

NCP Secure Enterprise Management for Windows OS

New Features version 1.03 to 2.05

What's New

high security remote access

Disclaimer

Considerable care has been taken in the preparation and publication of this document, errors in content, typographical or otherwise may occur. NCP makes no representations or warranties with respect to the contents or use of this manual, and explicitly disclaims all expressed or implied warranties of merchantability or use for any particular purpose. Furthermore NCP reserves the right to revise this publication and to make amendments to the content, at any time, without obligation to notify any person or entity of such revisions and changes.

Trademarks

All trademarks or registered trademarks appearing in this manual belong to their respective owners.

Overview

New Features in Version 2.05 relative to Version 2.04	2
New Features in Version 2.04 relative to Version 2.03	4
New Features in Version 2.03 relative to Version 2.02	4
New Features in Version 2.02 Build 40 relative to Version 2.0	5
New features of version 2.00 relative to version 1.03.....	6

New Features in Version 2.05 relative to Version 2.04

Central Management of Enterprise Mac Clients

The NCP Secure Enterprise Management (SEM from version 2.05) provides a "Single Point of Administration" that supports the automation for rollout, commissioning and efficient use Secure Enterprise Mac Clients (from version 2.01). The Mac Client operating system platforms supported are Mac OS X 10.5 Leopard (Intel) and Mac OS X 10.6 Snow Leopard.

The Secure Enterprise Management (SEM from version 2.05) makes use of a VPN connection or LAN (in the corporate network) to automatically supply the Enterprise Clients with:

- Configuration updates
- Certificate updates
- Updates to the Update Client

Program Icon for the Management Console

The Management Console Program Icon has been changed. During installation of or update to the latest software version the icons in the task bar and in the Start menu are changed.

Support for MySQL Server 5.5.8

The Enterprise Management System supports the MySQL Server 5.5.8 database. When importing data from older versions of MySQL Server, note the following:

Number of Managed Units

The total number of Managed Units to be licensed in a Secure Management Server system is the sum of the number of Client entries plus the number of entries for Remote Servers. The units forming the central server serving the Configuration Plug-ins (Secure Server and HA Server) do not count towards determining the number of Managed Units to be licensed.

Creation and Distribution of Server Certificates with the PKI Enrollment Plug-in

The Secure Server automatically accepts Server Certificates that have been generated and distributed by the SEM (Secure Enterprise Management).

Issuing a new Server Certificate is initiated at the management system in the "Server Certificate Configuration", from where it is also sent to the corresponding VPN gateway after the Server Configuration has been created. In the course of this distribution the filename and PIN are removed from the Server Certificate configuration.

Renewing a Certificate

As with all other certificates, a Server Certificate can be renewed. This can be done in one of two ways:

- via the Server Configuration plug-in: -Server Configuration / Secure Server / Issued Certificates

- or via the PKI Enrollment plug-in: PKI Enrollment / Issued Certificates

Alternatively, certificates can be renewed by a script.

Displaying the Certificate

The certificate currently in use by the gateway is always displayed under the "Server Certificates" node.

For this gateway, the certificate issued with the PKI plug-in is displayed under the node "Issued Certificates".

The name of the linked Server Certificate Configuration is displayed under "Info / Certificate Usage".

Prerequisite

- 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

When authenticating via LDAP, LDAP via SSL with the standard port 636 can be used.

Prerequisite: that the LDAP server supports LDAP over SSL. (from RADIUS Plug-in version 2.05 Build 2)

Selection of the Windows Certificate Template via the PKI Enrollment Plug-in

If the Enterprise Management System is to receive the certificate from the integrated Windows Certification Authority, which Windows Certificate Template from the Microsoft CA is to be used can be defined, using the PKI Enrollment Plug-in, while the Certificate Template is being created.

When using a Windows CA, if no template name is entered in the Certificate Template at the SEM, then the Windows Certificate Template given in the ncppkisrv.conf configuration file is used. This file and the ncppkisrv.exe service are located on the Windows CA. There can only

be one Windows Certificate Template per configuration file. (from SEM 2.05 Build 7 with ncppkisrv.exe dated 01.12.2010)

Displaying CRL Information

Using the Server Configuration Plug-in the following CRL information is displayed in the configuration of the respective gateway:

- CRL Issuer
- Valid from ... to
- Number of entries

(from SEM 2.05 from Build 7 with Secure Server Configuration Plug-in 8.05)

Scripting Enhancements

Using scripts new parameter values can be assigned to Enterprise Client Profiles. The Profile settings under "DNS / Management" (primary and backup DNS Server and Domain Name) are addressed via a script under CDestination using the following properties:

- dns1
- dns2
- domainName

Permission for entering the Authentication Code

When configuring Administrator Groups (in the main menu under "Edit"), differing permissions can be allocated, per installed Plug-in Module, to the respective Administrator Groups

Which Administrator Group is allowed to enter or change the Authentication Code can be defined for "Client Configuration" and PKI Enrollment". This is required for the Update functions for Configuration and Certificate Distribution.

New Features in Version 2.04 relative to Version 2.03

Service Release for optimized Configuration/Management Sessions

New Features in Version 2.03 relative to Version 2.02

New Configuration Options

Server Configuration Plug-in

The server configuration plug-in v. 8.0 build 20 maps the functionality of the Secure Enterprise Server (SES) v. 8.0 build 116. The plug-in allows the distribution of server configurations to licensed v.8 secure servers, and the import of existing configurations of a

v.8 secure server. Secure Enterprise Management 2.03 must be installed in order to be able to use the server configuration plug-in!

Configuration and licensing of the server with the server configuration plug-in is identical to a configuration and licensing with the web interface of the server and can be carried out centrally via the plug-in or locally via the web interface.

Documentation regarding the server plug-in, and the import and export of configurations can be found in the SES Navigator, in the PDF 'SES Parameters'.

New Configuration Option during the Update Process

With the update of the management system from version 2.02 to version 2.03, the new client configuration plug-in 9.10 build 50 will be installed.

This will provide additional differentiation options during the update process for the management system, particularly for older client configurations. (Please see the description 'SEM Automatic Update' in the SEM Navigator.)

New Features in Version 2.02 Build 40 relative to Version 2.0

Optimized Plug-in distribution concept

The plug-in distribution concept for Secure Enterprise Management allows to manage all plug-ins on the central Management Server. This ensures that all console PCs will work with the same plug-ins at all times.

The following plug-ins will be assigned to Management Server 2.02:

- NCP_MgmPlugin_Console_Win32_202_017.exe [Management Console Plug-in]
- NCP_MgmPlugin_Client_Win32_910_40.exe [Client Configuration Plug-in]
- NCP_MgmPlugin_Firewall_Win32_201_9.exe [Firewall Plug-in]
- NCP_MgmPlugin_LicMgm_Win32_201_13.exe [License Management Plug-in]
- NCP_MgmPlugin_PKIMgr_Win32_201_16.exe [PKI Management Plug-in]
- NCP_MgmPlugin_Policy_Win32_201_7.exe [Endpoint Policy Plug-in]
- NCP_MgmPlugin_Radius_Win32_201_7.exe [RADIUS Plug-in]
- NCP_MgmPlugin_Script_Win32_201_2.exe [Script Plug-in]

The following plug-ins are available as test software:

- NCP_MgmPlugin_SysMon_Win32_201_7.exe [System Monitor Plug-in]
- NCP_MgmPlugin_RemSrv_Win32_702_9.exe [Remote Server Configuration Plug-in]
- NCP_MgmPlugin_SrvCfg_Win32_800_12.exe [Server Configuration Plug-in]

New Configuration Options

The Enterprise Client's version 9.10 new configuration options have been adopted for the management system accordingly. They include:

- Multi Certificate Configuration
- Profile Filters (Profile Group Creation)
- Budget Manager
- LAN Update
- Software Update List

(With regard to these features see "What's New Secure Enterprise Client (Win 32/64) version 9.10)

Especially the Client Configuration plug-in was optimized.

Client Configuration Plug-in

Configuring the Modem Type

Under Modem in the profile settings, a particular modem can be selected either by choosing a type from the list box or editing the field as you wish.

RSU Secret for Rollout and LAN Update

Additional security for the first dial-in. The RSU Secret ensures that the user is unambiguously authenticated, no matter what the RSU ID.

Update Lists and Software Distribution

With Management System 2.02, update lists can be compiled based on different criteria.

Under "Software Management / Software Update Lists" in the console menu, the user can specify how the available updates should be handled, no matter what the client's connection medium:

- whether the update should not be run
- whether the update is mandatory, with no enquiry or
- whether and how often the user is asked

New supported Databases

MySQL ODBC Driver Version 5.1 and Microsoft SQL Server 2008.

New features of version 2.00 relative to version 1.03

New Configuration Options

Secure Enterprise Management 2.0 provides administration rights for NCP Secure Enterprise Clients including Enterprise versions 9.03. All configuration options of the Enterprise Clients were adopted in the management system accordingly. Furthermore, the following new options have been added:

Client Configuration Plug-in

Parameter Locks for WLAN Profiles

For each parameter, WLAN profile locks can be set up via Management Console (Templates / WLAN Profile / Locks). It is therefore possible to apply the update function 'Only update locked parameters' as with the configuration of destination systems.

Parameter Locks for EAP

A function for the generation of parameter lock-outs for EAP client configuration was added in Management Console.

Configuration for Hotspot Login

It is easier to preconfigure hotspot logins in the template for hotspot configuration.

User Information

The section 'Configuration / User Information' has been added in the client plug in. 5 description fields are provided, where any information regarding the user can be entered (e.g. name, telephone number).

User Access Rights for 'Known Networks'

The following rights have been added in the client plug-in under 'Template / Restrictions / Firewall / Known Networks':

- User is authorized to add own 'Known Networks'
- User is authorized to edit own 'Known Networks'
- User is authorized to delete own 'Known Networks'
- Deleting 'Known Networks' added by the user

Firewall Plug-in

User specific Firewall Rules

Firewall rules can be assigned to a user configuration via the firewall plug-in template. Afterwards, these rules can not be altered. In addition, user specific firewall rules may be added to a user configuration, which remain editable.

RADIUS Plug-in

RADIUS User Name Customization for External Authorization

RADIUS configuration allows the removal of a configured suffix or prefix for the group specific RADIUS user name for external RADIUS authentication. User configurations for an Active Directory or LDAP server can therefore remain unchanged.