Configuration Guide

NCP Exclusive Remote Access Solution for
Juniper SRX Gateways

Introduction

Installing VPN components correctly is critical for using a Virtual Private Network (VPN) environment without problems. VPN components must be correctly configured before being deployed in production – correcting configuration errors in production is made complicated by operational procedures, and a haphazard approach to VPN configuration is not recommended.

This configuration guide represents NCP's extensive experience in the installation and configuration of VPNs with the Juniper SRX Series Services Gateways and the NCP Secure Enterprise Management. The configuration guide describes a step-by-step guide for configuring each of the VPN components to achieve a working, correctly configured VPN infrastructure.

1. Configuration of NCP RADIUS Server

The NCP Secure Enterprise Management Server comes with a built in RADIUS server. The RADIUS server can be used in conjunction with SRX to authenticate users

Configure SRX

```
set security ike gateway RAVPN_GW tcp-encap-profile NCP
set security tcp-encap profile NCP
```

Configure SRX to use NCP Secure Enterprise Management Server as RADIUS server

CLI Quick Configuration

```
set security ike gateway RAVPN_GW aaa access-profile radius
set access profile radius authentication-order radius
set access profile radius radius-server 10.20.46.234 port 1812
set access profile radius radius-server 10.20.46.234 secret "12345678"
```

Step-by-step Procedure

1) Define access profile in gateway

```
set security ike gateway RAVPN_GW aaa access-profile radius
```

2) Create access profile

```
set access profile radius authentication-order radius
set access profile radius radius-server 10.20.46.234 port 1812
set access profile radius radius-server 10.20.46.234 secret "12345678"
```

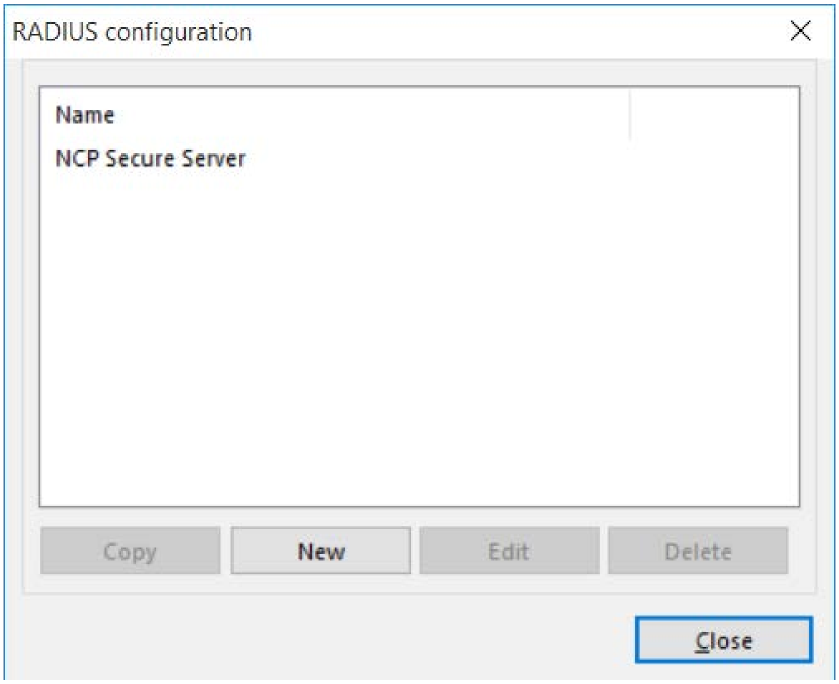
3) Commit changes

```
commit
```

2. Configure NCP Secure Enterprise Management Server to allow RADIUS requests from SRX

Open the NCP Secure Management Console and connect to the NCP Secure Management Server

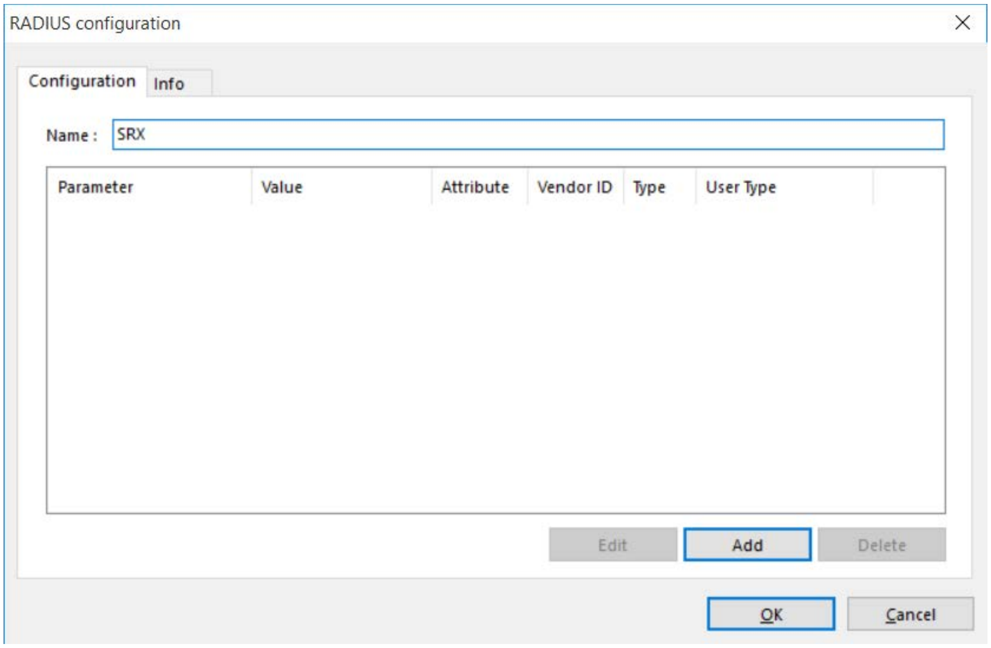
Go to “RADIUS” – Configuration and create a new Entry for SRX



RADIUS configuration

Name

NCP Secure Server



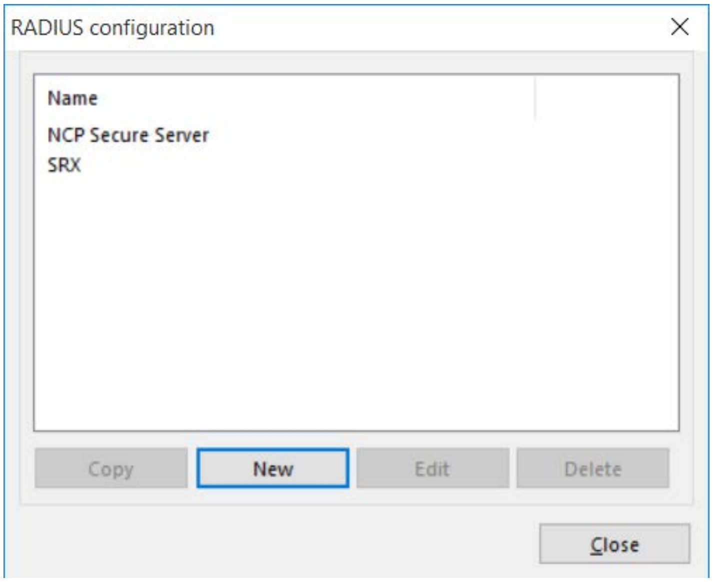
RADIUS configuration

Configuration | Info

Name : SRX

Parameter	Value	Attribute	Vendor ID	Type	User Type

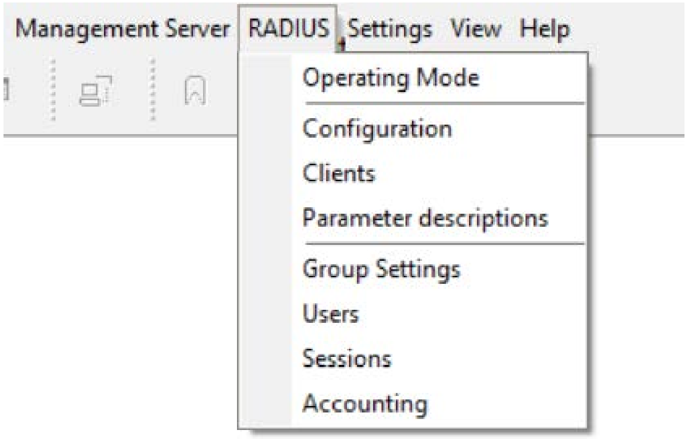
No Information needs to be added. Click “OK”



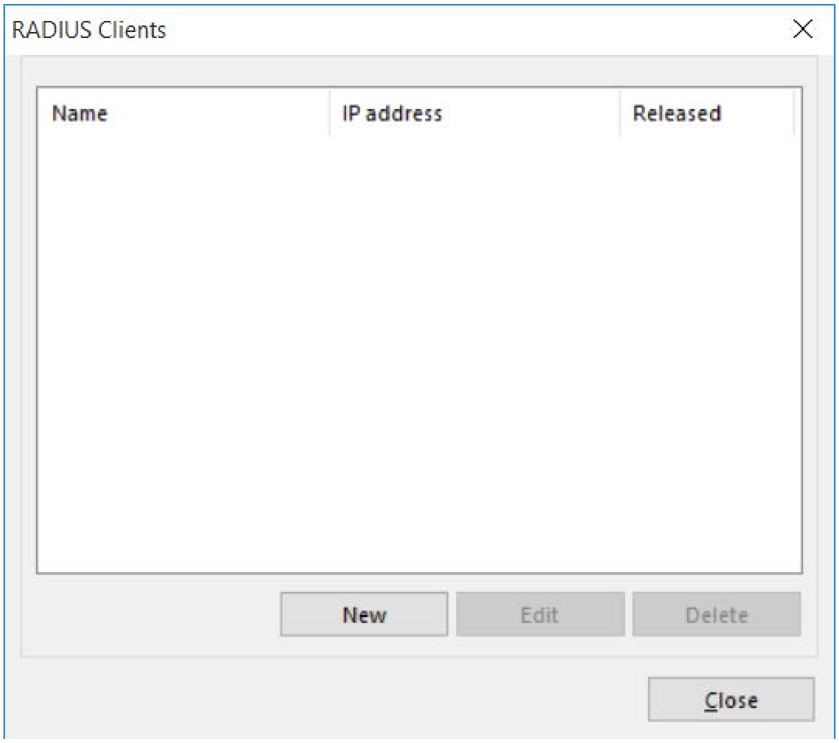
RADIUS configuration

Name
NCP Secure Server
SRX

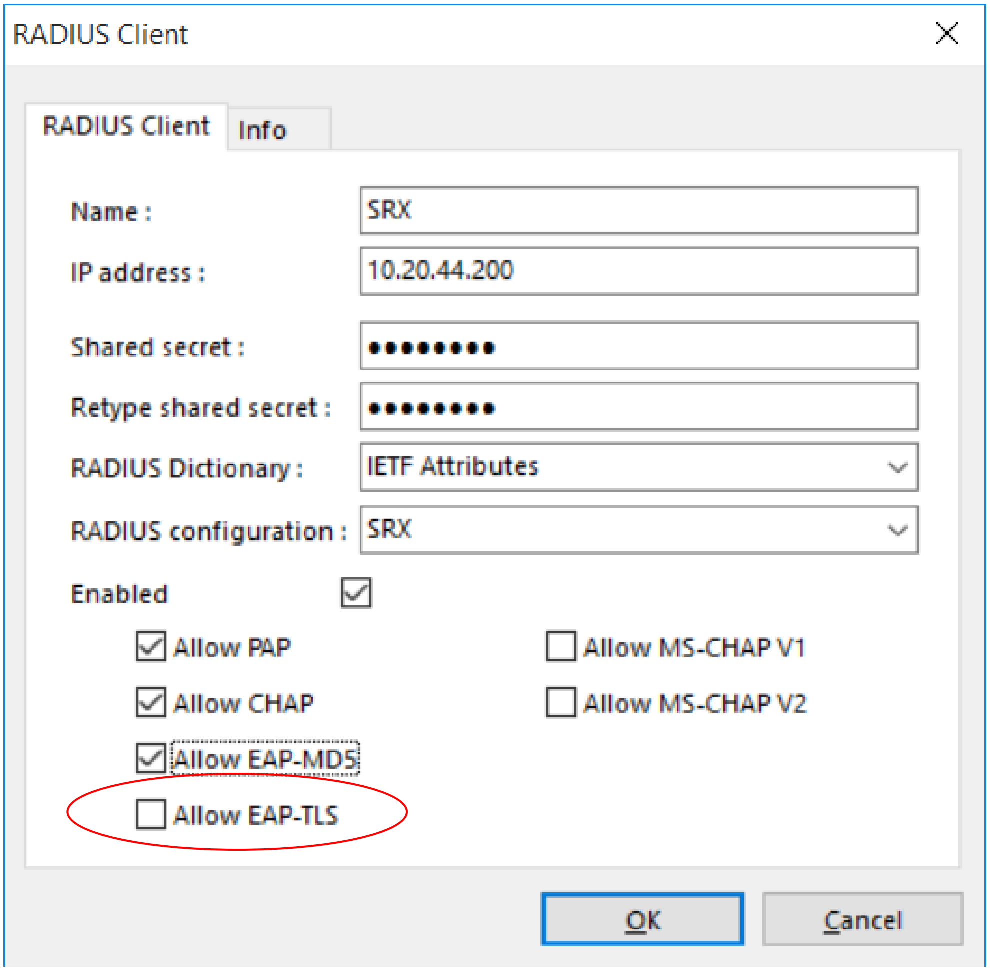
Go to “RADIUS” – “Clients”



Create a new RADIUS Client



For EAP-MD5 click “Allow EAP-MD5”



Name : SRX

IP address : 10.20.44.200

Shared secret : ●●●●●●●●

Retype shared secret : ●●●●●●●●

RADIUS Dictionary : IETF Attributes

RADIUS configuration : SRX

Enabled ☑

☑ Allow PAP

☐ Allow MS-CHAP V1

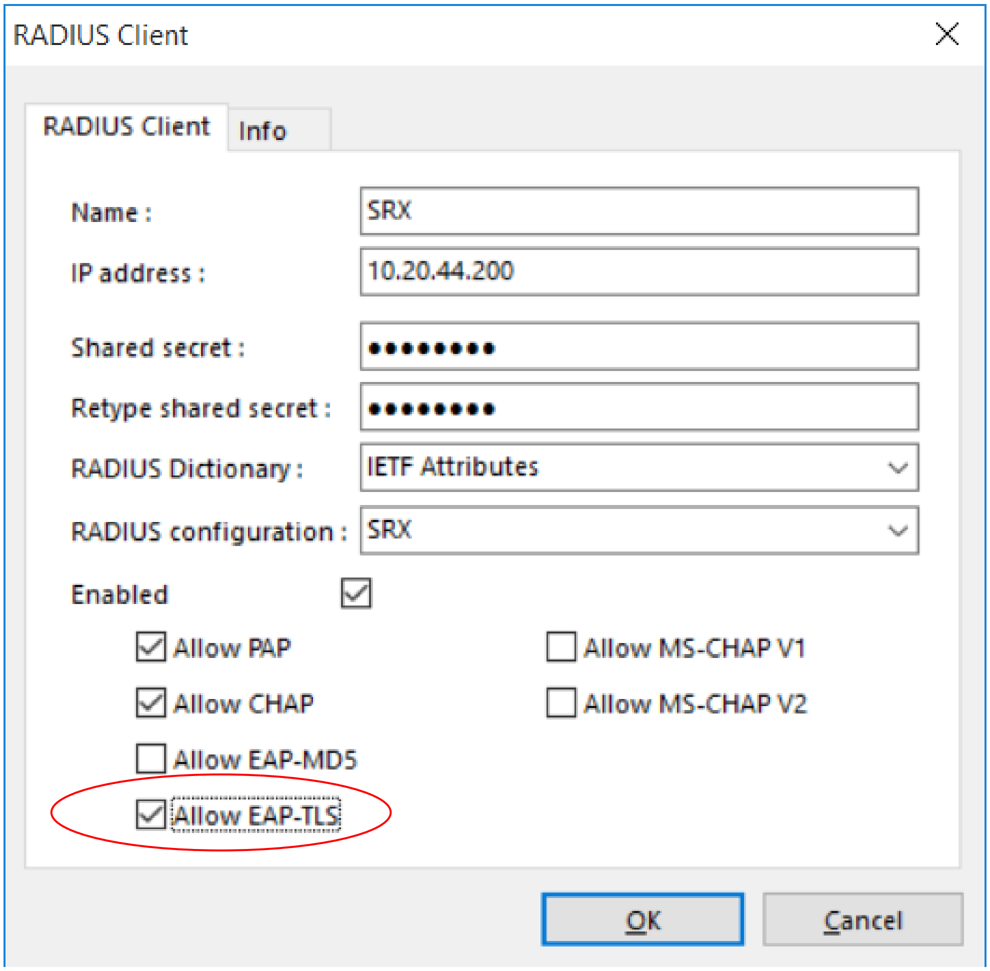
☑ Allow CHAP

☐ Allow MS-CHAP V2

☑ Allow EAP-MD5

☐ Allow EAP-TLS

For EAP-TLS click “Allow EAP-TLS”



RADIUS Client

Name : SRX

IP address : 10.20.44.200

Shared secret : ●●●●●●●●●

Retype shared secret : ●●●●●●●●●

RADIUS Dictionary : IETF Attributes

RADIUS configuration : SRX

Enabled ☑

☑ Allow PAP

☐ Allow MS-CHAP V1

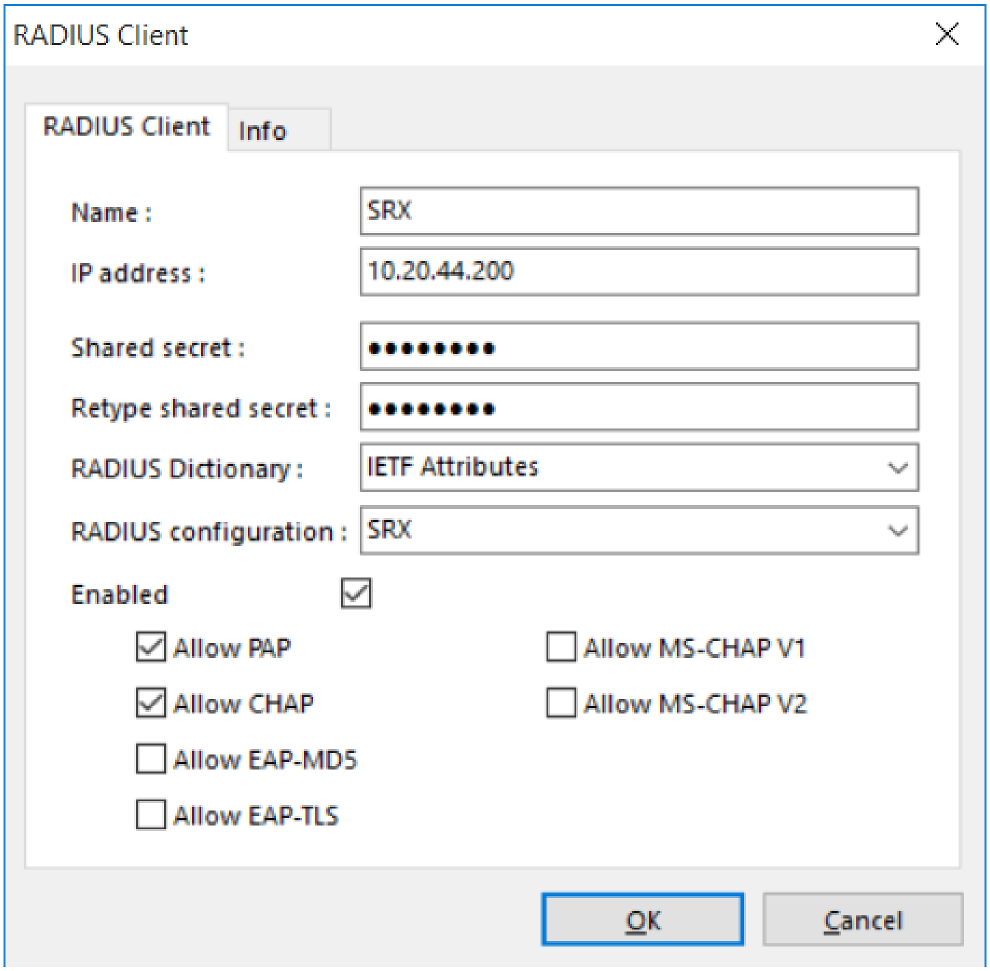
☑ Allow CHAP

☐ Allow MS-CHAP V2

☐ Allow EAP-MD5

☑ Allow EAP-TLS

IKEv1



RADIUS Client

RADIUS Client | Info

Name : SRX

IP address : 10.20.44.200

Shared secret : ●●●●●●●●●

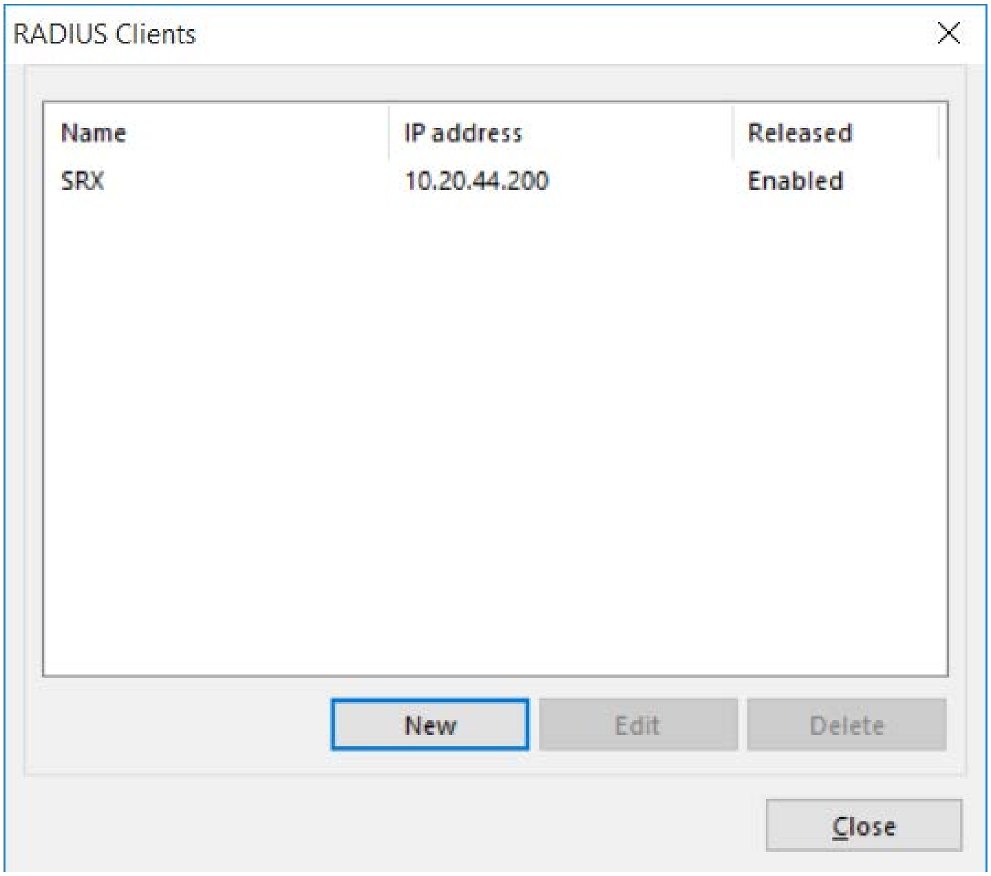
Retype shared secret : ●●●●●●●●●

RADIUS Dictionary : IETF Attributes

RADIUS configuration : SRX

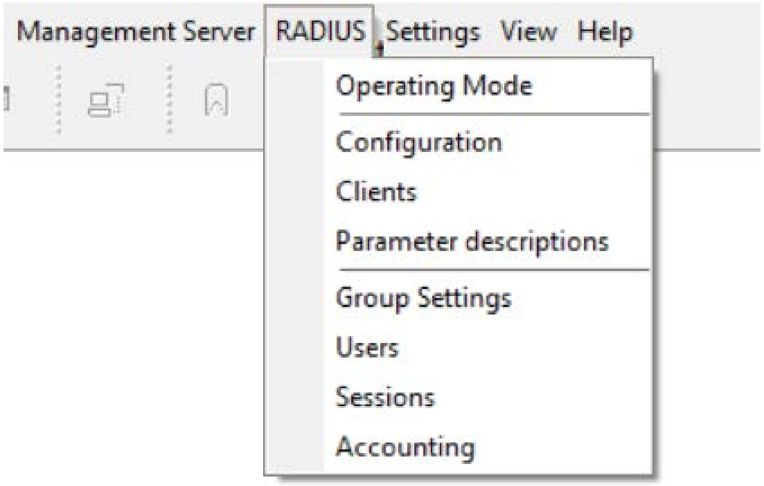
Enabled ☑

☑ Allow PAP
☑ Allow CHAP
☐ Allow EAP-MD5
☐ Allow EAP-TLS
☐ Allow MS-CHAP V1
☐ Allow MS-CHAP V2

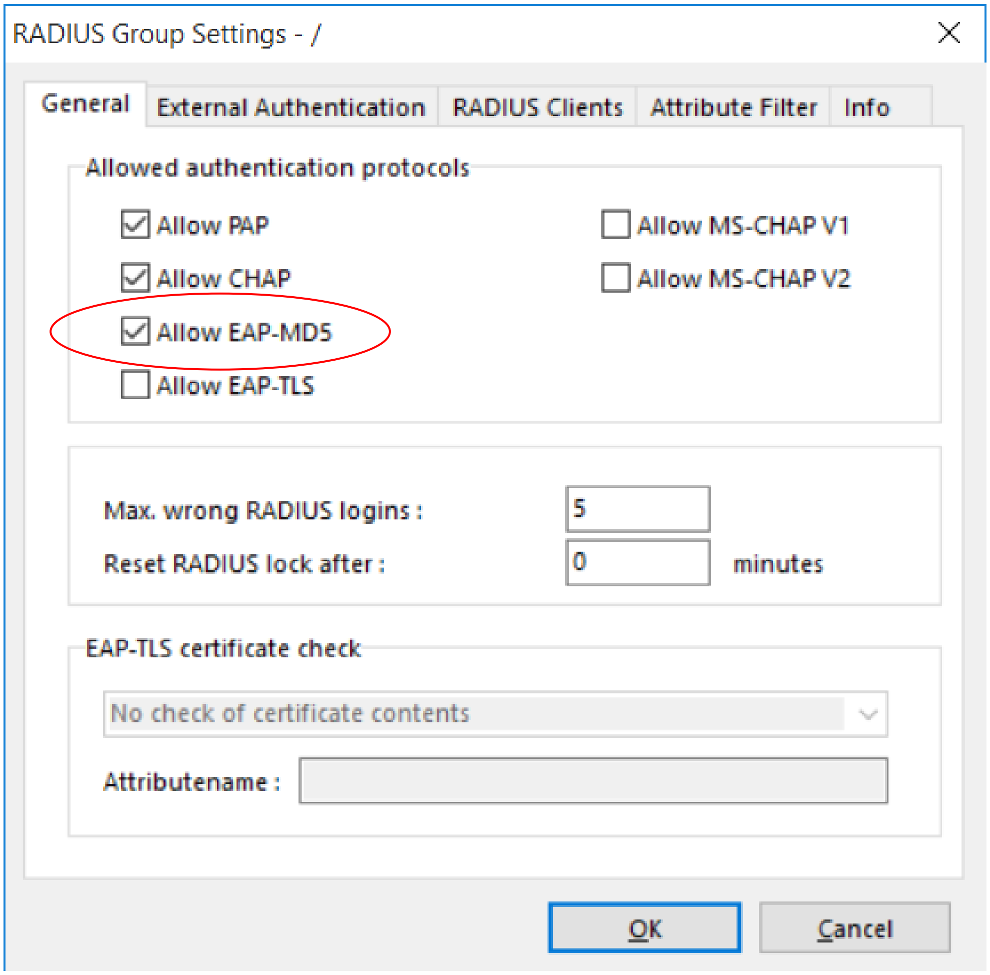


Name	IP address	Released
SRX	10.20.44.200	Enabled

Go to “RADIUS” – “Group Settings”



For EAP-MD5 click “Allow EAP-MD5”



RADIUS Group Settings - /

Allowed authentication protocols

☑ Allow PAP

☑ Allow CHAP

☑ Allow EAP-MD5

□ Allow EAP-TLS

□ Allow MS-CHAP V1

□ Allow MS-CHAP V2

Max. wrong RADIUS logins : 5

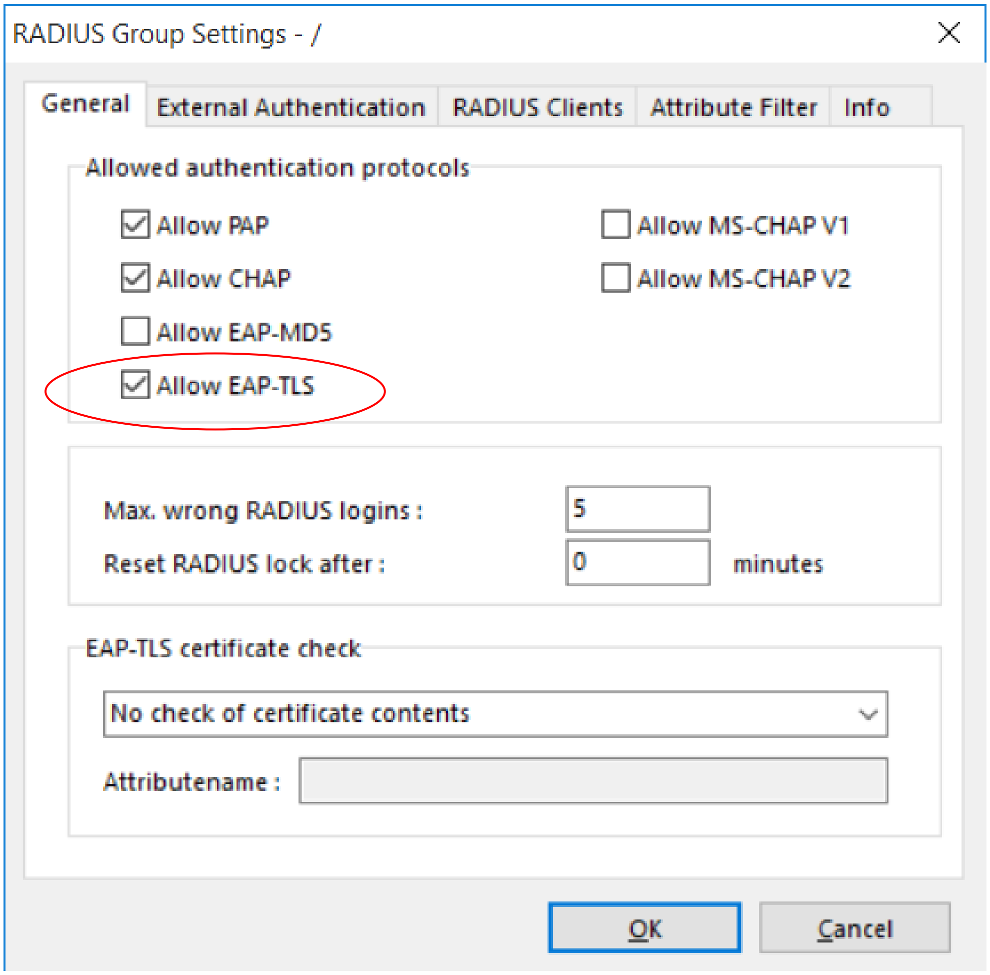
Reset RADIUS lock after : 0 minutes

EAP-TLS certificate check

No check of certificate contents

Attributename :

For EAP-MD5 click “Allow EAP-MD5”



RADIUS Group Settings - /

Allowed authentication protocols

☑ Allow PAP
☐ Allow MS-CHAP V1
☑ Allow CHAP
☐ Allow MS-CHAP V2
☐ Allow EAP-MD5
☑ Allow EAP-TLS

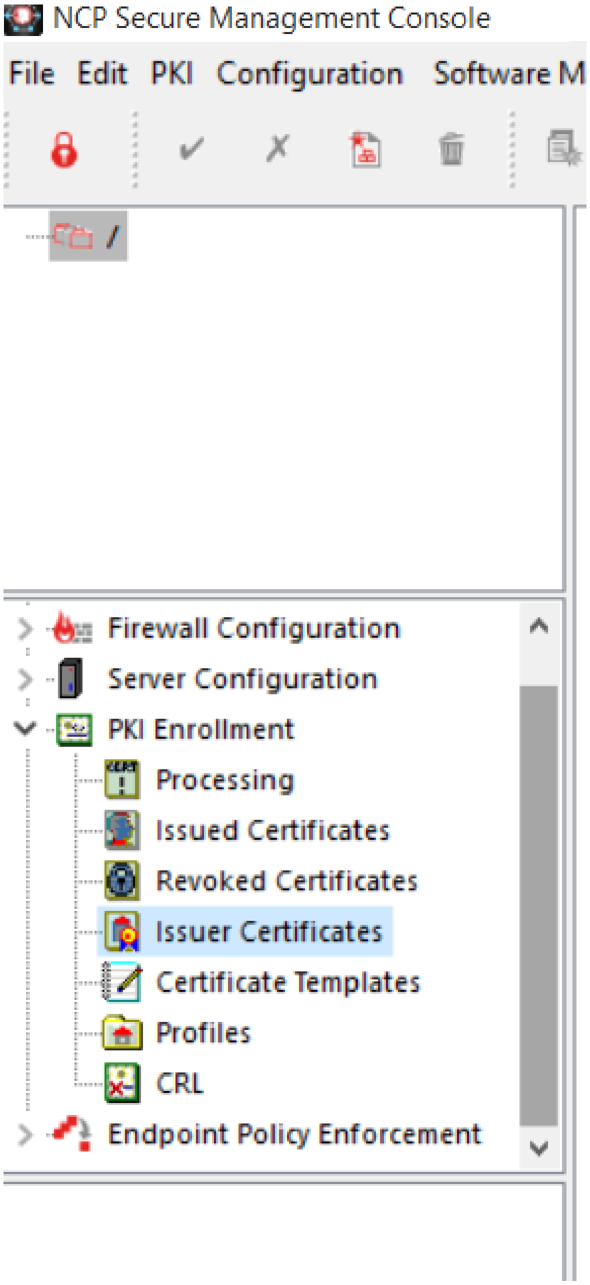
Max. wrong RADIUS logins : 5

Reset RADIUS lock after : 0 minutes

EAP-TLS certificate check

No check of certificate contents

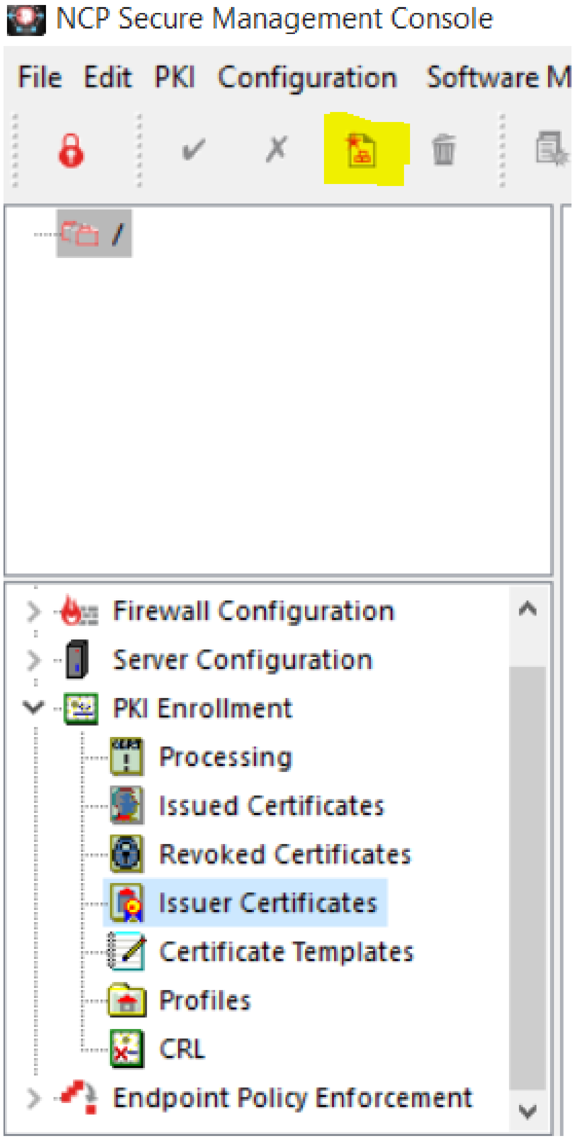
Attributename :

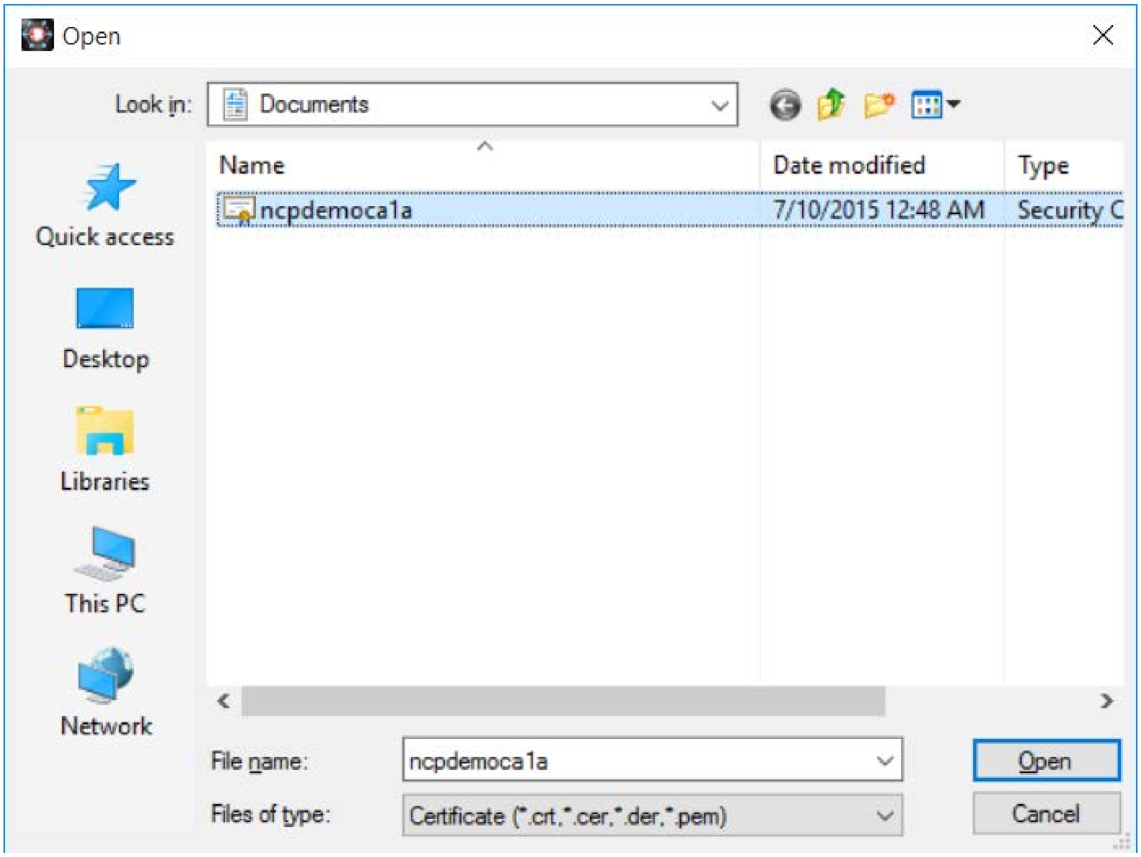


If EAP is used, you need to import the CA/issuer certificate into the NCP Secure Management Server.

Go to “PKI Enrollment” – “Issuer Certificates”

Import the CA/issuer profile by clicking on the “New Entry” icon on the menue



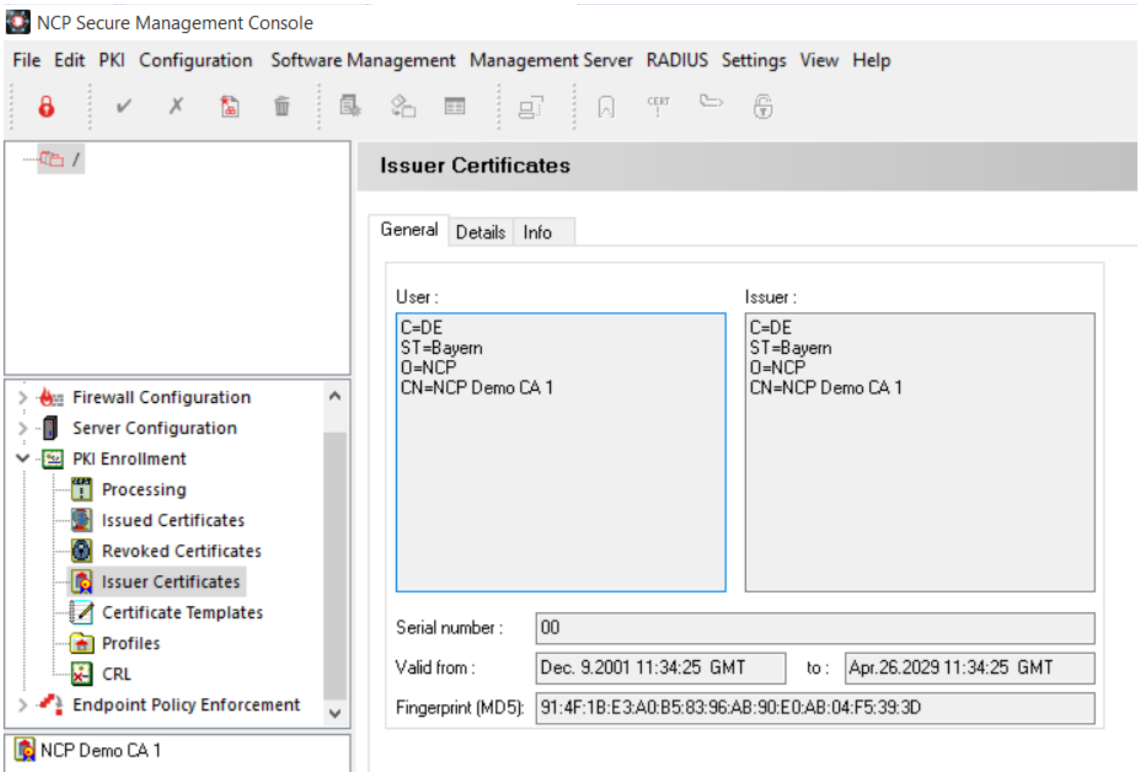


Look in: Documents

Name	Date modified	Type
ncpdemoca1a	7/10/2015 12:48 AM	Security C

File name: ncpdemoca1a

Files of type: Certificate (*.crt,*.cer,*.der,*.pem)



User :
C=DE
ST=Bayern
O=NCP
CN=NCP Demo CA 1

Issuer :
C=DE
ST=Bayern
O=NCP
CN=NCP Demo CA 1

Serial number : 00

Valid from : Dec. 9.2001 11:34:25 GMT to : Apr.26.2029 11:34:25 GMT

Fingerprint (MD5): 91:4F:1B:E3:A0:B5:83:96:AB:90:E0:AB:04:F5:39:3D

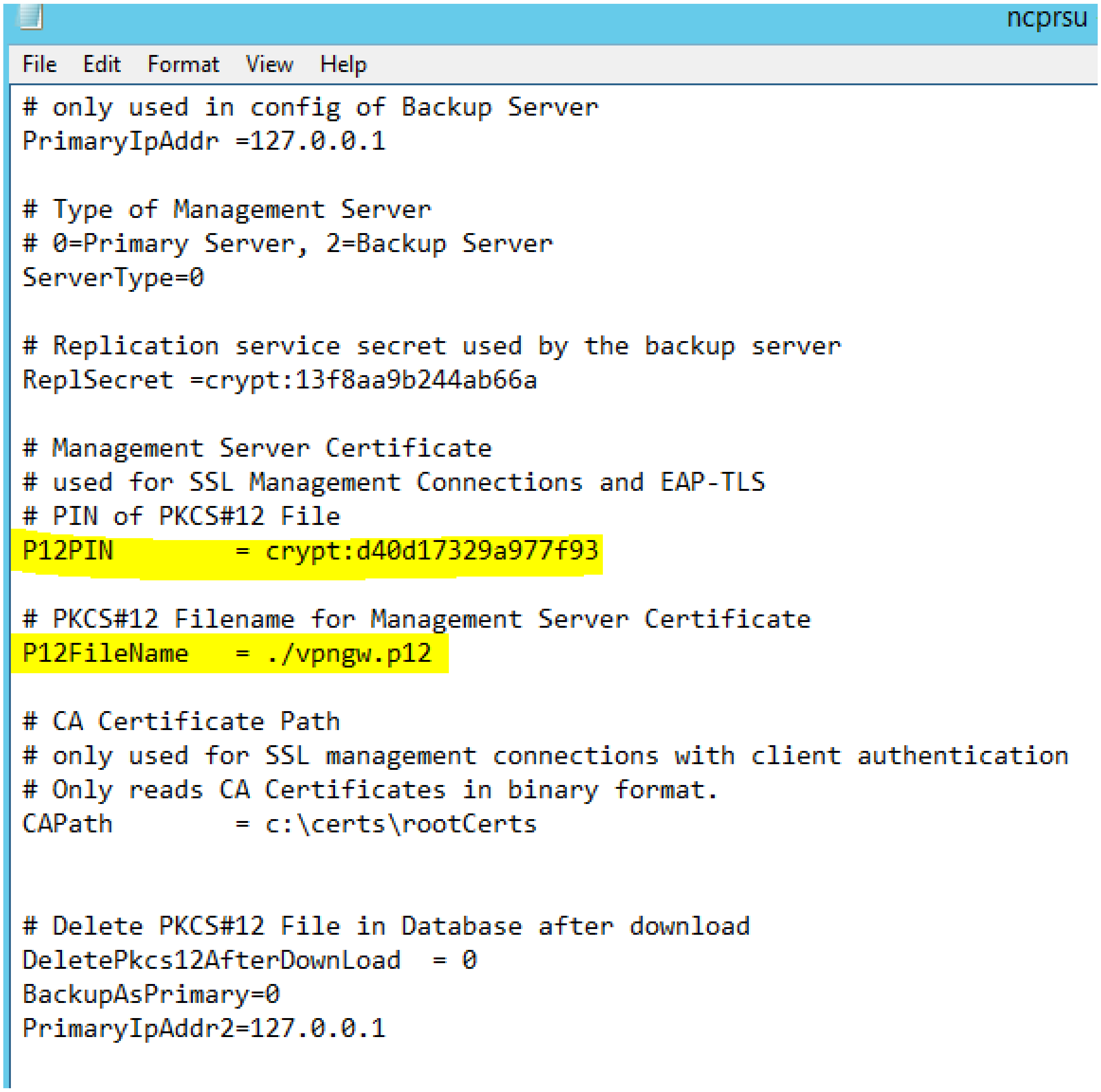
3. Configure the server certificate used for EAP-TLS on the NCP Management Server

Open the file ncprsu.conf

Windows: C:\Program Files\NCP\ManagementServer\ncprsu.conf

Linux: /opt/ncp/sem/ncprsu.conf

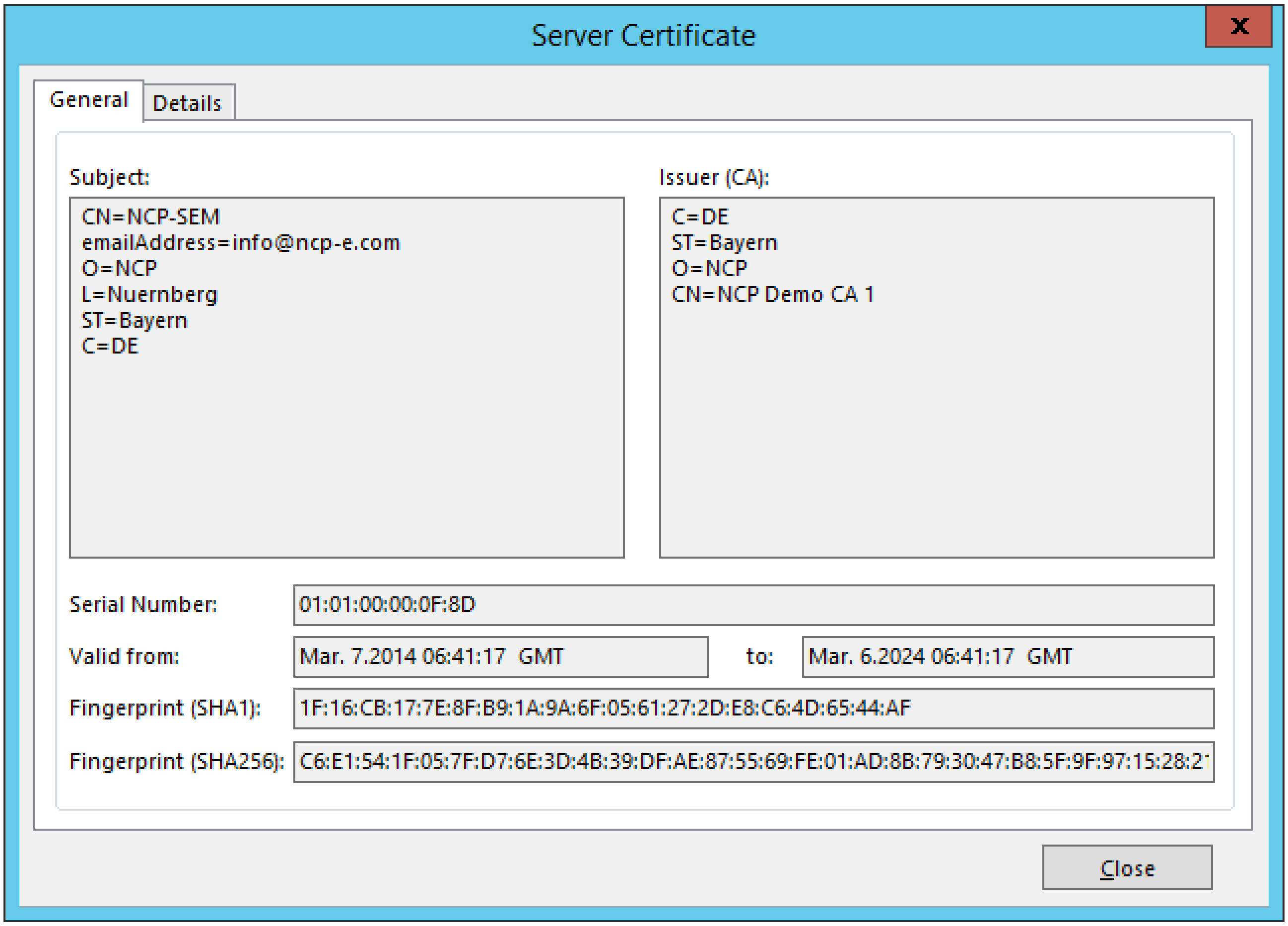
Enter the PIN of the server certificate and the path to the certificate



```
# only used in config of Backup Server
PrimaryIpAddr =127.0.0.1

# Type of Management Server
# 0=Primary Server, 2=Backup Server
ServerType=0

# Replication service secret used by the backup server
ReplSecret =crypt:13f8aa9b244ab66a

# Management Server Certificate
# used for SSL Management Connections and EAP-TLS
# PIN of PKCS#12 File
P12PIN         = crypt:d40d17329a977f93

# PKCS#12 Filename for Management Server Certificate
P12FileName    = ./vpngw.p12

# CA Certificate Path
# only used for SSL management connections with client authentication
# Only reads CA Certificates in binary format.
CAPath         = c:\certs\rootCerts


# Delete PKCS#12 File in Database after download
DeletePkcs12AfterDownLoad   = 0
BackupAsPrimary=0
PrimaryIpAddr2=127.0.0.1
```

Restart all NCP service or reboot the server.

The server certificate will be shown in the NCP Management Console on “Management Server” – “Server Certificate”



Subject:
CN=NCP-SEM
emailAddress=info@ncp-e.com
O=NCP
L=Nuernberg
ST=Bayern
C=DE

Issuer (CA):
C=DE
ST=Bayern
O=NCP
CN=NCP Demo CA 1

Serial Number: 01:01:00:00:0F:8D

Valid from: Mar. 7.2014 06:41:17 GMT to: Mar. 6.2024 06:41:17 GMT

Fingerprint (SHA1): 1F:16:CB:17:7E:8F:B9:1A:9A:6F:05:61:27:2D:E8:C6:4D:65:44:AF

Fingerprint (SHA256): C6:E1:54:1F:05:7F:D7:6E:3D:4B:39:DF:AE:87:55:69:FE:01:AD:8B:79:30:47:B8:5F:9F:97:15:28:2