NCP Secure Enterprise Management

für Windows

Release Notes

Service Release: **4.05 r35843**
Datum: **Juni 2017**

Voraussetzungen

Microsoft Windows Betriebssysteme:

Die folgenden Microsoft Windows Betriebssysteme werden mit diesem Release unterstützt:

- Windows Server 2016 64 Bit
- Windows Server 2012 R2 64 Bit
- Windows Server 2008 R2 64 Bit

Datenbank mit ODBC-Schnittstelle

Folgende x64 Datenbanken mit zugehörigem ODBC-Treiber wurden getestet und freigegeben:

Datenbank	ODBC-Treiber
MySQL Server 5.7.17	ODBC 5.3.6
MS SQL Server 2016	ODBC Driver 13 for SQL Server 13.0.1601.5
Oracle 11g Express x86	ODBC 11.02.00.03
Oracle 11g Express x64	ODBC InstantClient 12.01.00.02
Oracle 12c Enterprise x64	ODBC InstantClient 12.01.00.02

NCP empfiehlt die Verwendung der getesteten Treiber.

Lizenzierung des NCP Management Servers

Ab den Software-Versionen 4.0 wird ein Lizenzschlüssel der gleichen Version benötigt, um die Server-Komponenten produktiv nutzen zu können. Server früherer Versionen 3.x, die ohne die entsprechende Aktualisierung des Lizenzschlüssels auf die Version 4.0 oder höher mit einem Update angehoben werden sollen, verlieren ihre Funktionalität.

Die Notwendigkeit gleicher Software-Version und Lizenzschlüssel-Version zur Freischaltung der Software gilt ab der Version 4.0 für alle späteren Versionen.

1. Neue Leistungsmerkmale und Erweiterungen

Unterstützung mehrerer Server-Zertifikate im Secure Enterprise Server

Diese Version des Management-Systems unterstützt den Einsatz mehrerer Server-Zertifikate am Secure Enterprise Server 11.0.

2. Verbesserungen / Fehlerbehebungen

Automatische Integration des AddOn für „Advanced Authentication“

Das AddOn für Advanced Authentication wird sowohl bei einem Update als auch bei der Neuinstallation des Management Servers automatisch mit installiert.

Anzeige der ODCB-Bibliothek

Mit dem Kommando "ncprsud -testDB" wird die verwendete ODBC-Bibliothek angezeigt.

Performance-Steigerung bei Replikation

Bei Verwendung von Primary- und Backup-Server wurde die Performance der automatischen Replikation der geänderten Daten deutlich erhöht.

Script Plugin

Das Scripting zur Abfrage des Client-Betriebssystems wurde optimiert.

3. Bekannte Einschränkungen

Keine

Deutschland: NCP engineering GmbH · Dombühler Str. 2 · 90449 Nürnberg · Fon +49 911 9968-0 · Fax +49 911 9968-299
Americas: NCP engineering, Inc. · 678 Georgia Ave · Sunnyvale, CA 94085 · Phone: +1 (650) 316-6273 · www.ncp-e.com

NCP Secure Enterprise Management

für Windows

Release Notes

Service Release: **4.05 r34543**
Datum: **Mai 2017**

Voraussetzungen

Microsoft Windows Betriebssysteme:

Die folgenden Microsoft Windows Betriebssysteme werden mit diesem Release unterstützt:

- Windows Server 2016 64 Bit
- Windows Server 2012 R2 64 Bit
- Windows Server 2008 R2 64 Bit

Datenbank mit ODBC-Schnittstelle

Die unterstützen Datenbanken sind nachfolgend einzusehen:

Datenbank	ODBC-Treiber
MySQL Server 5.7.17	ODBC 5.3.6
MS SQL Server 2016	ODBC Driver 13 for SQL Server 13.0.1601.5
Oracle 11g Express x86	ODBC 11.02.00.03
Oracle 11g Express x64	ODBC InstantClient 12.01.00.02
Oracle 12c Enterprise x64	ODBC InstantClient 12.01.00.02

Lizenzierung des NCP Management Servers

Ab den Software-Versionen 4.0 wird ein Lizenzschlüssel der gleichen Version benötigt, um die Server-Komponenten produktiv nutzen zu können. Server früherer Versionen 3.x, die ohne die entsprechende Aktualisierung des Lizenzschlüssels auf die Version 4.0 oder höher mit einem Update angehoben werden sollen, verlieren ihre Funktionalität.
Die Notwendigkeit gleicher Software-Version und Lizenzschlüssel-Version zur Freischaltung der Software gilt ab der Version 4.0 für alle späteren Versionen.

1. Neue Leistungsmerkmale und Erweiterungen

Verteilung neuer Firmware für die NCP Secure VPN GovNet Box mit dem Secure Enterprise Management (SEM)

Ab dieser Version kann das Secure Enterprise Management dafür eingesetzt werden, Firmware-Updates an die Secure VPN GovNet Box zu übertragen, sofern diese bereits mit einer Firmware ab Version 10.10 betrieben wird.
Voraussetzung: NCP Secure VPN GovNet Suite ab Version 11.00

Lizenz- und Konfigurationsmanagement des NCP Secure Enterprise iOS Clients

Lizenzen und Konfigurationen von iOS Clients können über das Secure Enterprise Management verteilt werden.

Neue Icons für SEM und Konsole

Das Secure Enterprise Management und die Konsole stellen sich auf der Oberfläche des Desktops mit neuen Icons dar.

2. Verbesserungen / Fehlerbehebungen

Verbesserte Log-Suche am Management Server

Die Suchfunktion im Fenster des Log-Dialogs wurde verbessert. Die Zeilen mit dem gesuchten Text werden korrekt angezeigt. Dabei können die üblichen Wildcards eingesetzt werden:
Fragezeichen „?“ können als Platzhalter für einzelne Zeichen des Textes eingesetzt werden.
Ein Asterisk „*“ kann als Platzhalter für eine Zeichenkette eingesetzt werden.

Erweiterung der Konfigurationsmöglichkeiten

Für die IPsec-Konfiguration der Client-Profile wurden die Diffie-Hellman-Gruppen DH27 bis DH30 hinzugefügt.

Re-Login startete die SEM-Konsole minimiert

Nach Anmeldung des Administrators an den Secure Management Server und dem darauf folgenden Laden der Plug-ins wurde zeitweilig das Konsolenfenster nur minimiert in der Task-Leiste dargestellt. Dieser Fehler wurde behoben.

3. Bekannte Einschränkungen

Keine

Deutschland: NCP engineering GmbH · Dombühler Str. 2 · 90449 Nürnberg · Fon +49 911 9968-0 · Fax +49 911 9968-299
Americas: NCP engineering, Inc. · 678 Georgia Ave · Sunnyvale, CA 94085 · Phone: +1 (650) 316-6273 · www.ncp-e.com

NCP Secure Enterprise Management

für Windows

Release Notes

Service Release: **4.01 r32851**
Datum: **November 2016**

Voraussetzungen

Microsoft Windows Betriebssysteme:

Die folgenden Microsoft Windows Betriebssysteme werden mit diesem Release unterstützt:

- Windows Server 2008 R2 64 Bit
- Windows Server 2012 64 Bit
- Windows Server 2012 R2 64 Bit

Datenbank mit ODBC-Schnittstelle

Die unterstützen Datenbanken sind in den Release Notes zu Version 4.0 aufgelistet.

Lizenzierung des NCP Management Servers

Ab den Software-Versionen 4.0 wird ein Lizenzschlüssel der gleichen Version benötigt, um die Server-Komponenten produktiv nutzen zu können. Server früherer Versionen 3.x, die ohne die entsprechende Aktualisierung des Lizenzschlüssels auf die Version 4.0 oder höher mit einem Update angehoben werden sollen, verlieren ihre Funktionalität.
Die Notwendigkeit gleicher Software-Version und Lizenzschlüssel-Version zur Freischaltung der Software gilt ab der Version 4.0 für alle späteren Versionen.

1. Neue Leistungsmerkmale und Erweiterungen

Überarbeitete Client-Softwareverteilung

Mit der Freigabe der Clientversion 10.10 ist die Lizenzierung mit einem Lizenzschlüssel gleicher Version notwendig geworden, Lizenzschlüssel älterer Versionen werden nicht mehr angenommen.
Im Falle der Softwareverteilung via Secure Enterprise Management (SEM) wurde daraufhin ein Mischbetrieb unterschiedlicher Clientversionen nicht optimal unterstützt.
Aus diesem Grund werden ab der Client-Version 10.11 das Update der Konfiguration und das der Lizenz getrennt gehandhabt.
Folgende Komponenten sind dazu zwingend erforderlich:

- NCP Secure Enterprise Management Server 4.01
- NCP Client Plug-in 10.11
- NCP Lizenz Plug-in 10.11
- NCP Update Client 5.02

Script-Funktion zum Löschen von Client-Lizenzen

Löschen von Client-Lizenzen aus dem SEM sind mit der neuen Script Funktion CGroup.DelLicenseKey möglich. Seriennummern, die bereits für Benutzer vergeben sind, können wie bisher nicht gelöscht werden.

2. Verbesserungen / Fehlerbehebungen

Keine

3. Bekannte Einschränkungen

Upload-Prozess des Client-Update Packages

Aufgrund stärkerer Verschlüsselung beim Upload-Prozess des Client-Update Packages zum SEM 4.01, können die älteren Client-Update Packages **bis einschließlich der Client-Versionen 10.04 r31799 und 10.10 r31802 nicht verschlüsselt** auf den SEM hochgeladen werden.

Deutschland: NCP engineering GmbH · Dombühler Str. 2 · 90449 Nürnberg · Fon +49 911 9968-0 · Fax +49 911 9968-299
Americas: NCP engineering, Inc. · 678 Georgia Ave · Sunnyvale, CA 94085 · Phone: +1 (650) 316-6273 · www.ncp-e.com

NCP Secure Enterprise Management

für Windows

Release Notes

Major Release: 4.00 r29980 (Win)
Datum: Juni 2016

Voraussetzungen

Microsoft Windows Betriebssysteme:

Die folgenden Microsoft Windows Betriebssysteme werden mit diesem Release unterstützt:

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012

Datenbank mit ODBC-Schnittstelle

Die unterstützen Datenbanken sind nachfolgend einzusehen:

Datenbank	ODBC-Treiber
MySQL Server 5.5.28	ODBC 5.1.5
MySQL Server 2014	ODBC Driver 11 for SQL Server 2014
Oracle 11g Express x86	ODBC 11.02.00.03
Oracle 11g Express x64	ODBC InstantClient 12.01.00.02
Oracle 12c Enterprise x64	ODBC InstantClient 12.01.00.02

1. Neue Leistungsmerkmale und Erweiterungen

Management Plug-ins

Mit dem Secure Enterprise Management wird folgendes Plug-in freigegeben:
Endpoint Policy Plug-in 4.0 r29898

Lizenzierung des NCP Management Servers

Ab den Software-Versionen 4.0 wird ein Lizenzschlüssel der gleichen Version benötigt, um die Server-Komponenten produktiv nutzen zu können. Server früherer Versionen 3.x, die ohne die entsprechende Aktualisierung des Lizenzschlüssels auf die Version 4.0 oder höher mit einem Update angehoben werden sollen, verlieren ihre Funktionalität.
Die Notwendigkeit gleicher Software-Version und Lizenzschlüssel-Version zur Freischaltung der Software gilt ab der Version 4.0 für alle späteren Versionen.

NCP Management Server 4.0 als 64-Bit-Anwendung

Dies ist die erste freigegebene Version des NCP Secure Enterprise Management Servers als 64 Bit Anwendung und gleichzeitig die letzte freigegebene Version als 32-Bit-Anwendung. Das Update einer vorhergehenden Version kann daher mit der 32-Bit-Anwendung oder, wie nachfolgend aufgezeigt, durch Migration auf die 64-Bit-Anwendung erfolgen.

Update auf Version 4.0 unter Beibehaltung des Servers als 32-Bit-Anwendung
Soll der Management Server als 32-Bit-Anwendung beibehalten werden, wird mit dem Software-Paket NCP_SEM_Windows_x86_400_rev29980.exe ein Update auf eine Testversion 4.0 eingespielt. Nach Eingabe des Lizenzschlüssels für Version 4.0 wird die Vollversion freigeschaltet.
Das Software-Paket NCP_SEM_Windows_x86_400_rev29980.exe ist das letzte des Management Servers für 32 Bit. Alle künftigen Releases sind 64-Bit-Anwendungen**.**

Installation des NCP Management Servers 4.0 als 64-Bit-Anwendung
Die Migration des NCP Secure Enterprise Management Servers von einer 32- auf eine 64-Bit-Anwendung geschieht wie folgt:

- Beenden aller Dienste des vorhergehenden NCP Secure Enterprise Management Servers
- Sicherung der Konfigurationsdateien der alten Version:
  Inhalt der folgenden Verzeichnisse: „.\consoleplugins“, „.\rwsrsu“, „.\client“ und „.\packages“
  Folgende Dateien: „.\scripts\parameter.conf“, „ncprsu.conf“ und „rsudb.conf“
- Deinstallation des NCP Advanced Authentication Add-Ons (falls installiert)
- Deinstallation des alten NCP Secure Enterprise Management Servers
- Installation/Konfiguration eines 64 Bit ODBC-Treibers
- Installation des aktuellen 64 Bit NCP Secure Enterprise Management Servers ohne Auswahl der 64 Bit ODBC Datenbank (Abbruch innerhalb der NCP Secure Enterprise Management Server - Konfiguration) und Installation abschließen
- Ggf. Installation des NCP Advanced Authentication Add-Ons
- Beenden aller Dienste in der NCP Secure Enterprise Management Server – Konfiguration
- Einspielen der gesicherten Konfigurationsdateien der alten Version in die neue 64 Bit Installation des NCP Secure Enterprise Management Servers
- Eingabe des neuen Lizenzschlüssels mit dem Lizenzierungstool
- Starten der NCP Secure Enterprise Management Server – Konfiguration, Auswahl der 64 Bit ODBC Datenbank-Verbindung und Starten der Dienste

Administratoranmeldung über Active Directory

Alternativ zur lokalen Konfiguration eines Administrators im SEM kann nun das Administratorpasswort gegen Microsoft Active Directory geprüft werden.

Überarbeitung der Benutzeroberfläche

Es können diverse Farbschemata zur Darstellung ausgewählt werden.

Unterstützung der Datenbanken Oracle 12c* und MariaDB

* Bei Verwendung von Oracle 12c ist darauf zu achten die Datenbank von einem Common User mit „C##“-Prefix erstellen zu lassen.

Deutschland: NCP engineering GmbH · Dombühler Str. 2 · 90449 Nürnberg · Fon +49 911 9968-0 · Fax +49 911 9968-299
Americas: NCP engineering, Inc. · 678 Georgia Ave · Sunnyvale, CA 94085 · Phone: +1 (650) 316-6273 · www.ncp-e.com

2. Verbesserungen / Fehlerbehebungen

Optimierung der Datenbankanbindung für den Backup SEM-Betrieb.
Im Darstellungsmodus „Hoher Kontrast“ wurde die Darstellung optimiert.

3. Bekannte Einschränkungen

Keine

4. Hinweise zum NCP Secure Enterprise Management

Weitere Informationen zum letzten Stand der Entwicklung der NCP-Produkte erhalten Sie auf der Website:
https://www.ncp-e.com/de/service/
Weitere Unterstützung bei Fragen zum NCP Secure Enterprise Management, erhalten Sie über die Mail-Adressen auf folgender Seite:
https://www.ncp-e.com/en/support/

E-Mail: support@ncp-e.com

Deutschland: NCP engineering GmbH · Dombühler Str. 2 · 90449 Nürnberg · Fon +49 911 9968-0 · Fax +49 911 9968-299
Americas: NCP engineering, Inc. · 678 Georgia Ave · Sunnyvale, CA 94085 · Phone: +1 (650) 316-6273 · www.ncp-e.com

5. Leistungsmerkmale

Zentrale Verwaltung

Das NCP Secure Enterprise Management (SEM) ist der zentrale Bestandteil der NCP Next Generation Network Access Technology. Als **Single Point of Administration** schafft es die erforderliche Transparenz für Netzwerkadministratoren, um mobile und stationäre Telearbeitsplätze sowie remote VPN-Gateways in Filialnetzen zentral zu verwalten. Das NCP Software-Tool bietet alle Funktionalitäten und Automatismen, die für die Inbetriebnahme und den Betrieb eines Remote Access-Projektes erforderlich sind.
Mit dem Secure Enterprise Management werden Konfigurationen, Zertifikate und Software Updates zentral erzeugt und gespeichert bzw. verteilt und aktualisiert oder ausgerollt.
Die Richtlinien für eine Endpoint Security (Network Access Control) werden am Secure Enterprise Management (SEM) zentral erstellt. Entsprechend der erstellten Regeln erhält der Enterprise Client Zugang zum Firmennetz.

Lizenzierung der Managed Units

Die Gesamtzahl der zu lizenzierenden Managed Units (MU) für ein Secure Enterprise Management-System setzt sich aus der Anzahl der Client-Einträge (Benutzer) plus der Anzahl der Einträge für Remote Server zusammen. Die Einheiten der zentralen Server (Server Configuration Plug-ins mit Secure Server und HA Server) werden den Lizenzbestimmungen entsprechend nicht zu den Managed Units gezählt.

Komponenten des Secure Enterprise Managements

Das NCP Secure Enterprise Management (SEM) besteht aus dem Management Server und der Management Console. Das Datenbank-System ist nicht im Lieferumfang enthalten.

Voraussetzungen für die Server-Komponente

64-Bit Betriebssysteme
Windows Server 2008
Windows Server 2008 R2 Enterprise
Windows Server 2012 Datacenter
Rechner
CPU mind. Pentium III-800 MHz (abhängig von der Anzahl der Managed Units)
Mit RADIUS Plug-in: Pentium IV-1,5 GHz
Festplatte: min. 50 MB freier Speicher zzgl. Speicherplatz für Log-Dateien und ca. 20 MB pro Software-Paket

Deutschland: NCP engineering GmbH · Dombühler Str. 2 · 90449 Nürnberg · Fon +49 911 9968-0 · Fax +49 911 9968-299
Americas: NCP engineering, Inc. · 678 Georgia Ave · Sunnyvale, CA 94085 · Phone: +1 (650) 316-6273 · www.ncp-e.com

Unterstützte Datenbanken

Der Management Server ist ein datenbankbasiertes System und korrespondiert mit nahezu jeder Datenbank über ODBC:

- MySQL Server 5.5.28
- MS SQL Server 2014
- Oracle 11g Express x86
- Oracle 11g Express x64
- Oracle 12c Enterprise x86

Alle systemrelevanten Informationen werden in der Datenbank abgelegt und sind üblicherweise in den Backup-Prozess eingebunden. Dazu gehören unter anderem: Benutzer-Profile (Konfigurationen der Managed Units), Lizenzkeys und Authentisierungsdaten, Zertifikate, Providerkennungen etc. Unter Windows xxxx 64bit-Systemen gibt es zwei ODBC Data Sources. NCP empfiehlt, die Datenbank-Verbindung direkt über die NCP Secure Management Server - Konfiguration Utility (Start / NCP Management Server / Konfiguration) anzulegen.

Backup-System

Optional steht ein Backup-System mit integriertem Replikationsdienst für den Management Server zur Verfügung.

Unterstützte Certification Authorities

Microsoft Certificate Services als integrierte und stand alone CA.

Voraussetzungen für die Console

Über die Management Console werden die VPN-Benutzerdaten zentral verwaltet.

Betriebssysteme

Windows Desktop Betriebssysteme 32-Bit und 64-Bit

Management Server-Module

Die Management Server-Module werden als Plug-ins von jedem Rechner im lokalen Netzwerk unter Angabe der IP-Adresse des Management Servers auf diesem installiert. Dies gilt auch für die Management Console, die ebenfalls als Plug-in installiert werden kann. (Das Datenbank-System ist nicht im Produktumfang enthalten.)

Verfügbare Plug-ins

- Management Console Plug-in
- Client Configuration Plug-in
- Firewall Plug-in
- Remote Server Configuration Plug-in (Test-Software)
- Server Configuration Plug-in (HA Server und Secure Server)
- License Management Plug-in
- PKI Management Plug-in

- Endpoint Policy Plug-in
- Script Plug-in
- RADIUS Plug-in
- System Monitor Plug-in (Test-Software)

Unterstützte RFCs und Drafts

- RFC 2138 Remote Authentication Dial In User Service (RADIUS)
- RFC 2139 RADIUS Accounting
- RFC 2433 Microsoft CHAP
- RFC 2759 Microsoft CHAP V2
- RFC 2548 Microsoft Vendor-specific RADIUS Attributes
- RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP)
- RFC 2716 PPP EAP TLS Authentication Protocol
- RFC 2246 The TLS Protocol
- RFC 2284 PPP Extensible Authentication Protocol (EAP)
- RFC 2716 Certificate Management Protocol
- RFC 2511 Certificate Request Message Format
- Draft-ietf-pkix-cmp-transport-protocols-04.txt, Transport Protocols for CMP
- Draft-ietf-pkix-rfc2511bis-05.txt, Certificate Request Message Format (CRMF)

Zentrale Funktionalitäten

Administratoren-Management und Mandantenfähigkeit (Multi-Company Support)
Die Mandantenfähigkeit prädestiniert das Secure Enterprise Management für den Einsatz bei Managed Security Service Providern (MSSP) in sog. „Managed VPNs“ oder Remote Access-Strukturen, in denen mehrere Firmen gemeinsam eine VPN-Plattform nutzen (VPN Sharing).
Über die zentrale Administratoren-Verwaltung werden die Zugriffsrechte für die jeweiligen Administratoren auf die jeweiligen selbständigen Firmen mit angeschlossenen VPN-Benutzern definiert. Durch Gruppenzuordnung werden die Rechte der Administratoren so angelegt, dass jeder ausschließlich Zugriff auf seinen zu verwaltenden Mandantenkreis (Organisationsgruppe) hat. Ein Übergriff auf Daten anderer Mandanten ist ausgeschlossen.
Als VPN-Gateway kann der NCP Secure Enterprise Server aber auch das eines Fremdherstellers eingesetzt werden (siehe Kompatibilitätsliste unter www.ncp-e.com). Damit ist das Secure Enterprise Management auch in jede vorhandene IT-Infrastruktur integrierbar und ermöglicht den Betrieb auch in komplexen VPN-Umgebungen.

Lizenz-Management (License Management Plug-in)
Mit der Lizenzierung steht die Gesamtzahl der Managed Units für den Management Server zur freien

Deutschland: NCP engineering GmbH · Dombühler Str. 2 · 90449 Nürnberg · Fon +49 911 9968-0 · Fax +49 911 9968-299
Americas: NCP engineering, Inc. · 678 Georgia Ave · Sunnyvale, CA 94085 · Phone: +1 (650) 316-6273 · www.ncp-e.com

Verfügung. Die Managed Units können entweder als Benutzer- oder Remote Server-Lizenzen eingesetzt werden. Alle Lizenzen werden in einen Pool übernommen und nach festgelegten Richtlinien automatisiert verwaltet:

- Lizenzübernahme kann automatisiert erfolgen oder manuell vorgenommen werden
- Lizenz wird nach Ausscheiden eines Mitarbeiters in den Pool zurück gestellt
- Meldung wird ausgegeben wenn keine Lizenz mehr verfügbar ist

Erzeugung der Konfigurationen für die Managed Units

Mit der Management Console werden User-Daten abgerufen oder Konfigurationen und Zertifikate gespeichert. Alle relevanten Informationen werden in der Datenbank abgelegt und sind üblicherweise in den Backup-Prozess des VPN-Betreibers eingebunden.
Die Eingabe aller relevanten Daten kann an der Management Console interaktiv durch den Administrator vorgenommen oder skriptgesteuert über das Script Plug-in erfolgen.

Automatic Update (über LAN und VPN)

Der Update Service des Secure Enterprise Managements gestattet alle für das Remote Access-Umfeld relevanten Software-Komponenten zentral verfügbar zu halten. Sobald eine Verbindung zwischen Client und Corporate Network besteht, werden diese Komponenten automatisch auf der Client-Seite eingespielt. Sollte es während der Übertragung zu Störungen kommen, bleiben der bereits vorhandene Softwarestand sowie die Konfiguration unberührt. Erst nach einem komplettem, fehlerfreiem Transfer aller vordefinierten Daten findet das Update statt.

- Steuerung der Update-Pakete
  Mittels Update-Liste, die der Administrator nach den jeweiligen Erfordernissen zusammenstellt, erfolgt die Verteilung der Software-Komponenten. Dabei kann pro Komponente nach Verbindungsmedium, Häufigkeit der Ablehnungen eines Updates und Art des Updates differenziert werden.
- Update-Komponenten
  Folgende Software-Komponenten können für das automatische Update bereitgestellt werden:
  - Konfigurationen (Profile und Monitor-Einstellungen des Enterprise Clients)
  - Benutzer-Zertifikate (Soft-Zertifikate, p12-Format)
  - Aussteller-Zertifikate (Soft-Zertifikate, cer- und pem-Formate)
  - Update Client
  - Software-Versionen (Software Updates / Upgrades sind für Clients nur unter Windows Desktop-Betriebssystemen möglich)

- Verbindungsmedium
  Alle Verbindungsmedien, die die Remote-Seite unterstützt, können einer der Update-

Deutschland: NCP engineering GmbH · Dombühler Str. 2 · 90449 Nürnberg · Fon +49 911 9968-0 · Fax +49 911 9968-299
Americas: NCP engineering, Inc. · 678 Georgia Ave · Sunnyvale, CA 94085 · Phone: +1 (650) 316-6273 · www.ncp-e.com

Komponenten zugeordnet werden. So lässt sich zum Beispiel steuern, dass für große Datenmengen schnelle Verbindungsmedien genutzt werden.

- Update-Verfahren
  Alternativ zu einem Update über VPN, kann die Option des LAN Updates genutzt werden. (Eine NCP Dynamic Personal Firewall kann nur über LAN aktualisiert werden.) Bei einem Update über VPN werden alle Daten durch den Tunnel verschlüsselt übertragen. Bei einem LAN Update, wenn sich der Client PC im heimischen Firmennetz befindet, wird die SSL-Verschlüsselung eingesetzt.

Beschreibung der Plug-ins

System Monitor Plug-in (Test-Software)
Dieses Plug-in dient der schnellen Information über alle wichtigen Ereignisse innerhalb einer VPN-Installation als Balken- oder Linien-Diagramme. Der Administrator kann über den System Monitor je nach Bedarf aktuelle Status-Informationen in Echtzeit abrufen bzw. auf bereits gespeicherte Datenbestände der Remote Access-Umgebung zugreifen. Im jeweiligen Diagramm kann im Zeitraum beliebig zurück bzw. vorwärts geblättert werden. Die grafische Darstellung der Diagramme ist frei wählbar.

Client Configuration Plug-in
Hiermit werden die Profile der Secure Enterprise Clients erstellt, konfiguriert und verwaltet. Folgende Einstellungen sind damit möglich:

- alle gruppenspezifischen und verbindungstechnischen Parameter können mithilfe von Vorlagen (Templates) automatisiert generiert werden
- nur personenbezogene Daten werden manuell eingegeben (Authentisierungsdaten für Erstverbindung bei Rollout)
- Parametersperren, die der entfernte Benutzer nicht verändern kann, können definiert werden
- automatische Konfiguration der Benutzer-Profile für Zentralkomponenten (RADIUS, LDAP, SNMP)
- umfassendes Logging (Versionsstände, Zeitstempel für Konfigurationsänderungen, automatischer Upload von Client-Logdateien)
- Erzeugung eines generalisierten Init-Benutzers für Rollout
- automatisierte Erzeugung und Bereitstellung von Konfigurations-Updates

Firewall Plug-in
Zur Konfiguration der Personal Firewall in den Secure Enterprise Clients und der Dynamic Personal

Deutschland: NCP engineering GmbH · Dombühler Str. 2 · 90449 Nürnberg · Fon +49 911 9968-0 · Fax +49 911 9968-299
Americas: NCP engineering, Inc. · 678 Georgia Ave · Sunnyvale, CA 94085 · Phone: +1 (650) 316-6273 · www.ncp-e.com

Firewall der Client Suite. Folgende Einstellungen können vorgenommen werden:

- applikations- und verbindungsabhängige Filterregeln
- protokoll-, port- und adressbezogene Filterregeln
- Vorgaben für die Erkennung von „friendly networks“ (IP-Adresse Netzwerk, Netzwerkmaske, IP-Adresse des DHCP-Server, MAC-Adresse)
- Logging-Einstellungen
- FND-Serverkonfiguration (Friendly Net Detection)
- Firewall-Einstellungen, die der entfernte Benutzer nicht verändern kann, können definiert werden

Remote Server Configuration Plug-in und Server Configuration Plug-in

Mit dem Remote Server Configuration Plug-in werden entfernte Gateways zum Beispiel in Filialen als Managed Units lizenziert, konfiguriert und verwaltet.

Das Server Configuration Plug-in dient der Konfiguration und Verwaltung von Secure Servern (Secure Enterprise Server und Secure High Availability Server) im zentralen Netz. Die Lizenzierung der Server-Komponenten erfolgt dezentral an der jeweiligen Maschine über deren Web-Interface.

An der Management Console werden die Zugriffsrechte für den jeweiligen Server verwaltet und die komplette Konfiguration des Servers erstellt.

Die Konfigurations- und Statistik-Oberfläche des Web-Interfaces der Server-Komponente wird an der Management Console eins zu eins abgebildet. Darüber hinaus kann von der zentralen Management Console die Konfiguration über das Web-Interface vor Ort temporär gestattet werden. Konkurrierende Konfigurationsänderungen sind ausgeschlossen.

Zur Konfiguration einer Gruppe von Servern (Server Farm) können Vorlagen genutzt werden, ebenso wie für Client-Benutzergruppen.

PKI Enrollment Plug-in

Das Plug-in fungiert als Registration Authority (RA). Im Zusammenwirken mit unterschiedlichen Certification Authorities (CA) werden elektronische Zertifikate (X.509 v3) erstellt und verwaltet. Eine erzeugtes Zertifikat kann wahlweise zur Verwendung als Soft-Zertifikat (PKCS#12) oder für den Einsatz auf Smart Card oder USB-Token (PKCS#11) abgelegt werden. Die im Lieferumfang enthaltene NCP Demo-CA kann während der Testphase für die Abbildung einer PKI genutzt werden, ist jedoch nicht für den produktiven Einsatz vorgesehen. Die Umstellung auf eine externe CA ist problemlos möglich. Die wichtigsten Funktionalitäten des PKI Plug-ins sind:

- Erstellen von Benutzer- und Hardware-Zertifikaten (auch Bulk Mode)
- Verlängern der Zertifikatsgültigkeit (PKCS#7)
- Sperren von Zertifikaten
- Verteilung der Zertifikate (auch Multi-Client-Zertifikate)
- Anlegen der Benutzerkonfiguration über LDAP im Verzeichnisdienst

Deutschland: NCP engineering GmbH · Dombühler Str. 2 · 90449 Nürnberg · Fon +49 911 9968-0 · Fax +49 911 9968-299
Americas: NCP engineering, Inc. · 678 Georgia Ave · Sunnyvale, CA 94085 · Phone: +1 (650) 316-6273 · www.ncp-e.com

- Erstellen eines PAC-Briefes (Personal Authentication Code) für Erstverbindung und Lizenzierung
- Generieren und Verteilen von Server-Zertifikaten

Endpoint Policy Plug-in

Mit Hilfe dieses Plug-ins werden alle sicherheitsrelevanten Parameter definiert, die vor einem Zugriff auf das Firmennetz überprüft werden sollen (Network Access Control). Die Einhaltung der vorgegebenen Sicherheitsrichtlinien ist zwingend und vom Anwender nicht umgehbar oder manipulierbar. Folgende Einstellungen am entfernten Rechner des Benutzers können überprüft werden:

- Software-Stand des Secure Enterprise Clients
- Betriebssystem-Informationen, z. B. Version oder Hotfixstand
- Dienste-Informationen
- Datei-Informationen
- Status des Virenscanners
- Registry-Werte
- Inhalte von Benutzer- und Hardware-Zertifikaten

Abweichungen von den Sollvorgaben werden protokolliert und können unterschiedliche Meldungen bzw. Aktionen auslösen. Z. B.:

- Anzeige einer Meldung am Client
- Ausgabe einer Meldung im Log-Buch des Clients
- Senden einer Meldung zum Management Server
- Senden einer Meldung zu einem Syslog Server
- Freischalten der relevanten Firewall-Regeln
- Weiterleitung in eine Quarantänezone
- Trennung der VPN-Verbindung

RADIUS Plug-in

Für die Konfiguration der Managed Units (Benutzern) in den zentralen VPN-Gateways steht optional die RADIUS-Schnittstelle zur Verfügung. Das RADIUS Plug-in dient der Verwaltung des integrierten RADIUS Servers und deckt folgende Funktionen ab:

- Automatische Anlage von RADIUS-Accounts über die Client- und Remote Server Configuration Plug-ins
- Unterstützung von PAP/CHAP-Requests
- Erfassung von Accounting-Daten
- Sperren von Benutzern bei wiederholten fehlerhaften Anmeldungen
- Verwaltung von mehreren RADIUS-Konfigurationen unterschiedlicher Gateways

Deutschland: NCP engineering GmbH · Dombühler Str. 2 · 90449 Nürnberg · Fon +49 911 9968-0 · Fax +49 911 9968-299
Americas: NCP engineering, Inc. · 678 Georgia Ave · Sunnyvale, CA 94085 · Phone: +1 (650) 316-6273 · www.ncp-e.com

- RSA Authentication Manager Proxy-Funktionalität

Optional steht ein Backup RADIUS-Server zur Verfügung. Dies gestattet vorhandene RADIUS Server durch den integrierten RADIUS Server des Management-Systems zu ersetzen.