

Configuration Guide

NCP Exclusive Remote Access Solution for Juniper SRX Gateways



Introduction

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

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

1. Configuration of NCP RADIUS Server

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

Configure SRX

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

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

CLI Quick Configuration

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

Step-by-step Procedure

1) Define access profile in gateway

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

2) Create access profile

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

3) Commit changes

```
commit
```

Next Generation Network Access Technology

Configuration Guide

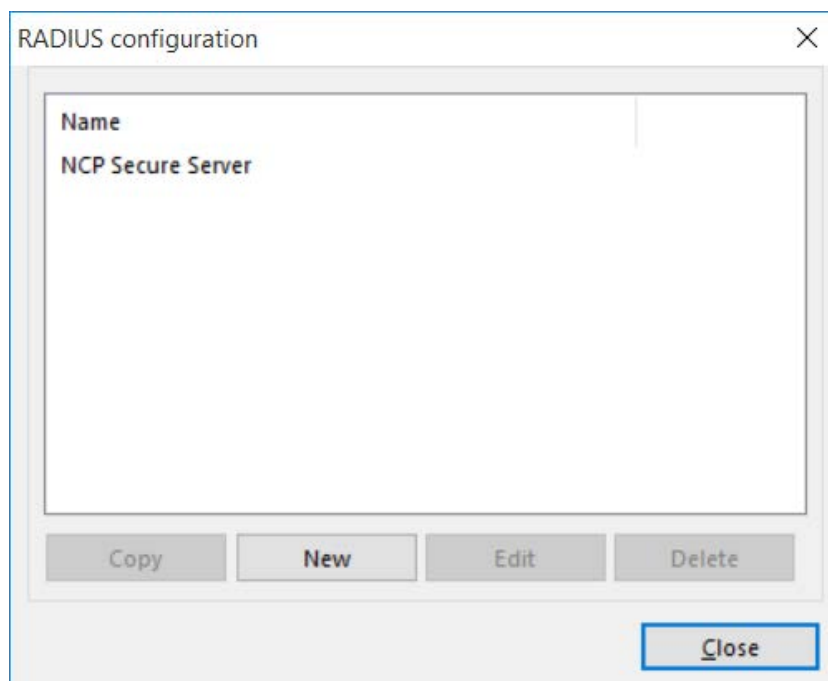
NCP Exclusive Remote Access Solution for Juniper SRX Gateways



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

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

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



Configuration Guide

NCP Exclusive Remote Access Solution for Juniper SRX Gateways



RADIUS configuration

Configuration Info

Name: SRX

Parameter	Value	Attribute	Vendor ID	Type	User Type
-----------	-------	-----------	-----------	------	-----------

Edit Add Delete

OK Cancel

No Information needs to be added. Click "OK"

RADIUS configuration

Name
NCP Secure Server
SRX

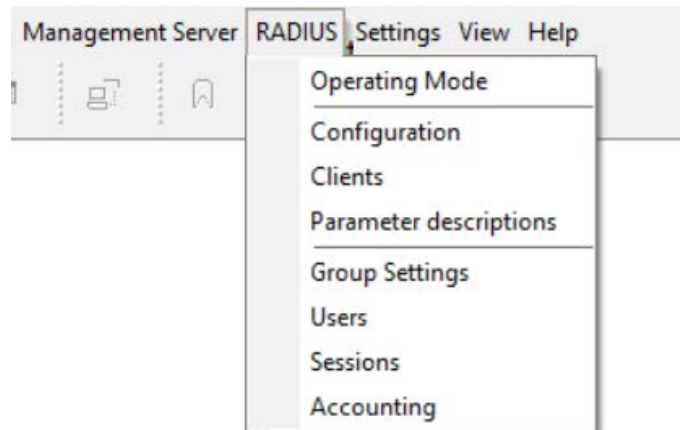
Copy New Edit Delete

Close

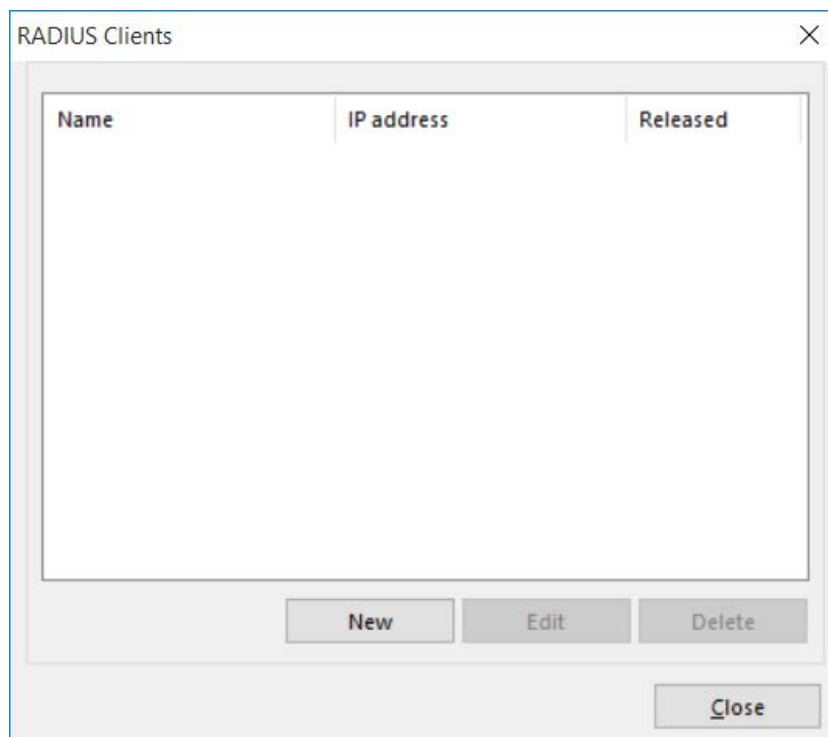
Configuration Guide

NCP Exclusive Remote Access Solution for Juniper SRX Gateways

Go to "RADIUS" – "Clients"



Create a new RADIUS Client



For EAP-MD5 click "Allow EAP-MD5"

Configuration Guide

NCP Exclusive Remote Access Solution for Juniper SRX Gateways



RADIUS Client

RADIUS Client Info

Name : SRX

IP address : 10.20.44.200

Shared secret : ●●●●●●●●

Retype shared secret : ●●●●●●●●

RADIUS Dictionary : IETF Attributes

RADIUS configuration : SRX

Enabled

Allow PAP Allow MS-CHAP V1

Allow CHAP Allow MS-CHAP V2

Allow EAP-MD5

Allow EAP-TLS

OK Cancel

Configuration Guide

NCP Exclusive Remote Access Solution for Juniper SRX Gateways



For EAP-TLS click "Allow EAP-TLS"

The image shows a 'RADIUS Client' configuration dialog box. It has a title bar with a close button (X) and two tabs: 'RADIUS Client' and 'Info'. The 'RADIUS Client' tab is active. The form contains the following fields and options:

- Name: SRX
- IP address: 10.20.44.200
- Shared secret: [Redacted]
- Retype shared secret: [Redacted]
- RADIUS Dictionary: IETF Attributes (dropdown)
- RADIUS configuration: SRX (dropdown)
- Enabled:
- Allow PAP:
- Allow CHAP:
- Allow EAP-MD5:
- Allow EAP-TLS: (This checkbox is circled in red in the original image)
- Allow MS-CHAP V1:
- Allow MS-CHAP V2:

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Configuration Guide

NCP Exclusive Remote Access Solution for Juniper SRX Gateways



IKEv1

RADIUS Client

RADIUS Client Info

Name : SRX

IP address : 10.20.44.200

Shared secret : ●●●●●●●●

Retype shared secret : ●●●●●●●●

RADIUS Dictionary : IETF Attributes

RADIUS configuration : SRX

Enabled

Allow PAP Allow MS-CHAP V1

Allow CHAP Allow MS-CHAP V2

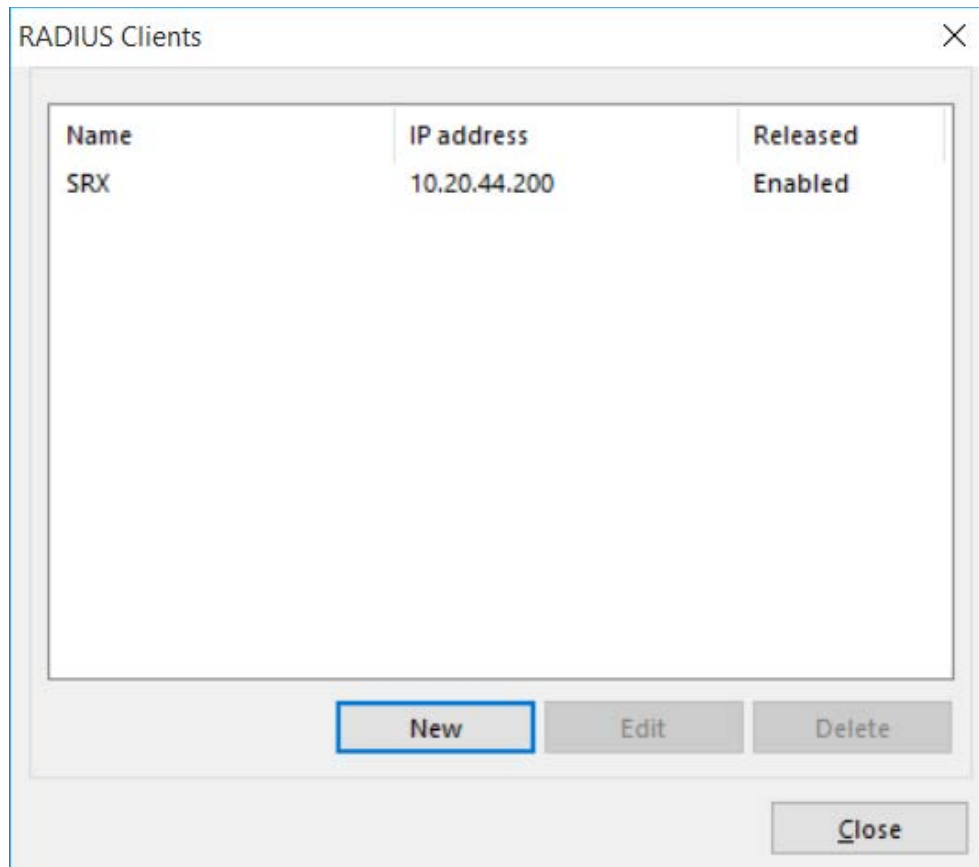
Allow EAP-MD5

Allow EAP-TLS

OK Cancel

Configuration Guide

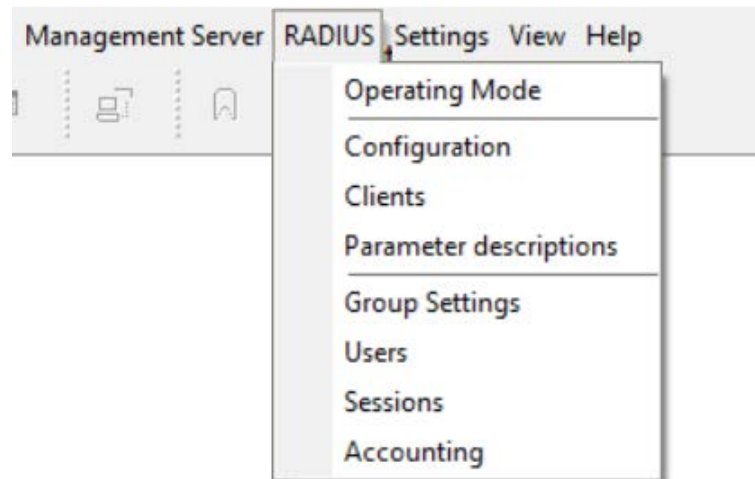
NCP Exclusive Remote Access Solution for Juniper SRX Gateways



Configuration Guide

NCP Exclusive Remote Access Solution for Juniper SRX Gateways

Go to "RADIUS" – "Group Settings"

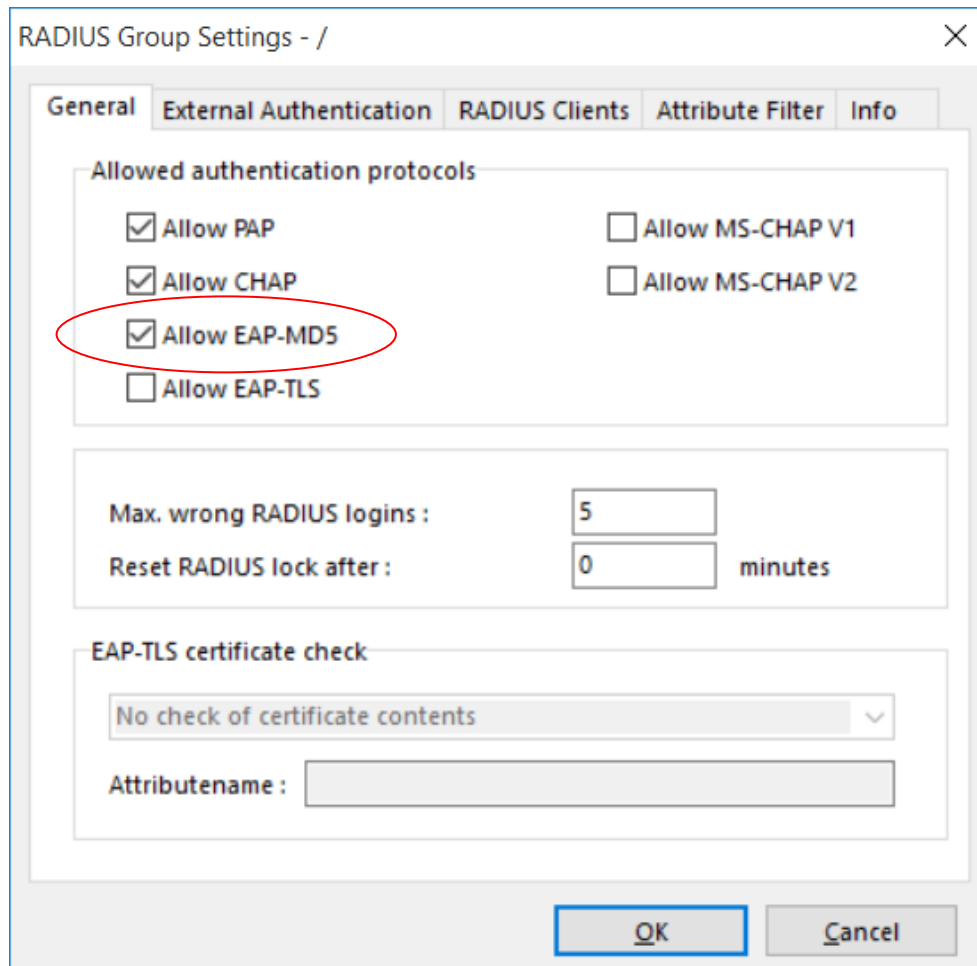


Configuration Guide

NCP Exclusive Remote Access Solution for Juniper SRX Gateways



For EAP-MD5 click "Allow EAP-MD5"



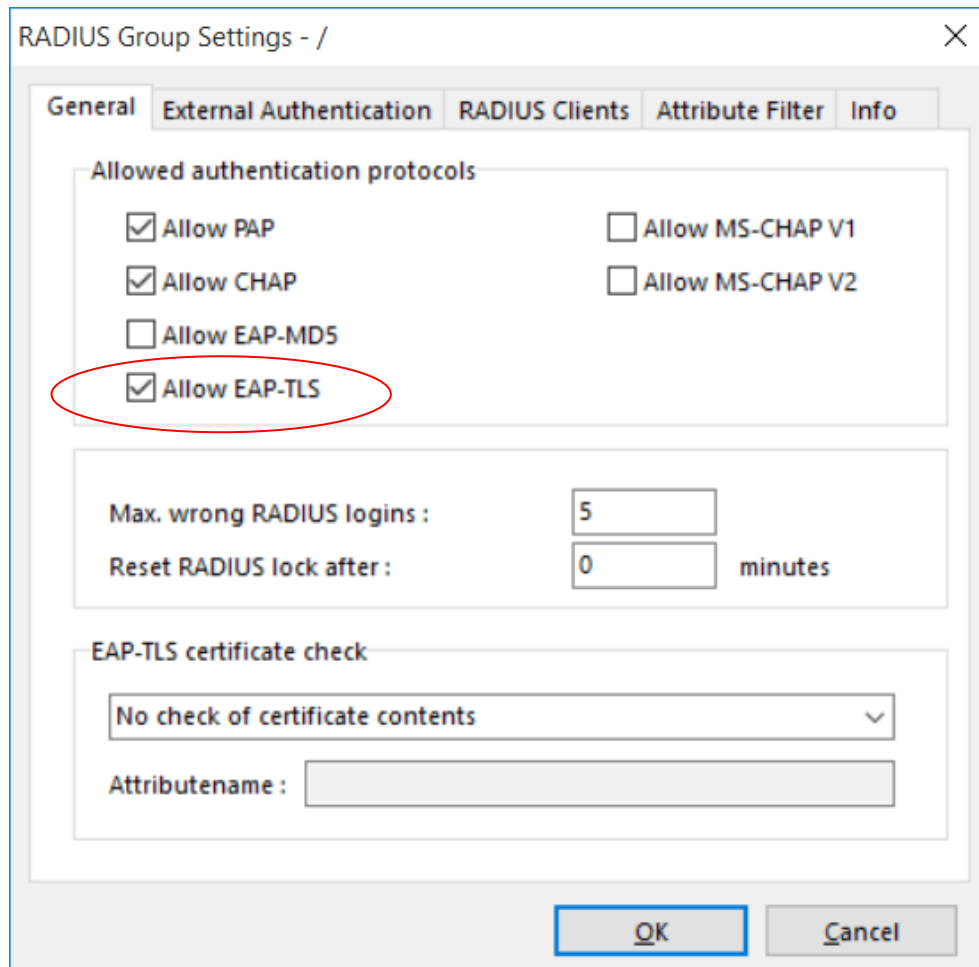
The screenshot shows a dialog box titled "RADIUS Group Settings - /". It has several tabs: "General", "External Authentication", "RADIUS Clients", "Attribute Filter", and "Info". The "General" tab is selected. Under the heading "Allowed authentication protocols", there are five checkboxes: "Allow PAP" (checked), "Allow CHAP" (checked), "Allow EAP-MD5" (checked and circled in red), "Allow EAP-TLS" (unchecked), "Allow MS-CHAP V1" (unchecked), and "Allow MS-CHAP V2" (unchecked). Below this section, there are two input fields: "Max. wrong RADIUS logins:" with a value of "5" and "Reset RADIUS lock after:" with a value of "0" and the unit "minutes". Under the heading "EAP-TLS certificate check", there is a dropdown menu set to "No check of certificate contents" and an empty "Attributename:" field. At the bottom right, there are "OK" and "Cancel" buttons.

Configuration Guide

NCP Exclusive Remote Access Solution for Juniper SRX Gateways



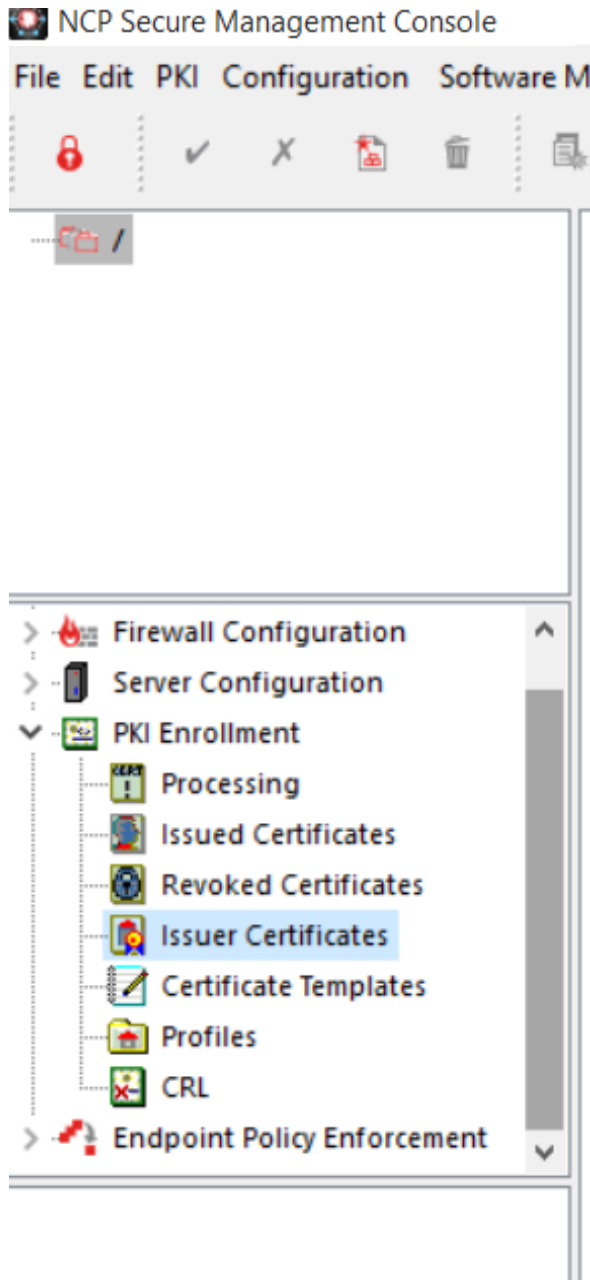
For EAP-MD5 click "Allow EAP-MD5"



The screenshot shows a dialog box titled "RADIUS Group Settings - /" with a close button (X) in the top right corner. The dialog has five tabs: "General", "External Authentication", "RADIUS Clients", "Attribute Filter", and "Info". The "General" tab is selected. Under the heading "Allowed authentication protocols", there are four checkboxes: "Allow PAP" (checked), "Allow CHAP" (checked), "Allow EAP-MD5" (unchecked), and "Allow EAP-TLS" (checked). The "Allow EAP-TLS" checkbox is circled in red. Below this section, there are two input fields: "Max. wrong RADIUS logins :" with a value of "5" and "Reset RADIUS lock after :" with a value of "0" and the unit "minutes". Under the heading "EAP-TLS certificate check", there is a dropdown menu set to "No check of certificate contents" and an empty "Attributename :" field. At the bottom of the dialog are "OK" and "Cancel" buttons.

Configuration Guide

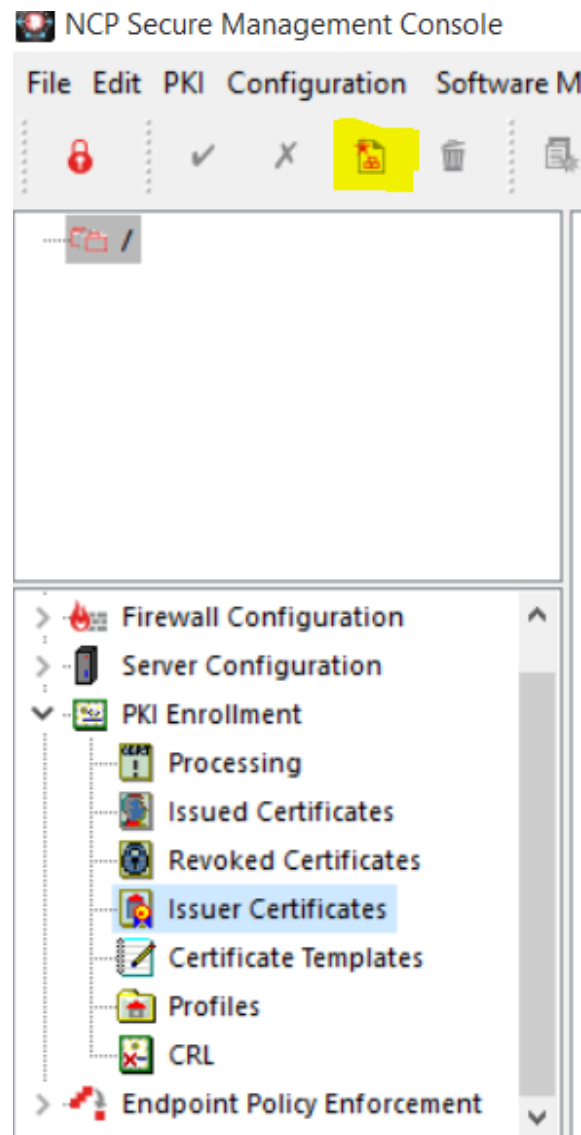
NCP Exclusive Remote Access Solution for Juniper SRX Gateways



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

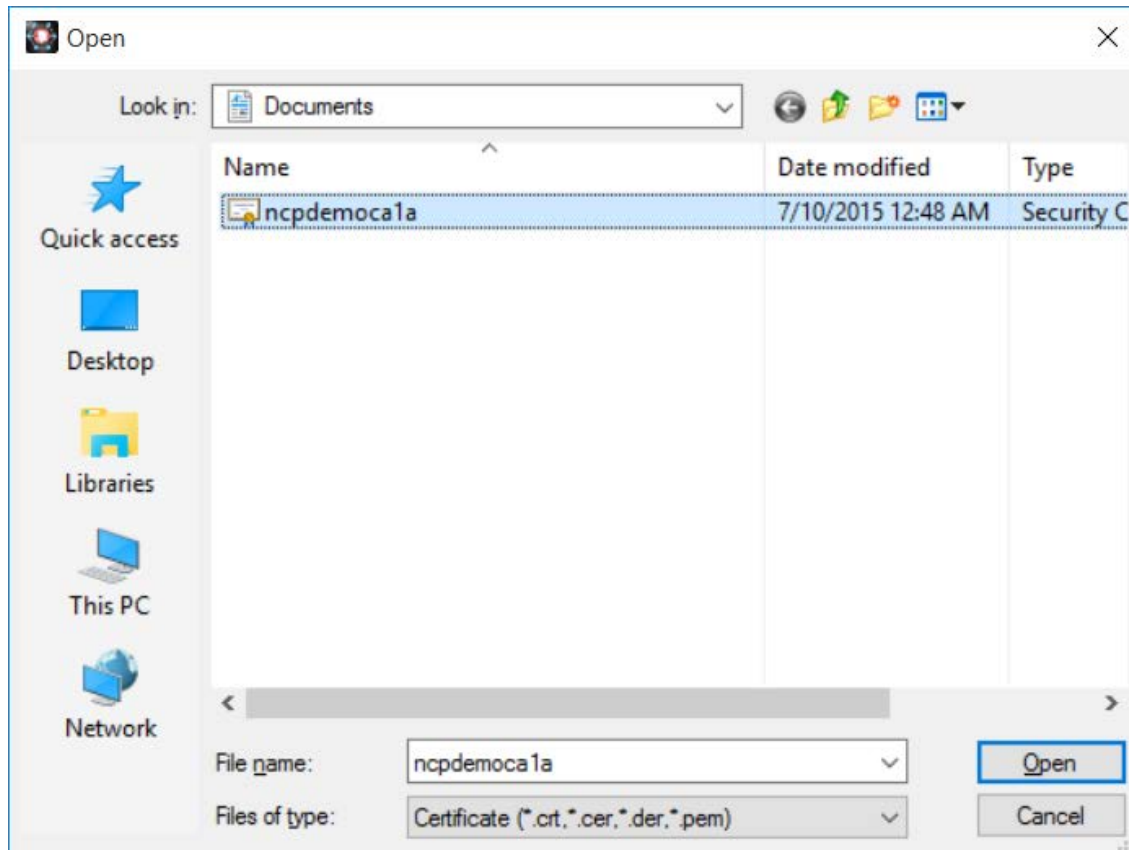
Go to “PKI Enrollment” – “Issuer Certificates”

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



Configuration Guide

NCP Exclusive Remote Access Solution for Juniper SRX Gateways



Configuration Guide

NCP Exclusive Remote Access Solution for Juniper SRX Gateways



The screenshot displays the NCP Secure Management Console interface. The main window is titled "Issuer Certificates" and has tabs for "General", "Details", and "Info". The "General" tab is active, showing two text boxes for "User" and "Issuer" containing the following text:

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

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

Below these boxes, the following fields are visible:

Serial number : 00
Valid from : Dec. 9.2001 11:34:25 GMT to : Apr.26.2029 11:34:25 GMT
Fingerprint (MD5): 91:4F:1B:E3:A0:B5:83:96:AB:90:E0:AB:04:F5:39:3D

The left sidebar shows a navigation tree with the following items:

- Firewall Configuration
- Server Configuration
- PKI Enrollment
 - Processing
 - Issued Certificates
 - Revoked Certificates
 - Issuer Certificates
 - Certificate Templates
 - Profiles
 - CRL
- Endpoint Policy Enforcement

The status bar at the bottom left indicates "NCP Demo CA 1".

Configuration Guide

NCP Exclusive Remote Access Solution for Juniper SRX Gateways



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

Open the file ncprsu.conf

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

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

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

A screenshot of a text editor window titled 'ncprsu'. The window shows the configuration file 'ncprsu.conf' with various settings. The settings are as follows:

```
File Edit Format View Help
# only used in config of Backup Server
PrimaryIpAddr =127.0.0.1

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

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

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

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

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

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

Next Generation Network Access Technology

Configuration Guide

NCP Exclusive Remote Access Solution for Juniper SRX Gateways



Restart all NCP service or reboot the server.

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

