# Installation and Configuration Guide

# Exclusive Remote Access Solution for Juniper SRX Series

v1.5 – 2017-12-21

**N**etwork
**C**ommunications
**P**roducts engineering

## USA

NCP engineering, Inc.
444 Castro Street, Suite 711
Mountain View, CA 94041
Tel.: +1 (650) 316-6273
Fax: +1 (650) 251-4155

## Germany

NCP engineering GmbH
Dombuehler Str. 2
D-90449 Nuremberg
Tel.: +49 (911) 9968-0
Fax: +49 (911) 9968-299

## Internet

http://www.ncp-e.com

## Email

info@ncp-e.com

## Support

NCP provides support for all international users by means of Fax and E-mail.

## Email Addresses

| | |
|---|---|
| helpdesk@ncp-e.com | (English) |
| support@ncp-e.com | (German) |

## Fax

| | |
|---|---|
| +1 (650) 251-4155 | (USA) |
| +49 (911) 9968-458 | (Europe) |

**When submitting a support request, please include the following information:**

- ► exact product name
- ► serial number
- ► version number
- ► an accurate description of your problem
- ► any error message(s)

## Copyright

While considerable care has been taken in the preparation and publication of this manual, errors in content, typo-graphical or otherwise, may occur. If you have any comments or recommendations concerning the accuracy, then please contact NCP. NCP makes no representations or warranties with respect to the contents or use of this manual, and explicitly disclaims all expressed or implied warranties of merchantability or suitability of use for any particular purpose.
Furthermore, NCP reserves the right to revise this publication and to make amendments to the contents, at any time, without obligation to notify any person or entity of such revisions or changes. This manual is the sole property of NCP and may not be copied for resale, commercial distribution or translated to another language without the express written permission of NCP engineering GmbH.
All trademarks or registered trademarks appearing in this manual belong to their respective owners.

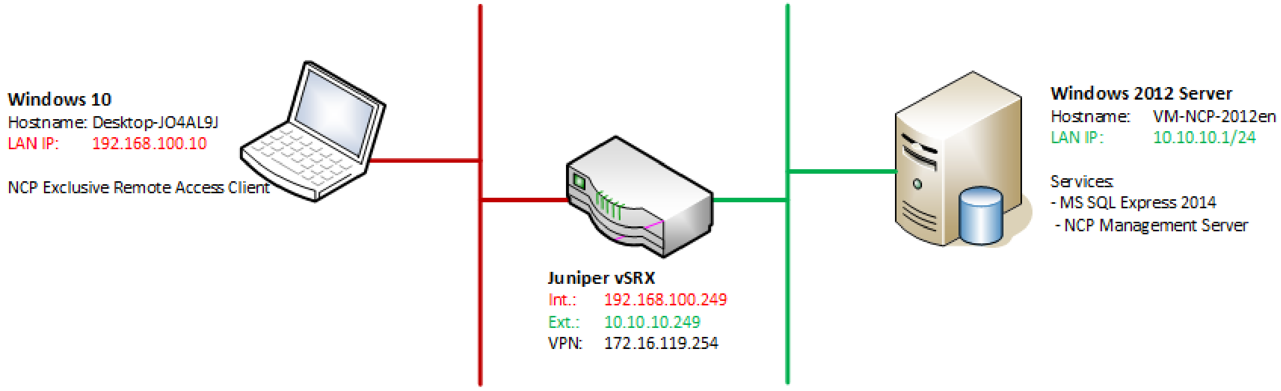
# Table of Contents

# 1. Installation of the NCP Exclusive Remote Access Management Server

## 1.1. Prerequisites

Before installing the NCP Exclusive Remote Access Management Server (in the following referred to as *Management Server*) you have to prepare an empty database with an according ODBC configuration. Please refer to the appendix A - Installation of supported database servers for details.

The scenario used for this documentation is a very simplified one. Underneath you see the systems involved including IP addresses used in this environment.



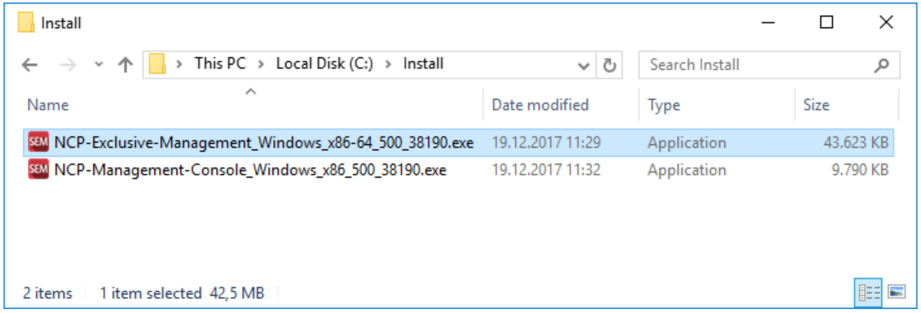
The following files are required for installation of the NCP Exclusive Remote Management solution (where “xxxxx” is the revision number of the released version which was not available while creating this document):

- Installation package for the Management Server
  NCP-Exclusive-Management_Windows_x86-64_500_xxxxx.exe
- Installation package for NCP Secure Management Console
  NCP-Management-Console_Windows_x86_500_xxxxx.exe

## 1.2. Installation of the Management Server on Windows

Open File Explorer and select the folder containing the Management Server installation package.

- Execute the installer package NCP-Exclusive-Management_Windows_x86-64_500_38190.exe



Install

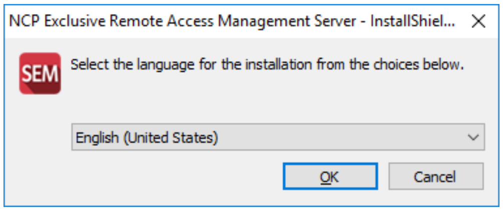
This PC › Local Disk (C:) › Install

Search Install

| Name | Date modified | Type | Size |
|---|---|---|---|
| NCP-Exclusive-Management_Windows_x86-64_500_38190.exe | 19.12.2017 11:29 | Application | 43.623 KB |
| NCP-Management-Console_Windows_x86_500_38190.exe | 19.12.2017 11:32 | Application | 9.790 KB |

2 items 1 item selected 42,5 MB

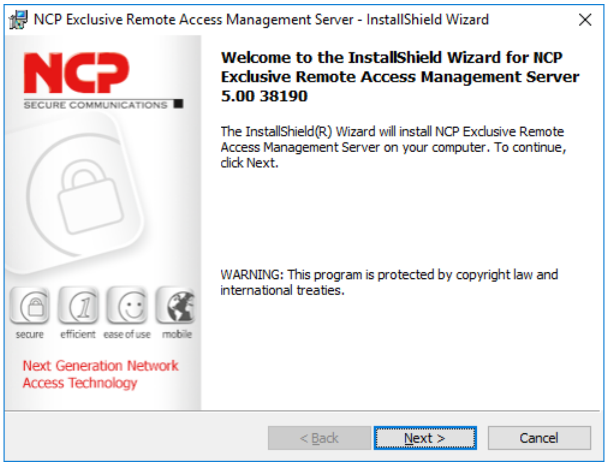
Select the preferred installation language and click next to start the “InstallShield Wizard”



NCP Exclusive Remote Access Management Server - InstallShiel...

Select the language for the installation from the choices below.

English (United States)



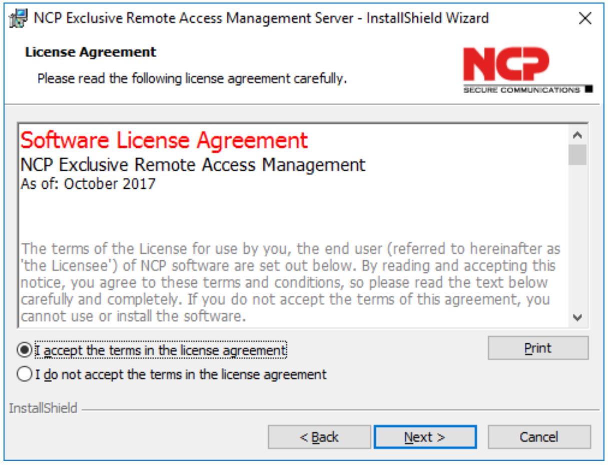
NCP Exclusive Remote Access Management Server - InstallShield Wizard

**Welcome to the InstallShield Wizard for NCP Exclusive Remote Access Management Server 5.00 38190**

The InstallShield(R) Wizard will install NCP Exclusive Remote Access Management Server on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

- Accept the “License Agreement” and select the “Destination Folder”



NCP Exclusive Remote Access Management Server - InstallShield Wizard

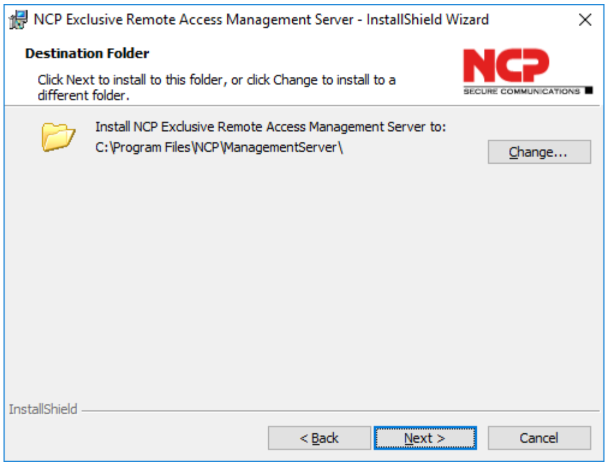
**License Agreement**

Please read the following license agreement carefully.

Software License Agreement
NCP Exclusive Remote Access Management
As of: October 2017

The terms of the License for use by you, the end user (referred to hereinafter as 'the Licensee') of NCP software are set out below. By reading and accepting this notice, you agree to these terms and conditions, so please read the text below carefully and completely. If you do not accept the terms of this agreement, you cannot use or install the software.

● I accept the terms in the license agreement
○ I do not accept the terms in the license agreement



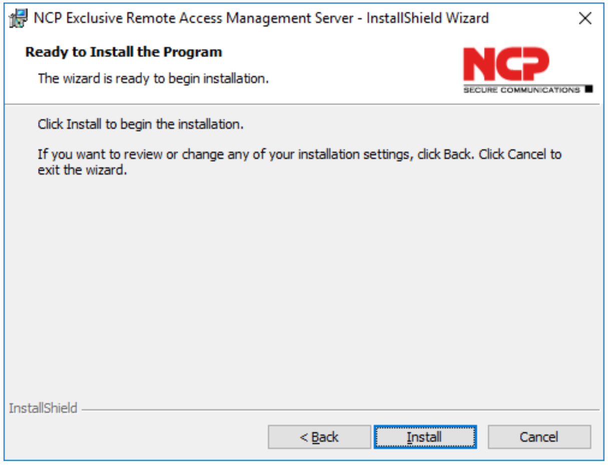
NCP Exclusive Remote Access Management Server - InstallShield Wizard

**Destination Folder**

Click Next to install to this folder, or click Change to install to a different folder.

Install NCP Exclusive Remote Access Management Server to:
C:\Program Files\NCP\ManagementServer\

- Confirm to start the installation by clicking “Install” and the Management Server software will be installed

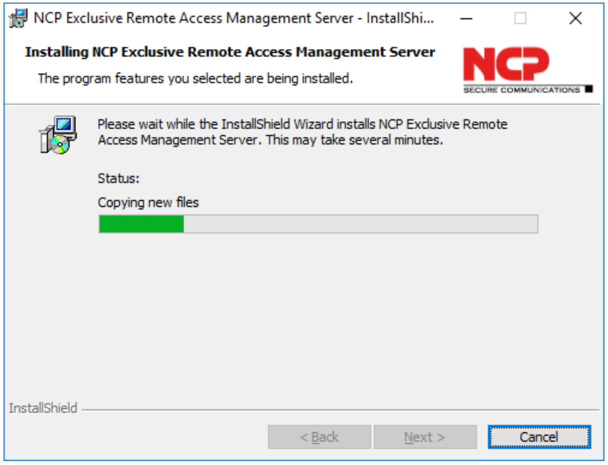

NCP Exclusive Remote Access Management Server - InstallShield Wizard

**Ready to Install the Program**

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.


NCP Exclusive Remote Access Management Server - InstallShi...

**Installing NCP Exclusive Remote Access Management Server**

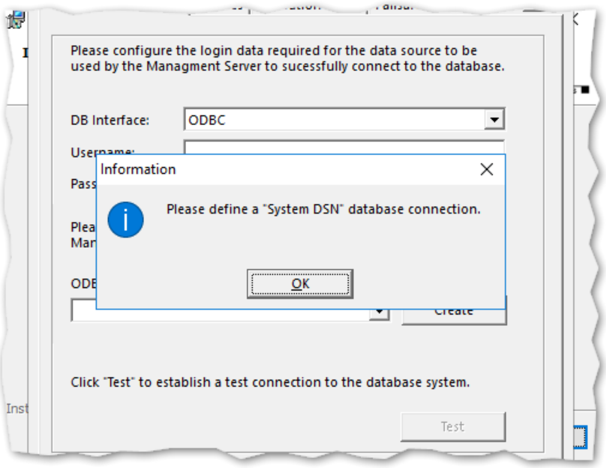
The program features you selected are being installed.

Please wait while the InstallShield Wizard installs NCP Exclusive Remote Access Management Server. This may take several minutes.

Status:

Copying new files

Once the software has been installed the *NCP Management Server – Configuration* will be started. It will come up with options for an ODBC based database connection which is not used in this sample setup. Therefore, press *OK* in the message box shown below and also close (or cancel) the *ODBC Data Source Administrator (64-bit)* dialog.


Please configure the login data required for the data source to be used by the Managment Server to sucessfully connect to the database.

DB Interface: ODBC

Username:

Pass

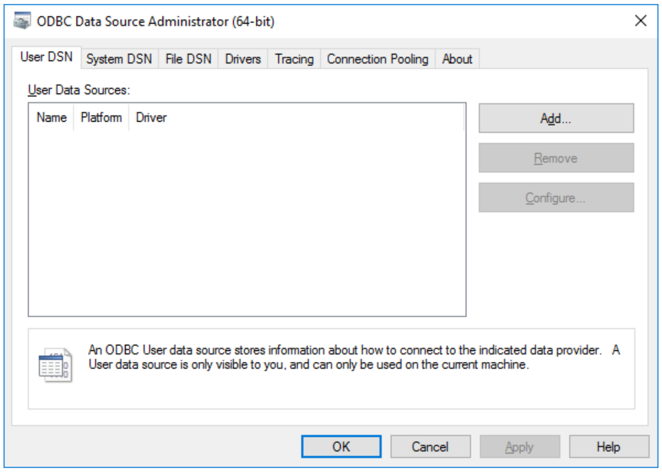
Plea
Mar

ODB

Information

Please define a "System DSN" database connection.

Click "Test" to establish a test connection to the database system.


ODBC Data Source Administrator (64-bit)

User Data Sources:

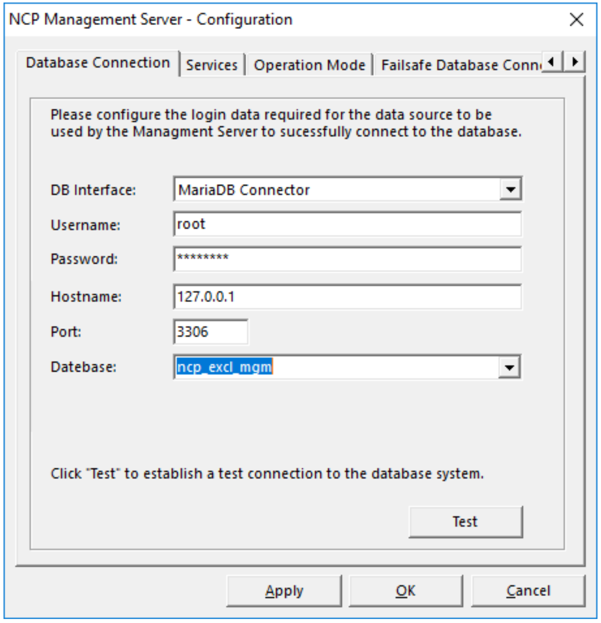
| Name | Platform | Driver |
|---|---|---|

An ODBC User data source stores information about how to connect to the indicated data provider. A User data source is only visible to you, and can only be used on the current machine.

In the tab *Database Connection* of the *NCP Management Server – Configuration*

- As *DB Interface* select *MariaDB Connector*
- Enter *Username* and *Password* of the database administrator
- Enter the *Hostname* or IP address of your database server (here: *localhost* or *127.0.0.1*)
- The standard *Port* for this setup is *3306*

- From the *Database* list select the previously created one (here: *ncp_excl_mgm*)

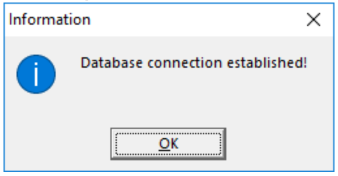

NCP Management Server - Configuration

Please configure the login data required for the data source to be used by the Managment Server to sucessfully connect to the database.

DB Interface: MariaDB Connector
Username: root
Password: ********
Hostname: 127.0.0.1
Port: 3306
Datebase: ncp_excl_mgm

Click "Test" to establish a test connection to the database system.

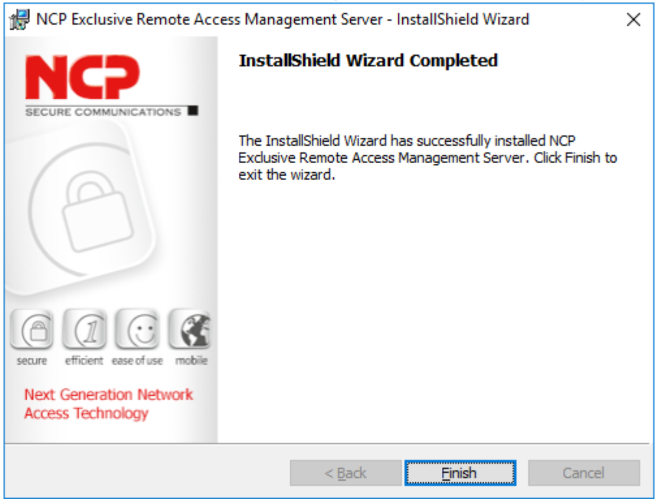
- Click “Apply”
- Click “Test” to verify a working connection
  You should get 'Database connection established!'


Information

Database connection established!

- Press “OK” to finish the installation

The installation of the Management Server is completed now. Press “Finish” in the “InstallShield Wizard”.


NCP Exclusive Remote Access Management Server - InstallShield Wizard

**InstallShield Wizard Completed**

The InstallShield Wizard has successfully installed NCP Exclusive Remote Access Management Server. Click Finish to exit the wizard.

## 1.3. Installation of the Management Server on Linux

### 1.3.1. Preparation of CentOS

This document describes how to install the NCP Exclusive Enterprise Management Server on CentOS 7 Linux. You need to provide a basic installation of CentOS 7 with the necessary routing and access settings required for your specific environment. The installation of the NCP Exclusive Remote Access Management Server requires root privileges. If you want to use an individual user, add the account to the sudoers.

### 1.3.2. Installation of the Management Server

Copy the NCP Exclusive Remote Access Management installation package to the Linux system and apply execute properties. For this document version 5.0 revision 38209 was used. However, the description provided below will apply for later versions as well.
Execute the binary installer ncp-exclusive-management_linux_x86-64_500_38209.bin and follow the instructions displayed in the console. The Management Server will be installed automatically with a 30-day trial license without functional limitations and a maximum of 100 managed units.
Below you see an excerpt of the installation routine:

```
[root@centos tmp]# ./ncp-exclusive-management_linux_x86-64_500_38209.bin
                   ------------------------------------------
                   > NCP Exclusive Remote Access Management <
                   ------------------------------------------

Verifying contained installation data... succeeded
Unpacking installation data... succeeded

=== Calling installation routine ===

Checking compatibility... succeeded

No previous installation of this product was found.

You are about to install the following product version:

        Product code name: sem
        Product full name: NCP Exclusive Remote Access Management
        Product version: 5.00
        OEM variant: junipersrx
        Target architecture: x86_64
        Target OS: linux
        Library type: shared
        Build type: release-speed
        Build label: trunk
        Build revision: rev38209
        Build date: Wed 20 Dec 2017 01:40:16 PM CET

Do you want to perform this installation?

        (yes/y/no/n): y

.
```

```
.
.

Installing
data.......................................................................................................
.......................................................................................................
............... succeeded

NCP Exclusive Remote Access Management has been successfully configured to start on boot.

NCP Exclusive Remote Access Management can be started by using the command

        /usr/bin/systemctl start ncp-sem.service

and stopped by using the command

        /usr/bin/systemctl stop ncp-sem.service
```

After the installation the Management Server cannot yet be started due to the database configuration still missing.

### 1.3.3. Configuration of the Management Server for MariaDB with Connector/C

Edit the `DB` section in the Management Server's configuration file `/opt/ncp/sem/ncprsu.conf` as shown below:

```
[DB]
DriverType       = mysql
DBUserName       = mydbadmin
DBPassword       = mypassword
Host             = 127.0.0.1
Port             = 3306
Database         = mydatabase
LibraryFileName  = /usr/lib64/mysql/libmysqlclient.so.18
```

### 1.3.4. Launching the Management Server

Now the Management Server has to be started which can be done with a reboot or by executing the command stated below:

```
sudo systemctl start ncp-sem.service
```

A CentOS default installation will automatically have the firewall enabled denying most incoming communication to the system also blocking the Management Console to connect. The easiest way to get around this is to disable the firewall on CentOS, as described below. Please make sure to follow your internal security policies whether this is a valid approach for your environment!

```
sudo systemctl disable firewalld
sudo systemctl stop firewalld
```

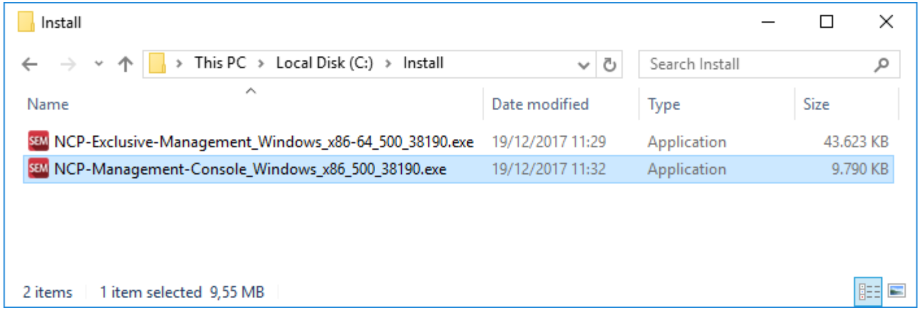
Now you can use the Management Console to work with the Management Server.

# 2. Management Console and plug-ins

## 2.1. Installation of the Management Console

Open File Explorer and select the folder containing the Management Server installation package.

- Execute the installer package NCP-Management-Console_Windows_x86_500_38190.exe



Install

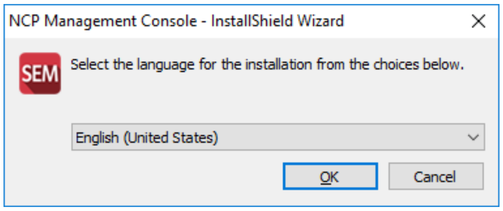
This PC › Local Disk (C:) › Install

Search Install

| Name | Date modified | Type | Size |
|---|---|---|---|
| NCP-Exclusive-Management_Windows_x86-64_500_38190.exe | 19/12/2017 11:29 | Application | 43.623 KB |
| NCP-Management-Console_Windows_x86_500_38190.exe | 19/12/2017 11:32 | Application | 9.790 KB |

2 items 1 item selected 9,55 MB

- Select the preferred installation language and Click next to start the “InstallShield Wizard”

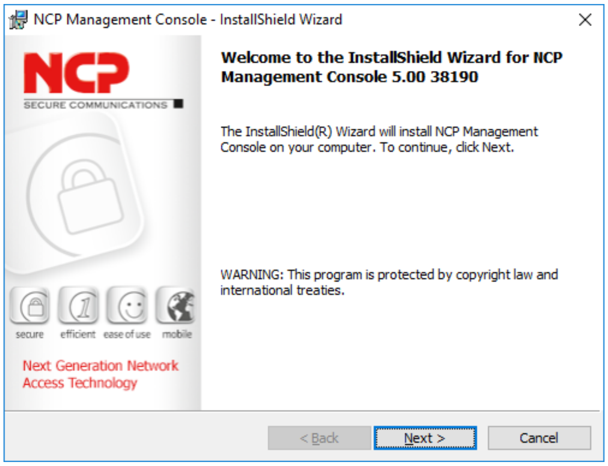


NCP Management Console - InstallShield Wizard

Select the language for the installation from the choices below.

English (United States)

OK Cancel



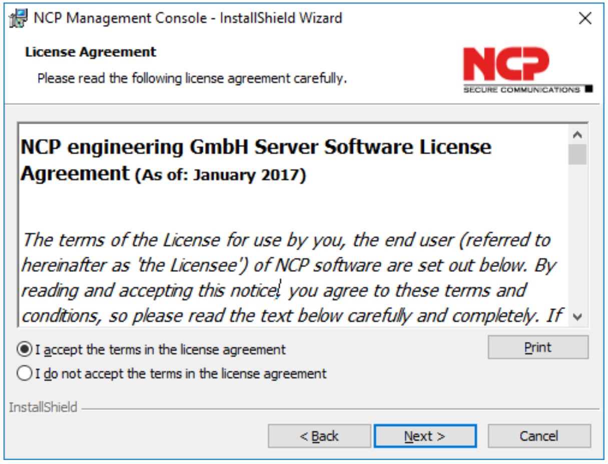
NCP Management Console - InstallShield Wizard

**Welcome to the InstallShield Wizard for NCP Management Console 5.00 38190**

The InstallShield(R) Wizard will install NCP Management Console on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

- Accept the “License Agreement” and select the “Destination Folder”



NCP Management Console - InstallShield Wizard

**License Agreement**

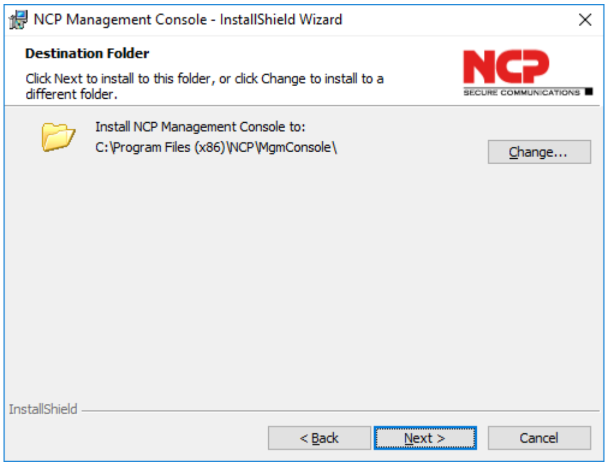
Please read the following license agreement carefully.

**NCP engineering GmbH Server Software License Agreement (As of: January 2017)**

*The terms of the License for use by you, the end user (referred to hereinafter as 'the Licensee') of NCP software are set out below. By reading and accepting this notice, you agree to these terms and conditions, so please read the text below carefully and completely. If*

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement



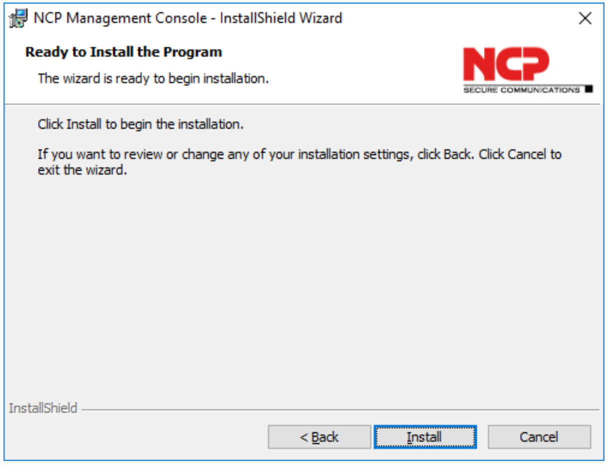
NCP Management Console - InstallShield Wizard

**Destination Folder**

Click Next to install to this folder, or click Change to install to a different folder.

Install NCP Management Console to:
C:\Program Files (x86)\NCP\MgmConsole\

- Confirm to start the installation by clicking “Install”



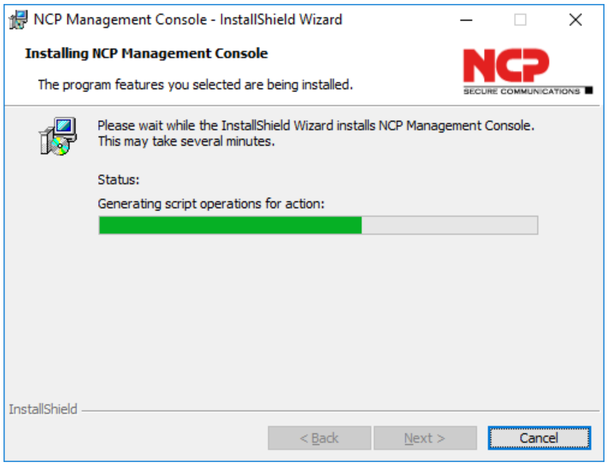
NCP Management Console - InstallShield Wizard

**Ready to Install the Program**

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.



NCP Management Console - InstallShield Wizard

**Installing NCP Management Console**

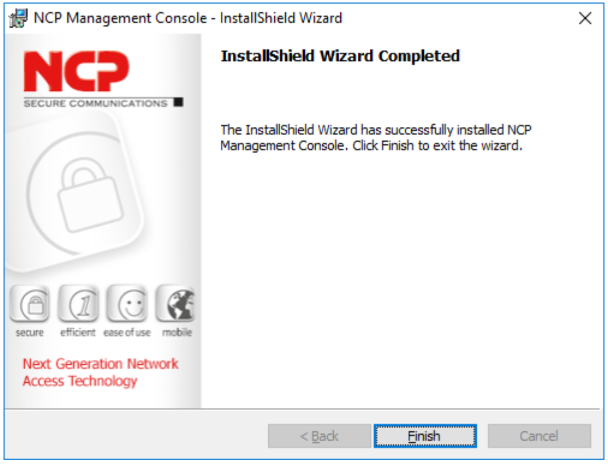
The program features you selected are being installed.

Please wait while the InstallShield Wizard installs NCP Management Console. This may take several minutes.

Status:

Generating script operations for action:

- The installation of the Management Console is completed now. Press “Finish” in the “InstallShield Wizard”.



NCP Management Console - InstallShield Wizard

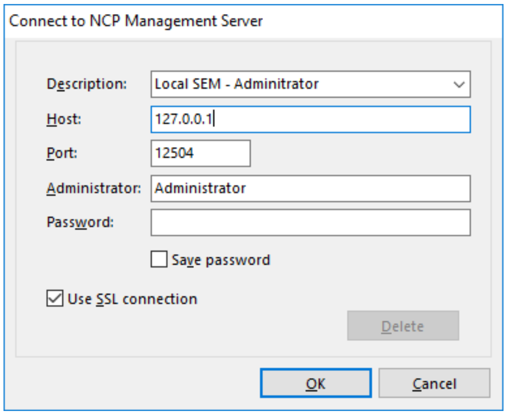
**InstallShield Wizard Completed**

The InstallShield Wizard has successfully installed NCP Management Console. Click Finish to exit the wizard.

NCP SECURE COMMUNICATIONS
secure
efficient
ease of use
mobile
Next Generation Network Access Technology
< Back
Finish
Cancel

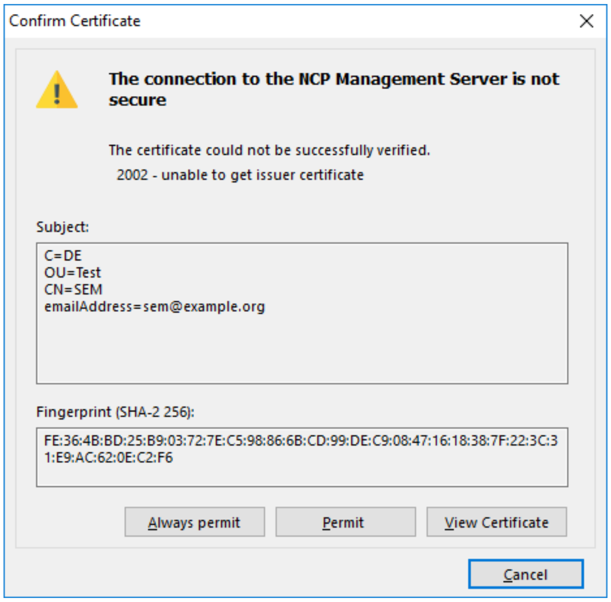
## 2.2. Installation of the Management Server plug-ins

Use the built-in *Administrator* account (without password) to connect to the Management Server for the first time. You must initially accept (permit) the default certificate presented by the Management Server securing the TLS connection. After that you will be prompted to define the *Password* for the *Administrator*.



Connect to NCP Management Server

Description: Local SEM - Adminitrator
Host: 127.0.0.1
Port: 12504
Administrator: Administrator
Password:
□ Save password
☑ Use SSL connection



Confirm Certificate

**The connection to the NCP Management Server is not secure**

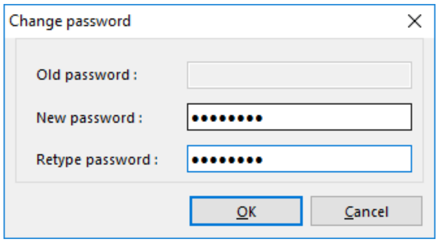
The certificate could not be successfully verified.
2002 - unable to get issuer certificate

Subject:

```
C=DE
OU=Test
CN=SEM
emailAddress=sem@example.org
```

Fingerprint (SHA-2 256):

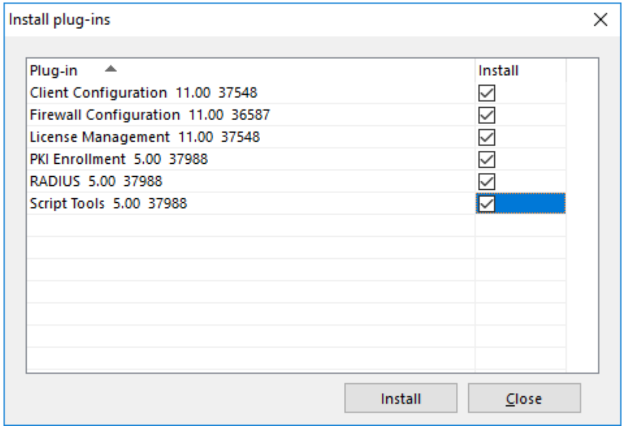
```
FE:36:4B:BD:25:B9:03:72:7E:C5:98:86:6B:CD:99:DE:C9:08:47:16:18:38:7F:22:3C:3
1:E9:AC:62:0E:C2:F6
```



Change password

Old password :
New password : ••••••••
Retype password : ••••••••

With the first Administrator logon to the Management Server you have to enable the plug-ins you want to use. In this example all available plug-ins are checked to be installed.

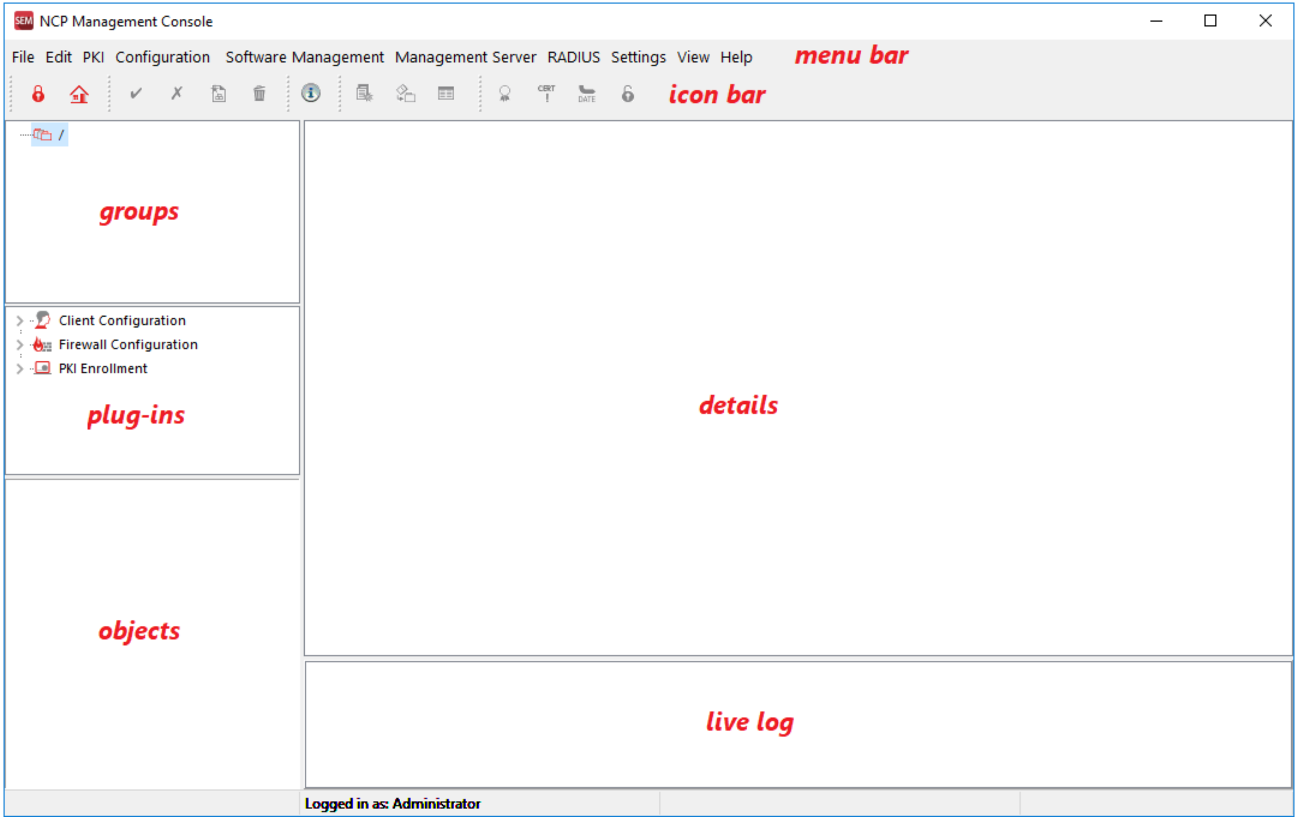


Install plug-ins

| Plug-in | Install |
|---|---|
| Client Configuration 11.00 37548 | ☑ |
| Firewall Configuration 11.00 36587 | ☑ |
| License Management 11.00 37548 | ☑ |
| PKI Enrollment 5.00 37988 | ☑ |
| RADIUS 5.00 37988 | ☑ |
| Script Tools 5.00 37988 | ☑ |

Next Generation Network Access Technology

After the initial setup is done the Management Console will open as shown below.

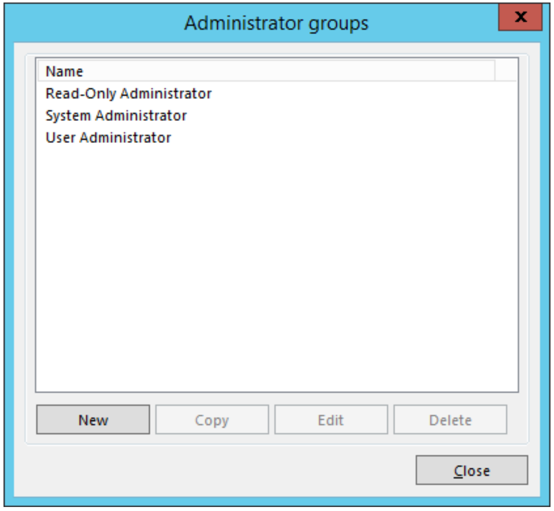


## 2.3. Creating a new administrator

We recommend to immediately create personalized administrator account for the respective users who are going to have administrative access to the Management Server. Administrator privileges are assigned through administrator groups which contain the levels of access. Therefore, it is also a recommendation to create a new administrator group (here: Full Admin) as a copy of the built-in "System Administrator" group.

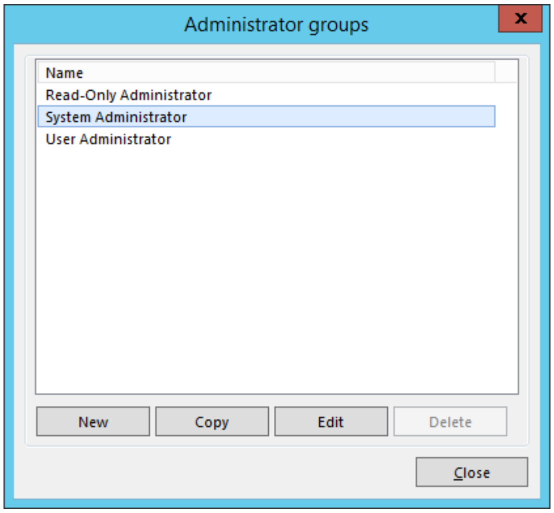
### 2.3.1. Creating a new administrator group

- From the "Edit" menu select "Administrator groups" and select "System Administrator" from the list and click Copy.



Administrator groups

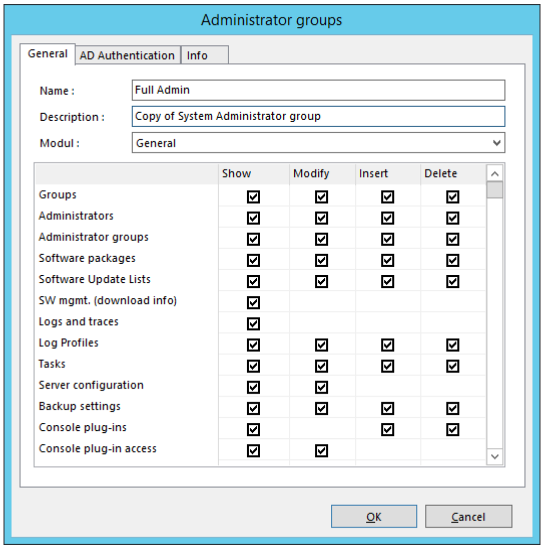
Name
Read-Only Administrator
System Administrator
User Administrator



Administrator groups

Name
Read-Only Administrator
System Administrator
User Administrator

- In the following dialogue you can enter "Name" and "Description" for the new administrator group. Leave everything else untouched. Then go to the "Info" tab and tick the option "Entry inherited to subgroups". This will make sure that the new administrator group is also available in any subgroup. Click "OK".

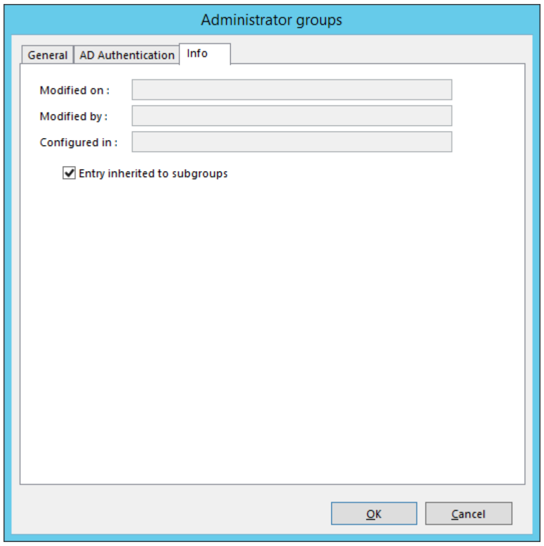


Administrator groups

General | AD Authentication | Info

Name : Full Admin
Description : Copy of System Administrator group
Modul : General

| | Show | Modify | Insert | Delete |
|---|---|---|---|---|
| Groups | ☑ | ☑ | ☑ | ☑ |
| Administrators | ☑ | ☑ | ☑ | ☑ |
| Administrator groups | ☑ | ☑ | ☑ | ☑ |
| Software packages | ☑ | ☑ | ☑ | ☑ |
| Software Update Lists | ☑ | ☑ | ☑ | ☑ |
| SW mgmt. (download info) | ☑ | | | |
| Logs and traces | ☑ | | | |
| Log Profiles | ☑ | ☑ | ☑ | ☑ |
| Tasks | ☑ | ☑ | ☑ | ☑ |
| Server configuration | ☑ | ☑ | | |
| Backup settings | ☑ | ☑ | ☑ | ☑ |
| Console plug-ins | ☑ | | ☑ | ☑ |
| Console plug-in access | ☑ | ☑ | | |



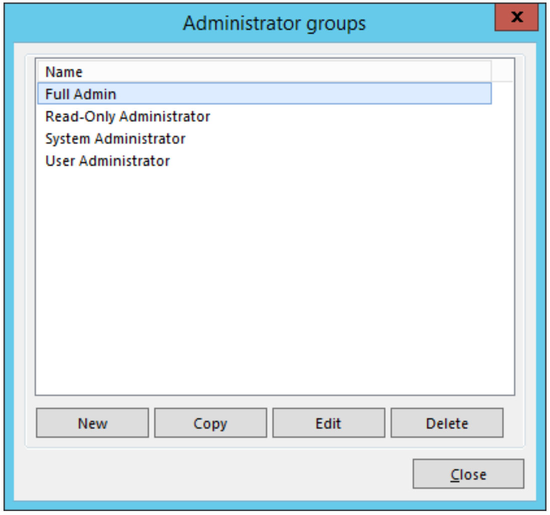
Administrator groups

General | AD Authentication | Info

Modified on :
Modified by :
Configured in :

☑ Entry inherited to subgroups

- The new group will be listed as shown below.



Administrator groups

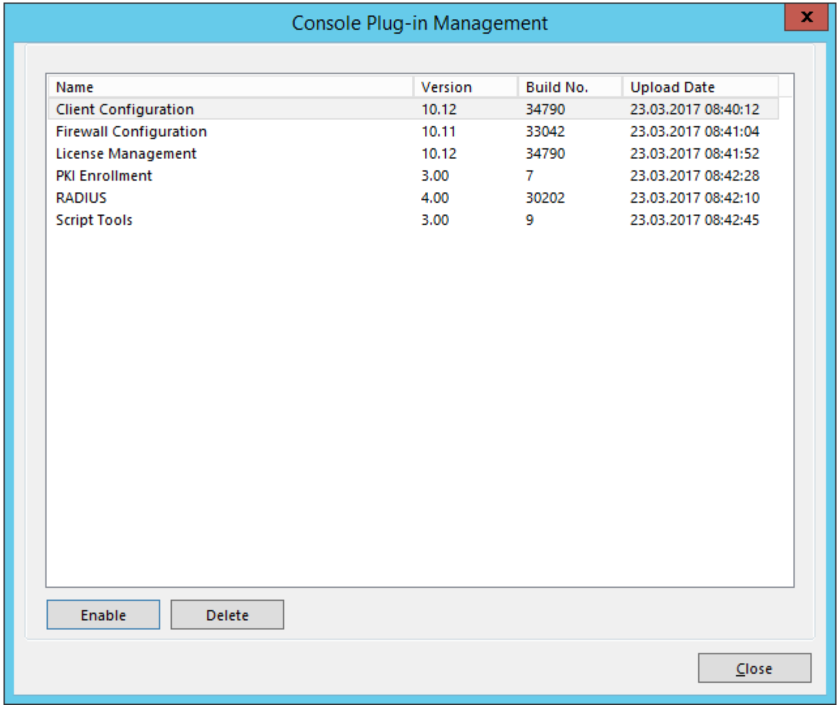
| Name |
|---|
| Full Admin |
| Read-Only Administrator |
| System Administrator |
| User Administrator |

Close the dialogue and then proceed with enabling the previously activated plug-ins for the new group.

## 2.3.2. Enabling plug-ins for the new administrator group

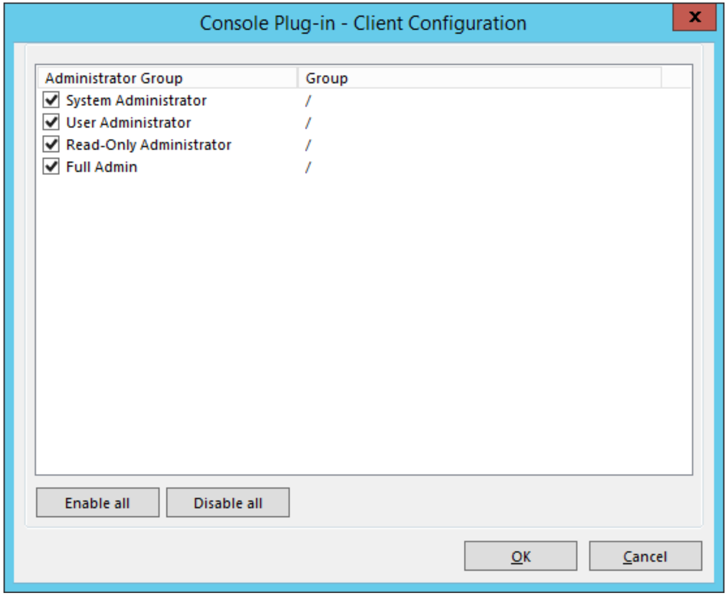
For any new administrator group, the plug-ins have to be enabled separately.

- Select “Console Plug-ins” from the “Management Server” menu



| Name | Version | Build No. | Upload Date |
|---|---|---|---|
| Client Configuration | 10.12 | 34790 | 23.03.2017 08:40:12 |
| Firewall Configuration | 10.11 | 33042 | 23.03.2017 08:41:04 |
| License Management | 10.12 | 34790 | 23.03.2017 08:41:52 |
| PKI Enrollment | 3.00 | 7 | 23.03.2017 08:42:28 |
| RADIUS | 4.00 | 30202 | 23.03.2017 08:42:10 |
| Script Tools | 3.00 | 9 | 23.03.2017 08:42:45 |

- Enable the required plug-ins for the “Full Admin” group and after having done so re-login with the Management Console to the Management Server.

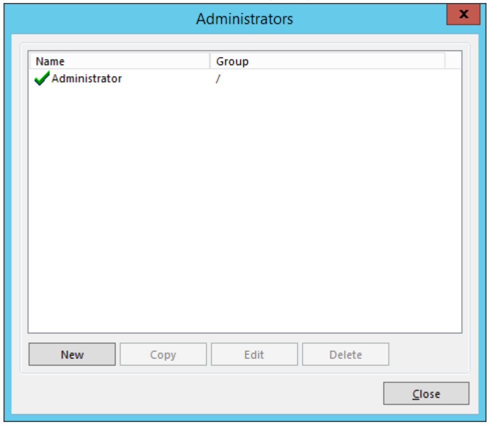


| Administrator Group | Group |
|---|---|
| ☑ System Administrator | / |
| ☑ User Administrator | / |
| ☑ Read-Only Administrator | / |
| ☑ Full Admin | / |

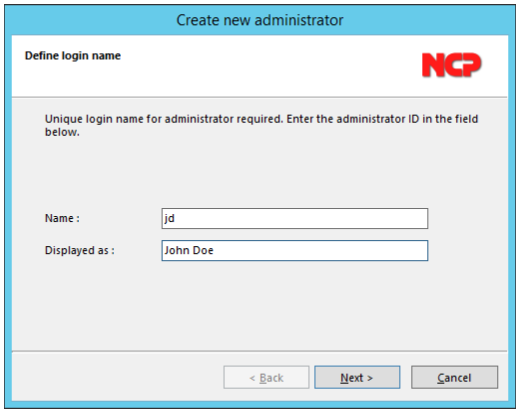
### 2.3.3. Creating a new administrator

With the administrator group in place the new administrator account can now be created.

- From the "Edit" menu select "Administrators", then click "New" to create a new individual admin account. Enter "Name" and "Displayed as" and click "Next".



| Name | Group |
|---|---|
| ✓ Administrator | / |



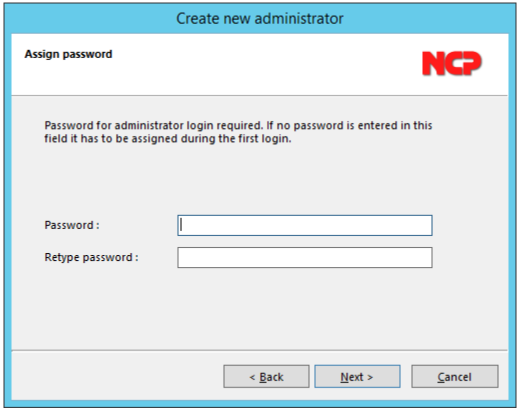
Define login name

Unique login name for administrator required. Enter the administrator ID in the field below.

Name : jd

Displayed as : John Doe

- Specify a password for the new account. If nothing is entered the administrator will be prompted for defining a password during first login. Click "Next" and then assign the previously created "Administrator group" to the new administrator. Click "Next"

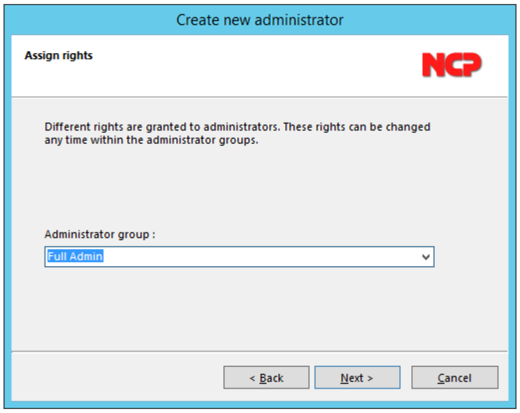


Assign password

Password for administrator login required. If no password is entered in this field it has to be assigned during the first login.

Password :

Retype password :

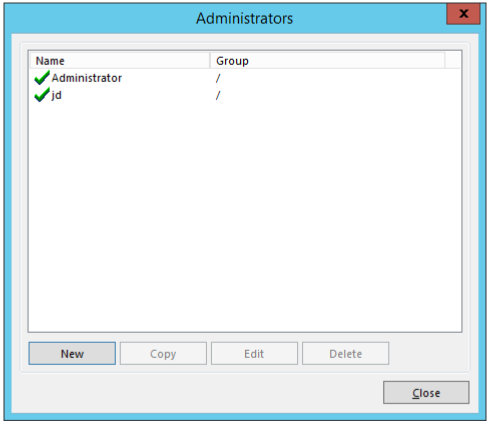


Assign rights

Different rights are granted to administrators. These rights can be changed any time within the administrator groups.

Administrator group : Full Admin

- Click “Next” and the new entry will be stored and listed in the Administrators overview:



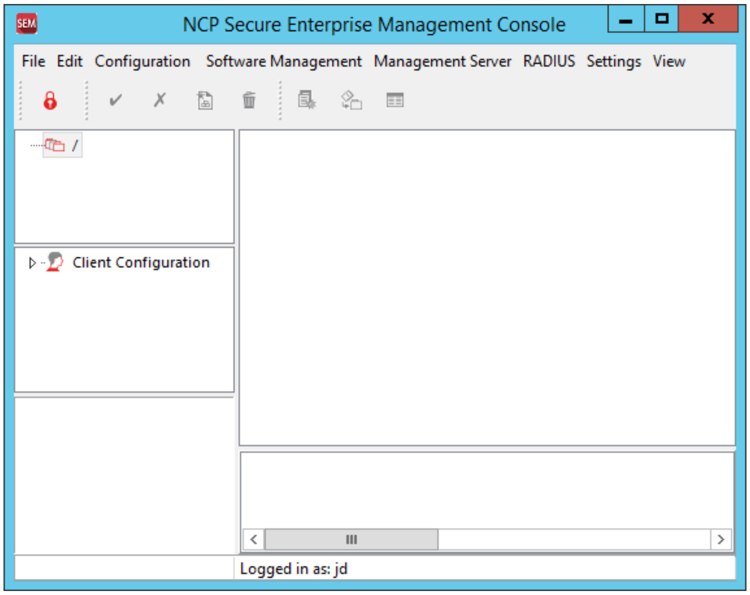
| Name | Group |
|---|---|
| ✓ Administrator | / |
| ✓ jd | / |

Instead of working with the rather anonymous built-in “Administrator” all admins should always work with their personal account to make sure that changes are bound to the according people. The “Administrator” overview can be closed now.

## 3. Configuration of the Management Server

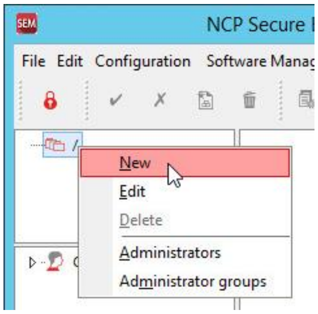
This description will help you set up the Management Server in a way that will be ideal for testing purposes or proof-of-concept. Therefore, some values will be modified especially to achieve quick feedback while testing. When these kinds of changes are suggested there will be a comment hinting for better settings in a productive setup.
The goal is to create an environment which not only handles the configurations and licenses of NCP Exclusive Remote Access Clients but also provides a RADIUS server for your Juniper SRX system allowing for EAP authentication using EAP-MD5 and EAP-TLS.
Let's get started…

Start the Management Console and logon to the Management Server with your own administrator account. The console will look open this:

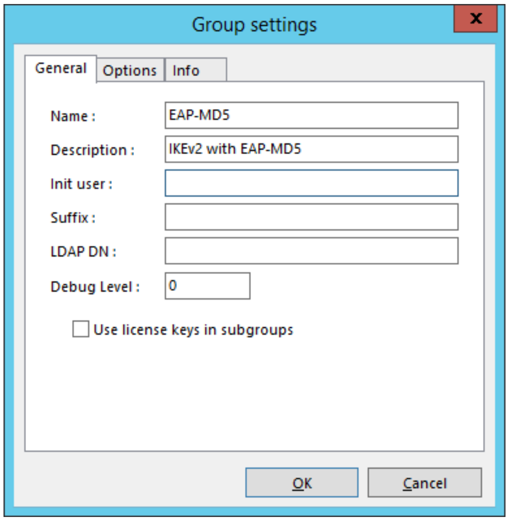

NCP Secure Enterprise Management Console
File Edit Configuration Software Management Management Server RADIUS Settings View
/
Client Configuration
Logged in as: jd

### 3.1. Group structure

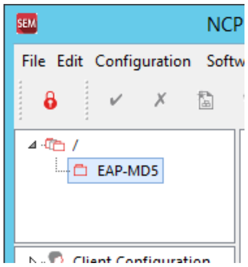
The Management Server lets you create a group structure which most of the time follows the structure already used within your Microsoft Active Directory (or maybe following the department structure in your organization). This sample configuration will have groups created according to the method of authentication of the clients configured within each group. As we are going to work with EAP-MD5 and EAP-TLS, as mentioned above, we will create two groups named exactly like this.
To create a new group move the mouse to the folder of the root group in the top left part of Management Console and perform a right mouse click which will open a context menu. Here select "New" as shown below:

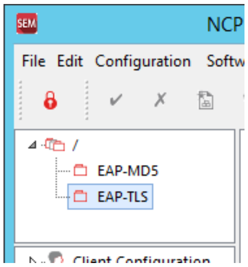


Enter the “Name” of the new group (here: EAP-MD5”) and an optional “Description”. Click “OK” to confirm. The new group will appear in the group tree under root. Create a second group with name “EAP-TLS” the same way you added the one above. Your group tree should look like this now:



Name : EAP-MD5
Description : IKEv2 with EAP-MD5
Init user :
Suffix :
LDAP DN :
Debug Level : 0
□ Use license keys in subgroups



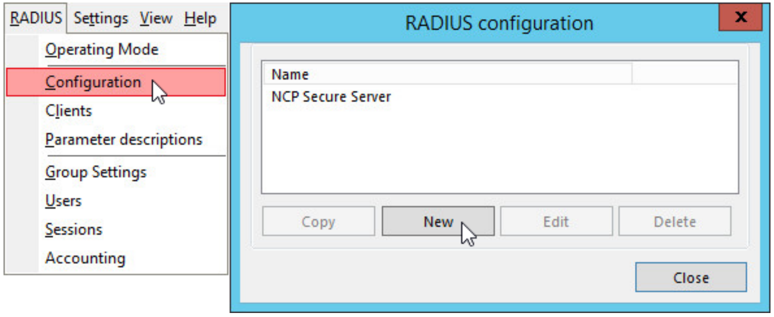


## 3.2. Configuring the Management Server’s integrated RADIUS server

The Management Server comes with an integrated RADIUS server supporting EAP-MD5 and EAP-TLS among others. Therefore, it can be used in a scenario where the Juniper SRX acts as an EAP proxy to authenticate remote access VPN users. In this test scenario these two authentication methods will be used.

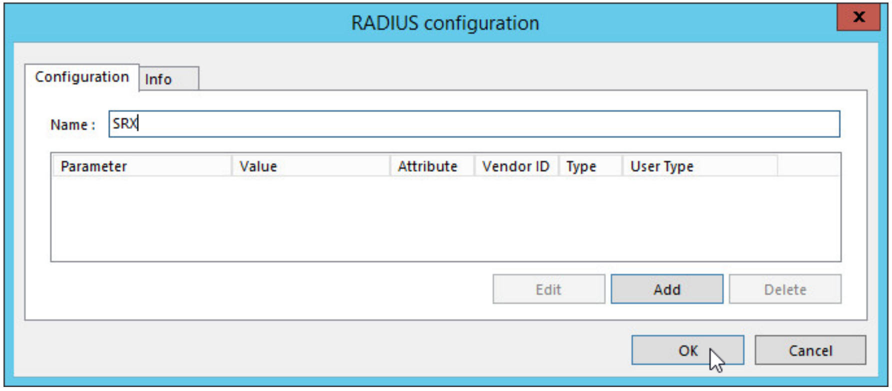
### 3.2.1. Adding a RADIUS configuration for the Juniper SRX

This setup will only work with username and password within the RADIUS configuration of the Management Server for the Juniper SRX RADIUS client. No special dictionaries or attribute value pair configuration is required for this scenario and just a minimal configuration must be created in the Management Server.
Make sure to be on the root group and select “Configuration” from the “RADIUS” menu.



| Name |
|---|
| NCP Secure Server |

Leave the “NCP Secure Server” entry untouched and click new to create a fresh “RADIUS configuration”.

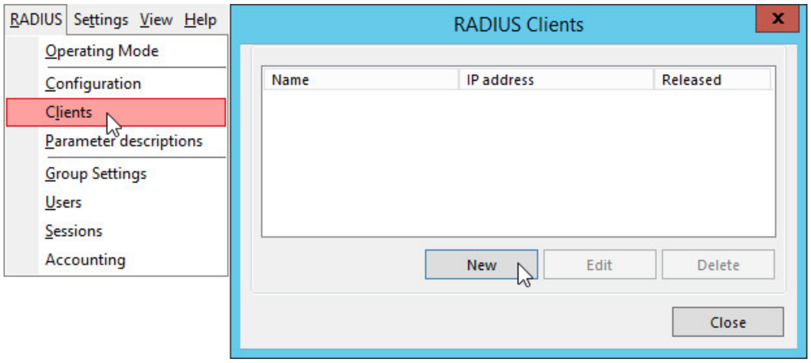


Name : SRX

Just enter a meaningful “Name” (here: SRX) for your Juniper SRX system, then click “OK” to save the changes. No further settings are required here.

## 3.2.2. Adding the Juniper SRX as RADIUS client

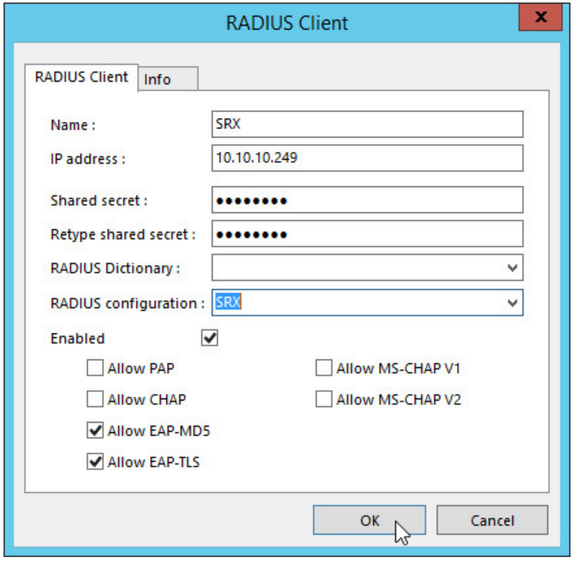
To permit RADIUS requests from the SRX to the Management Server RADIUS server the SRX must be added as RADIUS client. From the “RADIUS” menu select “Clients” and click “New”.



Enter a meaninful “Name” for your SRX and its “IP address” as well the “Shared secret” which must also be configured in your SRX system for this RADIUS server. In the Juniper SRX configuration the related settings are:

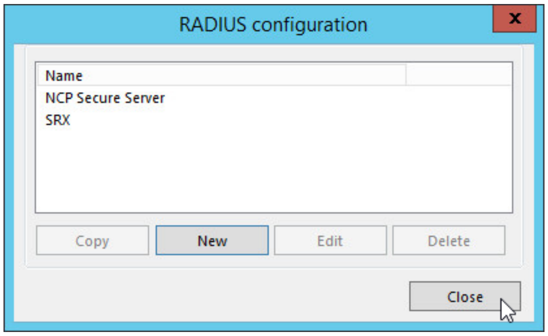
access profile [SRX aaa access-profile name] radius-server 10.10.10.250 port 1812
access profile [SRX aaa access-profile name] radius-server 10.10.10.250 secret "mysharedsecret"

Finally select the previously created “SRX” entry as “RADIUS configuration” then click “OK” to save the changes.



| | |
|---|---|
| Name : | SRX |
| IP address : | 10.10.10.249 |
| Shared secret : | •••••••• |
| Retype shared secret : | •••••••• |
| RADIUS Dictionary : | |
| RADIUS configuration : | SRX |
| Enabled | ☑ |

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

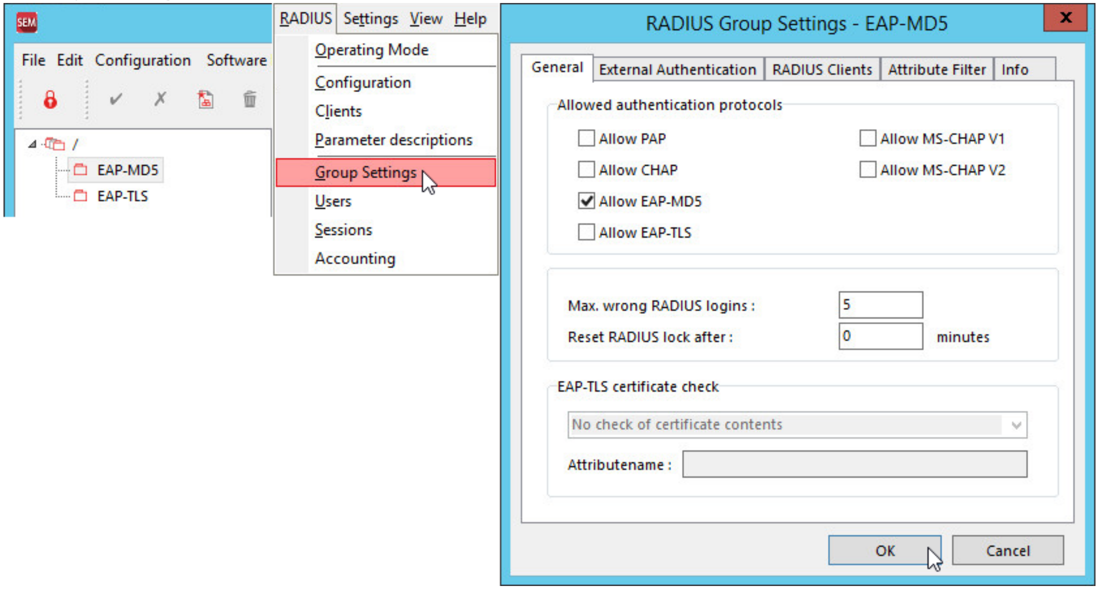


Name
NCP Secure Server
SRX

## 3.2.3. Defining EAP authentication for Management Server groups

To conclude the RADIUS server configuration, we need to let the Management Server know for which group we would like to have EAP-MD5 and for which EAP-TLS as authentication method. As our groups have been named accordingly it is easy to see which group should have which method, but how is this achieved?

Let's start with EAP-MD5 for the group EAP-MD5 and select the group in Management Console. Then go to "Group Settings" in the "RADIUS" menu.



RADIUS Group Settings - EAP-MD5

Allowed authentication protocols

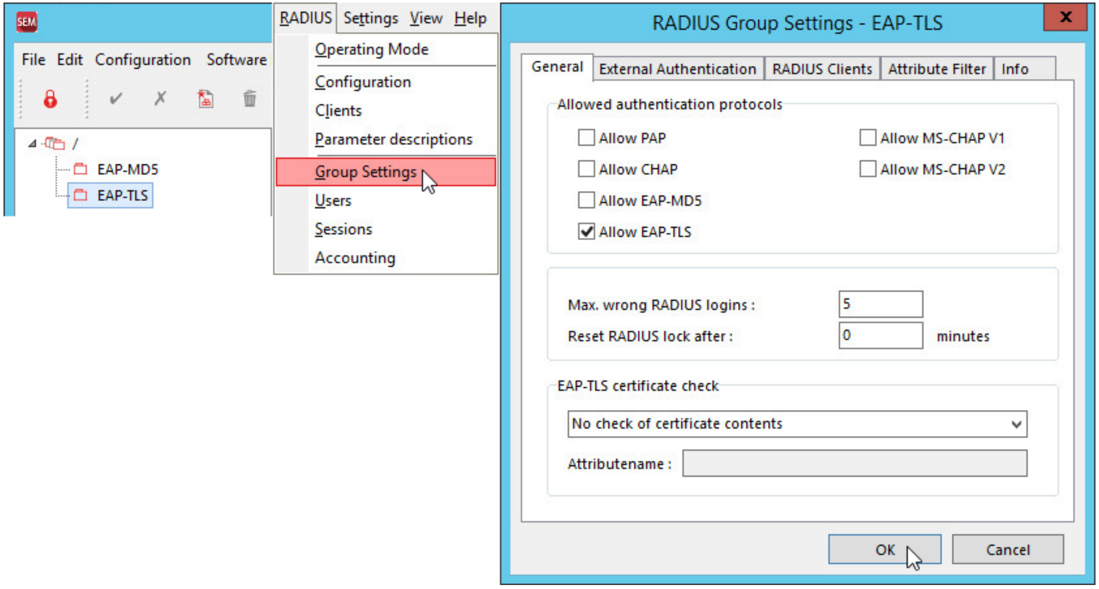
☐ Allow PAP
☐ Allow MS-CHAP V1
☐ Allow CHAP
☐ Allow MS-CHAP V2
☑ Allow EAP-MD5
☐ Allow EAP-TLS

Max. wrong RADIUS logins : 5
Reset RADIUS lock after : 0 minutes

EAP-TLS certificate check
No check of certificate contents
Attributename :

Enable the option "Allow EAP-MD5" to activate this authentication method for the group. Disable all other options as they are not required.

The same needs to be done for the EAP-TLS group only that "Allow EAP-TLS" must be enabled here.



RADIUS Group Settings - EAP-TLS

Allowed authentication protocols

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

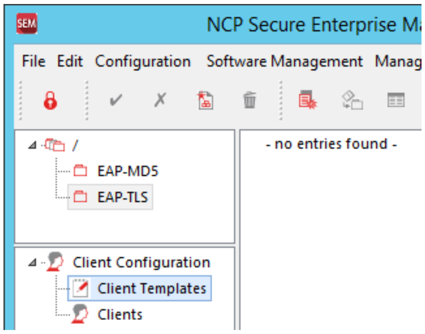
Max. wrong RADIUS logins : 5
Reset RADIUS lock after : 0 minutes

EAP-TLS certificate check
No check of certificate contents
Attributename :

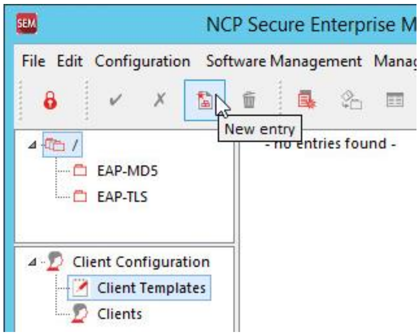
## 3.3. Configuring the Exclusive Remote Access Client in Management Server

### 3.3.1. Creating a configuration template for Exclusive Remote Access Client

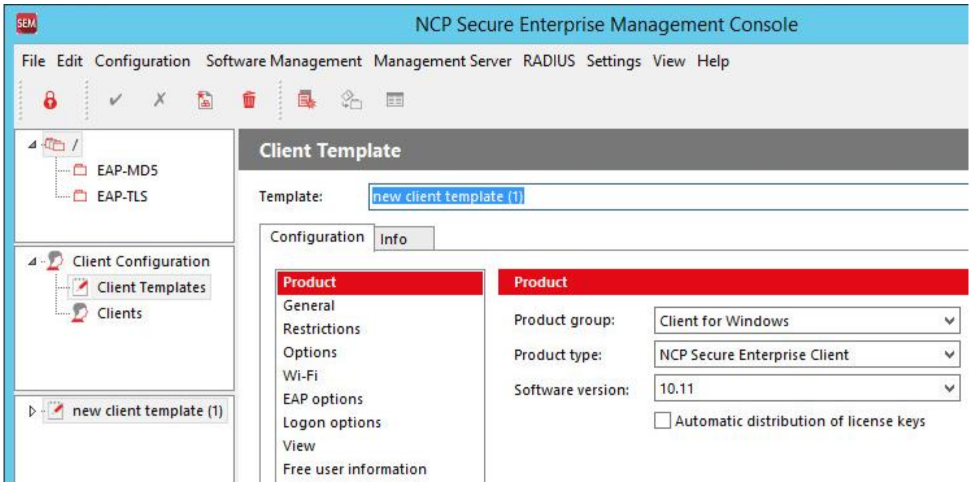
The next step is to create a configuration template for the Exclusive Remote Access Client which will eventually be used to connect the client to the SRX.
Select the root group in Management Console's group tree and then open the "Client Configuration" node in the plug-in section and select "Client Templates".
Insert a client template by clicking on the new entry symbol in the icon bar of the Management Console. The options for a new client template will be open as displayed in the following screenshots.



- no entries found -



- no entries found -



Template: new client template (1)

Product

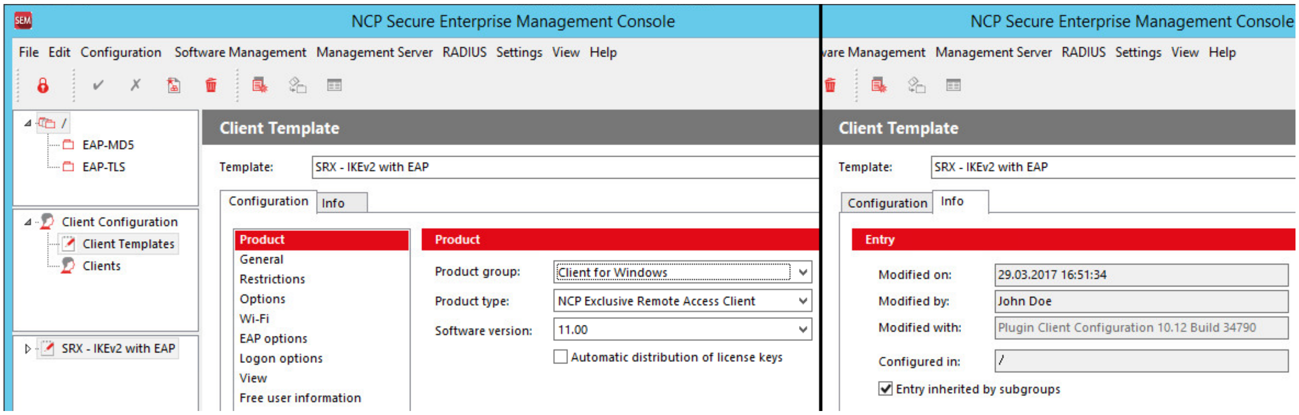
Product group: Client for Windows

Product type: NCP Secure Enterprise Client

Software version: 10.11

□ Automatic distribution of license keys

Change the name of the new "Template" to "SRX – IKEv2 with EAP" and change the "Product type" to "NCP Exclusive Remote Access Client". In the "Info" tab check the option "Entry inherited by subgroups" and save the altered settings by clicking the green tick in icon bar of the Management Console.



Template: SRX - IKEv2 with EAP

Product group: Client for Windows

Product type: NCP Exclusive Remote Access Client

Software version: 11.00

☐ Automatic distribution of license keys

Modified on: 29.03.2017 16:51:34

Modified by: John Doe

Modified with: Plugin Client Configuration 10.12 Build 34790

Configured in: /

☑ Entry inherited by subgroups

These settings will provide all configuration options for the Exclusive Remote Access Client and will make this template available not only within the root group but also all subgroups. Would you intend to create a template only available in one specific group, you will create this template in that group and not enable the option to inherit it by subgroups.

At this stage we will not yet modify any other of the configuration options here, this will come later on.

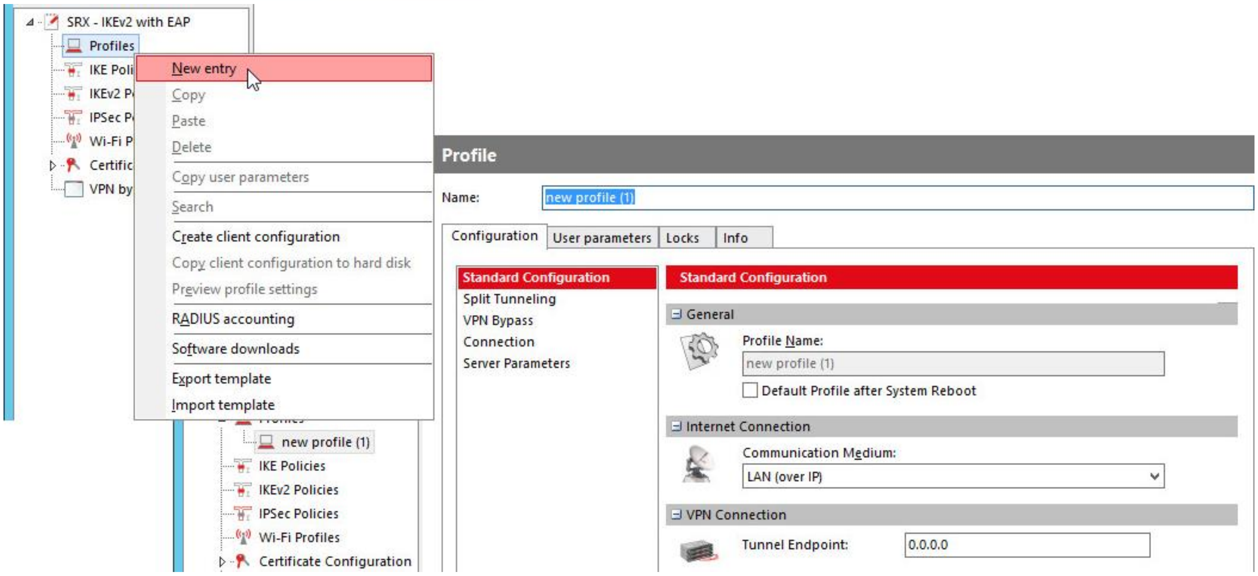
## Configuration of the connection profile to connect to the SRX

Open the template node “SRX – IKEv2 with EAP” and whole set of sub-nodes will appear:

- Profiles
  The profiles specify which configuration parameters to use in order to connect to the SRX
- IKE Policies
  Definition of proposals for IKE version 1
- IKEv2 Policies
  Definition of proposals for IKE version 2
- IPSec Policies
  Definition of proposals for ESP
- Wi-Fi Profiles
  Definition of connections parameters to connect to wireless access points using the clients built-in Wi-Fi management
- Certificate Configuration
  Definition of the certificate configuration to use when certificate based authentication is to be used
- VPN bypass
  Special option to allow specific application to communicate outside the VPN tunnel

Within this scenario we will only work with “Profiles” and “Certificate Configuration” (the latter when configuring EAP-TLS). The other options will be untouched in this documentation.

Create a new profile by selecting “Profiles” and perform a right mouse click. This will open a context menu where you can left-click on “New entry”.



Name: new profile (1)

Profile Name: new profile (1)

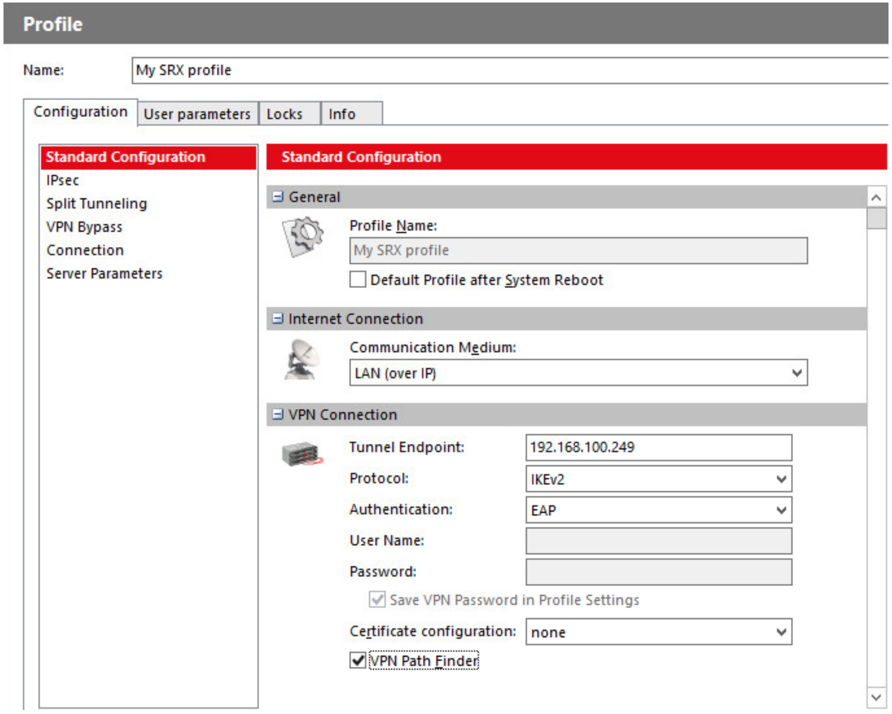
☐ Default Profile after System Reboot

Communication Medium: LAN (over IP)

Tunnel Endpoint: 0.0.0.0

We try to stick with the “Configuration” tab for now and specify the settings to eventually be able to properly connect to the SRX. The groups “Split Tunneling” and “VPN Bypass” will not be touched in this document as they are not required for the sample scenario.

## Group “Standard Configuration”



Name: My SRX profile

Profile Name: My SRX profile

☐ Default Profile after System Reboot

Communication Medium: LAN (over IP)

Tunnel Endpoint: 192.168.100.249

Protocol: IKEv2

Authentication: EAP

User Name:

Password:

☑ Save VPN Password in Profile Settings

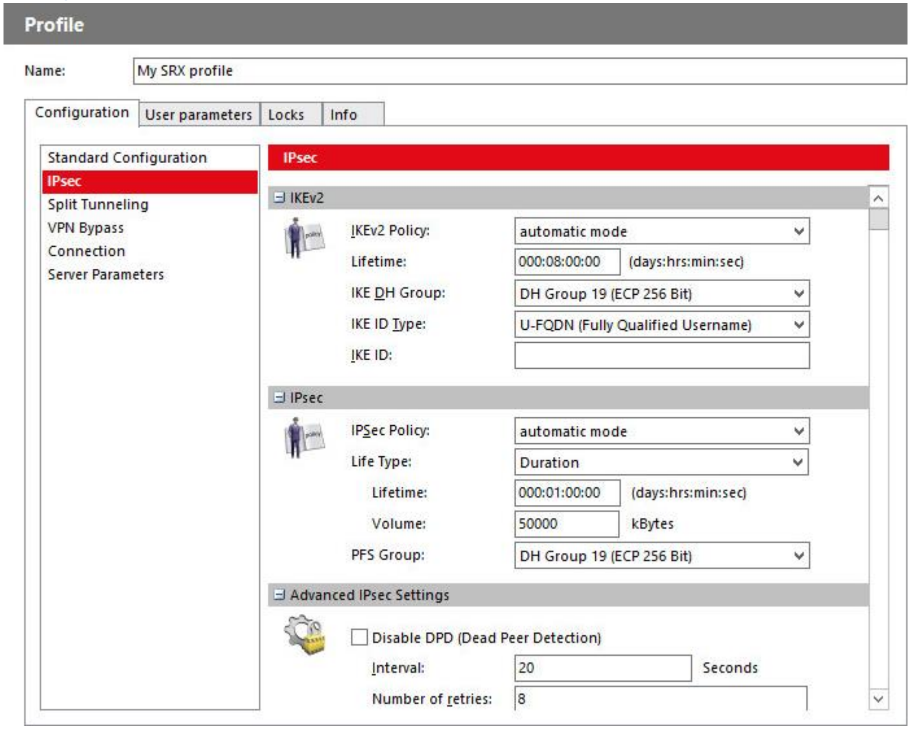
Certificate configuration: none

☑ VPN Path Finder

- “Profile Name”
  Enter a meaningful name as this will appear in client GUI and the user will maybe have to choose between different profiles to connect to different SRX systems or within different environments.

- “Tunnel Endpoint”
  This is either the IP address or hostname of the SRX to establish the connection to. Usually this will be an official address which can be access over the internet.
- “VPN Path Finder”
  Enable this option as it will guarantee to be able to establish the VPN tunnel even when the specific IPsec VPN ports are blocked by a firewall.

### Group “IPsec”



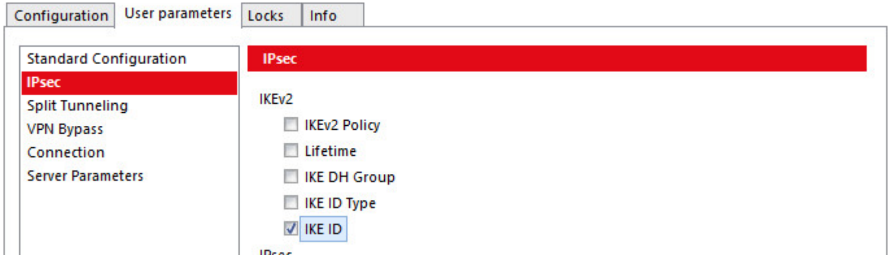
Name: My SRX profile

IKEv2 Policy: automatic mode
Lifetime: 000:08:00:00 (days:hrs:min:sec)
IKE DH Group: DH Group 19 (ECP 256 Bit)
IKE ID Type: U-FQDN (Fully Qualified Username)
IKE ID:

IPSec Policy: automatic mode
Life Type: Duration
Lifetime: 000:01:00:00 (days:hrs:min:sec)
Volume: 50000 kBytes
PFS Group: DH Group 19 (ECP 256 Bit)

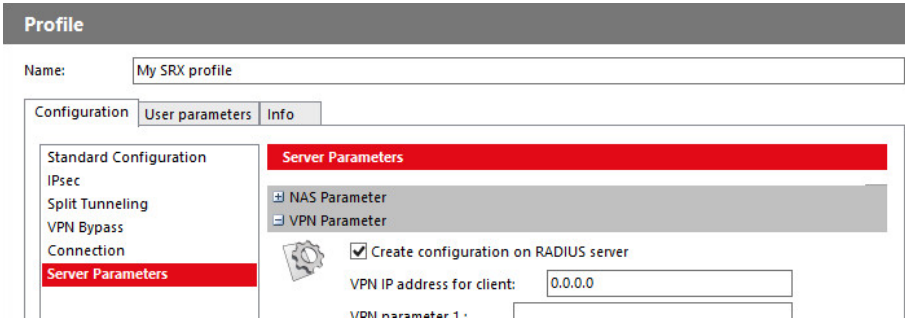
□ Disable DPD (Dead Peer Detection)
Interval: 20 Seconds
Number of retries: 8

Stick with the default values here only that the “IKE ID” has to be user specific. To do so switch to the “User parameters” tab and check the box for “IKE ID”. This will let us specify the IKE ID on a per user basis.



□ IKEv2 Policy
□ Lifetime
□ IKE DH Group
□ IKE ID Type
☑ IKE ID

### Group "Server Parameters"



Profile

Name: My SRX profile

☑ Create configuration on RADIUS server

VPN IP address for client: 0.0.0.0

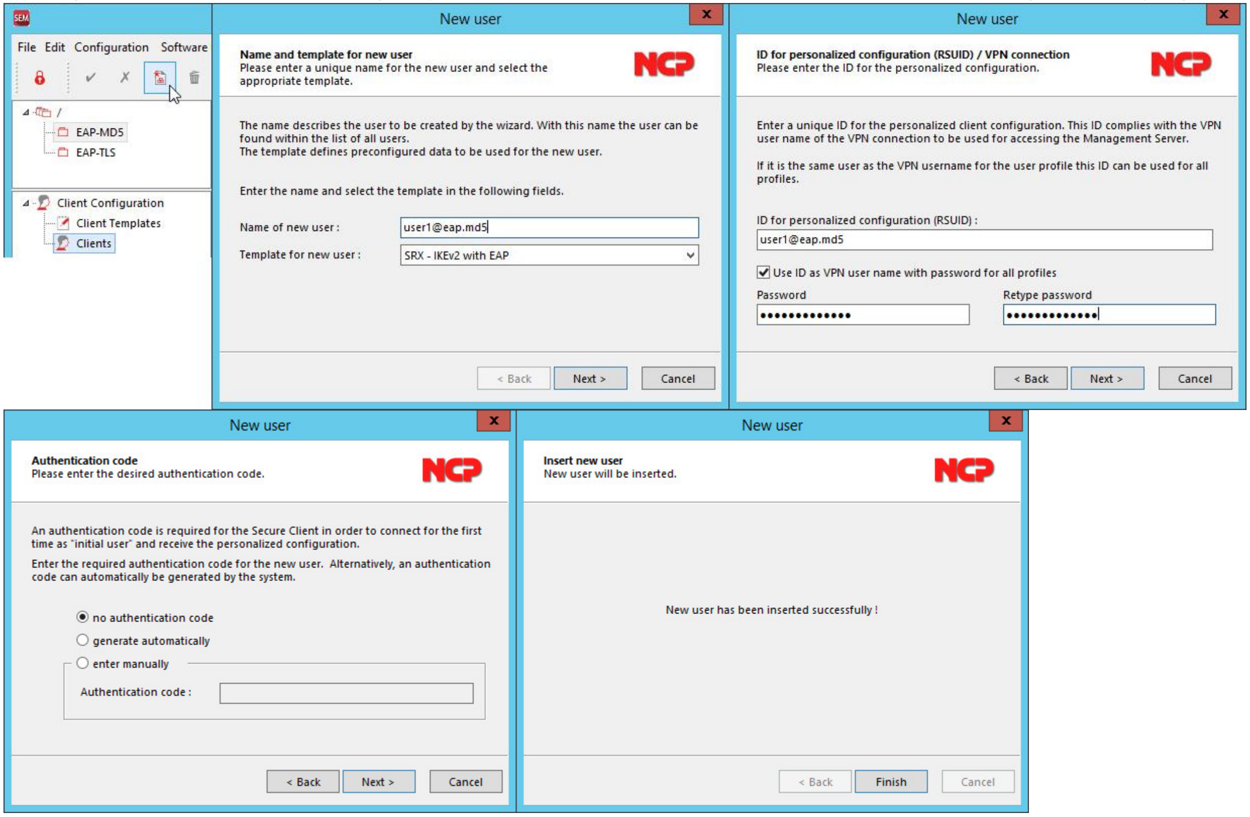
VPN parameter 1 :

Just check the box for "Create configuration on RADIUS server". This will automatically create an entry in the Management Server's internal RADIUS server whenever a new user is created using this template.

Save the changes by clicking on the green tick in the icon bar.

## 3.3.2. Creating a new user in the Management Server

To create a configuration for Exclusive Remote Access Client we need to create a new client entry in the Management Server. Select the group "EAP-MD5" and then "Clients" in the "Client Configuration" plug-in.



New user

**Name and template for new user**
Please enter a unique name for the new user and select the appropriate template.

The name describes the user to be created by the wizard. With this name the user can be found within the list of all users.
The template defines preconfigured data to be used for the new user.

Enter the name and select the template in the following fields.

Name of new user : user1@eap.md5

Template for new user : SRX - IKEv2 with EAP

New user

**ID for personalized configuration (RSUID) / VPN connection**
Please enter the ID for the personalized configuration.

Enter a unique ID for the personalized client configuration. This ID complies with the VPN user name of the VPN connection to be used for accessing the Management Server.

If it is the same user as the VPN username for the user profile this ID can be used for all profiles.

ID for personalized configuration (RSUID) : user1@eap.md5

☑ Use ID as VPN user name with password for all profiles

Password: •••••••••••••

Retype password: •••••••••••••

New user

**Authentication code**
Please enter the desired authentication code.

An authentication code is required for the Secure Client in order to connect for the first time as "initial user" and receive the personalized configuration.
Enter the required authentication code for the new user. Alternatively, an authentication code can automatically be generated by the system.

● no authentication code
○ generate automatically
○ enter manually

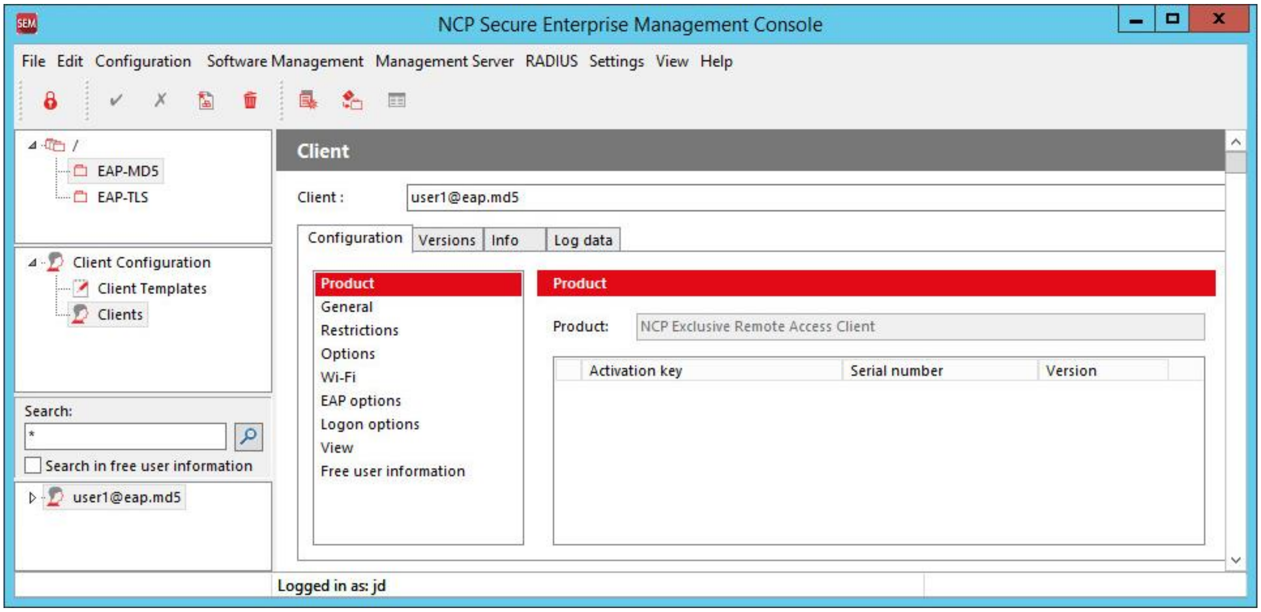
Authentication code :

New user

**Insert new user**
New user will be inserted.

New user has been inserted successfully !

After clicking "Finish" the just created "Client" configuration will be displayed in the Management Console window.



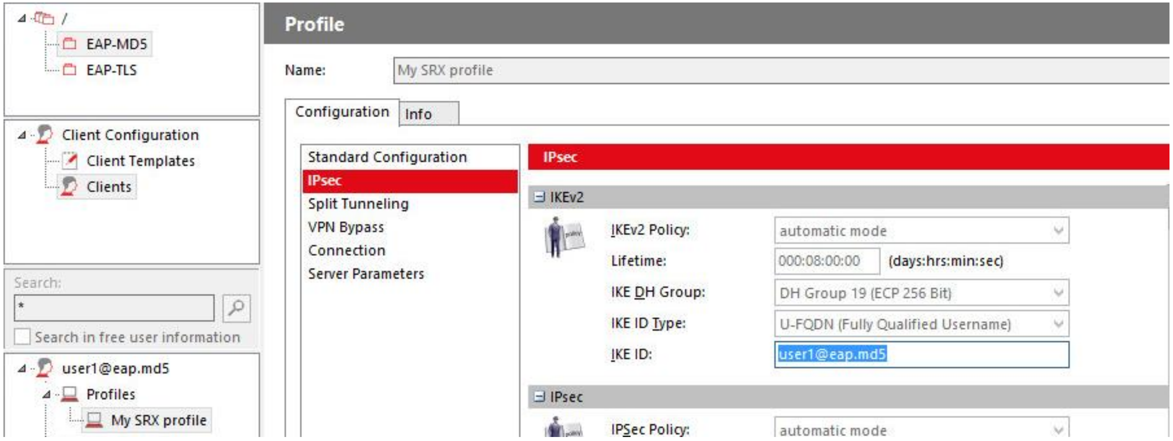
Client : user1@eap.md5

Product: NCP Exclusive Remote Access Client

| Activation key | Serial number | Version |
|---|---|---|

Logged in as: jd

As configured earlier the “IKE ID” parameter is set on a per user basis and so the according value has to be entered individually. Open the node of the user (here: user1@eap.md5) and the “Profiles”. Then select the previously defined profile (here: My SRX profile) and in the “Configuration” tab select the “IPsec” group. Underneath “IPsec” within the “IKEv2” settings, enter the username (here: user1@eap.md5) for the “IKE ID”.



Name: My SRX profile

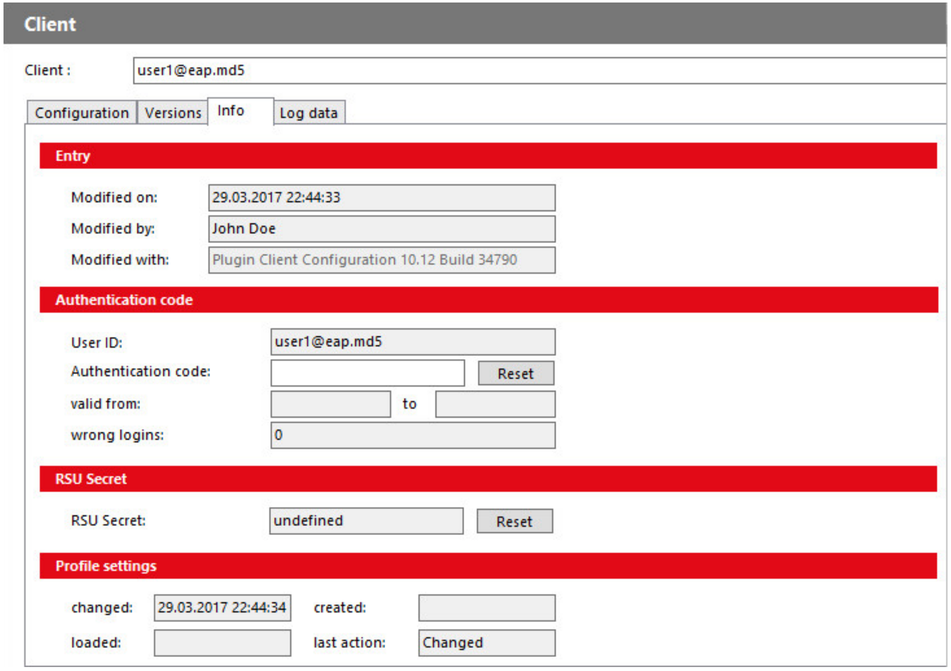
IKEv2 Policy: automatic mode
Lifetime: 000:08:00:00 (days:hrs:min:sec)
IKE DH Group: DH Group 19 (ECP 256 Bit)
IKE ID Type: U-FQDN (Fully Qualified Username)
IKE ID: user1@eap.md5

IPSec Policy: automatic mode

Save your changes with the green tick in the icon bar.

Note: The IKE ID can be the same for all users or be used to differentiate between user groups. Individual user authentication happens separately in EAP with the RADIUS server. For more information, please consult the IKEv2 related documentation of your Juniper SRX.

Select the “Info” tab to see the current status of the client configuration:



Client : user1@eap.md5

**Entry**

Modified on: 29.03.2017 22:44:33
Modified by: John Doe
Modified with: Plugin Client Configuration 10.12 Build 34790

**Authentication code**

User ID: user1@eap.md5
Authentication code:
valid from: to
wrong logins: 0

**RSU Secret**

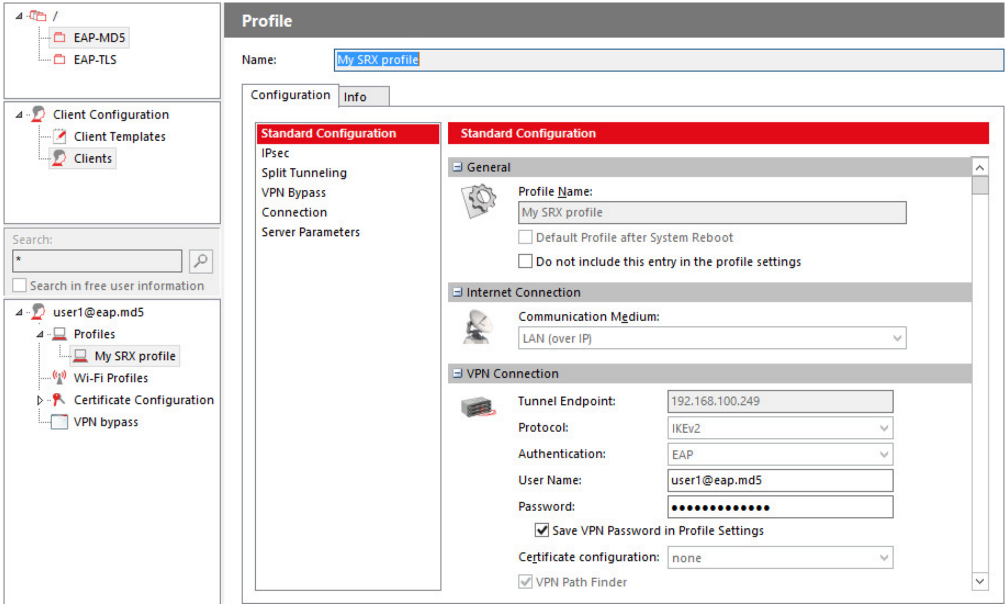
RSU Secret: undefined

**Profile settings**

changed: 29.03.2017 22:44:34
created:
loaded:
last action: Changed

In the “Profile settings” section you can see that configuration has already been “changed” but neither has it been “created” nor “loaded”. The “last action” is “Changed”. This means that no RADIUS entry has yet been created nor is the configuration available for download from the Management Server. This would be indicated by a time stamp in “created”. Had a client already downloaded the configuration there would also be time stamp in “loaded”.

Before moving on with creating the RADIUS entries for our new user first take a look at the “Profile” configuration. To do so click on “My SRX profile” (or whatever may be the name of the profile you defined previously) in the “Profiles” node on the left hand side.



Name: My SRX profile

Profile Name: My SRX profile

□ Default Profile after System Reboot

□ Do not include this entry in the profile settings

Communication Medium: LAN (over IP)

Tunnel Endpoint: 192.168.100.249

Protocol: IKEv2

Authentication: EAP

User Name: user1@eap.md5

Password: •••••••••••••

☑ Save VPN Password in Profile Settings

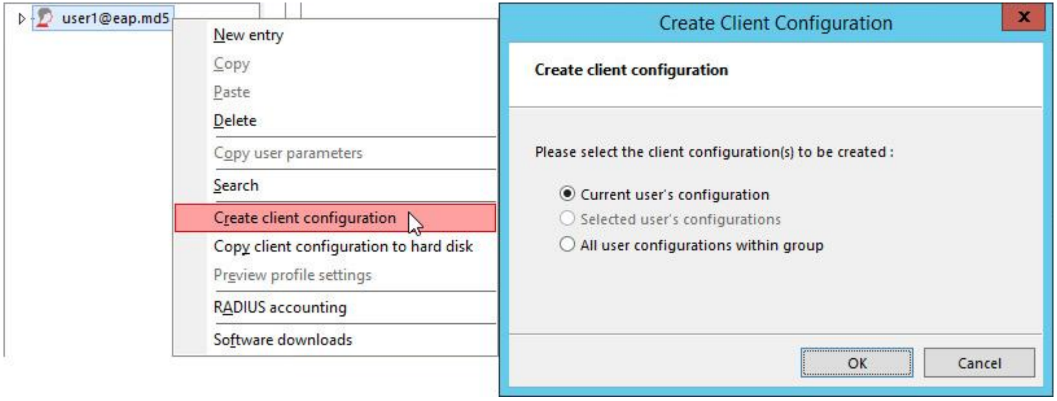
Certificate configuration: none

☑ VPN Path Finder

The display will show the values that you entered while having been walked through the new-client-wizard before.

### 3.3.3. Creating the RADIUS entries for the new client

Select the new client entry on the left side of the Management Console and perform a right mouse click to open the context menu. There click on “Create Client Configuration” and in the following dialogue confirm to create “Current user’s configuration” with “OK”.



Create client configuration

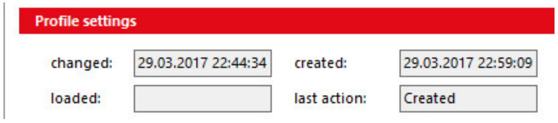
Please select the client configuration(s) to be created :

● Current user's configuration

○ Selected user's configurations

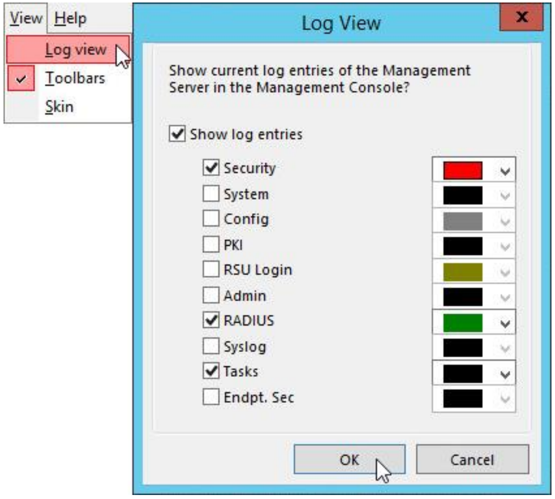
○ All user configurations within group

The status change for the configuration can be viewed in the “Info” tab of the client where the “Profile Settings” should similar to the one shown below:


Profile settings

| | | | |
|---|---|---|---|
| changed: | 29.03.2017 22:44:34 | created: | 29.03.2017 22:59:09 |
| loaded: | | last action: | Created |

However, it is wise to enable the live log viewer showing various information at bottom of the Management Console. Select “Log view” from the “View” menu where the live log can be enabled. Check the boxes for “Show log entries” and “Security” (here colored red), “RADIUS” (here colored green), “Tasks” (here colored black).

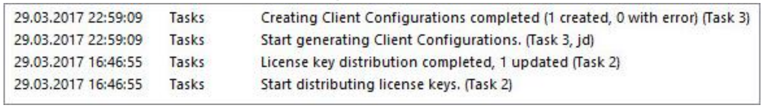


Show current log entries of the Management Server in the Management Console?

☑ Show log entries

- ☑ Security 🟥
- □ System ⬛
- □ Config ⬜
- □ PKI ⬛
- □ RSU Login 🟫
- □ Admin ⬛
- ☑ RADIUS 🟩
- □ Syslog ⬛
- ☑ Tasks ⬛
- □ Endpt. Sec ⬛

Then click “OK” to see the log information at the bottom of the console.



```
29.03.2017 22:59:09    Tasks    Creating Client Configurations completed (1 created, 0 with error) (Task 3)
29.03.2017 22:59:09    Tasks    Start generating Client Configurations. (Task 3, jd)
29.03.2017 16:46:55    Tasks    License key distribution completed, 1 updated (Task 2)
29.03.2017 16:46:55    Tasks    Start distributing license keys. (Task 2)
```

The latest entries are listed on top of the live log. You should see entries for the creation of the client configuration and license distribution. The important one right now is:

Creating Client Configurations completed (1 created, 0 with error) (Task x)

The significant part is “0 with error” which indicates that the RADIUS entries were successfully written. With this the Management Server side is good to go. Now we need to take care of the client.

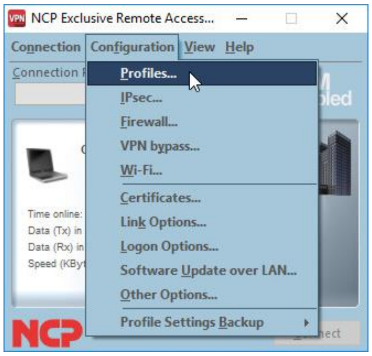
# 4. Installing and Configuring the Exclusive Remote Access Client

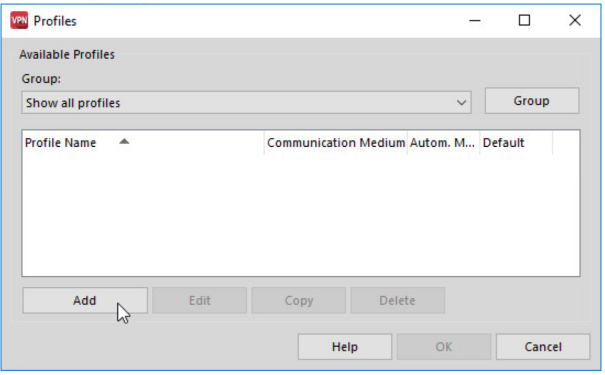
This chapter describes how the NCP Exclusive Remote Access Client is set up on the user's system.
Please refer to B Client Installation on Windows for detailed instructions.
After successful installation the client has to be configured to establish a VPN connection to the Juniper SRX gateway. There are two ways to do so:

- Creating the configuration directly in the client
  Matching all the settings already taken care of in the Management Server's client configuration.
- Copying the configuration previously created on the Management Server
  Saving the configuration with the Management Console and copying it over to the client system.

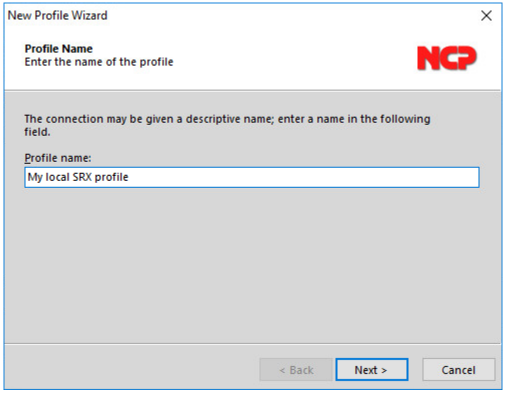
## 4.1. Creating a new client configuration

To create the configuration directly in the client the "Exclusive Remote Access Client Monitor" has to be started if not yet open. From the "Configuration" menu select "Profiles" and click "Add" to create a new entry.





The "New Profile Wizard" will prompt for the input of the "Profile name" (here: "My Local SRX profile"). Use a different name than already defined in the Management Server before as we will retrieve the configuration from the Management Server at a later stage and having different names is the easiest way to immediately determine when the config changed.

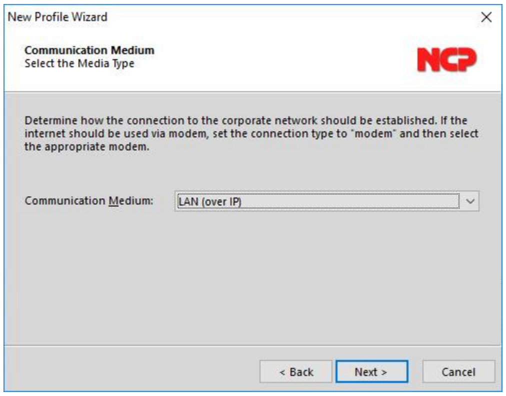


New Profile Wizard

**Profile Name**
Enter the name of the profile

The connection may be given a descriptive name; enter a name in the following field.

Profile name: My local SRX profile



New Profile Wizard

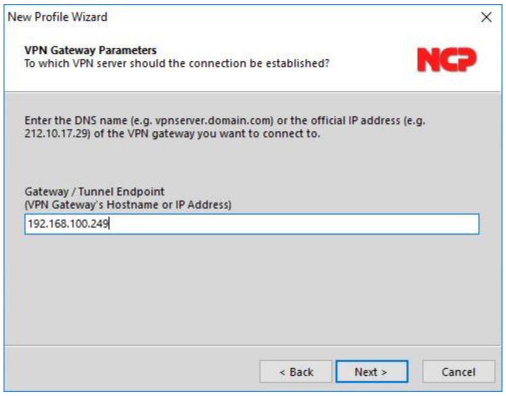
**Communication Medium**
Select the Media Type

Determine how the connection to the corporate network should be established. If the internet should be used via modem, set the connection type to "modem" and then select the appropriate modem.

Communication Medium: LAN (over IP)

Click "Next" to define the "Communication Medium" in the following dialogue. As nothing needs to be changed here, click "Next".

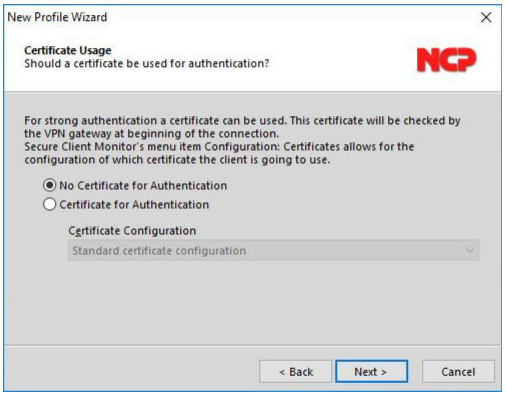
In “VPN Gateway Parameters” enter the IP address or hostname for the VPN gateway’s tunnel endpoint. With “Next” you get to the “Certificate Usage”. As no certificate is used on client side when working with EAP-MD5 select “No Certificate for Authentication” and click “Next”.


New Profile Wizard

**VPN Gateway Parameters**
To which VPN server should the connection be established?

Enter the DNS name (e.g. vpnserver.domain.com) or the official IP address (e.g. 212.10.17.29) of the VPN gateway you want to connect to.

Gateway / Tunnel Endpoint
(VPN Gateway's Hostname or IP Address)
192.168.100.249


New Profile Wizard

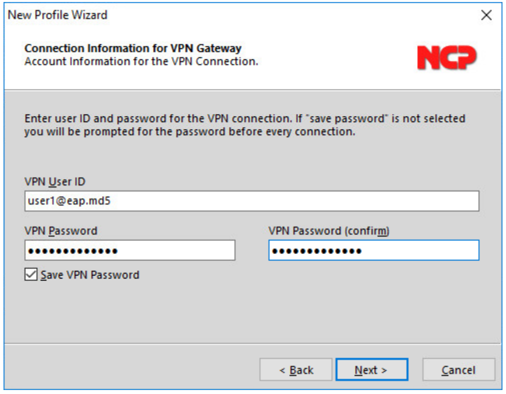
**Certificate Usage**
Should a certificate be used for authentication?

For strong authentication a certificate can be used. This certificate will be checked by the VPN gateway at beginning of the connection.
Secure Client Monitor's menu item Configuration: Certificates allows for the configuration of which certificate the client is going to use.

● No Certificate for Authentication
○ Certificate for Authentication

Certificate Configuration
Standard certificate configuration

After that provide “VPN User ID” and “VPN Password” which will be used for the EAP-MD5 authentication with the RADIUS server. Enter the same username and password as entered previously in the Management Server configuration. Then click “Next” to provide the “IKE ID” which is also the one you previously entered in the Management Server part.


New Profile Wizard

**Connection Information for VPN Gateway**
Account Information for the VPN Connection.

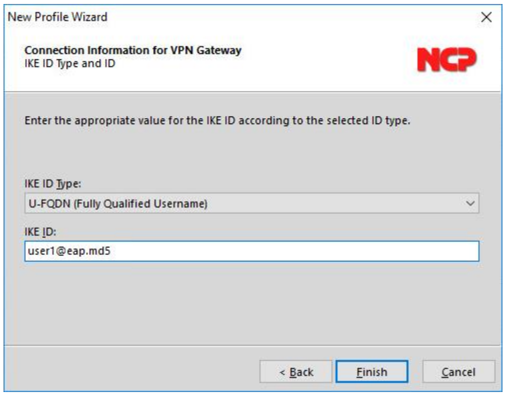
Enter user ID and password for the VPN connection. If "save password" is not selected you will be prompted for the password before every connection.

VPN User ID
user1@eap.md5

VPN Password
•••••••••••••

VPN Password (confirm)
•••••••••••••

☑ Save VPN Password


New Profile Wizard

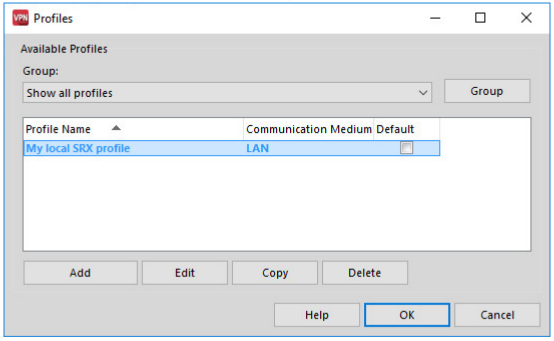
**Connection Information for VPN Gateway**
IKE ID Type and ID

Enter the appropriate value for the IKE ID according to the selected ID type.

IKE ID Type:
U-FQDN (Fully Qualified Username)

IKE ID:
user1@eap.md5

Click “Finish” to end the profile wizard.


Profiles

Available Profiles

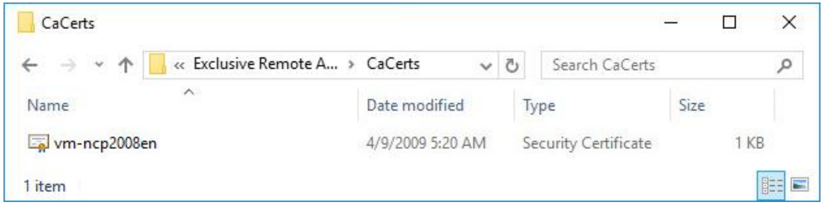
Group:
Show all profiles

| Profile Name | Communication Medium | Default |
|---|---|---|
| My local SRX profile | LAN | □ |

This concludes the profile configuration of the client. It will work with default IKEv2 and IPsec proposals which have to be configured accordingly on the SRX. These defaults are:

- IKEv2 policy
    - Encryption: AES-GCM 256 bit
    - Pseudo-Random-Function: HMAC SHA2 384 bit
    - IKE Diffie Hellman group: DH 19 (prime256v1)
- IPsec policy
    - Protocol: ESP
    - Encryption: AES-GCM 256 bit
    - PFS group: DH 19 (prime256v1)

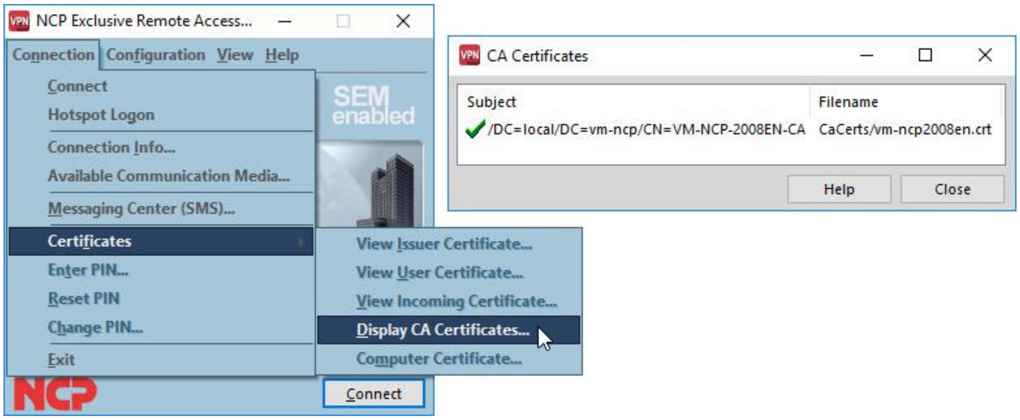
These proposals have to be configured accordingly on the Juniper SRX gateway to accept the proposals. Before starting to test the VPN connection the client must be prepared to be able to accept the certificate of the SRX which will always be presented within the IKEv2 negotiation when using EAP as authentication method. Therefore, the issuer certificate must be placed in the “CaCerts” folder in the client’s installation path.



| Name | Date modified | Type | Size |
|---|---|---|---|
| vm-ncp2008en | 4/9/2009 5:20 AM | Security Certificate | 1 KB |

1 item

You can verify that issuer has been accepted by the client by selecting “Display CA Certificates” under “Certificates” in the “Connection” menu of client’s GUI.

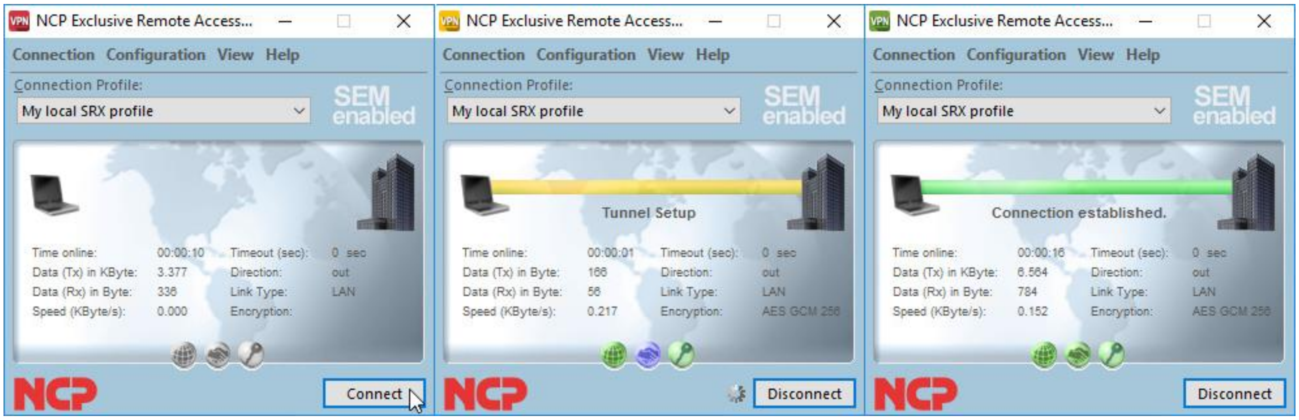


| Subject | Filename |
|---|---|
| ✓ /DC=local/DC=vm-ncp/CN=VM-NCP-2008EN-CA | CaCerts/vm-ncp2008en.crt |

As long the everything is set on the Juniper SRX gateway the Exclusive Remote Access Client is now good to go. Please refer to the Quick Configuration Guides provided on the NCP web site for detailed settings:
https://www.ncp-e.com/en/exclusive-remote-access-solution/documents-faq/

### 4.1.1. Testing the local client configuration

Click “Connect” to establish the VPN connection to the Juniper SRX.


NCP Exclusive Remote Access...
Connection Configuration View Help
SEM enabled
NCP
Connect
NCP Exclusive Remote Access...
Connection Configuration View Help
SEM enabled
NCP
Disconnect
NCP Exclusive Remote Access...
Connection Configuration View Help
SEM enabled
NCP
Disconnect

Connection Profile: My local SRX profile

```
Time online:          00:00:10   Timeout (sec):   0  sec
Data (Tx) in KByte:   3.377      Direction:       out
Data (Rx) in Byte:    336        Link Type:       LAN
Speed (KByte/s):      0.000      Encryption:
```

Connection Profile: My local SRX profile

Tunnel Setup

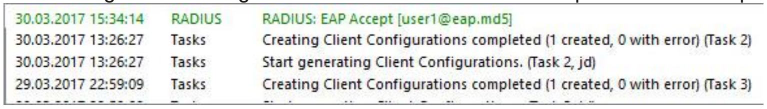
```
Time online:          00:00:01   Timeout (sec):   0  sec
Data (Tx) in Byte:    166        Direction:       out
Data (Rx) in Byte:    56         Link Type:       LAN
Speed (KByte/s):      0.217      Encryption:      AES GCM 256
```

Connection Profile: My local SRX profile

Connection established.

```
Time online:          00:00:16   Timeout (sec):   0  sec
Data (Tx) in KByte:   6.564      Direction:       out
Data (Rx) in Byte:    784        Link Type:       LAN
Speed (KByte/s):      0.152      Encryption:      AES GCM 256
```

The live log of the Management Console will show an accepted RADIUS request using EAP:



```
30.03.2017 15:34:14   RADIUS   RADIUS: EAP Accept [user1@eap.md5]
30.03.2017 13:26:27   Tasks    Creating Client Configurations completed (1 created, 0 with error) (Task 2)
30.03.2017 13:26:27   Tasks    Start generating Client Configurations. (Task 2, jd)
29.03.2017 22:59:09   Tasks    Creating Client Configurations completed (1 created, 0 with error) (Task 3)
```

The client’s log file shows the negotiation steps in detail. Select “Logbook..” from the “Help” menu to take a closer look. Below is just an excerpt of most significant lines.

Initiation of the VPN connection. The first line shows the start of the IPsec negotiation. The second line indicates which networking interface of the client system is used to send the first message out. Following this the client sends (XMIT) the initial INIT message to SRX (vpngw=[IP address] and reveives the response which is recognized as coming from a Juniper SRX gateway.

```
3/30/2017 3:34:13 PM - IPSec: Start building connection
3/30/2017 3:34:13 PM - ipsdial: internal connect chose the following interface address=192.168.100.10
3/30/2017 3:34:13 PM - Ike: ConRef=4, XMIT_MSG1_INIT, name=My local SRX profile, vpngw=192.168.100.249:500
3/30/2017 3:34:13 PM - Ike: ConRef=4,  RECV_MSG2_INIT, name=My local SRX profile, vpngw=192.168.100.249:500
3/30/2017 3:34:13 PM - Ike: ConRef=4, Remote peer is a JUNIPER-SRX
```

A few log lines later first AUTH messeage is sent (XMIT) to the SRX followed by additional info regarding the client’s IKE ID.

```
3/30/2017 3:34:13 PM - Ike: ConRef=4, XMIT_MSG1_AUTH, name=My local SRX profile, vpngw=192.168.100.249:500
3/30/2017 3:34:13 PM - Ikev2:send idi payload:ID_USER_FQDN:pid=0,port=0,user1@eap.md5
```

A little bit further down the log the client initiates the EAP negotiation and the confirmation that the client received the SRX’ certificate and that it is authenticating using RSA. A few lines down the IKE ID of SRX is also shown in the log.

```
3/30/2017 3:34:13 PM - IkeV2: ConRef=4,Auth - initiating an EAP session
3/30/2017 3:34:14 PM - Ikev2: ConRef=4, Received 1 certificates.
3/30/2017 3:34:14 PM - Auth: ConRef=4,Remote is authenticating with=1,RSA
…
3/30/2017 3:34:14 PM - Ikev2:recv IDR payload:ID_FQDN:pid=0,port=0,vsrx.vm-ncp.local
```

The log also shows information about the EAP negotiation indicating that MD5 is used here:

```
3/30/2017 3:34:14 PM - Eap-Md5Cp:Client Receiving MD5-Challenge
3/30/2017 3:34:14 PM - EAP:Sending MD5Response - user1@eap.md5
3/30/2017 3:34:14 PM - Eap: status=0,Method=MD5
3/30/2017 3:34:14 PM - Eap: status success,method=MD5
```

When everything works out fine the log will show information about assigned IP addresses and state the VPN tunnel was established successfully. The first success line listed below indicates that all the IPsec (ESP) phase was successful while the last line in the below informs that the assigned IP address was successfully bound to client's NIC and therefore the link is operational.

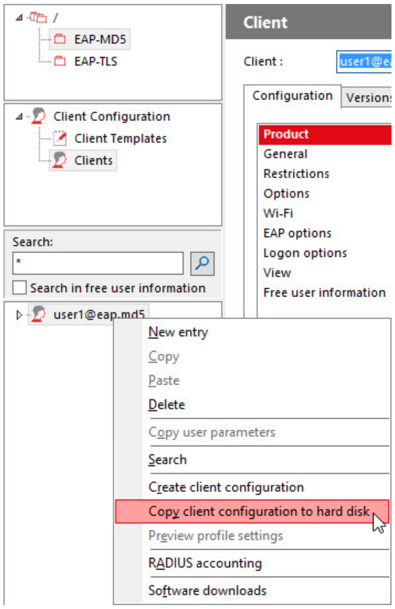
```
3/30/2017 3:34:14 PM - IPSec: Assigned IP Address:IPv4=172.16.119.13,IPv6=0.0.0.0
3/30/2017 3:34:14 PM - SUCCESS: IpSec connection ready
3/30/2017 3:34:17 PM - SUCCESS: Link -> <My local SRX profile> IP address assigned to IP stack - link is operational.
```

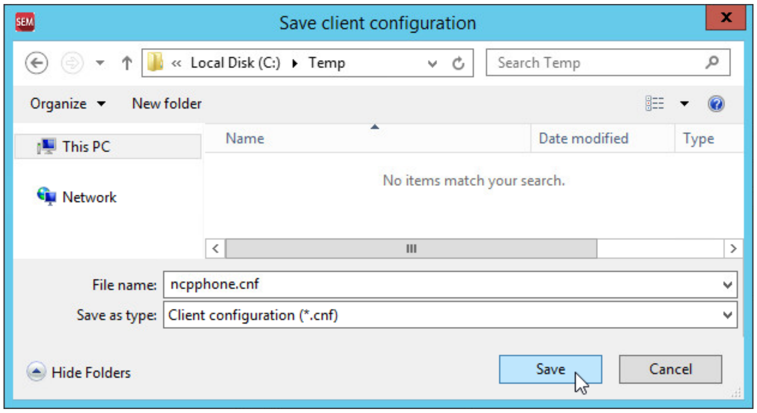
## 4.2. Copying the configuration previously created on the Management Server

As we now know that the Management Server configuration regarding the RADIUS EAP authentication works we look into the second option mentioned earlier in this chapter to configure the client. This will be by saving the configuration created previously in the Management Server to file and copying it over to the client.

### 4.2.1. Save the Management Server based client configuration to file

- Start the Management Console and logon to the Management Server.
- Select the "EAP-MD5" in the group section.
- Click on "Clients" in the "Client Configuration" plug-in
- Right click on the user object to open the context menu.
- Select "Copy Client Configuration to hard disk" and save the "ncpphone.cnf" file.





File name: ncpphone.cnf

Save as type: Client configuration (*.cnf)

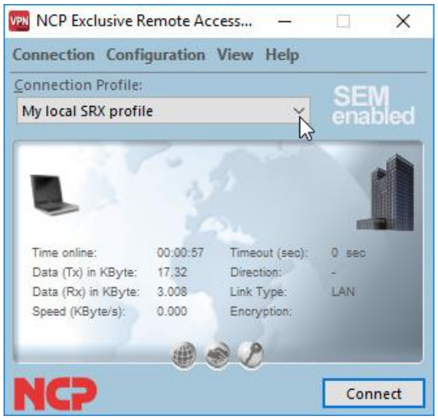
The NCP Exclusive Remote Access Clients processes two major configuration file formats:

- ncpphone.cfg
  This is the general configuration file written locally by the client. Whenever you locally change a setting the "ncpphone.cfg" file will be updated and stored.
- ncpphone.cnf
  This is the configuration file format created by the Management Server. In addition to the data provided by the "ncpphone.cfg" it can also contain information regarding installation and some other things. It is used to import configuration data into a "ncpphone.cfg".

### 4.2.2. Configuring the client using the "ncpphone.cnf" file

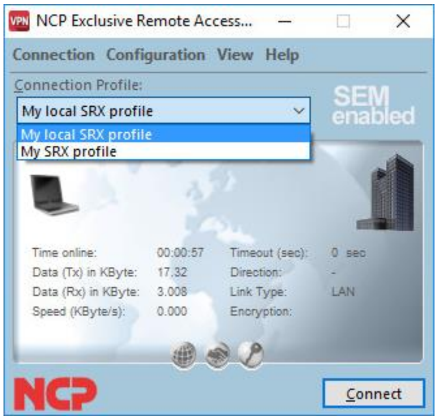
Copy the "ncpphone.cnf" file into the client's installation folder ("%programfiles%\NCP\Exclusive Remote Access Client\"). Mind that you must have administrator privileges to copy the file!
There will be several "ncpphone" files with different extensions in the client installation folder now. The ".bak" and ".sav" are internal backup files created by the client automatically and we don't need care for those.

As mentioned before the "ncpphone.cnf" is used as source to import information into an existing "ncpphone.cfg" file. The import can manually be triggered by monitor application starting up. Therefore, just exit the "NCP Exclusive Remote Access Client Monitor" (menu "Connection"; select "Exit") and open it again. At first glance you won't notice any change looking at the client monitor. However, when pulling down the list of "Connection profiles you will see two entries where there was only one before:



Connection Profile: My local SRX profile

Time online: 00:00:57
Data (Tx) in KByte: 17.32
Data (Rx) in KByte: 3.008
Speed (KByte/s): 0.000
Timeout (sec): 0 sec
Direction: -
Link Type: LAN
Encryption:



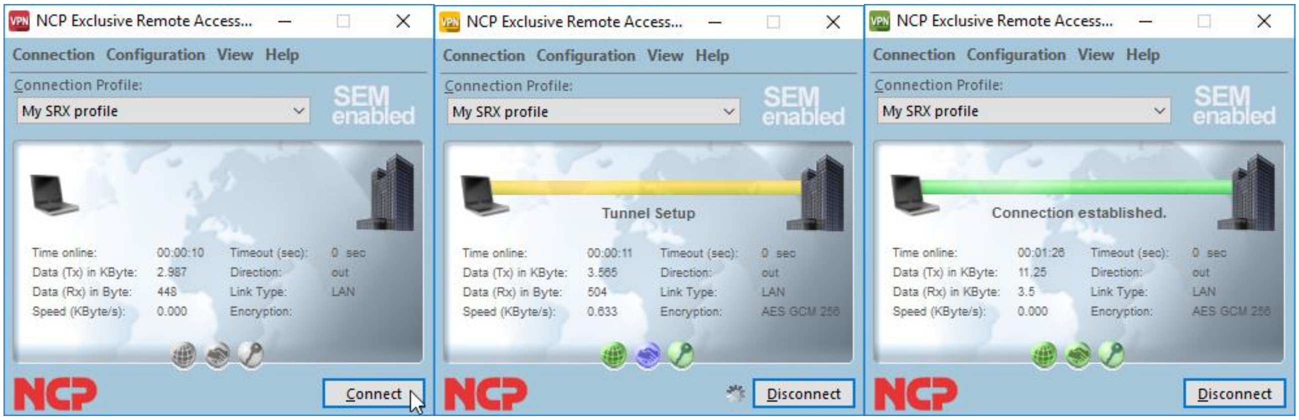
Connection Profile: My local SRX profile
My local SRX profile
My SRX profile

Time online: 00:00:57
Data (Tx) in KByte: 17.32
Data (Rx) in KByte: 3.008
Speed (KByte/s): 0.000
Timeout (sec): 0 sec
Direction: -
Link Type: LAN
Encryption:

In the example above the profile previously created in the client was named "My local SRX profile". The second profile "My SRX profile" imported from the "ncpphone.cnf" file was created with Management Console before. It should work as well as to connect with the SRX as locally configured one.

### 4.2.3. Testing the Management Server originating client configuration

Select the profile created on the Management Server (here: “My SRX profile”) and click “Connect”.


NCP Exclusive Remote Access...
Connection Configuration View Help
SEM enabled
Connect
Disconnect
Disconnect

Connection Profile: My SRX profile

Time online: 00:00:10 · Timeout (sec): 0 sec
Data (Tx) in KByte: 2.987 · Direction: out
Data (Rx) in Byte: 448 · Link Type: LAN
Speed (KByte/s): 0.000 · Encryption:

Connection Profile: My SRX profile

Tunnel Setup

Time online: 00:00:11 · Timeout (sec): 0 sec
Data (Tx) in KByte: 3.565 · Direction: out
Data (Rx) in Byte: 504 · Link Type: LAN
Speed (KByte/s): 0.633 · Encryption: AES GCM 256

Connection Profile: My SRX profile

Connection established.

Time online: 00:01:26 · Timeout (sec): 0 sec
Data (Tx) in KByte: 11.25 · Direction: out
Data (Rx) in KByte: 3.5 · Link Type: LAN
Speed (KByte/s): 0.000 · Encryption: AES GCM 256

## 5. Enabling communication between client and Management Server

This far it was only about connecting the VPN tunnel between client and SRX without any verification of data transfer through the tunnel. The NCP Exclusive Remote Access Client must be able to communicate with *its* Management Server. This is for two reasons, where the first one is licensing and second one central management of the client. The goal of this chapter is to describe how to configure client and Management Server to make this happen.

### 5.1. Basic network communication through the VPN tunnel

For ideal testing purposes make sure that you can “ping” the Management Server and that the traffic is not (yet) selectively blocked on port and protocol level. The Management Server must be accessible through the VPN tunnel.
Establish the VPN connection between client and SRX. Then open a command prompt on the client system and ping the IP address of the Management Server (here: 10.10.10.1). The result should be like this:

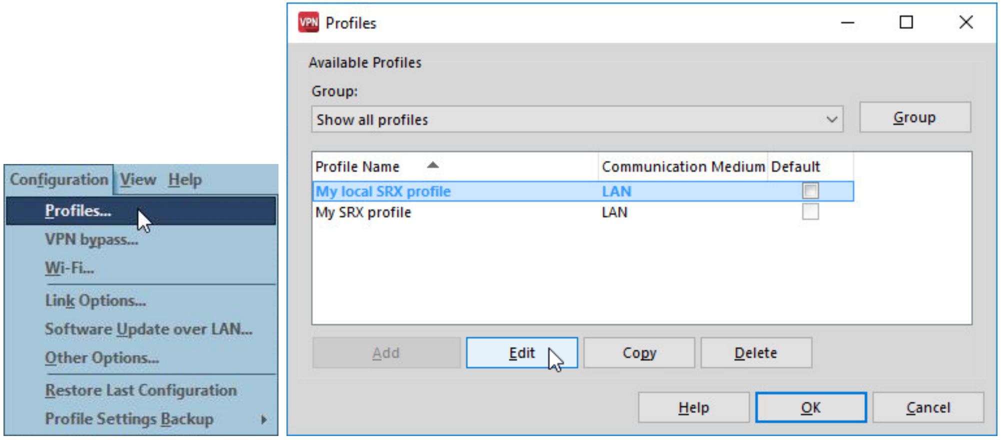
```
C:\>ping 10.10.10.1

Pinging 10.10.10.1 with 32 bytes of data:
Reply from 10.10.10.1: bytes=32 time=1ms TTL=126
Reply from 10.10.10.1: bytes=32 time<1ms TTL=126
Reply from 10.10.10.1: bytes=32 time<1ms TTL=126
Reply from 10.10.10.1: bytes=32 time<1ms TTL=126

Ping statistics for 10.10.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>
```

If you cannot ping the Management Server you have to check the network/firewall settings of your test environment until the Management Server can be reached through the tunnel. In this setup the client is assigned an IP address on the network 172.16.119.0, so the Management Server will have to have a route to the SRX for this network.

### 5.2. Enabling the client to reach out for the Management Server

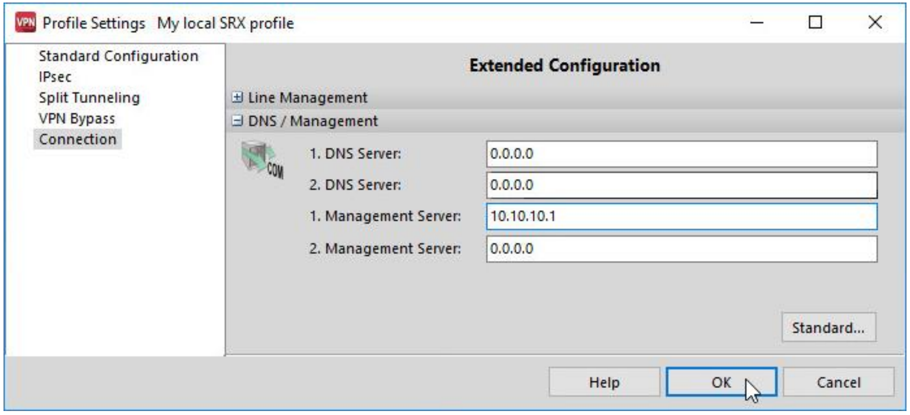
The part of the client responsible for communication with the Management Server is the “NCP Client Update Service” running in the background (short: “update client”). The update client needs to know the IP address of the Management Server and will start reaching out for the Management Server shortly after the VPN link is operational. It will try 5 times with a retry timer of 15 seconds. If there is no response from the Management Server the update client will go to sleep for 1 hour (3600 seconds) and then try again.

Configure the IP address of your Management Server directly in the locally created client profile “My local SRX profile”. To do so select “Profiles” from the “Configuration” menu and click “Edit”.



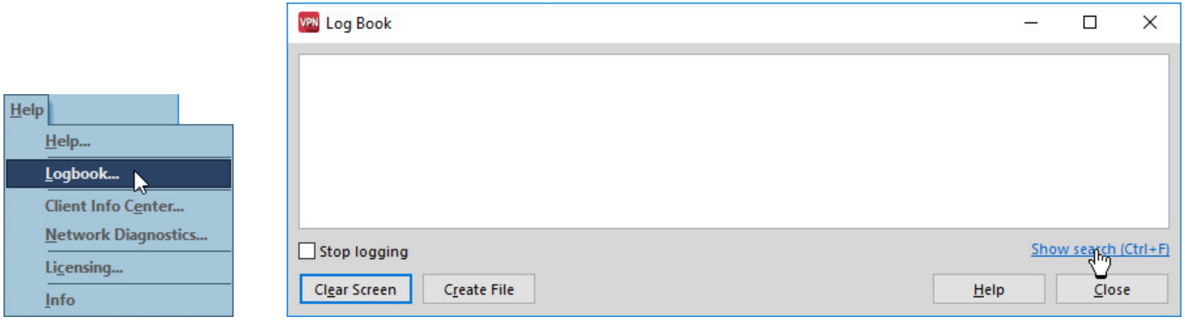
| Profile Name | Communication Medium | Default |
|---|---|---|
| My local SRX profile | LAN | □ |
| My SRX profile | LAN | □ |

Go to the “Connection” configuration group and in “DNS / Management” enter the IP address of your Management Server in “1. Management Server” (here: 10.10.10.1). Then click “OK” to confirm the changes and “OK” to close the “Profiles” dialogue.

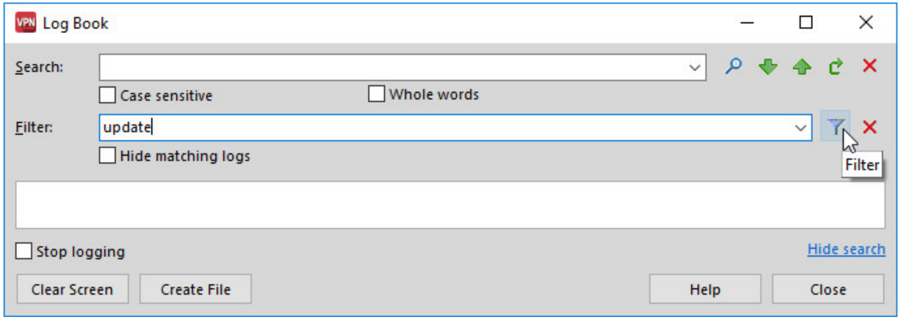


1. DNS Server: 0.0.0.0
2. DNS Server: 0.0.0.0
1. Management Server: 10.10.10.1
2. Management Server: 0.0.0.0

The following pages will describe the communication between update client and Management Server step by step. Therefore, it is best to also take look at the log of the client as it shows what is happening behind the scenes. Open the client’s log view by selecting “Logbook…” from the “Help” menu and in the “Log Book” window click on the link “Show search (Ctrl-F)” just above the “Close” button.

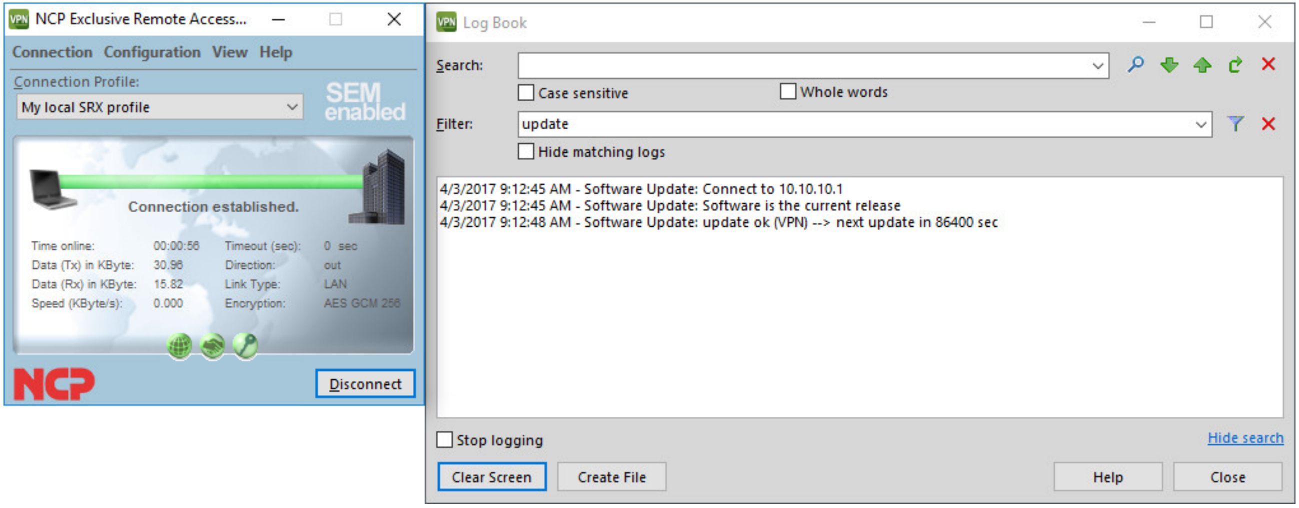


New options for log view will appear at the top of the window. Enter “update” in the “Filter” field and click on the “Filter” icon right next to the field.



This will only show log lines containing the string “update” and so only log entries related to the update process will be displayed while this filter is applied. As the configuration to reach out for the Management Server has already been added the update client should start to send requests to the Management Server as soon as the VPN tunnel is up.

So press “Connect” in the client monitor and wait for the connection to be established and the update client starting to send messages.



```
4/3/2017 9:12:45 AM - Software Update: Connect to 10.10.10.1
4/3/2017 9:12:45 AM - Software Update: Software is the current release
4/3/2017 9:12:48 AM - Software Update: update ok (VPN) --> next update in 86400 sec
```

As shown in the previous screenshot you should see log entries of a successful connection of the update client to the Management Server and the information that the “Software is the current release”. The update client will try again in 86400 seconds which is 24 hours.

With this result the client part is ready to go with the Management Server. However, there need to be some adjustments on the Management Server which are going to be dealt with subsequently.

## 5.3. Configuring the Management Server to provide updates for clients

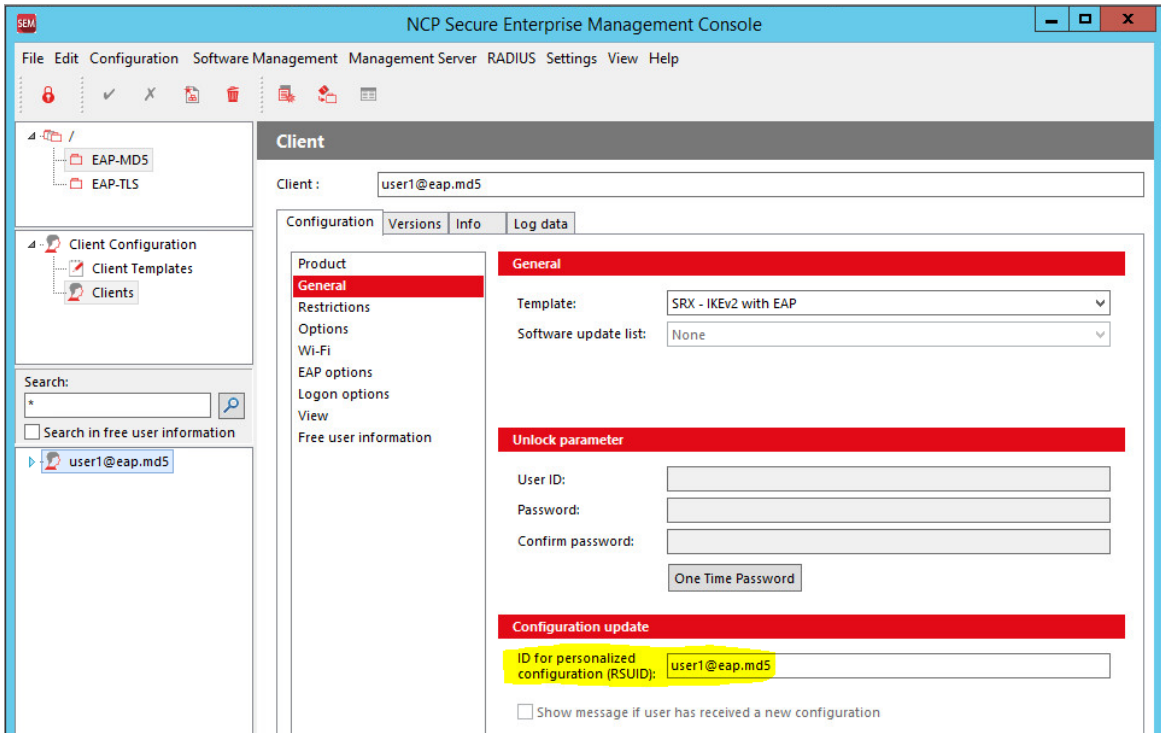
There are several things that need clarification before starting with further configuration of the Management Server. These are:

- How does the update client connect to the Management Server?
  Is there authentication in place and what protocol and ports are used?
- How can the update intervals be modified?
  It is not very useful to wait 24 hours for the next update attempt of the client, especially not in a test environment.
- What is the criteria for the update client to state that the “Software is the current release”?
  What kind of updates can be provided by the Management Server and how?

### 5.3.1. Connection parameters of the update

The connection of the update client to the Management Server is TCP based and there is the update method over VPN which is described here and over LAN which can be used independently of the VPN tunnel but is not part of this document. When connecting over VPN the update client sends its messages over TCP port 12501 to the Management Server (see the communication overview in the appendix for detailed information about the protocols and ports used). So any firewall between the SRX gateway and the Management Server is required to permit TCP port 12501 from the VPN clients’ address range to the Management Server.
When the update client is able to access the Management Server it will present two possible usernames (called the “Remote Software Update ID” or short: “RSUID” to the management server. These to RSUIDs are:

- Hostname
- VPN username



Client : user1@eap.md5

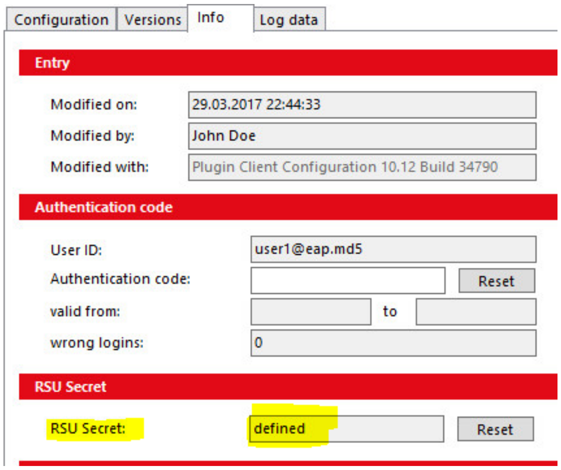
Template: SRX - IKEv2 with EAP

Software update list: None

ID for personalized configuration (RSUID): user1@eap.md5

□ Show message if user has received a new configuration

The Management Server will always first look for an entry with the hostname in all the Management Server's user database; if no entry is found then will it look for an entry matching the VPN username. In our sample configuration we defined the VPN username to be used as RSUID and when the user "user1@eap.md5" was created before the entry was saved accordingly. This can be looked up with the Management Console in the "Configuration" tab within the "General" group as highlighted in the previous screenshot.
With the first connection of the update client over VPN each client and the Management Server will negotiate a random shared secret, saved on both sides, which has to presented by the update client for future connections. Look in "Info" tab to see the status of the "RSU secret".



**Entry**

Modified on: 29.03.2017 22:44:33
Modified by: John Doe
Modified with: Plugin Client Configuration 10.12 Build 34790

**Authentication code**

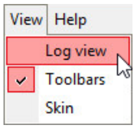
User ID: user1@eap.md5
Authentication code: 
valid from:  to 
wrong logins: 0

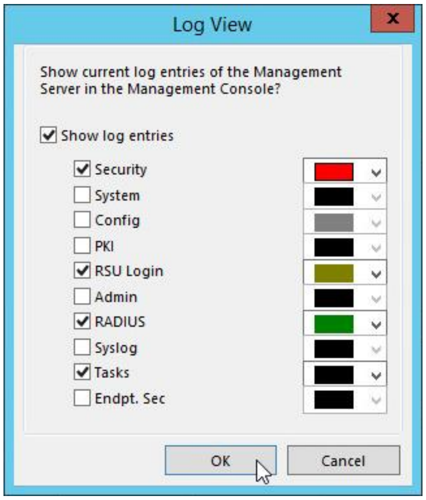
**RSU Secret**

RSU Secret: defined

You can "Reset" the "RSU secret" should you require to do so, for example if the client system is fully reset and the client won't hold the previously negotiated information anymore. A reset "RSU secret" will be negotiated again with the first contact over VPN.

The live log of the Management Console will also show helpful information for every update client connection to the Management Server. This has to be enabled in "View" menu selecting "Log view" as we already did before for "Security", "RADIUS" and "Tasks". Enable "RSU Login" to show update sessions related information then press "OK".



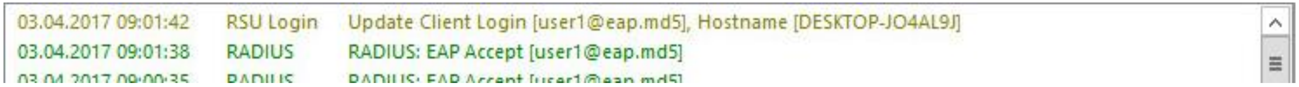


Show current log entries of the Management Server in the Management Console?

☑ Show log entries

- ☑ Security 🟥
- ☐ System ⬛
- ☐ Config ⬛
- ☐ PKI ⬛
- ☑ RSU Login 🟫
- ☐ Admin ⬛
- ☑ RADIUS 🟩
- ☐ Syslog ⬛
- ☑ Tasks ⬛
- ☐ Endpt. Sec ⬛

The log view will immediately show entries of recent update client activity:

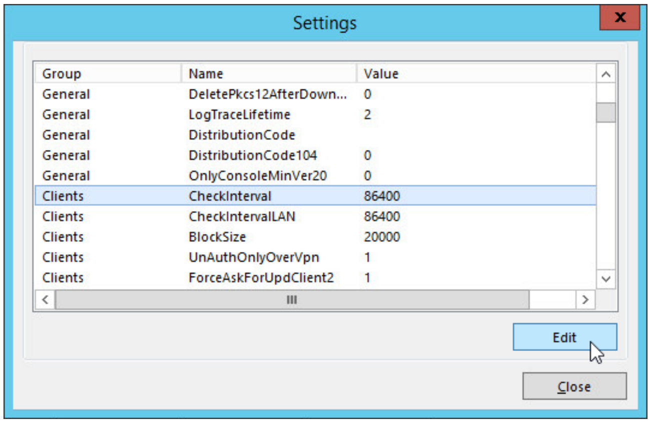


```
03.04.2017 09:01:42    RSU Login    Update Client Login [user1@eap.md5], Hostname [DESKTOP-JO4AL9J]
03.04.2017 09:01:38    RADIUS       RADIUS: EAP Accept [user1@eap.md5]
03.04.2017 09:00:35    RADIUS       RADIUS: EAP Accept [user1@eap.md5]
```

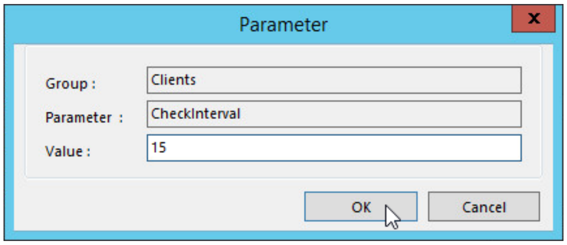
The top line stating that a client contacted the Management Server with RSUID “user1@eap.md5” and the hostname of the system the client is installed on (here: “DESKTOP-JO4AL9J”). Whenever a update client connects to the Management Server a log line like this will be displayed.

## 5.3.2. Modifying the update interval

Working in a test environment or setting up a PoC one will want the update clients to look for configurations much more frequently than in an eventual productive environment. When started (usually after the system has started up) the update client will wait for the VPN connection and then contact the Management Server. Within this session the update client will be informed at what intervals it shall re-connect asking for updates. As already mentioned previously the default value for this is 86400 seconds (24 hours). It would be quite inconvenient to wait that long to receive an update after changes. You could also stop and restart the “rwsrsu” service to force the update client to forget the timer but this also is not the most convenient approach. While testing or still setting up the environment just decrease the interval to 15 or 30 seconds instead. To do so call “Settings” from the “Management Server” menu and scroll down to the “Group” “Clients”, “Edit” the “Value” for the “CheckInterval” and change it to “15” seconds. Press “OK” to confirm the change and “Close” the settings window again. The modification will automatically be applied within a few seconds to the Management Server.



| Group | Name | Value |
|---|---|---|
| General | DeletePkcs12AfterDown... | 0 |
| General | LogTraceLifetime | 2 |
| General | DistributionCode | |
| General | DistributionCode104 | 0 |
| General | OnlyConsoleMinVer20 | 0 |
| Clients | CheckInterval | 86400 |
| Clients | CheckIntervalLAN | 86400 |
| Clients | BlockSize | 20000 |
| Clients | UnAuthOnlyOverVpn | 1 |
| Clients | ForceAskForUpdClient2 | 1 |

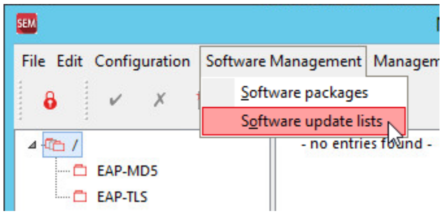


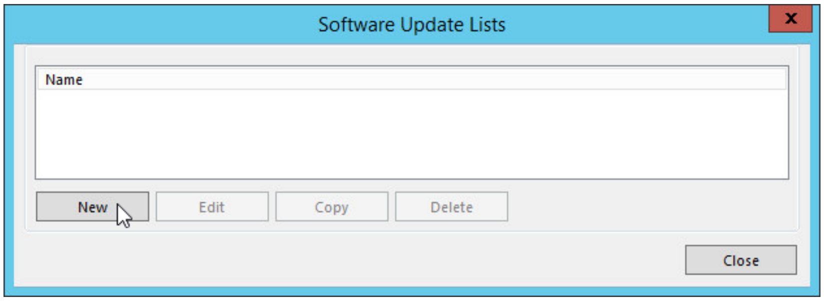
Group : Clients
Parameter : CheckInterval
Value : 15

With this the update client will re-connect to the Management Server every 15 seconds to look for modified configuration or other updates. Be aware that you should not use an update interval this short within a productive environment! Recommended values start are not less than 1 hour (3600 seconds) depending on the requirements.

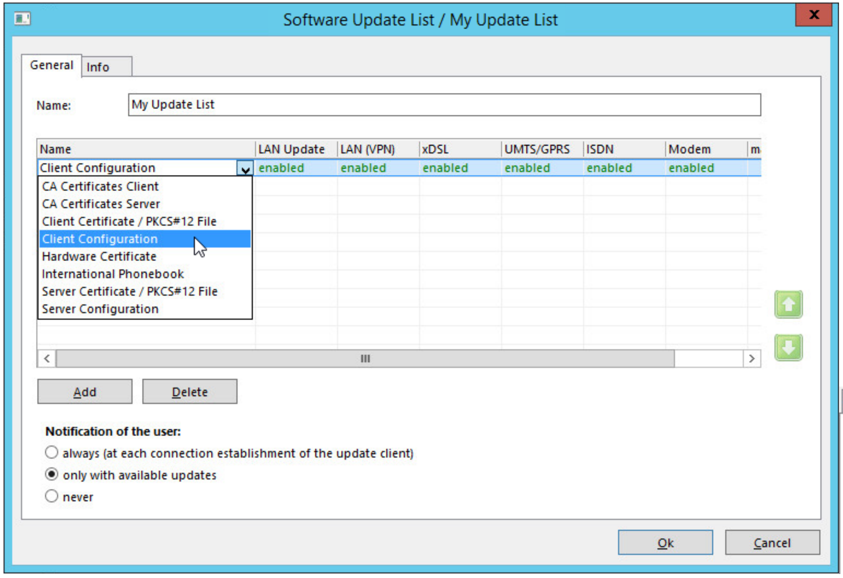
## 5.3.3. Defining updates for the clients

This far our client will not yet receive anything from the Management Server in spite of being able to establish an update session and us having created a configuration for “user1@eap.md5” previously. So how can it be achieved that the configuration is actually transferred the client?
The Management Server must be configured through a so-called “software update list” which information has to be provided to the clients. Software update lists are configured on group level and can be inherited by subgroups as already seen with the client templates.
It depends on the requirements of the setup whether to have one update list for all or differentiate between groups. In this sample installation we will use one root group based update list serving the EAP-MD5 and the EAP-TLS group.
To define an update list, go to the “Software Management” menu in the Management Console and select “Software update lists”. Then click “New” to create a new one.





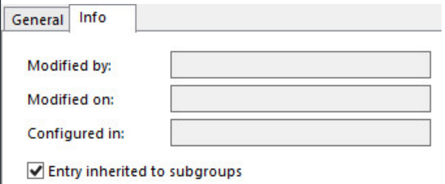
Enter a meaningful name for the update list (here: “My Update List”) and click the “Add” button to create a new package entry. A list of available packages will be presented in drop down list. Select “Client Configuration”. After that go to the “Info” tab and enable “Entry inherited to subgroups” to make this update list also available in the groups below root. Then click “OK” to save the new update list.



Name: My Update List

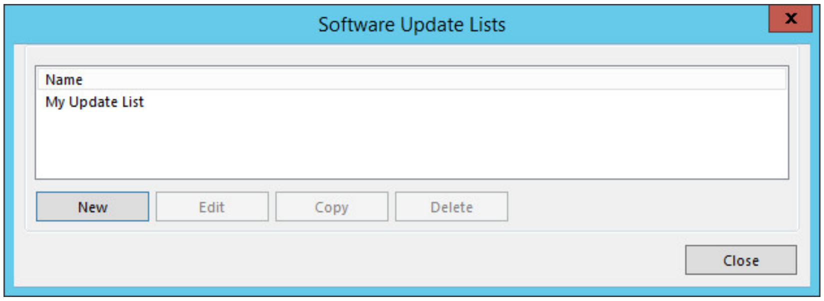
| Name | LAN Update | LAN (VPN) | xDSL | UMTS/GPRS | ISDN | Modem | m |
|---|---|---|---|---|---|---|---|
| Client Configuration | enabled | enabled | enabled | enabled | enabled | enabled | |

Notification of the user:
○ always (at each connection establishment of the update client)
● only with available updates
○ never



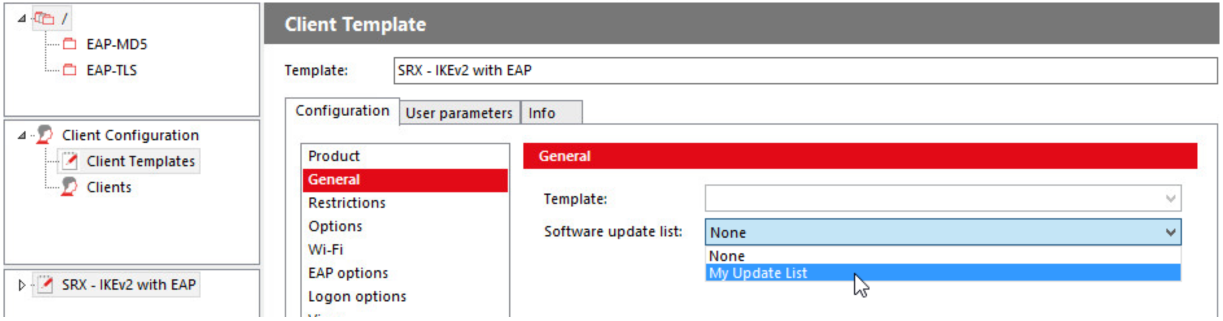
Modified by:
Modified on:
Configured in:
☑ Entry inherited to subgroups

Next Generation Network Access Technology


Software Update Lists

Name
My Update List

Now this new update list can be assigned to our client template. In the root group select the according client template (here: “SRX – IKEv2 with EAP”). Then in the “Configuration” tab select “General” and click on the “Software update list” which will show the available update list(s).



Template: SRX - IKEv2 with EAP

Template:

Software update list: None

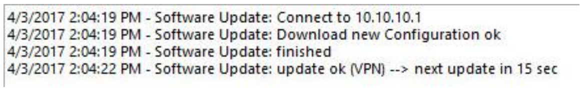
None
My Update List

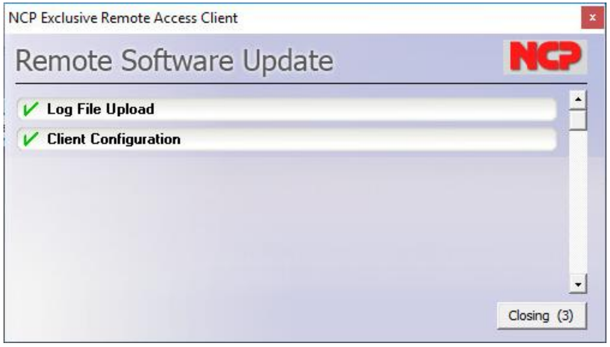
Select your update list (here: My Update List) and save the configuration via the green tick in the icon bar. This will immediately enable this update list for all existing users under this template.

## 5.3.4. Retrieve the update from Management Server

Remember that the update client will only reach out for the Management Server after the 24-hour timer has run down. You could either wait or – properly the better option – just restart the update client. With administrator privileges restart the “NCP Client Update Service” (alternatively call “net stop rwsrsu” followed by “net start rwsrsu” in a command prompt run with administrator privileges).

After that establish the client VPN connection and look at its log which should still be filtering on “update”. The log will start with the line of the update connect to the Management Server and after that the update info windows will pop up informing about the update packages being processed.


```
4/3/2017 2:04:19 PM - Software Update: Connect to 10.10.10.1
4/3/2017 2:04:19 PM - Software Update: Download new Configuration ok
4/3/2017 2:04:19 PM - Software Update: finished
4/3/2017 2:04:22 PM - Software Update: update ok (VPN) --> next update in 15 sec
```


NCP Exclusive Remote Access Client

Remote Software Update

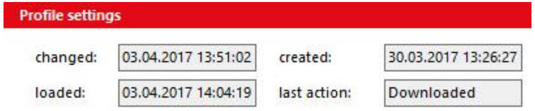
✓ Log File Upload
✓ Client Configuration

The “Remote Software Update” info window will automatically close after 5 seconds. The information displayed in this window depends on the assigned software update list. The “Log File Upload” is always shown no matter which packages have been added to the update list. As we only added the “Client Configuration” package to our list it is displayed here. Looking at the log file again you will see entries for the configuration download and that the update has finished. With the previously reduced “Check Interval” the update client will look for updates again in 15 seconds.
There also is a dedicated update client log named “rwsrsu.log” written to the log folder in the client’s installation path. For the recent update session this log contains the following lines (among others):

```
17-04-03 14:04:18 Start Update (VPN)
17-04-03 14:04:18 Software Update: Connect to 10.10.10.1
17-04-03 14:04:18 Request Logon (VpnUserID=user1@eap.md5, PcName=DESKTOP-JO4AL9J, fromCert=0)
17-04-03 14:04:19 Request Package [RWSCFG]
17-04-03 14:04:19   Downloading File C:\Program Files\NCP\Exclusive Remote Access
Client\rsudata\RWSCFG\v_1_0\2\ncpphone.cnf
17-04-03 14:04:19 Request Package RWSCFG ret = 0 new=1
17-04-03 14:04:19 Copy ncpphone.cnf file (ok=1, err=0, C:\Program Files\NCP\Exclusive Remote Access
Client\\rsudata/ncpphone.cnf->C:\Program Files\NCP\Exclusive Remote Access Client\/ncpphone.cnf)
17-04-03 14:04:19 Software Update: Download new Configuration ok
17-04-03 14:04:19 Disconnect
17-04-03 14:04:19 Software Update: finished
17-04-03 14:04:21 Software Update: update ok (VPN) --> next update in 15 sec
```

The first highlighted line “Request Package [RWSCFG]” states that the “Client Configuration” package is part of the software update list and in phase there is verified whether there is a new configuration available on the Management Server. This is stated by the second highlighted line with the info “new=1”; meaning there is a new configuration available and has to be downloaded.
Checking if there is a new configuration available on Management Server is done by comparing the “ncpphone.cnf” on the Management Server to the one existing on the client. The third highlighted entry above is “rsudata/ncpphone.cfg” which indicates that the “ncpphone.cnf” downloaded from the Management Server is not only copied to the regular installation path of the client but also to the “rsudata” folder in this path. The update client compares a “ncpphone.cnf” file in the client’s “rsudata” folder with the one available on Management Server. If there is no cnf-file in “rsudata” or the Management Server one is newer than the local one it will be download from Management Server. You can try this by keeping the VPN tunnel connected and deleting the “ncpphone.cnf” in the “rsudata” folder. With the next update session it will be downloaded again. Disconnecting the VPN connection will start the import process of the cnf-configuration into the “ncpphone.cfg” file as described earlier in this document.

In the Management Console’s live log you should see repeated “RSU Login” lines showing the update sessions of the client. In the management console you can also verify if the client already downloaded the configuration by looking at “Info” tab on the respective client entry (here: user1@eap.md5).



Profile settings

changed: 03.04.2017 13:51:02 created: 30.03.2017 13:26:27
loaded: 03.04.2017 14:04:19 last action: Downloaded

The entry for “last action” should be “Downloaded”. Whenever you change a client setting on Management Server and create the configuration for this client (or all in the group) it will be downloaded by the update client with the next session. Just play with it a little bit by changing the profile name in the template…

## 5.4. Licensing

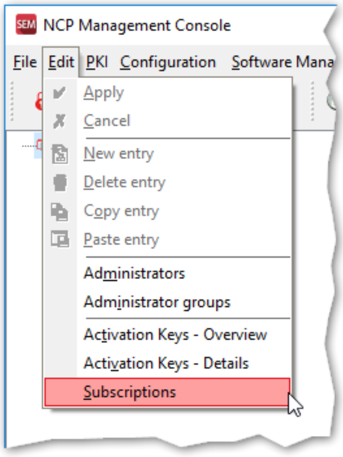
Every NCP software product comes with a 30-day trial period. Within this time frame the product can be tested without limitations. Before the trial expires for Management Server and clients they should be equipped with valid licenses each.

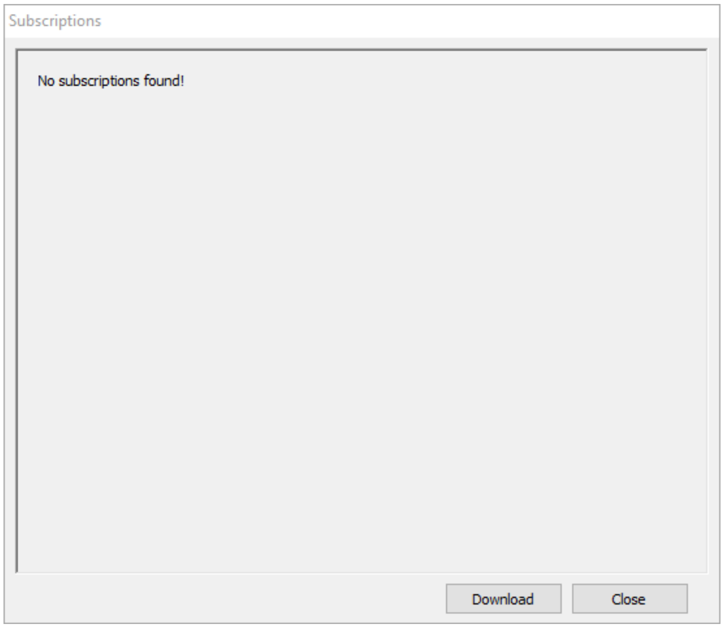
### 5.4.1. Subscription License

If you have purchased a subscription license for NCP Exclusive Remote Access Management Clients this will include the number of Managed Units for Management according to the number of clients you licensed. The following licenses are available:

- Desktop Clients
  A desktop client license can be used with these client flavors:
  - NCP Exclusive Remote Access Windows Client
  - NCP Exclusive Remote Access macOS Client
- Mobile Clients
  A mobile client license can be used with these client flavors:
  - NCP Exclusive Remote Access iOS Client
  - NCP Exclusive Remote Access Android Client

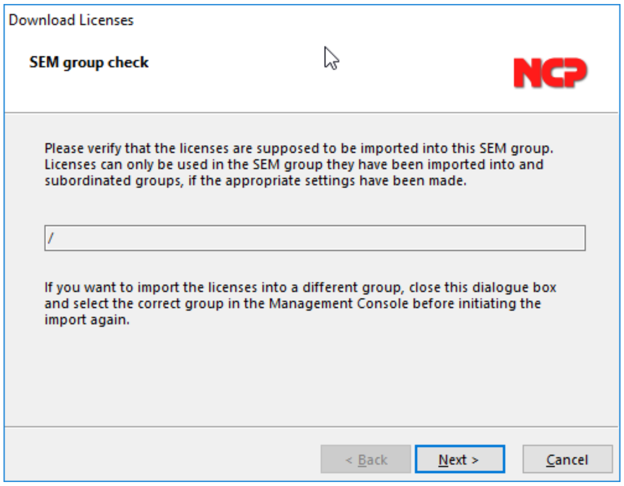
To provide the Exclusive Remote Access Management Console with your license go to the *Edit* menu and select *Subscriptions.* The information that no subscriptions have been found yet will be displayed. Click the *Download* button to proceed.





No subscriptions found!

First you have to specify within which groups on the Management Server the license is going to be available. In a multi-tenant environment, it could well be that different licenses are assigned to different groups (=tenants). This example works with a flat structure and therefore the license is assigned to the root ("/") group.
The next step is to enter the license information which enables the Management Server to download the respective subscription details from the NCP Activation Server. Enter *Subscription serial number*, *Download Key* and a valid *E-mail address*.



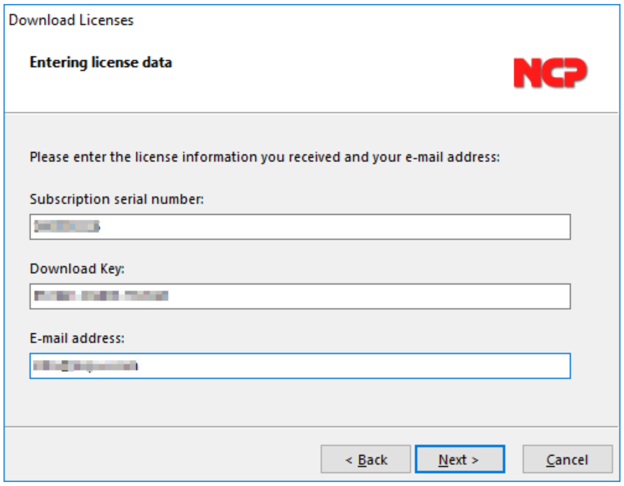
Download Licenses

**SEM group check**

Please verify that the licenses are supposed to be imported into this SEM group. Licenses can only be used in the SEM group they have been imported into and subordinated groups, if the appropriate settings have been made.

/

If you want to import the licenses into a different group, close this dialogue box and select the correct group in the Management Console before initiating the import again.



Download Licenses

**Entering license data**

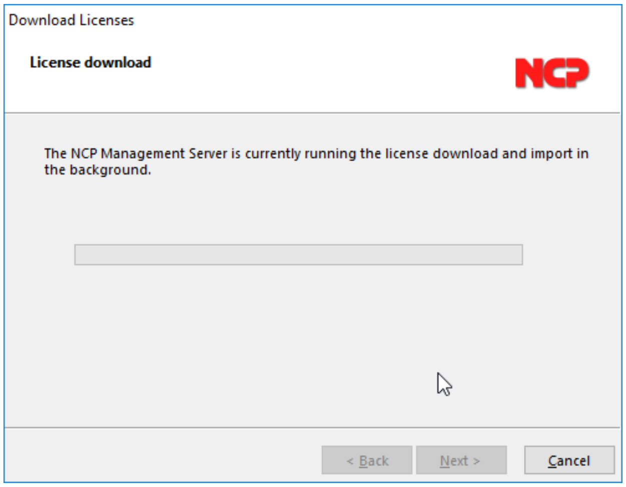
Please enter the license information you received and your e-mail address:

Subscription serial number: [redacted]

Download Key: [redacted]

E-mail address: [redacted]

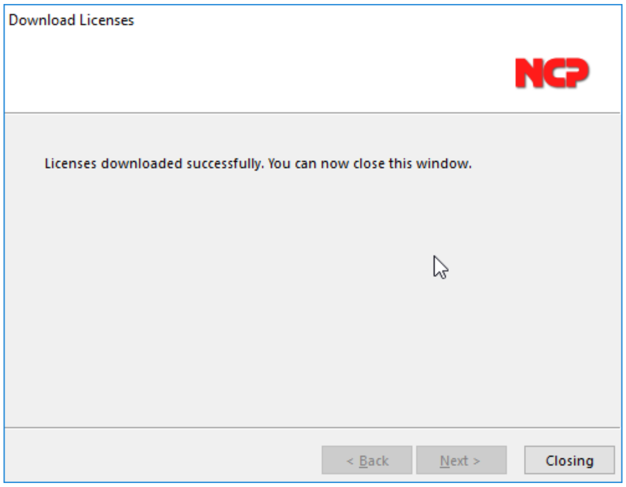
The Management Server will connect securely to the NCP Activation Server which verifies the validity of the subscription license and if successful will feed the Management Server with the respective subscription details.



Download Licenses

**License download**

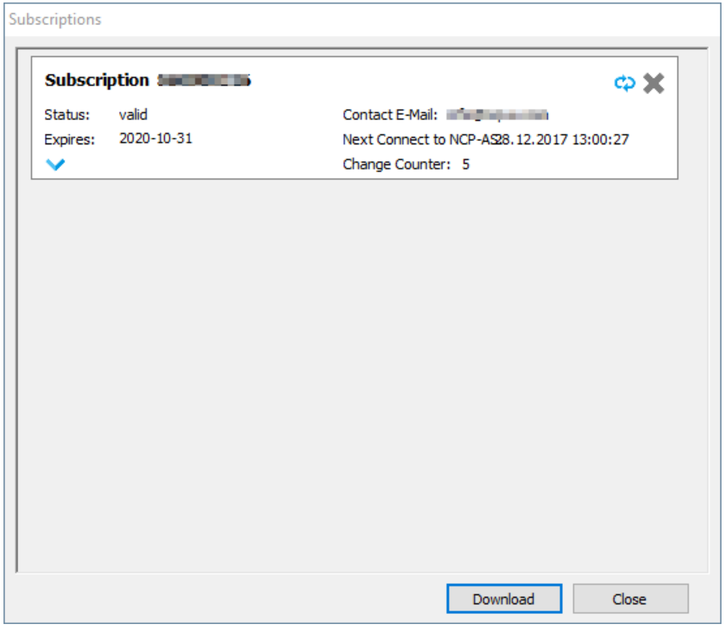
The NCP Management Server is currently running the license download and import in the background.



Download Licenses

Licenses downloaded successfully. You can now close this window.

After the successful verification and download the according information is displayed in the dialog.

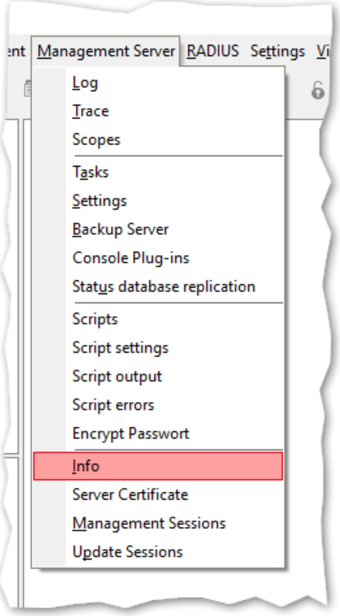


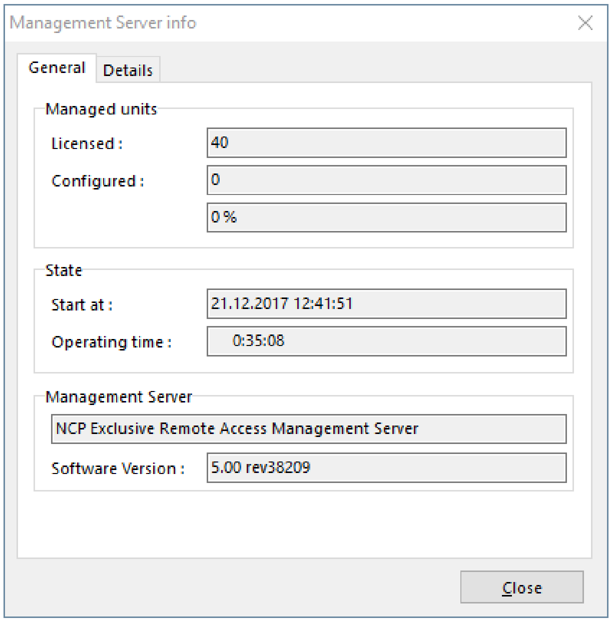
**Subscription** [redacted]

Status: valid
Expires: 2020-10-31
Contact E-Mail: [redacted]
Next Connect to NCP-AS28.12.2017 13:00:27
Change Counter: 5

Click the *Close* button to leave the subscription download.

Additionally, you can view the amount of licensed *Managed units* by selecting Info the *Management Server* menu:





Managed units

Licensed : 40
Configured : 0
0 %

State

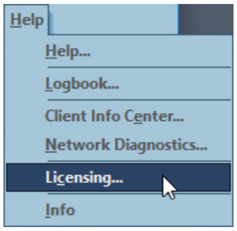
Start at : 21.12.2017 12:41:51
Operating time : 0:35:08

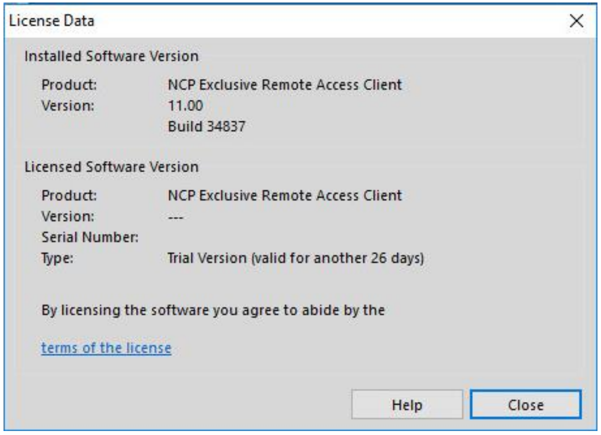
Management Server

NCP Exclusive Remote Access Management Server
Software Version : 5.00 rev38209

## 5.4.2. Client license deployment

Client licenses are solely handled by the Management Server and cannot be assigned locally on the client system. In the client GUI select “Licensing” from the “Help” menu to see how much trial days are still left.




License Data

Installed Software Version

| | |
|---|---|
| Product: | NCP Exclusive Remote Access Client |
| Version: | 11.00<br>Build 34837 |

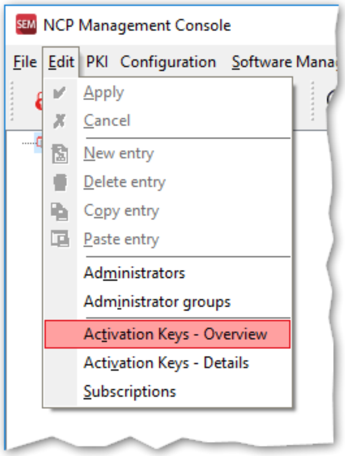
Licensed Software Version

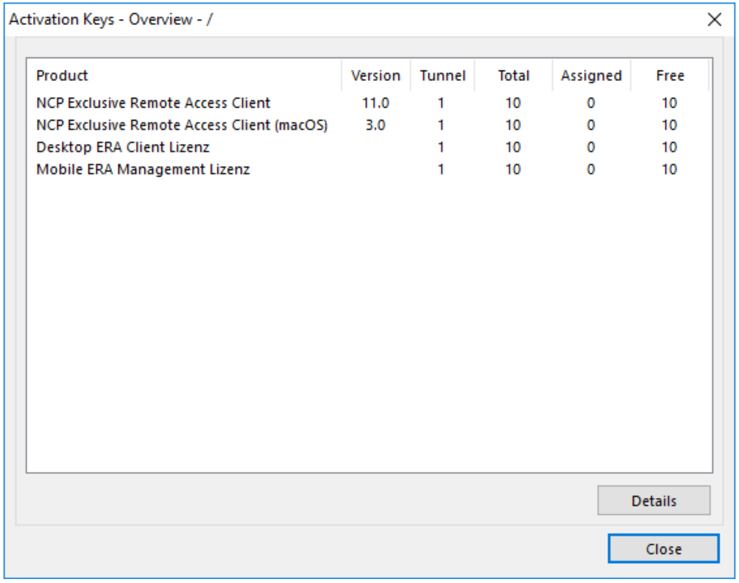
| | |
|---|---|
| Product: | NCP Exclusive Remote Access Client |
| Version: | --- |
| Serial Number: | |
| Type: | Trial Version (valid for another 26 days) |

By licensing the software you agree to abide by the

terms of the license

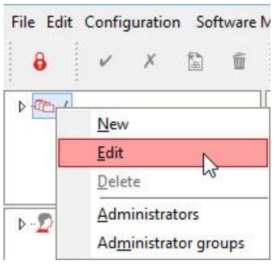
For an overview of the available client licenses coming with your subscription in the Management Console open the “Edit” menu and select “Activation Keys – Overview” and click “Import” in the following dialogue.

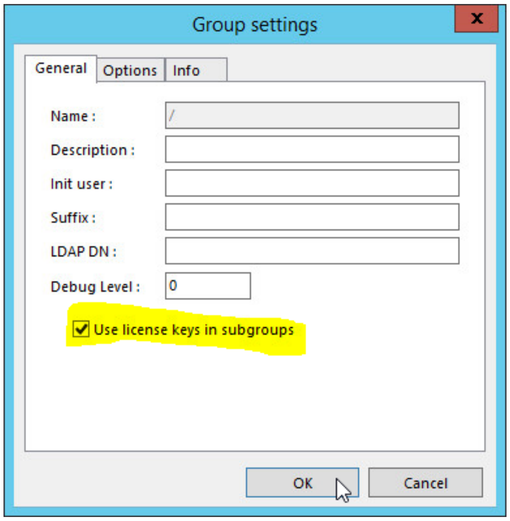



Activation Keys - Overview - /

| Product | Version | Tunnel | Total | Assigned | Free |
|---|---|---|---|---|---|
| NCP Exclusive Remote Access Client | 11.0 | 1 | 10 | 0 | 10 |
| NCP Exclusive Remote Access Client (macOS) | 3.0 | 1 | 10 | 0 | 10 |
| Desktop ERA Client Lizenz | | 1 | 10 | 0 | 10 |
| Mobile ERA Management Lizenz | | 1 | 10 | 0 | 10 |

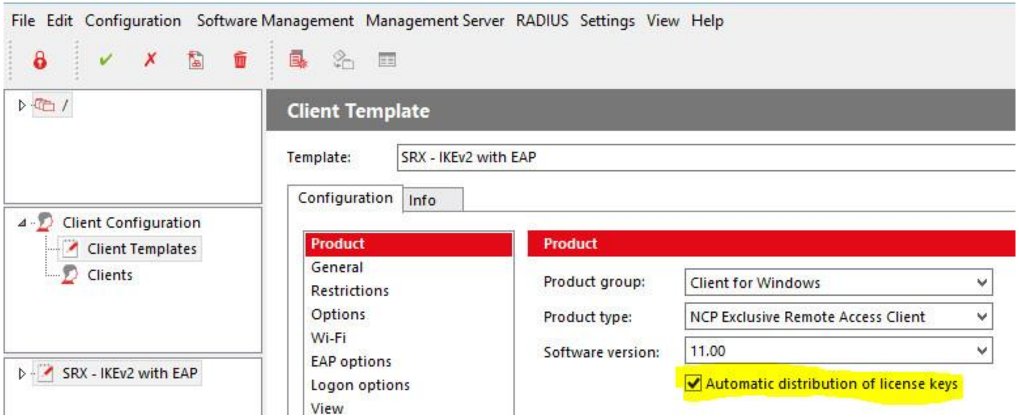
However, the Management Server still requires configuration to deploy these licenses. The first step is to configure the root group to make licenses available to subgroup. Right click on the root group and select “Edit” in the context menu. This will open the “Group settings” window for the root group (“/”) where the option “Use license keys in subgroups” must be enabled. Save the changes with “OK”.





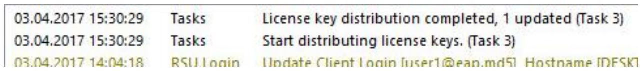
Name : /
Description :
Init user :
Suffix :
LDAP DN :
Debug Level : 0
☑ Use license keys in subgroups

Last but not least the client template must be modified to process licenses. Select the according template and in the “Configuration” tab select the “Product” group. Enable the option “Automatic distribution of license keys” as highlighted below and save the changes using the green tick on the icon bar.



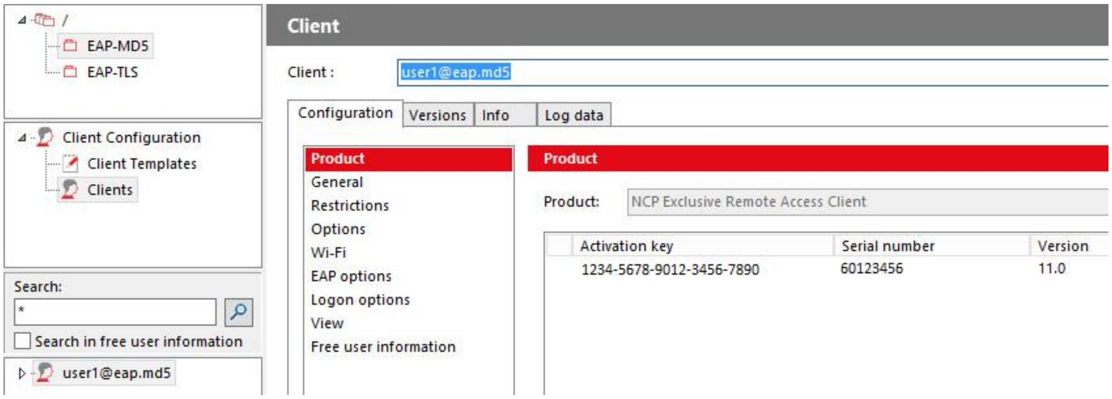
Template: SRX - IKEv2 with EAP
Product group: Client for Windows
Product type: NCP Exclusive Remote Access Client
Software version: 11.00
☑ Automatic distribution of license keys

The Management Console’s live log will immediately display “Tasks” related entries informing about the number of licenses having been distributed. As only one client object (“user1@eap.md5”) has been created so far the number here is “1”.



```
03.04.2017 15:30:29   Tasks       License key distribution completed, 1 updated (Task 3)
03.04.2017 15:30:29   Tasks       Start distributing license keys. (Task 3)
03.04.2017 14:04:18   RSU Login   Update Client Login [user1@eap.md5] Hostname [DESK]
```

Verify the assigned license by going to the client configuration and looking at the “Product” group in the “Configuration” tab. “Activation key”, “Serial number” and “Version” should be listed here.



Search: *

user1@eap.md5

Client : user1@eap.md5

Product

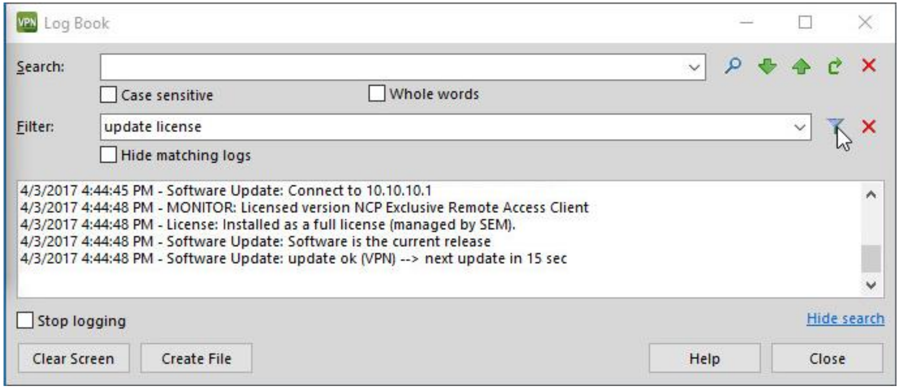
Product: NCP Exclusive Remote Access Client

| Activation key | Serial number | Version |
|---|---|---|
| 1234-5678-9012-3456-7890 | 60123456 | 11.0 |

It is not required to create the configuration for the user as the license part is handled outside the configuration between update client and Management Server.

## 5.4.3. Receiving license information on the client

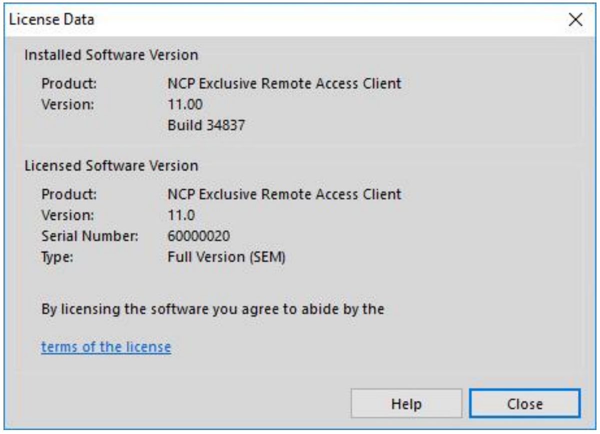
On the client open the “Logbook” again and extend the filter to “update license” which will show all log lines containing either the string “update” or “license”. Then establish the VPN connection to start the update session as already described before. After the tunnel is up the client log should soon show information about the software update and licensing as in following screenshot. The important line contains “Installed as a full license (managed by Management Server)”.



Filter: update license

```
4/3/2017 4:44:45 PM - Software Update: Connect to 10.10.10.1
4/3/2017 4:44:48 PM - MONITOR: Licensed version NCP Exclusive Remote Access Client
4/3/2017 4:44:48 PM - License: Installed as a full license (managed by SEM).
4/3/2017 4:44:48 PM - Software Update: Software is the current release
4/3/2017 4:44:48 PM - Software Update: update ok (VPN) --> next update in 15 sec
```

Also take a look at “Licensing” in the client’s “Help” menu to verify the current licensing status of the client.



Installed Software Version

Product: NCP Exclusive Remote Access Client
Version: 11.00
Build 34837

Licensed Software Version

Product: NCP Exclusive Remote Access Client
Version: 11.0
Serial Number: 60000020
Type: Full Version (SEM)

By licensing the software you agree to abide by the

terms of the license

The previously mentioned “rwsrsu.log” (written to the log folder in the client’s installation path) also shows the information of the recent update session (only specific lines listed below):

```
17-04-03 16:44:45 Software Update: Connect to 10.10.10.1
17-04-03 16:44:45 Reading license file
17-04-03 16:44:45 Call rwscmd -> new license from Management Server
17-04-03 16:44:46 Call ncpclientcmd -> check ncp.db
17-04-03 16:44:46 Disconnect
17-04-03 16:44:48 Software Update: update ok (VPN) --> next update in 15 sec
```

The updated license is written to the “ncp.db” which holds the license status of the client. The client has to get in touch with the Management Server at least once every 16 days. Otherwise it will lose its status of full license and only allow for a VPN connection to communicate with the Management Server. Any other communication will be blocked until the license status can be updated.

# Appendix

# A Installation of supported database servers

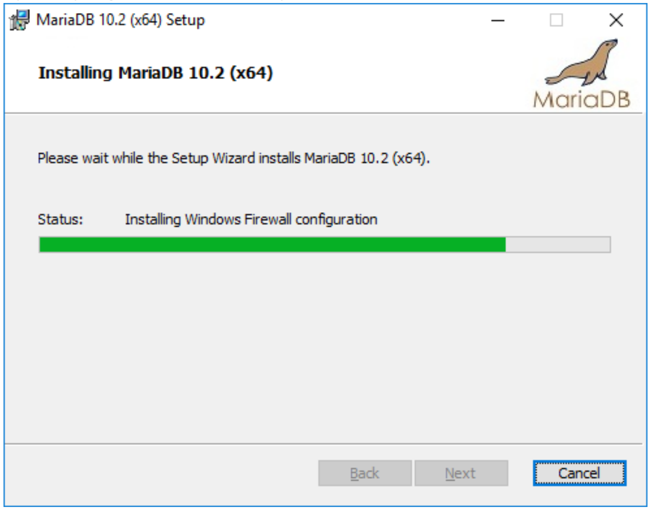
The NCP Exclusive Remote Management Server requires a separately installed database server and supports various of those, such as MariaDB, Microsoft SQL Server and others. This documentation describes how to install and setup MariaDB on Windows and Linux systems and furthermore Microsoft SQL Server 2014 Express. Please refer to the respective manuals of those database servers for more details regarding installation and operation if necessary.

## A.1. MariaDB

When using MariaDB we strongly recommend to use the Connector/C interface in combination with the NCP Exclusive Remote Management Server. While the installation package for Linux usually already contains the required library a separate installation is required on Windows.
This example is based on the MariaDB Server version 10.2.9 64-bit for Windows (mariadb-10.2.9-winx64.msi) in combination with the MariaDB Connector/C version 3.02 64-bit (mariadb-connector-c-3.0.2-win64.msi).

### A.1.1. Installing MariaDB Server on Windows

Execute the MariaDB Server's MSI package and use standard settings throughout the installation (with specifying an individual password for the root user).



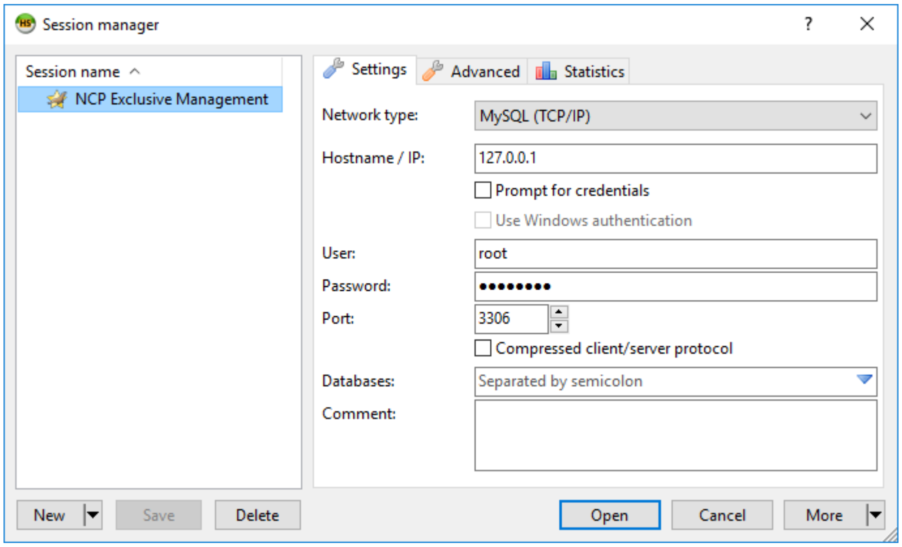
MariaDB 10.2 (x64) Setup

**Installing MariaDB 10.2 (x64)**

Please wait while the Setup Wizard installs MariaDB 10.2 (x64).

Status: Installing Windows Firewall configuration

The installation includes the HeidiSQL tool to create databases, users etc. Start HeidiSQL to prepare the MariaDB Server for the NCP Exclusive Remote Access Management Server.

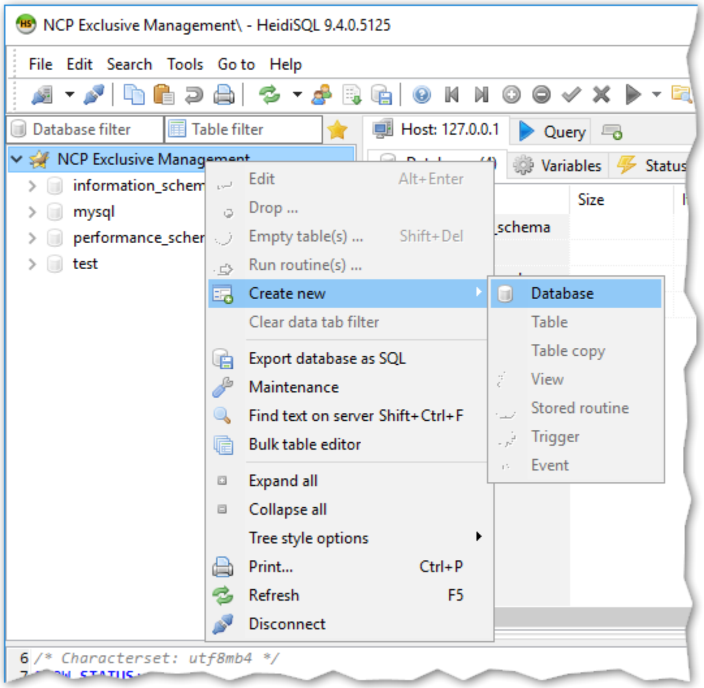


NCP Exclusive Management

Network type: MySQL (TCP/IP)
Hostname / IP: 127.0.0.1
□ Prompt for credentials
□ Use Windows authentication
User: root
Password: ••••••••
Port: 3306
□ Compressed client/server protocol
Databases: Separated by semicolon
Comment:

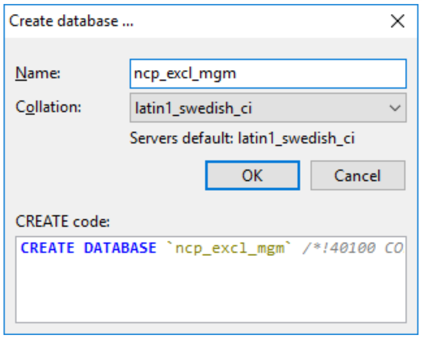
To connect to the database server (given it is installed on this system) enter the password for root user which had been defined during the MariaDB Server installation.

After logon create a new database as shown below:



```
6 /* Characterset: utf8mb4 */
```

Next Generation Network Access Technology



Create database ...

Name: ncp_excl_mgm

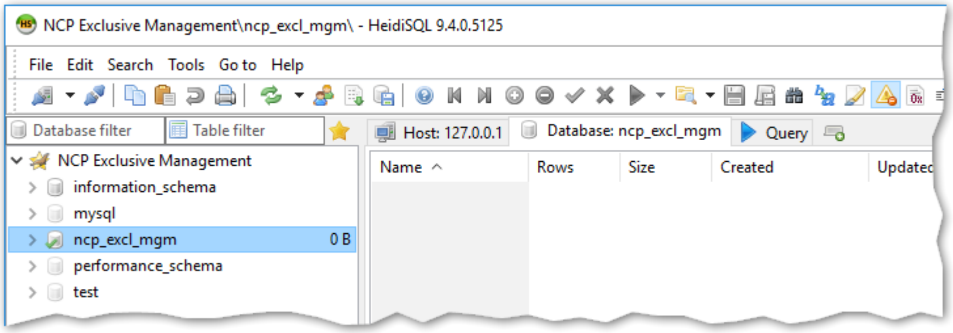
Collation: latin1_swedish_ci

Servers default: latin1_swedish_ci

CREATE code:

```
CREATE DATABASE `ncp_excl_mgm` /*!40100 CO
```

The new database should now be listed as shown in the screenshot below.

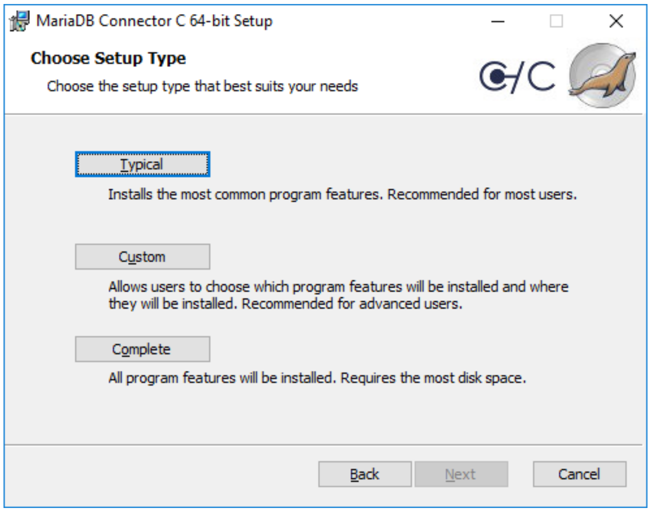


NCP Exclusive Management\ncp_excl_mgm\ - HeidiSQL 9.4.0.5125

Host: 127.0.0.1 · Database: ncp_excl_mgm

- NCP Exclusive Management
  - information_schema
  - mysql
  - ncp_excl_mgm 0 B
  - performance_schema
  - test

The tables for this yet empty database will be automatically created by the installation of the NCP Exclusive Remote Access Management Server.
To provide access to this database server the MariaDB Connector/C interface must be installed additionally. To do so execute the MSI package mariadb-connector-c-3.0.2-win64.msi and select the *Typical* setup without any special settings.



MariaDB Connector C 64-bit Setup

**Choose Setup Type**

Choose the setup type that best suits your needs

Typical
Installs the most common program features. Recommended for most users.

Custom
Allows users to choose which program features will be installed and where they will be installed. Recommended for advanced users.

Complete
All program features will be installed. Requires the most disk space.

This concludes the database setup and the NCP Exclusive Remote Access Management Server can be installed.

## A.1.2. Installing MariaDB on CentOS Linux

### Preparation of CentOS

You need to provide a basic installation of CentOS 7 with the necessary routing and access settings required for your specific environment. The installation of the NCP Exclusive Remote Access Management Server requires root privileges, so if you want to use an individual user, add the account to the sudoers.

### Providing a database with MariaDB

Use yum to install the packages for MariaDB as shown below.

```
sudo yum install mariadb-server
```

When all the packages have been installed, you need to start the database system and enable access.

```
sudo systemctl start mariadb
sudo systemctl enable mariadb
```

Create a database and a new user in MariaDB and all rights for the new user on the new database.

```
sudo mysql -u root
```

In the mysql client:

```
create database mydatabase;
create user 'mydbadmin' identified by 'mypassword';
grant all on mydatabase.* to 'mydbadmin'@'localhost' identified by 'mypassword' with grant option;
exit
```

This concludes the database setup and the NCP Exclusive Remote Access Management Server can be installed.

## A.2. Microsoft SQL Server 2014 Express Installation

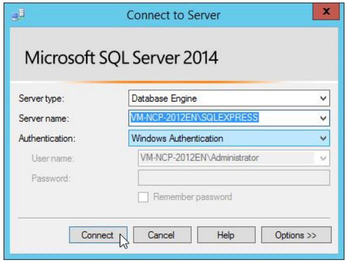
This example is based on the following setup package of MS SQL Server 2014 Express with Tools, product version 12.0.2000.8: SQLEXPRWT_x64_ENU.exe
The installation of the SQL Server requires .NET Framework 3.5 SP1 which cannot be installed if certain security updates have been applied. See the following link for further details:
https://support.microsoft.com/en-us/kb/3005628

### Installing the SQL Server

- SQL Server Installation Center - Installation
  Select "New SQL Server stand-alone installation or add feature to an existing installation"
- SQL Server 2014 Setup
  - License Terms
    Check "I Accept the license terms". and press "Next"
  - Microsoft Update
    Neglect the Microsoft Update part for now (to save time) and press "Next".
  - Feature Selection
    Use defaults and press "Next".
  - Instance Configuration
    Specify a decent "Instance ID" according to your likings then press "Next".
    (This example goes with the default "SQLEXPRESS")
  - Server Configuration
    Specify the Administrator account for "Account Name" and enter the according password in the "Password" column, then press "Next".
  - Database Engine Configuration
    Check "Mixed Mode (SQL Server authentication and Windows authentication)" and "Specify the password for the SQL Server system administrator (sa) account".
    Leave all other options at default settings. Then press "Next".
    (Installation progress will be shown for a while)

### Configuration of the SQL Server

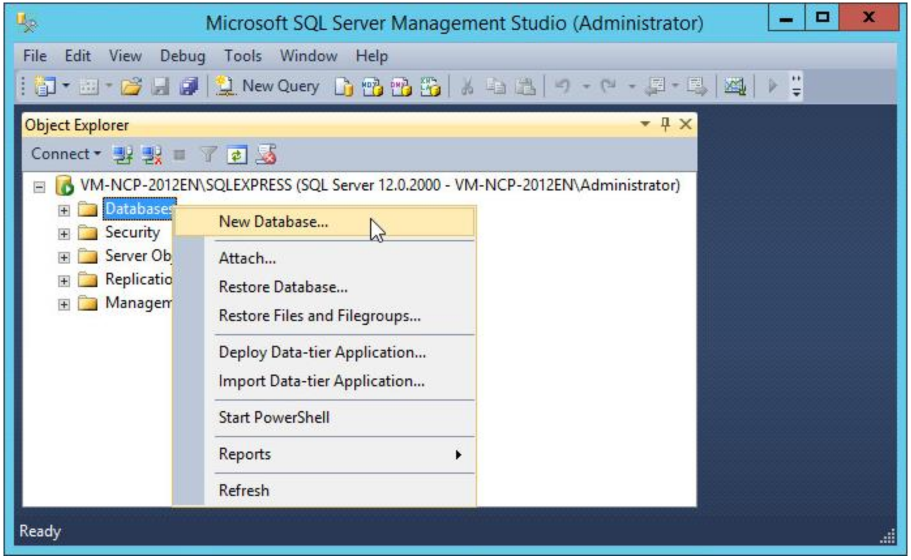
Start the "Microsoft SQL Server Management Studio" and connect using "Windows Authentication" which won't require any further credentials at this stage.



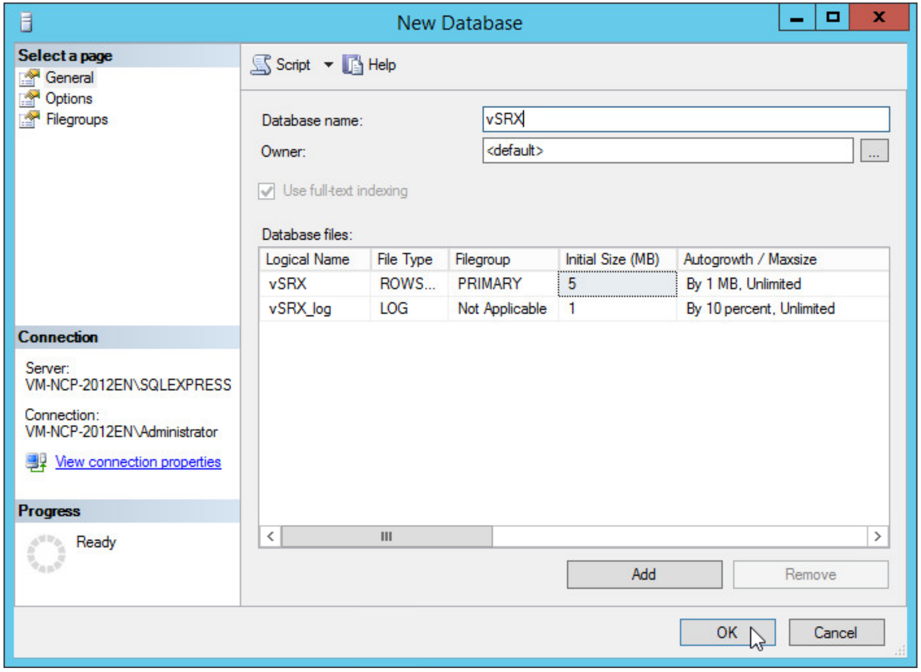
Server type: Database Engine
Server name: VM-NCP-2012EN\SQLEXPRESS
Authentication: Windows Authentication
User name: VM-NCP-2012EN\Administrator
Password:
☐ Remember password

## Create a new database for the Management Server

- Select “Databases” in your SQL Server and right click “Databases” and select “New Database...”


Microsoft SQL Server Management Studio (Administrator)
File Edit View Debug Tools Window Help
New Query
Object Explorer
Connect
VM-NCP-2012EN\SQLEXPRESS (SQL Server 12.0.2000 - VM-NCP-2012EN\Administrator)
Databases
Security
Server Ob
Replicatio
Managem
New Database...
Attach...
Restore Database...
Restore Files and Filegroups...
Deploy Data-tier Application...
Import Data-tier Application...
Start PowerShell
Reports
Refresh
Ready

- Enter the desired “Database name” then press “OK” to create the new and empty database



Database name: vSRX

Owner: <default>

☑ Use full-text indexing

Database files:

| Logical Name | File Type | Filegroup | Initial Size (MB) | Autogrowth / Maxsize |
|---|---|---|---|---|
| vSRX | ROWS... | PRIMARY | 5 | By 1 MB, Unlimited |
| vSRX_log | LOG | Not Applicable | 1 | By 10 percent, Unlimited |

Connection

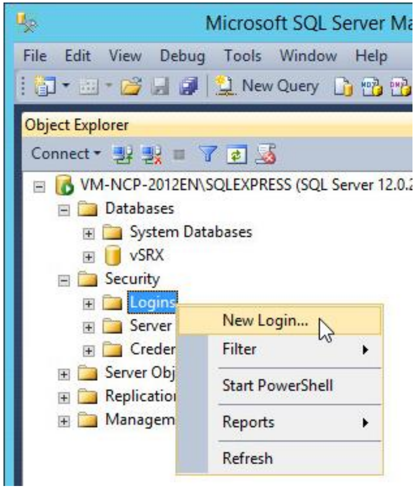
Server:
VM-NCP-2012EN\SQLEXPRESS

Connection:
VM-NCP-2012EN\Administrator

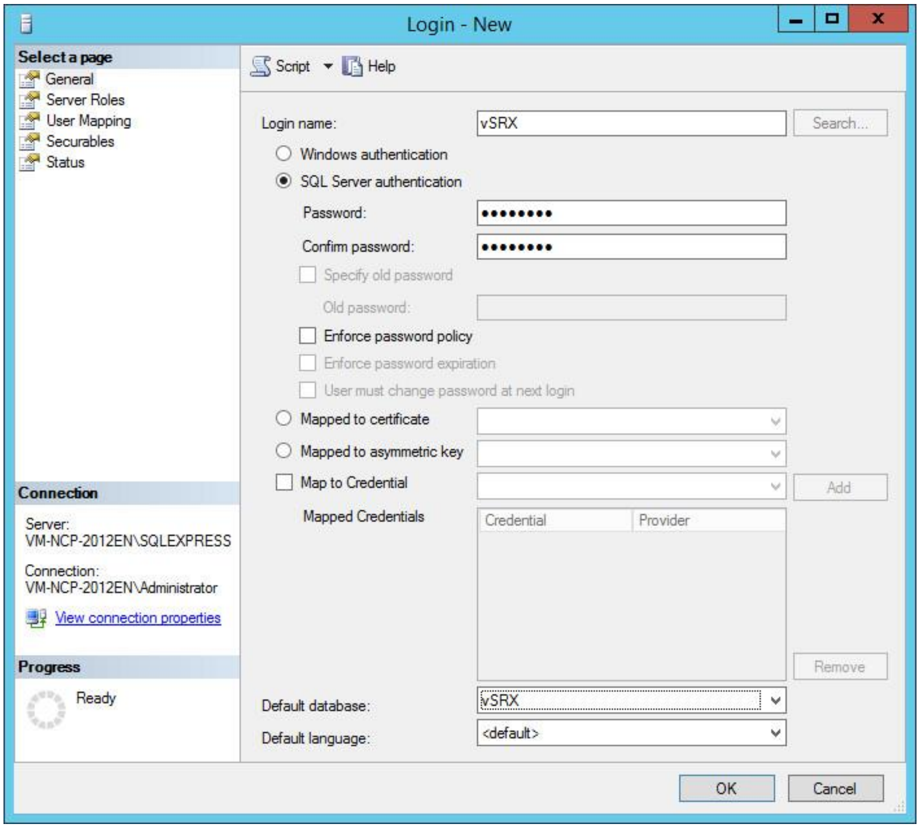
View connection properties

## Create a new user for the database

- Goto “Security” and select “Logins” then right click “Logins” and select “New Login...”



- “General”



Login name: vSRX

○ Windows authentication

● SQL Server authentication

Password: ••••••••

Confirm password: ••••••••

□ Specify old password

Old password:

□ Enforce password policy

□ Enforce password expiration

□ User must change password at next login

○ Mapped to certificate

○ Mapped to asymmetric key

□ Map to Credential

Mapped Credentials

Default database: vSRX

Default language: <default>

Connection

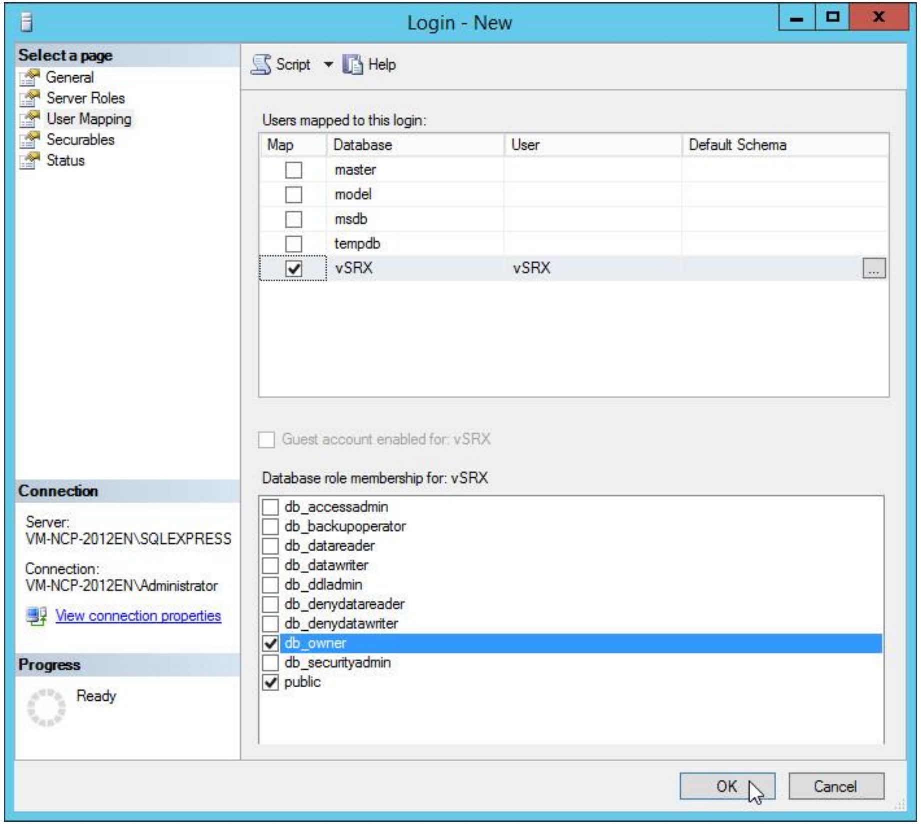
Server:
VM-NCP-2012EN\SQLEXPRESS

Connection:
VM-NCP-2012EN\Administrator

View connection properties

  - Enter the desired “Login name”
  - Select “SQL Server authentication”
  - Enter the “Password” and “Confirm password”
  - Uncheck “Enforce password policy” if desired
  - Select your previously created database in “Default database”

- “Server Roles”
  Stick with defaults
- “User Mapping”



Users mapped to this login:

| Map | Database | User | Default Schema |
|---|---|---|---|
| □ | master | | |
| □ | model | | |
| □ | msdb | | |
| □ | tempdb | | |
| ☑ | vSRX | vSRX | ... |

□ Guest account enabled for: vSRX

Database role membership for: vSRX

□ db_accessadmin
□ db_backupoperator
□ db_datareader
□ db_datawriter
□ db_ddladmin
□ db_denydatareader
□ db_denydatawriter
☑ db_owner
□ db_securityadmin
☑ public

Server:
VM-NCP-2012EN\SQLEXPRESS

Connection:
VM-NCP-2012EN\Administrator

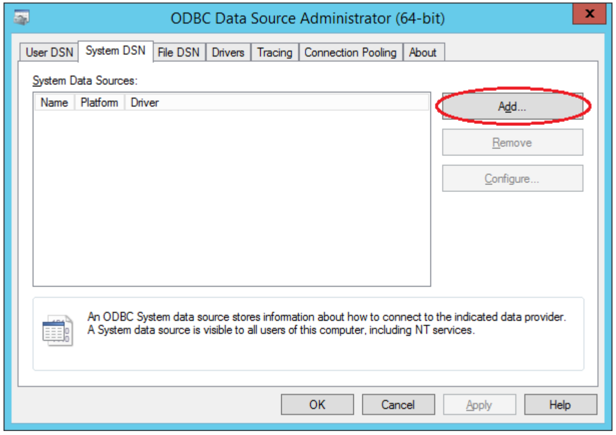
Ready

Check your previously created database in “Map” and check “db_owner” in “Database role membership” (here: “vSRX”)

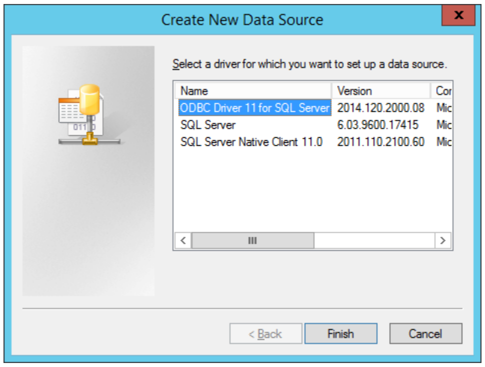
- “Securables”
  Stick with defaults
- “Status”
  Stick with defaults
- Confirm your entries with “OK”

### A.2.1. Creating an ODBC data source for the Management Server

Start “ODBC Data Sources (64-bit)” to create an ODBC connection. In the “ODBC Data Source Administrator (64-bit) move to the “System DSN” tab and click “Add…” for a new entry. In the following dialogue select “ODBC Driver 11 for SQL Server” and click “Finish”.



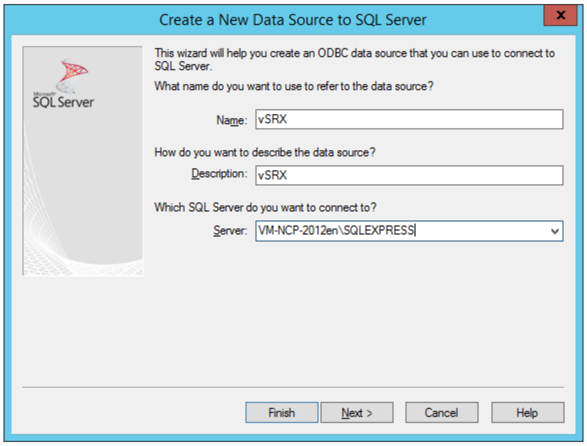
An ODBC System data source stores information about how to connect to the indicated data provider. A System data source is visible to all users of this computer, including NT services.



Select a driver for which you want to set up a data source.

| Name | Version | Cor |
|---|---|---|
| ODBC Driver 11 for SQL Server | 2014.120.2000.08 | Mic |
| SQL Server | 6.03.9600.17415 | Mic |
| SQL Server Native Client 11.0 | 2011.110.2100.60 | Mic |

In the window “Create a New Data Source to SQL Server” enter a meaningful “Name” (here: “vSRX”) and an optional “Description”. In “Server” enter the name of your SQL Server where the new database for your Management Server had been created previously, then click “Next”.
Enter “Login ID” and “Password” as assigned to the database user earlier under the option “With SQL Server authentication using a login ID and password entered by the user.” Then click “Next”.



This wizard will help you create an ODBC data source that you can use to connect to SQL Server.

What name do you want to use to refer to the data source?

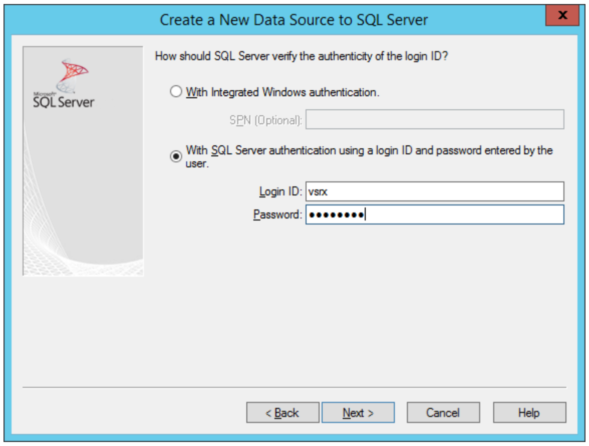
Name: vSRX

How do you want to describe the data source?

Description: vSRX

Which SQL Server do you want to connect to?

Server: VM-NCP-2012en\SQLEXPRESS



How should SQL Server verify the authenticity of the login ID?

○ With Integrated Windows authentication.

SPN (Optional):

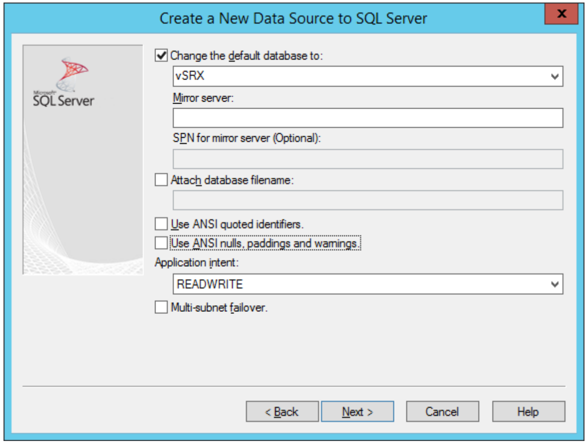
● With SQL Server authentication using a login ID and password entered by the user.

Login ID: vsrx

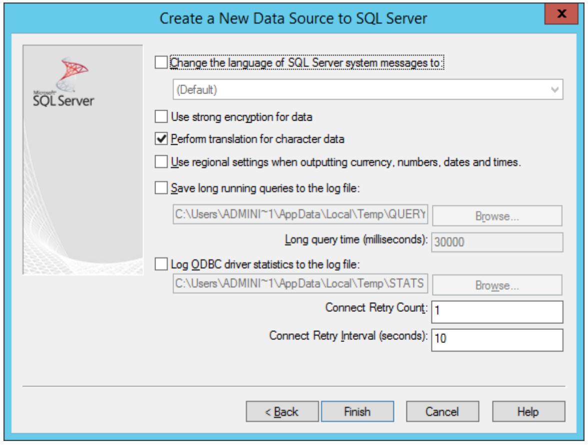
Password: ••••••••

Check the box “Change the default database to:” and enter/select the name of your Management Server database. Then uncheck both of the “ANSI” options and click “Next” to move to next page.

Stick with the given defaults and click “Finish” to complete the ODBC configuration.

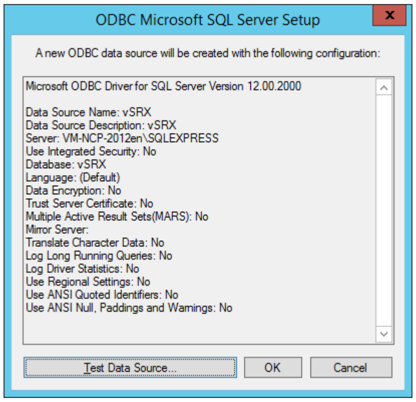

Create a New Data Source to SQL Server

☑ Change the default database to: vSRX
Mirror server:
SPN for mirror server (Optional):
□ Attach database filename:
□ Use ANSI quoted identifiers.
□ Use ANSI nulls, paddings and warnings.
Application intent: READWRITE
□ Multi-subnet failover.


Create a New Data Source to SQL Server

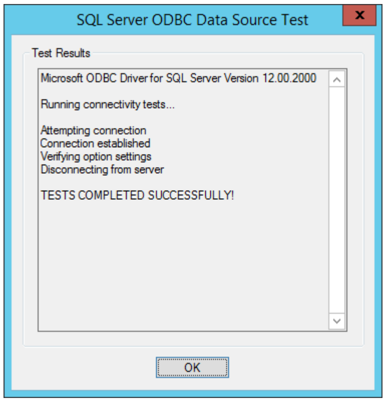
□ Change the language of SQL Server system messages to: (Default)
□ Use strong encryption for data
☑ Perform translation for character data
□ Use regional settings when outputting currency, numbers, dates and times.
□ Save long running queries to the log file: C:\Users\ADMINI~1\AppData\Local\Temp\QUERY
Long query time (milliseconds): 30000
□ Log ODBC driver statistics to the log file: C:\Users\ADMINI~1\AppData\Local\Temp\STATS
Connect Retry Count: 1
Connect Retry Interval (seconds): 10

A summary of the settings will be displayed and the settings can be verified by clicking “Test Data Source…”. This should result in “TESTS COMPLETED SUCCESSFULLY!” as shown in second screenshot below.


ODBC Microsoft SQL Server Setup

A new ODBC data source will be created with the following configuration:

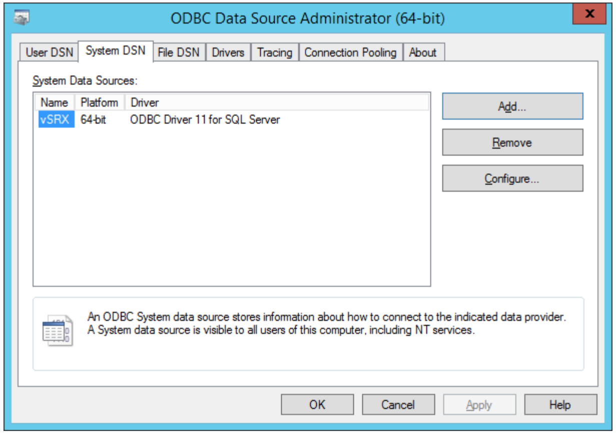
```
Microsoft ODBC Driver for SQL Server Version 12.00.2000

Data Source Name: vSRX
Data Source Description: vSRX
Server: VM-NCP-2012en\SQLEXPRESS
Use Integrated Security: No
Database: vSRX
Language: (Default)
Data Encryption: No
Trust Server Certificate: No
Multiple Active Result Sets(MARS): No
Mirror Server:
Translate Character Data: No
Log Long Running Queries: No
Log Driver Statistics: No
Use Regional Settings: No
Use ANSI Quoted Identifiers: No
Use ANSI Null, Paddings and Warnings: No
```


SQL Server ODBC Data Source Test

Test Results

```
Microsoft ODBC Driver for SQL Server Version 12.00.2000

Running connectivity tests...

Attempting connection
Connection established
Verifying option settings
Disconnecting from server

TESTS COMPLETED SUCCESSFULLY!
```

Database and ODBC source are now prepared so that the installation of NCP Secure Enterprise Management Server (Management Server) can be approached. Click “OK” to leave the ODBC data source configuration.


ODBC Data Source Administrator (64-bit)

System Data Sources:

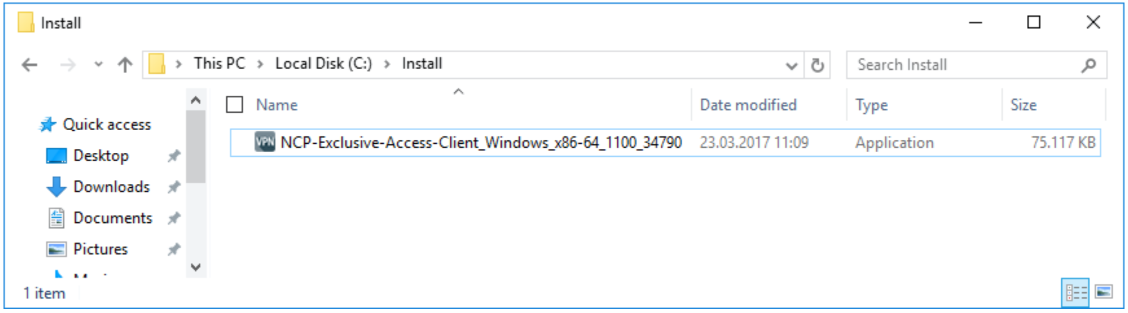
| Name | Platform | Driver |
|---|---|---|
| vSRX | 64-bit | ODBC Driver 11 for SQL Server |

An ODBC System data source stores information about how to connect to the indicated data provider. A System data source is visible to all users of this computer, including NT services.

# B Client Installation on Windows

This chapter describes how to install the NCP Exclusive Remote Access Client on Windows operating system. Please also consult the NCP web site for further information about the client software. https://www.ncp-e.com/en/exclusive-remote-access-solution/vpn-client

Open the folder with the installation package and execute it.



Install

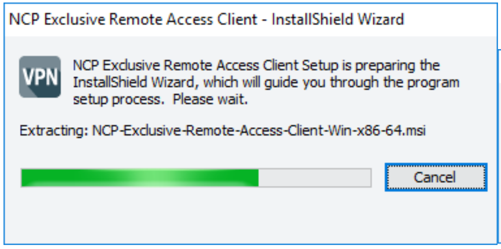
This PC › Local Disk (C:) › Install

Search Install

| Name | Date modified | Type | Size |
|---|---|---|---|
| NCP-Exclusive-Access-Client_Windows_x86-64_1100_34790 | 23.03.2017 11:09 | Application | 75.117 KB |

1 item

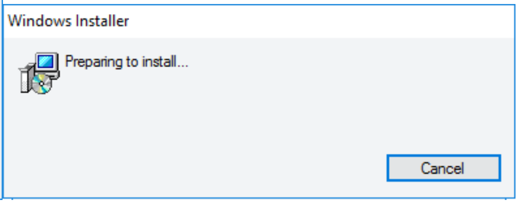
- After having selected the installation language the “Install Wizard” will guide through the setup



NCP Exclusive Remote Access Client - InstallShield Wizard

NCP Exclusive Remote Access Client Setup is preparing the InstallShield Wizard, which will guide you through the program setup process. Please wait.

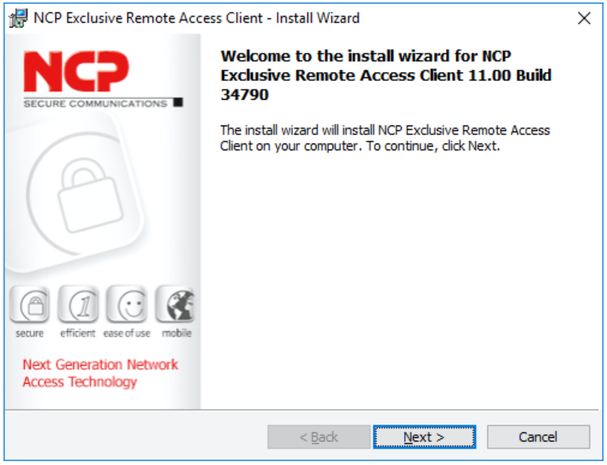
Extracting: NCP-Exclusive-Remote-Access-Client-Win-x86-64.msi



Windows Installer

Preparing to install...

- Accept the license agreement and click “Next”

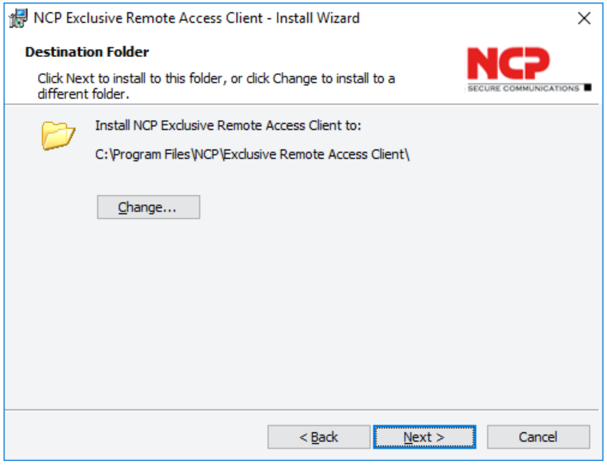


NCP Exclusive Remote Access Client - Install Wizard

**Welcome to the install wizard for NCP Exclusive Remote Access Client 11.00 Build 34790**

The install wizard will install NCP Exclusive Remote Access Client on your computer. To continue, click Next.

- Specify the “Destination Folder” and set “Advanced Options” according to your needs



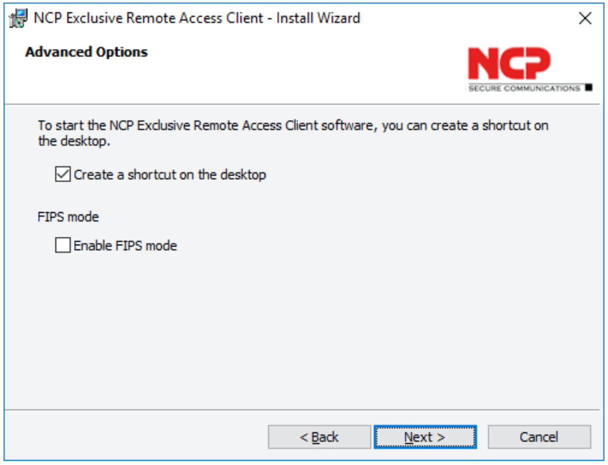
NCP Exclusive Remote Access Client - Install Wizard

**Destination Folder**

Click Next to install to this folder, or click Change to install to a different folder.

Install NCP Exclusive Remote Access Client to:

C:\Program Files\NCP\Exclusive Remote Access Client\



NCP Exclusive Remote Access Client - Install Wizard

**Advanced Options**

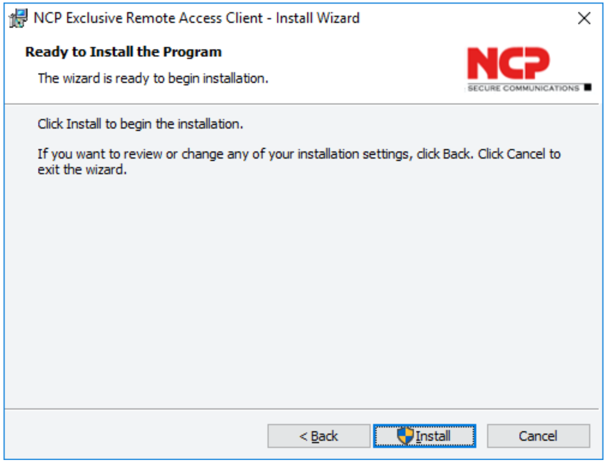
To start the NCP Exclusive Remote Access Client software, you can create a shortcut on the desktop.

☑ Create a shortcut on the desktop

FIPS mode

□ Enable FIPS mode

- The wizard is ready to start the installation. Click “Install” to begin



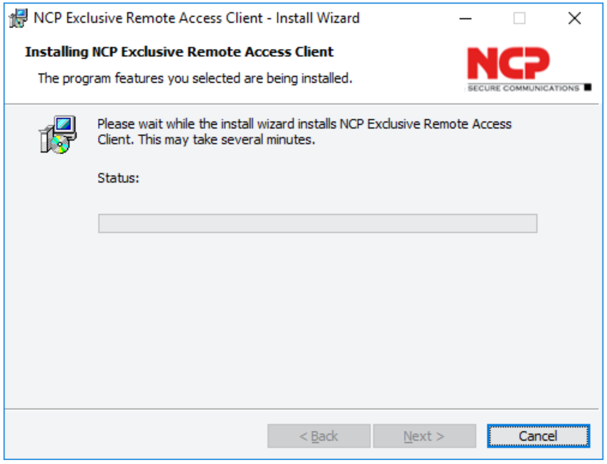
NCP Exclusive Remote Access Client - Install Wizard

**Ready to Install the Program**

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.



NCP Exclusive Remote Access Client - Install Wizard

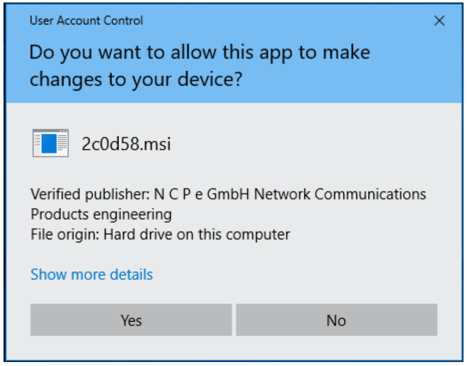
**Installing NCP Exclusive Remote Access Client**

The program features you selected are being installed.

Please wait while the install wizard installs NCP Exclusive Remote Access Client. This may take several minutes.

Status:

- If asked for permission by the UAC confirm with “Yes” to install the software



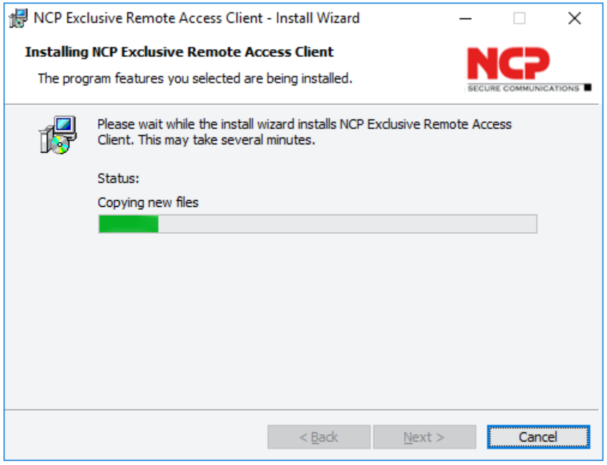
User Account Control

Do you want to allow this app to make changes to your device?

2c0d58.msi

Verified publisher: N C P e GmbH Network Communications Products engineering
File origin: Hard drive on this computer

- This will take a while as setup will go through various stages...
  When setup has completed click “Finish”



NCP Exclusive Remote Access Client - Install Wizard

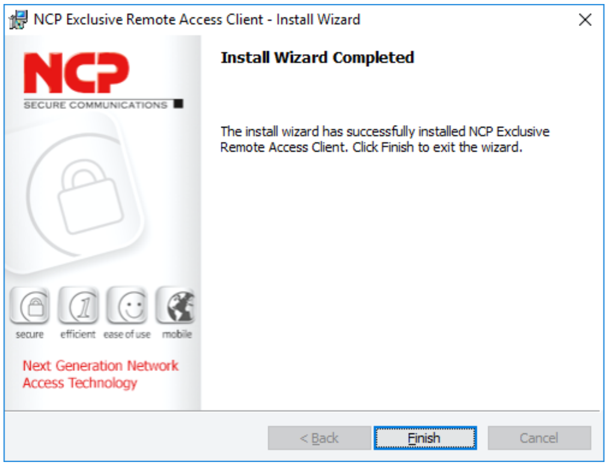
**Installing NCP Exclusive Remote Access Client**

The program features you selected are being installed.

Please wait while the install wizard installs NCP Exclusive Remote Access Client. This may take several minutes.

Status:

Copying new files



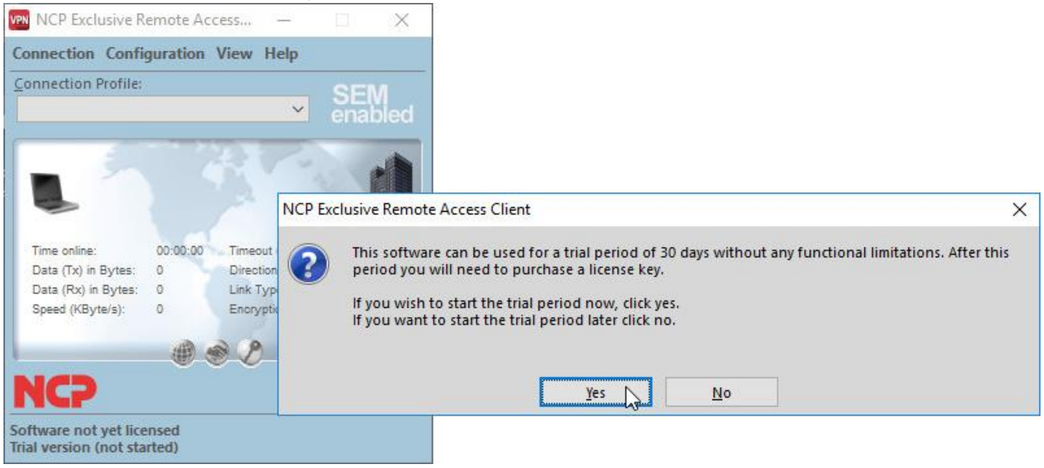
NCP Exclusive Remote Access Client - Install Wizard

**Install Wizard Completed**

The install wizard has successfully installed NCP Exclusive Remote Access Client. Click Finish to exit the wizard.

A restart of the system is required after the installation.

After the reboot the client starts automatically and will ask you to start the 30-day trial period.
Click “Yes” to start working with the client.



Software not yet licensed
Trial version (not started)

NCP Exclusive Remote Access Client

This software can be used for a trial period of 30 days without any functional limitations. After this period you will need to purchase a license key.

If you wish to start the trial period now, click yes.
If you want to start the trial period later click no.

# C SRX configuration sample

The configuration listed below is a very basic one, simplified and exclusively focused on the VPN connections used in this scenario. Please visit the NCP website for further configuration guides.
(https://www.ncp-e.com/en/exclusive-remote-access-solution/documents-faq/)

## C.1. General configuration

```
set interfaces ge-0/0/0 unit 0 family inet address 10.10.10.249/24
set interfaces ge-0/0/2 unit 0 family inet address 192.168.100.249/24
set interfaces st-0 unit 0 family inet address 172.16.119.254/24
set interfaces st-0 unit 1 family inet address 172.16.119.253/24

set security zones security-zone trust interfaces ge-0/0/0
set security zones security-zone trust interfaces ge-0/0/2
set security zones security-zone trust interfaces ge-0/0/0 host-inbound-traffic system-services all
set security zones security-zone trust interfaces ge-0/0/2 host-inbound-traffic system-services all
set security zones security-zone trust interfaces ge-0/0/0 host-inbound-traffic protocols all
set security zones security-zone trust interfaces ge-0/0/2 host-inbound-traffic protocols all

set security policies default-policy permit-all
set security zones security-zone trust interfaces st0.0 host-inbound-traffic system-services all
set security zones security-zone trust interfaces st0.0 host-inbound-traffic protocols all

set security pki ca-profile NCP_CA ca-identity ncp.juniper.net
set security pki ca-profile NCP_CA revocation-check disable
set security pki ca-profile NCP_VMDEMO_CA ca-identity vmncp.demo
set security pki ca-profile NCP_VMDEMO_CA revocation-check disable

set security ike proposal IKEv2_EAP_PROP authentication-method rsa-signatures
set security ike proposal IKEv2_EAP_PROP dh-group group19
set security ike proposal IKEv2_EAP_PROP encryption-algorithm aes-256-gcm
set security ike proposal IKEv2_EAP_PROP lifetime-seconds 10000

set security ike policy IKEv2_MD5_POL proposals IKEv2_EAP_PROP
set security ike policy IKEv2_MD5_POL certificate local-certificate NCP_CA
set security ike policy IKEv2_TLS_POL proposals IKEv2_EAP_PROP
set security ike policy IKEv2_TLS_POL certificate local-certificate NCP_VMDEMO_CA

set security ike gateway IKEv2_MD5_GW ike-policy IKEv2_MD5_POL
set security ike gateway IKEv2_MD5_GW dynamic hostname eap.md5
set security ike gateway IKEv2_MD5_GW dynamic user-at-hostname @eap.md5
set security ike gateway IKEv2_MD5_GW dynamic connections-limit 100
set security ike gateway IKEv2_MD5_GW dynamic ike-user-type group-ike-id
set security ike gateway IKEv2_MD5_GW local-identity distinguished-name
set security ike gateway IKEv2_MD5_GW external-interface ge-0/0/2.0
set security ike gateway IKEv2_MD5_GW aaa access-profile IKEv2_EAP_RAD
set security ike gateway IKEv2_MD5_GW version v2-only

set security ike gateway IKEv2_TLS_GW ike-policy IKEv2_TLS_POL
set security ike gateway IKEv2_TLS_GW dynamic hostname eap.tls
set security ike gateway IKEv2_TLS_GW dynamic user-at-hostname @eap.tls
set security ike gateway IKEv2_TLS_GW dynamic connections-limit 100
set security ike gateway IKEv2_TLS_GW dynamic ike-user-type group-ike-id
set security ike gateway IKEv2_TLS_GW local-identity distinguished-name
set security ike gateway IKEv2_TLS_GW external-interface ge-0/0/2.0
set security ike gateway IKEv2_TLS_GW aaa access-profile IKEv2_EAP_RAD
set security ike gateway IKEv2_TLS_GW version v2-only

set security ipsec proposal IPSEC_PROP protocol esp
set security ipsec proposal IPSEC_PROP encryption-algorithm aes-256-gcm
set security ipsec proposal IPSEC_PROP lifetime-seconds 3600
set security ipsec policy IPSEC_POL perfect-forward-secrecy keys group19
set security ipsec policy IPSEC_POL proposals IPSEC_PROP

set security ipsec vpn IKEv2_MD5_VPN bind-interface st0.0
set security ipsec vpn IKEv2_MD5_VPN ike gateway IKEv2_MD5_GW
set security ipsec vpn IKEv2_MD5_VPN ike ipsec-policy IPSEC_POL
set security ipsec vpn IKEv2_MD5_VPN traffic-selector TS1 local-ip 0.0.0.0/0
set security ipsec vpn IKEv2_MD5_VPN traffic-selector TS1 remote-ip 0.0.0.0/0

set security ipsec vpn IKEv2_TLS_VPN bind-interface st0.0
set security ipsec vpn IKEv2_TLS_VPN ike gateway IKEv2_TLS_GW
set security ipsec vpn IKEv2_TLS_VPN ike ipsec-policy IPSEC_POL
set security ipsec vpn IKEv2_TLS_VPN traffic-selector TS1 local-ip 0.0.0.0/0
set security ipsec vpn IKEv2_TLS_VPN traffic-selector TS1 remote-ip 0.0.0.0/0

set access profile IKEv2_EAP_RAD authentication-order radius
set access profile IKEv2_EAP_RAD radius-server 10.10.10.250 port 1812
set access profile IKEv2_EAP_RAD address-assignment pool IKEv2_EAP_POOL
set access profile IKEv2_EAP_RAD radius-server 10.10.10.250 secret "mysecret"

set access address-assignment pool IKEv2_EAP_POOL family inet network 172.16.119.0/24
set access address-assignment pool IKEv2_EAP_POOL family inet xauth-attributes primary-dns 172.16.119.254/32
set access address-assignment pool IKEv2_EAP_POOL family inet xauth-attributes primary-wins 172.16.119.254/32

set security ike gateway IKEv2_MD5_GW tcp-encap-profile NCP
set security tcp-encap profile NCP
```

## C.2. Certificate upload

```
request security pki local-certificate load filename vsrx.pem key vsrx.key certificate-id NCP_VMDEMO_CA
request security pki ca-certificate load ca-profile NCP_VMDEMO_CA filename vm-ncp2008en.crt
```