NCP Secure Enterprise Management

für Windows

Release Notes

Major-Release: **6.10 r29390**
Datum: **März 2022**

Voraussetzungen

Microsoft Windows Betriebssysteme:

Die folgenden Microsoft Windows Betriebssysteme werden mit diesem Release unterstützt:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

Datenbank:

Folgende x64 Datenbanken mit zugehörigem Treiber wurden getestet und freigegeben:

Datenbank	Treiber
MariaDB 10.5.10 (x64)	MariaDB Connector/ODBC 3.1.12 (x64)
MS SQL Server 2019	MS SQL Server 10.00.20348
MS SQL Server 2017	MS SQL Server 10.00.17763
Oracle 19c	ODBC InstantClient 19.03.0000

Voraussetzung für den Betrieb des NCP Secure Enterprise Management (SEM)

Um diese Management Version nutzen zu können bedarf es der folgenden Komponenten:

- NCP Management Console: Version 6.10
- VS GovNet Connector Configuration Plug-in: Version 2.10 oder neuer
- Client Configuration Plug-in: Version 13.00 oder neuer
- Firewall Plug-in: Version 13.00 oder neuer
- License Plug-in: Version 13.00 oder neuer
- Server Configuration Plug-in: Version 12.13 oder neuer
- Radius-Plug-in: Version 5.30 oder neuer
- PKI Enrollment Plug-in: Version 4.05 oder neuer
- Endpoint Policy Plug-in: Version 4.00 oder neuer
- Script Plug-in: Version 6.10 oder neuer

Hinweis für die Migration von einem NCP Exclusive Remote Access Management zum NCP Secure Enterprise Management Server 6.10

Achtung: Um einen unterbrechungsfreien Betrieb sicherzustellen ist darauf zu achten einen gültigen Lizenzschlüssel für den NCP Secure Enterprise Management Server 6.10 verfügbar zu haben.

Die Migration von einem NCP Exclusive Remote Access Management hin zum NCP Secure Enterprise Management Server 6.10 wird vom Updatevorgang unterstützt. Bereits eingespielte Lizenzen sind nach dem Update/Migration weiterhin nutzbar. Nach Abschluss des Updatevorganges ist darauf zu achten, eine gültige Lizenz für den NCP Secure Enterprise Management Server 6.10 in der Management Konsole einzuspielen.

Hinweis für die Nutzung der NCP 2-Faktor-Authentisierung

Achtung: Die Nutzung der NCP 2-Faktor-Authentisierung mittels TOTP-Softtoken oder SMS (Advanced Authentication) ist ab dieser SEM-Version eine kostenpflichtige Option für die ein eigener Lizenzschlüssel benötigt wird.

Hinweis für die automatisierte Ausführung von Skripten

Die automatisierte Ausführung von Skripten, z.B. durch Aktionen wie „Benutzer löschen“ oder „Zertifikat verlängern“, ist ab dieser SEM-Version deprecated und wird ab der Version 6.20 nicht mehr enthalten sein.

1. Neue Leistungsmerkmale und Erweiterungen

REST-API

Die ab dieser Version neu eingeführte REST-API ermöglicht eine noch bessere Integration des NCP Secure Enterprise Management Servers in die IT-Infrastruktur des Anwenders. Die folgenden Bereiche können über REST-API angesprochen werden:

- Basiseinstellungen des SEM
- Client Management
- PKI Management
- RADIUS Management
- Firewall Konfiguration
- Lizenz Management

Grundsätzlich kann der SEM via REST von beliebigen Programmiersprachen angesprochen werden. Um die Nutzung für Administratoren weiter zu erleichtern, bietet NCP für die Skriptsprache Python eine NCP Python-API an. Diese ist von pypi.org (Python Package Index) mittels Kommandozeilenbefehl `pip install NcpSemApi` installierbar.

Neuer Menüpunkt „Konfiguration Lizenzreport“

Der für die PayPerUse-Lizenzierung notwendig Lizenzreport, kann durch den Aufruf des neuen Menüeintrages „Konfiguration Lizenzreport“ konfiguriert und der zugehörige Mailversand getestet werden.

Unterstützung des NCP VS GovNet Connector 2.0

Ab dieser Version des NCP Secure Enterprise Management Servers wird der NCP VS GovNet Connector 2.0 oder höher in Verbindung mit dem zugehörigen Plug-in unterstützt.

Eigene Lizenz für NCP 2-Faktor-Authentisierung nach TOTP- oder SMS-Verfahren

Die Verwendung der NCP 2-Faktor-Authentisierung nach TOTP- oder SMS-Verfahren ist ab dieser Version des NCP Secure Enterprise Management Servers kostenpflichtig und benötigt daher eine eigene Lizenz.

Unterstützung des Audit-Logs im NCP VS GovNet Connector 2.0

Mittels des CLI-Aufrufs `rsulog -t auditlog …` kann das Audit-Log des NCP VS GovNet Connectors am NCP Secure Enterprise Management Server abgerufen werden.

Erweiterung des NCP Skript um einen Anmeldezeitraum für RADIUS-Benutzer

Diese Erweiterung von NCP Skript ermöglicht den Zugriff von bestehenden RADIUS-Benutzern auf definierte Zeitfenster zu beschränken.

2. Verbesserungen / Fehlerbehebungen

Verwendung von TLS 1.2

Jegliche TLS-Kommunikation des SEM geschieht ab dieser Version mit TLS 1.2. Sollte aus Gründen der Abwärtskompatibilität die Verwendung von TLS 1.0 oder 1.1 notwendig sein, so lässt sich dies in der Konfigurationsdatei `ncprsu.conf` in der Sektion `[General]` durch die Eingabe folgender Parameter konfigurieren:

- `MgmMinTLSVersion` (für Konsole, Script, Plug-in Upload Tool, Software Packages)
- `RsuMinTLSVersion` (Update Clients)
- `SrvCfgMinTLSVersion` ((v)SES, (v)HAS, Backup Server)

Mögliche Werte für diese Parameter sind "1.0", "1.1", "1.2". Sind diese Werte nicht gesetzt, so gilt TLS-Version 1.2. Die folgenden Softwareversionen benötigen zum SEM-Upload keine Anpassung der TLS-Version:

- Client SoftwareUpdatePackage ab 11.10
- Client Plug-in ab 11.10 (Ausnahme 11.21 r44244)
- Firewall Plug-in ab 12.00
- Lizenz Plug-in ab 11.10
- RADIUS Plug-in ab 5.10

- Server Plug-in ab 12.10

Generell ist der Plug-in-Import via .plugin-Datei unkritisch bzgl. der TLS-Version. Aktuelle Server, HA-Server, Windows-Clients der Version 12.x und macOS-Clients der Version 4.x sind ebenfalls unkritisch.

Neue Parameter im Account-Log

Die folgenden, vom NCP Secure Enterprise VPN Server (SES) an den SEM gesendeten RADIUS-Attribute werden im Account-Log gespeichert:

- NAS ID (32)
- NAS Port Type (61)
- Client Tunnel Endpoint (67)
- Server Tunnel Endpoint (66)
- Framed IP Address (8)
- Framed Protocol (7)
- DNS Name des Clients (190)

Erweiterung der Administrator-Gruppen-Konfiguration

Innerhalb der Administrator-Gruppen-Konfiguration kann unter „AD Authentisierung“ nun das Suchattribut für die Authentisierung des Konsolen-Administrators in LDAP konfiguriert werden. Standardmäßig ist hier „sAMAccountName“ für Microsoft Active Directory gesetzt.

Rekursives Erzeugen von Client-Konfigurationen

Geänderte Client-Konfigurationen können nun durch Setzen der Option „Auch in Untergruppen erzeugen“ rekursiv für die in den Untergruppen befindlichen Clients erzeugt werden.

Neue Standard-Werte im RADIUS Dictionary bei Neuinstallation

Bei einer Neuinstallation des SEM werden die Parameternamen im RADIUS-Dictionary auf NCP-Standardwerte gesetzt. Im Updatefall bleiben die Parameternamen unverändert.

Fehlermeldung „Package not compatible“

Wurde in der Client-Vorlage am SEM eine Clientversion für einen macOS, Linux, Android Client oder VS GovNet Connector eingestellt, so kam die Rückmeldung „Package not compatible“. Dieses Problem wurde behoben.

Hohe CPU-Last

Wurde im SEM ein neuer Benutzer angelegt, so erhöhte sich dadurch die CPU-Last deutlich. Dieses Problem wurde behoben.

Externe Authentisierung via Kerberos

Die Externe Authentisierung via Kerberos ist im Standardfall case insensitive, d.h. VPN-Benutzernamen werden via Kerberos, unabhängig von der Groß- oder Kleinschreibung, mit dem

Active Directory überprüft. Mittels der neu im SEM eingeführten RADIUS Einstellung `KrbSendEncTimeStamp=1` kann die Überprüfung auf case sensitive umgestellt werden.

CA-Zertifikat-Import – „Eintrag konnte nicht eingefügt werden“

CA-Zertifikate deren Authority Key Identifier (AKID) eine Länge von 70 Byte besitzt konnten nicht im SEM importiert werden und es wurde die Fehlermeldung „Eintrag konnte nicht eingefügt werden“ ausgegeben. Dieses Problem wurde behoben.

Problembehebung bei der Erstellung eines detaillierten Lizenzreports

Doppelter RADIUS-Benutzer

Unter bestimmten Umständen konnte ein RADIUS-Benutzer doppelt angelegt werden. Dieses Problem wurde behoben.

Replikationsfehler bzw. Ausfall des Backup SEM

Bei der Übertragung einer großen Benutzeranzahl mit State=0 kam es zu einem Timeout am Primary SEM. Dieses Problem wurde behoben.

Fehlende Task ID in Ausgabedateien

Die einer angelegten Task zugehörigen Ausgabedateien `task.out` und `task.err` enthielten keine Task ID. Dieses Problem wurde behoben.

Anzeige genutzter iOS-Client-Lizenzen

Beim Löschen eines iOS-Clients wurde die zugehörige Device ID nicht freigegeben, weshalb es zu einer falschen Anzeige freier iOS-Client-Lizenzen kam. Dieses Problem wurde behoben.

Log-Ausgabe „Usage error: tried to wait on non-existent child“

Der Skriptgesteuerte Versand des Lizenzreports erzeugte die Log-Ausgabe „Usage error: tried to wait on non-existent child“. Dieses Problem wurde behoben.

Problembehebungen bei Verwendung von Subscription-Lizenzierung

Bei der Verwendung von Subscription-Lizenzierung sind Probleme in Verbindung mit einem Proxy-Server oder der Anzeige des Subscription Status im HA-Server aufgetreten. Diese Probleme wurden behoben.

Fehlender Gruppenname in Log-Ausgabe

Wurde einem Benutzer eine Lizenz zugewiesen oder entfernt, so war in der zugehörigen Log-Ausgabe der Gruppenname nicht enthalten. Dieses Problem wurde behoben.

Problembehebung mit Benutzername und darin enthaltenen Umlauten

Benutzernamen mit Umlauten und externer RADIUS-Authentisierung via MS-CHAPv2 konnten nicht authentisiert werden. Dieses Problem wurde behoben.

Problembehebung bei der Umbenennung einer VPN Bypass-Liste im Plug-in

Problembehebung bei der Eingabe neuer Server- und HA-Server Lizenzen neuerer Version

Erweiterung der geschriebenen Logs um den Namen des genutzten Management Servers

Um in den Log-Einträgen unterscheiden zu können welcher Management Server (Primary oder Backup) die Einträge erstellt hat, wird diesen Einträgen der Name des Management Servers hinzugefügt.

Anlegen von RADIUS-Benutzern ohne konfiguriertes Passwort

Mit dieser Version des NCP Secure Enterprise Management Servers können RADIUS-Benutzer für den Fall einer externen Authentisierung ohne Passwort angelegt werden. Bisher wurde dafür immer ein zufälliges Dummy-Passwort generiert. Mit dieser Änderung soll verhindert werden, dass bei einem versehentlichen Abschalten der externen Authentisierung der betreffende RADIUS-Benutzer sich mit dem Dummy-Passwort anmelden könnte. Benutzer ohne konfiguriertes Passwort sind für den Fall der fehlenden, externen Authentisierung gesperrt.

Problembehebung mit Zertifikaten deren Common Name 63 Zeichen oder länger ist

Fehlermeldung … `tpb.zip" does not exist! errno=2`

Im Falle eines Updates des NCP Secure Enterprise Management Servers konnte es zu einer Fehlermeldung mit dem Inhalt … `tpb.zip" does not exist! errno=2` kommen. Dieses Problem wurde behoben.

NCP-Skript `user.createConfig` liefert immer positive Rückgabewert

Die NCP-Skript-Methode `createConfig` der Klasse `CUser` lieferte immer den Rückgabewert 1, auch wenn die Methode fehlschlägt. Dieses Problem wurde behoben.

Anzeigefehler in der Benachrichtigung „SEM Server-Zertifikat wird bald ungültig“

Unter bestimmten Bedingungen fehlte in der Benachrichtigung „SEM Server-Zertifikat wird bald ungültig“ das Ablaufdatum des Zertifikats. Dieses Problem wurde behoben.

Fehlerbehebungen beim Abspeichern einer Secure Server-Vorlage

Deinstallation des NCP Secure Enterprise Management Servers

Nach der Deinstallation des NCP Secure Enterprise Management Servers wurden nicht alle Log-Dateien entfernt. Dieses Problem wurde behoben.

Konfiguration des NCP Virtual Secure Enterprise VPN Servers

Änderungen in der Konfiguration eines NCP Virtual Secure Enterprise VPN Servers werden an das

Gateway übertragen jedoch nicht angezeigt. Dieses Problem wurde behoben.

Package und Download des Internationalen Phonebook entfernt

Das Package und der Download des Internationalen Phonebook für die Nutzung eines externen Dialers (iPass) am Client wurde entfernt.

Problembehebung bei RADIUS-Benutzern mit Umlauten im Namen

Option „Lizenz / Benutzte VPN Gateways im HA LB Modus“ im Server Plug-in

Die Option „Lizenz / Benutzte VPN Gateways im HA LB Modus“ lässt sich im Server Plug-in nicht aktivieren. Dieses Problem wurde behoben.

Advanced Authentication mit Sophos MCS

Der SMS Dienstleister Sophos MCS wurde aus der Konfiguration der Advanced Authentication entfernt, da er seinen Dienst eingestellt hat.

Problembehebung innerhalb der Wiederherstellung der primären Management Server Konfiguration aus der Failsafe-Replikation mittels `rsurestore`

Neue Konfigurationsoption für den Abgleich von Subscription-Lizenzen über einen Proxy in den Einstellungen des NCP Secure Enterprise Management Servers

Problembehebung mit Zertifikats-Vorlagen deren Name 63 Zeichen oder länger ist

Lizenz Plug-in importiert nur noch Lizenzversionen die ihm bekannt sind

Bisher konnten mit dem Lizenz Plug-in auch neuere Lizenzversionen als ihm bekannt sind eingespielt werden. Dies führte jedoch unter bestimmten Umständen zu Problemen in anderen Bereichen. Daher können ab dieser Version nur noch bekannte Lizenzversionen über das Lizenz Plug-in eingespielt werden.

Sicherheitsupdate der verwendeten OpenLDAP-Bibliothek auf die Version 2.4.57

Mit dem Sicherheitsupdate auf die OpenLDAP-Bibliothek 2.4.57 werden die folgenden Sicherheitslücken in OpenLDAP geschlossen: CVE-2020-36221 CVE-2020-36222 CVE-2020-36223 CVE-2020-36224 CVE-2020-36225 CVE-2020-36226 CVE-2020-36227 CVE-2020-36228 CVE-2020-36229 CVE-2020-36230

Löschen alter, in das Management geladener Logs nach dem neuen Anlegen eines Clients

Nach dem deinstallieren und anschließendem Neuinstallieren eines Clients waren dessen Logs noch am zentralen Management vorhanden. Dieses Problem wurde behoben.

Behebung eines XAUTH-Fehlers nachdem länger als 8 Stunden keine Anmeldung durch einen RADIUS-Benutzer erfolgte

Optimierung der Umschaltung des primären Management Servers auf einen sekundären Management Server

3. Bekannte Einschränkungen

Der NCP VS GovNet Connector 1.10 wird nicht mehr unterstützt

Die Verwaltung des NCP VS GovNet Connector 1.10 ist ab dieser Version des NCP Secure Enterprise Management Servers nicht mehr möglich.

Unterscheidung von NCP Secure Enterprise Client und VS GovNet Connector in einer Administrator-Gruppe nicht möglich

Wird eine Administrator-Gruppe angelegt, dann wird für das Client-Plug-in und das Connector-Plug-in jeweils der Eintrag „Client-Konfiguration“ angezeigt. Eine individuelle Konfiguration dieser beiden Client-Einträge ist nicht möglich.

Anzeige der Audit-Logs im VS GovNet Connector Plug-in aktuell nicht verfügbar

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/de/service/support/

E-Mail: support@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

Betriebssysteme
Siehe Voraussetzungen auf Seite 1.
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

Unterstützte Datenbanken
Siehe Voraussetzungen auf Seite 1.
Der Management Server ist ein datenbankbasiertes System und korrespondiert mit nahezu jeder Datenbank über ODBC oder den nativen Datenbanktreiber.
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 mittels Management Console auf diesem installiert. (Das Datenbank-System ist nicht im Produktumfang enthalten.)

Verfügbare Plug-ins

- Client Configuration Plug-in
- Firewall Plug-in
- 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 (experimental)
- VS GovNet Connector Configuration Plug-in

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 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 kompletten, fehlerfreien 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-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 (experimental)

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 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

Server Configuration Plug-in
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. Ein 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
- 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
- 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.