



IEEE 802.1x Configuration Management

Administration Manual

A31003-J4200-M100-15-76A9

Our Quality and Environmental Management Systems are implemented according to the requirements of the ISO9001 and ISO14001 standards and are certified by an external certification company.

Contents

802.1X Authentication for IP Telephones 6

Introduction	6
What is 802.1X?	6
Why is 802.1X important?	6
Who needs 802.1X?	6
IEEE 802.1X Authentication of Telephones	6
Setting up and Using IEEE 802.1X	9
Connection overview	9
IEEE 802.1X security – how it works	10
Overview of EAP-TLS	11
Required environment	12
Released features	12
Additional documentation	12

Installing the RADIUS Server. 14

Installation Overview	14
Linux solution under openSuSE	14
Microsoft Windows Server	14
XCertificate and Key management with Windows	14
Certificate administration in DLS	14
Flow Chart for Introduction of IEEE 802.1X	15
Installation under openSuSE	17
Installing OpenSSL	17
Installing the FreeRADIUS server	17
Installing TinyCA2	17
Creating certificates	17
Certificate requirements	17
Rules for logon names	18
Create root certificate with TinyCA2	19
Create server certificate with TinyCA2	21
Create client certificate with TinyCA2	23
Export certificates	24
Configure and start FreeRADIUS server for EAP-TLS	25
Certificates for OpenStage, OpenScape Desk Phones and optiPoint phones	26
Certificate formats	28
Simple certificate (client certificate) in text format	29
Microsoft solution with Windows Server 2008/2012	31
Creating certificates with XCertificate and Key management	32
First Start	32
XCA configuration	32
Create Templates for repeating tasks	33
Create a new Certificate Authority (Root CA Certificate)	36
Create a new Sub-Certificate Authority	39
Create a new Server Certificate	42
Create a new Client Certificate	45
Create a Certificate Signing Request	48
Import Certificates into the database	51
Import random certificates into XCA	51
Import Root CA certificate and private key from OpenScape Voice	53
Export Certificates from the database for 802.1x	54
Export Certificates for Web Based Management	56

Managing Certificates in the DLS	57
Plug & Play – template.	57
Plug & Play with IEEE 802.1X	58
Overview	58
Test Environment	58
Configure Phone for DHCP	58
Configuring Plug & Play in DLS	59
Plug & Play – creating profiles	59
DHCP Address Pool (Scope)	59
Switch Configuration using Example of Cisco Catalyst 3560	60
Limitations	60
Configuration	61
Cisco configuration (port used fa0/12)	61
Plug & Play Function	64
Plug & Play function with VLAN transmission via DLS	64
Phones and PC interoperability	64
Example: Phone has certificate but PC has no certificate	64
Location or Network Change.	66
Examples of Switch Configurations.	68
Switch example 1: "Cisco configuration"	68
Switch example 2: "Enterasys Matrix N1 Platinum Configuration".	70
Switch example 3: "ProCurve configuration"	74
PEAP Implementation	75
802.1x Network Access Protection overview	75
Example Configuration Overview (LAB environment)	76
Configuration.	77
Add the Radius-Server to the Domain	77
Join the RADIUS-Server to the Domain	77
Create a user account in Active Directory	78
Add user1 to the Domain Admins group.	79
Set up an enterprise root CA	79
Install an enterprise root CA	80
Create a security group	81
Configure Network Policy Server on Radius-Server.	82
Group Policy Management	83
Certificate on NPS Radius Server	84
Configure NAP on the NPS Server	86
Select Network Connection Method	86
Switch Properties	87
Configure an Authentication Method	88
Configure Traffic Controls.	89
Configure Radius Attributes: Tunnel-Type	90
Configure Attribute Information: Tunnel-Type	91
Configure RADIUS Attributes: Tunnel-Medium-Type	92
Configure Attribute Information: Tunnel-Medium-Type	92
Configure RADIUS Attributes: Tunnel-Pvt-Group-ID	93
Configure Attribute Information: Tunnel-Pvt-Group-ID	94
Vendor-Specific Attributes	95
Set Attribute Information: Cisco AV Pair.	96
Configure VLAN properties for noncompliant phones	96
Verify NAP Policies.	97

Configure Policies on the NPS	98
Configure Network Policy: New Network Policy	98
Configure Network Policy: Select Condition	99
Configure Network Policy: Windows Groups	99
Configure Network Policy: Select Group	100
Configure Network Policy: Select Condition	100
Configure Network Policy: NAS Port Type	101
Configure Network Policy: Specify Conditions	102
Specify Access Permissions	103
Configure Authentication Methods	104
Configure Settings	106
Add Vendor Specific Attribute	107
Configure Settings	109
Completing Network Policy	110
Configure 802.1X on DLS	111
802.1x Settings on DSL	112
Import RADIUS Server CA Certificate	113
Activate RADIUS Server CA Certificate	114
Verify RADIUS Server CA Certificate	115
Configure Cisco Switch	116
Verify the successful Logon	117
 Glossary	 118
 Abbreviations	 122
 Index	 123

802.1X Authentication for IP Telephones

Introduction

What is 802.1X?

- 802.1X is used to authenticate an → Entity (such as a PC or a phone) within the network.
- Authentication takes place on Layer 2 (OSI) and is based on the MAC address of the → Entity.
- An → Entity can be a server, PC, laptop, printer or IP phone.

Why is 802.1X important?

- It controls access to the network.
- Access can be controlled and restricted to certain resources by using a management system.
- Access by unauthorized devices/persons is made difficult.

Who needs 802.1X?

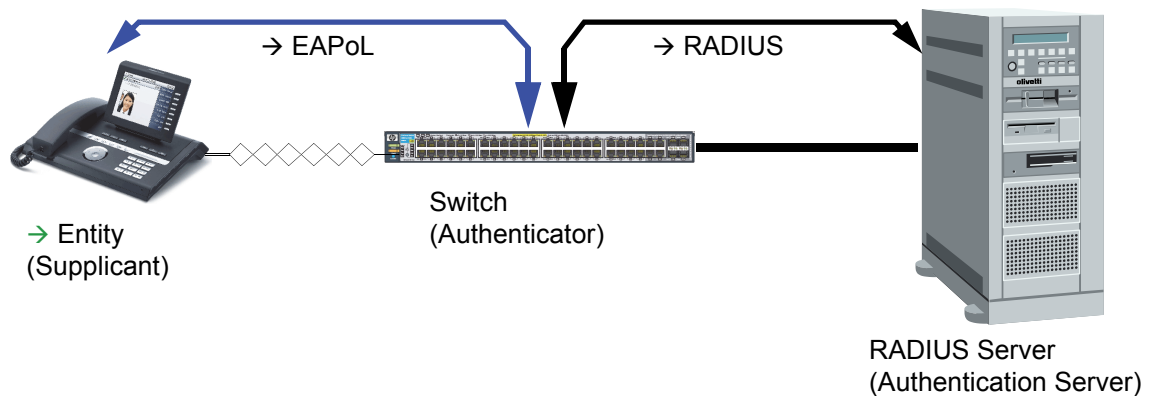
- All enterprises wishing to prevent unauthorized devices from accessing the company network.
- Economic aspects have to be taken into consideration:
 - ease of mobility within the network;
 - flexible office;
 - project teams that only cooperate for certain periods of time;
 - guest accounts in the network, business partners, for example;
- as well as administrative aspects:
 - assignment of network resources;
 - business management applications (SAP);
 - rules-based administration of groups.

IEEE 802.1X Authentication of Telephones

802.1X authentication is done using digital certificates and → EAP-TLS via a → RADIUS server.

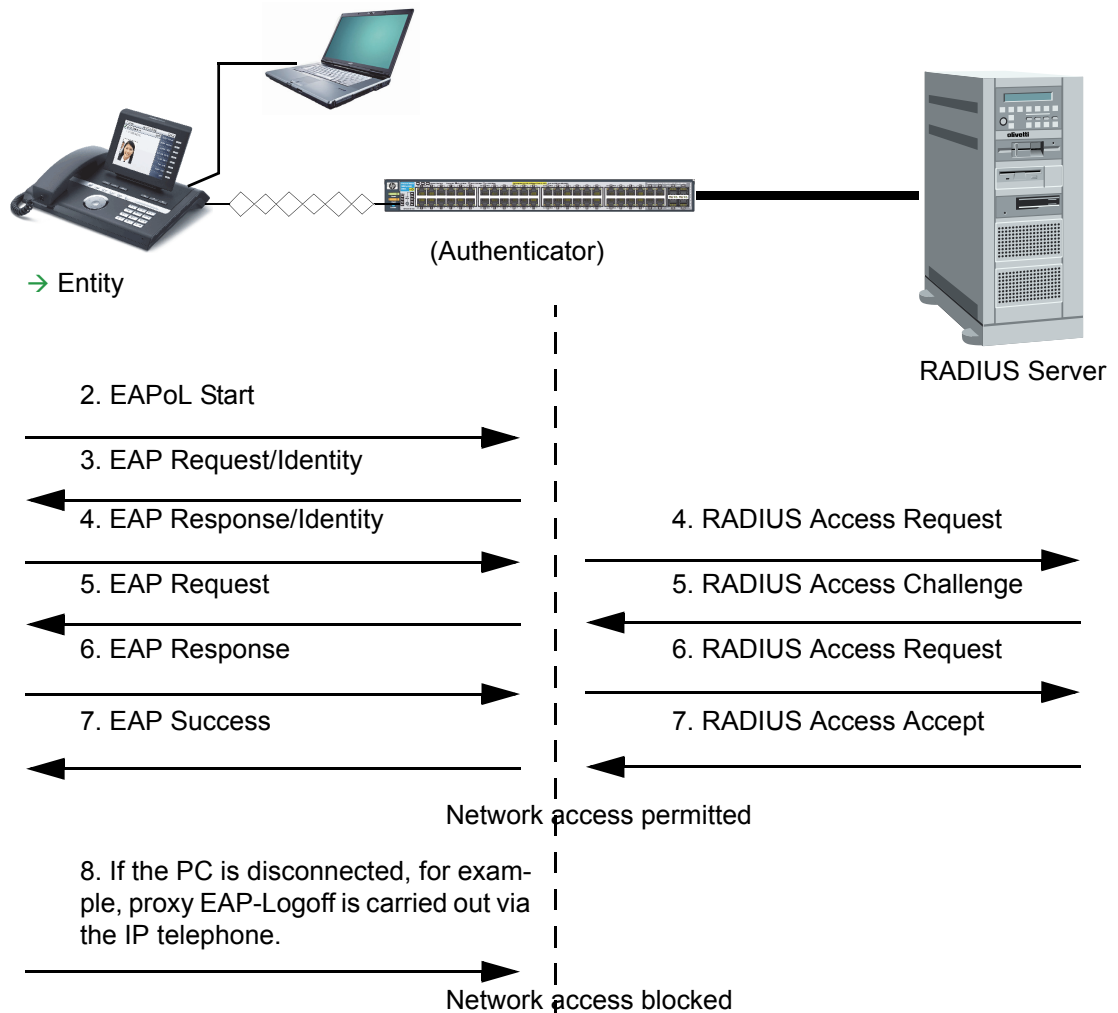
Initial State / Preparation / Deployment

- The switch only allows initial access to the telephone management tool (DLS) via a "guest" → VLAN with restricted access.
- The telephone only "sees" the DLS (the DLS provides the IP address) and is not registered at any proxy.
- The telephone is not yet logged on to the customer network.
- The DLS server downloads the certificates generated in the → CA (trust center) to the telephone (user certificate and server certificate).

802.1X Authentication Procedure

- The 802.1X authentication is triggered by a reboot of the telephone.
- The network switch sends an 802.1X request to the port to which the telephone and PC (if available) are connected.
- The telephone and/or PC respond to this request.
- Mutual authentication is performed by exchanging certificates (user certificate and → RADIUS certificate); both certificates are available for phone and → RADIUS server.
- The → Entity (the phone in this case) may only send one 802.1X request for network access; all other data packets from this → Entity are discarded (EAP protocol).
- The Layer 2 switch forwards the request to the RADIUS server.
- The → RADIUS server (Microsoft IAS, ACS from Cisco or FreeRADIUS server under Linux) compares the certificates using a database connected via Active Directory, for example.
- If the certificate comparison is successful, the RADIUS server sends a success message to the Layer 2 switch.
- The Layer 2 switch releases the switch port to which the authenticated devices are connected.
- This completes first-time authentication.
- Periodic re-authentication can be configured via the switch.

Procedure for a complete authentication using → EAPoL



1. The port to the user system is in unauthorized status, which means that network access is refused.
2. The → Entity begins the exchange with an EAPoL start message.
3. The "normal" EAP exchange begins when the authenticator sends an EAP request/identity packet.
4. The → Entity then responds with an EAP response/identity which is forwarded by the authenticator as a RADIUS access request.
5. The RADIUS server responds with a RADIUS access challenge packet, which is transmitted by the authenticator to the user system using a suitable protocol with all necessary data.
6. This then sends the data entered by the user back to the authenticator as an EAP response. The authenticator then packs and forwards the results data in the data field of a RADIUS access request.
7. The RADIUS server approves access with a RADIUS access accept, after which the authenticator sends an EAP success to the → Entity and sets the port to authorized status. The → Entity is authorized to use the network and can access the network.
8. If, for example, the PC is disconnected from the → Entity, it sends an EAPoL-Logoff to the authenticator, which in turn resets the port for the PC to unauthorized status to prevent connection of an unknown device.

➡ The user system does not necessarily have to send an EAPoL start message. The authenticator can send an EAP request/identity at any time to update the authentication data.

Setting up and Using IEEE 802.1X

Connection overview

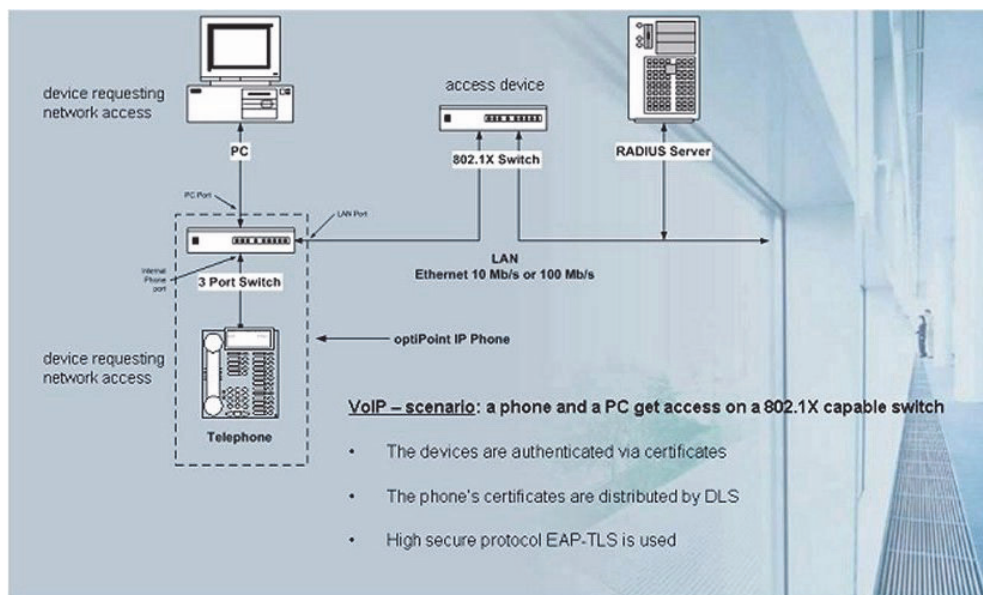
802.1X was first introduced for wireless LAN (WLAN) to secure access and protect data via an access point. The same standard is used to secure access to devices in a LAN via an access switch.

An IP phone uses the → EAPoL protocol or → EAP-TLS, which is a certificates-based form of authentication.

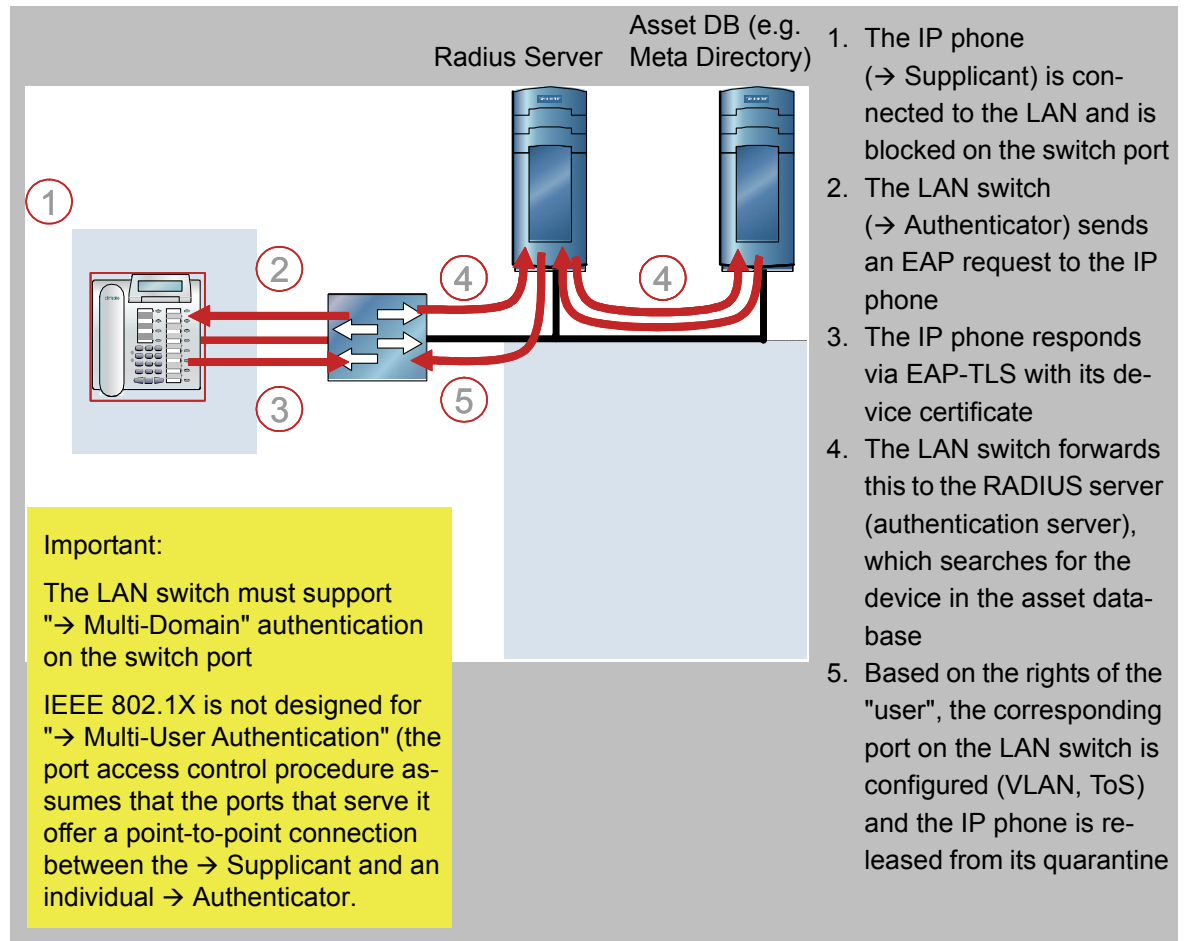
This certificates-based authentication (→ EAP-TLS) is much more secure than the other methods and meets the requirements of a device like a phone or a PC.

IEEE 802.1X

Security for IP networks – connectivity

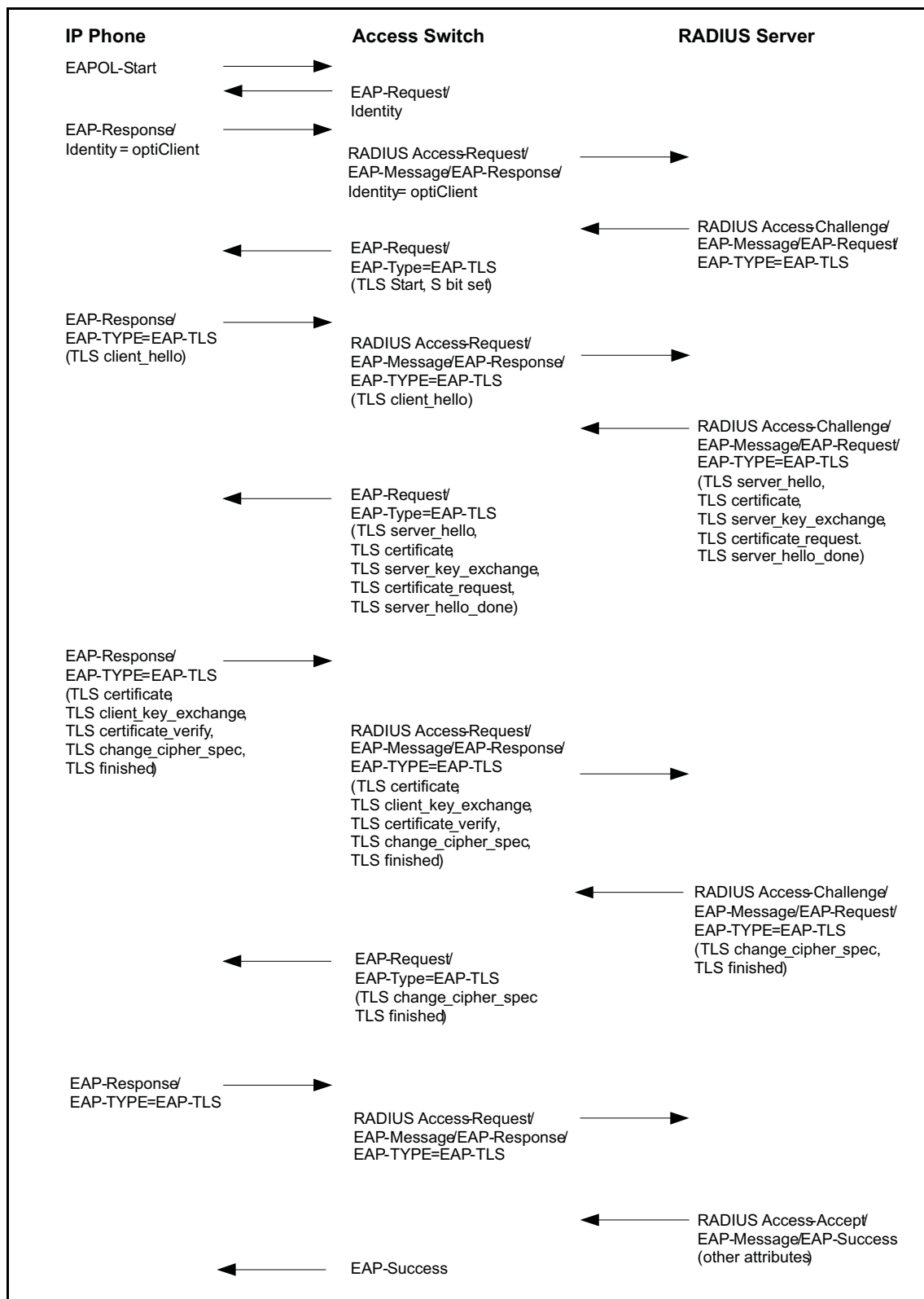


IEEE 802.1X security – how it works



Overview of EAP-TLS

The figure below shows the data flow between IEEE 802.1X components during EAP-TLS-based authentication.



Required environment

- IP phones
 - All versions of optiPoint HFA with firmware V5 R4.2.0 or later
 - All versions of optiPoint SIP V6 with firmware V6 R2.67.0 or later
 - All versions of optiPoint SIP V7 with firmware V7 R0.9.0 or later
 - The following versions apply if EAPoL-Logoff with 802.1X is not activated or there are no certificates on the phone:
 - All versions of optiPoint HFA with firmware V5 R4.6.0 or later
 - All versions of optiPoint V7 with firmware V7 R1.3.0 or later
 - OpenStage 20, 40 and OpenStage 60/80 from software release V1 R3.2.15 (FP 4.3) and V0 R7.10.138 (FP 4.4)
 - OpenScape Desk Phone IP 35/55G from software release V3 R2.0
- Access switch which supports 802.1X
 - Cisco Catalyst 3560
 - ProCurve Switch 3500yl (HP)
 - Enterasys Matrix N1 Platinum
 - Nortel
 - Huawei
 - among others
- → RADIUS server which supports EAP-TLS
 - MS IAS
 - Cisco RADIUS
 - Cisco ACS
 - FreeRADIUS
 - among others
- → Public Key Infrastructure (PKI) with a certificate service (Certificate Authority or CA) which can create certificates and distribute them to → RADIUS and the Deployment Server (DLS).
- The IP address of an NTP server has to be entered in the phone, and the constant availability of this IP address must be guaranteed.

Released features

OpenStage SIP and optiPoint 410/420 SIP/HFA have had the following features since 2008. They were released for OpenStage HFA in 2009:

- Support 802.1X (authentication method: EAP-TLS) with EAPoL-Logoff
- MAB – MAC Authentication Bypass
- MDA – Multi Domain Authentication (Cisco)
- MUA – Multi User Authentication (Enterasys)

Additional documentation

The following table lists some references you may find useful. The IEEE standard is fairly readable. The RFCs are also fairly clearly written.

[IEEE 802.1X standard document](#)

[IEEE_802.1X_on_wikipedia](#)

[EAP standard, RFC 2284](#)

[EAP TLS, RFC 2716](#)

[One-Time Password, RFC 1938](#)

[EAP: IETF draft search page](#)

[RADIUS, RFC 2865](#)

[RADIUS_on_wikipedia](#)

[RADIUS Accounting, RFC 2866](#)

[RADIUS Tunneling Attributes support, RFC 2867](#)

[RADIUS Tunneling Attributes support, RFC 2868](#)

[RADIUS Extensions, RFC 2869](#)

[RADIUS Support for EAP, RFC 3579](#)

[IEEE 802.1X Remote Authentication Dial In User Service \(RADIUS\), RFC 3580](#)

Installing the RADIUS Server

The following components are needed to introduce IEEE 802.1X:

- → RADIUS server as authentication server
(including a supplicant, such as a PC or telephone)
- Server root and client certificates

Installation Overview

The → RADIUS server can be installed as a Linux or Windows Server solution. A workstation with a Windows Server Enterprise version is used with the necessary administration tools for the Microsoft solution.

Refer to the → Flow Chart for Introduction of IEEE 802.1X for descriptions of the individual installation steps.

Linux solution under openSuSE

Perform the following steps:

- Installing OpenSSL (→ Seite 17)
- Installing the FreeRADIUS server (→ Seite 17)
- Installing TinyCA2 (→ Seite 17)
- Creating certificates (→ Seite 17)
- Configure and start FreeRADIUS server for EAP-TLS (→ Seite 25)

Microsoft Windows Server

Microsoft solution with Windows Server 2008/2012 (→ Seite 31)

XCertificate and Key management with Windows

Creating certificates with XCertificate and Key management (→ Seite 32)

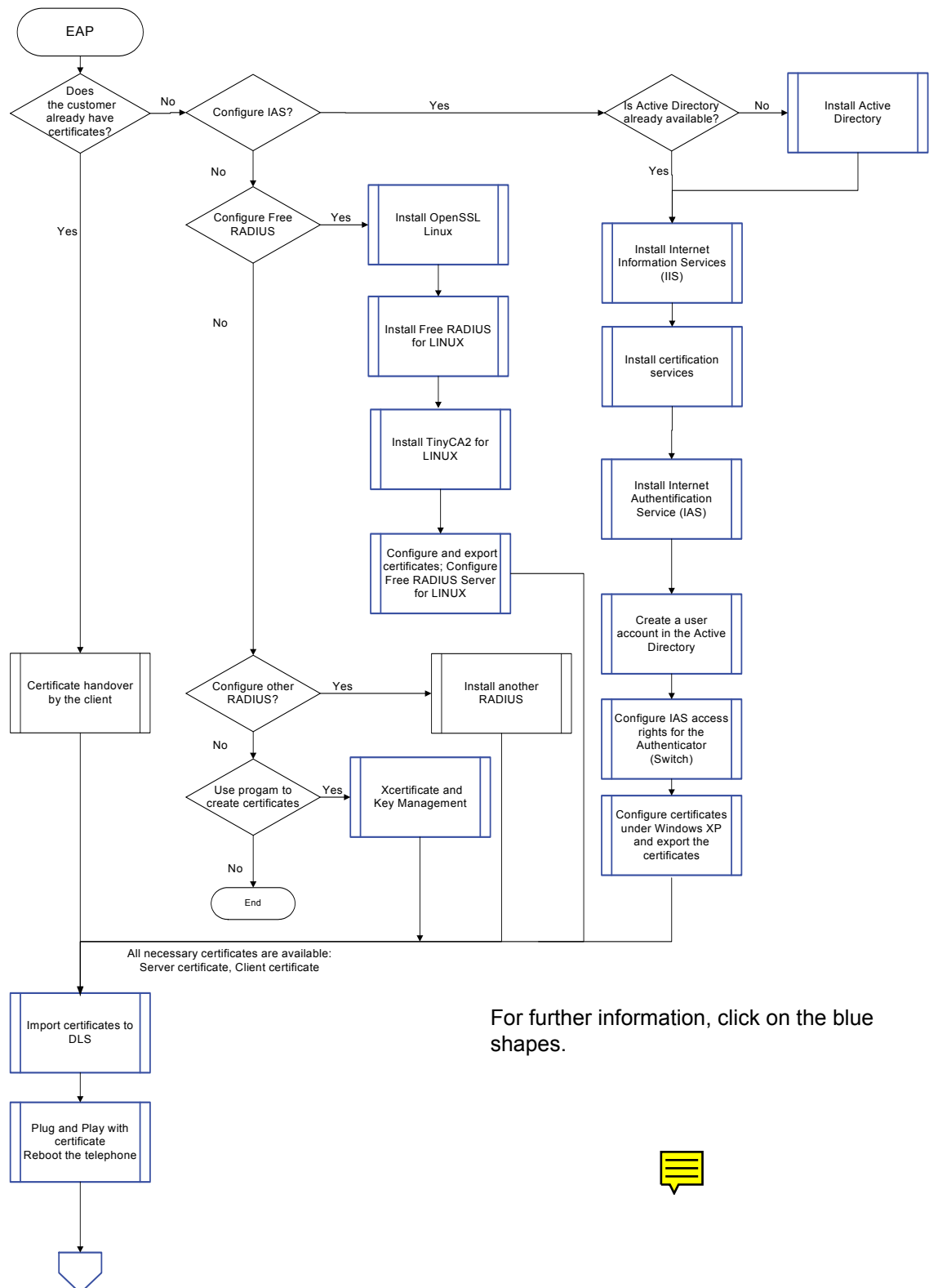
- First Start (→ Seite 32)
- Create a new Certificate Authority (Root CA Certificate) (→ Seite 36)
- Create a new Sub-Certificate Authority (→ Seite 39)
- Create a new Server Certificate (→ Seite 42)
- Create a new Client Certificate (→ Seite 45)
- Create a Certificate Signing Request (→ Seite 48)
- Import Certificates into the database (→ Seite 51)
- Import Root CA certificate and private key from OpenScape Voice (→ Seite 53)
- Export Certificates from the database for 802.1x (→ Seite 54)
- Export Certificates for Web Based Management (→ Seite 56)

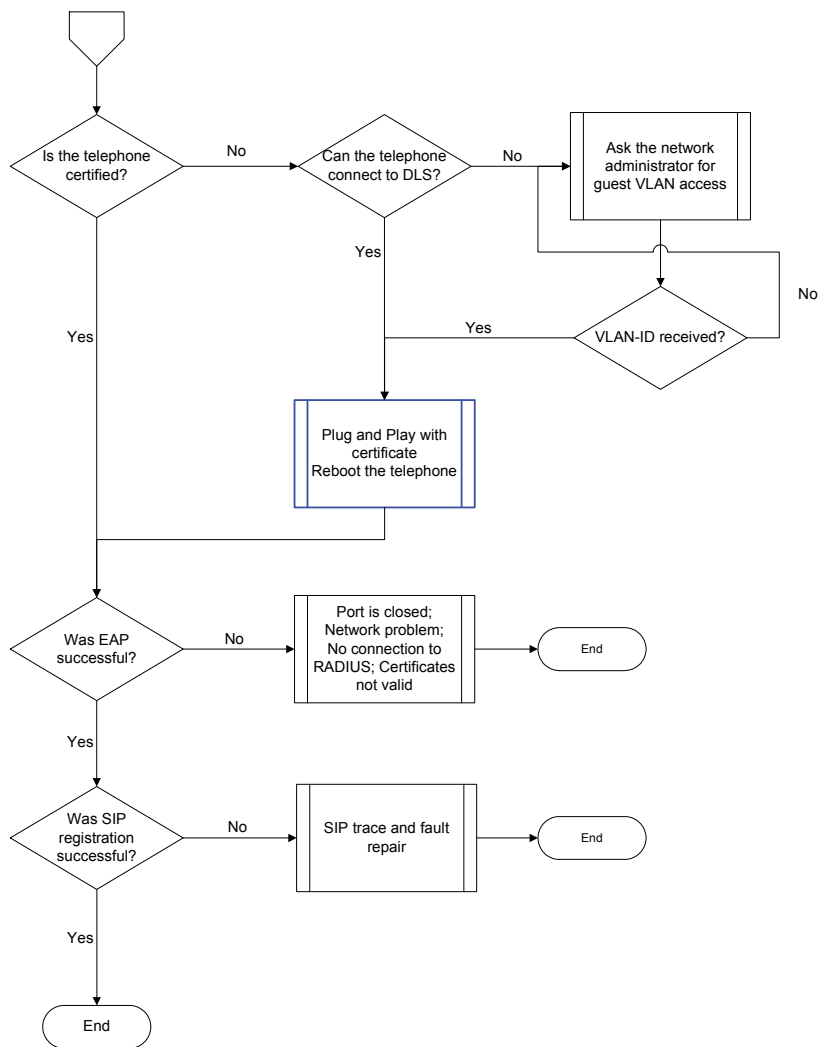
Certificate administration in DLS

- Plug & Play – template (→ Seite 57)

Flow Chart for Introduction of IEEE 802.1X

For further information, click on the blue shapes.





Installation under openSuSE

FreeRADIUS/Windows Authentication Setup

This section describes how to set up a FreeRADIUS server for TLS and PEAP authentication, and how to configure it for Windows clients (→ Supplicants). The server is configured for a home (or test) LAN.

Three papers have been written about TLS authentication with a FreeRADIUS server:

1. www.missl.cs.umd.edu/wireless/eaptls
2. www.freeradius.org/doc/EAPTLS.pdf
3. www.denobula.com

These papers provide an excellent background, but are somewhat out of date. We recommend that you follow the steps outlined below rather than the steps in these documents.

Installing OpenSSL


OpenSSL is usually already installed. If not, you can install the latest version using the YaST software management tool by entering "openssl" in the search field and then marking "openssl" and "openssl-certs".

Installing the FreeRADIUS server

You can install the latest version of the server using the YaST software management tool by entering "freeradius" in the search field and then marking "freeradius-server".

Installing TinyCA2

You can install the latest version of TinyCA2 using the YaST software management tool by entering "tinyca2" in the search field and then marking "tinyca2".

 TinyCA2 is intended for use in a test environment. More suitable tools are available for Enterprise applications. For advice, contact your switch vendor (example: Cisco Secure Access Control Server (ACS) Version 5.1).

The next step is to create the required certificates.

Creating certificates

When using → EAP-TLS, both the authentication server and all the → Supplicants (clients) need certificates[RFC2459].

If you are using EAP-TTLS or PEAP, only the authentication server requires certificates.
→ Supplicant Certificates are optional.

You get certificates from the → Certificate Authority (CA). If there is no → Certificate Authority available, OpenSSL may be used to generate self-signed certificates.

Certificate requirements

The following attributes need to be considered for certificate creation:

Phone certificate:

- X509v3 Extended Key Usage: TLS Web Client Authentication
- RSA Public Key: (1024 bit) with optiPoint, (2048) with OpenStage

RADIUS certificate:

- RSA Public Key: (2048 bit)
- X509v3 extensions:
 - X509v3 Key Usage: Critical, Digital Signature, Key Encipherment, Key Agreement, Certificate Sign
 - X509v3 Extended Key Usage: TLS Web Server Authentication, TLS Web Client Authentication

SubCA Certificate:

- RSA Public Key: (2048/4096 bit)
- X509v3 extensions:
 - X509v3 Basic Constraints: critical, CA:TRUE
 - X509v3 Key Usage: Critical, Digital Signature, Certificate Sign, CRL Sign

RootCA Certificate:

- RSA Public Key: (2048/4096 bit)
- X509v3 extensions:
 - X509v3 Basic Constraints: Critical, CA:TRUE
 - X509v3 Key Usage: Critical, Digital Signature, Certificate Sign, CRL Sign

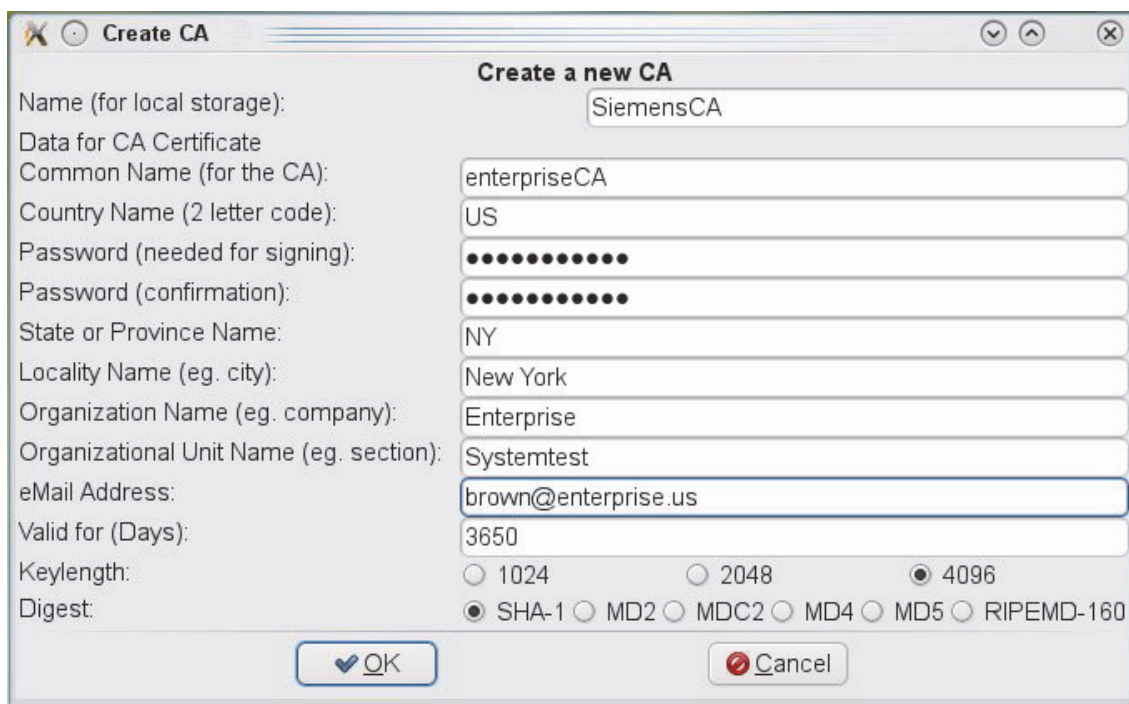
Rules for logon names

The certificate element "CommonName" must meet the requirements of Microsoft's "Rules for Logon Names" or UPN (User Principal Names) (see MS Windows Server, Internet Authentication Service (IAS) Operation Guide).

- Logon names must follow these rules:
 - Local logon names must be unique on a workstation, and global logon names must be unique throughout a domain.
 - Logon names can be up to 104 characters. However, it is not practical to use logon names that are longer than 64 characters.
 - A Microsoft Windows NT¹ logon name is given to all accounts, which by default is set to the first 20 characters of the Windows 2000 logon name. The Microsoft Windows NT¹ logon name must be unique throughout a domain.
 - Users logging on to the domain from Windows 2000 computers can use their Windows 2000 logon name or their Windows NT¹ logon name, regardless of the domain operations mode.
 - Logon names cannot contain the following characters: " / \ [] : ; | = , + * ? < >
 - Logon names can contain all other special characters, including spaces, periods, dashes and underscores. However, it is generally not a good idea to use spaces in account names.
- LAN-connected client computers: The following requirements must be met for the user and computer certificates installed on these computers:
 - They must have a corresponding private key.
 - They must contain the client authentication ECU (OID "1.3.6.1.5.5.7.3.2").
 - Computer certificates must be installed in the computer's local certificate store.
 - Computer certificates must contain the FQDN of the wired client computer in the "Subject Alternative Name" property.
 - User certificates must be installed in the current user certificate store.
 - User certificates must contain the User Principal Name (UPN) of the user account in the "Subject Alternative Name" property.

Create root certificate with TinyCA2

Access the TinyCA2 program. The **Create a new CA** dialog appears. The following screenshot shows a sample completed dialog:



The screenshot shows the 'Create a new CA' dialog box. The fields and their values are as follows:

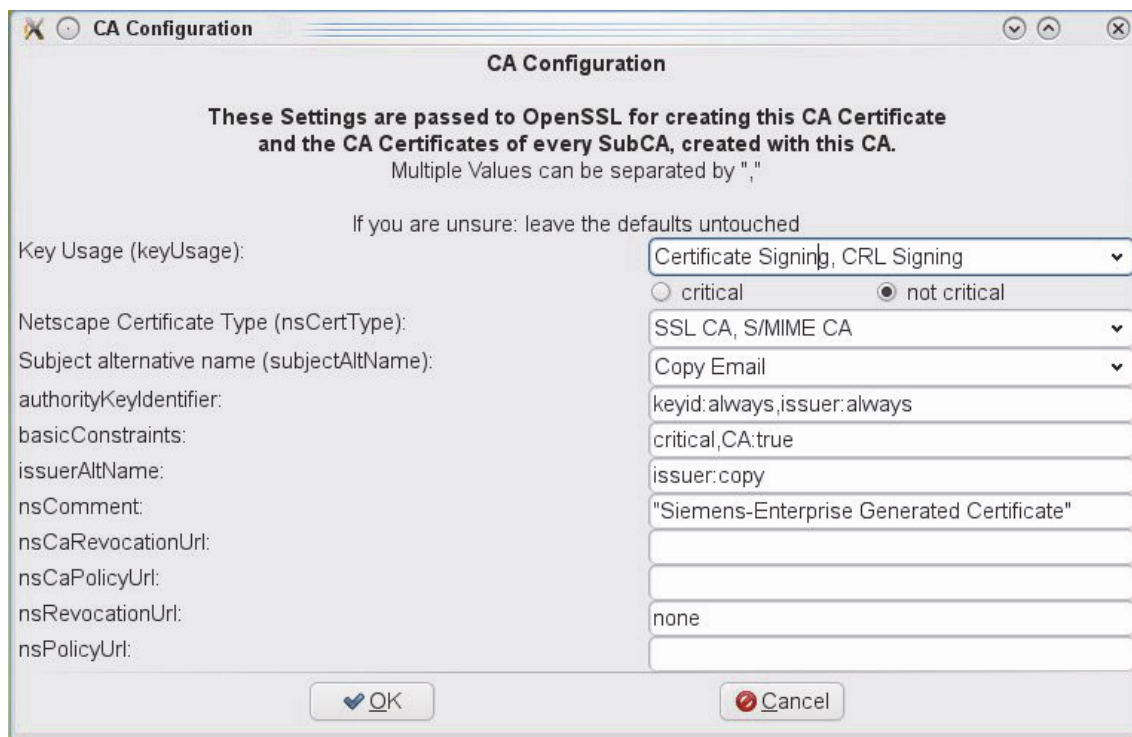
Field	Value
Name (for local storage):	SiemensCA
Common Name (for the CA):	enterpriseCA
Country Name (2 letter code):	US
Password (needed for signing):
Password (confirmation):
State or Province Name:	NY
Locality Name (eg. city):	New York
Organization Name (eg. company):	Enterprise
Organizational Unit Name (eg. section):	Systemtest
eMail Address:	brown@enterprise.us
Valid for (Days):	3650
Keylength:	<input type="radio"/> 1024 <input type="radio"/> 2048 <input checked="" type="radio"/> 4096
Digest:	<input checked="" type="radio"/> SHA-1 <input type="radio"/> MD2 <input type="radio"/> MDC2 <input type="radio"/> MD4 <input type="radio"/> MD5 <input type="radio"/> RIPEMD-160

Buttons: OK, Cancel

The following values were entered for illustration purposes:

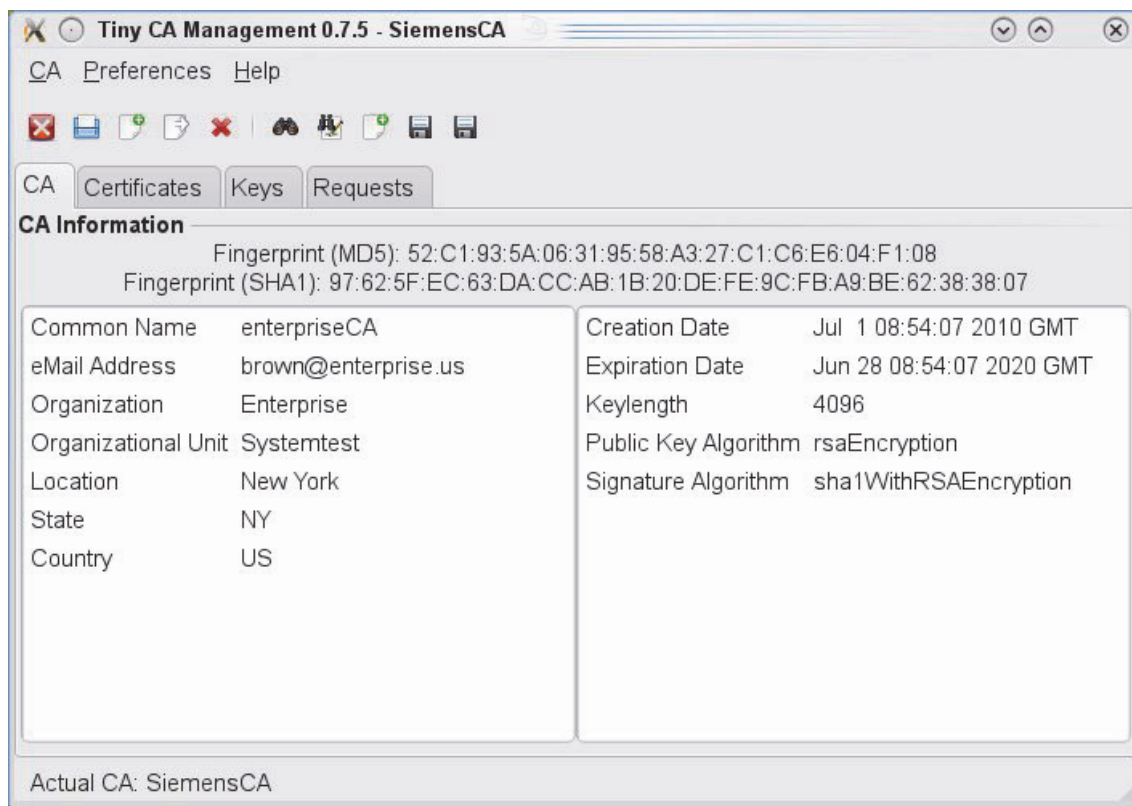
- **Name:** Directory name under which the root certificate will be stored on the hard disk. You will also find all certificates that were signed with this name in this directory.
- **Common Name:** The certificate's actual name.
- **Country Name:** Country code
- **Password:** Always needed for signing new certificates
- **State or Province Name:** Code used for state, such as NY for New York
- **Locality Name:** City or place name
- **Organization Name:** Name of company
- **Organizational Unit Name:** Section or department, for example
- **eMail Address:** Person to contact for certificates
- **Valid for:** Validity of certificate in days (should be the same as the example, if appropriate)
- **Keylength:** 4096 is the recommended value
- **Digest:** Hash function The option SHA-1 from the example can be used.

Confirm by clicking OK. The following dialog will then appear so you can verify the settings.



Modify the **nsComment** field if required and confirm by clicking **OK**.

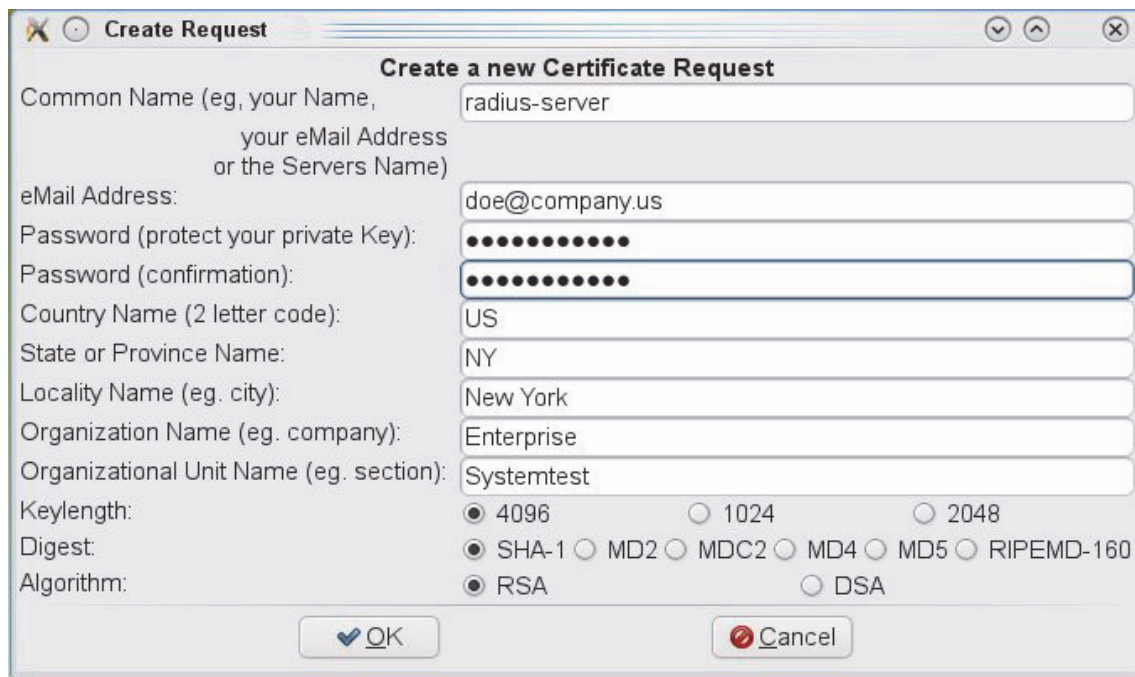
Confirm the next message with **OK**. The following list will appear:



All root certificates created to date are shown in the **CA** tab.

Create server certificate with TinyCA2

The FreeRADIUS server (client) certificate can now be created. First, go to the **Requests** tab. Right-click to access the context menu and click **New**. The following dialog is displayed:



The screenshot shows a 'Create Request' dialog box with the title 'Create a new Certificate Request'. It contains the following fields and options:

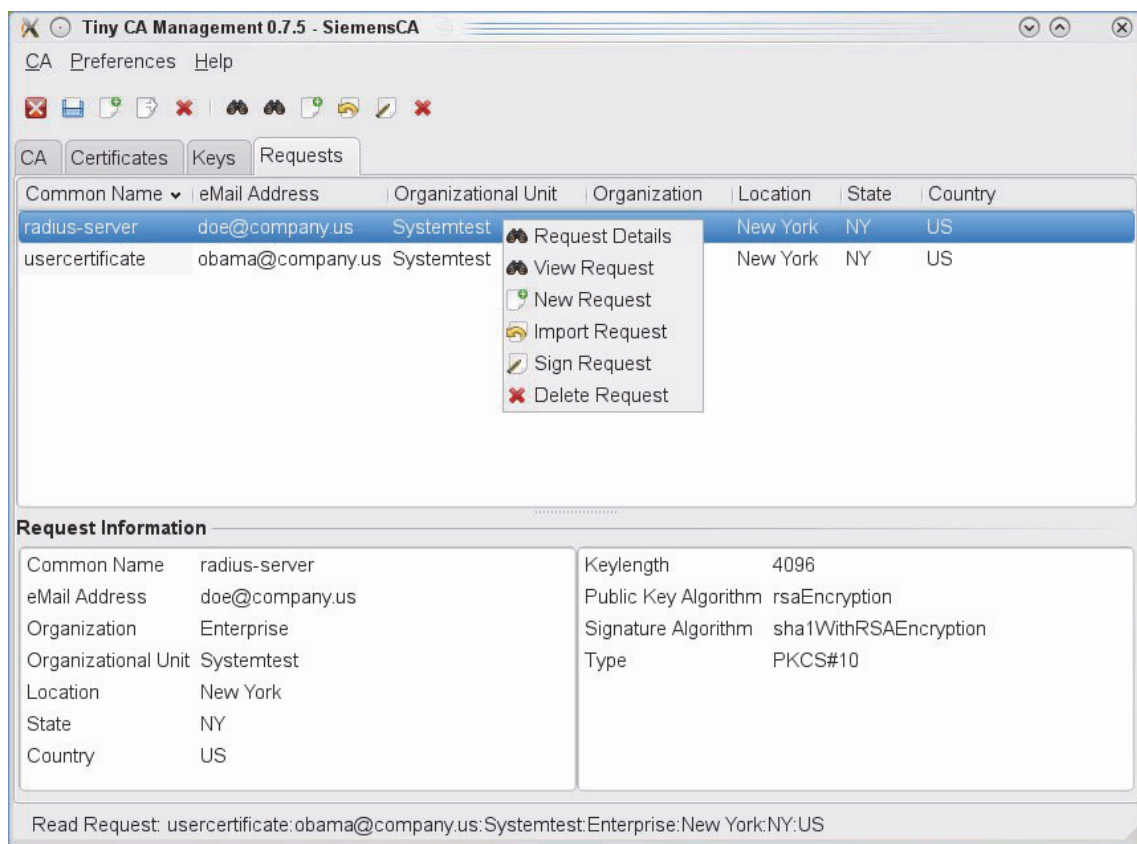
- Common Name (eg, your Name, your eMail Address or the Servers Name): radius-server
- eMail Address: doe@company.us
- Password (protect your private Key): [masked]
- Password (confirmation): [masked]
- Country Name (2 letter code): US
- State or Province Name: NY
- Locality Name (eg. city): New York
- Organization Name (eg. company): Enterprise
- Organizational Unit Name (eg. section): Systemtest
- Keylength: ☒ 4096 ☐ 1024 ☐ 2048
- Digest: ☒ SHA-1 ☐ MD2 ☐ MDC2 ☐ MD4 ☐ MD5 ☐ RIPEMD-160
- Algorithm: ☒ RSA ☐ DSA

At the bottom, there are 'OK' and 'Cancel' buttons.

- **Common Name:** Name of server, for example full DNS name.
- **eMail Address:** eMail address of person responsible for the server
- **Password:** Password for private key
- **Digest:** Default value can be kept
- **Algorithm:** Keep default value

Confirm by clicking OK.

Go to the **Requests** tab. In the following dialog, right-click on the relevant root certificate.



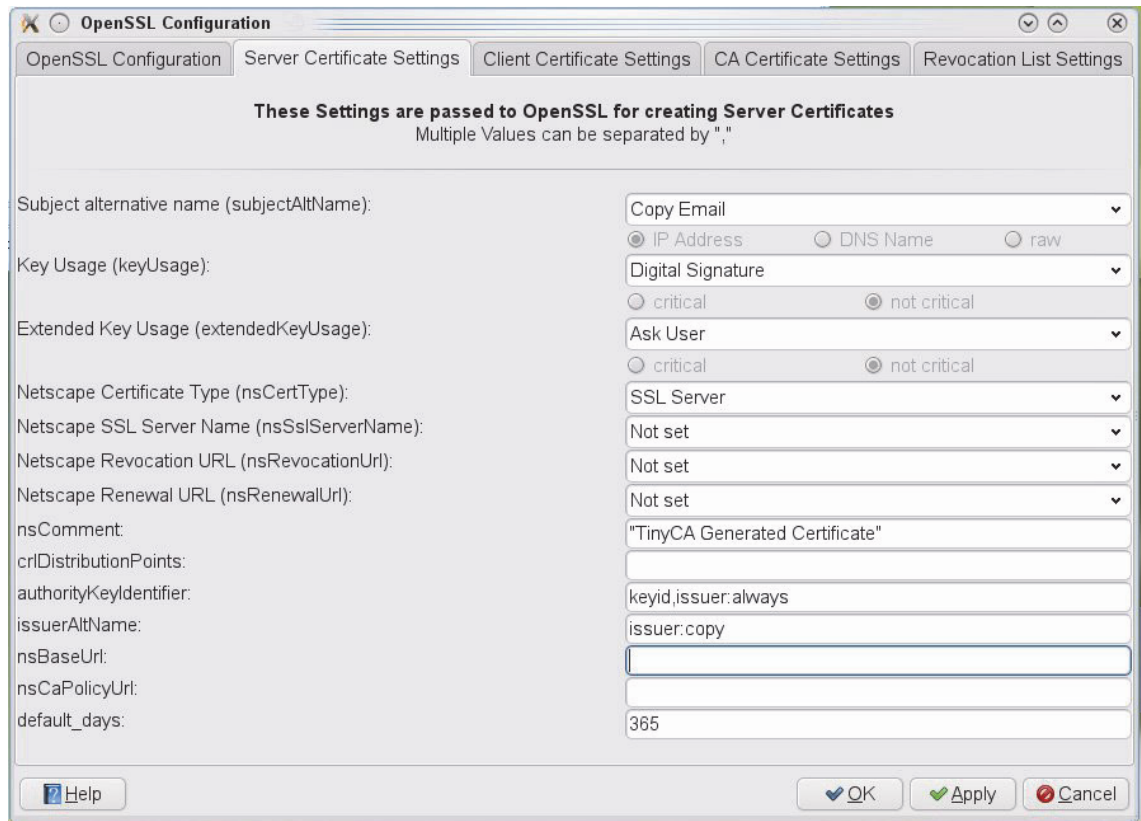
Select **Sign Request (Server)** in the pop-up that appears. Enter the password of the root certificate in the next dialog and specify the certificate's validity period in days.



You can choose whether to add the eMail address. If you wish to use certificates for Windows applications also, note that this dialog will contain the field "Extended Key Usage".

The Extension "1.3.6.1.5.5.7.3.1" must be entered in this field. Otherwise, authentication will not work under Windows. Confirm by clicking OK.

If this field is not displayed, you will need to make an additional entry in the OpenSSL settings of TinyCA2. Close the previous dialog. Click **Settings** and go to **OpenSSL Configuration**. Click the **Server Certificate Settings** tab. The following dialog is displayed:



For **Extended Key Usage**, select **Ask User**. This setting must be configured for client certificates also. Confirm by clicking **OK**.

➡ If an error occurs during signing (usually due to an incorrect password), close TinyCA2 and restart.

A confirmation message will appear on screen.

Create client certificate with TinyCA2

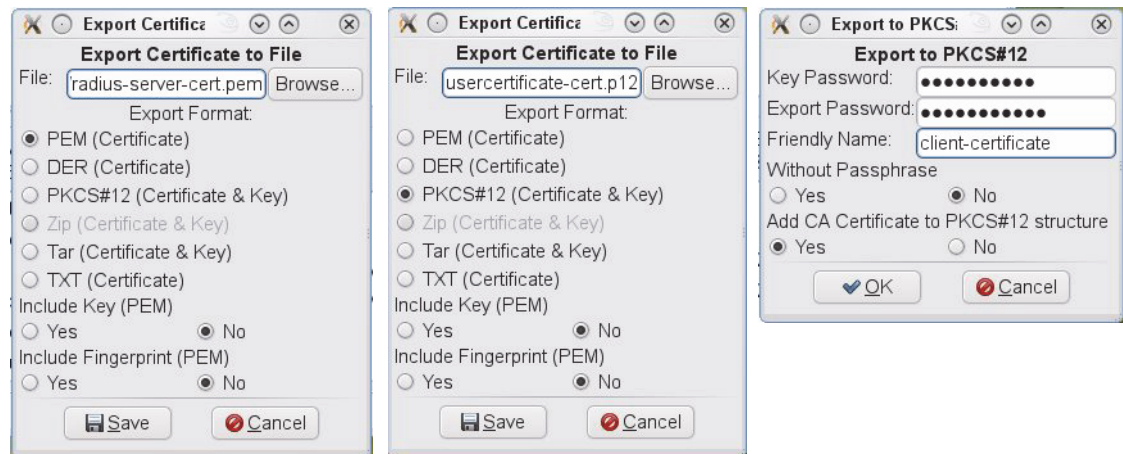
For new certificates, you must first create a new request with a new name, as described under Create server certificate with TinyCA2 (→ Seite 21). For **Sign Request**, select **Sign Request (User)**. If necessary, first go to **Settings** in **OpenSSL Configuration** in the **Client Certificate Settings** tab and select the option **Ask User for Extended Key Usage**.

If you get a message asking you to **Overwrite Certificate**, implying that a certificate with the same name already exists, click cancel, restart TinyCA2 and repeat the process.

Export certificates

1. Server Certificate

Click the **Certificates** tab. You will find the server certificate and the client certificate here. Mark the server certificate first and then right-click to bring up the context menu. Select **Export Certificate**. The following dialog is displayed:



Enter a meaningful name (for example: "radius-server-cert.pem") in the **File** field. Save the file. A confirmation message will appear onscreen.

Next, go to the **Keys** tab and perform the same steps as for the certificate. Enter a name, such as "radius-server-key.pem" and save the file. You will get a confirmation message.

2. Client Certificate

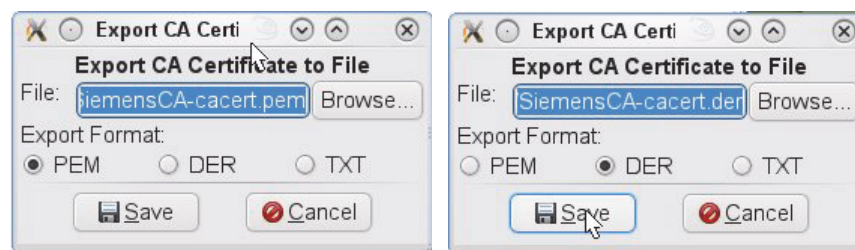
Go back to the **Certificates** tab and export the client certificate. Select PKCS#12 as the export format. Click **Save** and complete the dialog that appears. You will get a confirmation message. The key will be saved with the certificate in this format and as such must not be exported separately.

3. Root Certificate

To export the root certificate, go to the **CA** tab. As you have to save a root certificate on both the RADIUS server (Linux) and the client (Windows), you will need two formats:

- **.pem** for Linux
- **.der** for Windows

Click **Export CA** (last icon but one).



Export the root certificate in .pem and .der format. You will get a confirmation message.

Configure and start FreeRADIUS server for EAP-TLS

Copy the certificates that have been created (root, server and key certificates) to the directory /etc/raddb/certs. If this folder does not contain a "dh1024.pem" file (Diffie-Hellman parameters), you will have to create it yourself. Enter the following command:

```
openssl dhparam -out dh1024.pem 1024
```

EAP is already provided for in the RADIUS configuration ("/etc/raddb/radius.conf") under "authorize" and "authenticate".

Now modify the /etc/raddb/eap.conf file as per your requirements, using the following example as a guide:

```
eap {
    default_eap_type = tls
    timer_expire     = 60
    ignore_unknown_eap_types = no
    cisco_accounting_username_bug = no
    .
    .
    .
    .
    tls {
        certdir = ${confdir}/certs
        cadir = ${confdir}/certs
        private_key_password = 01735959004
        private_key_file = ${certdir}/radius-server-key.pem
        certificate_file = ${certdir}/radius-server-cert.pem
        CA_file = ${cadir}/SiemensCA-cacert.pem
        dh_file = ${certdir}/dh1024.pem
        random_file = ${certdir}/random
        fragment_size = 1024
        include_length = yes
        .
        .
    }
}
```

You can now start the RADIUS server using the command:

```
radiusd -X &
```

(the parameter **X** stands for debug mode).

Certificates for OpenStage, OpenScape Desk Phones and optiPoint phones

Copy (using FTP, for example) the client certificate (in ".pkcs#12" format) and the root certificate (".der") to the required Windows workstation.

1. Import Root Certificate

Double-click the relevant certificate file. The following dialog is displayed:



Click **Install Certificate...**, and then **Next** and **Finish**. Confirm the security message.

For verification, go to

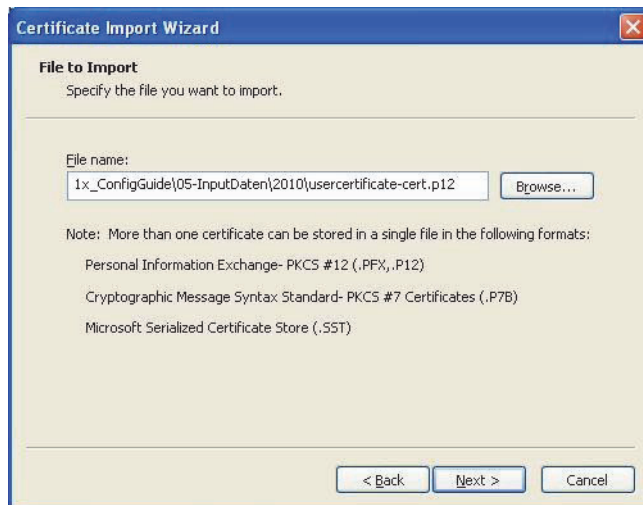
"Control Panel> Internet Options -> Content -> Certificates".

The root certificate should be listed in the "Trusted Root Certification Authorities" tab.

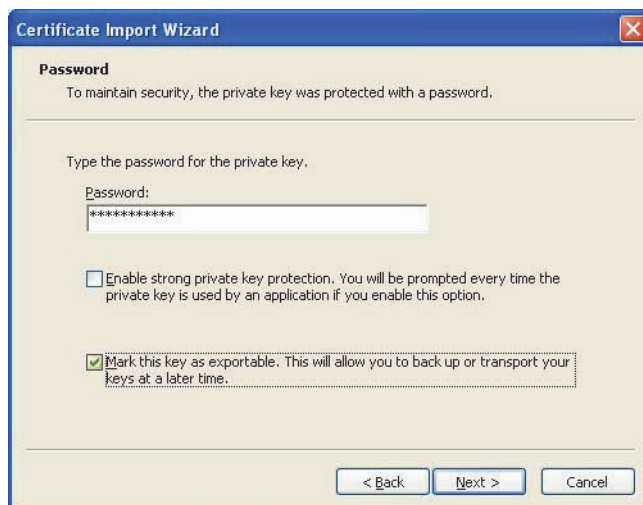
You have to export the certificate in order to be able to use it.

2. Import Client Certificate

Double-click the relevant certificate file. The Certificate Import Wizard appears.



If the correct file name is selected, click **Next**.



Enter the password for the private key. Select the option **Mark this key as exportable** and click **Next**. Confirm the following dialog with **Next** and complete the process by clicking **Finish**.

For verification, go to

"Control Panel> Internet Options -> Content -> Certificates".

The client certificate should be listed in the "Personal" tab.

You have to export the certificate in order to be able to use it.

Certificate formats

The PEM format uses the header and footer lines:

```
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
```

It will also handle files containing:

```
-----BEGIN X509 CERTIFICATE-----
-----END X509 CERTIFICATE-----
```

Trusted certificates have the lines:

```
-----BEGIN TRUSTED CERTIFICATE-----
-----END TRUSTED CERTIFICATE-----
```

The conversion to **UTF8 format** used with the name options assumes that T61 strings use the ISO 8859-1 character set. This is wrong, but Netscape and MSIE do this as do many certificates. So although this is incorrect, it is more likely to display the majority of certificates correctly.

The fingerprint option takes the digest of the DER-encoded certificate. This is commonly called a "fingerprint". Because of the nature of message digests, the fingerprint of a certificate is unique to that certificate. As such, two certificates with the same fingerprint can be considered to be the same.

The Netscape fingerprint uses MD5, whereas MSIE uses SHA1.

The **-email** option searches the subject name and the subject alternative name extension. Only unique email addresses will be output: the same address will not be output more than once.

-inform DER|PEM|NET

These parameters determine the input format. Normally, the command will expect an X509 certificate, but this can change if other options such as **-req** are present. The DER format is the DER encoding of the certificate and PEM is the base64 encoding of the DER encoding with header and footer lines added. The NET option is an obscure Netscape server format that is now obsolete.

For further information, see subsections 7.1.2 and 7.1.3 of [RFC 2459](#).

Simple certificate (client certificate) in text format

Sample:

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 4 (0x4)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=DE, ST=BY, L=Munich, O=Enterprise, OU=Systemtest, CN=enterpriseCA/email-
Address=kremer@teamone.de
    Validity
      Not Before: May 17 12:50:26 2010 GMT
      Not After: May 17 12:50:26 2011 GMT
    Subject: C=DE, ST=BY, L=Munich, O=Enterprise, OU=Systemtest, CN=enterpriseCA/email-
Address=kremer@teamone.de
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (4096 bit)
      Modulus (4096 bit):
        00:de:9e:ac:aa:06:bd:aa:97:2b:a5:aa:44:35:fd:
        4c:f0:f0:dc:92:ac:39:14:1d:35:d6:72:db:e1:68:
        85:49:e2:e0:79:22:81:34:13:58:5a:df:dc:eb:79:
        43:26:7f:16:38:86:75:1d:d4:32:79:c8:5f:04:d2:
        3f:77:35:99:be:8f:24:89:93:30:59:ae:e9:e1:14:
        f4:6f:a8:d2:5b:d3:5d:49:04:f4:14:df:63:49:f5:
        da:b5:78:27:9b:90:f5:9f:1f:67:ef:60:05:36:08:
        2d:39:27:54:92:9b:a1:c5:b5:83:0b:7e:c4:5b:33:
        4a:79:af:02:43:9b:2d:e9:61:b1:2e:b0:d2:93:46:
        70:52:1a:23:f9:44:17:1c:9e:32:bb:36:2d:75:d6:
        f6:53:89:0f:14:8c:f0:c7:10:e9:cc:cc:33:1a:e0:
        e9:a3:a3:96:80:81:78:97:ec:42:40:b0:9d:63:7d:
        de:4f:d3:ad:7c:0a:ad:73:f2:66:e4:ff:f6:ff:0e:
        47:7e:6b:b0:5e:9f:14:23:19:b4:4e:29:7e:d2:b3:
        95:c2:c7:89:3f:be:c7:2c:a1:07:b7:76:74:b5:56:
        bb:81:f1:96:4c:1d:38:67:cc:76:33:7b:7d:d1:2f:
        fb:e8:d7:9b:63:62:51:0e:5e:1f:70:e9:5e:4b:7b:
        e4:55:06:aa:c3:45:50:e4:84:29:67:40:98:90:c1:
        48:59:c4:01:c8:d6:f2:3a:ca:67:8c:54:e2:14:16:
        3b:8f:33:79:39:de:7a:68:77:98:de:34:87:c8:01:
        b0:b2:09:2b:b3:ab:ff:d8:00:50:cd:40:80:ff:7f:
        7b:2f:63:1a:71:4d:12:0e:4a:c4:05:b7:c6:81:67:
        63:07:d8:34:97:cf:18:e6:c7:f6:d7:3b:e5:84:0a:
        1d:81:82:a4:7b:00:e3:d6:00:e2:b1:d2:c3:70:8d:
        54:04:e3:5e:ce:46:7a:3b:57:33:7c:37:ce:9e:1b:
        06:20:84:35:6c:fa:bb:8f:08:25:fa:7c:dd:50:de:
        66:3e:4f:87:56:ef:1b:5d:c7:a8:8a:57:64:2e:42:
        f0:37:6e:c5:f4:58:d9:f9:ab:f8:09:7f:dd:30:88:
        05:ad:f4:d4:42:05:7d:95:52:1b:c9:58:67:03:72:
        d1:64:fc:66:64:1c:af:86:17:06:b1:9f:a8:ec:3b:
        24:f4:31:d9:15:a6:e0:bb:f2:f4:a4:b4:0e:e4:25:
        01:be:cb:ae:be:1e:8f:b2:64:44:96:f0:35:06:02:
        4c:09:81:ba:0d:b7:f6:06:c7:af:d2:63:2d:a0:55:
        61:2b:11:d5:48:98:79:39:58:35:28:0a:db:81:61:
        a3:bd:c5
      Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Basic Constraints:
        CA:FALSE
      Netscape Cert Type:
        SSL Client, S/MIME, Object Signing
      Netscape Comment:
        TinyCA Generated Certificate
```

```

X509v3 Subject Key Identifier:
    18:77:51:1F:83:60:D8:09:E3:F9:46:B0:B5:13:63:2A:91:42:BC:F4
X509v3 Authority Key Identifier:
    keyid:8F:DB:7A:D7:97:FE:5E:A6:16:A7:FE:BD:29:B9:F9:C1:A2:A6:F2:10
    DirName:/C=DE/ST=BY/L=Munich/O=Enterprise/OU=Systemtest/CN=enterpriseCA/
    emailAddress=kremer@teamone.de
    serial:9A:9D:17:C1:79:C5:7B:EC

X509v3 Issuer Alternative Name:
    email:kremer@teamone.de
X509v3 Subject Alternative Name:
    email:usercertificate
X509v3 Key Usage: critical
    Digital Signature, Key Encipherment
X509v3 Extended Key Usage: critical
    1.3.6.1.5.5.7.3.0.1
Signature Algorithm: sha1WithRSAEncryption
e0:a1:8e:71:ad:1a:00:6c:50:02:f9:7a:bd:65:93:c4:74:b5:
7e:3d:f8:26:d0:63:5a:92:c5:96:1b:73:25:5c:59:97:cf:31:
cd:a6:c6:b0:14:1c:03:40:68:d4:2b:9d:55:de:07:b9:4b:85:
0b:db:60:44:ae:77:c0:cf:00:45:e8:bc:cb:3c:6a:e4:5f:3b:
2b:43:28:df:29:05:ea:eb:6d:b0:1d:61:7f:21:ea:5e:c2:4e:
07:da:8f:7e:f3:f4:b4:80:82:90:56:38:d5:04:ef:24:55:8a:
66:d0:f7:06:54:37:86:87:c5:63:e6:b9:59:53:88:81:fb:cd:
22:1e:61:9f:85:bf:9e:18:e1:94:91:3b:88:9b:19:c1:c6:b0:
8d:90:65:2e:49:41:14:d3:89:0a:eb:1b:97:8a:33:c8:d5:f5:
61:75:3c:30:48:ac:25:3a:dc:ea:b5:26:3c:e7:11:39:75:98:
fe:41:52:32:55:1e:de:9b:b5:70:be:af:51:fe:2d:8f:69:64:
36:de:f7:7d:a5:59:6d:e8:3d:02:07:3b:4a:35:87:b3:ae:f0:
1c:2b:d8:50:ea:f6:d8:d5:cf:d3:e7:87:fa:89:8a:82:c2:21:
70:30:88:ba:03:3d:d3:ac:96:f8:cb:ce:b7:d2:83:7e:0e:c3:
35:f7:42:99:46:0b:18:b5:11:28:97:87:5b:b5:8d:ce:6f:b6:
c0:2e:87:99:24:08:85:47:79:3d:89:72:dd:c9:de:aa:ff:7e:
fd:8e:e2:75:15:ae:d4:54:6c:b3:ba:d5:fc:29:4f:40:4f:08:
34:d8:2d:97:08:2a:78:6e:55:03:3f:6a:a4:d7:4a:e7:1e:e1:
43:38:26:cf:4c:3b:b9:3f:e0:00:7f:43:85:b1:65:68:6f:c5:
08:20:7d:23:a0:32:9c:63:30:bd:c2:58:37:95:d9:2d:2f:1e:
eb:fa:bf:59:23:e7:4e:26:a2:26:69:0f:dc:01:e0:bf:33:3f:
86:4f:36:3c:44:c7:02:ed:d5:4a:4e:ac:6a:ee:3b:78:7b:9b:
a7:67:ed:41:f1:58:d4:fa:b0:ec:fe:6a:85:c6:ad:a9:2e:ec:
d8:cf:7a:42:73:b4:4a:8d:87:8c:6c:c2:81:85:6b:b9:de:95:
ba:75:e8:2a:35:38:60:cd:ad:fd:4a:fd:b3:86:9d:5c:9e:4f:
43:7a:5d:3a:9a:72:2d:d3:cb:fc:70:c1:1a:ae:f3:9e:08:d5:
1c:84:99:2a:2f:8f:4b:48:7e:ff:48:81:bf:da:fb:d3:a6:2f:
be:3e:26:4e:12:b2:46:e0:02:71:40:ac:3b:51:86:7c:6e:38:
44:f5:d8:43:1a:a5:

```

Microsoft solution with Windows Server 2008/2012

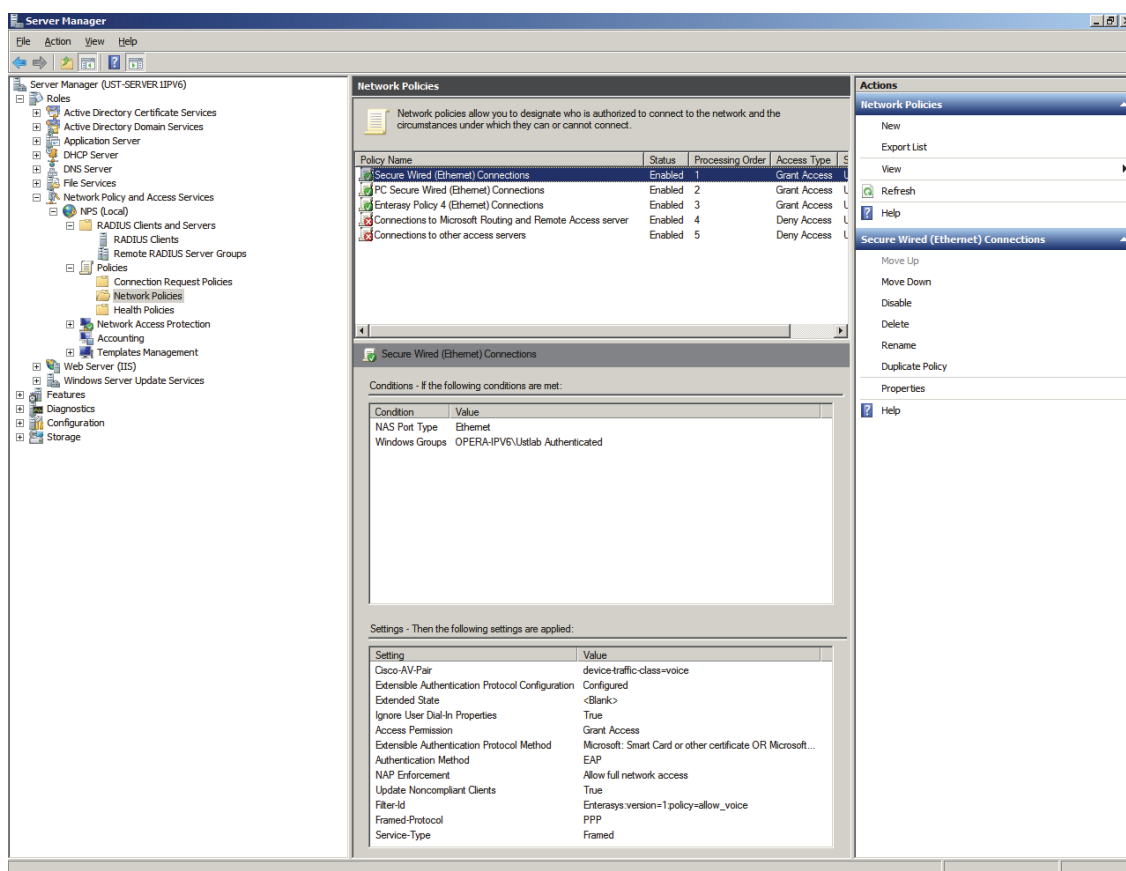
Network Policy Server (NPS) is the Microsoft implementation of a Remote Authentication Dial-in User Service (RADIUS) server and proxy in Windows Server 2008/2012. NPS is the replacement for Internet Authentication Service (IAS) in Windows Server 2003. For most comprehensive information please read the original Microsoft documentation of NPS:

<http://technet.microsoft.com/en-us/network/bb629414.aspx>

There you will also find a Migration Guide from IAS to NPS and other Step-by-Step Guides. Administering your NPS deployment requires the same basic steps as described for IAS in the previous chapter.

Final prerequisites:

- Domain Controller with Active Directory is installed
- You have to create user and group in the Active Directory
- You have to install the Certificate Services (Certificate Authority or CA)
- You have to install the NPS Server role
- You have to configure Radius Client in NPS
- With Network Policy you have to determine which Authentication methods can be used (see screen shot).



Creating certificates with XCertificate and Key management

Download and install the the latest version of XCA-Software (Freeware) on a windows computer (e.g. setup_xca-0.9.0.exe).

First Start

XCA configuration

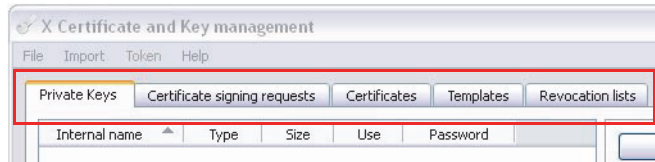
After the first start of the tool, you need to create a database to store all your certificates in.

- Select "File" -> "New Database"
- Select a place on your PC where you want to store the database file
- Select a password for protecting your database file

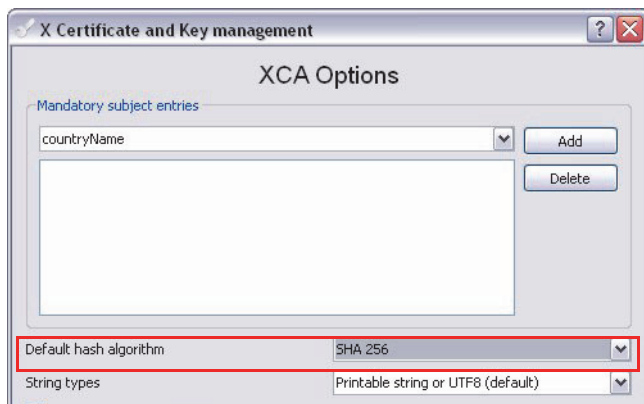


This password is required every time you want to open your database. All certificates and private keys that are stored in your database file, are stored without an additional password. Only the database password will give you access to your certificates. So let's call it the "Master-Password".

XCA has a separate tab for your Private Keys, Certificate Signing Requests, Certificates, Templates and Revocation Lists.



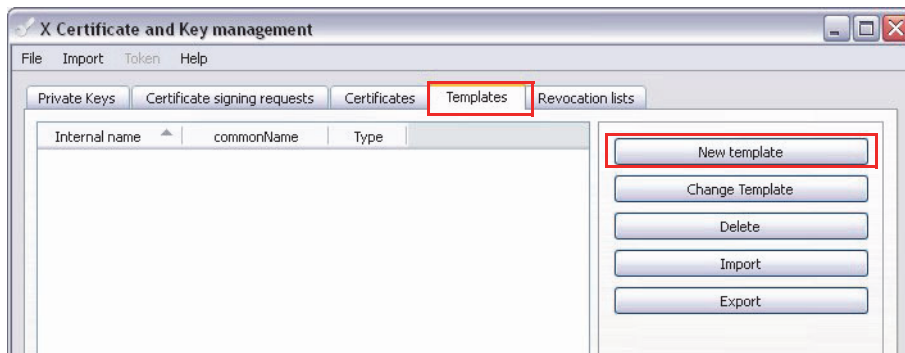
As a first action, change the default hash algorithm via File ' Options to the hashing algorithm SHA 256. The default SHA 1 is known to be weak, so we replace it with SHA 256.



Create Templates for repeating tasks

You can create templates to make it easier and faster if you need to create a lot of different server or client certificates.

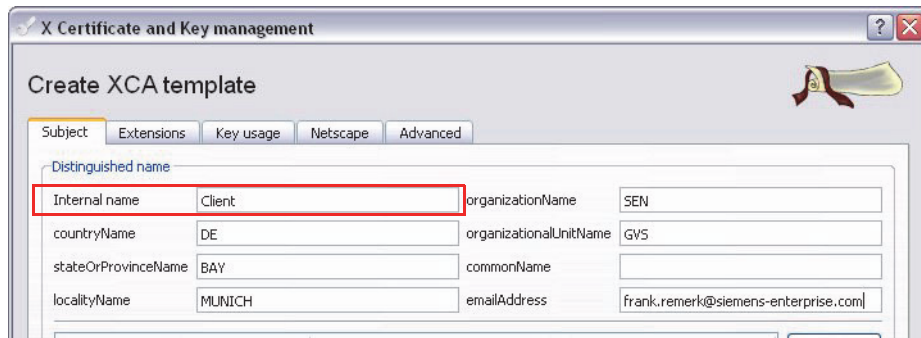
Go to tab "Templates" and select "New template".



Don't select a preset, just select OK and start with adding common subject information that will be identical across all certificates.



At least, define a name for the template.



X Certificate and Key management

Create XCA template

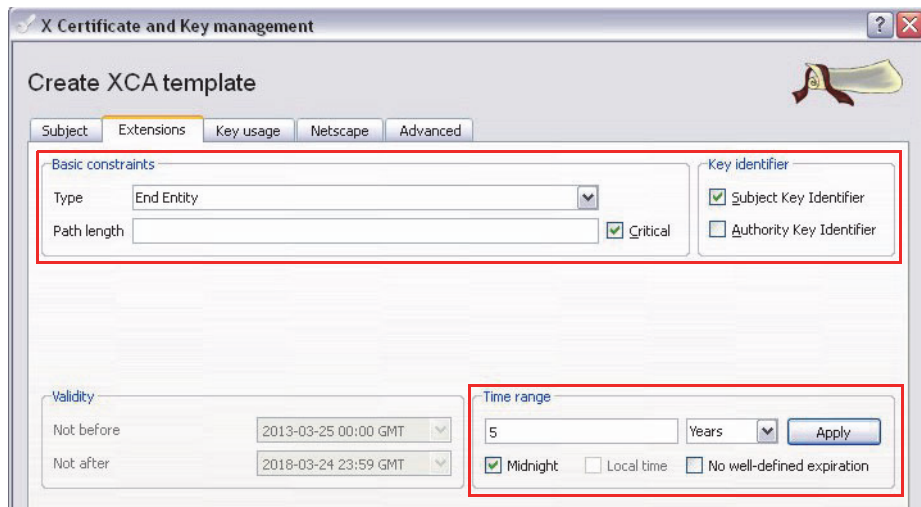
Subject Extensions Key usage Netscape Advanced

Distinguished name

Internal name	Client	organizationName	SEN
countryName	DE	organizationalUnitName	GVS
stateOrProvinceName	BAY	commonName	
localityName	MUNICH	emailAddress	frank.remerk@siemens-enterprise.com

You can also predefine the type of certificate and the validity-time range. In case of client or server certificate, be sure to select:

- End Entity
- Critical
- Subject Key Identifier



X Certificate and Key management

Create XCA template

Subject Extensions Key usage Netscape Advanced

Basic constraints

Type: End Entity

Path length: ☒ Critical

Key identifier

☒ Subject Key Identifier

☐ Authority Key Identifier

Validity

Not before: 2013-03-25 00:00 GMT

Not after: 2018-03-24 23:59 GMT

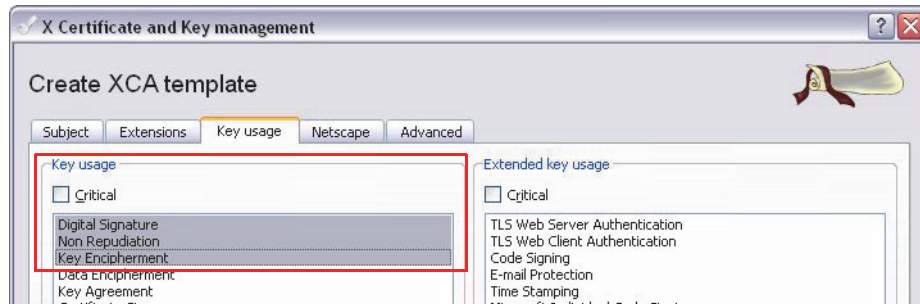
Time range

5 Years

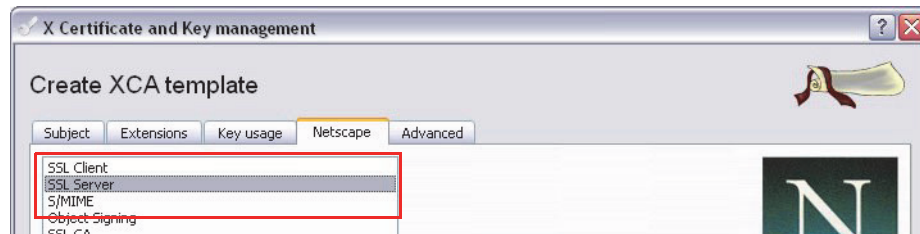
☒ Midnight ☐ Local time ☐ No well-defined expiration

Depending on the customer requirements, choose the validity-time wisely.

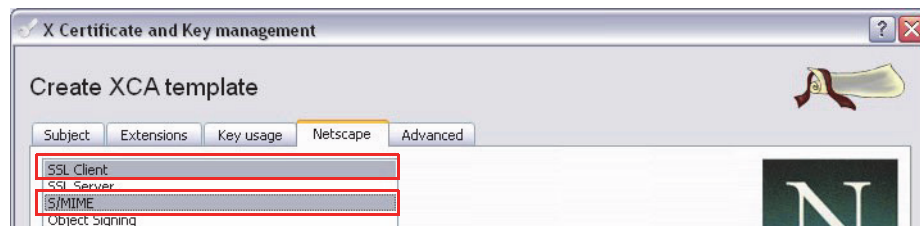
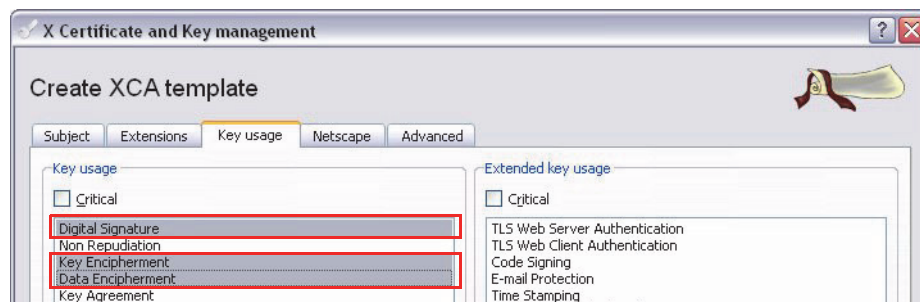
In case you want to create a template for a **server** certificate, be sure to select the following in the tab "Key usage"...



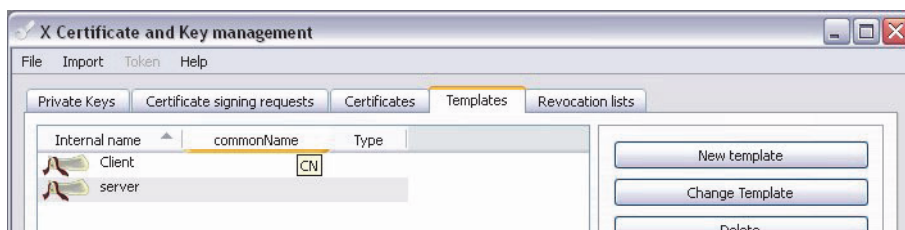
...and the following in the tab "Netscape"



If you want to create a template for a **client** certificate, be sure to select the following.

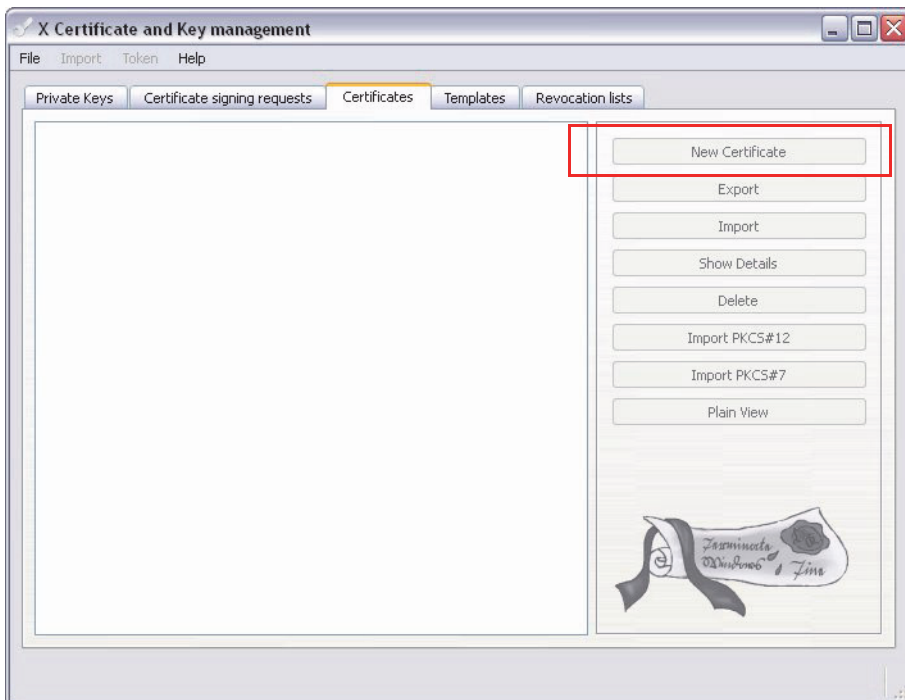


Select OK and you can find your templates in the "Templates" tab.

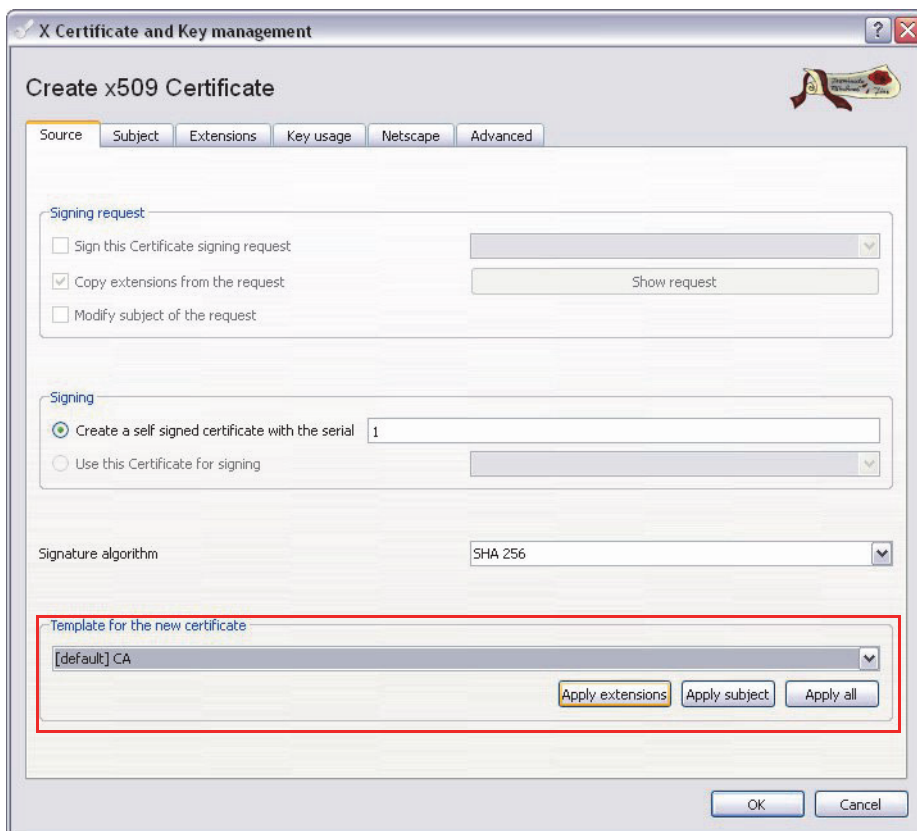


Create a new Certificate Authority (Root CA Certificate)

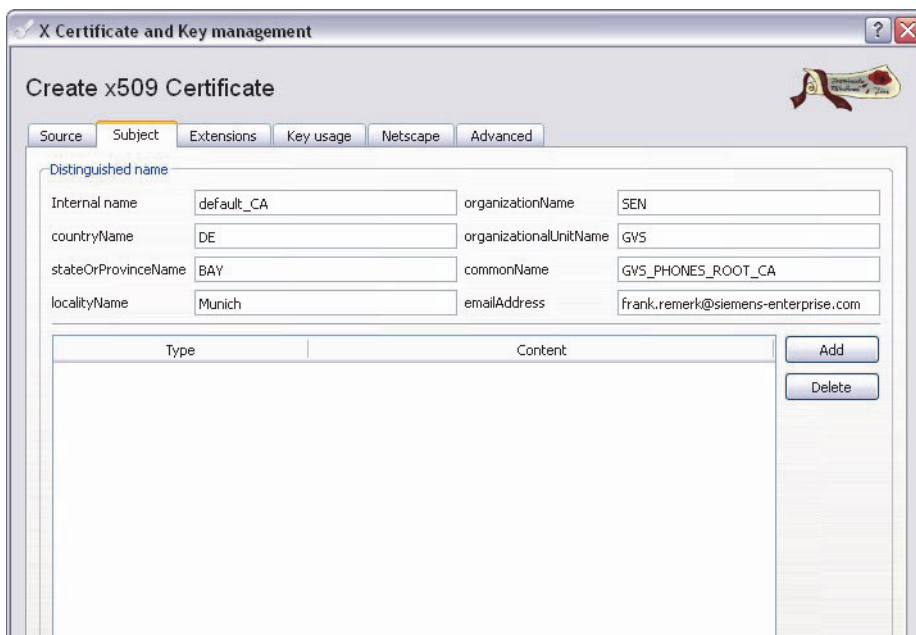
Go to tab "Certificates" and select "New Certificate".



In the new window you start on the "Source" tab. Select the default "CA" template and press "Apply extensions".



Continue on the "Subject" tab. Select an internal name so you will recognize the certificate and fill out the rest of the form according to your location and organization information.

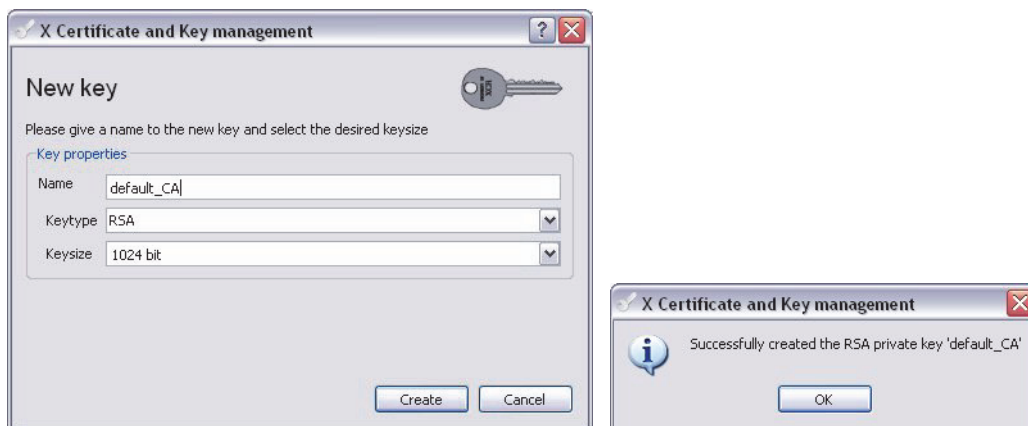


The screenshot shows the 'Create x509 Certificate' dialog box with the 'Subject' tab selected. The 'Distinguished name' section contains the following fields:

Distinguished name	
Internal name	default_CA
organizationName	SEN
countryName	DE
organizationalUnitName	GVS
stateOrProvinceName	BAY
commonName	GVS_PHONES_ROOT_CA
localityName	Munich
emailAddress	frank.remerk@siemens-enterprise.com

Below the fields is a table with columns 'Type' and 'Content', and buttons 'Add' and 'Delete'.

On the same tab, select "generate a new key" in order to generate a private key for your Certificate Authority. Verify that the newly created key is selected from the list.



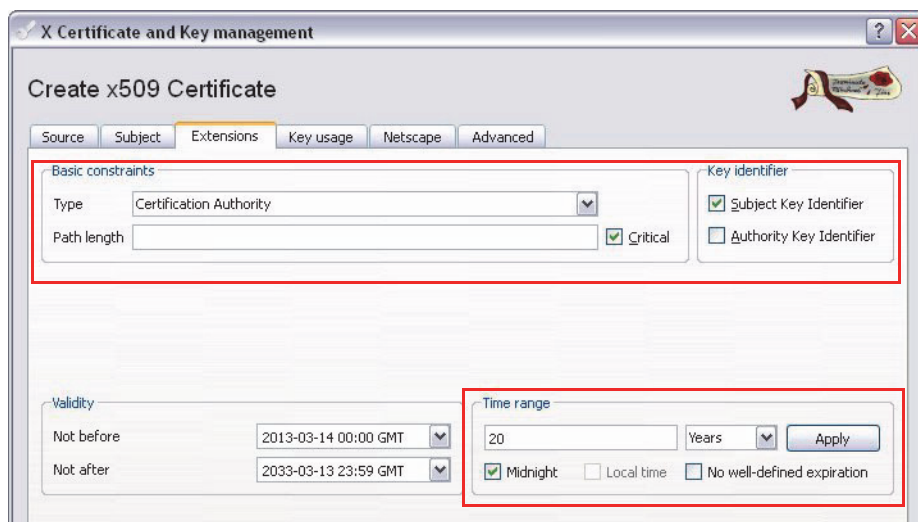
The screenshot shows the 'New key' dialog box with the following fields:

Key properties	
Name	default_CA
Keytype	RSA
Keysize	1024 bit

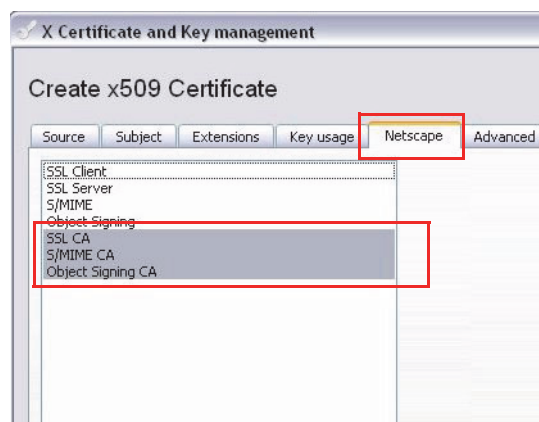
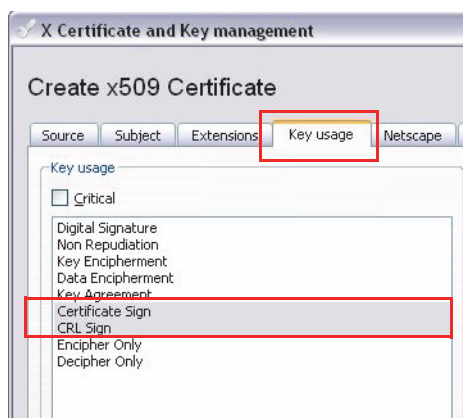
Buttons 'Create' and 'Cancel' are at the bottom.

To the right, a smaller dialog box shows the message: 'Successfully created the RSA private key 'default_CA'' with an 'OK' button.

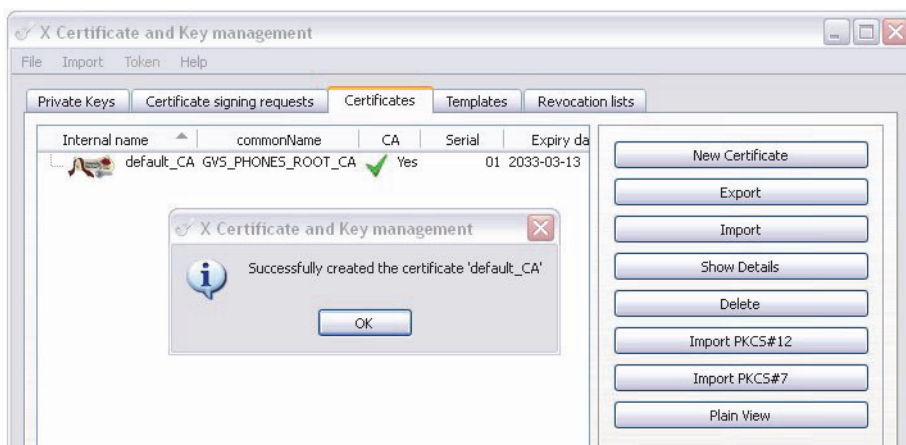
Switch to the "Extensions" tab and verify the settings as shown below



Verify the settings on the "Key Usage" and "Netscape" tab as shown below.

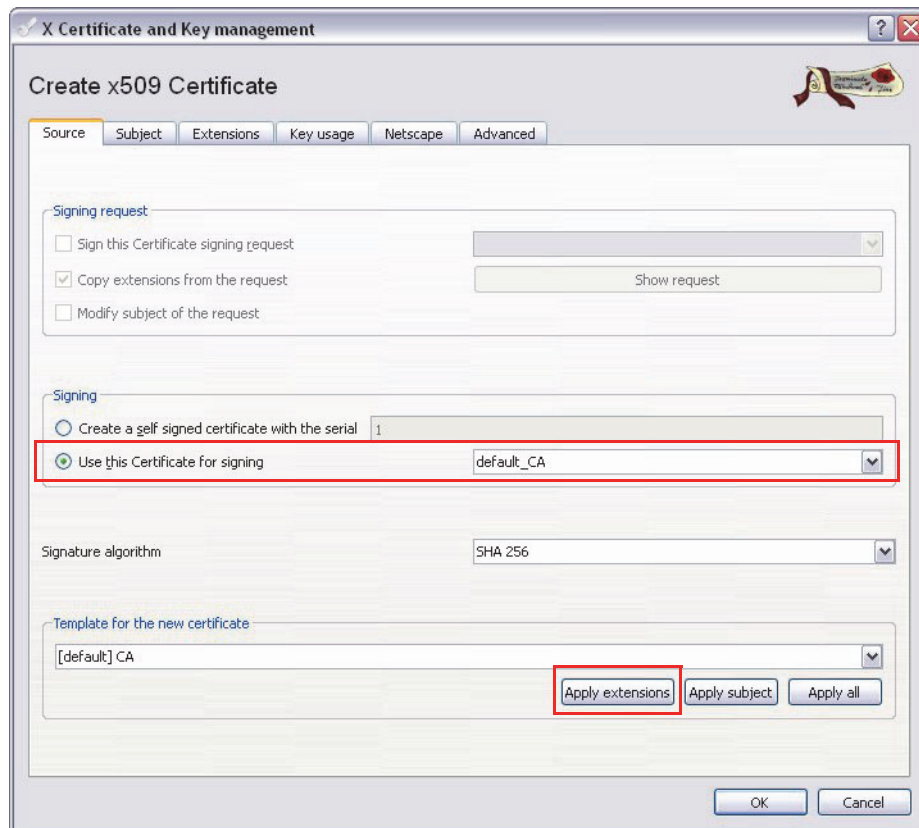


Press "OK" to finally create your new Certificate Authority and it will be listed in the "Certificates" tab of the main application.



Create a new Sub-Certificate Authority

Go to tab "Certificates" and select "New Certificate". In the new window you start on the "Source" tab. Use your Certificate Authority to sign this Sub-CA. Select the default "CA" template and press "Apply extensions".



The screenshot shows the 'Create x509 Certificate' dialog box with the 'Source' tab selected. The 'Signing request' section has 'Copy extensions from the request' checked. The 'Signing' section has 'Use this Certificate for signing' selected, with 'default_CA' in the dropdown. The 'Signature algorithm' is 'SHA 256'. The 'Template for the new certificate' is '[default] CA'. The 'Apply extensions' button is highlighted with a red box. The 'OK' and 'Cancel' buttons are at the bottom right.

Continue on the "Subject" tab. Select an internal name so you will recognize the certificate and fill out the rest of the form according to your location and organization information.

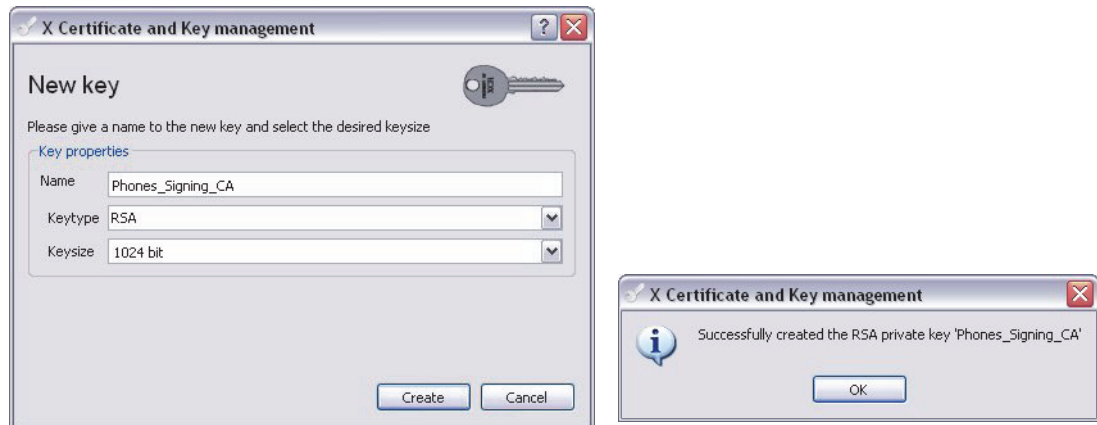


The screenshot shows the 'Create x509 Certificate' dialog box with the 'Subject' tab selected. The 'Distinguished name' section contains the following fields:

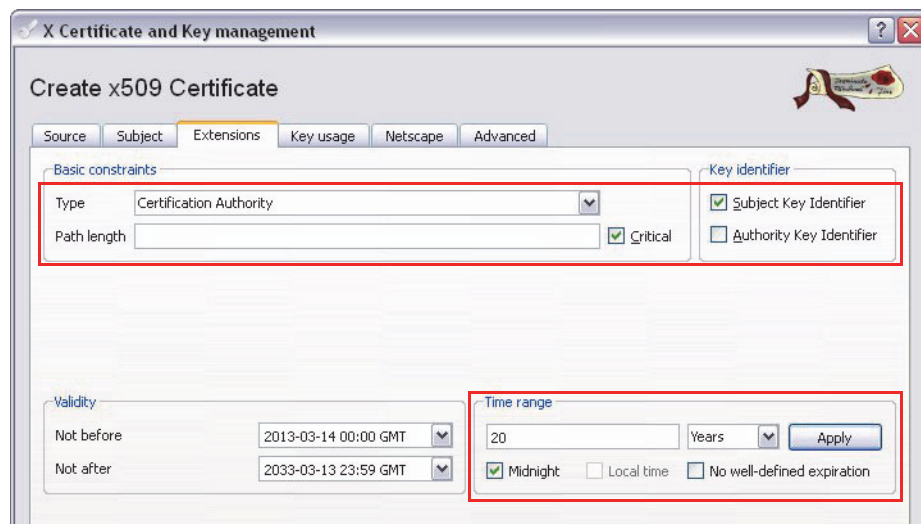
Type	Content
Internal name	Phones_Signing_CA
countryName	DE
stateOrProvinceName	BAY
localityName	MUNICH
organizationName	SEN
organizationalUnitName	GVS
commonName	GVS_PHONES_SIGNING_CA
emailAddress	frank.remerk@siemens-enterprise.com

The 'Add' button is at the bottom right.

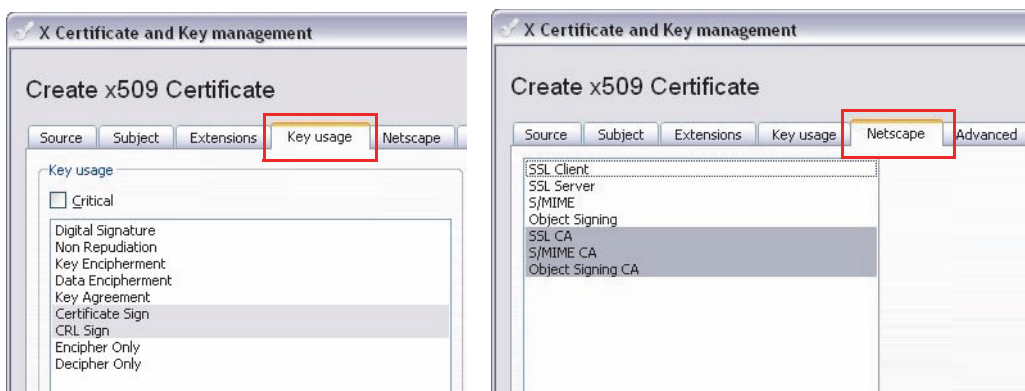
On the same tab, select "generate a new key" in order to generate a private key for your Sub-CA. Verify that the newly created key is selected from the list.



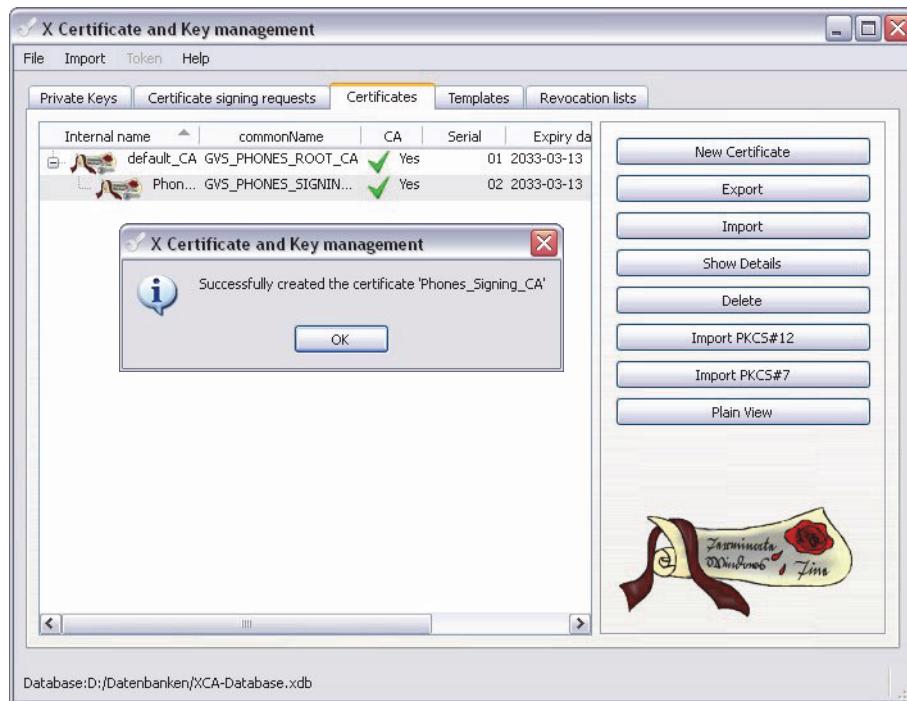
Switch to the "Extensions" tab and verify the settings as shown below.



Verify the settings on the "Key Usage" and "Netscape" tab as shown below.



Press "OK" to finally create your Sub-CA and it will be listed in the "Certificates" tab of the main application. It will be listed below the Certificate Authority that signed the Sub-CA to indicate the certificate chain.



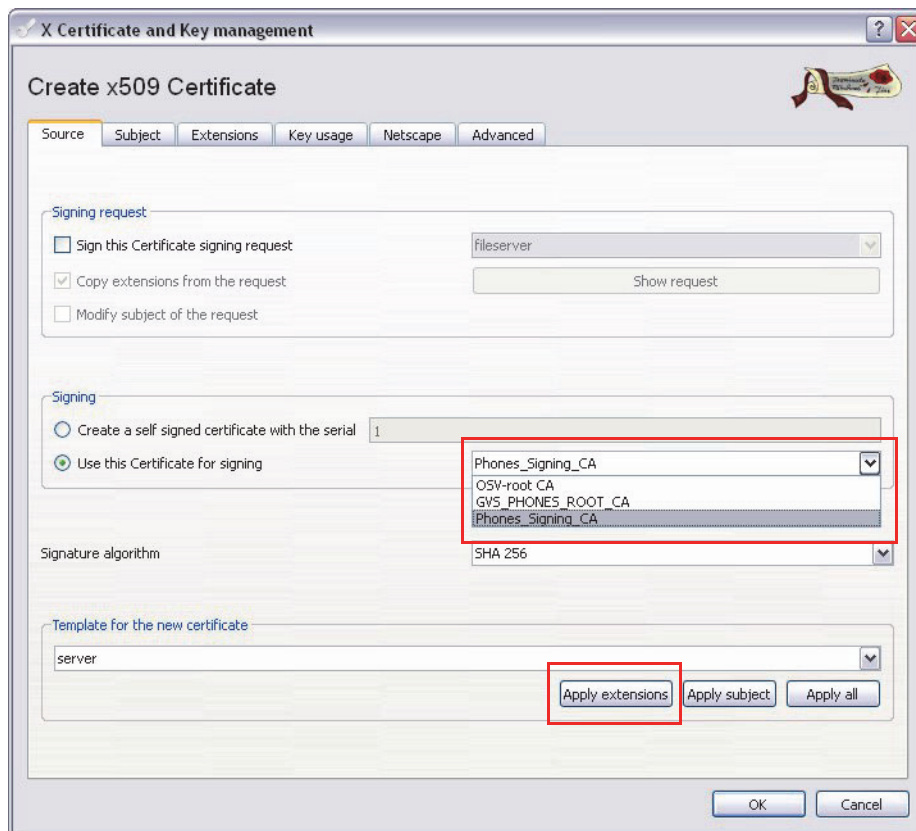
Create a new Server Certificate

The server certificate that will be created can be used for any "server based" authentication, e.g.

- OpenStage WBM Certificate
- SIP Server TLS Certificate
- Webserver Certificate
- etc.

This example demonstrates the creation of an OpenStage WBM certificate.

Go to tab "Certificates" and select "New Certificate". In the new window you start on the "Source" tab. Use your desired CA certificate to sign this server certificate. Select the default "Server" template and press "Apply extensions".



Continue on the "Subject" tab. Select an internal name so you will recognize the certificate and fill out the rest of the form according to your location and organization information. Chose the "Common Name" according to the way you would open the WBM of the device in the browser. This can be an FQDN or an IP Address, e.g.

- <https://4989722100.voice.gvs.local>
- <https://192.168.254.20>

The screenshot shows the 'Create x509 Certificate' dialog box with the 'Subject' tab selected. The 'Distinguished name' section contains the following fields:

Internal name	OpenStage WBM	organizationName	SEN
countryName	DE	organizationalUnitName	GVS
stateOrProvinceName	BAY	commonName	4989722100.voice.gvs.local
localityName	MUNICH	emailAddress	

On the same tab, select "generate a new key" in order to generate a private key for your Server certificate.

The screenshot shows the 'New key' dialog box. The 'Key properties' section contains the following fields:

Name	OpenStage WBM
Keytype	RSA
Keysize	1024 bit



An unsecure method to create one certificate for your whole domain is a wild card certificate. It is strongly recommended to not use this method, but for testing purposes it is a fast way to deploy a certificate to a lot of devices.

The screenshot shows the 'Create x509 Certificate' dialog box with the 'Subject' tab selected. The 'Distinguished name' section contains the following fields:

Internal name	OpenStage WBM	organizationName	SEN
countryName	DE	organizationalUnitName	GVS
stateOrProvinceName	BAY	commonName	*voice.gvs.local
localityName	MUNICH	emailAddress	

Besides a wild card certificate, it's sometimes necessary to have more than one "Common Name" in a certificate. For this you can add a "Subject Alternative Name". This can be done in the Extensions tab, e.g.

IP:192.168.254.20,4989722100.voice.gvs.local

Multiple entries can be added comma separated.

subject alternative name ✓ IP:192.168.254.20,DNS:4989722100.voice.gvs.local Edit

issuer alternative name Edit

CRL distribution point Edit

Authority Info Access OCSP Edit

OK Cancel

Verify the other settings on the "Extensions", "Key Usage" and "Netscape" tab as shown below.

Create x509 Certificate

Source Subject Extensions Key usage Netscape Advanced

Basic constraints

Type End Entity

Path length Critical

Key identifier

Subject Key Identifier

Authority Key Identifier

Validity

Not before 2013-03-14 00:00 GMT

Not after 2023-03-13 23:59 GMT

Time range

10 Years

Midnight

No well-defined expiration

Apply

Create x509 Certificate

Source Subject Extensions Key usage Netscape

Key usage

Critical

Digital Signature

Non Repudiation

Key Encipherment

Data Encipherment

Key Agreement

Certificate Sign

CRL Sign

Encipher Only

Create x509 Certificate

Source Subject Extensions Key usage Netscape Advanced

SSL Client

SSL Server

S/MIME

Object Signing

SSL CA

S/MIME CA

Object Signing CA

Press OK and the new created Server Certificate will be added to the list according to the CA you selected for signing the Server Certificate.

X Certificate and Key management

File Import Tokens Help

Private Keys Certificate signing requests Certificates Templates Revocation lists

Internal name commonName CA Se

default_CA GVS_PHONES_ROOT_CA Yes

Phones_Signing_CA GVS_PHONES_SIGNING_CA Yes

OpenStage WBM 4989722100.voice.gvs.local No

Successfully created the certificate 'OpenStage WBM'

OK

New Certificate

Export

Import

Show Details

Delete

Import PKCS#12

Import PKCS#7

Create a new Client Certificate

The Client Certificate that will be created can be used for any "client based" authentication, e.g. 802.1x

This example demonstrates the creation of an 802.1x client certificate.

Go to tab "Certificates" and select "New Certificate". In the new window you start on the "Source" tab. Use your desired CA certificate to sign this client certificate. Select the default "Client" template and press "Apply extensions".

The screenshot shows the 'Create x509 Certificate' dialog box with the 'Source' tab selected. The 'Signing request' section has 'Sign this Certificate signing request' unchecked, 'Copy extensions from the request' checked, and 'Modify subject of the request' unchecked. The 'Signing' section has 'Use this Certificate for signing' selected, with 'Phones_Signing_CA' chosen from the dropdown. The 'Signature algorithm' is set to 'SHA 256'. The 'Template for the new certificate' is set to 'Client'. Buttons for 'Apply extensions', 'Apply subject', and 'Apply all' are at the bottom right.

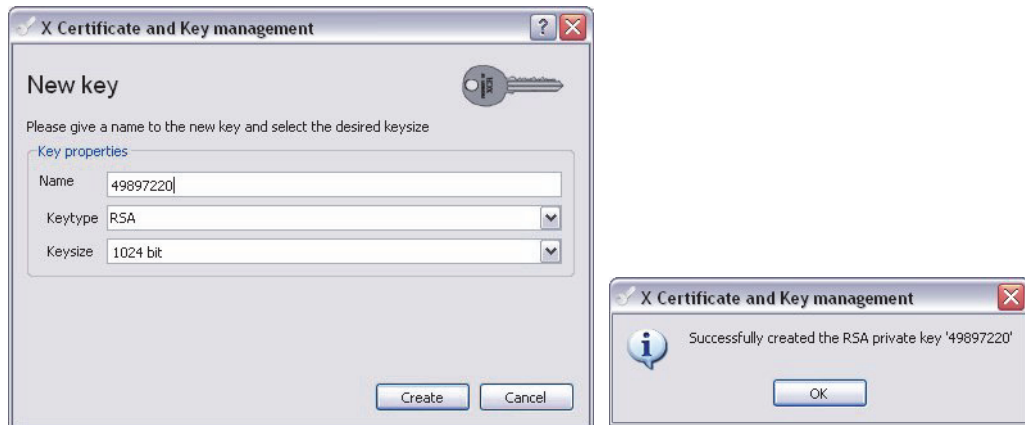
Continue on the "Subject" tab. Select an internal name so you will recognize the certificate and fill out the rest of the form according to your location and organization information. Choose a "Common Name" for 802.1x authentication.

The screenshot shows the 'Create x509 Certificate' dialog box with the 'Subject' tab selected. The 'Distinguished name' section contains the following fields:

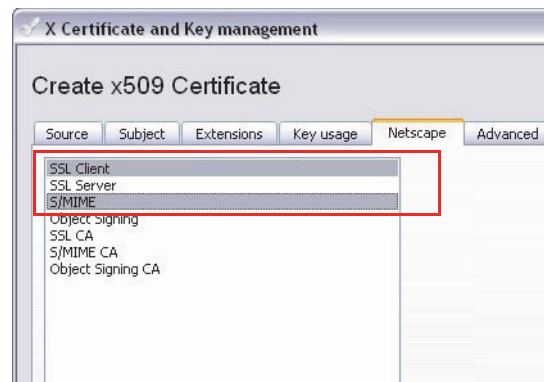
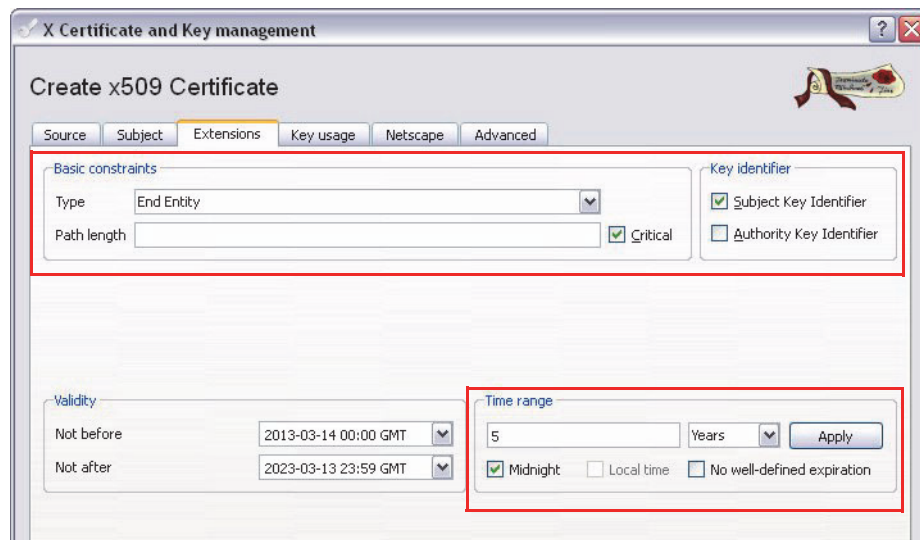
Internal name	802.1x	organizationName	SEN
countryName	DE	organizationalUnitName	GV5
stateOrProvinceName	BAY	commonName	49897220.voice.gvs.local
localityName	MUNICH	emailAddress	

The 'commonName' field is highlighted with a red rectangle.

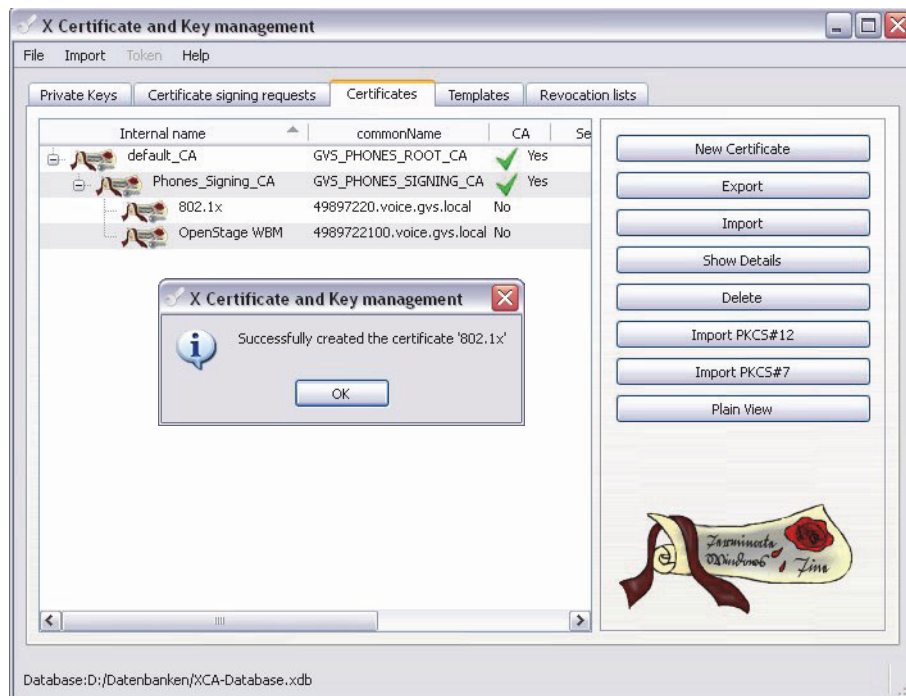
On the same tab, select "generate a new key" in order to generate a private key for your Client certificate.



Verify the other settings on the "Extensions", "Key Usage" and "Netscape" tab as shown below.

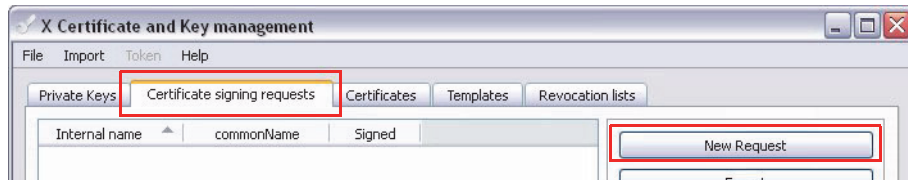


Press OK and the new created Client Certificate will be added to the list according to the CA you selected for signing the Client Certificate.

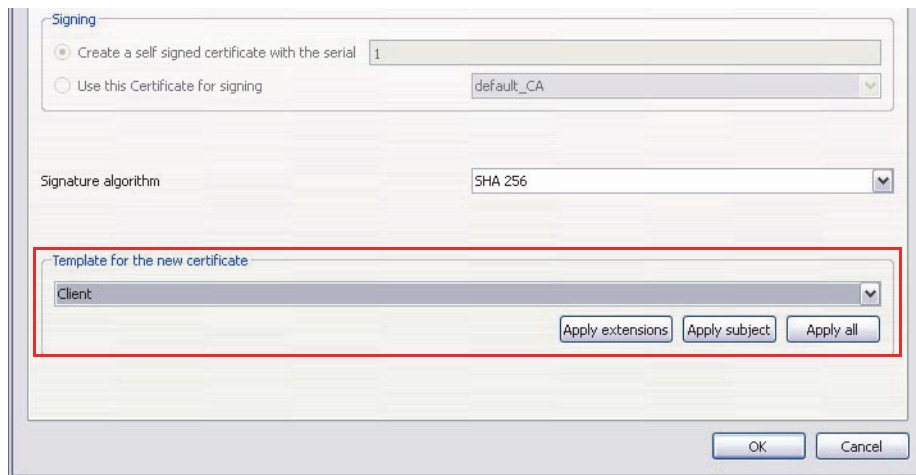


Create a Certificate Signing Request

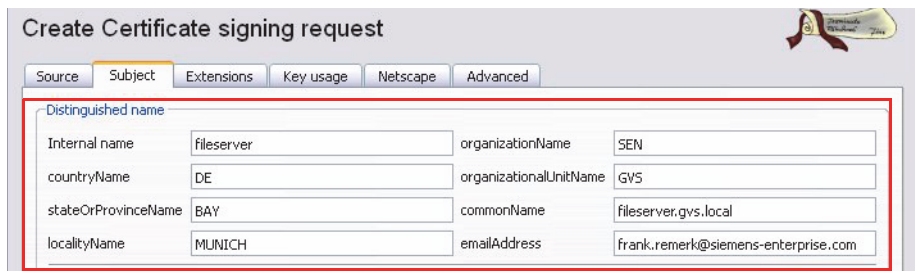
If you need to create a Certificate Signing Request (CSR) that will be signed by e.g. the customers CA, go to tab "Certificate signing requests"



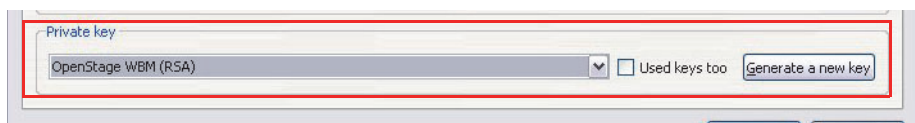
and select "New Request"



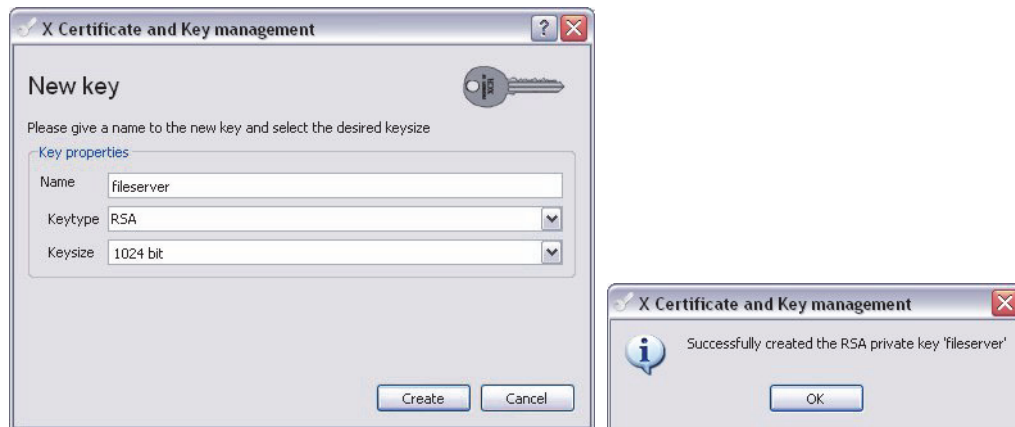
Select either the Client or Server template depending on what kind of CSR you want to create and press "Apply extensions".



Choose an internal name for the CSR and adapt the location/organization information if this is required by the signing CA. Also choose a common name (CN) for this certificate (e.g. FQDN for a server certificate)



Now you need to create the private key. Select "Generate a new key",

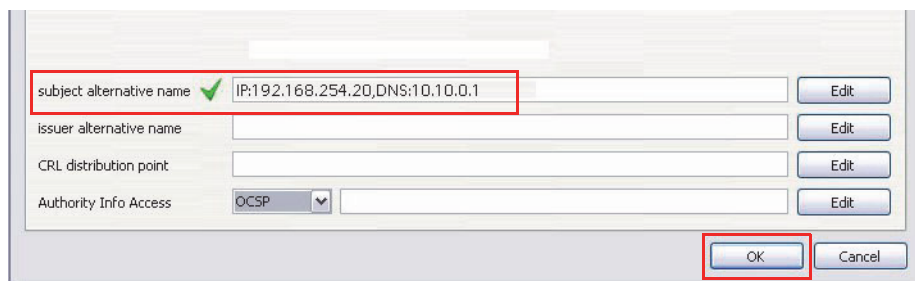


...change the settings if required and select "Create".

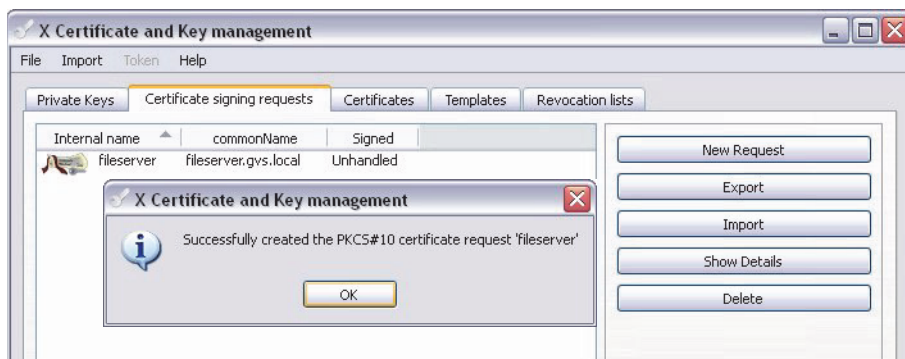
Verify the settings on the tab "Extensions"...



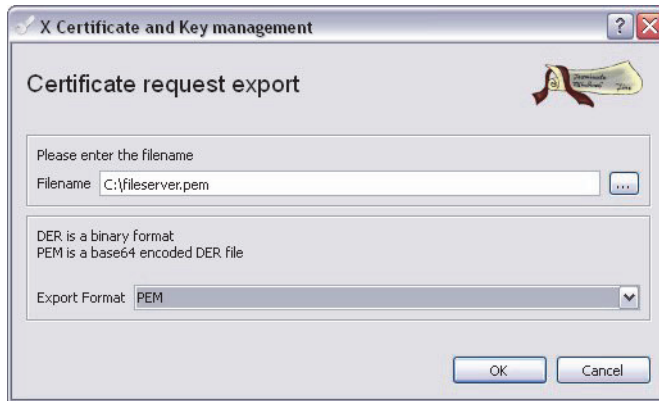
...and add a "subject alternative name" if required. E.g.:



Finally select OK and your CSR is listed in the "Certificate signing requests" tab.



You can now export the CSR, so it can be signed by the customers CA. Select the CSR and press "Export".



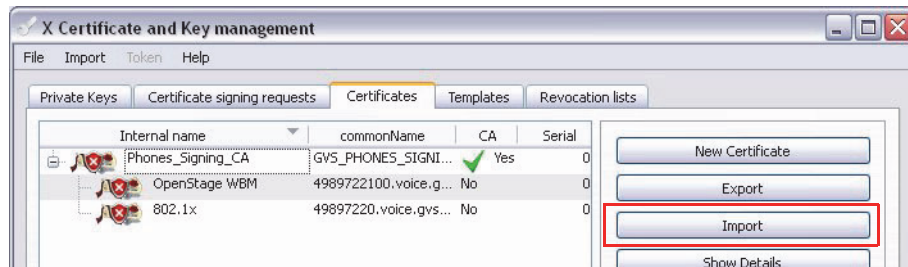
You can choose to export this CSR in PEM or DER format. Once you receive the signed certificate from the customer, you can import it back into the XCA database. Take a look at chapter Import Certificates into the database (→ Seite 51).

Import Certificates into the database

Import random certificates into XCA

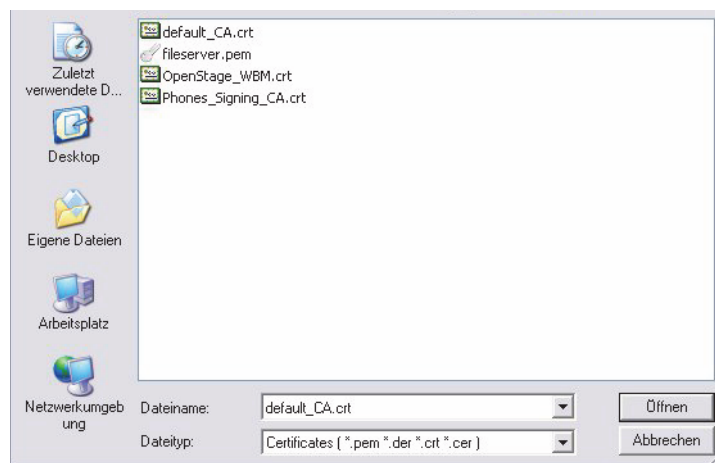
You can import any certificate and private key into the database. The certificates can be in DER (binary) or PEM (Base64) format. Either as file, or you can copy and paste the content of a file.

Select Import from the right hand menu.

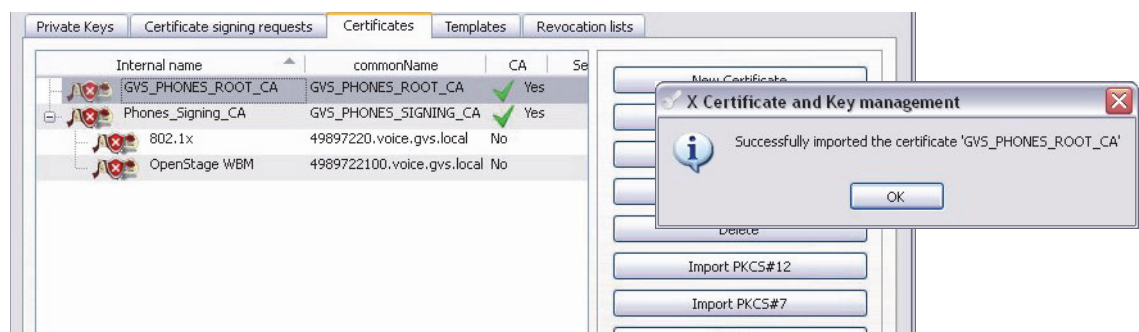


- Keys: Import private keys
- Requests: Import Certificate requests
- Certificates: Import Certificates (Server, Client, Sub-CA or CA Certificate)
- PKCS#12: Certificate container file in PKCS#12 format
- PKCS#7: Certificate container file in PKCS#7 format
- Template: Import XCA Certificate template files
- Revocation list: Import a Revocation list
- PEM file: Import a PEM file that may contain a single certificate or a certificate chain
- Paste PEM file: Copy and Paste a certificate in Base64 format

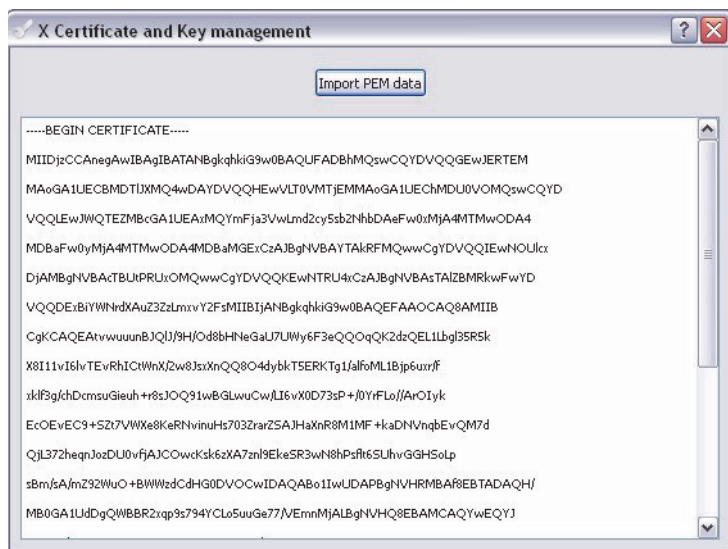
This example will show you how to import a single certificate or a certificate chain the save way. In the default, XCA will list files ending with ".pem", ".der", ".crt" and ".cer".



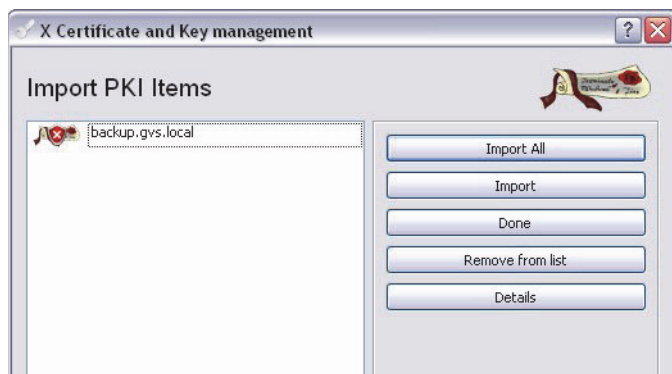
Select „Open“. The certificate will be imported at once.



In case you received a Base64 encoded certificate in text format, select "Import" and "paste PEM file" from the main menu.



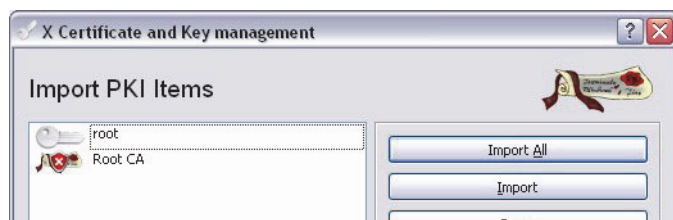
Copy and Paste the data into the window and select "Import PEM data". You are again presented with the certificates found in the text data and you can select which one of them you want to import.



All imported certificates will be listed in the "Certificates" tab in the main window.

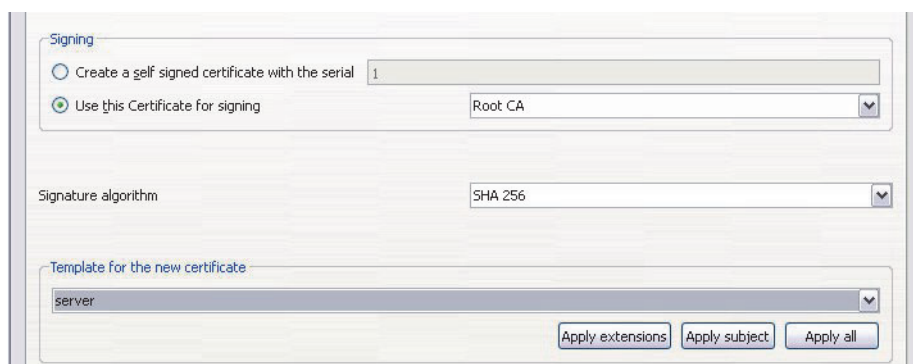
Import Root CA certificate and private key from OpenScape Voice

In case you need to work with the default CA of OpenScape Voice, you can simply import it into XCA. Download `/usr/local/ssl/certs/root.pem` from the OpenScape Voice using (e.g.) WinSCP and import it as PEM file like described before.

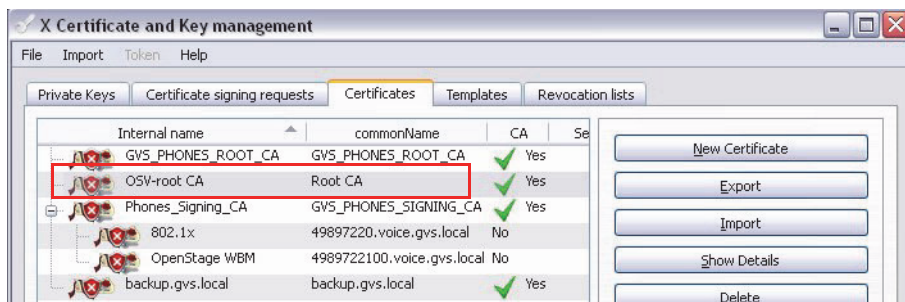


You will see 2 entries here, the Root CA Certificate and the private key. Select "Import all" in order to import these files into the database.

Whenever you want to create a new server or client certificate that has to be signed by this CA, follow the appropriate chapter in this document, but select this root certificate to sign the server or client certificate you want to create.

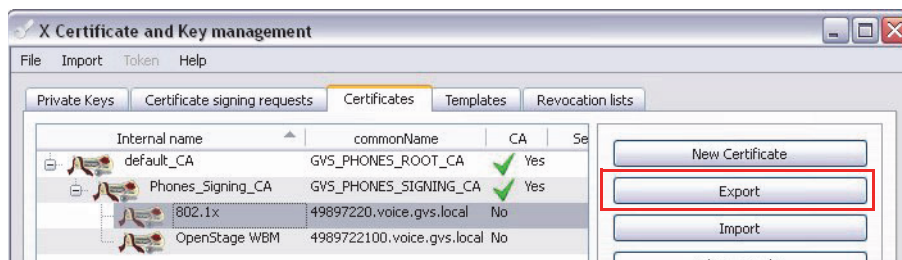


To correctly identify the OSV Root CA certificate, you can also rename it.



Export Certificates from the database for 802.1x

Select the Certificate for 802.1x usage and select Export from the right hand menu.



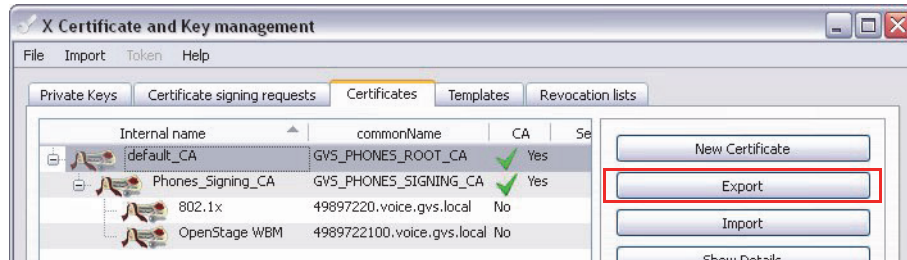
In the new window, select a place where to save the file.



Select PKCS #12 as the export format and press OK. You need to select a password to protect the PKCS 12 file because it contains your private key. Therefore it is required to password protect the file.



Next, export the Certificate Authority, which is the Root Certificate of the whole Certificate Chain. Select the Certificate and press "Export" from the right menu.



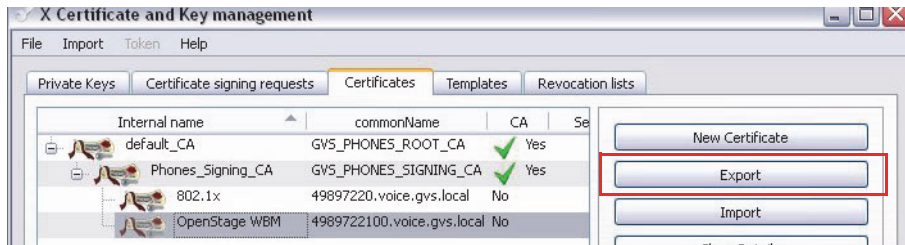
Select a place where to save the file and choose PEM as the export format.



You can now import both files into DLS and deploy them onto a phone for 802.1x authentication.

Export Certificates for Web Based Management

Select the Certificate for the phone internal Webserver (WBM) and select Export from the right hand menu.



In the new window, select a place where to save the file.



Select "PKCS #12 with Certificate chain" as the export format and press OK. You need to select a password to protect the PKCS 12 file because it contains your private key. Therefore it is required to password protect the file.



You can now import the file into DLS and deploy them onto a phone for replacing the current WBM Certificate.

Managing Certificates in the DLS



Client and server certificates for the following server/client configurations can be managed in the

- **Server:** DLS
Client: IP Phone
- **Server:** RADIUS Server
Client: IP Phone



Certificates can only be managed via the DLS, **not** via WBM or directly on the phone.

Please ensure that all devices are provided with the current time via NTP server before the certificates are deployed.

For further information, please refer to the Administration Manual "Deployment Service".

Plug & Play – template

To preconfigure certificates via Plug & Play, these need to be saved in a template which in turn needs to be part of a profile.

To import certificates in the DLS, proceed as follows:

1. Go to **IP Devices > IP Phone Configuration > IEEE 802.1X**.
2. Select "**Template**" view.
3. Go to the "**Phone Certificate**" tab and click "**Import Certificate**" to import the phone certificate from the user certificate.
4. Select "**RADIUS Server CA Certificate 1**" tab and click "**Import Certificate**" to import the server certificate from the root certificate.

If a second certificate is required to enable the switching of certificates: Select "**RADIUS Server CA Certificate 2**" tab and click "**Import Certificate**" to import the server certificate from the root certificate.

5. Click "**Save**" to save it in a new or existing template.
6. To preconfigure certificates via Plug & Play, these need to be saved in a template in DLS which in turn needs to be part of a profile.



For more information on how to create the templates, refer to the section "Importing Phone and RADIUS Certificates (Certificate for IEEE 802.1X)" and "Editing Templates (Generating and Managing Templates)" in the Administration and Installation Manual for the "OpenScape Deployment Service".

Plug & Play with IEEE 802.1X

Overview

A three-phase configuration is needed to set up the plug & play feature that downloads parameters and certificates. This section describes the three configuration phases and the Plug & Play function.

Previous sections of this documentation described how to create certificates and how to install and configure the RADIUS server.

The three phases are:

- Configuring Plug & Play in DLS
- DHCP Configuration
- Switch Configuration (Cisco in this case)

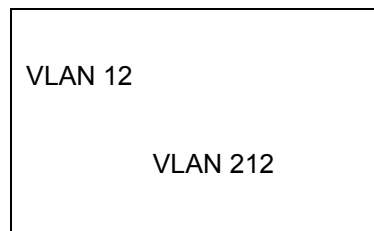
Test Environment

First of all, here is some information about the DATA network of the test environment. The test uses two Catalyst 3560s (referred to as Lab 12 and Lab 11).

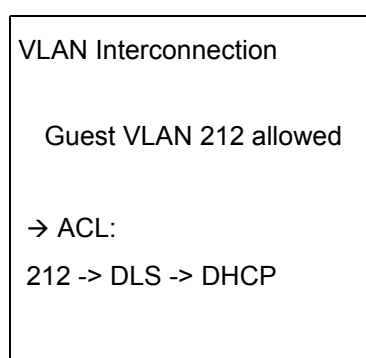
The XP client, in this case the telephone (→ Supplicant), and the "Authentication Server" (RADIUS) are connected to the first switch referred to as "→ Authenticator" in the following sections.

The second switch is the router (Inter-VLAN Routing – connects the address ranges); the DLS and the DHCP server are connected to this switch. The connection between the two switches is tunneled (IEEE 802.1X-transparent).

Switch (→ Authenticator)



Router



Configure Phone for DHCP

With a new telephone right out of the box, the only parameter known is the MAC address. The presetting for DHCP is "on".

As the telephone does not have a certificate and the switch is configured with IEEE 802.1X Guest VLAN, the telephone is – after the → EAP check – assigned to the Guest VLAN 212 (address range 212).

During switch monitoring (after a timeout), you can see that the port is assigned to VLAN 212.

Configuring Plug & Play in DLS

Plug & Play – creating profiles

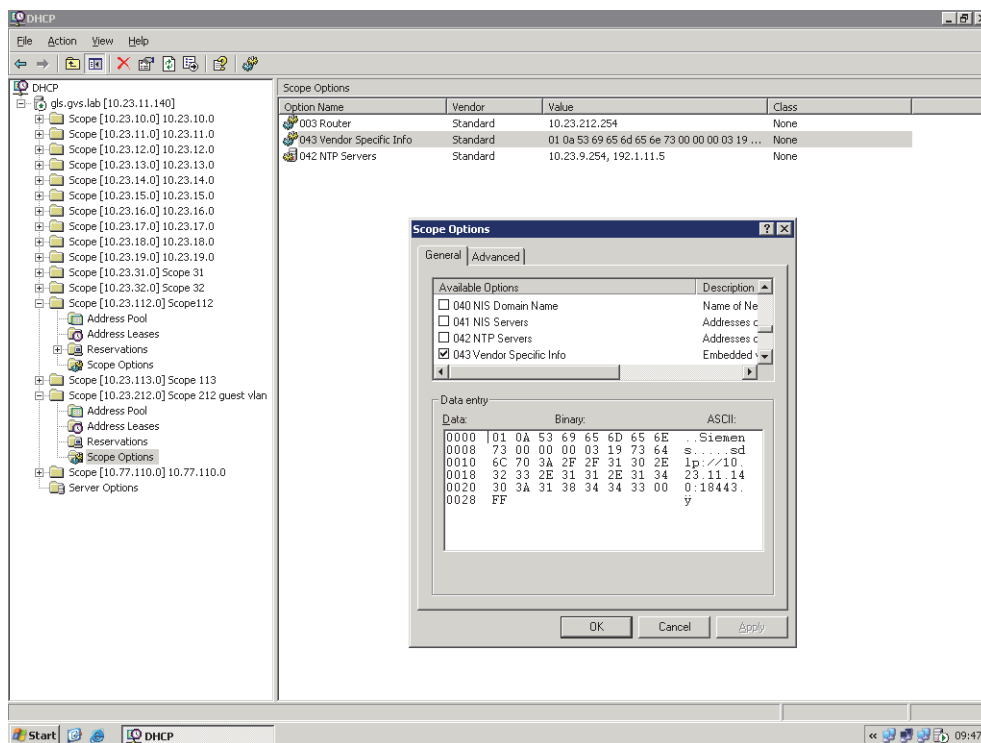
Once you have opened the Deployment Service in a browser, proceed as follows:

1. Go to Profile Management > Device Profile
2. Either search for an existing device profile using the search function or create a new one.
3. In the "Templates" tab, add the previously created template of the IEEE 802.1X tab (→ Seite 57) to the selected profile.
4. If you want the current profile to be the default profile, ensure that the "Default Profile" button is activated.
5. The configuration data in a profile is assigned to certain terminals via virtual devices. From the DLS's point of view, these are complete devices which will later be assigned a physical device and all the configuration parameters of the virtual device are applied to the physical device. For the different ways to create virtual devices and to change the assignment between virtual and physical devices, please refer to the "Workpoint Autoconfiguration (Plug & Play)" section in the DLS administration manual.

DHCP Address Pool (Scope)

If the start address is sent following the DHCP request, the gateway address is set to 10.12.212.254 (gateway presetting for VLAN 212). Using this address, the DHCP address space 10.23.212.0 is available.

The following screenshot shows the DHCP address pool, which makes it possible to provide an IP address (in this case 10.23.212.1) and the "DLS IP address" so that DLS can be run.



Switch Configuration using Example of Cisco Catalyst 3560



If you intend to configure User Authentication with enterasys switch please refer to:

<http://wiki.unify.com/wiki/enterasys-CUA>

Limitations

Testing is not carried out with other RADIUS servers like IAS or CISCO RADIUS.

If the IAS RADIUS test is necessary, it will be planned.

ACL list of FreeRADIUS is outside of this scope.

Only one PC behind the phone is possible.

If the phone has voice VLAN and the switch did not receive the "cisco-av-pair" string "device-traffic-class=voice", the Cisco switch goes into a violation state and the port is deactivated (as described).

The Plug & Play function can work in two different modes.

VOICE VLAN transmission over DHCP

MAB and EAP-TLS must be completed with `Cisco-AVPair = "device-traffic-class=voice"`.

Not recommended

VOICE VLAN transmission over DLS

MAB without Cisco-AVPair, EAP-TLS with `Cisco-AVPair = "device-traffic-class=voice"`

TRACE and Debug FreeRADIUS are designed for Plug & Play (not recommended scenario).

Configuration

Cisco configuration (port used fa0/12)

```
version 12.2
no service pad
service timestamps debug datetime
service timestamps log datetime
service password-encryption
!
hostname Switch
!
logging buffered 65535 debugging
enable secret 5 $1$ffD2$IsDN7o4qaMWo9nTctonq61
!
username cisco password 7 01100F175804
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
!
aaa session-id common
clock timezone utc 1
clock summer-time CEST recurring last Sun Mar 2:00 last Sun Oct 2:00
system mtu routing 1500
ip subnet-zero
no ip domain-lookup
ip domain-name GVS.LAB
ip dhcp excluded-address 10.23.12.254
ip dhcp excluded-address 10.23.12.1 10.23.12.100
!
!
dot1x system-auth-control
no file verify auto
!
spanning-tree mode mst
spanning-tree extend system-id
!
spanning-tree mst configuration
    name GVSLAB
!
!
vlan internal allocation policy ascending
```

```
!  
!  
interface FastEthernet0/1  
  switchport access vlan 12  
  switchport mode access  
  duplex half  
  spanning-tree portfast  
!  
.  
!  
interface FastEthernet0/12  
  switchport access vlan 112  
  switchport mode access  
  switchport voice vlan 12  
  dot1x mac-auth-bypass eap  
  dot1x pae authenticator  
  dot1x port-control auto  
  dot1x host-mode multi-domain  
  dot1x timeout quiet-period 20  
  dot1x timeout tx-period 10  
  spanning-tree portfast  
!  
.  
.  
!  
!  
interface FastEthernet0/23  
  switchport access vlan 12  
  switchport trunk encapsulation dot1q  
  switchport mode trunk  
  spanning-tree portfast  
!  
interface FastEthernet0/24  
  description --- Trunk to GVSLAB_r01 int fa0/14 ---  
  switchport trunk pruning vlan none  
!  
!  
interface Vlan1  
  ip address 10.23.9.2 255.255.255.0  
!  
ip default-gateway 10.23.9.254  
ip classless  
ip http server  
!
```

```
!  
ip access-list extended DLSServerOnly  
!  
radius-server host 10.23.12.99 auth-port 1812 acct-port 1813 key 7 1213091D515A5E577E7E  
radius-server source-ports 1645-1646  
!  
control-plane  
!  
!  
line con 0  
  password 7 030954090F03285857  
line vty 0 4  
  password 7 030954090F03285857  
line vty 5 15  
  exec-timeout 30 0  
  password 7 030954090F03285857  
!  
!  
monitor session 1 source interface Fa0/12, Fa0/19  
monitor session 1 destination interface Fa0/23 encapsulation replicate ingress untagged  
vlan 112  
ntp clock-period 36028550  
ntp server 10.23.9.254  
end
```

Plug & Play Function

Plug & Play function with VLAN transmission via DLS

The phone starts without certificate (factory reset).

The phone boots.

The phone sends <<DHCP discover>> in untagged frame.

With the Cisco switch, the Data VLAN is in blocked state and the Voice VLAN in learning state.

The Cisco switch sends an EAP <<request identity>> to the phone.

The phone does not answer (no certificates).

On no answer -> dot1x timeout in the Cisco switch.

On dot1x timeout, the Cisco switch sends <<Access request>> to the RADIUS (MAB function) (MAB = MAC Authentication Bypass).

RADIUS returns <<Access accept>> (because PAP was included in USER list -> see user list in "FreeRADIUS configuration (user file)").

Cisco adds a TCAM entry for the phone to the DATA VLAN.

DATA VLAN IS OPEN.

The phone continues to send <<DHCP discover>>. This DHCP message is now sent on the DATA VLAN to the DHCP scope for DATA (DHCP server).

The phone receives an IP address in the DATA VLAN scope (STILL NO VOICE VLAN).

The phone reaches the DLS (Plug & play active).

The phone receives from DLS the CERTIFICATES, the VOICE VLAN + other items.

The phone reboots with certificates in VOICE VLAN.

The Voice VLAN is in learning state in the Cisco switch.

The Cisco switch sends an EAP <<request identity>> to the phone.

As the certificates are now configured in the phone, the phone returns a <<response identity>> (tagged frame) to the switch with the "CN" from the certificate as user name.

→ RADIUS responds to this message with "Access accept" (as the EAP-TLS FreeRADIUS and the CN from the certificate were added to the USER list). Certificate negotiation now commences. For this user, the string "cisco-av-pair=device-traffic-class=voice" is added and returned to the Cisco switch. With this string, Cisco removes the TCAM entry for the Data VLAN and adds the Phone TCAM entry for the VOICE VLAN.

VOICE VLAN IS OPEN.

The phone continues to send <<DHCP discover>>. This DHCP is now sent via the VOICE VLAN (tagged frame). The phone receives from the DHCP VOICE VLAN scope all the items for the registering SIP server.

Phones and PC interoperability

Example: Phone has certificate but PC has no certificate

Switch#show dot1x interface fastEthernet 0/12 det

Dot1x Info for FastEthernet0/12

PAE	=	AUTHENTICATOR
PortControl	=	AUTO
ControlDirection	=	Both
HostMode	=	MULTI_DOMAIN
ReAuthentication	=	Disabled
QuietPeriod	=	20
ServerTimeout	=	30
SuppTimeout	=	30
ReAuthPeriod	=	3600 (Locally configured)
ReAuthMax	=	2

MaxReq	=	2
TxPeriod	=	10
RateLimitPeriod	=	0
Mac-Auth-Bypass	=	Enabled (EAP)

Dot1x Authenticator Client List

Domain	=	DATA
Supplicant	=	0004.7611.8a14
Auth SM State	=	AUTHENTICATED
Auth BEND SM Stat	=	IDLE
Port Status	=	AUTHORIZED
Authentication Method	=	MAB
Authorized By	=	Authentication Server
Vlan Policy	=	N/A

Domain	=	VOICE
Supplicant	=	0001.e326.1dfb
Auth SM State	=	AUTHENTICATED
Auth BEND SM Stat	=	IDLE
Port Status	=	AUTHORIZED
Authentication Method	=	Dot1x
Authorized By	=	Authentication Server

Location or Network Change

When the VLAN ID for the Voice network is to be changed, one has to consider whether the Voice VLAN ID is configured manually or dynamically (LLDP-MED or DHCP).

Misconfiguration of the Voice VLAN ID by choosing an incorrect VID can block network access (which is needed for remote configuration via DLS or WebM).

In such a case, a correction can usually only be made via the phone's local admin menu, or by temporarily configuring the access switch port with the "incorrect" Voice VLAN ID and subsequently correcting it, which can be done remotely.

Scenario:

1. 802.1X is used as before, the RADIUS server remains the same, but the Voice VLAN ID changes:

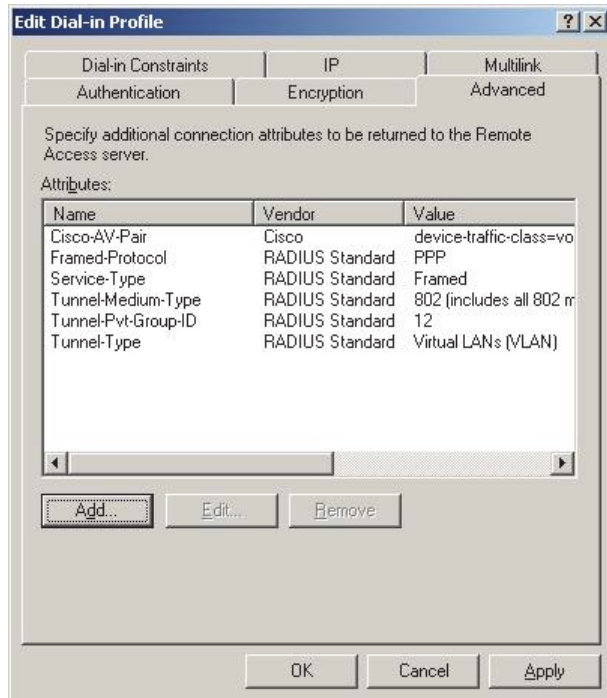
The port at the access switch or the access switch itself changes.

The new access switch port must be configured for authentication (802.1X enabled) and the VLANs (Guest VLAN, AuthFail VLAN, Data VLAN and Voice VLAN) must be configured appropriately.

Important: With Cisco access switches, RADIUS provides the "Voice VLAN ID" and the "device-traffic-class" as additional information (for example: Win2kx IAS => Remote Access Policy, FreeRADIUS => raddb/users).

The VLAN ID configured on the new access switch port must be identical to the Tunnel-Pvt-Group-ID on the IAS and device-traffic-class must be set to "voice".

IAS-Remote Access Policy



The same applies to FreeRADIUS.

```
/etc/raddb/users:
# Entry for Cisco 3650
# 0001e32e0327 Auth-Type == EAP
0001e32e0327
    Tunnel-Type = 13,
    Tunnel-Medium-Type = 6,
```

```
Tunnel-Private-Group-ID = 12,
Cisco-AVPair = "device-traffic-class=voice"
```

2. 802.1X is not used or not activated at the access switch:

As the certificates on the phone are probably not deleted, a non-recurring additional delay of 3x30 seconds will occur after reboot before the phone is ready.

This is due to the three retries which are required by the 802.1X protocol before the internal status can be set to "Authenticated".

If 802.1X is activated at the new access switch port, but the status is set to "force-authorized", there will be no delay because the access switch will send "EAP-Success" immediately.

So, the 802.1X authentication delay can be circumvented for the time being by using "force-authorized".

3. A different RADIUS server is used

The RADIUS certificate is changed.

However, if the root CA is the same as the one that signed the "old" RADIUS server, nothing will change on the phone side (RADIUS server CA certificates 1 and 2 remain unchanged).

Nevertheless, the "new" RADIUS server must be able to access the phone certificates for validation (Win2kx => Active Directory, FreeRADIUS => raddb/eap.conf).

If the configuration of the phone is to be changed only with regard to IP and Voice VLAN ID (SIP server, certificates, and so on remain unchanged), it is recommended to assign the Voice VLAN ID via LLDP-MED and the IP address via DHCP.

For a complete configuration change, it might be feasible to initiate a factory reset first and then use the Plug & Play capability with templates for this "new" network (note that with DLSv3 and Mobility, patch MRH65227 is required).



Guest VLAN / Authfail VLAN ...

Can be reached by phone or PC (connected to phone) if no authentication is possible.

If a VLAN ID is set on the phone, however, VLAN tagging prevents access to the Guest VLAN/Authfail VLAN (= untagged).

Data VLAN ... VLAN

This is usually reached by PCs (connected to the phone) if they authenticate successfully.

Voice VLAN ... VLAN

This is reserved for voice and voice signaling. Reached by the phone if authentication has been successful and the Voice VLAN ID has been set.

If the Voice VLAN ID was not set but authentication was successful, the phone will be assigned to the Data VLAN (untagged) => Error

Examples of Switch Configurations

Switch example 1: "Cisco configuration"

```
GVSLAB_s02#show dot1x interface fastEthernet 0/12
Supplicant MAC <Not Applicable>
AuthSM State           = CONNECTING
BendSM State           = IDLE
Posture                 = N/A
  ReAuthPeriod         = 15 Seconds (Locally Configured)
  ReAuthAction         = Reauthenticate
  TimeToNextReauth     = N/A
PortStatus             = UNAUTHORIZED
MaxReq                 = 2
MaxAuthReq             = 2
HostMode               = Multi
PortControl            = Auto
ControlDirection       = Both
QuietPeriod            = 60 Seconds
Re-authentication      = Enabled
ReAuthPeriod           = 15 Seconds
ServerTimeout          = 30 Seconds
SuppTimeout            = 30 Seconds
TxPeriod               = 30 Seconds
Guest-Vlan = 212
AuthFail-Vlan          = 0
AuthFail-Max-Attempts = 3
Critical Port          = Disabled


GVSLAB_s02#show dot1x interface fastEthernet 0/12
Supplicant MAC <Not Applicable>
AuthSM State= AUTHENTICATED(GUEST_VLAN)
BendSM State           = IDLE
Posture                 = N/A
  ReAuthPeriod         = 15 Seconds (Locally Configured)
  ReAuthAction         = Reauthenticate
  TimeToNextReauth     = N/A
PortStatus             = AUTHORIZED(GUEST-VLAN)
MaxReq                 = 2
MaxAuthReq             = 2
HostMode               = Multi(GUEST VLAN)
```



This table shows the port configuration (GVSLAB_s02) where the phone (→ Supplicant) is connected.

```
!
interface FastEthernet0/12
  switchport access vlan 112
  switchport mode access
  switchport voice vlan 12
  dot1x port-control auto
  dot1x host-mode multi-host
  dot1x timeout reauth-period 15
  dot1x guest-vlan 212
  dot1x reauthentication
  spanning-tree portfast
```

At this point it is necessary to enable the guest VLAN (address space 212) to receive execution rights on the DHCP and DLS server.

The VLAN interconnection is created in the router. An → ACL is generated to assign only execution rights for the DLS (10.23.11.140) and the DHCP (bootps and bootpc) to the Guest VLAN.

The setting **dot1x** → Host Mode →  and an 802.1X client authenticated at the first VLAN client indicates that other clients are possible without restriction on the "Voice VLAN" if 802.1X authentication was successful on the first VLAN.

/1/ If you set **dot1x host mode** →  , only one 802.1X client is permitted on the first VLAN; other devices are blocked.

If you set **dot1x host mode** → Multi-Domain, the telephone and PC must authenticate themselves individually.

Ensure that **port-control** is set to "auto".

```
GVSLAB_r01#show run
Building configuration...
!
interface Vlan212
 ip address 10.23.212.254 255.255.255.0
 ip access-group PermitDLSServerOnly in
 ip helper-address 10.23.11.140
!
ip access-list extended PermitDLSServerOnly
 permit ip 10.23.212.0 0.0.0.255 host 10.23.11.140
 permit ip 10.23.212.0 0.0.0.255 host 10.23.12.1
 permit udp any any range bootps bootpc
!
```

Switch example 2: "Enterasys Matrix N1 Platinum Configuration"

```
M M A T R I X   N 1   P L A T I N U M
Command Line Interface
Enterasys Networks, Inc.
50 Minuteman Rd.
Andover, MA 01810-1008 USA
Phone: +1 978 684 1000
E-mail: support@enterasys.com
Website: http://www.enterasys.com
(c) Copyright Enterasys Networks, Inc. 2007
Chassis Serial Number: 06125174630P
Chassis Firmware Revision: 05.42.06
Matrix N1 Platinum(su)->show config
This command shows non-default configurations only.
Use 'show config all' to show both default and non-default configurations.
begin
# ***** NON-DEFAULT CONFIGURATION *****
# ip
set ip address 10.23.9.96 mask 255.255.255.0
set ip route default 10.23.9.254
# arp
# authentication
# banner
# cdp
# cep
# ciscodp
# cli
# console
# cos port-config
# cos port-resource
# cos reference
# cos settings
# cos state
# dot1x
set dot1x enable
set dot1x auth-config authcontrolled-portcontrol forced-auth fe.1.1
set dot1x auth-config reauthperiod 120 fe.1.7
set dot1x auth-config reauthperiod 120 fe.1.8
set dot1x auth-config reauthperiod 120 fe.1.11
set dot1x auth-config reauthperiod 120 fe.1.12
set dot1x auth-config reauthenabled true fe.1.7-8,11-12 ***** Ports Guest *****
# flowlimit
# forcelinkdown
# garp
# gvrp
# history
```

```
# history
# igmp
# inlinepower
# lacp
set lacp disable
# length
# license
# line-editor
# linkflap
# lldp
# logging
set logging application RtrAcl level 8
set logging application CLI level 8
set logging application SNMP level 8
set logging application Webview level 8
set logging application System level 8
set logging application RtrFe level 8
set logging application Trace level 8
set logging application RtrLSNat level 8
set logging application FlowLimit level 8
set logging application UPN level 8
set logging application AAA level 8
set logging application Router level 8
set logging application AddrNtfy level 8
# logout
# mac
# macauthentication
set macauthentication enable
set macauthentication password demo
set macauthentication port enable fe.1.11-12
set macauthentication quietperiod 30 fe.1.11-12
set macauthentication reauthperiod 120 fe.1.11-12
set macauthentication reauthentication enable fe.1.11-12
# maclock
# mgmt-auth-notify
# movedaddrtrap
# mtu
# multiauth
set multiauth mode multi
set multiauth precedence dot1x mac pwa cep
set multiauth port mode auth-reqd fe.1.12
***** Authentication is always required *****
# netflow
# newaddrtrap
# nodealias
# physical
```

```

# policy
set policy profile 1 name "allow access voice" pvid-status enable pvid 12 (Voice VLAN)
set policy profile 2 name "allow access data" pvid-status enable pvid 112 (DATA VLAN)
set policy profile 3 name "allow access guest" pvid-status enable pvid 212 (GUEST VLAN)
set policy rule admin-profile port fe.1.7 mask 16 port-string fe.1.7 admin-pid 3
set policy rule admin-profile port fe.1.8 mask 16 port-string fe.1.8 admin-pid 3
set policy rule admin-profile port fe.1.11 mask 16 port-string fe.1.11 admin-pid 3
set policy rule admin-profile port fe.1.12 mask 16 port-string fe.1.12 admin-pid 3
**** Ports 7, 8, 11 and 12 should use Profile 3, that is, go to the Guest VLAN. ****
set policy autoclear enable
set policy autoclear profile enable
set policy maptable response both
!
# port
set port mirroring create fe.1.11 fe.1.2 both
set port mirroring create fe.1.12 fe.1.2 both
set port mirroring disable fe.1.12 fe.1.2
set port vlan fe.1.2 12 *****
set port vlan fe.1.7 12
set port vlan fe.1.8 12 Assign to VLAN 12 = VOICE VLAN
set port vlan fe.1.11 12
set port vlan fe.1.12 12 *****
# prompt
# pwa
set pwa enable
set pwa enhancedmode enable
set pwa gueststatus authnone
set pwa protocol chap
set pwa portcontrol enable fe.1.12
# rad
# radius
set radius enable
set radius server 1 10.23.12.99 1812 :dcf48ed62c5bfb984158d7648a9cfed2f325fbb7:
# rmon alarm
# rmon capture
# rmon channel
# rmon event
# rmon filter
# rmon history
# rmon host
# rmon matrix
# rmon stats
# rmon topN
# router
# smon

```

```
# snmp
set snmp access groupRW security-model v1 exact read All write All notify All
set snmp access groupRW security-model v2c exact read All write All notify All
set snmp community public
set snmp group groupRW user public security-model v1
set snmp group groupRW user public security-model v2c
set snmp view viewname All subtree 1
set snmp view viewname All subtree 0.0

# snmp
# spantree
# ssh
# summertime
# system
set system login enterasys read-only disable password :c8f6b8ae63473088dcf9c7e80
0a245d445b50d62:
set system login mobility read-only disable password :29c6bff7ed3e5e334a43253c13
6cb9a8c5a40cb9:
# tacacs
# telnet
# timezone
# vlan
set vlan create 12,112,212 ***** Create VLAN *****
set vlan name 12 VOICE
set vlan name 112 DATA
set vlan name 212 GUEST *****
clear vlan egress 1 fe.1.2,7-9,11-12
set vlan egress 1 lag.0.1-48;host.0.1;fe.1.1,3-6,10,13-48 untagged
set vlan egress 12 fe.1.1,11-12 tagged ***** sign port 12 to tagged VLAN 12 *****
set vlan egress 12 fe.1.2,7-9,13 untagged
set vlan egress 112 fe.1.1 tagged
set vlan egress 112 fe.1.7-9,11-13 untagged ***** sign port 12 to untagged VLAN 112 **
set vlan egress 212 fe.1.1 tagged
set vlan egress 212 fe.1.11-12 untagged ***** sign port 12 to untagged VLAN 212 *****
set vlan dynamic egress 12,112,212 enable
***** fe 1.1 is the connection to the router *****
# vlanauthorization
# webview
# width
end
```

Switch example 3: "ProCurve configuration"

```
running configuration:
; J8164A Configuration Editor; Created on release #H.10.50
hostname "ProCurve Switch 2626-PWR"
vlan 1
name "DEFAULT_VLAN" (Guest VLAN for unauthorized access)
untagged 25-26
ip address 192.168.1.20 255.255.255.0
no untagged 1-24
exit
vlan 202
name "voiceVlanSN2" (Voice VLAN for Phones)
ip address 192.168.6.2 255.255.255.0
tagged 1-26
exit
vlan 2 (Data VLAN for PCs)
name "Testust1"
untagged 1-24
ip address 192.168.2.2 255.255.255.0
tagged 25
exit
aaa authentication port-access eap-radius Configuration 802.1X Authentication Method: eap-radius)
radius-server host 192.168.1.2
radius-server key global_key_string
aaa port-access authenticator 14,17-18,20 Ports 14, 17,18,20 Make available for 802.1X authentication.
aaa port-access authenticator 14 reauth-period 3600 Authentication checked after 1 hour.
aaa port-access authenticator 14 unauth-vid 1 Clients on port 14 which cannot be authenticated only have access to the Guest VLAN with access to the DLS. (Certificate Download)
aaa port-access authenticator 14 client-limit 3 Number of permitted authenticated devices. (On our 2626-PWR with FW H.10.50, 3 must be entered here if access is to be granted to 2 devices (phone and PC))
aaa port-access authenticator 17 reauth-period 3600 No Guest VLAN is configured on port 17 as a PC is connected behind the phone.
aaa port-access authenticator 17 client-limit 3
aaa port-access authenticator 18 reauth-period 3600
aaa port-access authenticator 18 unauth-vid 1
aaa port-access authenticator 18 client-limit 3
aaa port-access authenticator 20 reauth-period 3600
aaa port-access authenticator 20 unauth-vid 1
aaa port-access authenticator 20 client-limit 3
aaa port-access authenticator active "Activate" 802.1X authentication.
```

PEAP Implementation

Openstage SIP phones used to only support the EAP-TLS authentication method when using port based authentication (801.1x). New in SW version V3R0 is the Protected Extensible Authentication Protocol (Protected EAP or PEAP) as a possible authentication method.

PEAP is an authentication method used extensively in Microsoft environments.

Now the dot1x Supplicant used in Openstage IP phones (wpa_supplicant) supports both PEAP (PEAPv0/EAP-MSCHAPv2) and EAP-TLS.

To further maintain compatibility with current field releases the phone will default to EAP-TLS mode.

Depending if the phone contains dot1x credentials (either EAP-TLS or PEAP) the phone starts the wpa_supplicant in according mode.

802.1x Network Access Protection overview

The IEEE 802.1X-2001 and 802.1X-2004 standards define port-based user authentication methods used when accessing both wired and wireless network infrastructures. An 802.1X deployment consists of three major components:

Supplicant

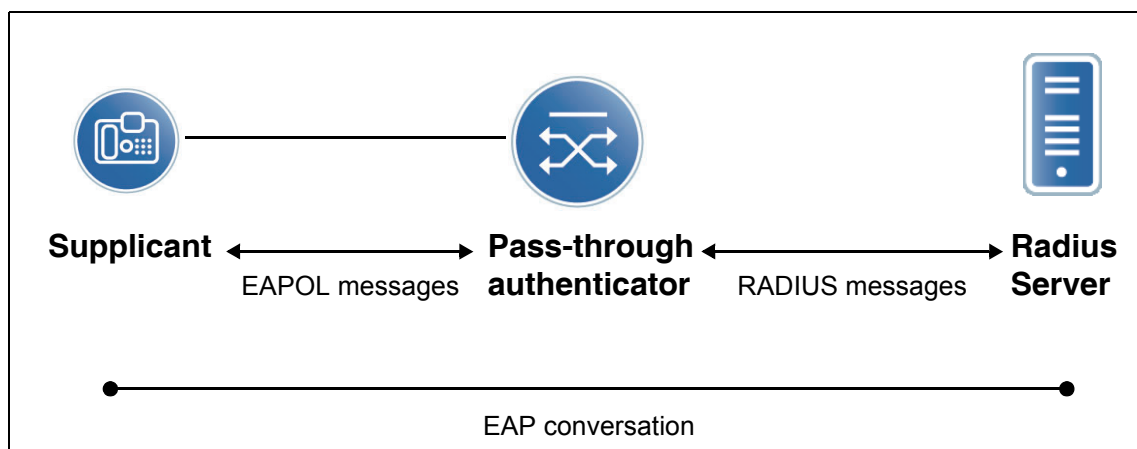
A computer that requests access to a network. The supplicant is attached to the pass-through authenticator.

Pass-through authenticator

Typically a switch or wireless AP that enforces port-based authentication.

Authentication server

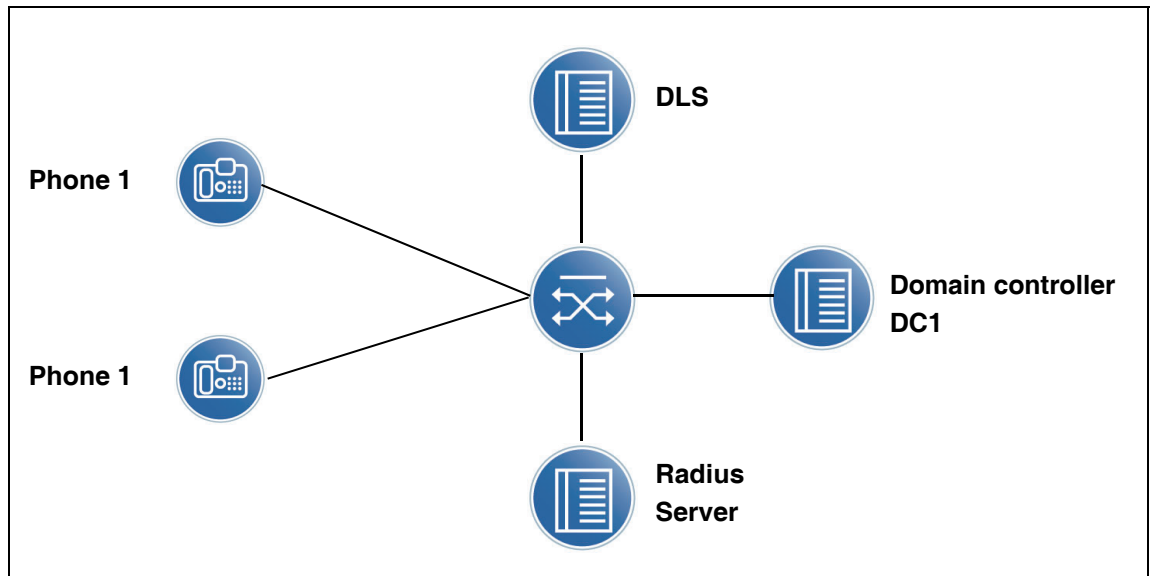
A computer that authenticates and authorizes a supplicant connection attempt on behalf of the pass-through authenticator. Supplicant credentials are validated by the authentication server using an authentication service, such as the Remote Authentication Dial-In User Service (RADIUS).



Requirements

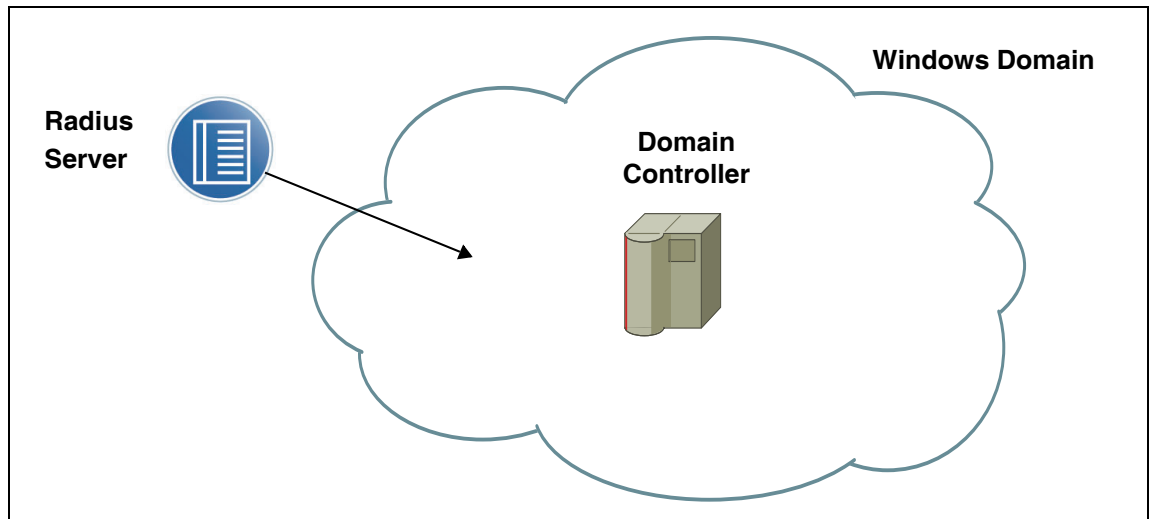
- Computer with Windows Server 2008 R2 or later
- Layer 2 or layer 3 switch that supports 802.1X port-based authentication and RADIUS tunnel attributes for VLAN assignment
- OpenStage Phone with V2R0.59.0 or later
- DLS with V6R0.16.0 or later
- Server running Windows Server 2003 or later version, the Server is configured as a domain controller with Active Directory service.

Example Configuration Overview (LAB environment)

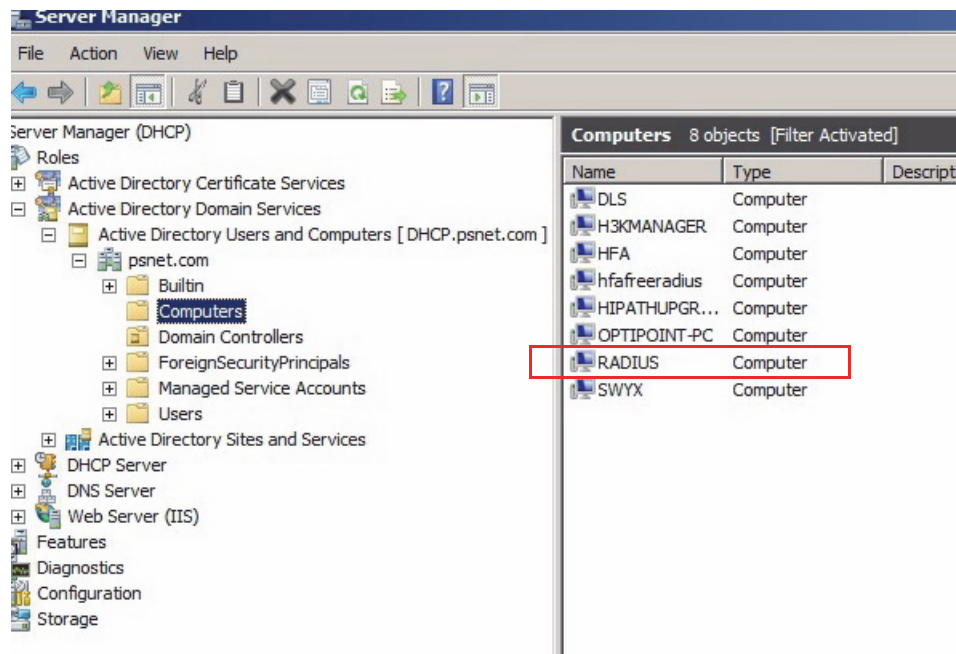


Configuration

Add the Radius-Server to the Domain

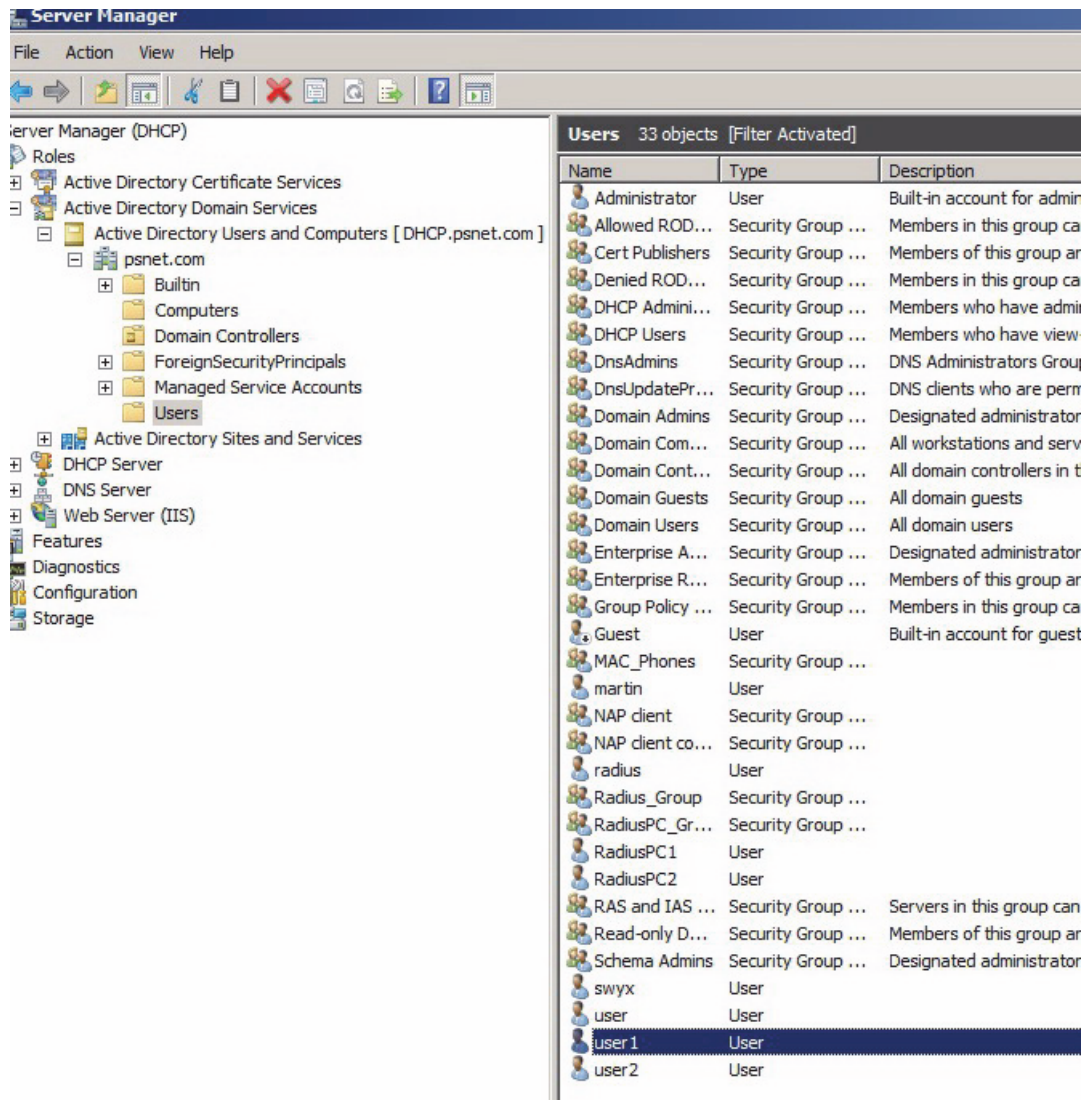


Join the RADIUS-Server to the Domain



Create a user account in Active Directory

E.G. user 1 with password e.g. 123456



Server Manager (DHCP)

Roles

- Active Directory Certificate Services
- Active Directory Domain Services
 - Active Directory Users and Computers [DHCP.psnet.com]
 - psnet.com
 - Builtin
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipals
 - Managed Service Accounts
 - Users**
 - Active Directory Sites and Services
- DHCP Server
- DNS Server
- Web Server (IIS)

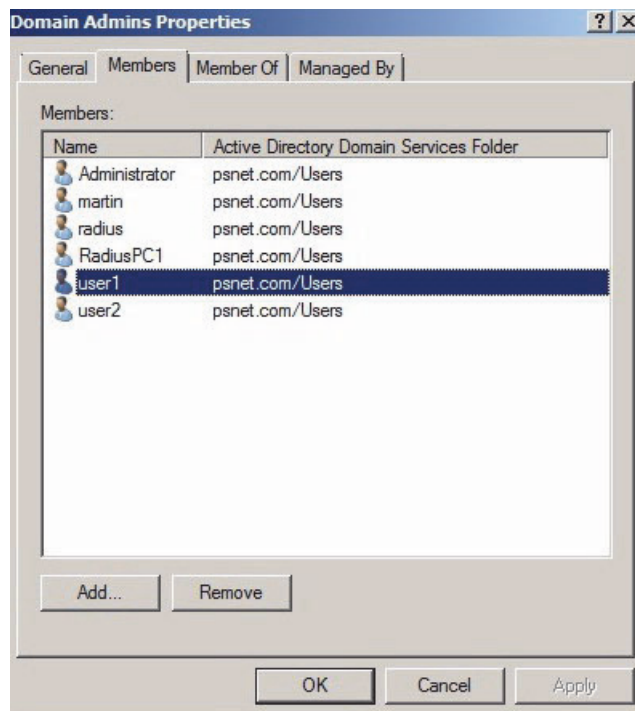
Features

- Diagnostics
- Configuration
- Storage

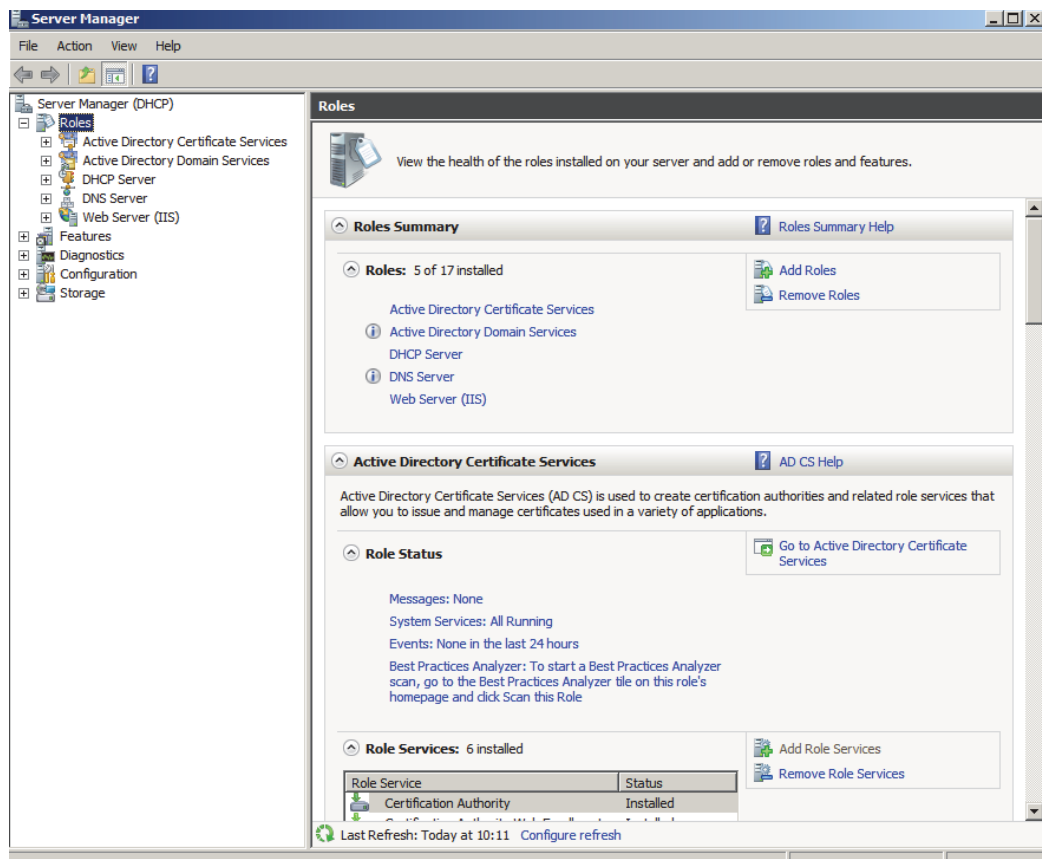
Users 33 objects [Filter Activated]

Name	Type	Description
Administrator	User	Built-in account for admin
Allowed ROD...	Security Group ...	Members in this group ca
Cert Publishers	Security Group ...	Members of this group ar
Denied ROD...	Security Group ...	Members in this group ca
DHCP Admini...	Security Group ...	Members who have admini
DHCP Users	Security Group ...	Members who have view:
DnsAdmins	Security Group ...	DNS Administrators Grou
DnsUpdatePr...	Security Group ...	DNS clients who are perr
Domain Admins	Security Group ...	Designated administrator
Domain Com...	Security Group ...	All workstations and serv
Domain Cont...	Security Group ...	All domain controllers in t
Domain Guests	Security Group ...	All domain guests
Domain Users	Security Group ...	All domain users
Enterprise A...	Security Group ...	Designated administrator
Enterprise R...	Security Group ...	Members of this group ar
Group Policy ...	Security Group ...	Members in this group ca
Guest	User	Built-in account for guest
MAC_Phones	Security Group ...	
martin	User	
NAP client	Security Group ...	
NAP client co...	Security Group ...	
radius	User	
Radius_Group	Security Group ...	
RadiusPC_Gr...	Security Group ...	
RadiusPC1	User	
RadiusPC2	User	
RAS and IAS ...	Security Group ...	Servers in this group can
Read-only D...	Security Group ...	Members of this group ar
Schema Admins	Security Group ...	Designated administrator
swyx	User	
user	User	
user 1	User	
user 2	User	

Add user1 to the Domain Admins group



Set up an enterprise root CA



- Log on to DC1 as a domain administrator
- Click **Start**, point to **Administrative Tools** and then click **Server Manager**.
- In the **Roles Summary** section click **Add roles**.

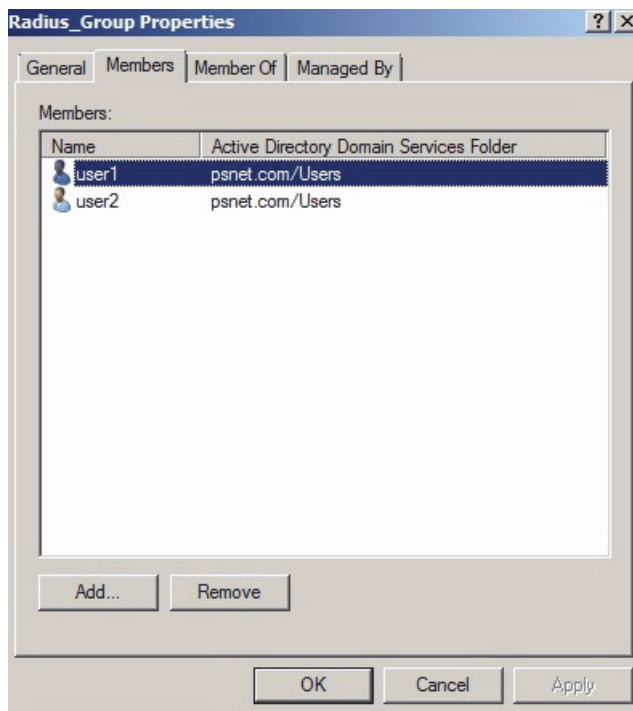
- On the **Select Server roles** page, select the **Active Directory Certificate Service** check box. Click **Next** to times.
- On the **Specify Setup Type** page, click **Enterprise**, and then click **Next**.
- On the **Specify CA Type** page, click **Root CA**, and then click **Next**.
- On the **Set Up Private key** and **Configure Cryptography for CA** pages, you can configure optional configuration settings, including cryptographic service providers. However, for basic testing purposes, accept the default values by clicking **Next** twice.

Install an enterprise root CA



- In the **Common name for this CA** box, type the common name of this CA, **RadiusCA**, and then click **Next**.
- On the **Set the Certificate Validity Period** page, accept the default validity duration or enter a validity duration you want for the RadiusCA and then click **Next**.
- On the **Configure Certificate Database** page, accept the default values or specify other storage locations for the certificate database and the certificate database log, and then click **Next**.
- After verifying the information on the **Confirm Installation Options** page, click **Install**.
- Review the information on the confirmation screen to verify that the installation was successful.

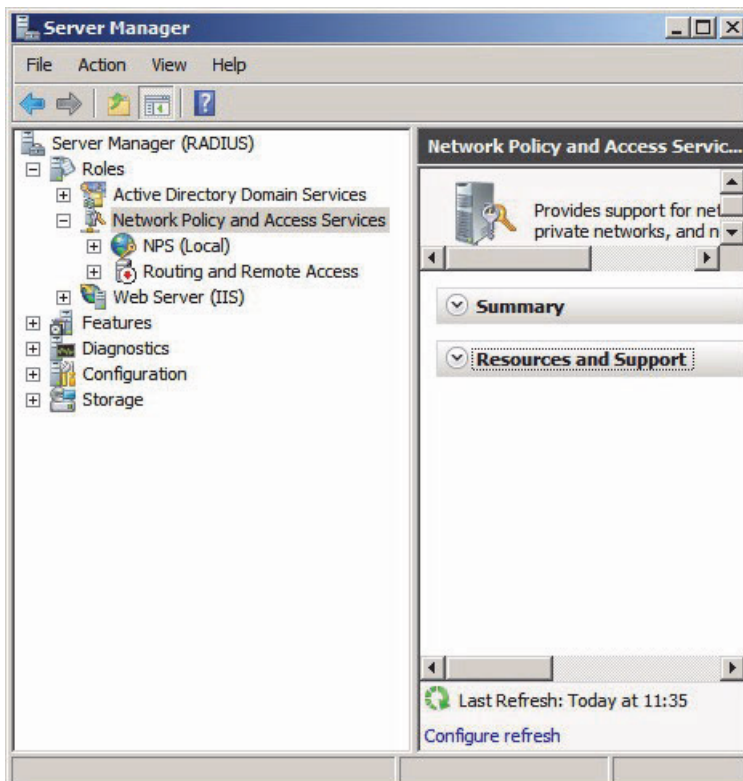
Create a security group



- In the Active Directory Users and Computers console tree, right-click **psnet.com** (domain-name), point to New, and then click **Group**.
- In the New **Object – Group** dialog box, under **Group name** type, type **Radius_Group**.
- Under Group scope, choose **Global**, under **Group type**, choose **Security**, and then click **OK**.
- Close the Active Directory Users and Computers console

Configure Network Policy Server on Radius-Server

Install the NPS server role

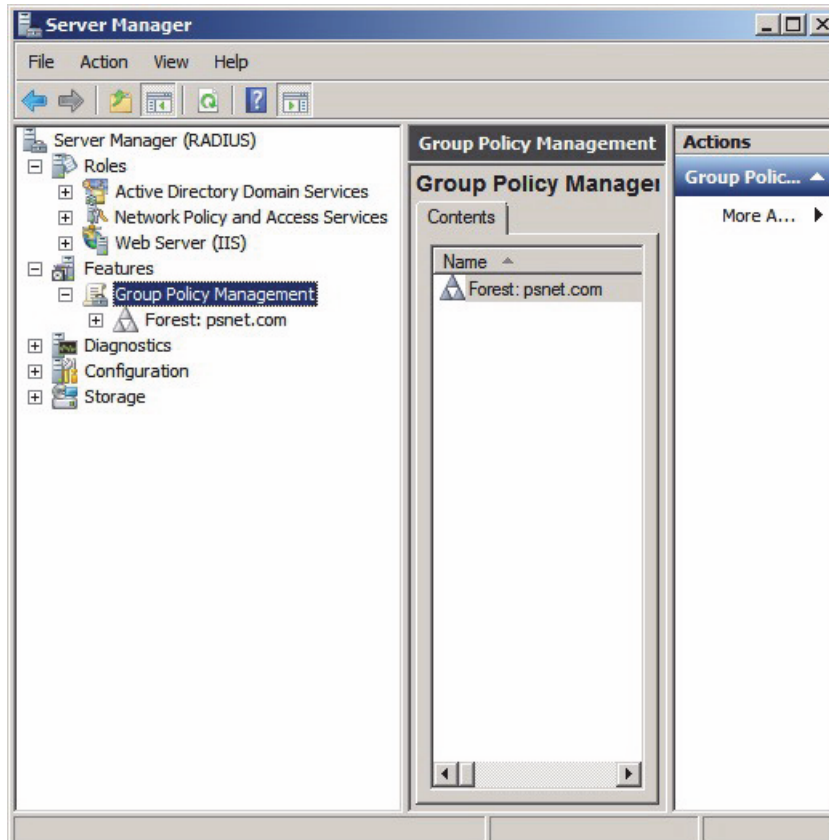


- Click **Start**, and then click **Server Manager**.
- Under **Roles Summary**, click **Add Roles**, and then click **Next**.
- Select the **Network Policy and Access Services** check box, and then click **Next** twice.
- Select the **Network Policy Server** check box, click **Next**, and then click **Install**.
- Verify the installation was successful, and then click **Close** to close the **Add Roles Wizard** dialog box.
- Leave Server Manager open for the following procedure.

Group Policy Management

Install the Group Management feature

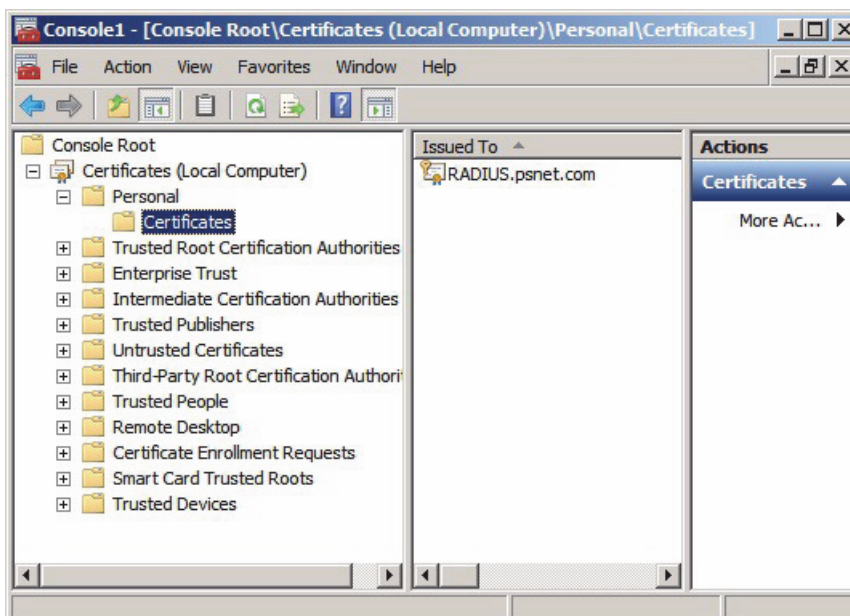
Group Policy will be used to configure NAP client settings. To access these settings, the Group Policy Management feature must be installed on a computer running Windows Server 2008.



- In Server Manager, under **Features Summary**, click **Add Features**.
- Select the **Group Policy Management** check box, click **Next**, and then click **Install**.
- Verify the installation was successful, and click **Close** to close the **Add Features Wizard** dialog box.
- Close Server Manager

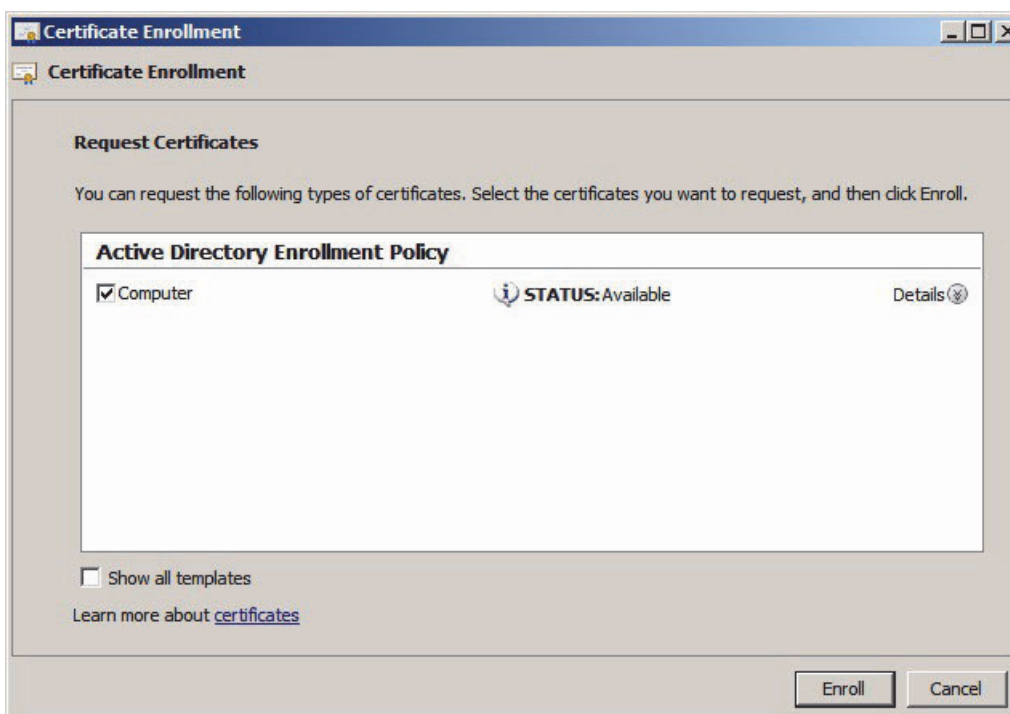
Certificate on NPS Radius Server

Obtain a computer certificate on NPS (1)



- Click **Start**. Click **Run** in **Open**, type **mmc**, and then press ENTER.
- On the **File** menu click **Add/Remove snap-in**.
- In the **Add or Remove Snap-ins** dialog box, click **Certificates**, click **Add**, select **Computer account**, click **Next**, and then click **Finish**.
- Click **OK** to close the **Add or Remove Snap-ins** dialog box.
- In the left pane, double-click **Certificates**, right-click **Personal**, point to **All Tasks**, and then click **Request New Certificate**.

Obtain a computer certificate on NPS (2)

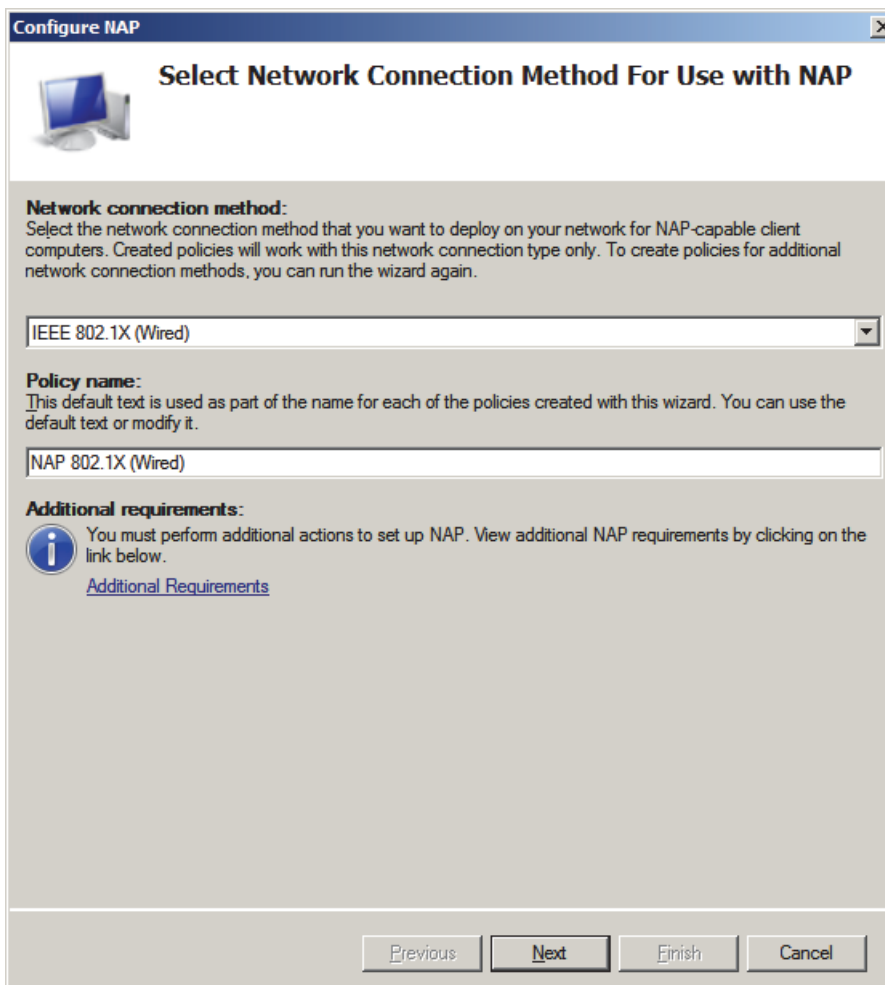


- The **Certificate Enrollment** dialog box opens. Click **Next**.

- On the Select **Certificate Enrollment Policy** page, select **Active Directory Enrollment Policy**, click **Next**, select **Computer**, and then click **Enroll**.
- Select the **Computer** check box and then click **Enroll**.
- Verify that **Succeeded** is displayed to indicate the status of certificate installation, and then click **Finish**.
- Close the **Console1** window.
- Click **No** when prompted to save console settings.

Configure NAP on the NPS Server

Select Network Connection Method



Configure NAP

Select Network Connection Method For Use with NAP

Network connection method:
Select the network connection method that you want to deploy on your network for NAP-capable client computers. Created policies will work with this network connection type only. To create policies for additional network connection methods, you can run the wizard again.

IEEE 802.1X (Wired)

Policy name:
This default text is used as part of the name for each of the policies created with this wizard. You can use the default text or modify it.

NAP 802.1X (Wired)

Additional requirements:
You must perform additional actions to set up NAP. View additional NAP requirements by clicking on the link below.
[Additional Requirements](#)

Previous Next Finish Cancel

- Click **Start**, click **Run**, type **nps.msc** and then press ENTER.
- In the Network Policy Server console tree, click **NPS (Local)**.
- In the details pane, under **Standard Configuration**, click **Configure NAP**. The NAP configuration wizard will start.
- On the selected **Network Connection Method for use with NAP** page, under **Network connection method**, select **IEEE 802.1X (Wired)**, and then click **Next**.
- On the **Specify 802.1X Authentication Switches** page, click **Add**.
- In the **New RADIUS Client** dialog box, under **Friendly name**, type **802.1X Switch**. Under **Address (IP or DNS)**, type 192.1.254.116 (IP-Address of the switch where the phones are connected)

Switch Properties

802.1X Switch Cisco 3560 Properties

Settings

☐ Select an existing template:

Phone 5004

Name and Address

Friendly name:

802.1X Switch Cisco 3560

Address (IP or DNS):

192.1.254.116 [Verify...](#)

Shared Secret

Select an existing Shared Secrets template:

None

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

☒ Manual ☐ Generate

Shared secret:

.....

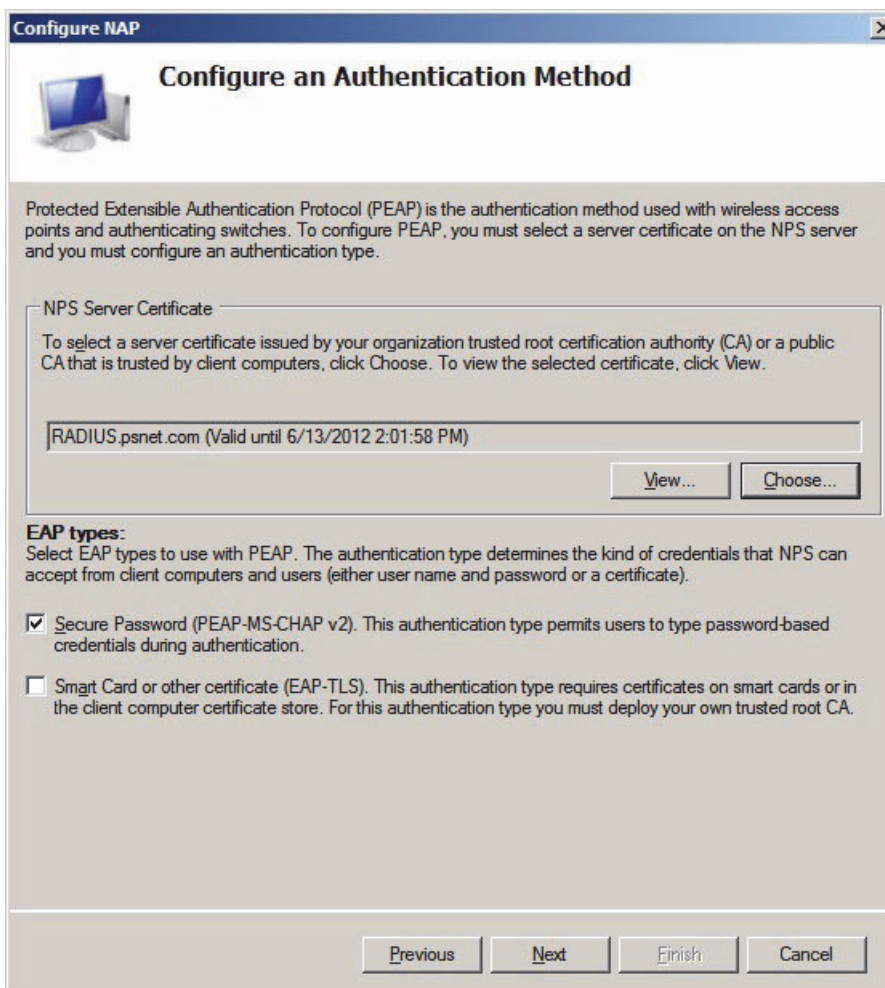
Confirm shared secret:

.....

OK Cancel Apply

- Under **Shared secret**, type a user defined password e.g. **secret**.
- Under **Confirm shared secret**, type **secret**, click **OK**, and then click **Next**.

Configure an Authentication Method



The screenshot shows the 'Configure an Authentication Method' window from the 'Configure NAP' wizard. The window has a title bar with 'Configure NAP' and a close button. Below the title bar is a small icon of a computer and the title 'Configure an Authentication Method'. The main text explains that Protected Extensible Authentication Protocol (PEAP) is used with wireless access points and switches, and that a server certificate must be selected on the NPS server and an authentication type configured. There is a section for 'NPS Server Certificate' with instructions to select a certificate issued by a trusted root certification authority (CA) or a public CA. A text box displays 'RADIUS.psnet.com (Valid until 6/13/2012 2:01:58 PM)'. Below this are 'View...' and 'Choose...' buttons. The 'EAP types' section instructs to select EAP types to use with PEAP. Two options are listed: 'Secure Password (PEAP-MS-CHAP v2)' which is selected with a checked checkbox, and 'Smart Card or other certificate (EAP-TLS)' which is not selected with an unchecked checkbox. At the bottom are 'Previous', 'Next', 'Finish', and 'Cancel' buttons.

Configure an Authentication Method

Protected Extensible Authentication Protocol (PEAP) is the authentication method used with wireless access points and authenticating switches. To configure PEAP, you must select a server certificate on the NPS server and you must configure an authentication type.

NPS Server Certificate

To select a server certificate issued by your organization trusted root certification authority (CA) or a public CA that is trusted by client computers, click Choose. To view the selected certificate, click View.

RADIUS.psnet.com (Valid until 6/13/2012 2:01:58 PM)

View... Choose...

EAP types:

Select EAP types to use with PEAP. The authentication type determines the kind of credentials that NPS can accept from client computers and users (either user name and password or a certificate).

☒ **Secure Password (PEAP-MS-CHAP v2).** This authentication type permits users to type password-based credentials during authentication.

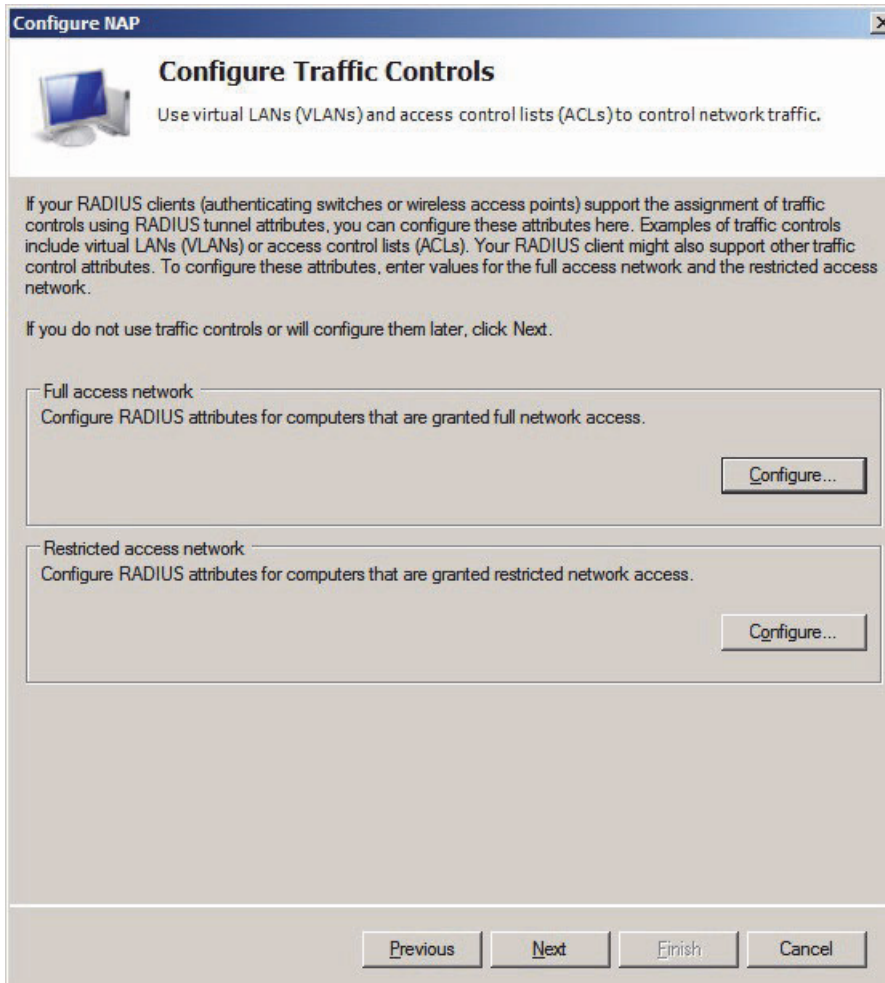
☐ **Smart Card or other certificate (EAP-TLS).** This authentication type requires certificates on smart cards or in the client computer certificate store. For this authentication type you must deploy your own trusted root CA.

Previous Next Finish Cancel

- On the **Configure User Groups and Machine Groups** page, click **Next**. You do not need to configure groups.
- On the **Configure an Authentication Method** page, confirm that a computer certificate obtained in the previous procedure is displayed under **NPS Server Certificate**, and that **Secure Password (PEAP-MSCHAP v2)** is selected under **EAP types**. Click **Next**.

Configure Traffic Controls

Use the following steps to configure VLAN properties for the compliant phones. In this example, VLAN ID 20 will be used for compliant phones.



Configure NAP

Configure Traffic Controls

Use virtual LANs (VLANs) and access control lists (ACLs) to control network traffic.

If your RADIUS clients (authenticating switches or wireless access points) support the assignment of traffic controls using RADIUS tunnel attributes, you can configure these attributes here. Examples of traffic controls include virtual LANs (VLANs) or access control lists (ACLs). Your RADIUS client might also support other traffic control attributes. To configure these attributes, enter values for the full access network and the restricted access network.

If you do not use traffic controls or will configure them later, click **Next**.

Full access network
Configure RADIUS attributes for computers that are granted full network access.

Restricted access network
Configure RADIUS attributes for computers that are granted restricted network access.

Previous **Next** **Finish** **Cancel**

On the **Configure Traffic Controls** page, under **Full access network**, click **Configure**.

Configure Radius Attributes: Tunnel-Type

Configure RADIUS Attributes

RADIUS Standard Attributes | Vendor-Specific Attributes

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.

Attributes:

Name	Value
Filter-Id	<not configured>
Tunnel-Type	<not configured>
Tunnel-Medium-Type	<not configured>
Tunnel-Pvt-Group-ID	<not configured>
Tunnel-Assignment-ID	<not configured>

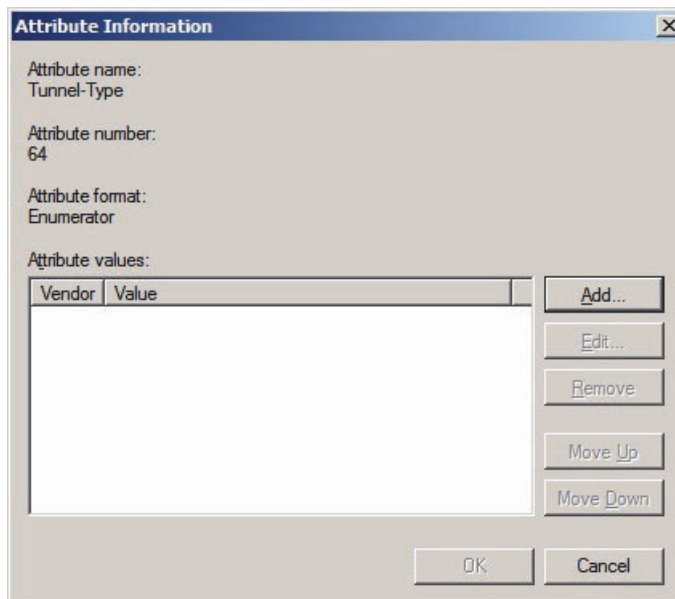
Description:
Specifies the tunneling protocols used.

Edit...

OK Cancel

In the **Configure RADIUS Attributes**, on the **RADIUS standard attributes** tab, click **Tunnel-Type**, and then click **Edit**.

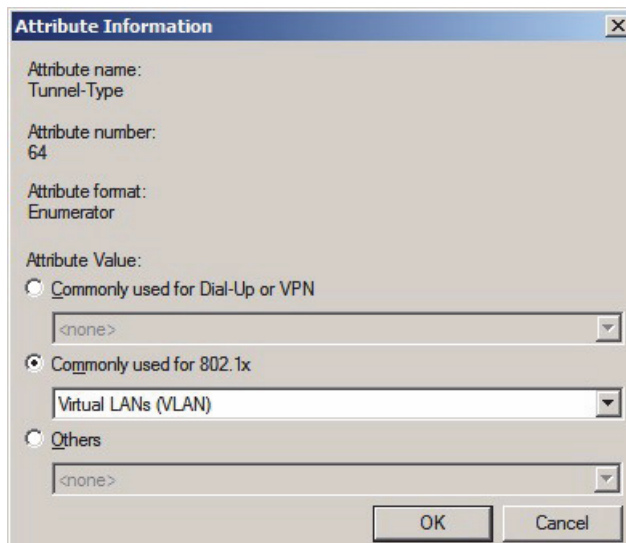
Configure Attribute Information: Tunnel-Type



The **Attribute Information** dialog box is shown. It contains the following fields and controls:

- Attribute name:** Tunnel-Type
- Attribute number:** 64
- Attribute format:** Enumerator
- Attribute values:** A table with two columns: **Vendor** and **Value**. The table is currently empty.
- Buttons:** **Add...**, **Edit...**, **Remove**, **Move Up**, **Move Down**, **OK**, and **Cancel**.

In the **Attribute Information** dialog box, click **Add**. Another **Attribute Information** dialog box is displayed.

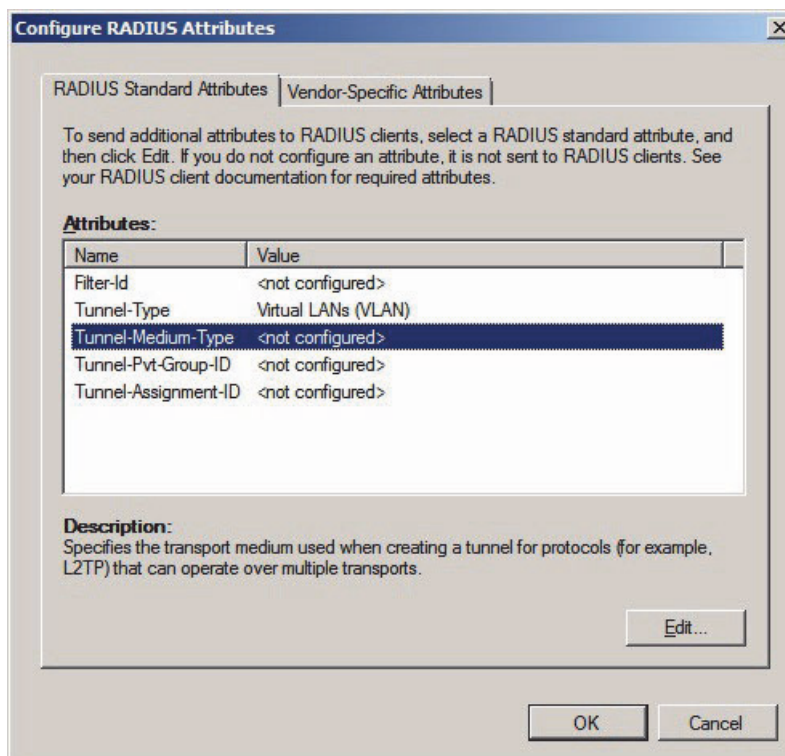


The **Attribute Information** dialog box is shown again, but with additional options for the **Attribute Value**:

- Attribute name:** Tunnel-Type
- Attribute number:** 64
- Attribute format:** Enumerator
- Attribute Value:** Three radio buttons are present:
 - ☐ **Commonly used for Dial-Up or VPN**: Below this is a dropdown menu showing **<none>**.
 - ☒ **Commonly used for 802.1x**: Below this is a dropdown menu showing **Virtual LANs (VLAN)**.
 - ☐ **Others**: Below this is a dropdown menu showing **<none>**.
- Buttons:** **OK** and **Cancel**.

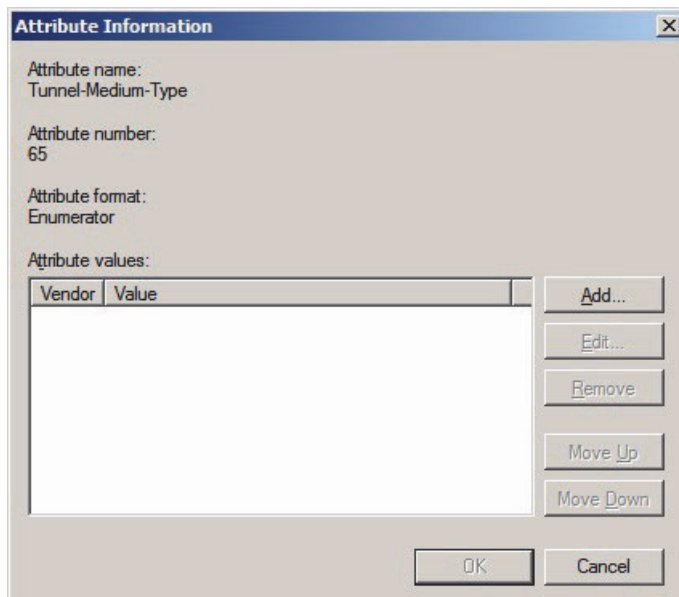
Under **Attribute Value**, choose **Commonly used for 802.1X**, verify that **Virtual LANs (VLAN)** is selected, and then click **OK** twice.

Configure RADIUS Attributes: Tunnel-Medium-Type

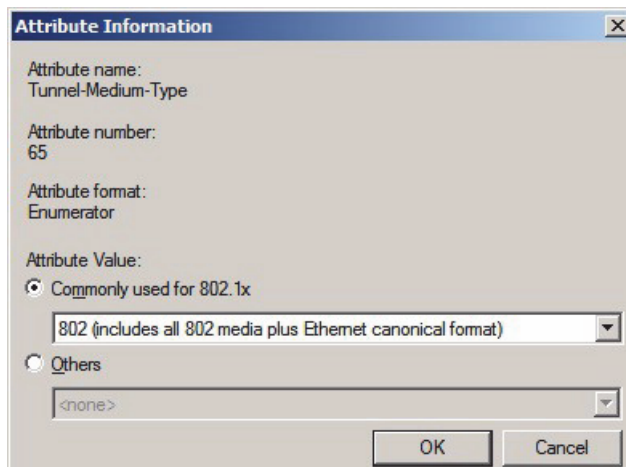


In the **Configure RADIUS Attributes** dialog box on the **RADIUS Standard Attributes** tab, click **Tunnel-Medium-Type**, and then click **Edit**.

Configure Attribute Information: Tunnel-Medium-Type



In the **Attribute Information** dialog box, click **Add**. Another **Attribute Information** dialog box is displayed.



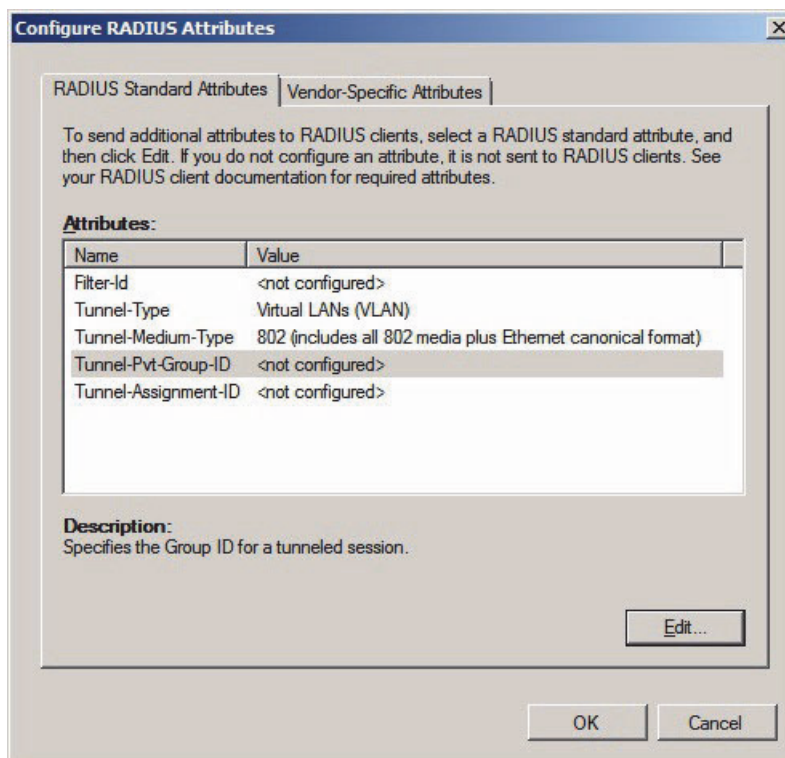
The **Attribute Information** dialog box displays the following information:

- Attribute name: Tunnel-Medium-Type
- Attribute number: 65
- Attribute format: Enumerator
- Attribute Value:
 - ☒ Commonly used for 802.1x
 - 802 (includes all 802 media plus Ethernet canonical format)
 - ☐ Others
 - <none>

Buttons: OK, Cancel

Under **Attribute Value**, choose **Commonly used for 802.1X**, verify that **802 (Include all 802 media plus ethernet canonical format)** is selected, and then click **OK** twice.

Configure RADIUS Attributes: Tunnel-Pvt-Group-ID



The **Configure RADIUS Attributes** dialog box has two tabs: **RADIUS Standard Attributes** and **Vendor-Specific Attributes**. The **RADIUS Standard Attributes** tab is active.

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.

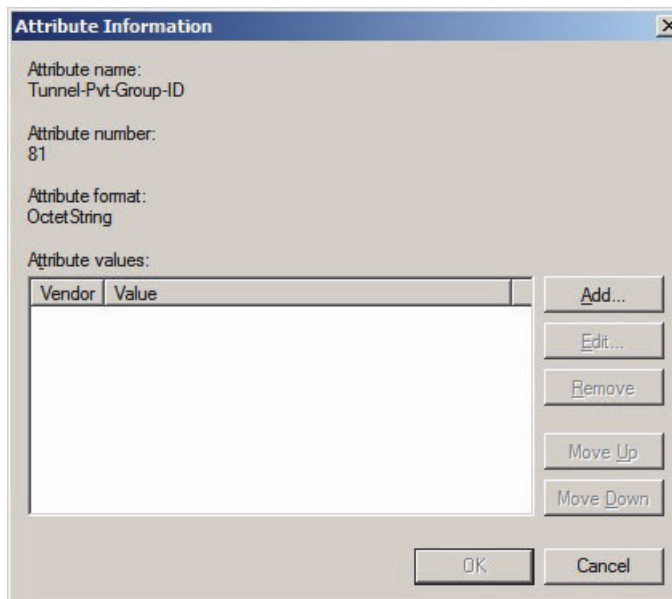
Name	Value
Filter-Id	<not configured>
Tunnel-Type	Virtual LANs (VLAN)
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical format)
Tunnel-Pvt-Group-ID	<not configured>
Tunnel-Assignment-ID	<not configured>

Description:
Specifies the Group ID for a tunneled session.

Buttons: Edit..., OK, Cancel

In the **Configure RADIUS Attributes** dialog box on the **RADIUS standard attributes** tab, click **Tunnel-Pvt-Group-ID**, and then click **Edit**.

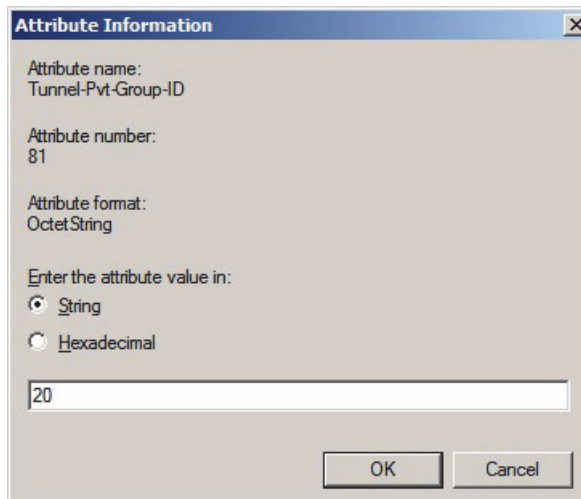
Configure Attribute Information: Tunnel-Pvt-Group-ID



The dialog box titled "Attribute Information" contains the following fields and controls:

- Attribute name: Tunnel-Pvt-Group-ID
- Attribute number: 81
- Attribute format: OctetString
- Attribute values: A table with two columns, "Vendor" and "Value".
- Buttons: Add..., Edit..., Remove, Move Up, Move Down, OK, and Cancel.

In the **Attribute Information** dialog box, click **Add**. Another **Attribute Information** dialog box is displayed.

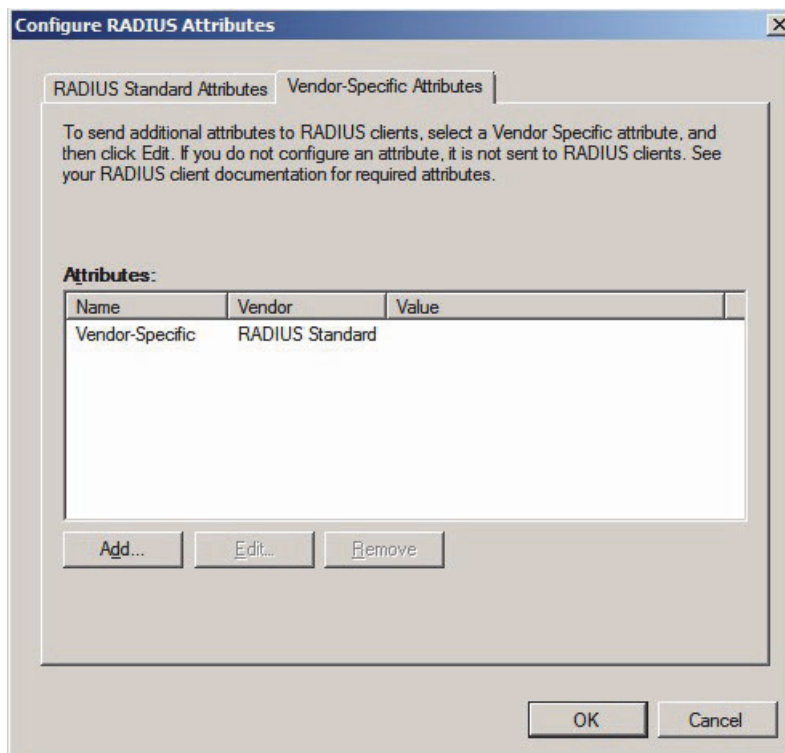


The dialog box titled "Attribute Information" contains the following fields and controls:

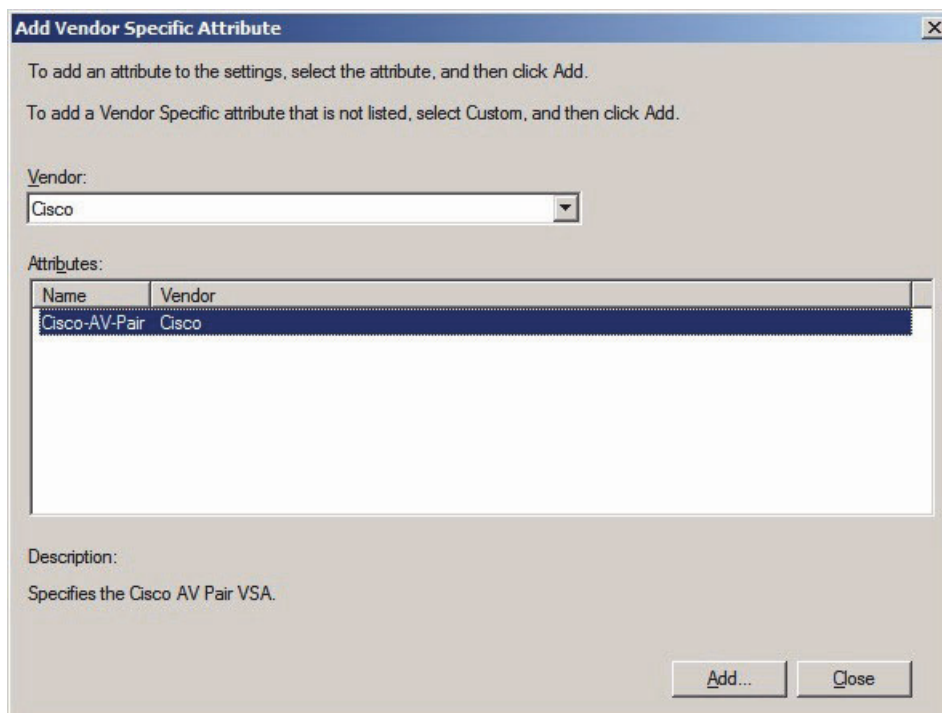
- Attribute name: Tunnel-Pvt-Group-ID
- Attribute number: 81
- Attribute format: OctetString
- Enter the attribute value in:
 - ☒ String
 - ☐ Hexadecimal
- Text input field: 20
- Buttons: OK and Cancel.

Under **Enter the attribute value in**, choose **String**, type **20** (your VLAN) and then click **OK** twice. This value represents the compliant VLAN ID is used.

Vendor-Specific Attributes

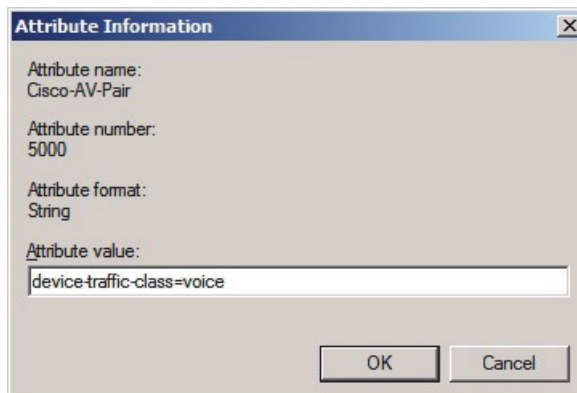


In the Configure RADIUS Attributes dialog box, click the Vendor Specific attributes tab, and then click Add. The dialog **Add Vendor Specific Attribute** box is displayed.



- In the **Add Vendor Specific Attribute** dialog box, under **Vendor** select **Cisco**.
- In the **Add Vendor Specific Attribute** dialog box, under **Attributes**, select **Cisco-AV-Pair**, and then click **Add**.

Set Attribute Information: Cisco AV Pair



Attribute Information

Attribute name:
Cisco-AV-Pair

Attribute number:
5000

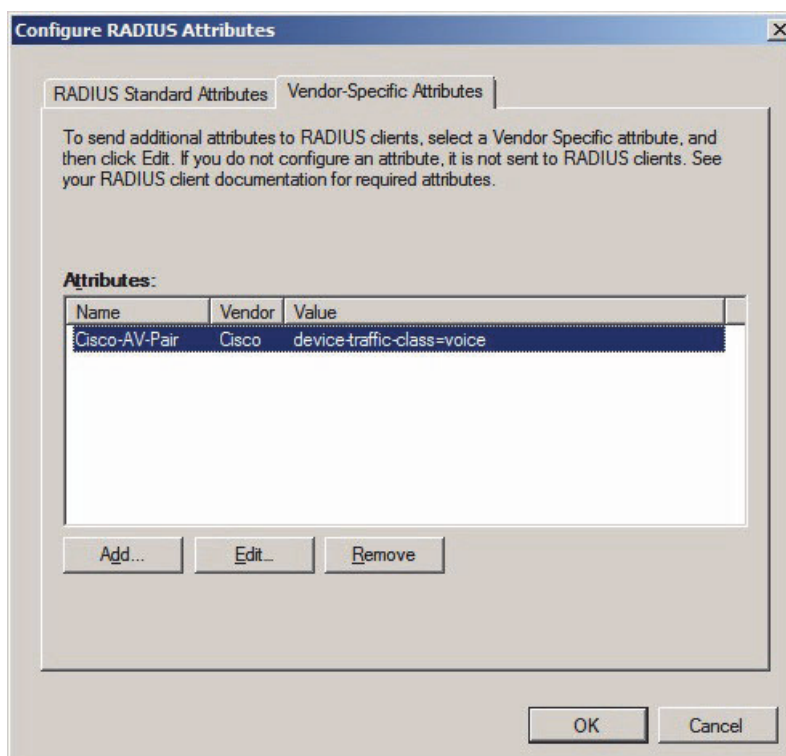
Attribute format:
String

Attribute value:
device-traffic-class=voice

OK Cancel

In the **Attribute Information** dialog box, under **Attribute value**, type **device-traffic-class=voice**, and then click **OK**.

➡ The Tunnel-tag value is populated in all attributes used in this policy, and serves to group these attributes together, identifying them as belonging to a particular tunnel. Consult your vendor documentation to determine if a unique Tunnel-Tag value is required for your switch.



Configure RADIUS Attributes

RADIUS Standard Attributes Vendor-Specific Attributes

To send additional attributes to RADIUS clients, select a Vendor Specific 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.

Attributes:

Name	Vendor	Value
Cisco-AV-Pair	Cisco	device-traffic-class=voice

Add... Edit... Remove

OK Cancel

Click **Close**, and then click **OK**.

Configure VLAN properties for noncompliant phones

Use the following steps to configure VLAN properties for noncompliant computers. These steps are identical to those used for compliant phones with the exception that VLAN ID 222 is configured for noncompliant phones.

- On the **Configure Traffic Controls** page, under **Restricted access network**, click **Configure**.
- In the **Configure RADIUS Attributes** dialog box, on the **RADIUS standard attributes** tab, click **Tunnel-Type**, and then click **Edit**.
- In the **Attribute Information** dialog box, click **Add**.

- Another **Attribute Information** dialog box is displayed. Under **Attribute Value**, choose **Commonly used for 802.1X**, verify that **Virtual LANs (VLAN)** is selected, and then click **OK** twice.
- On the **RADIUS standard attributes** tab, click **Tunnel-Medium-Type**, and then click **Edit**.
- In the **Attribute Information** dialog box, click **Add**.
- Another **Attribute Information** dialog box is displayed. Under **Attribute Value**, choose **Commonly used for 802.1x**, verify that **802 (Include all 802 media plus Ethernet canonical format)** is selected, and then click **OK** twice.
- In the **Configure RADIUS Attributes** dialog box, on the **RADIUS standard attributes** tab, click **Tunnel-Pvt-Group-ID**, and then click **Edit**.
- In the **Attribute Information** dialog box, click **Add**.
- Another **Attribute Information** dialog box is displayed. Under **Enter the attribute value in**, choose **String**, type **222**, and then click **OK** twice. This value represents the noncompliant VLAN ID used in this lab.
- In the **Configure RADIUS Attributes** dialog, click the **Vendor Specific attributes** tab, and then click **Add**.
- In the **Add Vendor Specific Attribute** dialog box, under **Vendor** select **Cisco**.
- In the **Add Vendor Specific Attribute** dialog box, under **Attributes**, select **Cisco-AV-Pair**, and then click **Add**.
- In the **Attribute Information** dialog box, under **Attribute value**, type **device-traffic-class=voice**, and then click **OK** twice.
- Click **Close**, and then click **OK**.
- This completes the configuration of VLAN properties for compliant and noncompliant computers. Click **Next**.
- On the **Define NAP Health Policy** page, verify that **Windows Security Health Validator** and **Enable auto-remediation of client computers** check boxes are selected, and then click **Next**.
- On the **Completing NAP Enforcement Policy and RADIUS Client Configuration** page click **Finish**.
- Leave the NPS console open for the following procedure.

Verify NAP Policies

In order for the health status of NAP client computers or phones to be correctly evaluated by NPS, NAP policies that were created in the previous procedure must be enabled and configured with the correct processing order. By default, the NAP configuration wizard will create policies that are lower in processing order than any existing policies, but higher in processing order than the default policies. However, if policies are created and removed, it is possible to change processing order of the default connection request policy and network policies. Therefore, you should verify that the NAP policies created in the previous procedure are configured with the correct processing order.

To verify NAP policies

- In the Network Policy Server console tree, double-click **Policies**, and then click **Connection Request Policies**.
- Verify that the NAP connection request policy you created in the previous procedure is first in the processing order, or that other policies that match NAP client authentication attempts are disabled. Also verify that the status of the policy is **Enabled**. The default name of this policy is **NAP 802.1x (Wired)**.
- Click **Network Policies**, and verify that the network policies you created in the previous procedure are higher in the processing order than other policies that match NAP client authorization attempts, or these other policies are disabled. Also verify that the status of this policies is **Enabled**. The default name of the three network policies created by the NAP configuration wizard are **NAP 802.1X (Wired) Compliant**, **NAP 802.1X (Wired) Noncompliant**, and **NAP 802.1X (Wired) Non NAP-Capable**.
- Click **Health Policies**, and verify that two policies were created. By default these policies are named **NAP 802.1X (Wired) Compliant** and **NAP 802.1X (Wired) Noncompliant**.

Configure Policies on the NPS

Configure Network Policy: New Network Policy

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:

Secure Wired (Ethernet) Connections

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

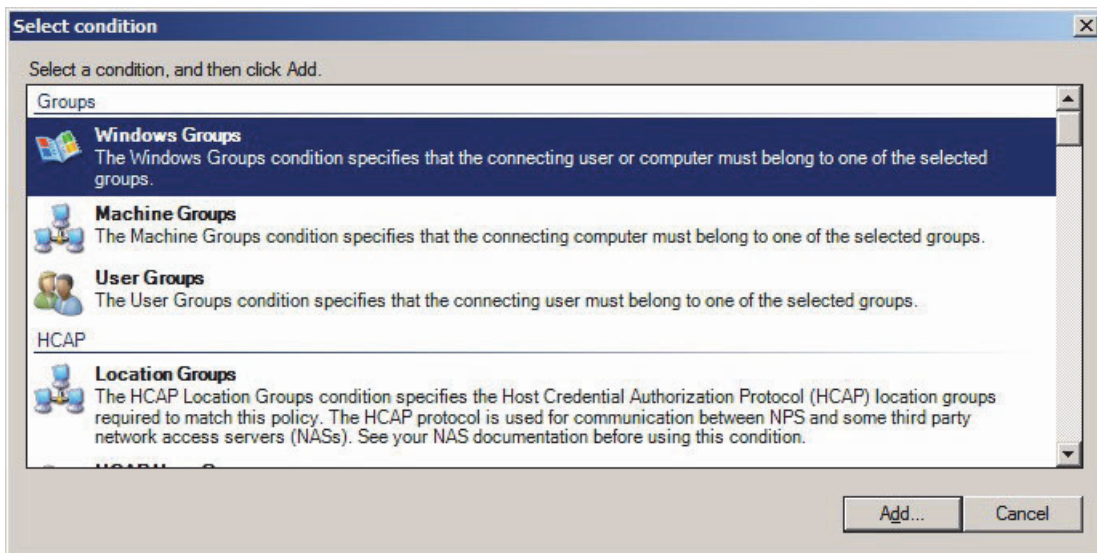
☐ **Vendor specific:**

10

Previous Next Finish Cancel

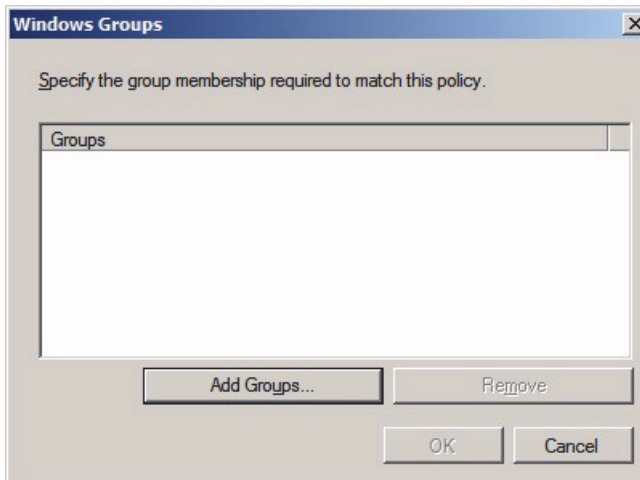
- In the Network Policy Server console tree double-click **Policies**, then click **Network Policies**.
- Right click on **New**.
- On the **New Network Policy** page, under **Policy name type Secure Wired (Ethernet) Connections**.
- Leave the **Type of network access server** to **Unspecified**. Then click **Next**.

Configure Network Policy: Select Condition



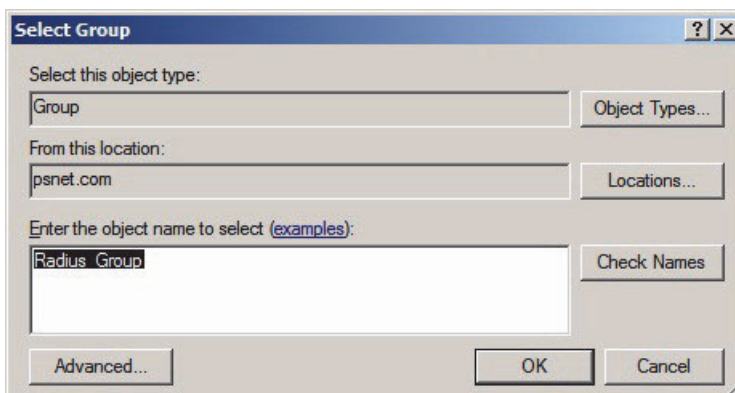
- On the **New Network Policy** page, click **Add**.
- On the **Select condition** page, select **Windows Groups**.
- Click **Add**.

Configure Network Policy: Windows Groups



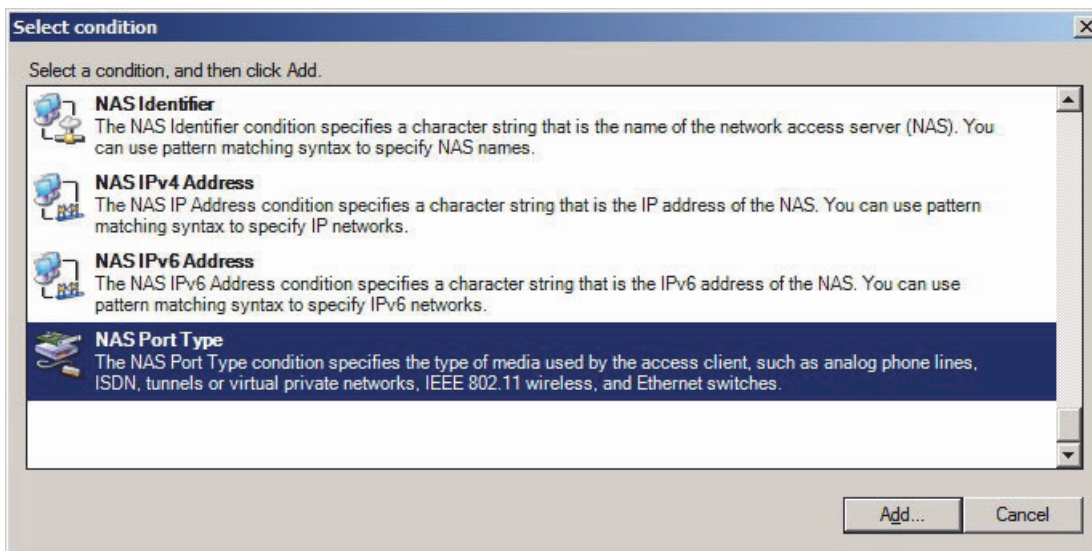
- On the **Windows Groups** page, click **Add Groups**.

Configure Network Policy: Select Group



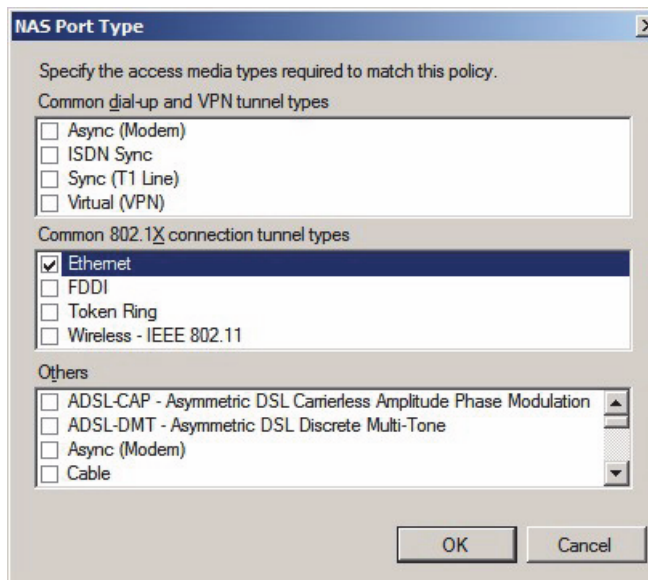
- On the **Select Group** page, click **Add Groups**.
- In the **Enter the object name to select** dialog box enter the name of the former in Configuration Step 6 created Radius_Group.
- Click on Check Names, then the RADIUS-Group will have an underline, then click **OK** twice.

Configure Network Policy: Select Condition



- On the **Specify condition** page, select **NAS Port Type**.
- Click **Add**.

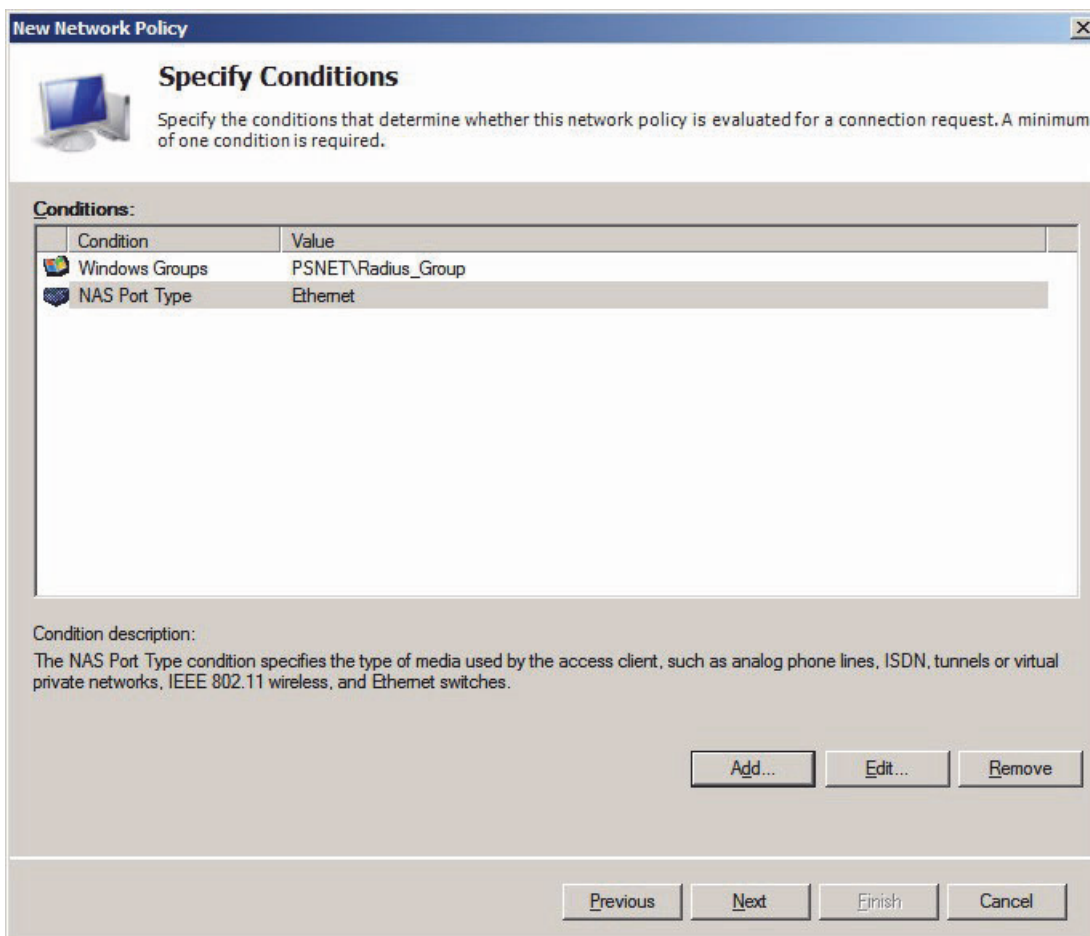
Configure Network Policy: NAS Port Type



The screenshot shows a Windows-style dialog box titled "NAS Port Type". Inside, there is a text label "Specify the access media types required to match this policy." followed by three sections of checkboxes. The first section, "Common dial-up and VPN tunnel types", includes "Async (Modem)", "ISDN Sync", "Sync (T1 Line)", and "Virtual (VPN)". The second section, "Common 802.1X connection tunnel types", includes "Ethernet" (which is checked), "FDDI", "Token Ring", and "Wireless - IEEE 802.11". The third section, "Others", includes "ADSL-CAP - Asymmetric DSL Carrierless Amplitude Phase Modulation", "ADSL-DMT - Asymmetric DSL Discrete Multi-Tone", "Async (Modem)", and "Cable". At the bottom right are "OK" and "Cancel" buttons.

- On the **NAS Port Type** page, under **Common 802.1X connection tunnel types**, select **Eth-ernet**.
- Click **OK**.

Configure Network Policy: Specify Conditions



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	PSNET\Radius_Group
NAS Port Type	Ethernet

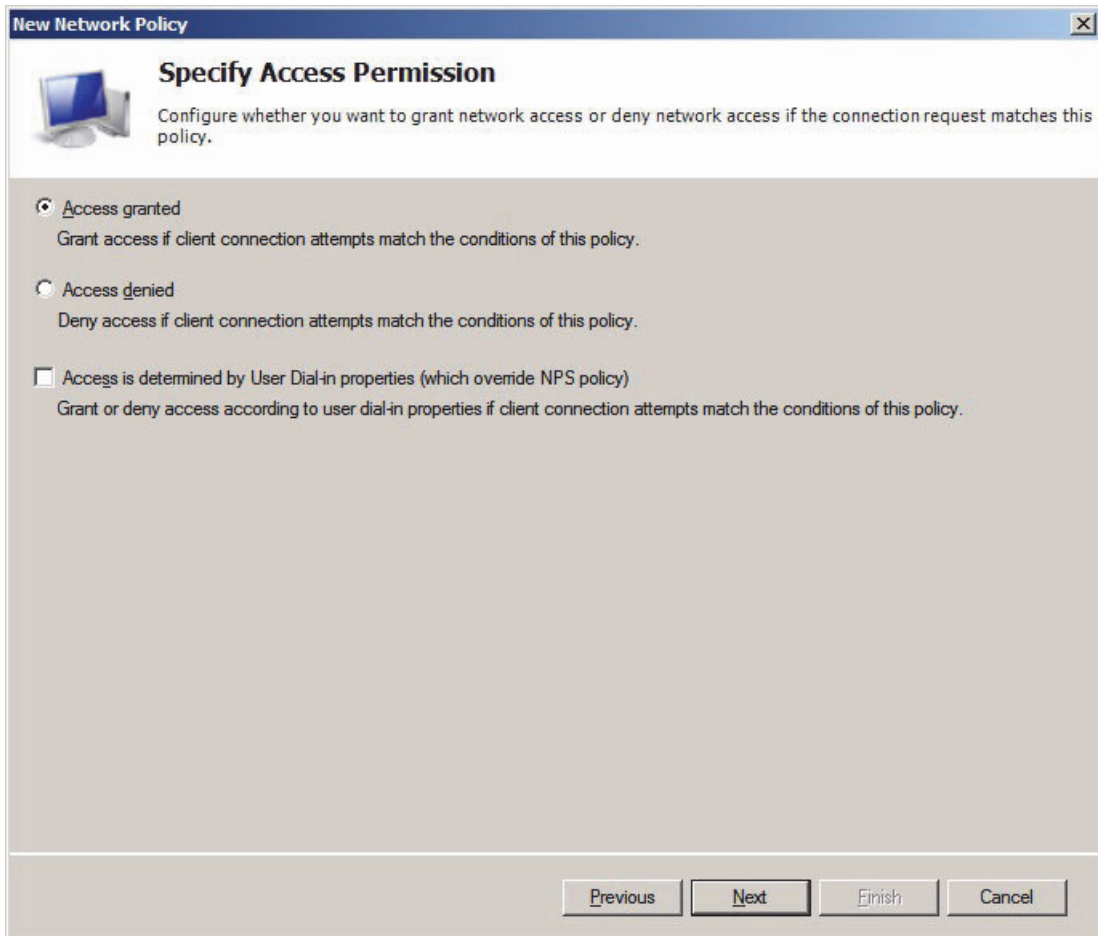
Condition description:
The NAS Port Type condition specifies the type of media used by the access client, such as analog phone lines, ISDN, tunnels or virtual private networks, IEEE 802.11 wireless, and Ethernet switches.

Add... Edit... Remove

Previous Next Finish Cancel

On the **New Network Policy** page, click **Next**

Specify Access Permissions



The image shows a Windows-style dialog box titled "New Network Policy". Inside, there is a sub-header "Specify Access Permission" with a small computer icon. Below this, a text box explains: "Configure whether you want to grant network access or deny network access if the connection request matches this policy." There are three radio button options: "Access granted" (selected), "Access denied", and "Access is determined by User Dial-in properties (which override NPS policy)". Each option has a descriptive text line below it. At the bottom right, there are four buttons: "Previous", "Next", "Finish", and "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.

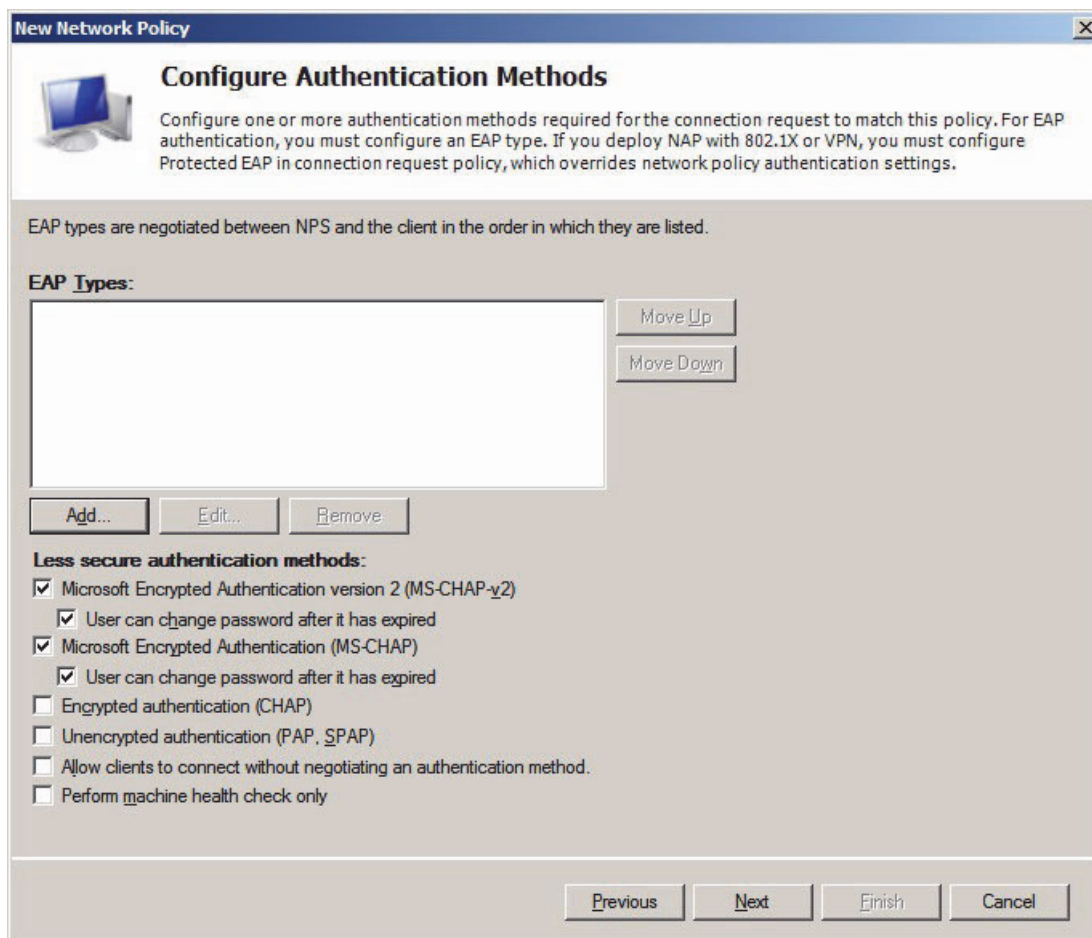
☐ **Access denied**
Deny access if client connection attempts match the conditions of this policy.

☐ **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.

Previous **Next** **Finish** **Cancel**

- On the **New Network Policy** page, select **Access granted**.
- Click **Next**.

Configure Authentication Methods



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:

[Empty list box]

Move Up
Move Down

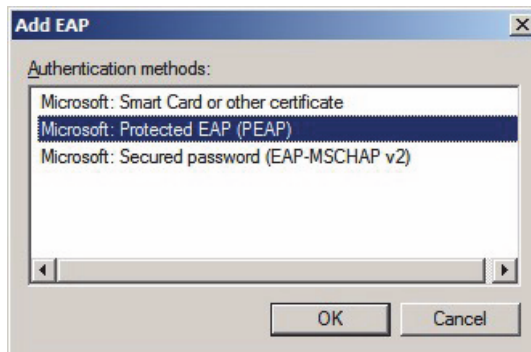
Add... Edit... Remove

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

Add EAP



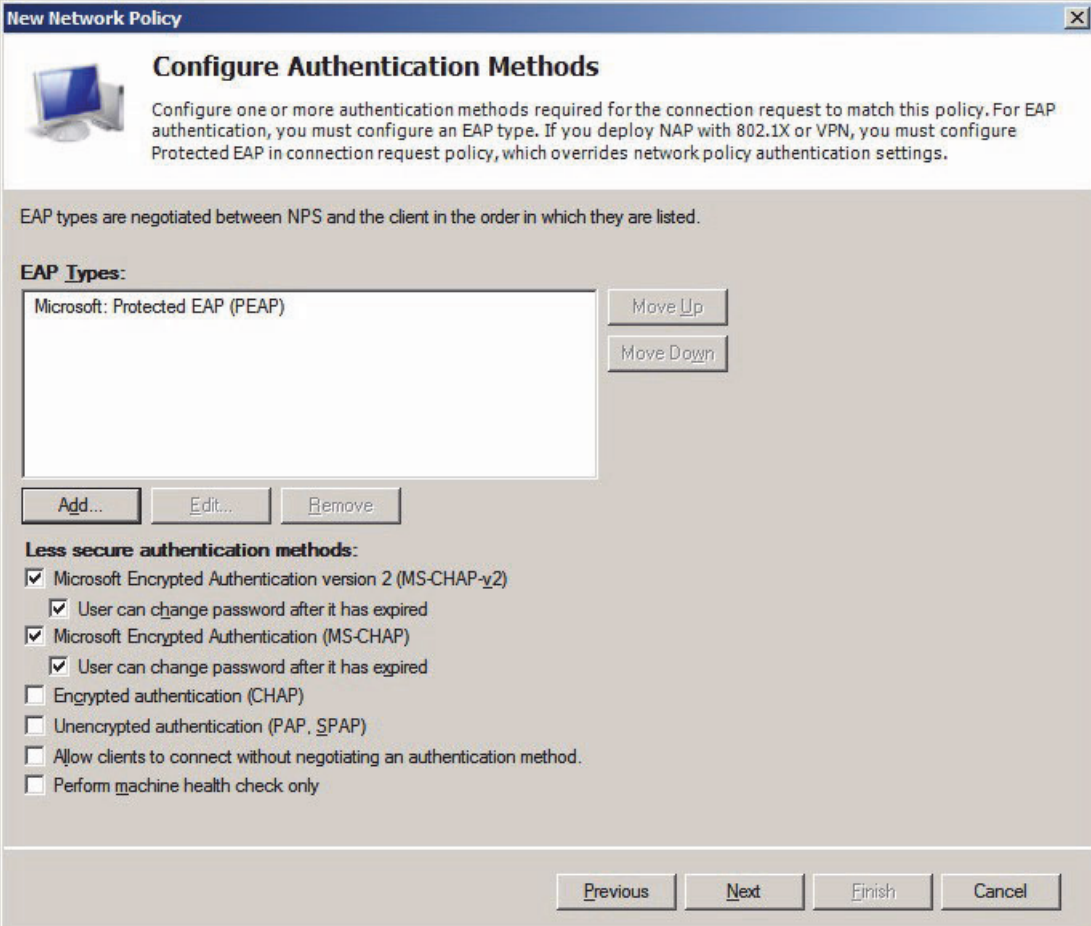
Add EAP

Authentication methods:

- Microsoft: Smart Card or other certificate
- Microsoft: Protected EAP (PEAP)**
- Microsoft: Secured password (EAP-MSCHAP v2)

OK Cancel

On the **Add EAP** page, select **Microsoft: Protected EAP (PEAP)**, then click **OK**. The **New Network Policy** page dialog box is displayed again.



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:

- Microsoft: Protected EAP (PEAP)

Move Up
Move Down

Add... Edit... Remove

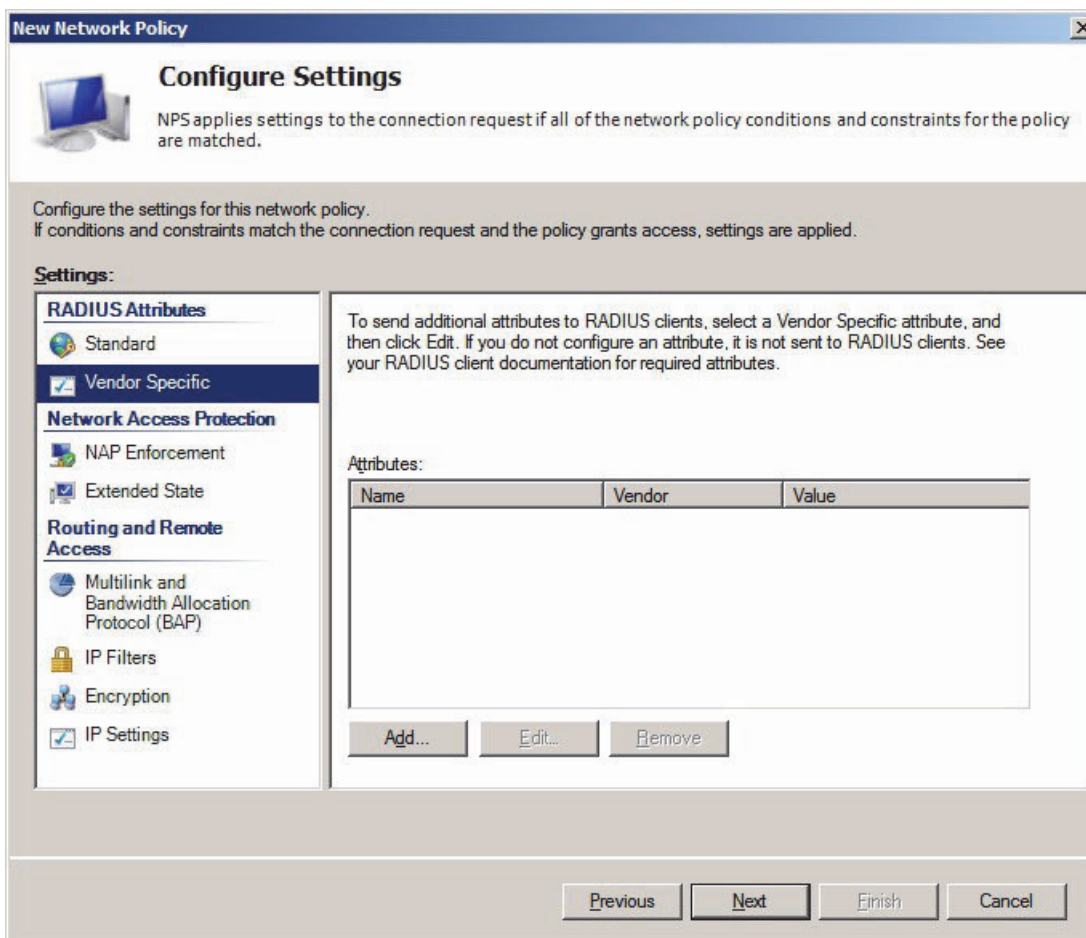
Less secure authentication methods:

- ☒ 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

Select **Next**.

Configure Settings



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 Vendor Specific 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.

Attributes:

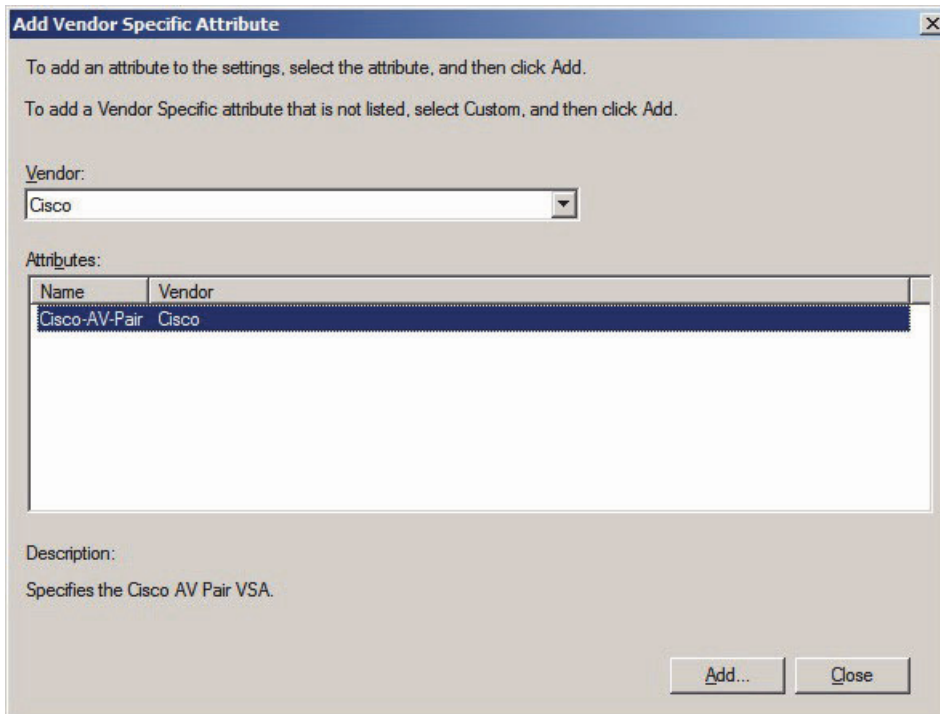
Name	Vendor	Value
------	--------	-------

Add... **Edit...** **Remove**

Previous **Next** **Finish** **Cancel**

- On the Configure Settings page, select **Vendor Specific**.
- Click **Add**.

Add Vendor Specific Attribute

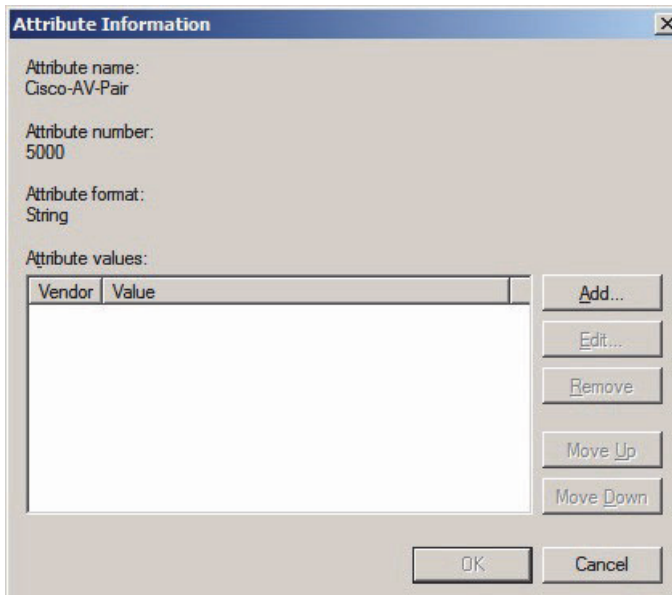


The dialog box titled "Add Vendor Specific Attribute" contains instructions at the top: "To add an attribute to the settings, select the attribute, and then click Add." and "To add a Vendor Specific attribute that is not listed, select Custom, and then click Add." Below the instructions is a "Vendor:" dropdown menu with "Cisco" selected. Underneath is an "Attributes:" table with two columns: "Name" and "Vendor". The table contains one row: "Cisco-AV-Pair" under "Name" and "Cisco" under "Vendor". Below the table is a "Description:" field with the text "Specifies the Cisco AV Pair VSA." At the bottom right are "Add..." and "Close" buttons.

Name	Vendor
Cisco-AV-Pair	Cisco

- On the **Add Vendor Specific Attribute** page, select e. g. **Cisco-AV-Pair**.
- Click **Add**.

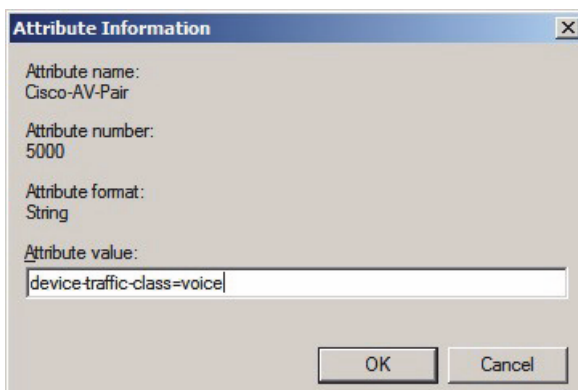
Attribute Information



The dialog box titled "Attribute Information" displays the following information: "Attribute name: Cisco-AV-Pair", "Attribute number: 5000", and "Attribute format: String". Below this is an "Attribute values:" section with a table that has two columns: "Vendor" and "Value". To the right of the table are five buttons: "Add...", "Edit...", "Remove", "Move Up", and "Move Down". At the bottom are "OK" and "Cancel" buttons.

Vendor	Value
--------	-------

On the **Attribute Information** page, click **Add**. Another **Attribute Information** dialog box is displayed.



Attribute Information

Attribute name:
Cisco-AV-Pair

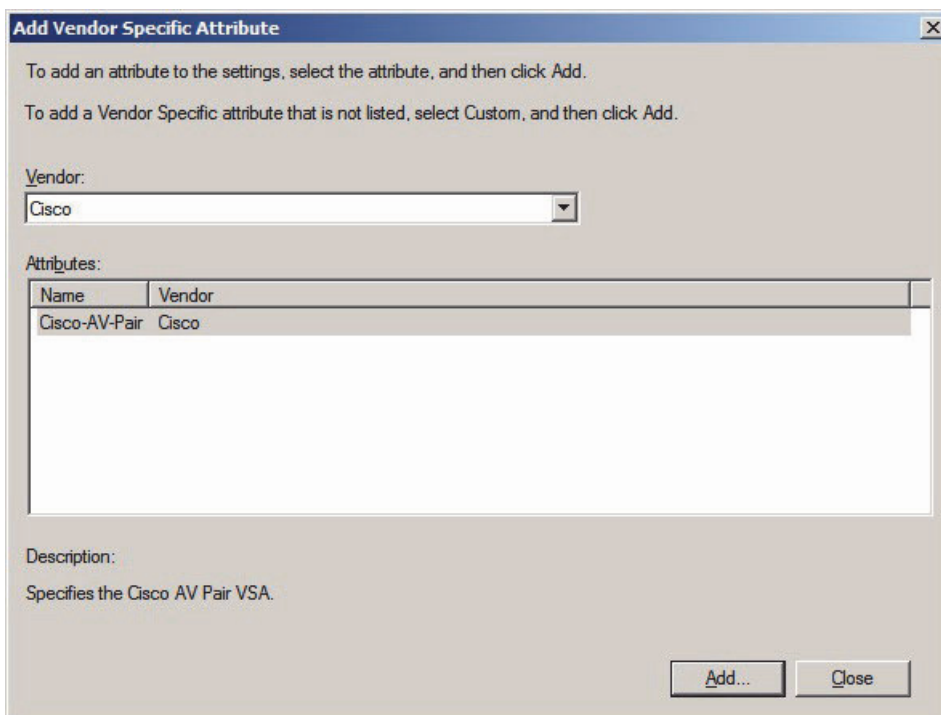
Attribute number:
5000

Attribute format:
String

Attribute value:

OK Cancel

- On the **Attribute Information** page, under Attribute value, type: **device-traffic-class=voice**.
- Click **OK** twice. The **Add Vendor Specific Attribute** dialog box is displayed again.



Add Vendor Specific Attribute

To add an attribute to the settings, select the attribute, and then click Add.

To add a Vendor Specific attribute that is not listed, select Custom, and then click Add.

Vendor:

Attributes:

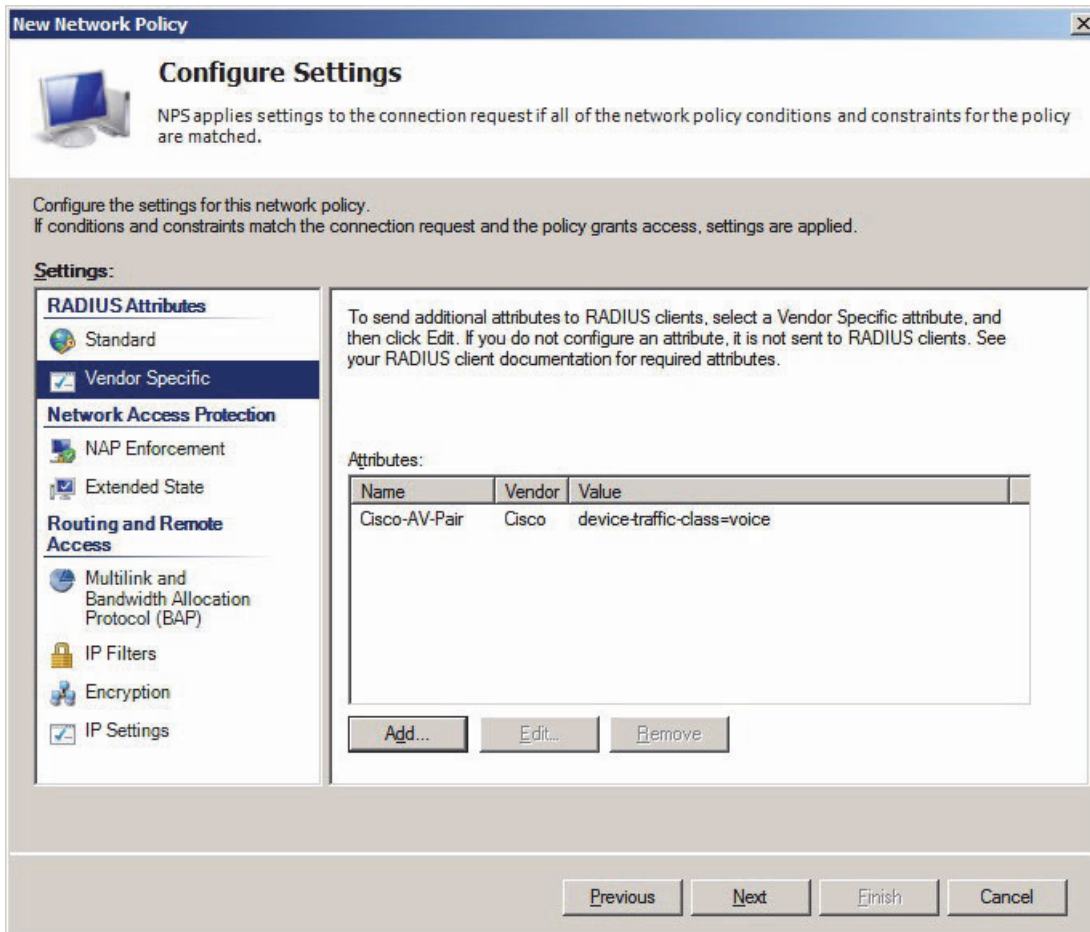
Name	Vendor
Cisco-AV-Pair	Cisco

Description:
Specifies the Cisco AV Pair VSA.

Add... Close

Click **Close**.

Configure Settings



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 Vendor Specific 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.

Attributes:

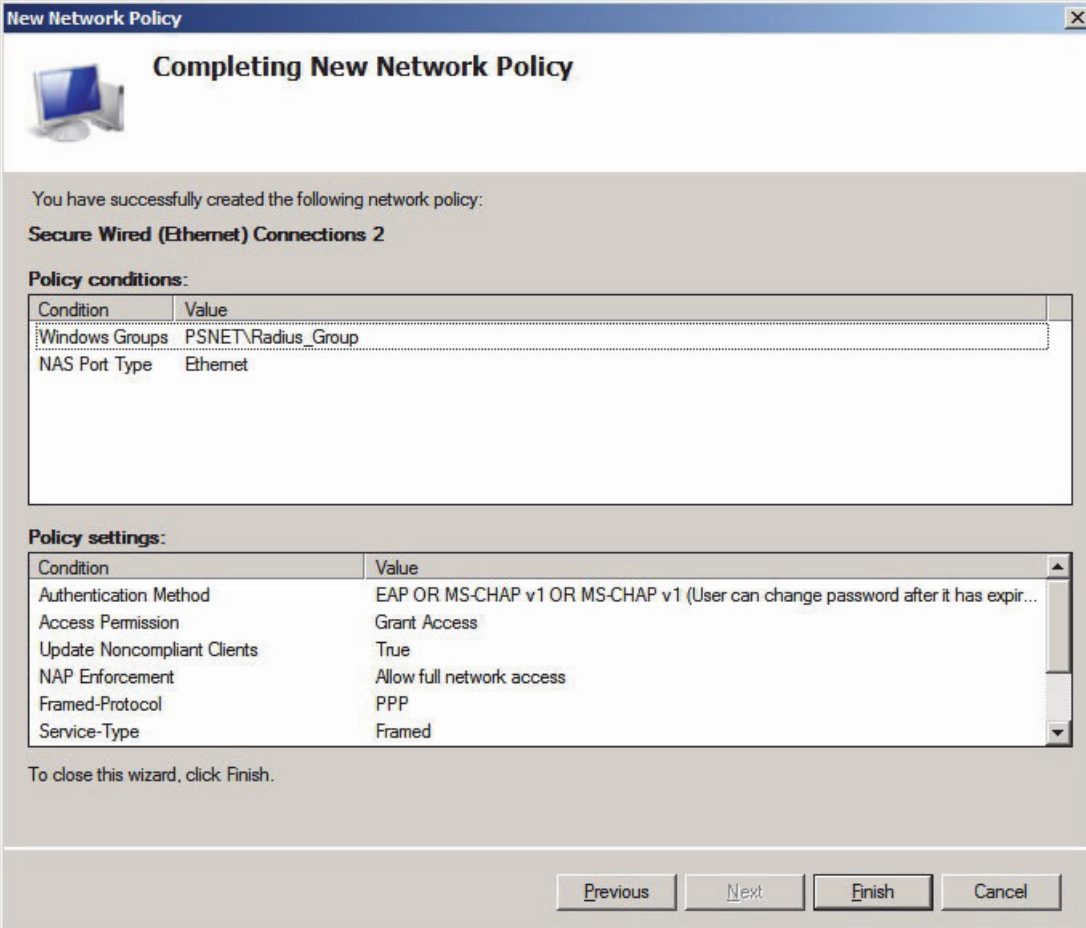
Name	Vendor	Value
Cisco-AV-Pair	Cisco	device-traffic-class=voice

Buttons: Add... Edit... Remove

Navigation: Previous Next Finish Cancel

On the **New Network Policy** page, click **Next**.

Completing Network Policy



The image shows a Windows XP-style dialog box titled "New Network Policy". The main heading inside is "Completing New Network Policy" with a small computer icon to the left. Below this, a message states: "You have successfully created the following network policy: **Secure Wired (Ethernet) Connections 2**".

Under the heading "Policy conditions:", there is a table with two columns: "Condition" and "Value".

Condition	Value
Windows Groups	PSNET\Radius_Group
NAS Port Type	Ethernet

Below the conditions table is the "Policy settings:" section, which contains another table with "Condition" and "Value" columns.


Condition	Value
Authentication Method	EAP OR MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has expir...
Access Permission	Grant Access
Update Noncompliant Clients	True
NAP Enforcement	Allow full network access
Framed-Protocol	PPP
Service-Type	Framed

At the bottom of the dialog, a message says: "To close this wizard, click Finish." Below this message are four buttons: "Previous", "Next", "Finish", and "Cancel". The "Finish" button is highlighted with a darker border.

On the **New Network Policy** page, with the title **Completing New Network Policy** click on **Finish**.

Configure 802.1X on DLS

On the DLS go to IP Devices / IP Phone Configuration / IEE 802.1X to tab 802.1X Settings.

 Please be aware that the appearance of the DLS screenshots shown might have slightly changed since that documentation release.

The screenshot shows the OpenStage Deployment Service V6 web interface. The left sidebar contains a tree view of the configuration structure, with 'IEEE 802.1x' selected under 'IP Phone Configuration'. The main content area displays the configuration for IEEE 802.1x. The 'Object' tab is active, showing fields for IP Address (10.1.22.108), Device ID (00:1AE8:3A:DD:33), Device Type (OpenStage 40), and EAP settings. The EAP settings are configured for EAP-TLS with a PEAP authentication type. The bottom of the interface shows a status bar with 'Clear', 'Discard', 'Save', 'Import Certificate', 'Remove Certificate', 'Read', and 'Refresh' buttons.

Deployment Service Administration IP Devices IP Phone Configuration Gateway / Server IP Routing Ports Features Quality of Service QoS Data Collection Security Settings Telephony Small Remote Site Redundancy Dialing Properties Time Parameters Audio Settings SNMP Settings Applications LDAP User Settings SIP Mobility HFA Mobility Keysets / Keylayout WLAN Settings Signaling and Payload Encryption IEEE 802.1x Diagnosis Miscellaneous File Deployment IP Client Configuration IP Gateway Configuration IP Device Interaction IP Device Management Mobile Users Gateways Software Deployment Element Manager Profile Management Job Coordination Help Logoff admin

IEEE 802.1x Job ID: Exec Time: asap

Object Edit View Action Help

Views: Search Object Table Template

IP Address: 10.1.22.108 IP Address 2: IP Protocol Mode: IPv4

Device ID: 00:1AE8:3A:DD:33 SW Version: V2 R0.68.0

Device Type: OpenStage 40 SW Type: Siemens HFA

E.164: 41105 Reg-Address: 192.1.24.65

Basic E.164: Last Registration: 2011-11-28 15:02:20

Remarks:

802.1x Settings Phone Certificate RADIUS Server CA Certificate 1 RADIUS Server CA Certificate 2

Authentication Type: PEAP

EAP-TLS

☐ Validate Server Certificate Login Name: Password:

EAP-TLS or PEAP

MSCHAP Identity: user1 EAP-TLS Digest:

MSCHAP Password: ***** EAP-TLS One Time Password:

EAP-FAST

EAP-FAST Secret:

LEAP

Login Name: Password:

Discard Save Import Certificate Remove Certificate Read Refresh

Clear

802.1x Settings on DSL

The screenshot shows a configuration window titled "802.1x Settings" with four tabs: "802.1x Settings", "Phone Certificate", "RADIUS Server CA Certificate 1", and "RADIUS Server CA Certificate 2". The "802.1x Settings" tab is active. It contains the following fields and controls:

- Authentication Type:** A dropdown menu with "PEAP" selected.
- EAP-TLS section:**
 - ☐ **Validate Server Certificate**
 - Login Name:** An empty text field.
 - Password:** An empty password field.
- EAP-TTLS or PEAP section:**
 - MSCHAP Identity:** A text field containing "user1".
 - MSCHAP Password:** A password field containing "*****".
 - EAP-TTLS Digest:** A label for a field that is partially visible on the right.
 - EAP-TTLS One Time Pas:** A label for a field that is partially visible on the right.

- On the **802.1x Settings** tab, on the **Authentication Type** dialog box select **PEAP**.
- On the EAP-TTLS or PEAP section enter **user1** in the **MSCHAP Identity** field and the **user1** password in the **MSCHAP Password** field.

Import RADIUS Server CA Certificate

Device ID: 00:1A:E8:30:00:16

Certificate Type

- ☐ Phone Certificate
- ☒ RADIUS Server CA Certificate 1
- ☐ RADIUS Server CA Certificate 2

☒ Import certificate to DLS and activate on device (1-step)

Import using: ☒ File ☐ PKI

Import from File

☐ Individual certificate files for each selected object

Certificate File Names based on ...

- ☒ Device ID
- ☐ E.164 number

Filename : p:\HFA\Certificates\802.1x\PEAP\MicrosoftRoot_CA.cer Browse...

Passphrase:

Import from PKI

PKI Configuration: Internal Connector (default)

OK Cancel

- On the **RADIUS Server CA Certificate 1** tab, select **Import Certificate** and select the **Root_CA Certificate**, that you former created in → Install an enterprise root CA.
- Click **OK**.

Activate RADIUS Server CA Certificate

802.1x Settings		Phone Certificate	RADIUS Server CA Certificate 1	RADIUS Server CA Certificate 2
Status Active/Import:	no active certificate		<input checked="" type="checkbox"/> Activate certificate (RADIUS 1)	
Active Certificate:		Imported Certificate:		
PKI Configuration:				
Serial Number:		198D3FBA453CCEB742299526A0FE5906		
Owner:		DC=com,DC=psnet,CN=RadiusCA		
Issuer:		DC=com,DC=psnet,CN=RadiusCA		
Valid from:		2011-05-02 14:13:38		
Valid to:		2021-05-02 14:23:37		
Key Algorithm:		RSA		
Key Size:		2048		
Fingerprint (SHA-1):		70B81841EB84A96D6B67CD9505A390423481E914		
Expires in ... [days]:		3442		
Alarm Status:		valid		
<div> 1 / 1 Discard Save Import Certificate Remove Certificate </div>				

On the **RADIUS Server CA Certificate 1** tab, select **Activate certificate (RADIUS 1)** and click on **Save**.

Verify RADIUS Server CA Certificate

802.1x Settings | Phone Certificate | **RADIUS Server CA Certificate 1** | RADIUS Server CA Certificate 2

Status Active/Import: ☐ Activate certificate (RADIUS 1)

Active Certificate: Imported Certificate:

PKI Configuration:

Serial Number:	198D3FBA453CCEB742299526A0FE5906	198D3FBA453CCEB742299526A0FE5906
Owner:	DC=com,DC=psnet,CN=RadiusCA	DC=com,DC=psnet,CN=RadiusCA
Issuer:	DC=com,DC=psnet,CN=RadiusCA	DC=com,DC=psnet,CN=RadiusCA
Valid from:	2011-05-02 14:13:38	2011-05-02 14:13:38
Valid to:	2021-05-02 14:23:37	2021-05-02 14:23:37
Key Algorithm:	RSA	RSA
Key Size:	2048	2048
Fingerprint (SHA-1):	70B81841EB84A96D6B67CD9505A390423481E914	70B81841EB84A96D6B67CD9505A390423481E914
Expires in ... [days]:	3443	3443
Alarm Status:	valid	valid

1 / 1 Discard Save Import Certificate Remove Certificate

- On the **RADIUS Server CA Certificate 1** tab, click on the Refresh Button.
- In the Status Active/Import field now appears **equal**.

Configure Cisco Switch

You have to configure the Network Switch with the IP-Adress of the radius server and with the password, you have created on configuration step 12 (see picture on the left side) and you have to enable dot1x on the desired port.

802.1X Switch Cisco 3560 Properties

Settings

☐ Select an existing template:

Phone 5004

Name and Address

Friendly name:

802.1X Switch Cisco 3560

Address (IP or DNS):

192.1.254.116

Verify...

Shared Secret

Select an existing Shared Secrets template:

None

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

☒ Manual ☐ Generate

Shared secret:

.....

Confirm shared secret:

.....

OK Cancel Apply

e.g. radius server entry on a Cisco 3560 switch:

```
H4K-S116(config)#radius-server host 192.1.26.100 auth-port 1812 acct-port 1813 key 123456
```

Verify the successful Logon

Network Policy and Access Services Number of events: 23,634 (1) New events available

Number of events: 23,634

Level	Date and Time	Source	Event ID	Task Category
Information	28.11.2011 15:01:11	Microsoft Windows security audit...	6278	Network Policy Server
Information	28.11.2011 15:01:11	Microsoft Windows security audit...	6272	Network Policy Server
Information	28.11.2011 14:59:09	Microsoft Windows security audit...	6278	Network Policy Server
Information	28.11.2011 14:59:09	Microsoft Windows security audit...	6272	Network Policy Server
Information	28.11.2011 14:56:09	Microsoft Windows security audit...	6278	Network Policy Server

Event 6278, Microsoft Windows security auditing.

General | **Details**

Network Policy Server granted full access to a user because the host met the defined health policy.

User:
 Security ID: PSNET\user1
 Account Name: PSNET\user1
 Account Domain: PSNET
 Fully Qualified Account Name: psnet.com/Users/user1

Client Machine:
 Security ID: NULL SID
 Account Name: -
 Fully Qualified Account Name: -
 OS-Version: -
 Called Station Identifier: 00-1D-A2-0A-F2-10
 Calling Station Identifier: 00-1A-E8-3A-DD-33

NAS:
 NAS IPv4 Address: 192.1.254.116
 NAS IPv6 Address: -
 NAS Identifier: -
 NAS Port-Type: Ethernet
 NAS Port: 50014

RADIUS Client:
 Client Friendly Name: 8021X Switch Cisco 3560
 Client IP Address: 192.1.254.116

Authentication Details:
 Connection Request Policy Name: NAP 802.1X (Wired) test
 Network Policy Name: Secure Wired (Ethernet) Connections 2
 Authentication Provider: Windows
 Authentication Server: Radius.psnet.com
 Authentication Type: PEAP
 EAP Type: Microsoft: Secured password (EAP-MSCHAP v2)
 Account Session Identifier: -

Quarantine Information:
 Result: Full Access
 Extended-Result: -
 Session Identifier: -
 Help URL: -
 System Health Validator Result(s): -

Log Name: Security
Source: Microsoft Windows security
Event ID: 6278
Level: Information
User: N/A
OpCode: Info
More Information: [Event Log Online Help](#)

Logged: 28.11.2011 15:01:11
Task Category: Network Policy Server
Keywords: Audit Success
Computer: Radius.psnet.com

On the NPS-Server:

Go the Event Viewer/Custom Views/Server Roles/Network Policy and Access Service and verify the log entries. You have to receive a Full Access message.

Glossary

ACL

Abbreviation for **Access List**. This is a list of restrictions that apply to the Guest VLAN.

Authenticator

An "Authenticator" in the context of IEEE 802.1X is a Network Access Server acting as a gate-keeper in a → RASsolution. Clients (called "supplicants") apply for access, and the authenticator decides whether to grant or deny access after consultation with a central authentication server using the RADIUS protocol.

Auto-Enrollment

Available in Windows Server 2003 and later versions. Introduces the capability of automatically requesting and distributing certificates if this is necessary according to the policies.

CA

See Certificate Authority

Certificate Authority

A Certificate Authority, or CA, is an organization that issues digital certificates. In IT, a digital certificate is more or less the equivalent to a passport and is used to verify that a public key belongs to an individual or an organization. The CA certifies this by digitally signing the certificate.

Certificates comprise "keys" and additional information required for authentication as well as encryption and decryption of sensitive or confidential data sent over the Internet or other networks. Additional information may be expiry dates, references to certificate revocation lists, and so on, and are included in the certificate by the CA.

The basic task of a CA is to issue and verify these digital certificates. It is responsible for providing and assigning certificates and checking their integrity. As such, it is an important part of the Public Key Infrastructure.

EAP

EAP (**E**xtensible **A**uthentication **P**rotocol) facilitates negotiation prior to actual authentication. Use of a wider variety of authentication protocols makes unauthorized access even more difficult.

The following methods are available:

- EAP-MD5User name/password (not secure)
- EAP-TLS PKI (certificates), secure authentication
- EAP-TTLSUser name/password (secure)
- MS-CHAPv2Microsoft user name/password (not secure)
- PEAPMicrosoft/Cisco tunnel module for secure transport of MS-CHAPv2

EAP uses simple request/response interaction to describe the exchange of authentication data from the user to the authentication server and its response. Certificates are one of the authentication mechanisms used. When EAP is used over 802.1X, the authentication data is transmitted via EAPoL (Extensible Authentication Protocol over LAN). The EAP asks the user – the phone in this case – to authenticate itself. The authentication information is firstly forwarded to the port or authenticator, which in turn forwards it to the RADIUS server. The RADIUS server uses the stored user profile to authenticate the user (phone), in other words, it decides whether the user (phone) may access the requested services or not. If authentication was successful, the confirmation message which the RADIUS server returns to the switch will contain the words "RADIUS/EAP Success". The authenticator will then immediately enable the relevant port for data transport. German-speaking users can find additional information in Section 5 of the following document: [WLAN im Archiv der TU Chemnitz](#).

EAPoL

The Extensible Authentication Protocol over LAN (EAPoL, defined in IEEE 802.1X) is a transport protocol for EAP. The special feature of EAPoL is the start and logoff frames. Data is encapsulated in EAP packets. With EAPoL, EAP can also be used in heterogeneous WAN environments.

EAPoL-Logoff

A device can (periodically) log off from an authentication server and then log on again. A special feature is Proxy-EAPoL-Logoff. If an IP phone is directly connected to a PC in the LAN, the IP phone sends an EAPoL-Logoff with the PC's MAC address to the authentication server to log the device off. This prevents connection of an unknown IP device instead of the PC.

EAP-OTP

EAP-One Time Password

EAP-TLS

The EAP-Transport Layer Security protocol – a combination of EAP and SSL – requires mutual certificate-base authentication of the server and the client (phone) on the transport layer (TLS connection). License-free clients for EAP-TLS are available for LINUX (for example: Open1x) and Windows XP (integrated).

EAP-TTLS

EAP-TTLS is an extension of EAP-TLS. In addition to enabling authentication via certificates (as does EAP-TLS), EAP-TTLS also allows the use of other EAP methods such as MD5 Challenge and One-Time Password.

Entity

In Information Technology, an entity (synonym: information object) is a uniquely defined object to which information is assigned. The objects can be tangible (like Mount Kilimanjaro) or intangible (like Department RK12 of company Demo Ltd.). An entity may be in a relationship with other entities as well as with itself.

Host Mode

Host mode is a switch command in the format

```
dot1x host-mode {multi-host | single-host}
```

This configuration command determines whether a single authenticated host (client) or several authenticated hosts are permitted at the IEEE802.1X port.

IIS

Microsoft HTTP server

LEAP

Cisco Light EAP uses login and password-based authentication. It is a proprietary protocol developed by Cisco and it supports session keys which are replaced after a certain period.

Multi-Domain

Multi-Domain authentication allows an IP phone and a PC, for example, to authenticate on the same switch port while it places them on appropriate Voice and Data VLANs. Note that Cisco firmly restricts the assignment to 1 device/user in the Voice VLAN and 1 device/user in the Data VLAN.

Multi Host

See → Host Mode

Multi-User Authentication

This allows several users or devices to authenticate on the port and enables assignment of different policies. Multi-User authentication is an Enterasys implementation enabling the separate authentication of several devices/users on a physical port.

PAE

Port Authentication Entities

PEAP

Protected EAP works in a similar way to TTLS and likewise uses a tunnel. PEAP only supports the transport of other EAP authentications, however. It is a proprietary protocol and is mainly supported by Microsoft and Cisco.

PING

Abbreviation for "**P**acket **I**nternet **G**roper".

An echo request packet is sent to the target address. If the target supports the protocol and if it is available, it returns an echo reply.

Proxy EAPoL-Logoff

See → EAPoL-Logoff

Public Key Infrastructure (PKI)

Provides an arrangement for using public keys and is a combination of software, encryption technologies and services. A PKI should provide the following functions:

- Certificate Authorities that can issue and revoke certificates
- Public directories where certificates are stored and can be looked up
- Tools for management of keys and certificates
- Programs and applications that can use public keys.

RADIUS

RADIUS (**R**emote **A**uthentication **D**ial-In **U**ser **S**ervice – specified in [RADIUS, RFC 2865](#)) is a protocol used for authentication in distributed RAS solutions. It facilitates the exchange of authentication, authorization and configuration data between a central authentication server and the local **N**etwork **A**ccess **S**ervers (NAS), which work as clients of the RADIUS server. If a user works remotely and connects to the NAS, the NAS requests a username, password, NAS ID and port ID. The server then verifies the information (and, if necessary, the requirements for the session and the service ports) using the RADIUS database. Thus, for each user the use of higher IP protocols can be allowed or denied individually and to centrally manage all of this. RADIUS supports a number of authentication methods, including PAP, CHAP and EAP.

RAS

Remote **A**ccess **S**ervice is an application-oriented data communication service which allows a user working remotely to access the corporate network, for example.

SAM

The **S**ecurity **A**ccount **M**anager manages the local user accounts.

Single Host

See → Host Mode

Supplicant

In the context of IEEE 802.1X, a supplicant is a client which issues a request for network access to an authenticator.

VLAN

A **V**irtual **L**ocal **A**rea **N**etwork is located within a physical switch or an entire network. A distinction is made between port-based and packet-based tagged VLANs, which are defined under the IEEE 802.1Q standard. The shortened form is dot1q (Cisco switches). Tagged VLANs can be described as networks that use network packets with VLAN marking.

Wrapper

Generally speaking, this is a program acting as the interface between the calling and the "wrapped" program code. Wrappers can be used for compatibility reasons if, for instance, the wrapped code uses a different programming language, for security reasons, that is, to restrict or extend access, or for emulation purposes. A program initially written for DirectX can thus be modified to use OpenGL for graphics.

A Certificate Authority may be a specific company (for example: GlobalSign, Cybertrust, VeriSign) or an institution within a company that has installed their own server (for example: Microsoft Certificate Server). Public bodies and government agencies may also act as CAs (like the Federal Network Agency in Germany).

Abbreviations

This list comprises the abbreviations used in this manual.

Abbreviation	Definition
--------------	------------

AP	Access Point
CA	Certificate Authority
DHCP	Dynamic Host Configuration Protocol.
DLS	Deployment and Licensing Service
DNS	Domain name server
EAP	Extensible Authentication Protocol
EAPOL	Extensible Authentication Protocol Over LAN
FTP	File Transfer Protocol“.
IAS	Internet Authentication Service
IETF	Internet Engineering Task Force; Internet standards body
IIIS	Internet Information Server
IP	Internet Protocol
NAP	Network Access Protection
NPS	Network Policy Server
PEAP	Protected Extensible Authentication Protocol
PKI	Public Key Infrastructure
RFC	Request For Comments; A IETF Protocol Specification
TAP	Techniker Arbeits Platz (in most cases an engineer’s notebook, equipped with special software and hardware)
TLS	Transport Layer Security
TTLS	Tunneled Transport Layer Security
VID	Virtual LAN ID (0-4095)
VLAN	Virtual LAN

Index

C

Certificate	
formats	28
receive, create	17
sample	29
Certificate Authority	12
Certificate service	12

E

EAP-TLS	25
---------------	----

F

Flow chart	15
------------------	----

I

IEEE	12
Import client certificate	27
Import root certificate	26

L

Linux	14, 17
Logon name	18

O

OpenSSL	
installation	17
openSuSE 11.2	14, 17

R

Rules for logon names	18
-----------------------------	----

T

TinyCA2	17
client certificate	23
root certificate	19
server certificate	21