enter the key type and key parameter.



[sc_GenerateClientCertificate_for_LDAP-user_Key-type, 1, en_US]

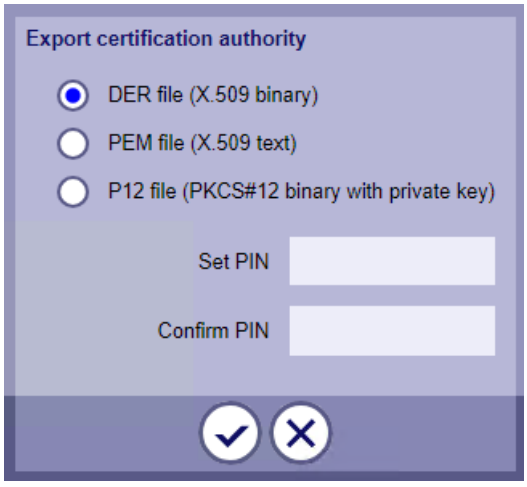
The attribute authority is created.

[sc_Sicam GridPass_attribute-authority, 1, en_US]

Exporting the Attribute Authority and Installing in DIGSI 5

✧ Export the attribute authority from SICAM GridPass as a *.DER file.

[sc_Sicam GridPass_export_attribute-authority, 1, en_US]

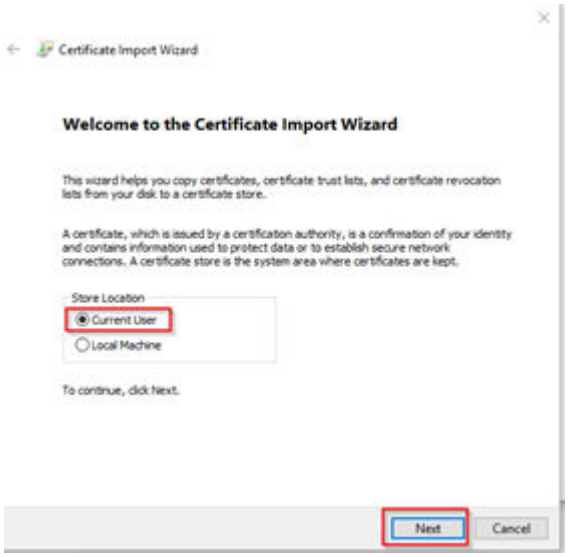


[sc_Sicam GridPass_export_attribute-authority_DER-file, 1, en_US]

✧ Copy the exported *.DER file to the DIGSI 5 system, double-click and install the AA certificate.

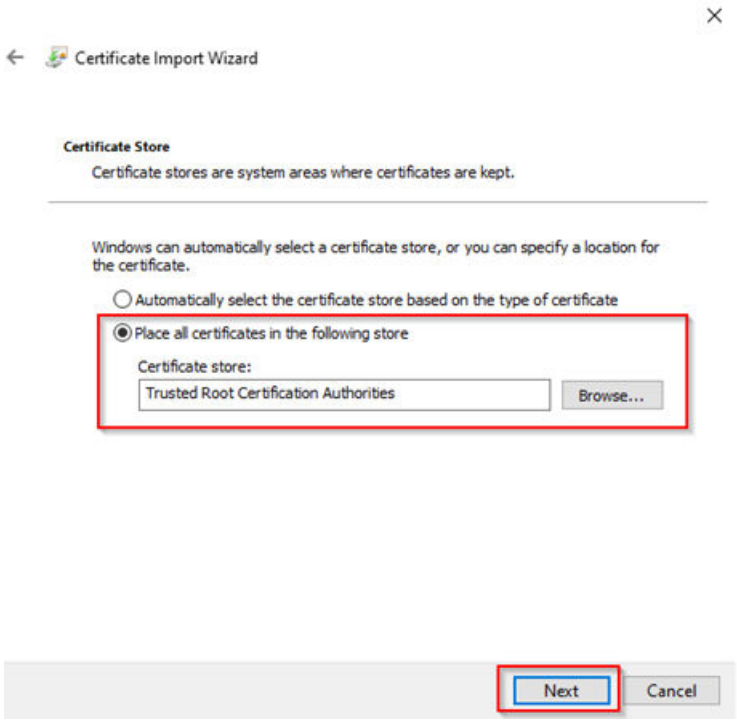
Importing the Certificate

✧ In the installation wizard, select **Current user**.



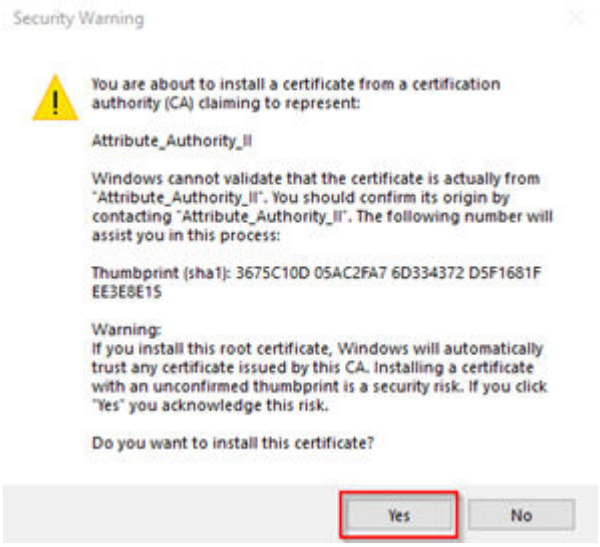
[sc_install-certificate_for_current-user, 1, en_US]

✧ Activate **Place all certificates in the following store** and select **Trusted Root Certification Authorities**.



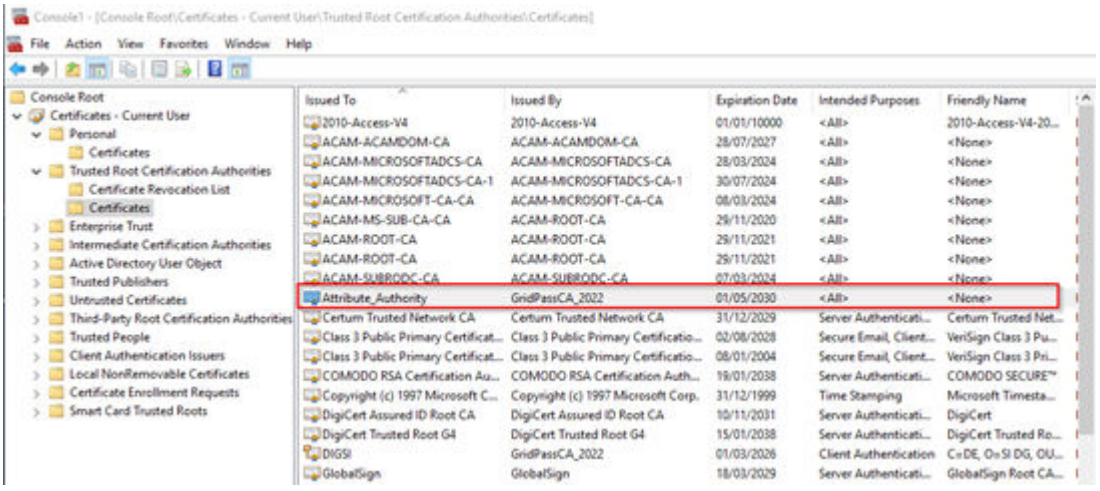
[sc_install-certificate_trusted-root-certification-authorities-stores, 1, en_US]

✧ Confirm with **Yes**.



[sc_install-certificate, 1, en_US]

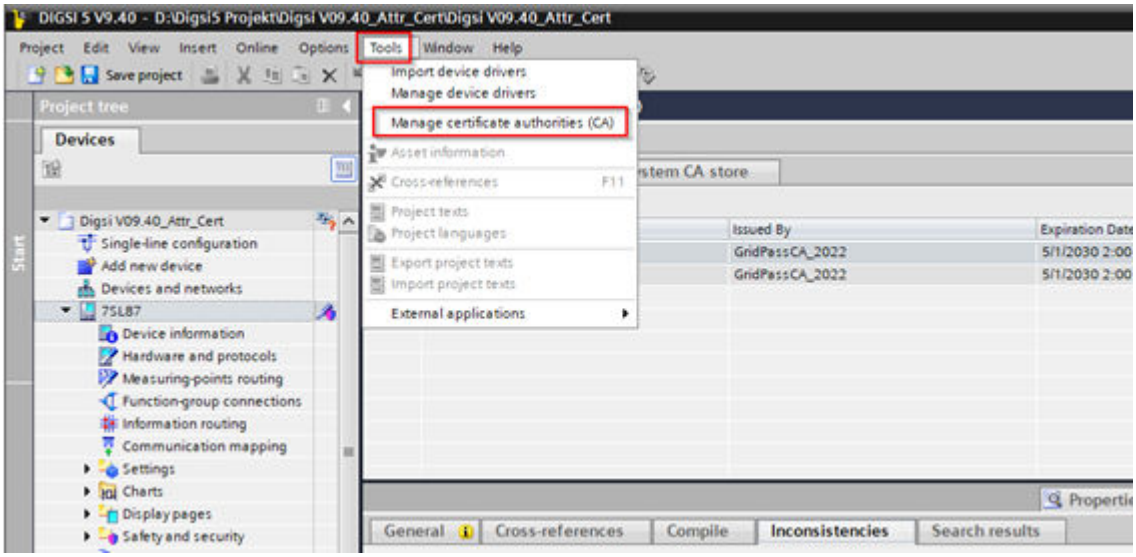
The attribute authority is available on the DIGSI 5 system.



[sc_attribute-authority_on_DIGSI5-machine, 1, en_US]

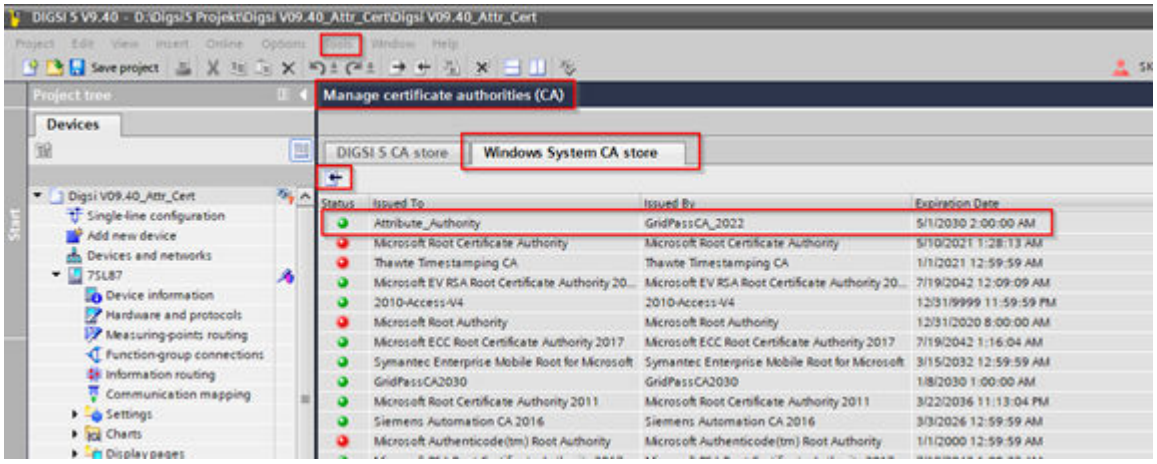
Configuring Attribute Authority in DIGSI 5

✧ Open **DIGSI 5** > **Tools** > **Manage certificate authorities (CA)** > **Windows System CA store**.

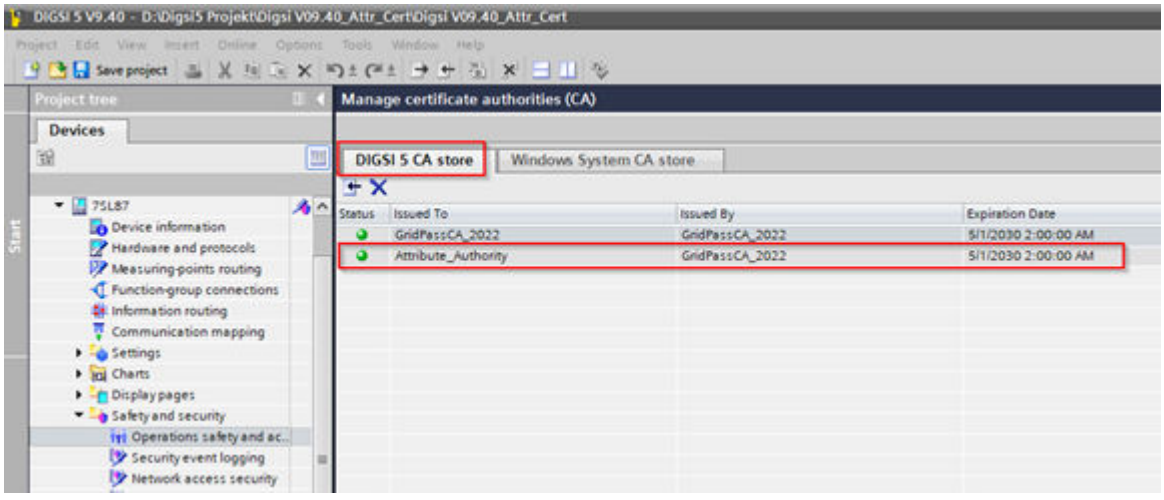


[sc_Digs5_manage-certificate-authorities, 1, en_US]

✧ Select the imported attribute authority and import it to the DIGSI 5 CA store.



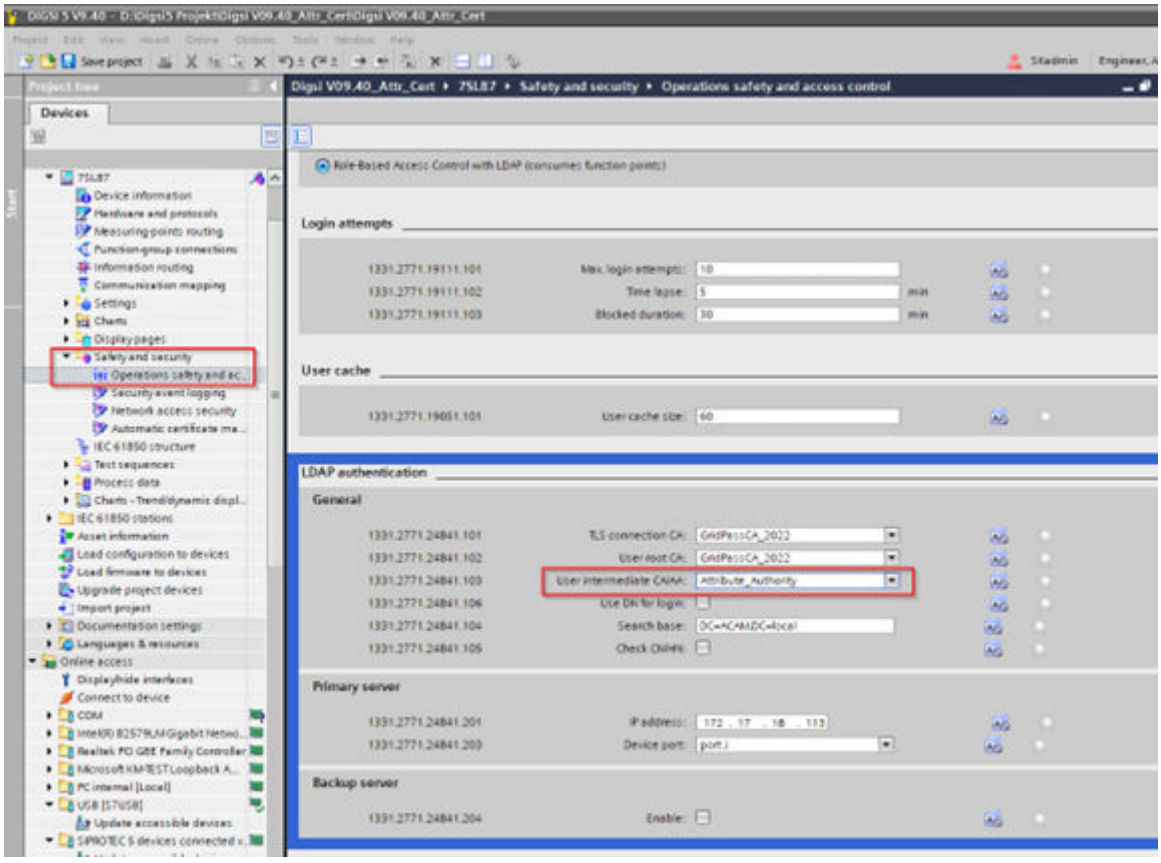
[sc_export-attribute-authority_DIGSI5-CA-store, 1, en_US]



[sc_attribute-authority_DIGSI5-CA-store, 1, en_US]

✧ Open **Safety and security** > **Operation safety and access control** > **LDAP authentication**.

✧ Select the imported AA in **User intermediate CA/AA**.



[sc_DIGSI5_operation-safety_access-control, 1, en_US]

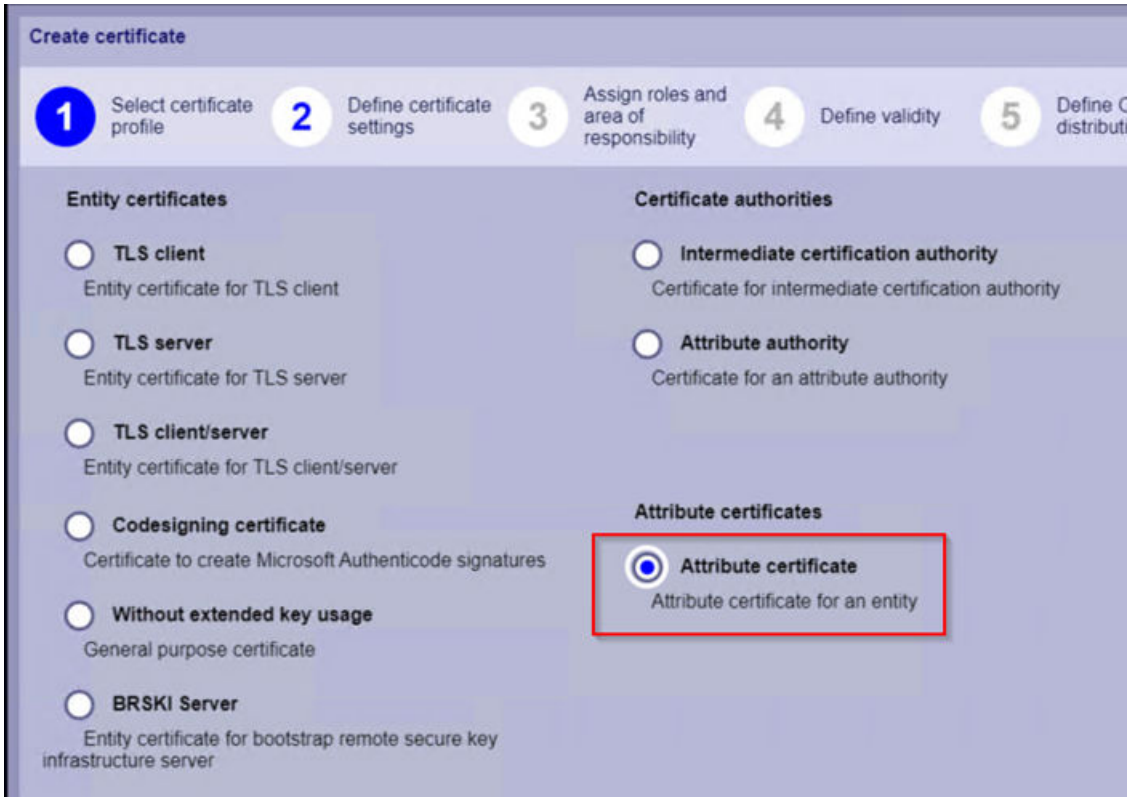
Generating Attribute Certificates in SICAM GridPass

NOTE

Generate 2 attribute certificates in SICAM GridPass:

- **Security Administrator** (default)
- **OPERATOR** (substitute)

✧ Select **Attribute certificate** under **Select certificate profile** and create a new attribute certificate.



[sc_Sicam GridPass_create-new-attribute-authority_certificate, 1, en_US]

✧ Under **Define certificate settings**, select the already created attribute authority and enter the entity name of the user SECADM.

[sc_Sicam GridPass_select_username_for_entity-name, 1, en_US]

✧ Under **Assign roles and area of responsibility**, select the role SECADM and fill in the **Area of responsibility**.

[sc_Sicam GridPass_create_attribute-authority_select-role_AoR, 1, en_US]

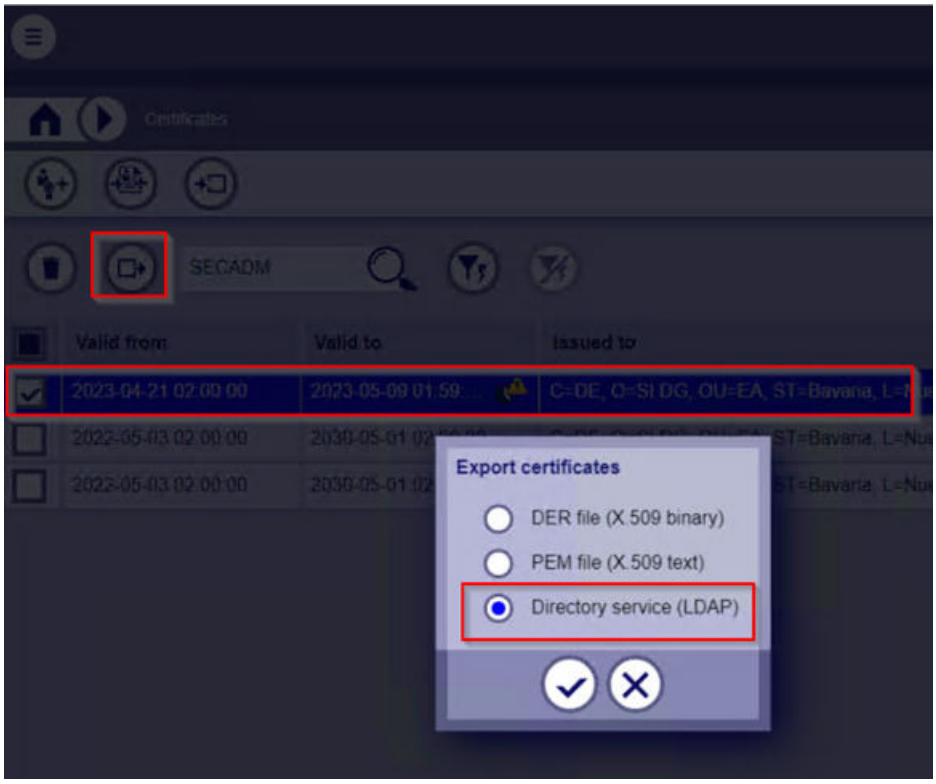
NOTE

Use ***:Local** for login at the device (local users).
Use ***:Remote** if you are a Web UI user.

✧ Define the validity.

[sc_Sicam GridPass_create-attribute-certificate_validity, 1, en_US]

✧ Export the attribute certificate as LDAP.

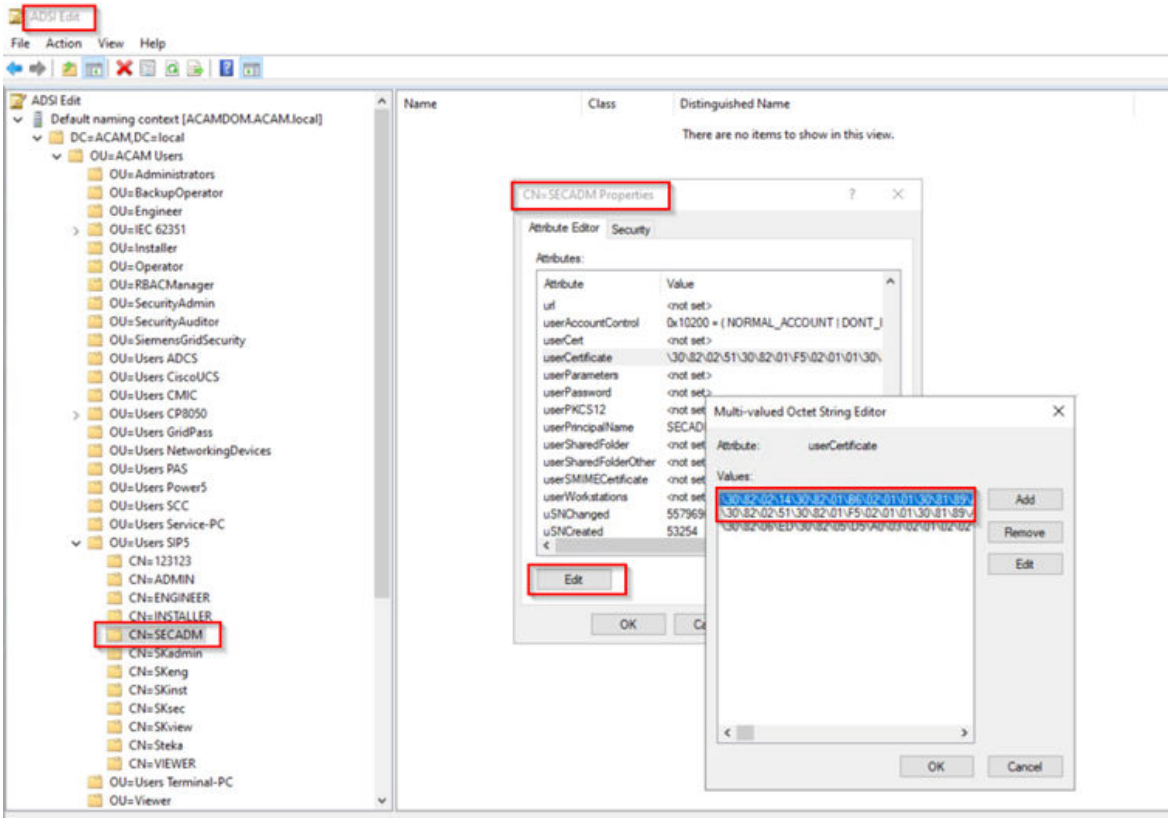


[sc_Sicam GridPass_export-AC-as-LDAP, 1, en_US]

✧ Log on to LDAP with the LDAP/domain admin user.

[sc_SicamGridPass_create_ Attribute-Certificate_export_LDAPuser-logon, 1, en_US]

You can find the attribute certificate in the tool AD LDS (ADSI Edit).



[sc_attribute-certificate_AD-LDS, 1, en_US]

Repeat the procedure also for the substitute role, for example **OPERATOR**.

3 Logon of an LDAP User

3.1 Example for Logon Procedure

The following example shows how LDAP works with attribute certificates.

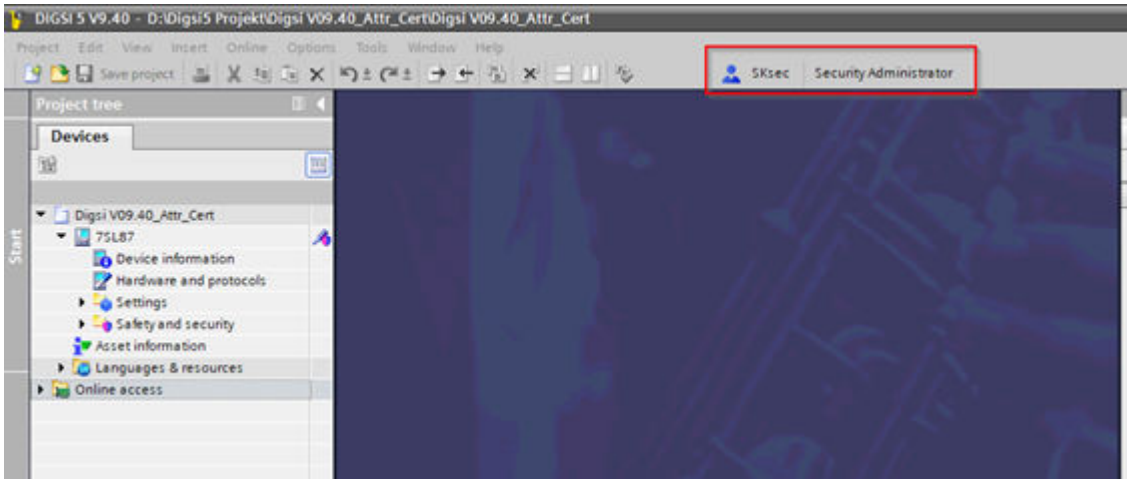
Preconditions

The user **SKsec** (remote user) has the roles **Security Administrator** and **OPERATOR** assigned with attribute certificates.

✧ Log on to the DIGSI 5 system with the user **SKsec**.

✧ Start DIGSI 5.

In DIGSI 5, you can see the role **Security Administrator** as a blue user icon.

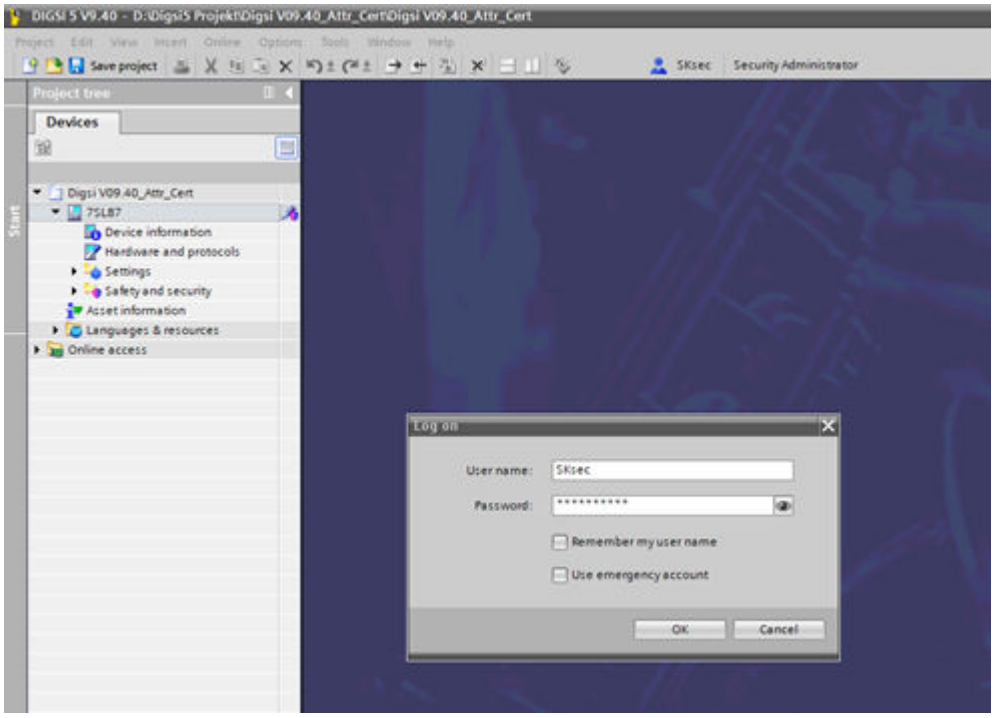


[sc_DIGSI5_user-role-given_AC-certificate, 1, en_US]

✧ Load the security settings to the device by selecting the device with a right mouse click.
It is not necessary to change any security values before.

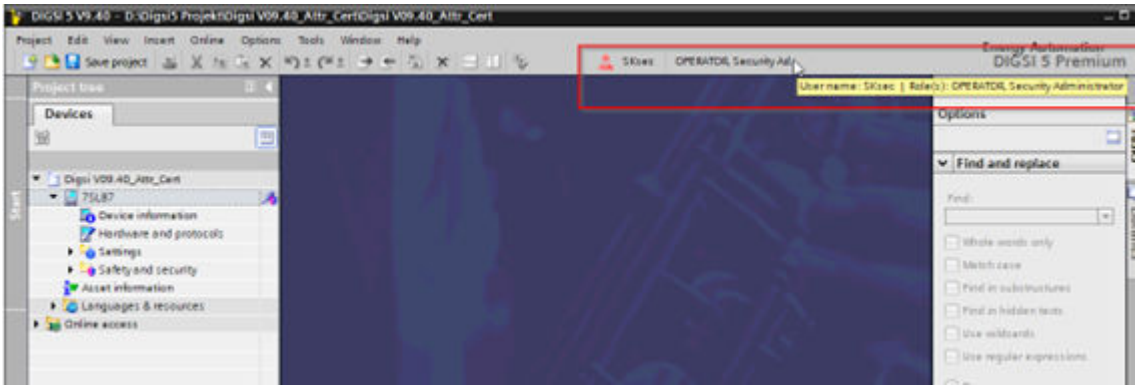
The logon dialog for the SIPROTEC 5 device to the LDAP server is displayed.

✧ Enter the credentials of your user account, for example **SKsec**.



[sc_DIGSI5_authentication_through_LDAP-server, 1, en_US]

✧ If the logon is successful, you can see a red user icon with all roles assigned via the attribute certificates.



[sc_DIGSI5_user-roles-of-attribute-certificates, 1, en_US]