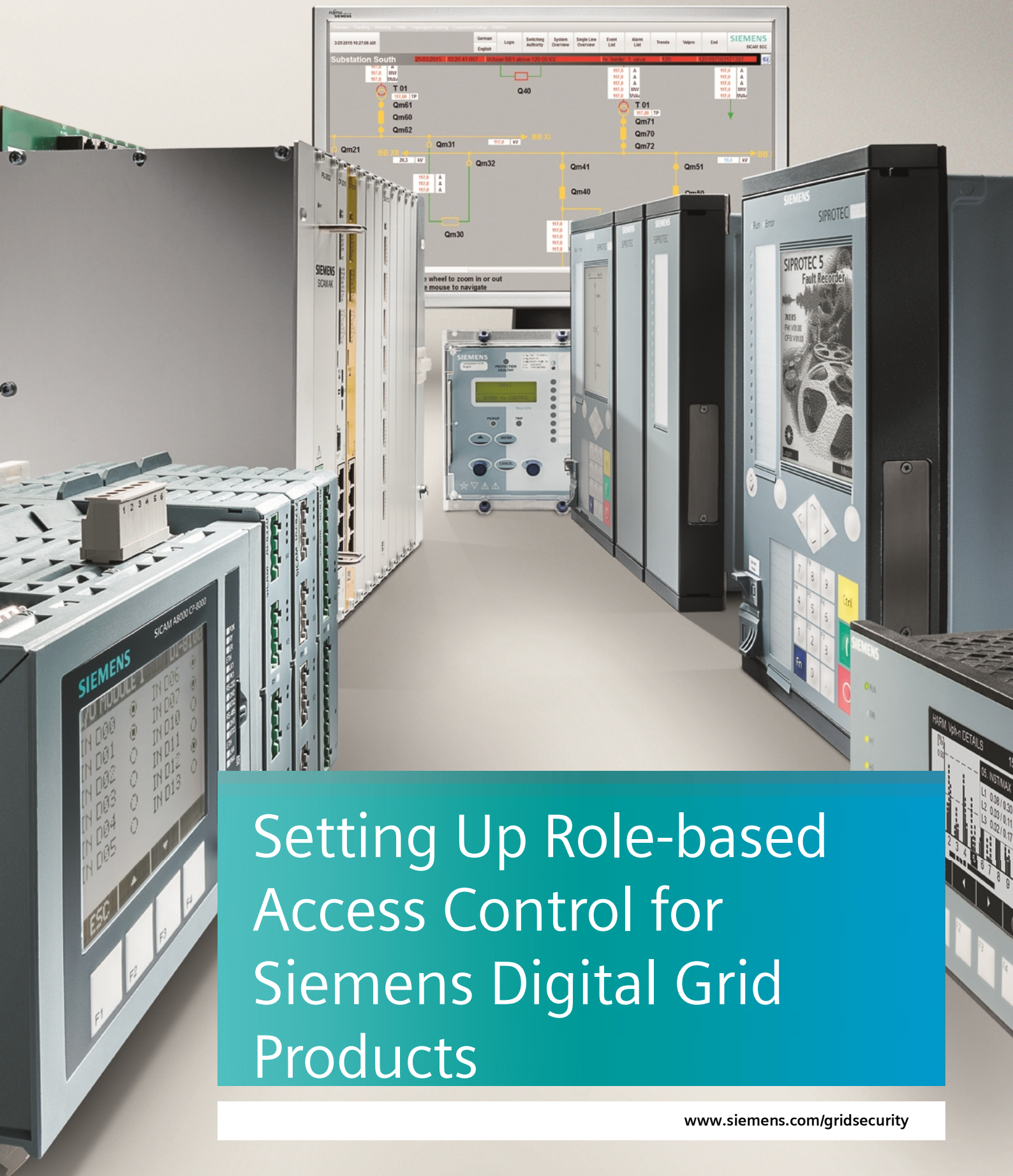


SIEMENS

Ingenuity for life



Setting Up Role-based Access Control for Siemens Digital Grid Products

www.siemens.com/gridsecurity

Cyber Security Application

Setting Up Role-Based Access Control for Siemens Digital Grid Products

APN-051, Edition 1

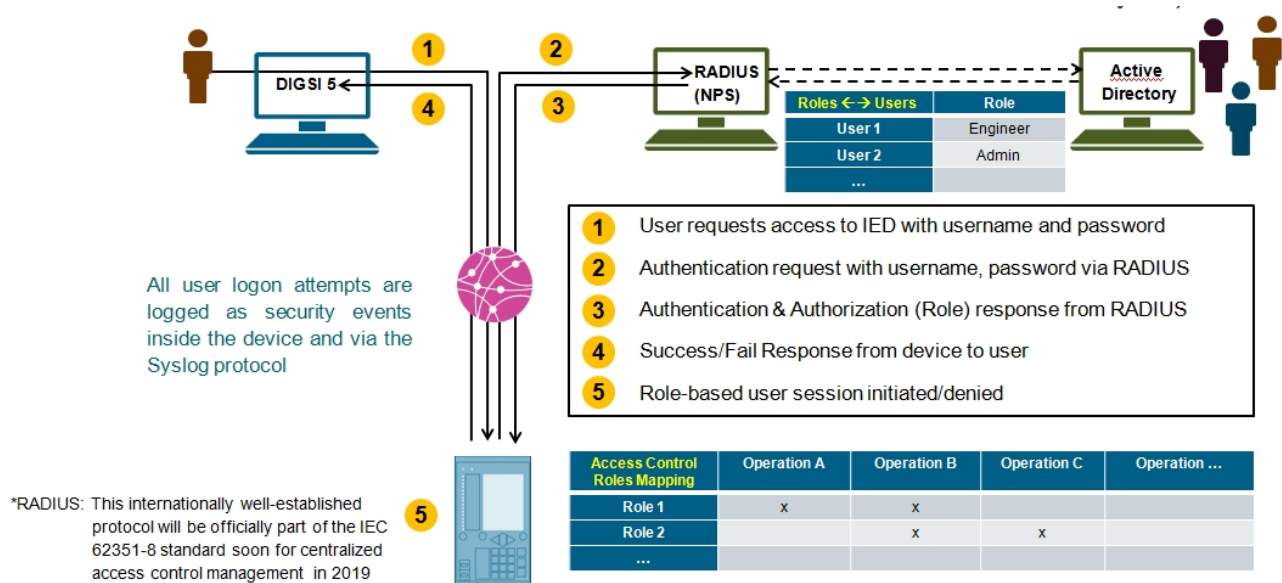
Content

| | | |
|-----|--|----|
| 1 | Setting Up Role-Based Access Control for Siemens Digital Grid Products | 3 |
| 1.1 | Introduction..... | 3 |
| 1.2 | Fundamentals..... | 3 |
| 1.3 | Implementation according IEC 62351-8 Ed.2 Standard..... | 4 |
| 1.4 | Brief Overview | 4 |
| 1.5 | Detailed description | 5 |
| 1.6 | IEC 62351 Appendix..... | 32 |
| 1.7 | Siemens Appendix..... | 34 |
| 1.8 | Summary | 36 |

1 Setting Up Role-Based Access Control for Siemens Digital Grid Products

1.1 Introduction

SIPROTEC 5 and SICAM A8000 devices support role-based access control with central user management in RADIUS/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. All SIPROTEC 5 and SICAM A8000 devices can be connected to a central RADIUS server containing the authentication and authorization configuration. RADIUS is a standardized client/server protocol and the client implementation is integrated in the SIPROTEC 5 and SICAM A8000 device firmware.



This document describes the usage of SIPROTEC 5, SICAM A8000 devices and SICAM GridPass (certificate management product) with RADIUS server option of activated in an Active Directory Network Policy Server (NPS) installation on a Windows 2016 or Windows 2012R2 system. An Active Directory Server (ADS) needs to be installed and the NPS feature has to be activated to use the RADIUS server option within the ADS environment. Furthermore, for the local user login on a SIPROTEC 5 device over the RADIUS protocol, the ADS policy has to be adjusted. This specific configuration is also part of this documentation.

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](#).^{[1][2]} Initially, Active Directory was only in charge of centralized domain management. Starting with [Windows Server 2008](#), however, Active Directory became an umbrella title for a broad range of directory-based identity-related services

Active Directory Server (ADS)

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, e.g. when a user [logs into](#) 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

management and storage of information, provides authentication and authorization mechanisms, and establishes a framework to deploy other related services: Certificate Services

Network Policy Server (NPS)

Network Policy Server (NPS) is the Microsoft implementation of a Remote Authentication Dial-in User Service (RADIUS) server and proxy. It is the successor of Internet Authentication Service (IAS). As a RADIUS server, NPS performs authentication, authorization, and accounting for wireless, authenticating switch, and remote access dial-up and virtual private network (VPN) connections.

Remote Authentication Dial In User Service RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a networking protocol, operating on port 1812 that provides centralized Authentication, Authorization, and Accounting (AAA or Triple A) management for users who connect and use a network service. This internationally well-established protocol will be officially part of the IEC 62351-8 standard soon (2019) for centralized access control management.

RADIUS Server

The main tasks of the RADIUS server are the authentication and control of user access rights. During authentication, the service determines who the connecting user is. Unique user names and passwords are used to check whether the user is actually who they claim. If the user is clearly identified, the authorization handles assignment of the access rights. The user receives specific access rights to data or services of the SIPROTEC 5 device.



RADIUS Client

All SIPROTEC 5 and SICAM A8000 devices (RADIUS Client) can be connected to up to two RADIUS authentication servers containing the authentication configuration. RADIUS is a client/server protocol and the client implementation is integrated in the Siemens device firmware. During a user logon, the Siemens device sends the user name and password to a RADIUS authentication server. This server checks the user data and, in case of successful authentication, sends the assigned roles of the specific user back to the Siemens device. Siemens devices have an advanced role-based access control with predefined roles.

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 IEC 62351-8 Ed.2 Standard

Siemens has implemented the RADIUS protocol according the upcoming IEC 62351-8 Ed.2 standard. During the release of the products and this document, the Edition 2 of the IEC 62351-8 has not yet released which includes the RADIUS implementation of Role-Base Access Control (RBAC). This means that all hints and implementations mentioning IEC 62351 in conjunction with RADIUS are subject to approval by the responsible IEC TC 57/WG 15 for the IEC 62351-8 standard. But all definitions of attributes used here in this application note are in conjunction with the current released IEC62351-8 Ed.1. To get more information see <http://www.iec.ch/smartgrid/standards/> for Smart Grid Security.

1.4 Brief Overview

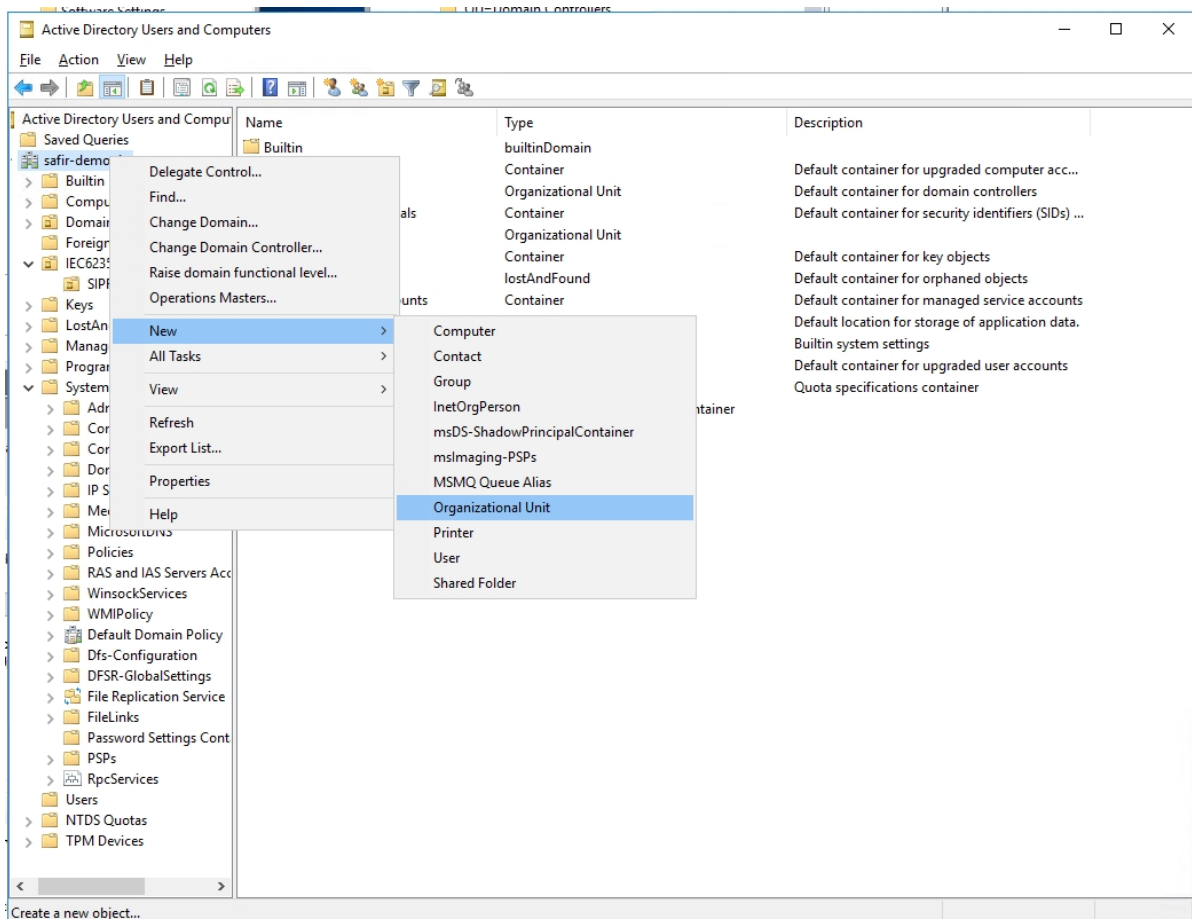
The procedure describes an example using the Network Policy Server (NPS). A RADIUS server like a FreeRADIUS for using this RADIUS protocol with the Siemens Digital Grid devices together with the information in this document can also be used.

1. Create a new Organizational Unit (OU) called *IEC 62351*.
2. Add the IEC 62351 standardized roles and Siemens-specific roles as Windows global security groups to this Organizational Unit.
3. For the *SIPROTEC local HMI* user
 - a. Add under the OU *IEC 62351* the new OU *SIPROTEC HMI User*.
 - b. Because the HMI users can have only simple numeric passcodes for entering locally you need to change password policies only for these HMI-users to create users with simple passwords.
 - c. Create a HMI user group and link this group to the new password policy.
 - d. Create the local HMI users; add these users to the HMI user group and to the corresponding IEC 62351 or Siemens specific (roles) groups. Set numeric-only passcodes for these users.
4. Start Network Policy Server (NPS) and configure the policies and RADIUS Clients

1.5 Detailed description

1.5.1 Create a new Organizational Unit (OU) called *IEC 62351 Group*

1. Open the Active Directory users Directory Users and Computers via the Server Manager and the Tools menu
2. Right click on domain level and create the new OU *IEC 62351 group* (or whatever you want to name it)



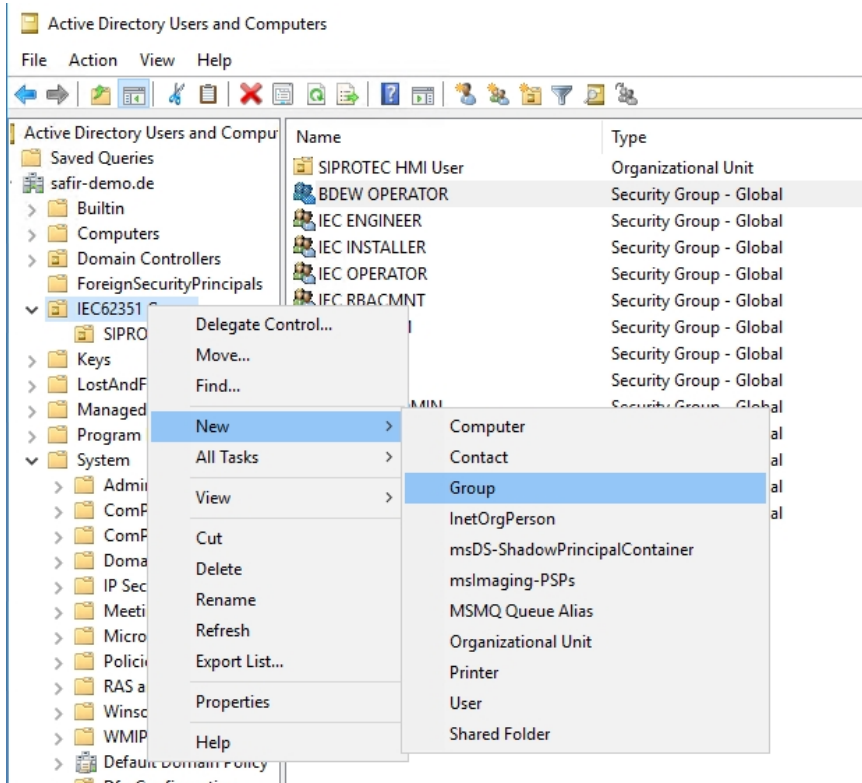
1.5.2 Add Global Security Groups

On OU level create all necessary IEC 62351 and Siemens roles as *Global Security Groups* as shown below.

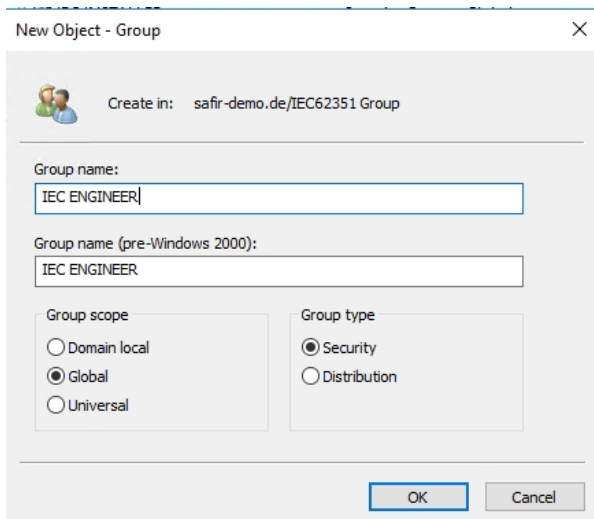
Note: You can choose any other group names because the mapping to RADIUS attributes follows in a later step. The name is not essential for a proper functionality of the devices.

Cyber Security

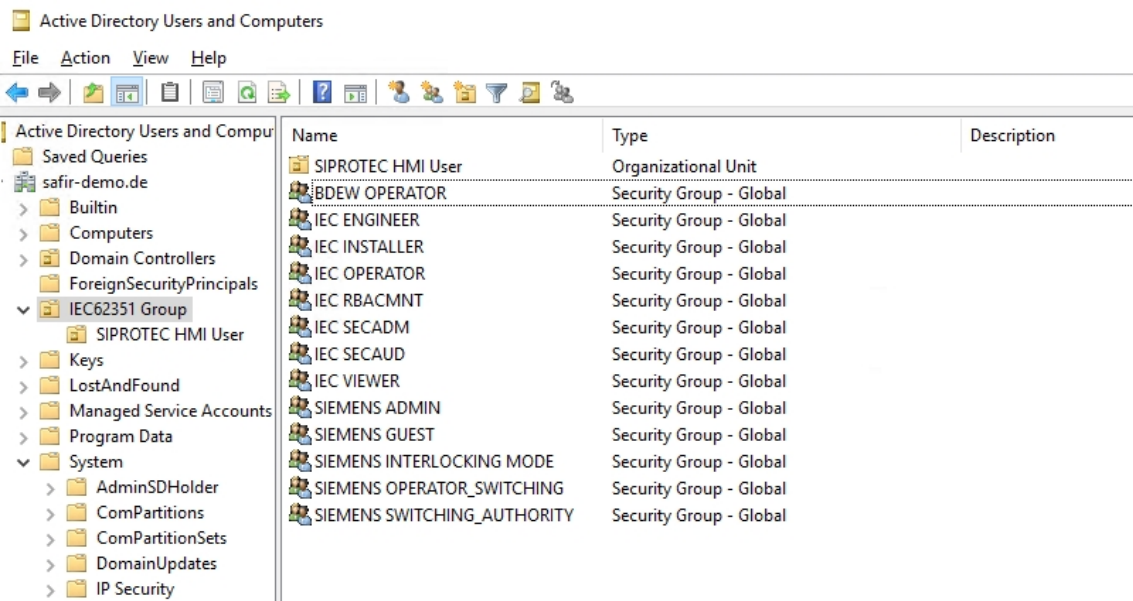
Configuration of a Windows Active Directory and NPS



Create new roles with a right click to the IEC 62351 group and select New → Group



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

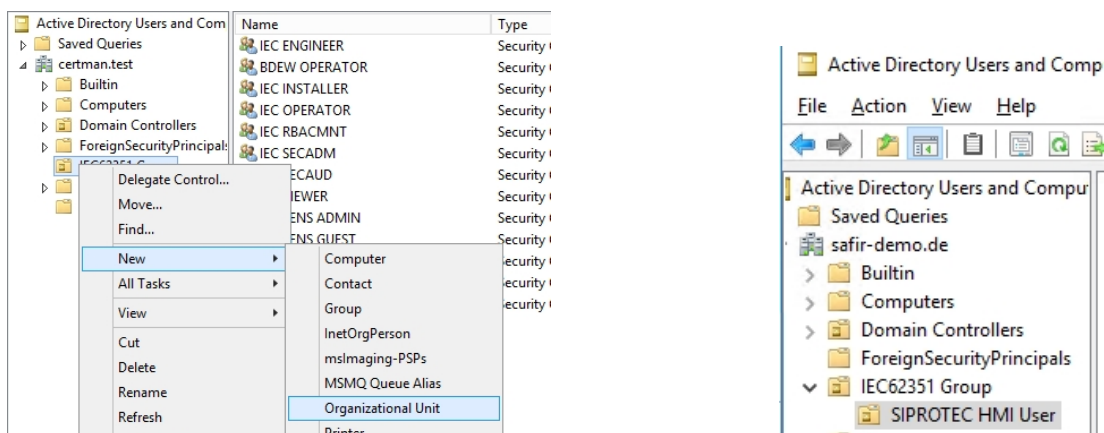


1.5.3 Local users for SIPROTEC 5 devices

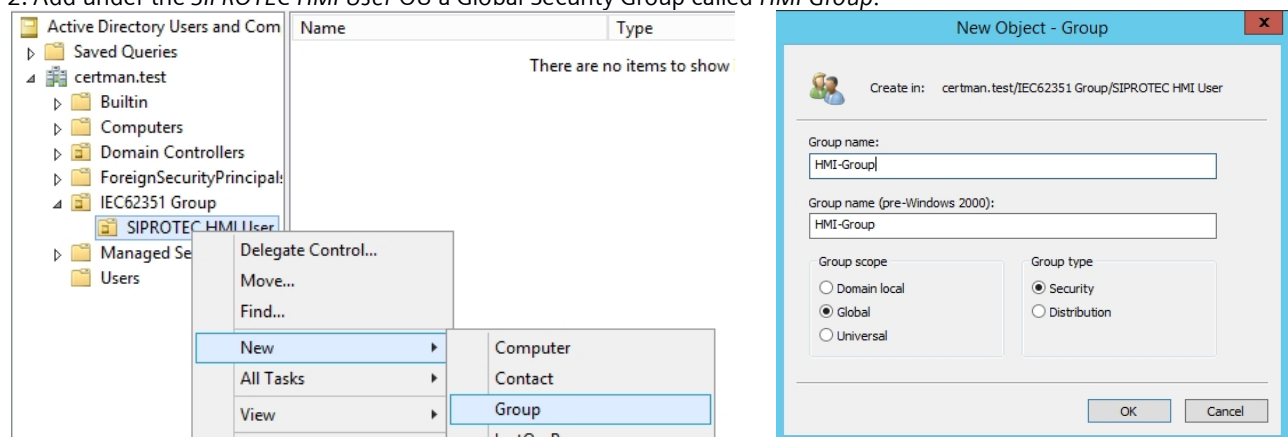
Add an additional Organizational Unit (OU) called SIPROTEC HMI User.

Note: Other group names can also be chosen. The name is not essential for the proper functionality of the devices.

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



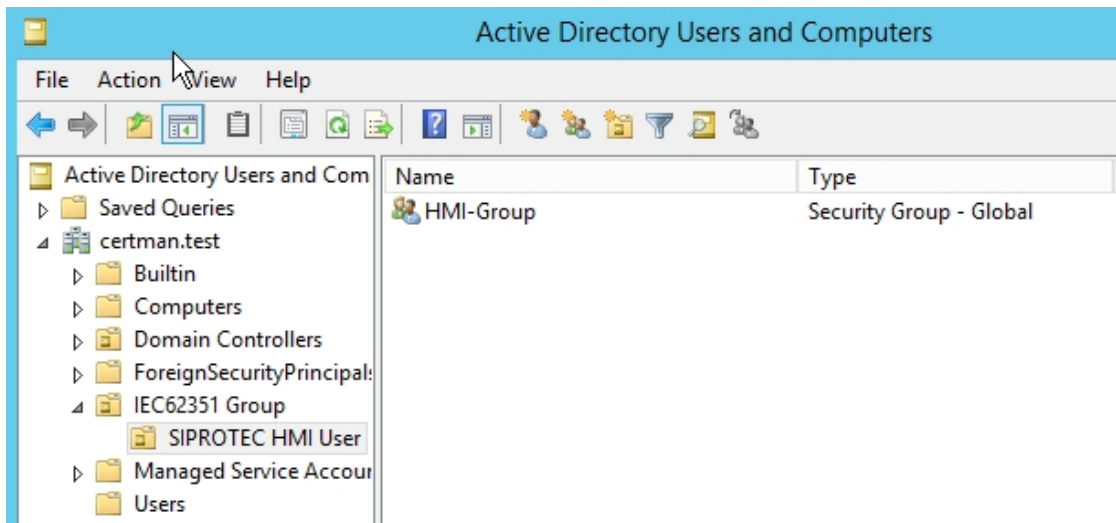
2. Add under the *SIPROTEC HMI User* OU a Global Security Group called *HMI Group*.



Cyber Security

Configuration of a Windows Active Directory and NPS

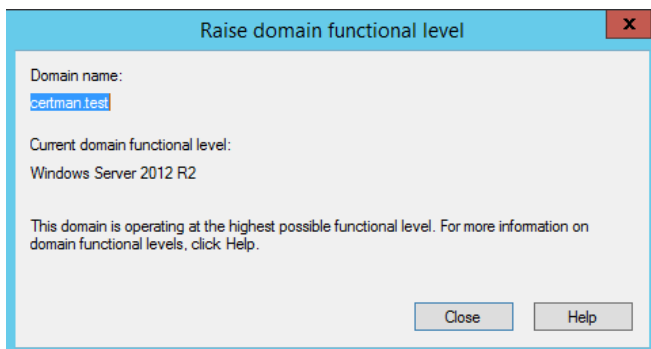
This group is needed for users using the weak password policy with numeric passcodes



3. Due to HMI user can have only simple numeric passcodes, the password policy of the HMI users need only be changed. The following instruction has been used: <http://www.grouppolicy.biz/2011/08/tutorial-how-to-setup-default-and-fine-grain-password-policy/>

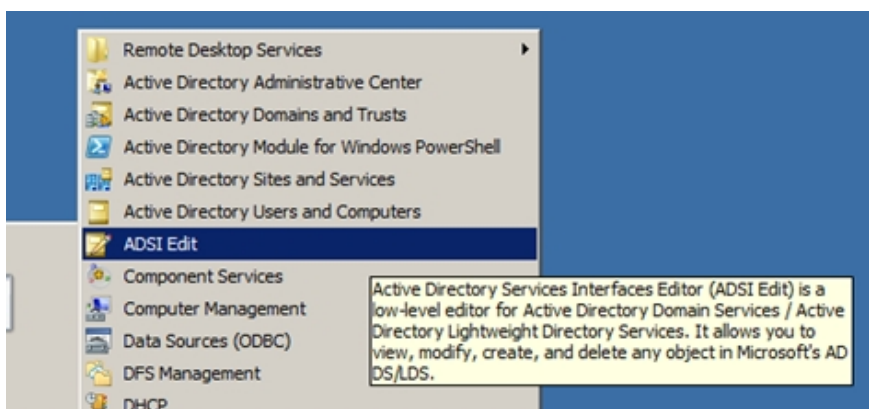
PRE-REQUISITES/RESTRICTIONS

Your domain must be Windows Server 2008 Native Mode or later, this means ALL of your domain controllers must be running Windows Server 2008 or later. You can check this by selection the "Raise domain functional level" on the top of the domain in Active Directory Users and Computers.



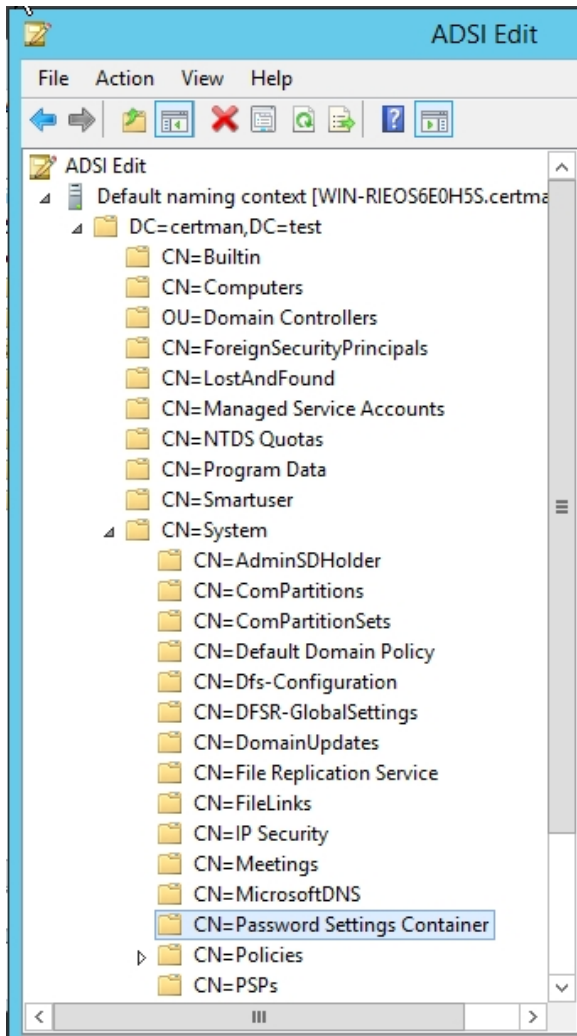
CREATING A PASSWORD SETTING OBJECT (PSO)

Step 1: Start ADSI Edit via Server Manager Tools Menu or under Administrator Tools Open ADSI Edit and connect it to a domain and domain controller you want to setup the new password policy

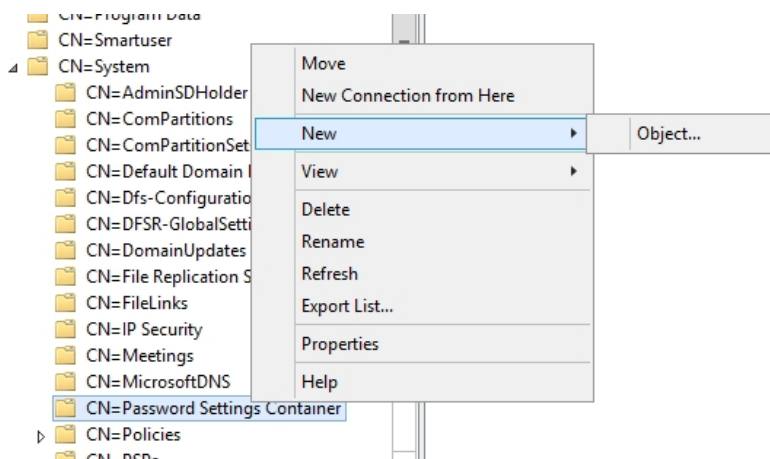


Note: If this option does not be appeared, go to “Turn Windows Features On or Off” and make sure the “AD DS and AD LDS Tools” are installed. RSAT need also to be installed in the operating system Windows 7.

Step 2: Double click on the “CN=DomainName”, then double click on “CN=System” and then double click on “CN=Passowrd Settings Container”.



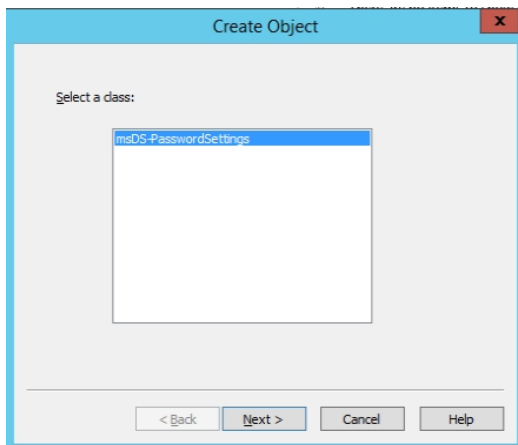
Step 3: Right click on “CN=Password Settings Container” and the nclick on “New” then “Object...”



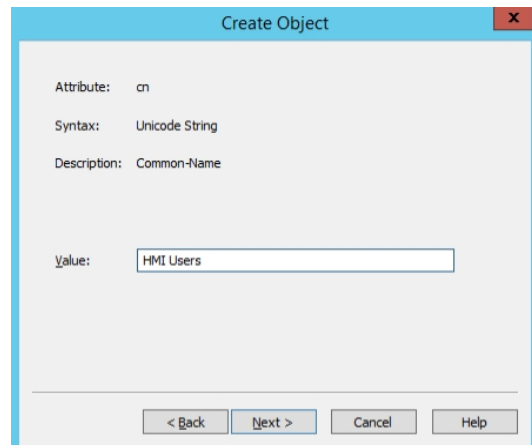
Step 4: Click on “Next”

Cyber Security

Configuration of a Windows Active Directory and NPS



The 'Create Object' dialog box shows the 'Select a class:' section with a list box containing 'msDS-PasswordSettings'. The 'Next >' button is highlighted.



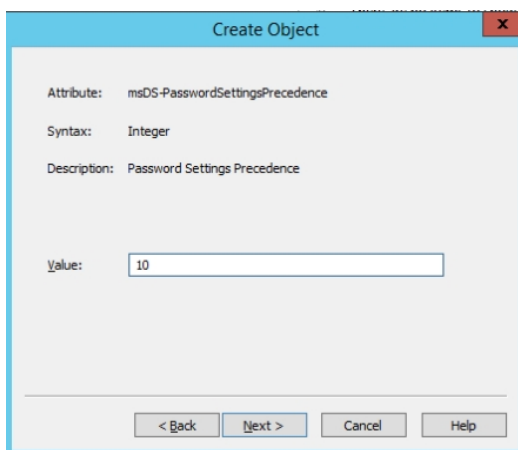
The 'Create Object' dialog box shows the 'Attribute: cn', 'Syntax: Unicode String', and 'Description: Common-Name'. The 'Value:' field contains 'HMI Users'.

Step 5: Type the name "HMI Users" of the PSO in the "Value" field and then click "Next"

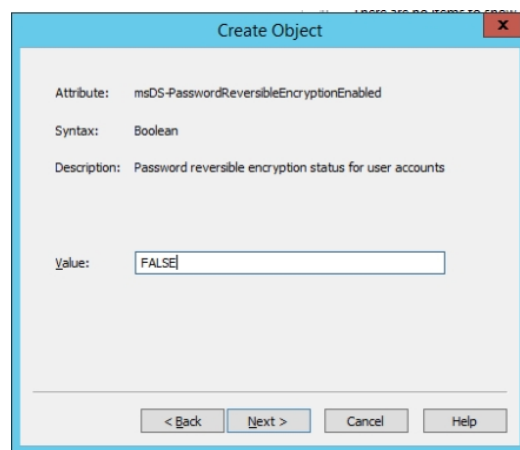
Note: With the exception of the password length the following values are all the same as the default values in "Default Domain Policy".

Step 6: Type in a number that will be the Precedence for this Password Policy then click "Next".

Note: This is used if a user has multiple Password Settings Object (PSO) definitions applied to them.



The 'Create Object' dialog box shows the 'Attribute: msDS-PasswordSettingsPrecedence', 'Syntax: Integer', and 'Description: Password Settings Precedence'. The 'Value:' field contains '10'.

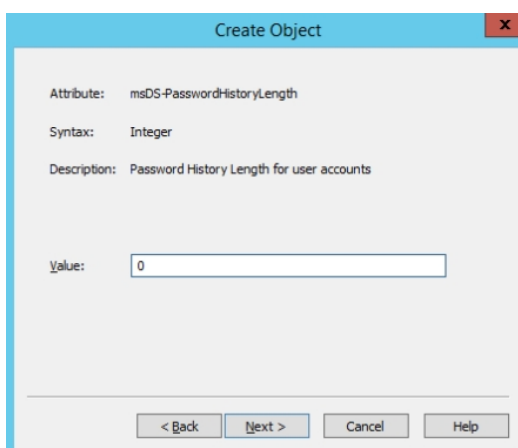


The 'Create Object' dialog box shows the 'Attribute: msDS-PasswordReversibleEncryptionEnabled', 'Syntax: Boolean', and 'Description: Password reversible encryption status for user accounts'. The 'Value:' field contains 'FALSE'.

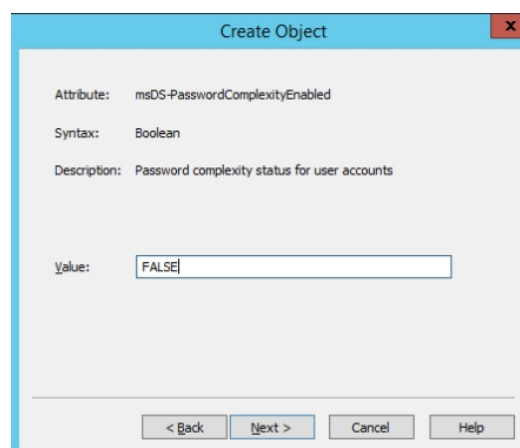
Step 7: Type "FALSE" in the value field and click "Next"

Note: You should almost never use "TRUE" for this setting.

Step 8: Type "0" in the "Value" field and click "Next"



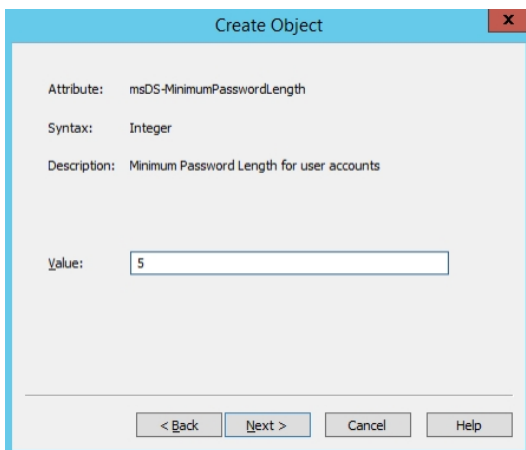
The 'Create Object' dialog box shows the 'Attribute: msDS-PasswordHistoryLength', 'Syntax: Integer', and 'Description: Password History Length for user accounts'. The 'Value:' field contains '0'.



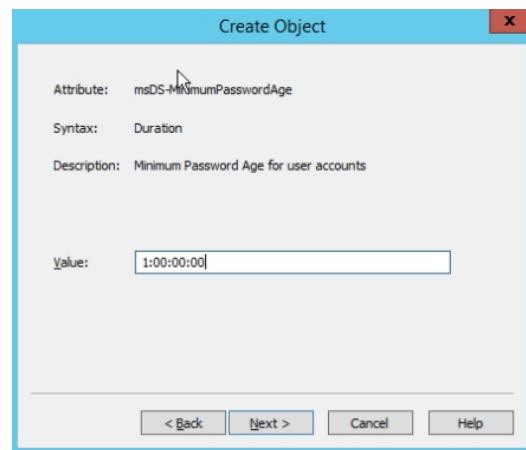
The 'Create Object' dialog box shows the 'Attribute: msDS-PasswordComplexityEnabled', 'Syntax: Boolean', and 'Description: Password complexity status for user accounts'. The 'Value:' field contains 'FALSE'.

Step 9: Type "FALSE" in the "Value" field and click "Next"

Step 10: Type "5" in the "Value" field and click "Next"



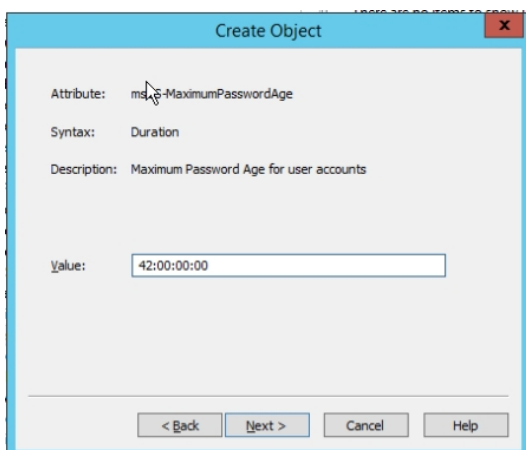
The 'Create Object' dialog box shows the configuration for the 'msDS-MinimumPasswordLength' attribute. The attribute is of type 'Integer' and is described as 'Minimum Password Length for user accounts'. The 'Value' field contains the number '5'. At the bottom, there are buttons for '< Back', 'Next >', 'Cancel', and 'Help'.



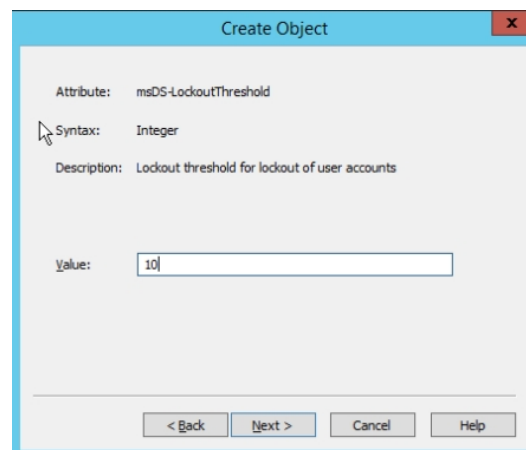
The 'Create Object' dialog box shows the configuration for the 'msDS-MinimumPasswordAge' attribute. The attribute is of type 'Duration' and is described as 'Minimum Password Age for user accounts'. The 'Value' field contains the time '1:00:00:00'. At the bottom, there are buttons for '< Back', 'Next >', 'Cancel', and 'Help'.

Step 11: Type "1:00:00:00" in the "Value" field and click "Next"

Step 12: Type "42:00:00:00" in the "Value" field and click "Next"



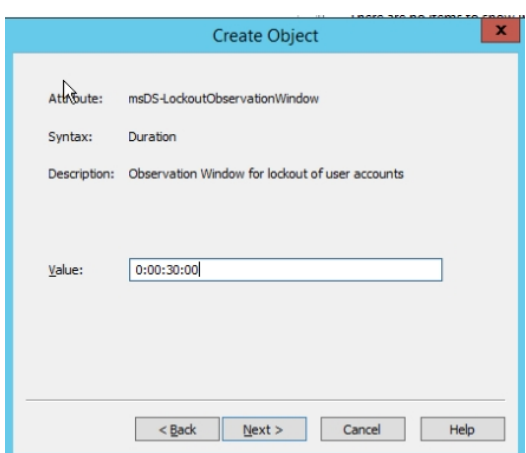
The 'Create Object' dialog box shows the configuration for the 'msDS-MaximumPasswordAge' attribute. The attribute is of type 'Duration' and is described as 'Maximum Password Age for user accounts'. The 'Value' field contains the time '42:00:00:00'. At the bottom, there are buttons for '< Back', 'Next >', 'Cancel', and 'Help'.



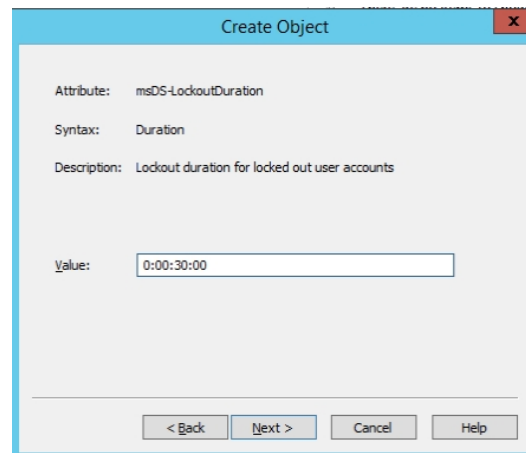
The 'Create Object' dialog box shows the configuration for the 'msDS-UnlockThreshold' attribute. The attribute is of type 'Integer' and is described as 'Lockout threshold for lockout of user accounts'. The 'Value' field contains the number '10'. At the bottom, there are buttons for '< Back', 'Next >', 'Cancel', and 'Help'.

Step 13: Type "10" in the "Value" field and click "Next"

Step 14: Type "0:00:30:00" field and click "Next"



The 'Create Object' dialog box shows the configuration for the 'msDS-LockoutObservationWindow' attribute. The attribute is of type 'Duration' and is described as 'Observation Window for lockout of user accounts'. The 'Value' field contains the time '0:00:30:00'. At the bottom, there are buttons for '< Back', 'Next >', 'Cancel', and 'Help'.



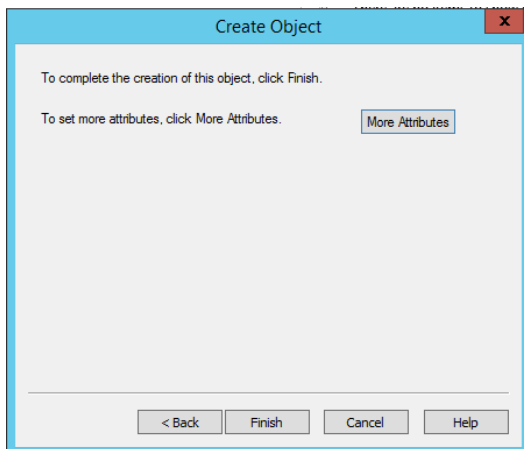
The 'Create Object' dialog box shows the configuration for the 'msDS-LockoutDuration' attribute. The attribute is of type 'Duration' and is described as 'Lockout duration for locked out user accounts'. The 'Value' field contains the time '0:00:30:00'. At the bottom, there are buttons for '< Back', 'Next >', 'Cancel', and 'Help'.

Step 15: Type "0:00:30:00" in the "Value" field and click "Next"

Cyber Security

Configuration of a Windows Active Directory and NPS

Step 16: Click "Finish".



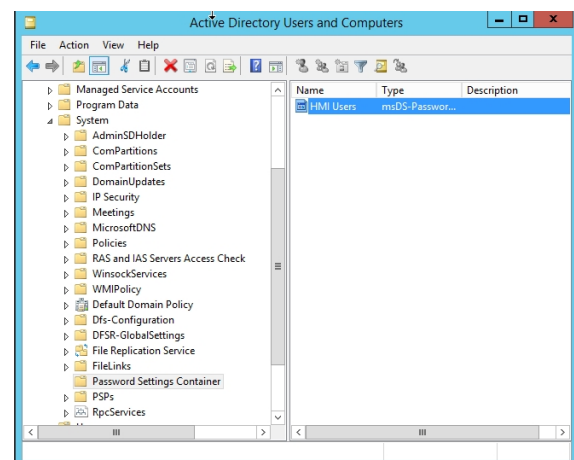
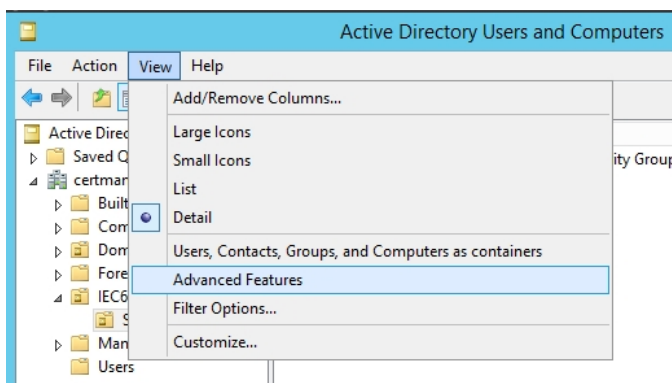
You have created the Password Settings Object (PSO) and you can close the ADSI Edit tool.

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

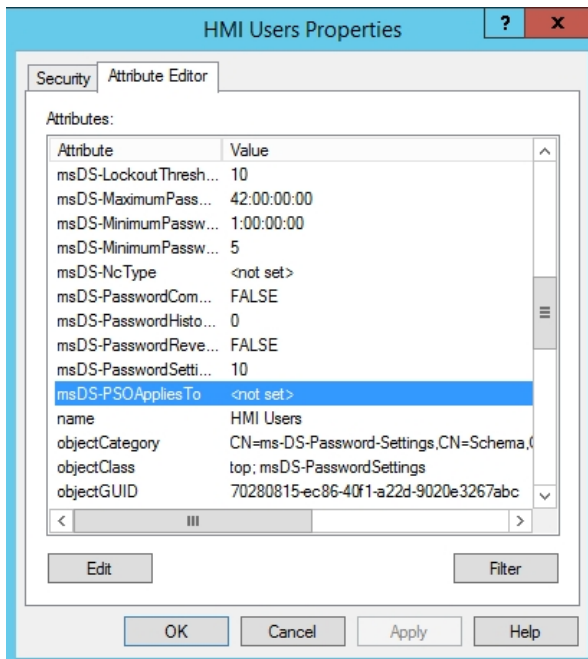
4. Now to apply the PSO to an user or group...

Step 17: Open *Active Directory Users and Computers* and navigate to "System > Password Settings Container".

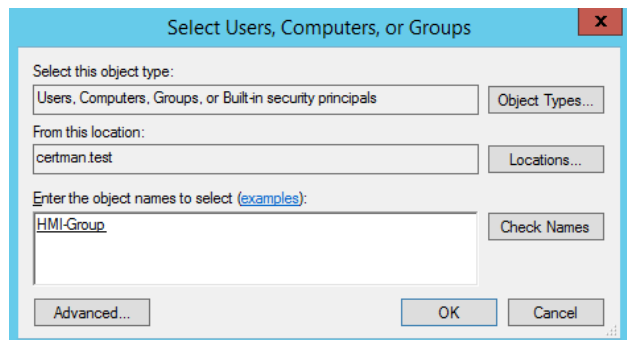
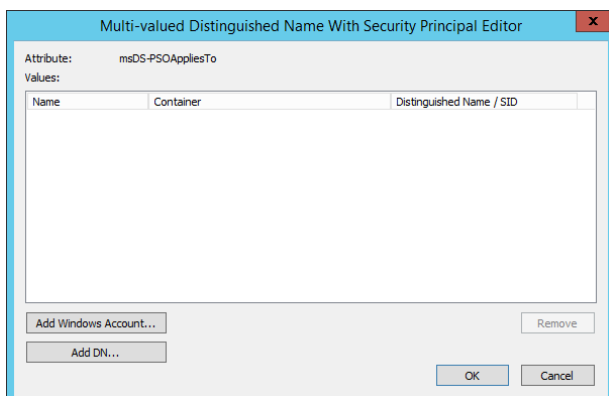
Note: Advanced Mode needs to be enabled and press refresh in case of the Container is not visible.



Step 18: Double click on the PSO you created then click on the "Attribute Editor" tab and then select the "*msDS-PSOAppliedTo*" attribute...
... and click "Edit"



Step 19: Click "Add Windows Accounts...." button.

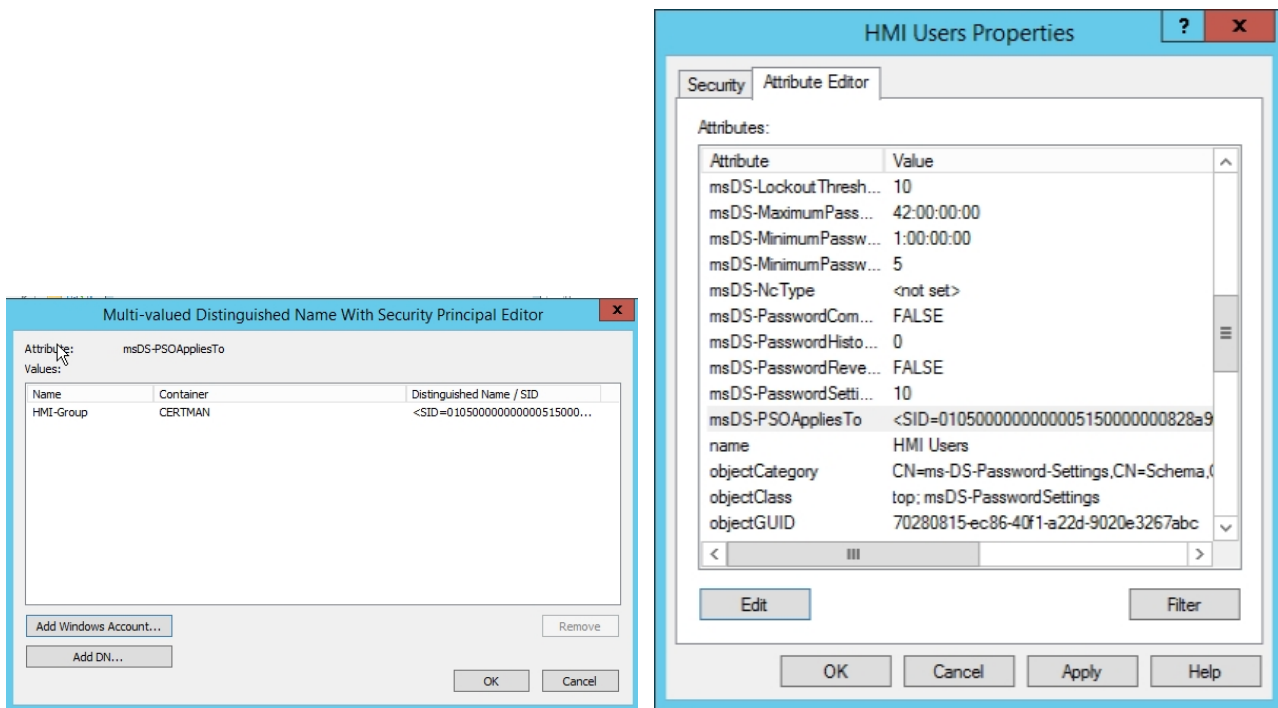


Step 20: Select the group "HMI-Group" to apply this PSO and click "OK"

Step 21: Click "OK"

Cyber Security

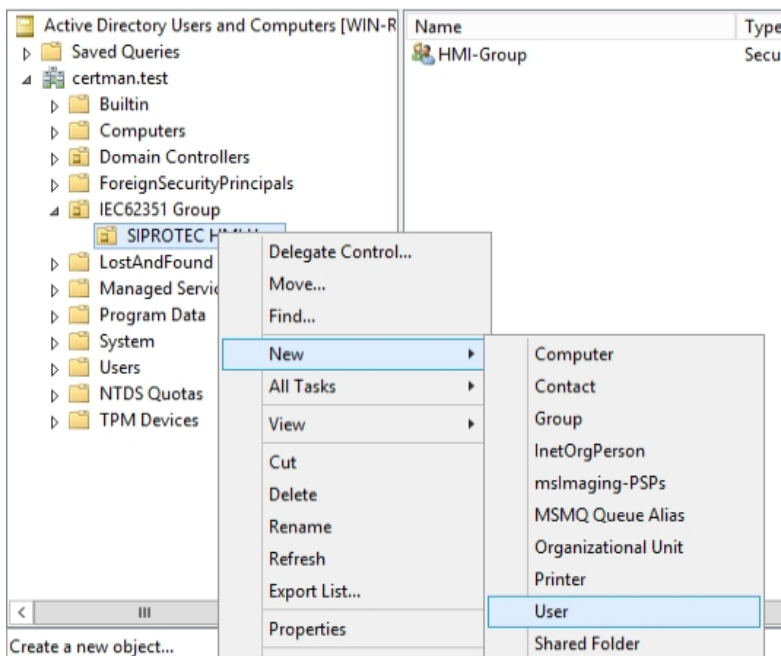
Configuration of a Windows Active Directory and NPS



Step 22: Click "OK"

And now it is done in AD SI.

5. Now, add all HMI users under "SIPROTEC HMI User" in a first step with a strong password.



Be sure that the *User logon name* is identical to the name. Create in the same way following users:

ADMIN, ENGINEER, VIEWER, INSTALLER, OPERATOR, SECADM, SECAUD,
Operator_Switching, Switching_Authority, Interlocking_Mode

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

Note: You have to use a strong password during user creation phase also in case you have mapped the weak security policy in an earlier step.

Cyber Security

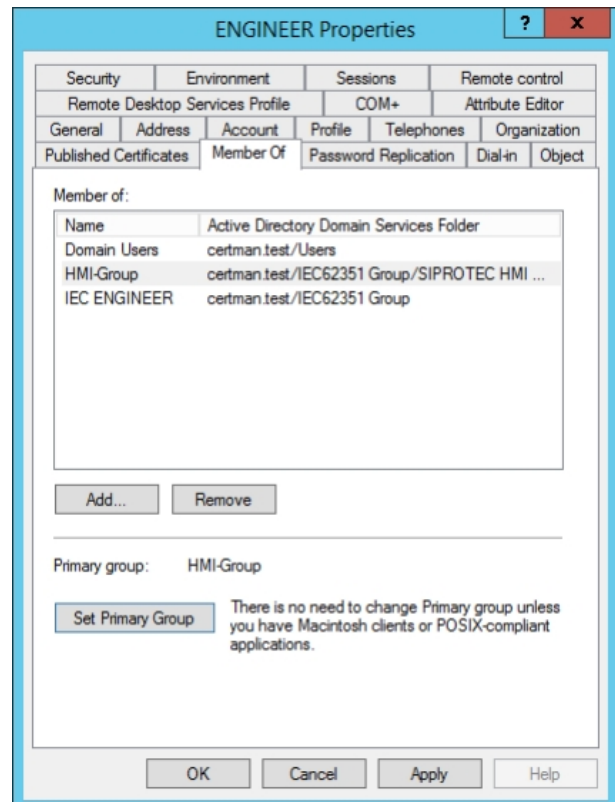
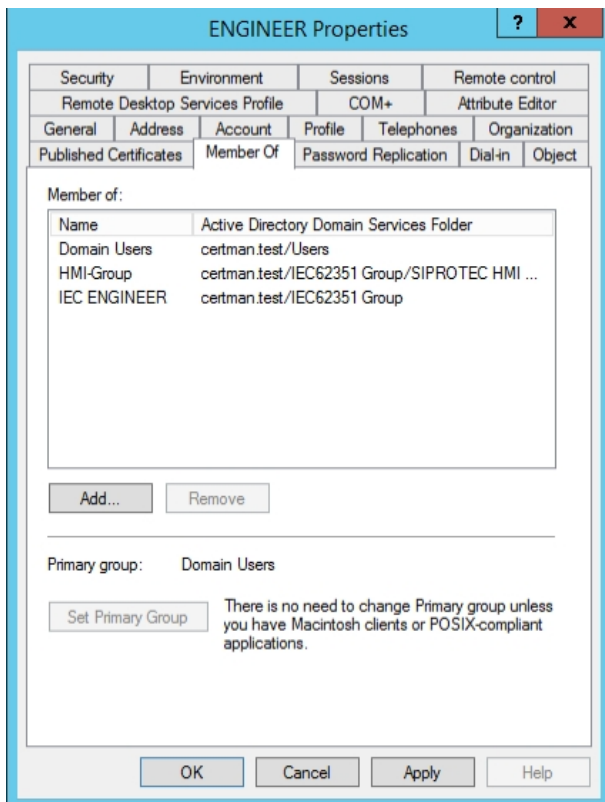
Configuration of a Windows Active Directory and NPS

| Active Directory Users and Computers [WIN-R] | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|------|------|-------|------|----------|------|-----------|-------------------------|-----------|------|-------------------|------|----------|------|--------------------|------|--------|------|--------|------|---------------------|------|--------|------|
| <ul style="list-style-type: none"> Active Directory Users and Computers [WIN-R] <ul style="list-style-type: none"> Saved Queries certman.test <ul style="list-style-type: none"> Builtin Computers Domain Controllers ForeignSecurityPrincipals IEC62351 Group <ul style="list-style-type: none"> SIPROTEC HMI User LostAndFound Managed Service Accounts Program Data System | <table> <thead> <tr> <th>Name</th><th>Type</th></tr> </thead> <tbody> <tr><td>ADMIN</td><td>User</td></tr> <tr><td>ENGINEER</td><td>User</td></tr> <tr><td>HMI-Group</td><td>Security Group - Global</td></tr> <tr><td>INSTALLER</td><td>User</td></tr> <tr><td>Interlocking_Mode</td><td>User</td></tr> <tr><td>OPERATOR</td><td>User</td></tr> <tr><td>Operator_Switching</td><td>User</td></tr> <tr><td>SECADM</td><td>User</td></tr> <tr><td>SECAUD</td><td>User</td></tr> <tr><td>Switching_Authority</td><td>User</td></tr> <tr><td>VIEWER</td><td>User</td></tr> </tbody> </table> | Name | Type | ADMIN | User | ENGINEER | User | HMI-Group | Security Group - Global | INSTALLER | User | Interlocking_Mode | User | OPERATOR | User | Operator_Switching | User | SECADM | User | SECAUD | User | Switching_Authority | User | VIEWER | User |
| Name | Type | | | | | | | | | | | | | | | | | | | | | | | | |
| ADMIN | User | | | | | | | | | | | | | | | | | | | | | | | | |
| ENGINEER | User | | | | | | | | | | | | | | | | | | | | | | | | |
| HMI-Group | Security Group - Global | | | | | | | | | | | | | | | | | | | | | | | | |
| INSTALLER | User | | | | | | | | | | | | | | | | | | | | | | | | |
| Interlocking_Mode | User | | | | | | | | | | | | | | | | | | | | | | | | |
| OPERATOR | User | | | | | | | | | | | | | | | | | | | | | | | | |
| Operator_Switching | User | | | | | | | | | | | | | | | | | | | | | | | | |
| SECADM | User | | | | | | | | | | | | | | | | | | | | | | | | |
| SECAUD | User | | | | | | | | | | | | | | | | | | | | | | | | |
| Switching_Authority | User | | | | | | | | | | | | | | | | | | | | | | | | |
| VIEWER | User | | | | | | | | | | | | | | | | | | | | | | | | |

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

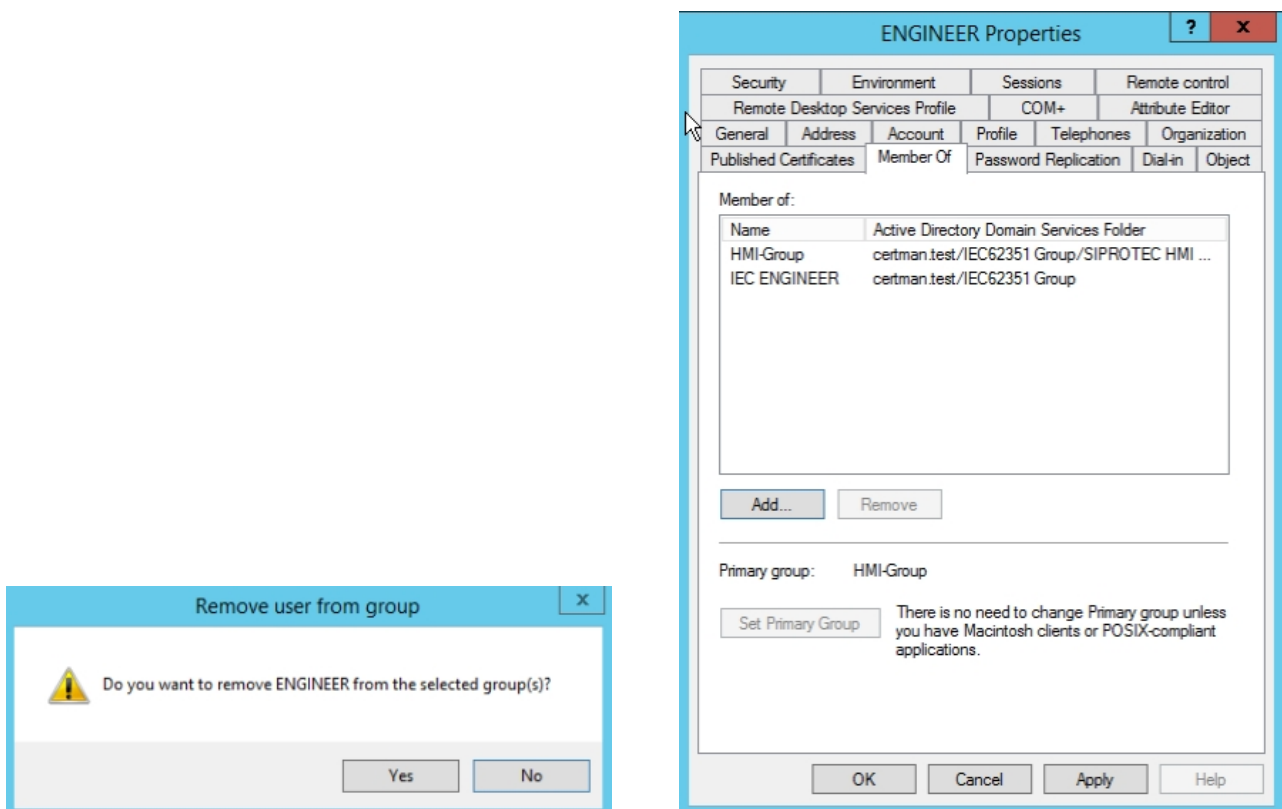
| Users of HMI-Group | IEC or Siemens Group |
|---------------------|-----------------------------|
| ADMIN | SIEMENS ADMIN |
| VIEWER | IEC VIEWER |
| OPERATOR | IEC OPERATOR |
| ENGINEER | IEC ENGINEER |
| INSTALLER | IEC INSTALLER |
| SECADM | IEC SECADM |
| SECAUD | IEC SECAUD |
| RBACMNT | IEC RBACMNT |
| Operator_Switching | SIEMENS OPERATOR_SWITCHING |
| Switching_Authority | SIEMENS SWITCHING_AUTHORITY |
| Interlocking_Mode | SIEMENS INTERLOCKING MODE |

| Active Directory Users and Computers | | | |
|--------------------------------------|-----------------------------|-------------------------|-------------|
| File Action View Help | | | |
| | | | |
| Active Directory Users and Computers | Name | Type | Description |
| Saved Queries | SIPROTEC HMI User | Organizational Unit | |
| safir-demo.de | BDEW OPERATOR | Security Group - Global | |
| Builtin | IEC ENGINEER | Security Group - Global | |
| Computers | IEC INSTALLER | Security Group - Global | |
| Domain Controllers | IEC OPERATOR | Security Group - Global | |
| ForeignSecurityPrincipals | IEC RBACMNT | Security Group - Global | |
| IEC62351 Group | IEC SECADM | Security Group - Global | |
| SIPROTEC HMI User | IEC SECAUD | Security Group - Global | |
| Keys | IEC VIEWER | Security Group - Global | |
| LostAndFound | SIEMENS ADMIN | Security Group - Global | |
| Managed Service Accounts | SIEMENS GUEST | Security Group - Global | |
| Program Data | SIEMENS INTERLOCKING MODE | Security Group - Global | |
| System | SIEMENS OPERATOR_SWITCHING | Security Group - Global | |
| AdminSDHolder | SIEMENS SWITCHING_AUTHORITY | Security Group - Global | |
| ComPartitions | | | |
| ComPartitionSets | | | |
| DomainUpdates | | | |
| IP Security | | | |



7. Set HMI-Group as Primary Group.

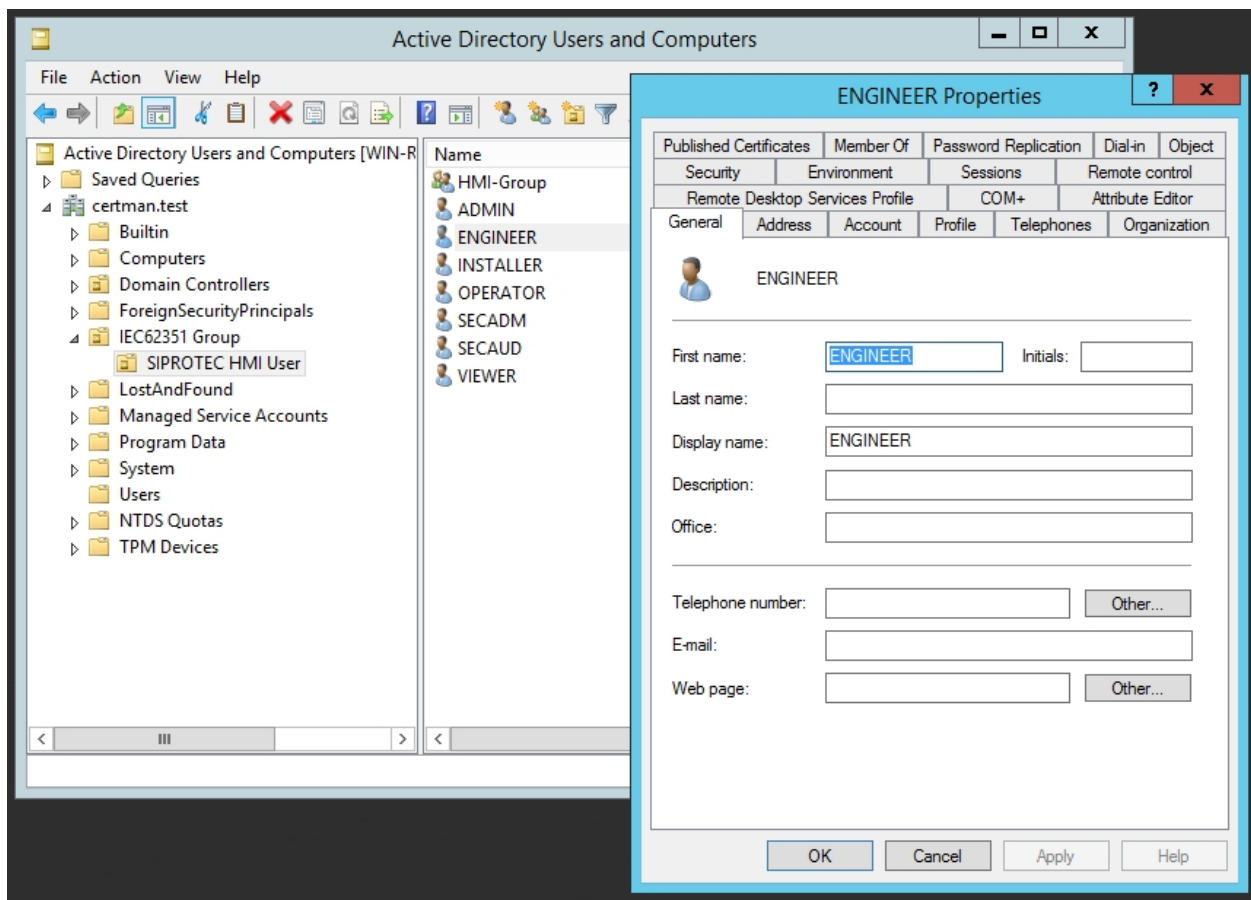
8. Then remove "Domain Users" default group.



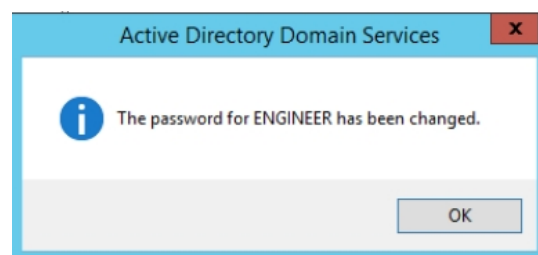
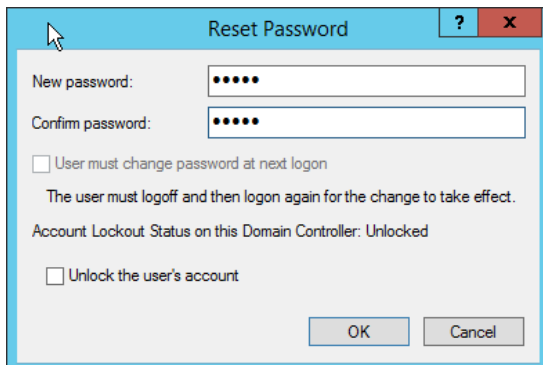
Now it should look like as follows for all users:

Cyber Security

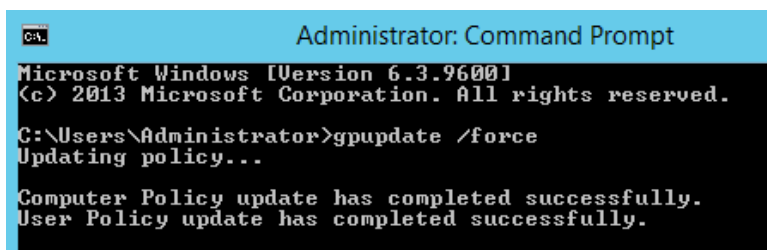
Configuration of a Windows Active Directory and NPS



9. Now the HMI Passwords can be set to a simple numeric passcode, e.g 12345 (recommended to be with at least 5 digits)



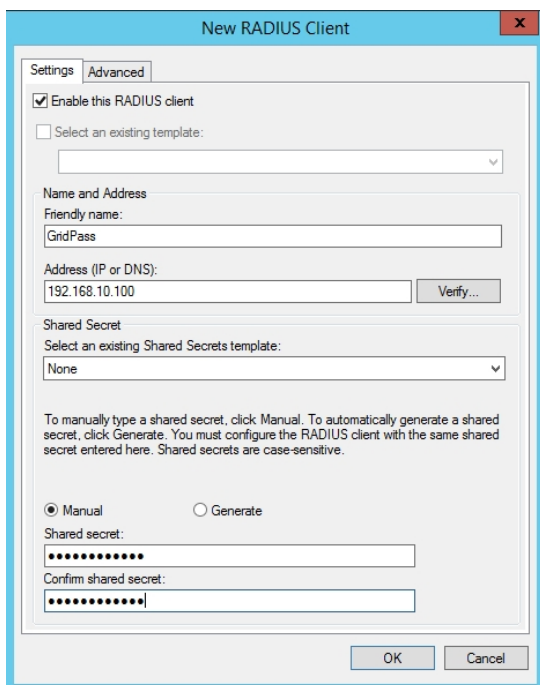
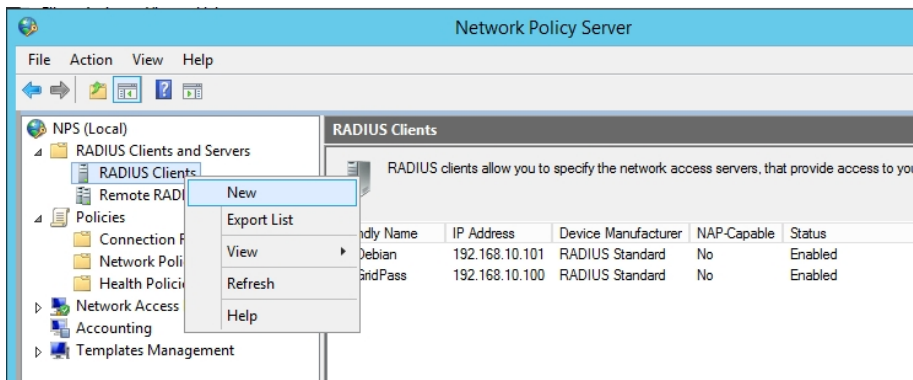
Before starting NPS update Computer and User Policy via the command shell and following command: `gpupdate /force`



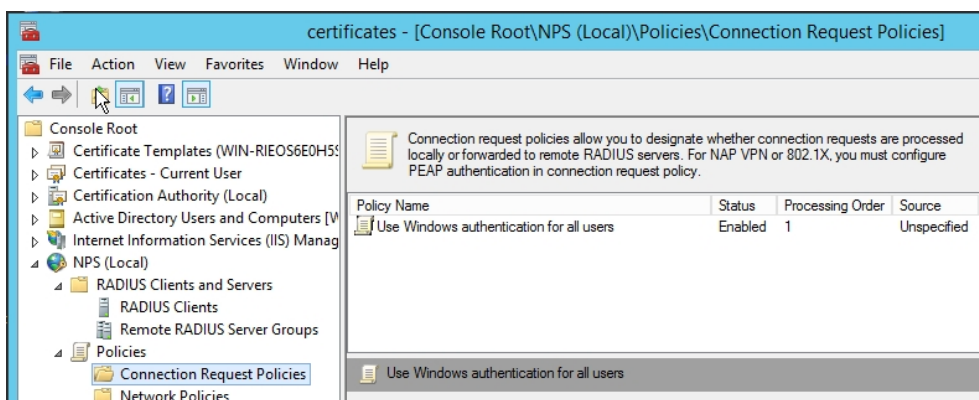
1.5.4 Configuration of the Network Policy Server

Start the Network Policy Server via the Server Manager Tools.

1. Add all RADIUS Clients with friendly name and the IP which comes with the requested UDP packet to the NPS and choose a shared secret which you have also to enter in the client system.



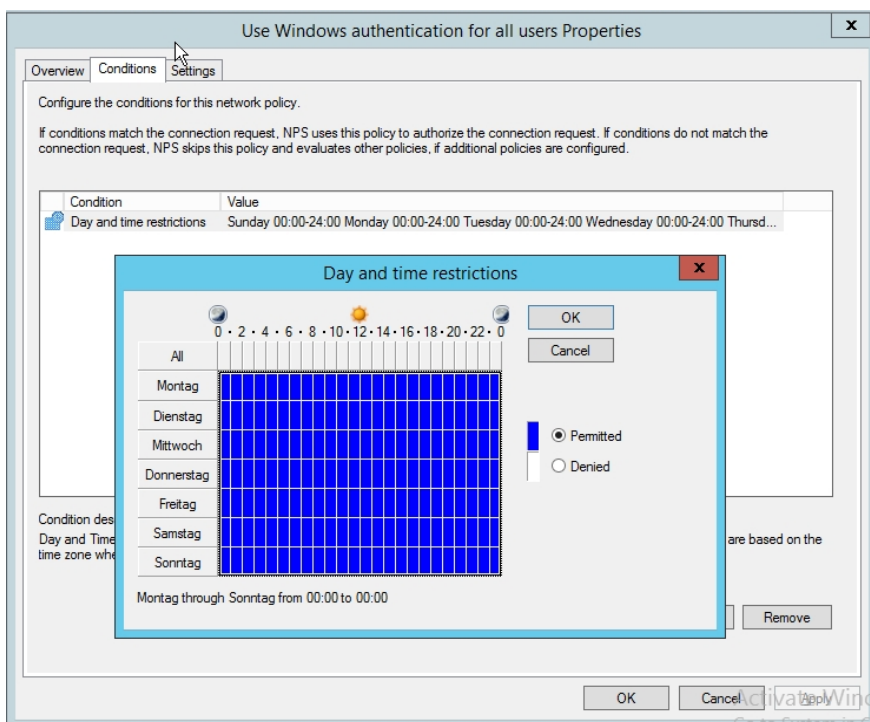
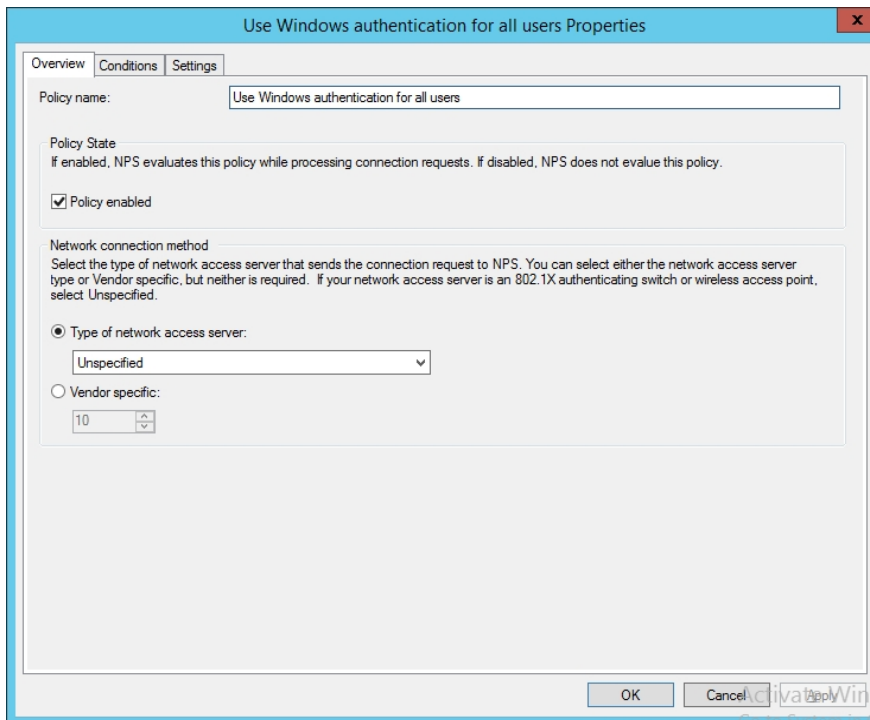
2. Add at least one allowing connection policy.



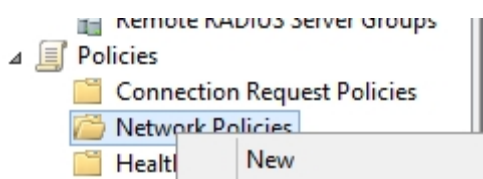
e.g. for day and time restriction

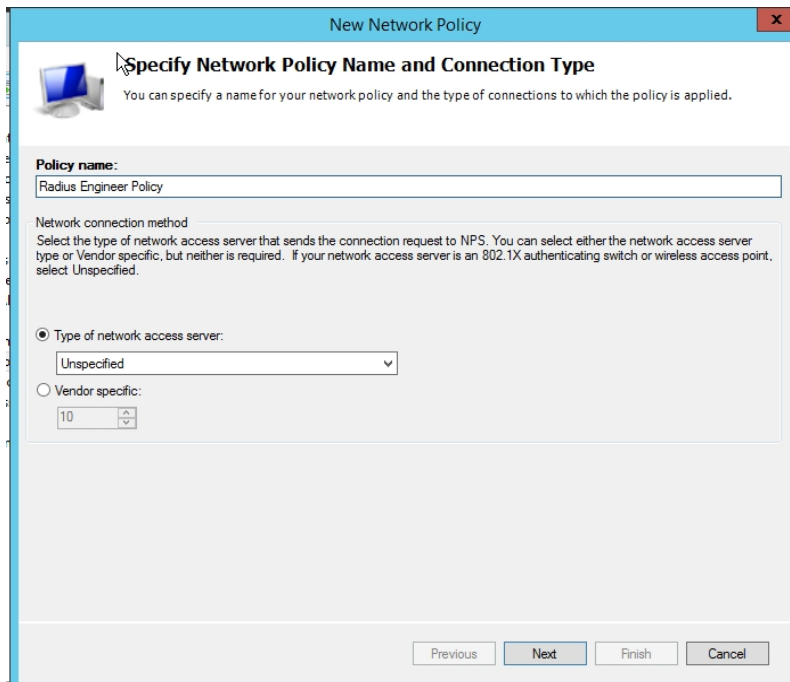
Cyber Security

Configuration of a Windows Active Directory and NPS



3. Create the network policies with the context menu and choose New,





New Network Policy

Specify Network Policy Name and Connection Type
You can specify a name for your network policy and the type of connections to which the policy is applied.

Policy name:
Radius Engineer Policy

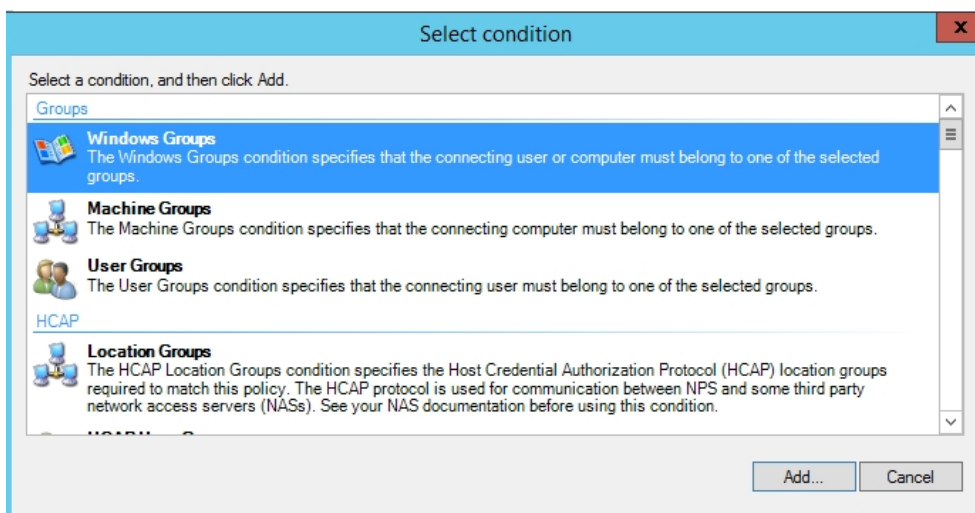
Network connection method
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

☒ **Type of network access server:**
Unspecified

☐ **Vendor specific:**
10

Previous Next Finish Cancel

Click Next and add a Windows Group as Condition



Select condition

Select a condition, and then click Add.

Groups

- Windows Groups**
The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups.
- Machine Groups**
The Machine Groups condition specifies that the connecting computer must belong to one of the selected groups.
- User Groups**
The User Groups condition specifies that the connecting user must belong to one of the selected groups.

HCAP

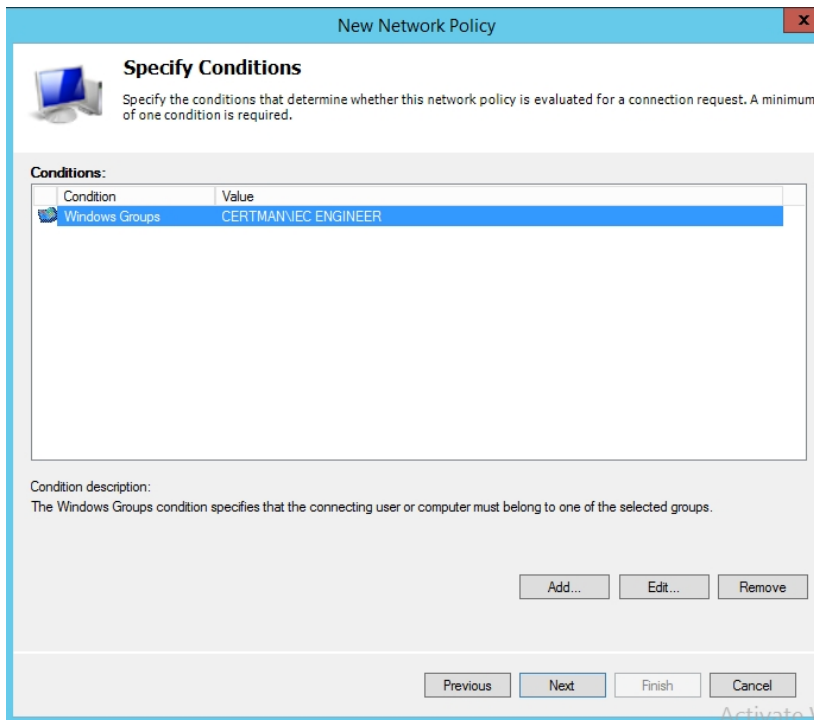
- Location Groups**
The HCAP Location Groups condition specifies the Host Credential Authorization Protocol (HCAP) location groups required to match this policy. The HCAP protocol is used for communication between NPS and some third party network access servers (NASs). See your NAS documentation before using this condition.

Add... Cancel

Choose the corresponding IEC or Siemens group for the created policy

Cyber Security

Configuration of a Windows Active Directory and NPS



New Network Policy

Specify Conditions

Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

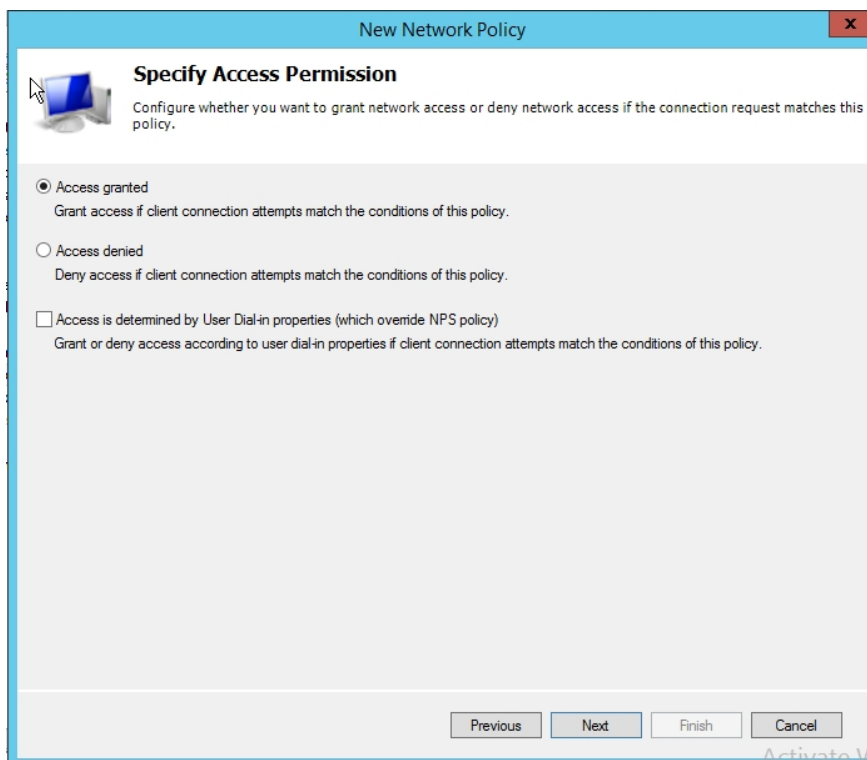
Conditions:

| Condition | Value |
|----------------|---------------------|
| Windows Groups | CERTMANNEC ENGINEER |

Condition description:
The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups.

Buttons: Add..., Edit..., Remove

Navigation: Previous, Next, Finish, Cancel



New Network Policy

Specify Access Permission

Configure whether you want to grant network access or deny network access if the connection request matches this policy.

☒ Access granted
Grant access if client connection attempts match the conditions of this policy.

☐ Access denied
Deny access if client connection attempts match the conditions of this policy.

☐ Access is determined by User Dial-in properties (which override NPS policy)
Grant or deny access according to user dial-in properties if client connection attempts match the conditions of this policy.

Navigation: Previous, Next, Finish, Cancel

Choose the additional authentication method PAP

New Network Policy

Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

Move Up
Move Down

Add... Edit... Remove

Less secure authentication methods:

- ☒ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
 - ☒ User can change password after it has expired
- ☒ Microsoft Encrypted Authentication (MS-CHAP)
 - ☒ User can change password after it has expired
- ☐ Encrypted authentication (CHAP)
- ☒ Unencrypted authentication (PAP, SPAP)
- ☐ Allow clients to connect without negotiating an authentication method.
- ☐ Perform machine health check only

Previous Next Finish Cancel

New Network Policy

Configure Constraints

Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Constraints are optional; if you do not want to configure constraints, click Next.

Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.

Constraints:

Constraints

- Idle Timeout
- Session Timeout
- Called Station ID
- Day and time restrictions
- NAS Port Type

Specify the maximum time in minutes that the server can remain idle before the connection is disconnected

☐ Disconnect after the maximum idle time

1

Previous Next Finish Cancel

Cyber Security

Configuration of a Windows Active Directory and NPS

New Network Policy

Configure Settings

NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

- RADIUS Attributes**
 - ☒ Standard
 - ☒ Vendor Specific
- Network Access Protection**
 - ☒ NAP Enforcement
 - ☒ Extended State
- Routing and Remote Access**
 - ☒ Multilink and Bandwidth Allocation Protocol (BAP)
 - ☒ IP Filters
 - ☒ Encryption
 - ☒ IP Settings

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

| Name | Value |
|-----------------|--------|
| Framed-Protocol | PPP |
| Service-Type | Framed |

Add... Edit... Remove

Previous Next Finish Cancel

Remove the standard Attributes

New Network Policy

Configure Settings

NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

- RADIUS Attributes**
 - ☒ Standard
 - ☒ Vendor Specific
- Network Access Protection**
 - ☒ NAP Enforcement
 - ☒ Extended State
- Routing and Remote Access**
 - ☒ Multilink and Bandwidth Allocation Protocol (BAP)
 - ☒ IP Filters
 - ☒ Encryption
 - ☒ IP Settings

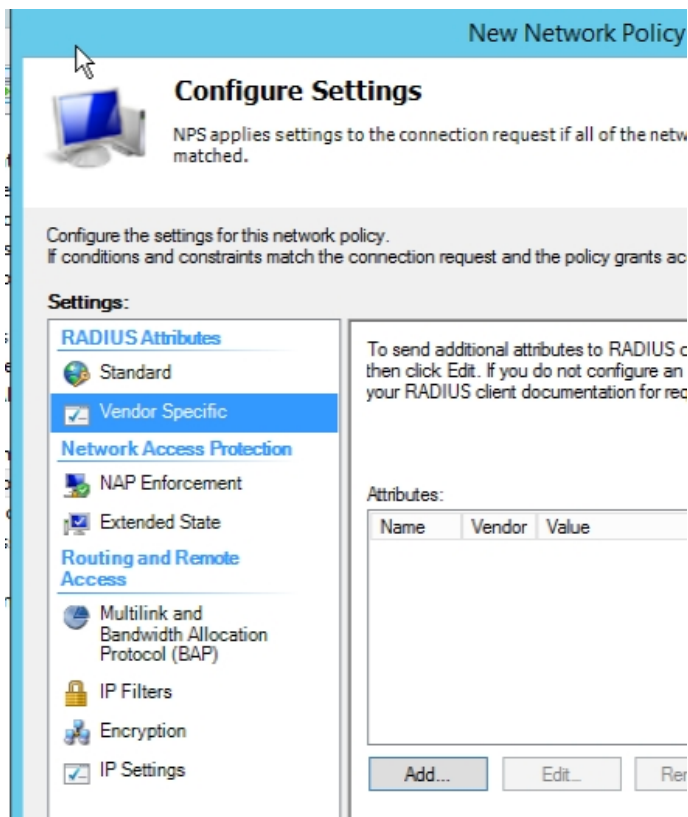
To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

| Name | Value |
|------|-------|
|------|-------|

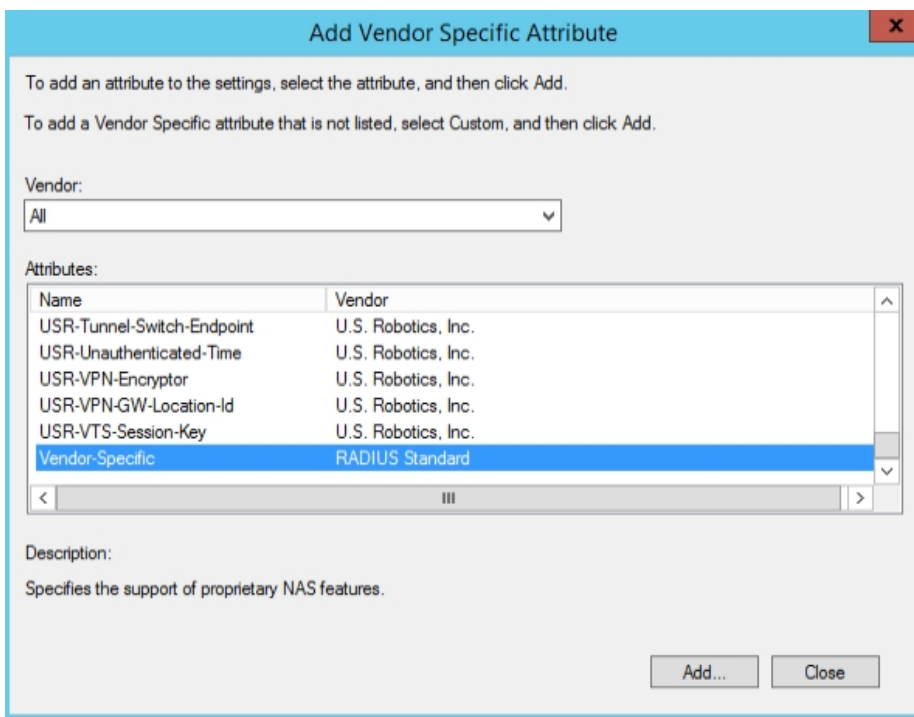
Add... Edit... Remove

Previous Next Finish Cancel

And add Vendor Specific Attributes



Add Vendor Specific



Cyber Security

Configuration of a Windows Active Directory and NPS

Attribute Information

Attribute name:
Vendor-Specific

Attribute number:
26

Attribute format:
OctetString

Attribute values:

| Vendor | Value |
|--------|-------|
|--------|-------|

Add... Edit... Remove Move Up Move Down

OK Cancel

And add the necessary IEC 62351 attributes to the Policy

Note, enclosed the current IEC62351 Dictionary for Radius for a better understanding see **Error! Reference source not found.**

| Attribute Name | Attribute Value | Required |
|-----------------------------|-----------------|-----------|
| IEC62351-8-RoleID-i | (i*10)+1 | mandatory |
| IEC62351-8-roleDefinition-i | (i*10)+2 | optional |
| IEC62351-8-aor-i | (i*10)+3 | mandatory |
| IEC62351-8-revision-i | (i*10)+4 | mandatory |
| IEC62351-8-ValidFrom-i | (i*10)+5 | optional |
| IEC62351-8-ValidTo-i | (i*10)+6 | mandatory |

Note: integer i=0..N

```
VENDORInternational Electrotechnical Commission41912
BEGIN-VENDORInternational Electrotechnical Commission
```

| | | | |
|-----------|-----------------------------|----|-----------------|
| ATTRIBUTE | IEC62351-8-RoleID-0 | 1 | integer |
| ATTRIBUTE | IEC62351-8-roleDefinition-0 | 2 | string OPTIONAL |
| ATTRIBUTE | IEC62351-8-aor-0 | 3 | string |
| ATTRIBUTE | IEC62351-8-revision-0 | 4 | integer |
| ATTRIBUTE | IEC62351-8-ValidFrom-0 | 5 | string OPTIONAL |
| ATTRIBUTE | IEC62351-8-ValidTo-0 | 6 | string |
| ATTRIBUTE | IEC62351-8-RoleID-1 | 11 | integer |
| ATTRIBUTE | IEC62351-8-roleDefinition-1 | 12 | string OPTIONAL |
| ATTRIBUTE | IEC62351-8-aor-1 | 13 | string |
| ATTRIBUTE | IEC62351-8-revision-1 | 14 | integer |
| ATTRIBUTE | IEC62351-8-ValidFrom-1 | 15 | string OPTIONAL |
| ATTRIBUTE | IEC62351-8-ValidTo-1 | 16 | string |
| ATTRIBUTE | IEC62351-8-RoleID-2 | 21 | integer |
| ATTRIBUTE | IEC62351-8-roleDefinition-2 | 22 | string OPTIONAL |
| ATTRIBUTE | IEC62351-8-aor-2 | 23 | string |
| ATTRIBUTE | IEC62351-8-revision-2 | 24 | integer |
| ATTRIBUTE | IEC62351-8-ValidFrom-2 | 25 | string OPTIONAL |
| ATTRIBUTE | IEC62351-8-ValidTo-2 | 26 | string |

```
END-VENDORInternational Electrotechnical Commission
```

Note: For limitations see chapter Siemens Appendix

Vendor-Specific Attribute Information

Attribute name:
Vendor Specific

Specify network access server vendor.

☐ Select from list: RADIUS Standard

☒ Enter Vendor Code: 41912

Specify whether the attribute conforms to the RADIUS RFC specification for vendor specific attributes.

☒ Yes. It conforms

☐ No. It does not conform

Configure Attribute...

OK Cancel

Configure Attribute...

Configure VSA (RFC Compliant)

Vendor-assigned attribute number:
1

Attribute format:
Decimal

Attribute value:
2

OK Cancel

Note and Example: Vendor-assigned attribute, number "1" means IEC6235-8-RoleID-0

ATTRIBUTE IEC62351-8-RoleID-0 1 integer

Attribute format: Decimal means integer, "2" means IEC roleID "ENGINEER"

Note: for negative values use the Hexadecimal format because of RADIUS RFC2865 defines the integer as unsigned int32. Using signed integer with NPS use the hexadecimal format

Range for signed int32: from -2.147.483.648 to 2.147.483.647

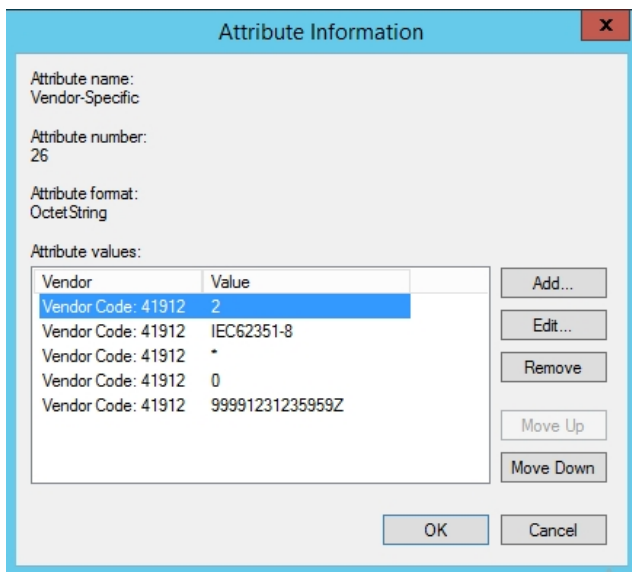
Range for unsigned int32: from 0 to 4.294.967.295

→ For example - 101 decimal results to FFFFFFF9B hex

Add all attributes and values to the Policy. For example, for the role IEC ENGINEER

Cyber Security

Configuration of a Windows Active Directory and NPS



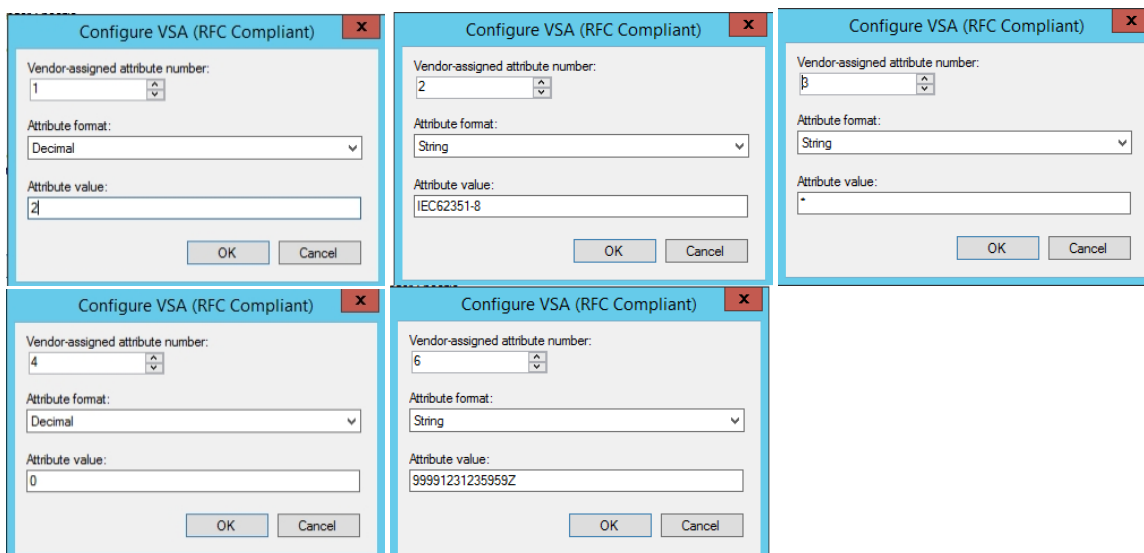
The 'Attribute Information' dialog box shows the configuration for an attribute. The attribute name is 'Vendor-Specific' and the attribute number is '26'. The attribute format is 'OctetString'. The attribute values are listed in a table with columns 'Vendor' and 'Value'. The table contains five rows: 'Vendor Code: 41912' with value '2', 'Vendor Code: 41912' with value 'IEC62351-8', 'Vendor Code: 41912' with value '*', 'Vendor Code: 41912' with value '0', and 'Vendor Code: 41912' with value '99991231235959Z'. Buttons for 'Add...', 'Edit...', 'Remove', 'Move Up', and 'Move Down' are on the right. 'OK' and 'Cancel' buttons are at the bottom.

| Vendor | Value |
|--------------------|-----------------|
| Vendor Code: 41912 | 2 |
| Vendor Code: 41912 | IEC62351-8 |
| Vendor Code: 41912 | * |
| Vendor Code: 41912 | 0 |
| Vendor Code: 41912 | 99991231235959Z |

Note:

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

Example for the Engineer policy/role:



Five 'Configure VSA (RFC Compliant)' dialog boxes are shown, each for a different vendor-assigned attribute number. Each dialog box has fields for 'Vendor-assigned attribute number', 'Attribute format', and 'Attribute value'. The attribute format is set to 'Decimal' for attribute numbers 1, 4, and 6, and 'String' for attribute numbers 2 and 3. The attribute values are: '2' for attribute 1, 'IEC62351-8' for attribute 2, '*' for attribute 3, '0' for attribute 4, and '99991231235959Z' for attribute 6. Each dialog box has 'OK' and 'Cancel' buttons.

| Vendor-assigned attribute number | Attribute format | Attribute value |
|----------------------------------|------------------|-----------------|
| 1 | Decimal | 2 |
| 2 | String | IEC62351-8 |
| 3 | String | * |
| 4 | Decimal | 0 |
| 6 | String | 99991231235959Z |

Combined roles include more than one Windows groups.

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

Note: Combined roles have to be placed at the beginning. Windows handles the policy rules like a firewall.

Radius Engineer Operator Policy Properties

Overview
Conditions
Constraints
Settings

Configure the conditions for this network policy.

If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.

| Condition | Value |
|----------------|----------------------|
| Windows Groups | CERTMAN\IEC OPERATOR |
| Windows Groups | CERTMAN\IEC ENGINEER |

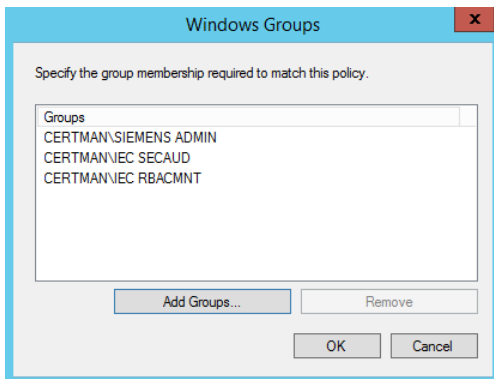
Note: You can add more roles to one policy but all other values have to be unique. Use another ID instead within the Policy for combined roles. The following example shows a combined role for SIEMENS ADMIN, SECAUD, RBACMNT. You have to use the shown "Vendor assigned attribute number" (x) to create a policy called "Radius Siemens Admin IEC SECAUD RBACMNT"

- (1) IEC62351-8-roleID-0=31648,
- (2) IEC62351-8-roleDefinition-0="SiemensGridSecurity"
- (3) IEC62351-8-aor-0="*",
- (4) IEC62351-8-revision-0=0,
- (6) IEC62351-8-ValidTo-0="99991231235959Z"
- (11) IEC62351-8-roleID-1+=5,
- (11) IEC62351-8-roleID-1+=6,
- (12) IEC62351-8-roleDefinition-1="IEC62351-8
- (13) IEC62351-8-aor-1="*",
- (14) IEC62351-8-revision-1=0,

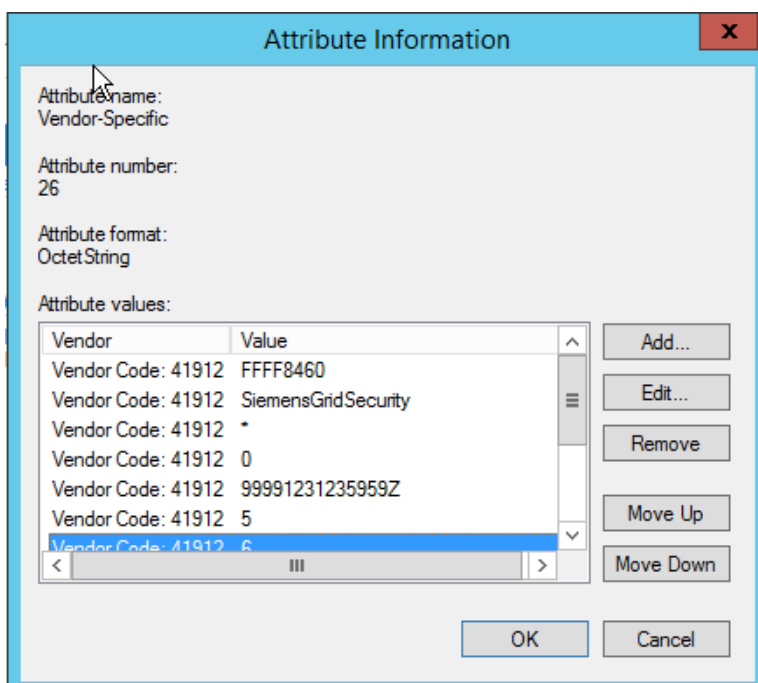
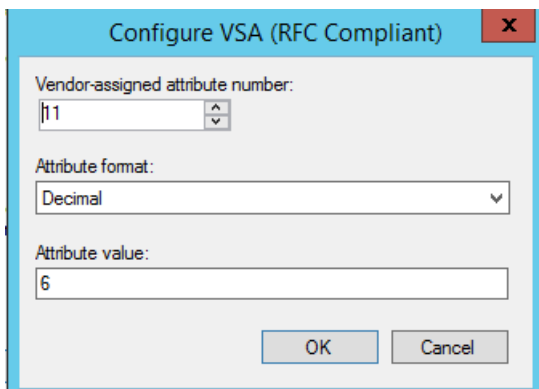
Cyber Security

Configuration of a Windows Active Directory and NPS

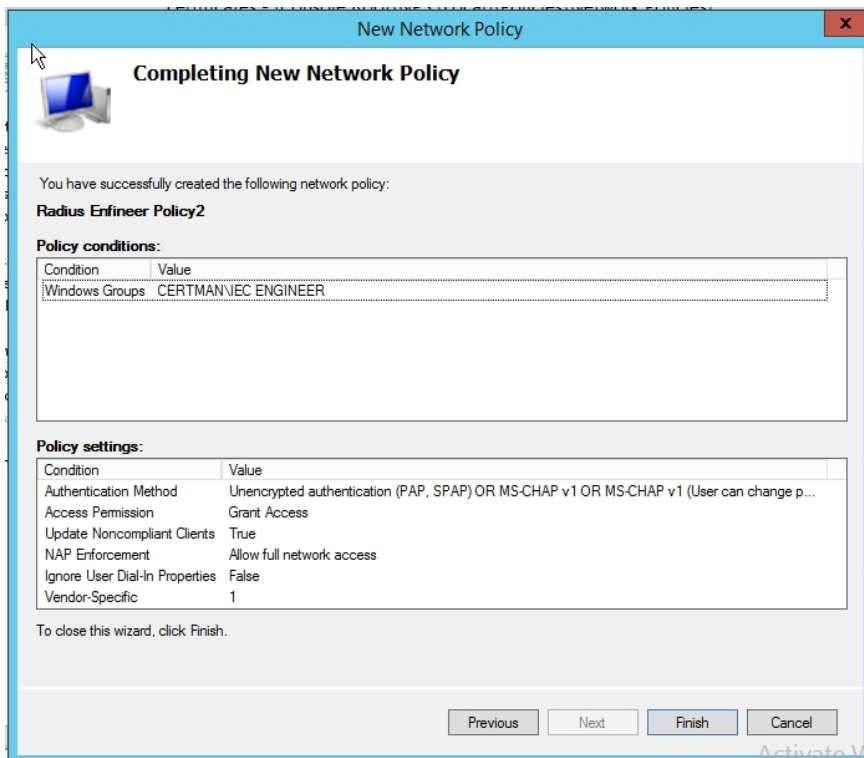
(16) IEC62351-8-ValidTo-1="99991231235959Z"



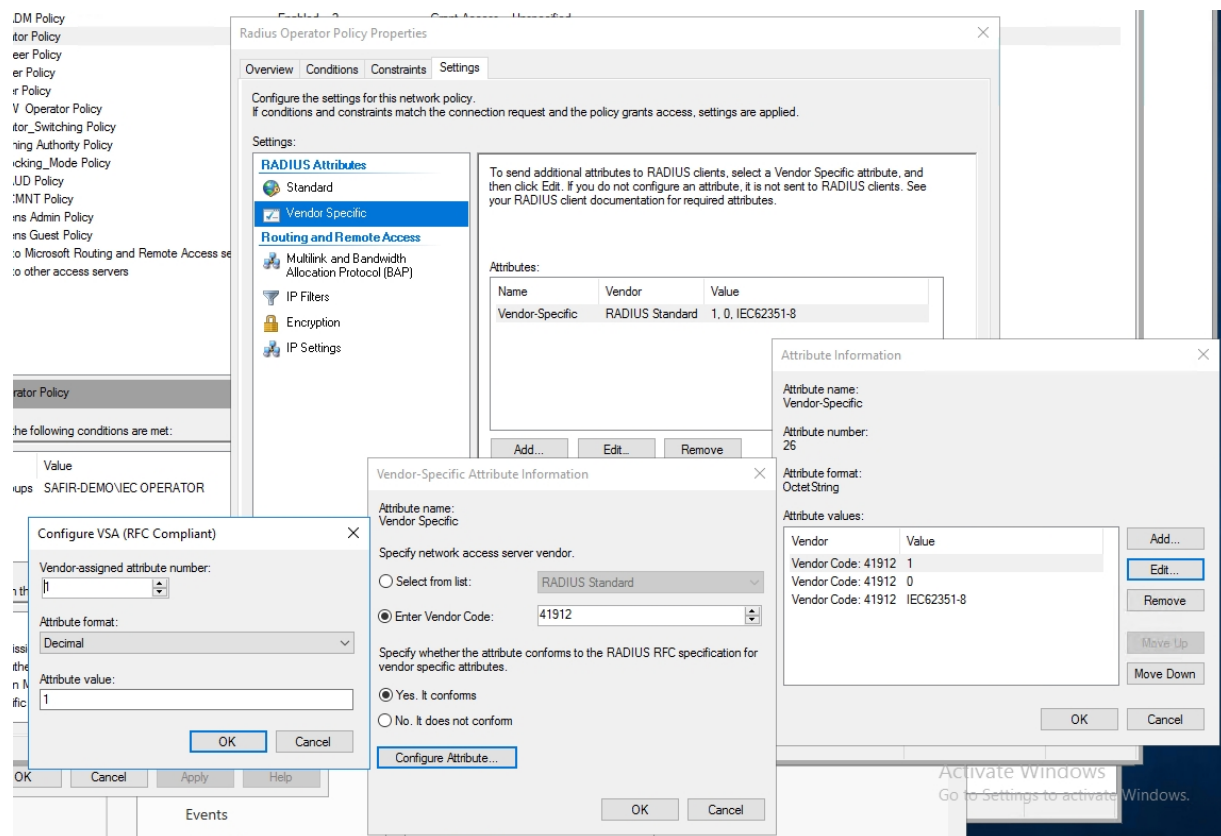
For example Vendor assigned attribute number = (11) for roleID=6 (RBACMNT)



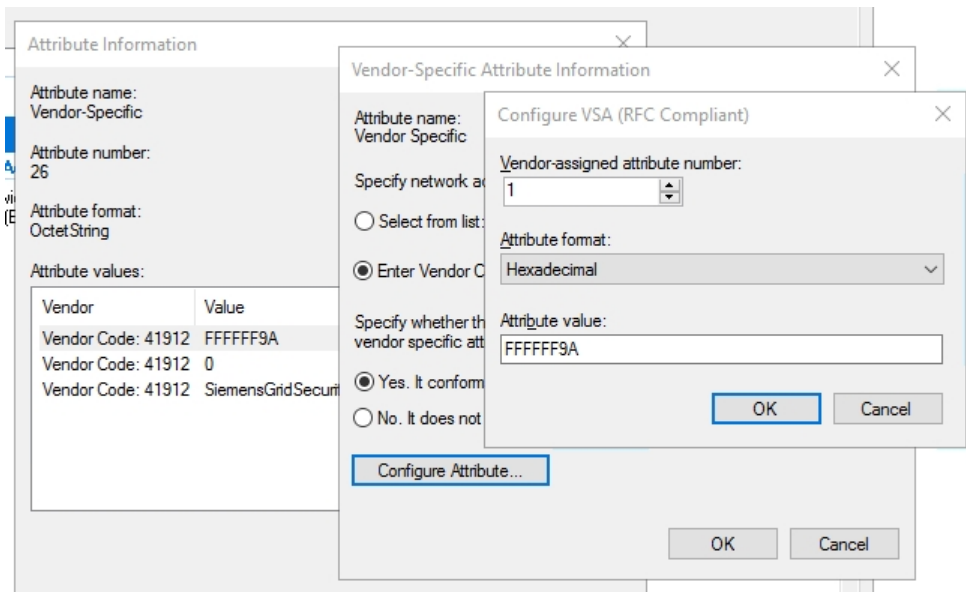
Finish the wizard



4. Add or adjust vendor specific attributes if necessary:



Note: For negative values add in hexadecimal values!



1.6 IEC 62351 Appendix

1.6.1 IEC 62351-8 Dictionary

Below is the IEC 62351 vendor specific dictionary subject to approval by the responsible IEC TC 57/WG 15! Adjusted and enclosed in the RADIUS server configuration, a RBAC token that is transmitted as part of the vendor specific attribute (VSA) – see <https://tools.ietf.org/html/rfc2865#page-47>) contains the following set of information:

| Attribute Name | Attribute Value | Required |
|-----------------------------|-----------------|-----------|
| IEC62351-8-RoleID-i | (i*10)+1 | mandatory |
| IEC62351-8-roleDefinition-i | (i*10)+2 | optional |
| IEC62351-8-aor-i | (i*10)+3 | mandatory |
| IEC62351-8-revision-i | (i*10)+4 | mandatory |
| IEC62351-8-ValidFrom-i | (i*10)+5 | optional |
| IEC62351-8-ValidTo-i | (i*10)+6 | mandatory |

Note: integer i=0..N

This approach resembles the sequences described for the X.509 digital certificate extension in profile A and B of the IEC62351-8 standard.

Note that the roleID is always related to the same IEC62351-8-aor, IEC62351-8-roleDefinition (if the field is provided), IEC62351-8-revision, and IEC62351-8-ValidTo field. To support also different roles with either the same or different Area of Responsibility (AoR) associations, multiple instances may be supported according to RFC 2865.

To enable the RADIUS server to process the VSA with the RBAC information, a dictionary file is necessary. The following example shows a dictionary file for the case i=2, providing a distinction between three sets of RBAC information:

```
VENDORInternational Electrotechnical Commission          41912
BEGIN-VENDORInternational Electrotechnical Commission

  ATTRIBUTE IEC62351-8-RoleID-0          1          integer
  ATTRIBUTE IEC62351-8-roleDefinition-0  2          string OPTIONAL
  ATTRIBUTE IEC62351-8-aor-0             3          string
  ATTRIBUTE IEC62351-8-revision-0        4          integer
  ATTRIBUTE IEC62351-8-ValidFrom-0       5          string OPTIONAL
  ATTRIBUTE IEC62351-8-ValidTo-0         6          string

  ATTRIBUTE IEC62351-8-RoleID-1          11         integer
```

| | | | | |
|-----------|-----------------------------|----|---------|----------|
| ATTRIBUTE | IEC62351-8-roleDefinition-1 | 12 | string | OPTIONAL |
| ATTRIBUTE | IEC62351-8-aor-1 | 13 | string | |
| ATTRIBUTE | IEC62351-8-revision-1 | 14 | integer | |
| ATTRIBUTE | IEC62351-8-ValidFrom-1 | 15 | string | OPTIONAL |
| ATTRIBUTE | IEC62351-8-ValidTo-1 | 16 | string | |
| ATTRIBUTE | IEC62351-8-RoleID-2 | 21 | integer | |
| ATTRIBUTE | IEC62351-8-roleDefinition-2 | 22 | string | OPTIONAL |
| ATTRIBUTE | IEC62351-8-aor-2 | 23 | string | |
| ATTRIBUTE | IEC62351-8-revision-2 | 24 | integer | |
| ATTRIBUTE | IEC62351-8-ValidFrom-2 | 25 | string | OPTIONAL |
| ATTRIBUTE | IEC62351-8-ValidTo-2 | 26 | string | |

END-VENDOR International Electrotechnical Commission

1.6.2 IEC 2351-8 defined roles

A role is explicit defined by the set of a *roleID*, a *revision* and a *roleDefinition* and is defined in the IEC62351-8 standard. In general a role is a set of permissions. In case of the permission assignment is changed for an existing role (*roleID*) than the revision has to be increased. All IEC62351 roles are based on the IEC62351-8 standard. Therefore the *roleDefinition* is IEC62351-8. Any other defined roles, for example customer-defined roles or manufacturer defined roles in the future, have own defined role Definitions because the role name (*roleID*) could be the same. More information can be found in the standard.

| Role | roleID | revision | roleDefinition | used for |
|-----------|--------|----------|----------------|------------------------------------|
| VIEWER | 0 | 0 | IEC62351-8 | SICAM A8000/SIPROTEC 5 |
| OPERATOR | 1 | 0 | IEC62351-8 | SICAM A8000/SIPROTEC 5 |
| ENGINEER | 2 | 0 | IEC62351-8 | SICAM A8000/SIPROTEC 5 |
| INSTALLER | 3 | 0 | IEC62351-8 | SICAM A8000/SIPROTEC 5 |
| SECADM | 4 | 0 | IEC62351-8 | SICAM A8000/SIPROTEC5/ GridPass |
| SECAUD | 5 | 0 | IEC62351-8 | SICAM A8000/SIPROTEC 5 |
| RBACMNT | 6 | 0 | IEC62351-8 | SICAM A8000/SIPROTEC5/ GridPass |

Besides these IEC62351-8 defined roles, other roles can be defined within the numbers range <-32768 .. -1>. They are reserved for private usage. In case of using the IEC62351 roles the declaration of the *roleDefinition* is optional, for private usage the *roleDefinition* is mandatory

1.6.3 IEC 62351-8 Definition (Extract from the IEC 62351-8 Edition 1)

1.6.3.1 Role ID (9.4.4.1)

The role is defined using a mapping to an integer space, whereby the numbers:

- <0 .. 32767> are reserved for application within IEC 62351;
- <-32768 .. -1> are reserved for private usage, e.g. by other protocols like IEEE 1815

All roles to be used in the context of IEC protocols shall be defined as part of IEC/TS 62351-8. The current definition of roles comprises IEC 61850 specific roles.

Format: INTEGER (-32767 .. 32767)

1.6.3.2 Role definition (9.4.4.2)

To allow for uniqueness of roles in terms of an unique role-to-right mapping, a further parameter is used to provide information about the used data model. This parameter (*roleDefinition*) is optional and to be treated as "IEC 62351-8" per default for positive role IDs. In case of the private usage numbers (negative numbers), it reflects the associated role definition standard. An own role definition may be provided by other standards (other than IEC/TS 62351-

8, by an utility operator. The `roleDefinition` is valid in the context of the defined `UserRoleInfo` (access token). If multiple role definitions are used, multiple access tokens shall be used to ensure a unique role-top-right mapping.

If the `roleDefinition` field is present the relying party shall use the mapping defined by that field.

The replying party shall reject any role ID that has a `roleDefinition` associated value that it does not recognize.

Format: `UTF8String (0 .. 23)`

1.6.3.3 Revision number (9.4.4.8)

The revision number is a monotonically increasing integer number and represents the version of the subject-to-role mapping.

1.7 Siemens Appendix

1.7.1 Defined roles by Siemens

Siemens has defined own roles with own assigned permissions. Not all roles are necessary and available in all Siemens Energy Management Digital Grid products. Which explicit permissions are assigned inside the device depends on the functionality of the device and will be found in the product manual.

| Role | roleID hexadecimal | roleID decimal | revision | roleDefinition | used for |
|---------------------|-----------------------|-------------------|----------|---------------------|----------------------------|
| ADMIN | FFFF8460 | -31648 | 0 | SiemensGridSecurity | SICAM A8000/ SIPROTEC 5 |
| GUEST | FFFFAFC7 | -20537 | 0 | SiemensGridSecurity | SIPROTEC 5 |
| Operator_Switching | FFFFFF9A | -102 | 0 | SiemensGridSecurity | SIPROTEC 5 |
| Switching_Authority | FFFFFF99 | -103 | 0 | SiemensGridSecurity | SIPROTEC 5 |
| Interlocking_Mode | FFFFFF98 | -104 | 0 | SiemensGridSecurity | SIPROTEC 5 |

1.7.2 Limitations of roles to user assignment and other limitations

1.7.2.1 SIPROTEC 5

SIPROTEC 5 is supporting all IEC62351-8 roles and the SIEMENS role ADMIN; GUEST, Operator_Switching, Switching Authority; Interlocking_Mode. All IEC62351-8 attributes are supported:

| Attribute Name | Attribute Value | Required |
|-----------------------------|-----------------|-----------|
| IEC62351-8-RoleID-i | (i*10)+1 | mandatory |
| IEC62351-8-roleDefinition-i | (i*10)+2 | optional |
| IEC62351-8-aor-i | (i*10)+3 | mandatory |
| IEC62351-8-revision-i | (i*10)+4 | mandatory |
| IEC62351-8-ValidFrom-i | (i*10)+5 | optional |
| IEC62351-8-ValidTo-i | (i*10)+6 | mandatory |

According the RADIUS RFC you can assign more than one `roleID` to one user if needed.

- Max. i=24 is per user supported
- Max. 32 roles per user
- According the IEC62351-8 definition only the `roleID` can be used multiple times for one "i"
- AoR is mandatory but will be not analyzed at the moment
- Revision has to be always "0"
- The `roleDefinition` is optional in case of "IEC62351-8" and mandatory in case of all other `roleDefinitions` according the IEC62351-8 standard
- In case of different `validTo` values for one user for different token the earliest day will be used

- In case of one invalid or doubled token entry the complete token will be discarded
- The minimum length of the shared secret has to be 16 characters, the maximum length is 100
- NAS identifier is SIPROTEC510

1.7.2.2 SICAM GridPass

SICAM GridPass supports the IEC 62351-8 roles SECADM and RBACMNT. So far, only the following attributes are supported:

| | | | |
|-----------|-----------------------------|---|-----------------|
| ATTRIBUTE | IEC62351-8-RoleID-0 | 1 | integer |
| ATTRIBUTE | IEC62351-8-roleDefinition-0 | 2 | string OPTIONAL |
| ATTRIBUTE | IEC62351-8-revision-0 | 4 | integer |

In this case only the OID 1,2 and 4 will be analyzed in the RADIUS server accept response. All other values will be discarded. According the RADIUS RFC you can assign more than one roleID to one user if needed.

- According the IEC62351-8 definition only the roleID can be used multiple times for one “i”
- The roleDefinition is optional in case of “IEC62351-8” and mandatory in case of all other roleDefinitions according the IEC62351-8 standard
- AoR is mandatory but will be not analyzed at the moment

1.7.2.3 SICAM A8000 CP-8000, CP-802x and 8050

SICAM A8000 CP8050 V2.0, SICAM A8000 CP802x V14 and SICAM A8000 CP8000 V14 are supporting all IEC62351-8 roles and the SIEMENS role ADMIN. All IEC62351-8 attributes are supported:

| Attribute Name | Attribute Value | Required |
|-----------------------------|-----------------|-----------|
| IEC62351-8-RoleID-i | (i*10)+1 | mandatory |
| IEC62351-8-roleDefinition-i | (i*10)+2 | optional |
| IEC62351-8-aor-i | (i*10)+3 | mandatory |
| IEC62351-8-revision-i | (i*10)+4 | mandatory |
| IEC62351-8-ValidFrom-i | (i*10)+5 | optional |
| IEC62351-8-ValidTo-i | (i*10)+6 | optional |

Due to compatibility reasons the *ValidTo* Attribute is optional.

According the RADIUS RFC you can assign more than one roleID to one user if needed.

- According the IEC62351-8 definition only the roleID can be used multiple times for one “i”
- The roleDefinition is optional in case of “IEC62351-8” and mandatory in case of all other roleDefinitions according the IEC62351-8 standard
- NAS identifier is the MAC address

1.7.3 Microsoft Links

Import NPS:

<https://docs.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-manage-export>

or

[https://technet.microsoft.com/de-de/library/cc753571\(v=ws.10\).aspx](https://technet.microsoft.com/de-de/library/cc753571(v=ws.10).aspx)

1.8 Summary

Secure products in energy automation are the basis for a secure system for energy automation. Role-based access control with central management is one of the benefits of SIPROTEC and SICAM beside other features for security like security logging, digital signed FW/SW, asset monitoring and secured communication.

Access Control in SIPROTEC 5

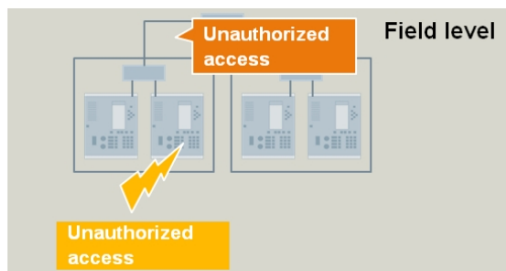
Deny **unauthorized Access** with RBAC and User Management

SIEMENS

Ingenuity for Life

Risks with protection relays without secured access control:

- Without password control it is easily possible to access the relays anonymously
- Unencrypted / weakly encrypted password handling enables "sniffing"
- Simple passwords and eternally valid passwords acquire "feet" over time



Role-Based Access Control in SIPROTEC 5

- Authorize users to perform operations based on their role – new RBAC option with centralized user management support based on RADIUS
- Transfer of credentials from DIGSI5 to device over secured SSL/TLS connection
- Secured storage of sensitive information (e.g. passwords, keys) in device
- Confirmation codes for safety-critical operations and connection password support for non-RBAC usage
- Security event logging of access attempts in device – optionally also transmitted over Syslog UDP to a central Syslog server





Published by
Siemens AG 2018
Energy Management Division
Digital Grid
Automation Products
Humboldtstr. 59
90459 Nuremberg, Germany

www.siemens.com/siprotec

For more information,
please contact our
Customer Support Center.

Tel.: +49 180 524 70 00
Fax: +49 180 524 24 71
(Charges depending on provider)

Email: support.energy@siemens.com

© 2016 Siemens. 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.

For all products using security features of OpenSSL, the
following shall apply:
This product includes software developed by the OpenSSL
Project for use in the OpenSSL Toolkit.
(<http://www.openssl.org/>)
This product includes cryptographic software written by
Eric Young (eay@cryptsoft.com)
This product includes software written by Tim Hudson
(tjh@cryptsoft.com)
This product includes software developed by Bodo Moeller.