

NCP Secure Enterprise Management (für Windows-Betriebssysteme)

Neue Features Version 1.03 bis 2.05

Haftungsausschluss

Die in diesem Dokument enthaltenen Informationen können ohne Vorankündigung geändert werden und stellen keine Verpflichtung seitens der NCP engineering GmbH dar. Änderungen zum Zwecke des technischen Fortschritts bleiben der NCP engineering GmbH vorbehalten.

Warenzeichen

Alle genannten Produkte sind eingetragene Warenzeichen der jeweiligen Urheber.

© 2011 NCP engineering GmbH.
Technische Änderungen vorbehalten

Inhalt

Neue Features der Version 2.05 gegenüber Version 2.04	2
Neue Features der Version 2.04 gegenüber Version 2.03	4
Neue Features der Version 2.03 gegenüber Version 2.02	4
Neue Features der Version 2.02 gegenüber Version 2.00	5
Neue Features der Version 2.00 gegenüber Version 1.03	6

Neue Features der Version 2.05 gegenüber Version 2.04

Zentrale Verwaltung von Enterprise Mac Clients

Das NCP Secure Enterprise Management (SEM ab Version 2.05) bietet als „Single Point of Administration“ alle Funktionalitäten und Automatismen für Rollout, Inbetriebnahme und den wirtschaftlichen Einsatz eines **Secure Enterprise Mac Clients** (ab Version 2.01). Die Betriebssystemplattformen des Mac Clients sind **Mac OS X 10.5 Leopard (Intel) und Mac OS X 10.6 Snow Leopard**.

Das Secure Enterprise Management (SEM ab Version 2.05) versorgt den Enterprise Client über die VPN-Verbindung oder LAN (im Firmennetz) automatisch mit

- Konfigurations-Updates
- Zertifikats-Updates
- Aktualisierungen des Update Clients

Programm-Icon für die Management-Konsole

Das Programm-Icon für die Management-Konsole wurde geändert. Bei der Installation der aktuellen Software-Version bzw. einem Update auf die aktuelle Version wird das Icon in der Taskleiste und im Windows Start-Menü ausgetauscht.

Unterstützung von MySQL Server 5.5.8

Das Enterprise Management System unterstützt die Datenbank des MySQL Server 5.5.8.

Anzahl der Managed Units

Die Gesamtzahl der zu lizenzierenden Managed Units (MU) eines Secure Enterprise Management-Systems setzt sich aus der Anzahl der Client-Einträge plus der Anzahl der Einträge für Remote Server zusammen. Die Einheiten der zentralen Server des Server Configuration Plugins (Secure Server und HA Server) werden den Lizenzbestimmungen entsprechend nicht zu den Managed Units gezählt.

Erstellen und Verteilen der Server-Zertifikate mit dem PKI Enrollment Plug-in

Der Secure Server nimmt automatisch Server-Zertifikate an, die vom Secure Enterprise Management (SEM) generiert und verteilt wurden.

Ausstellen eines Zertifikats

Das Ausstellen eines neuen Server-Zertifikats erfolgt am Management-System in der "Server-Zertifikats-Konfiguration", von wo es auch nach der Erzeugung der Server-Konfiguration an das entsprechende VPN Gateway geschickt wird. Bei dieser Verteilung werden der Dateiname und die PIN aus der Server-Zertifikats-Konfiguration entnommen.

Verlängern eines Zertifikats

Ein Server-Zertifikat kann wie jedes andere Zertifikat verlängert werden. Dafür sind zwei Wege möglich:

- über das Server Configuration Plug-in: Server-Konfiguration / Secure Server / ausgestellte Zertifikate
- oder über das PKI Enrollment Plug-in: PKI Enrollment / ausgestellte Zertifikate.

Alternativ kann die Verlängerung auch über Script erfolgen.

Anzeige der Zertifikate

Unter dem Knoten "Server-Zertifikate" wird immer das Zertifikat angezeigt, das aktuell am Gateway eingesetzt ist.

Unter dem Knoten "ausgestellte Zertifikate" werden die mit dem PKI Plug-in ausgestellten Zertifikate für dieses Gateway angezeigt.

Unter "Info / Verwendungszweck" wird der Name der verknüpften Server-Zertifikats-Konfiguration angezeigt.

Voraussetzungen

- Management Server 2.05 Build 7
- Management Console 2.05 Build 3
- Server Configuration Plug-in 8.05 Build 14
- PKI Enrollment Plug-in 2.05 Build 2
- NCP Secure Server 8.05 Build 20

LDAP over SSL

Bei externer Authentisierung mit LDAP kann auch LDAP über SSL mit Standard-Port 636 genutzt werden. Voraussetzung ist, dass der LDAP-Server LDAP über SSL unterstützt. (ab RADIUS Plug-in 2.05 Build 2)

Selektion der Windows-Zertifikatsvorlage über das PKI Enrollment Plug-in

Soll das Enterprise Management System von der integrierten Windows Certification Authority die Zertifikate erhalten, so kann bei Erstellung einer Zertifikatsvorlage mit dem PKI Enrollment Plug-in bestimmt werden, welche Windows Zertifikatsvorlage von der Microsoft CA verwendet werden soll. Unter "Optionen" kann der Name der Vorlage angegeben werden (Windows Certificate Server Template Name). Pro Zertifikatsvorlage am SEM kann eine Windows Zertifikatsvorlage angegeben werden.

Wird in der Zertifikatsvorlage am SEM bei Einsatz einer Windows CA kein Vorlagenname eingetragen, so wird genau die Windows Zertifikatsvorlage verwendet, die in der Konfigurationsdatei ncppkisrv.conf angegeben ist. Diese Datei wie auch der Dienst ncppkisrv.exe befinden

den sich auf der Windows CA. Pro Konfigurationsdatei kann nur eine Windows Zertifikatsvorlage angegeben werden. (ab SEM 2.05 Build 7 mit ncppkisrv.exe von 01.12.2010)

Anzeige von CRL-Informationen

Mit dem Server Configuration Plug-in werden in der Konfiguration des jeweiligen Gateways unter "CA Zertifikate" folgende Informationen zur CRL angezeigt:

- CRL Aussteller
- Gültig von ... bis
- Anzahl der Einträge (ab SEM 2.05 ab Build 7 mit Secure Server Configuration Plug-in 8.05)

Scripting-Erweiterungen

Über Script können den Profilen des Enterprise Clients neue Parameterwerte zugewiesen werden. Den Profil-Einstellungen unter "DNS / Management" (Erster und zweiter DNS-Server, sowie Domain-Name) entsprechen im Script unter CDestination folgende neue Eigenschaften:

- dns1
- dns2
- domainName

Recht zur Eingabe des Authentisierungs-Codes

Bei Konfiguration der Administrator-Gruppen (im Hauptmenü unter "Bearbeiten") können pro installiertem Plug-in-Modul differenzierte Rechte an die jeweilige Administrator-Gruppe vergeben werden.

Für die Module "Client-Konfiguration" und "PKI Enrollment" kann bestimmt werden, welche Administrator-Gruppe den Authentisierungs-Code eingeben bzw. ändern darf. Dieser ist für die Update-Funktionen der Konfigurations- und Zertifikats-Verteilung nötig.

Neue Features der Version 2.04 gegenüber Version 2.03

Service Release zur Optimierung von Konfigurations-/Management-Sitzungen

Neue Features der Version 2.03 gegenüber Version 2.02

Neue Konfigurations-Optionen

Server Configuration Plug-in

Das Server Configuration Plug-in V. 8.0 Build 20 bildet die Funktionalität des Secure Enterprise Servers (SES) V. 8.0 Build 116 ab. Das Plug-in gestattet die Verteilung von Server-Konfigurationen an lizenzierte Secure Server der Version 8.0, wie auch den Import bereits bestehender Konfigurationen eines Secure Servers der Version 8.0. Das Server Configuration Plug-in setzt die Verwendung des Secure Enterprise Managements 2.03 voraus!

Konfiguration und Lizenzierung des Servers mit dem Server Configuration Plug-in entspricht der Konfiguration und Lizenzierung mit dem Web-Interface des Servers und sie können alternativ entweder zentral über das Plug-in oder lokal über das Web-Interface vorgenommen werden.

Die Dokumentation zum Server Plug-in, zu Import und Export der Konfiguration, finden Sie im SES-Navigator, dort im PDF SES-Parameter.

Neue Konfigurationsmöglichkeit im Update-Prozess

Mit der Aktualisierung des Management-Systems von Version 2.02 auf Version 2.03 wird auch das neue Client Configuration Plug-in 9.10 Build 50 installiert.

Damit wird eine weitere Differenzierung im Update-Prozess des Management-Systems für spezielle ältere Client-Konfigurationen möglich. (Beachten Sie dazu auch die Beschreibung

Neue Features der Version 2.02 gegenüber Version 2.00

Überarbeitetes Plug-In Verteilungs-Konzept

Das neue Plug-In Verteilungs-Konzept ermöglicht, dass alle Plug-In's zentral am Management Server verwaltet werden. Allen Console PCs stehen somit zu jeder Zeit die gleichen Plug-In's zur Verfügung.

Folgende Plug-ins wurden hinsichtlich Leistungsumfang und Funktionalität aktualisiert:

- Management Console Plug-in
- Client Configuration Plug-in
- Firewall Plug-in
- License Management Plug-in
- PKI Management Plug-in
- Endpoint Policy Plug-in (Network Access Control)
- RADIUS Plug-in
- Script Plug-in

Weitere Plug-ins stehen als Testversion zur Verfügung:

- System Monitor Plug-in
- Remote Server Configuration Plug-in
- Local Server Configuration Plug-in

Neue Konfigurations-Optionen

Die Konfigurationsmöglichkeiten der aktuellen Secure Enterprise Client Version 9.10 wurden in das Secure Enterprise Management-System abgebildet. Dazu gehören:

- Multi-Zertifikatskonfiguration (Erweiterte Zertifikatskonfiguration)
- Profil-Filter (Profil-Gruppenbildung)
- Budget Manager
- LAN Update
- Software Update-Liste

(Siehe hierzu auch das Dokument „What's New Secure Enterprise Client (Win32/64) Version 9.10“)

Insbesondere der Leistungsumfang des Client Configuration Plug-in wurde erweitert:

Konfiguration des Modemtyps

Die Auswahl des Modems kann direkt aus einer Listbox erfolgen oder frei editiert werden.

RSU Secret für Rollout und LAN Update (Remote Software Update)

Zusätzliche Sicherheit bei der Ersteinwahl. Der Benutzer bekommt ein „RSU-Secret“, das dessen eindeutige Authentisierung unabhängig von der Benutzer-ID gewährleistet.

Update-Listen bei Software-Verteilung

Update-Listen (Zusammenstellung der Download-Parameter) können nach verschiedenen Kriterien zusammengestellt werden. Weiter kann, abhängig vom Verbindungsmedium des Clients festgelegt werden, wie mit den zur Verfügung stehenden Updates umgegangen werden soll. Optionen: kein Update, erzwungener Update, interaktiver Update.

Zusätzlich unterstützte Datenbanken

MySQL ODBC Driver Version 5.1 und Microsoft SQL Server 2008.

Neue Features der Version 2.00 gegenüber Version 1.03

Neue Konfigurations-Optionen

Mit dem Secure Enterprise Management 2.0 können NCP Secure Enterprise Clients einschließlich der Enterprise-Versionen 9.03 administriert werden. Die Konfigurationsmöglichkeiten des Enterprise Clients wurden entsprechend in das Management-System übernommen.

Darüber hinaus sind in folgenden Plug-ins Neuerungen aufgenommen worden:

Client Configuration Plug-in

Parameter-Sperren für WLAN-Profile

Für WLAN-Profile kann über die Management-Console für jeden Parameter eine Parametersperre gesetzt werden (Vorlagen / WLAN-Profil / Sperren). Dadurch ist es möglich, die Update-Funktion "Nur gesperrte Parameter ändern" analog wie bei der Konfiguration der Zielsysteme einzusetzen.

Parameter-Sperren für EAP

Die Management-Console wurde hinsichtlich der EAP-Konfiguration um das Anlegen von Parametersperren für den Client erweitert.

Konfiguration für Hotspot-Anmeldung

Die Hotspot-Anmeldung kann auf einfache Weise in der Vorlage vorkonfiguriert werden.

Benutzer-Informationen

In einer speziellen Rubrik können in 5 Beschreibungsfeldern beliebige Benutzerdaten eingetragen werden (z. B. Name, Rufnummer). Die Felder können individuell beschriftet werden.

Benutzerberechtigung für "bekannte Netze"

Dem Benutzer können unabhängig von den übrigen Firewall-Einstellungen, Berechtigungen zum Einrichten von Friendly Networks zugewiesen werden,.

Optionen:

- Benutzer darf eigene "Bekannte Netze" hinzufügen
- Benutzer darf "Bekannte Netze" bearbeiten
- Benutzer darf "Bekannte Netze" löschen
- Durch den Benutzer hinzugefügte "Bekannte Netze" löschen

Firewall Plug-in

Benutzerspezifische Firewall-Regeln

Aus der Vorlage des Firewall Plug-ins können einer Benutzerkonfiguration neben frei editierbaren, benutzerspezifischen Firewall-Regeln weitere Firewall-Regeln zugewiesen werden; die nicht editierbar sind.

RADIUS Plug-in

Anpassung des RADIUS-Benutzernamens für externe Authentisierung

Um ggf. Benutzerkonfigurationen eines Active Directory oder LDAP Servers unverändert zu belassen, wurde die RADIUS-Konfiguration so modifiziert, dass ein konfigurierter Suffix oder Prefix des gruppenspezifischen RADIUS-Benutzernamens für die externe RADIUS-Authentisierung entfernt werden kann..