NCP Secure Enterprise VPN Server (Linux)
Release Notes

Service Release:	**11.01 r38204**
Date:	**December 2017**

Prerequisites

Linux Distributions:

The following Linux distributions are supported with this release:

- CentOS 7.4
- Debian GNU/Linux 9.2.1
- SUSE Linux Enterprise Server 12 SP3
- Ubuntu Server 16.04.3 LTS

Update Prerequisites

Please read the instructions for updates of previous versions carefully!
(See NCP_RN_SES_10_and_HAS_10_Update_and_License_de.PDF)

The following versions are required for using other NCP components

- Secure Enterprise Management Server Version 4.05 or later
- Management Console Version 4.05 or later
- Management Plug-in Server Configuration: Version 11.00 or later
- Secure Enterprise HA Server Version 10.01 or later

Note: From version 10.0, a license key for the same version of Secure Enterprise VPN Server is required to use this product.

1. New Features and Enhancements

None

2. Improvements / Problems Resolved

The VRRP script can now be executed on CentOS 7.4.

Installation on Debian 9.0 or higher now supports scenarios where a password was not assigned to the root user during the operating system installation.

Next Generation Network Access Technology

After updating to version 11.0 or reinstalling this version, the system had to be rebooted before the server could be started. This issue has now been resolved. SNMP queries are also possible after restarting the SNMP service.

When downloading the CRL list, the ncpsrvmgm service could crash. This issue has now been resolved.

SEM requests for software updates over LAN are no longer forwarded.

The RADIUS attribute "NCPS-PCCertCN" = "*" enforces the use of a hardware certificate.

Redirection of "VPN IP addresses not bound to the Secure Server Adapter" has been fixed.

The server certificate is selected as configured, either "automatically" by the server or "manually".

The server changed the order in the configuration file ncpwsupd.conf at startup. This issue has been resolved.

When data is no longer sent over the VPN connection, PathFinder sessions no longer remain open, but are automatically closed.

The Secure Enterprise Server now also supports PathFinder 2 and SSL VPN when configuring ECC certificates.

The following message appeared sporadically in the configuration web page of the SES caused by an error: "Changes require restarting the NCP Secure Enterprise Server!"

With the "ARRE" option configured the server may have refused VPN connections. This issue has now been resolved.

If filters were set for the VPN data, packets were still forwarded very sporadically. This issue has been resolved.

3. Known Issues

None

Next Generation Network Access Technology

Major Release: **11.0 r36600**
Date: **August 2017**

Prerequisites

Linux Distributions:

The following Linux distributions are supported with this release:

- CentOS 7.3
- Debian GNU/Linux 8.7
- SUSE Linux Enterprise Server 12 SP2
- Ubuntu Server 16.04.2 LTS

Update Prerequisites

Please read the instructions for updates of previous versions carefully!
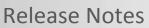(See NCP_RN_SES_10_and_HAS_10_Update_and_License_de.PDF)

Prerequisites for Configuration via Secure Enterprise Management (SEM)

- Secure Enterprise Management Server: Version 4.05 or later
- Management Plugin - Server Configuration: Version 11.00 or later

Prerequisites for High Availability

If the Secure Enterprise VPN Server 11.00 is used in a high availability network, ensure that the High Availability Server (HA Server) is version 10.01 or later.

Note: From version 10.0, a license key for the same version of Secure Enterprise VPN Server is required to use this product.

Next Generation Network Access Technology

1. New Features and Enhancements

None

2. Improvements / Problems Resolved

Removed Domain Groups after update to version 11.0

If the option „Enable selected CA Certificates only" is set within the Domain Group configuration, configured Domain Groups, including the Default Domain Group, will be removed while updating the NCP Secure Enterprise VPN Server to version 11.0. This issue has now been resolved.

3. Known Issues

None

Next Generation Network Access Technology

Americas: NCP engineering, Inc. · 1045 Linda Vista Ave. Unit-A · Mountain View, CA 94043 · Phone: +1 (650) 316-6273 · www.ncp-e.com   **4 / 9**
Others: NCP engineering GmbH · Dombuehler Str. 2 · 90449 Nuremberg · Germany · Fon +49 911 9968-0 · Fax +49 911 9968-299

Major Release:	**11.00 r36322**
Date:	**July 2017**

Prerequisites

Linux Distributions:

The following Linux distributions are supported with this release:

- CentOS 7.3
- Debian GNU/Linux 8.7
- SUSE Linux Enterprise Server 12 SP2
- Ubuntu Server 16.04.2 LTS

Update Prerequisites

Please read the instructions for updates of previous versions carefully!
(See NCP_RN_SES_10_and_HAS_10_Update_and_License_de.PDF)

Prerequisites for Configuration via Secure Enterprise Management (SEM)

- Secure Enterprise Management Server:　　Version 4.05 or later
- Management Plugin - Server Configuration:Version 11.00 or later

Prerequisites for High Availability

If the Secure Enterprise VPN Server 11.00 is used in a high availability network, ensure that the High Availability Server (HA Server) is version 10.01 or later.

Note: From version 10.0, a license key for the same version of Secure Enterprise VPN Server is required to use this product.

Next Generation Network Access Technology

4. New Features and Enhancements

None

5. Improvements / Problems Resolved

IKEv2 Connection with Device and User Certificate

If a VPN connection using IKEv2 required authentication of the device via device certificate and the user authentication via user certificate **at the same time**, the connection failed. This issue has now been resolved.

Incorrect Display of Users Authenticated via LDAP

VPN users authenticated via LDAP are listed incorrectly in the statistics under "Link Profiles (local)". This issue has been fixed so that it is now correctly displayed under "Link profiles (RADIUS/LDAP)".

The maximum number of LDAP Users has been increased from 10,000 to 40,000.

6. Known Issues

None

7. Getting Help for the NCP Secure Enterprise VPN Server

To ensure that you always have the latest information about NCP's products, always check the NCP website at:

https://www.ncp-e.com/en/products/centrally-managed-vpn-solution/gateway/

Next Generation Network Access Technology

Major Release: 11.00 r36173
Date: July 2017

Prerequisites

Linux Distributions:

The following Linux distributions are supported with this release:

- CentOS 7.3
- Debian GNU/Linux 8.7
- SUSE Linux Enterprise Server 12 SP2
- Ubuntu Server 16.04.2 LTS

Update Prerequisites

Please read the instructions for updates of previous versions carefully!
(See NCP_RN_SES_10_and_HAS_10_Update_and_License_de.PDF)

Prerequisites for Configuration via Secure Enterprise Management (SEM)

- Secure Enterprise Management Server: Version 4.05 or later
- Management Plugin - Server Configuration: Version 11.00 or later

Prerequisites for High Availability

If the Secure Enterprise VPN Server 11.00 is used in a high availability network, ensure that the High Availability Server (HA Server) is version 10.01 or later.

Note: From version 10.0, a license key for the same version of Secure Enterprise VPN Server and the Secure Enterprise HA Server is required to use these two products in combination.

Next Generation Network Access Technology

1. New Features and Enhancements

Advanced License Management for iOS Clients

From this version of the NCP Secure Enterprise VPN Server the license management of the NCP Secure Enterprise iOS client is supported.

Significant Performance Improvements

Higher Number of Outgoing Connections

The maximum number of outgoing VPN connections has been increased from 750 to 10,000.

Support for IKEv2 Signature Authentication (RFC 7427 with RSA-PSS padding)

A new certificate authentication method according to RFC7427 has added to the client and server.

The following key types are supported for user and hardware certificates: RSA, ECC NIST, ECC BP in different key lengths.

In the "Certificate Verification" of a domain group, the "Enable RSA Authentication with PKCS # 1 V1.5 Padding" option is activated by default. The previous IKEv2 RSA certificate authentication can only still be used if this option is disabled.

Client VPN IP Address Assignment for Metered Connections

This featured is used in home office environments, where the internet connection is metered (particularly routers using mobile data). In this scenario, the user workstation is connected to the Internet router via Wi-Fi. The Wi-Fi profile in the NCP Secure Client can be configured as a "metered connection" under the profile settings. This setting is sent to the NCP Secure Enterprise VPN Server.

In order to reduce costs for metered connections, the client receives an IP address from a pool assigned for clients with a mobile connection during tunnel setup. Centralized applications that provide the client with updates can therefore only transfer the most necessary data traffic.

The pool ranges for metered connections are defined in the server under "address allocation", and each pool receives a number. After entering the pool number in the link profile under "Routing" the client is assigned an IP address from the corresponding pool. If the pool numbers are set to zero and no fixed IP address is assigned, the IP address range of the configured DHCP server is used.

Support for Several Server Certificates

Several standard certificates can now be set for each domain group. The Secure Enterprise VPN Server can select the one that best suits the client's request (e.g. the longest expiry period) for the respective domain group.

Additional Security

The services ncpwsupd and ncpsrvmgmd are now run with restricted rights to make potential attacks more difficult.

Next Generation Network Access Technology

Display of Additional Connection Information

The following information is displayed in the statistics under "Link profile":
- NCP VPN Path Finder version
- Seamless Roaming
The account log shows which local endpoint IP address the client connects to.

2. Improvements / Problems Resolved

Netmasks were not not transferred correctly during client connection. This issue has been resolved.

New Tool for Creating the Scripts for dve_up and dve_down under [SES-INSTALL-DIR] / sbin / ses-vrrp-setup.

3. Known Issues

None

4. Getting Help for the NCP Secure Enterprise VPN Server

To ensure that you always have the latest information about NCP's products, always check the NCP website at:

https://www.ncp-e.com/en/products/centrally-managed-vpn-solution/gateway/

Next Generation Network Access Technology