



## RSA SecurID Ready Implementation Guide

Last Modified: August 25, 2005

### Partner Information

---

Product Information	
Partner Name	NCP engineering GmbH
Web Site	<a href="http://www.ncp.de/">www.ncp.de/</a>
Product Name	NCP Secure Communications Products
Version & Platform	NCP Secure Enterprise Client v8.11 NCP Secure Enterprise Server v6.09 NCP Secure Entry Client v8.21
Product Description	<p><a href="#">NCP Secure Enterprise Servers</a> represent the central components for the Secure Enterprise (or Entry) Clients. They supply the platform for all forms of access to the corporate network from distributed standalone PCs and branch office networks. Designed for performance in larger remote access projects involving several thousand users.</p> <p><a href="#">NCP Secure Enterprise Client</a> software sets new standards and integrates all technologies that contribute to achieving maximum security, universality, administrative control, and profitability (TCO), in remote access projects. Stationary PC and mobile PC workstations are integrated as equal participants in the corporate network over public networks and beyond. Teleworkers work in their accustomed manner as they do at office workstations. All LAN applications and resources are available to them 1:1 on their remote PC.</p> <p><a href="#">NCP Secure Entry Client</a> product line is a subset of the Secure Enterprise Solution. The NCP Secure Entry Client communicates with VPN gateways supplied by a wide range of manufacturers, on the basis of the IPSec standard. This involves client software that can be used as an alternative to the software clients offered on the market in the firewall and router area. The Secure Entry Client is differentiated from other IPSec clients through its feature set and through its software architecture.</p>
Product Category	Perimeter Defense (Firewalls, VPNs& Intrusion Detection)

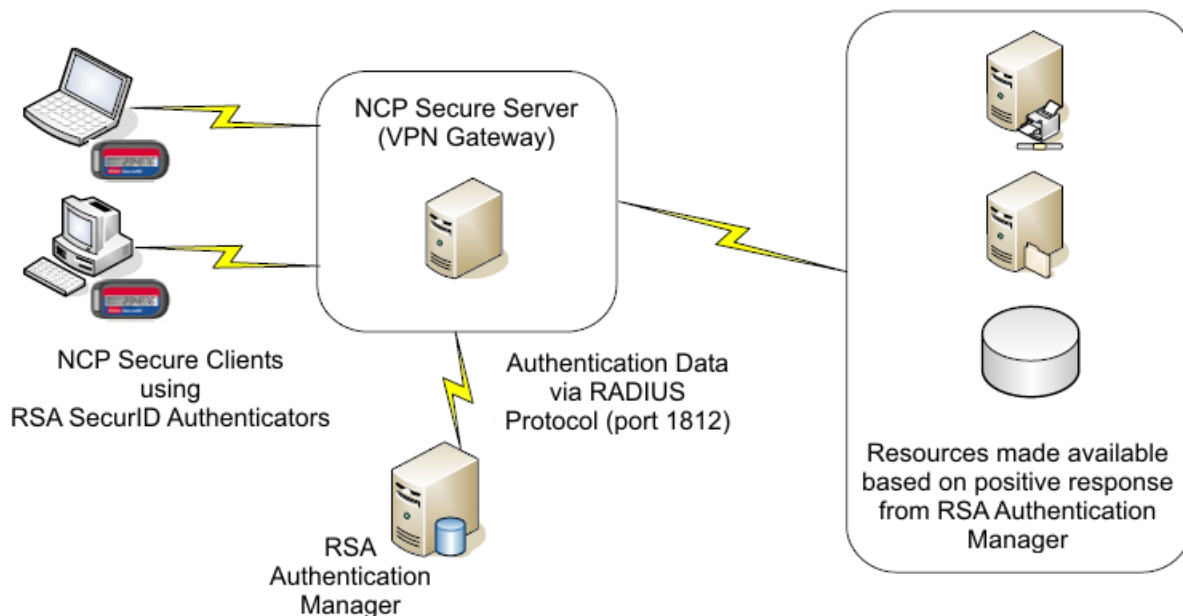


## Solution Summary

The [NCP Secure Enterprise Solution](#) is a comprehensive Remote Access solution on the highest technical level. It offers all components that are required for introduction, implementation, operation, management, and serviceability. Communications & security technologies combine in a unique manner to form an integral whole.

The Secure Enterprise/Entry Clients are used to establish secure remote access or VPN connections to remote access/VPN gateways, these can be either NCP Secure Servers or other vendor's gateways. This document will cover NCP Secure Clients establishing connections to NCP Secure Servers. During the authentication phase, the clients can be configured to use RSA SecurID Authenticators as a means to authenticate. The Secure Server relays the authentication request to the RSA Authentication Manager via the RADIUS protocol, and then the user is either permitted or denied based on the response.

Partner Integration Overview	
Authentication Methods Supported	RADIUS
List Library Version Used	N/A
RSA Authentication Manager Name Locking *	N/A
RSA Authentication Manager Replica Support *	N/A
Secondary RADIUS Server Support	Yes, secondary OTP server can be configured
Location of Node Secret on Agent	None stored
RSA Authentication Agent Host Type	Communication Server
RSA SecurID User Specification	Designated Users
RSA SecurID Protection of Administrative Users	No
RSA Software Token API Integration	No
Use of Cached Domain Credentials	No



# Product Requirements

---

## Secure Server Requirements:

The Secure Server can fulfill different roles, ranging from (direct dial-in) access server to full blown PKI enabled VPN gateway. Depending on which role the gateway fulfills, the platform requirements differ accordingly. The requirements below list what is required for a typical Secure Server acting as PKI-enabled VPN gateway

<b>Partner Product Requirements: NCP Secure Server</b>	
<b>CPU</b>	Minimum: Pentium III 500Mhz (Data throughput of app. 2 Mbit can be realized for each 150 MHz (incl. 128-bit / 448-bit symmetric encryption)
<b>Memory</b>	64 MB RAM for each 250 concurrently usable tunnels
<b>Storage</b>	Minimum: 50 Mb

<b>Operating System</b>	
<b>Platform</b>	<b>Required Patches</b>
Windows NT 4.0	Service Pack 5 or higher
Windows 2000	
Windows 2003	
Linux	
Solaris	

## Secure Client Requirements:

The Secure Client is available for a number of different platforms, ranging from PDAs with PocketPC to Desktops with Windows XP, as well as Linux based platforms. The hardware requirements differ depending on what platform is chosen.

<b>Operating System</b>	
<b>Platform</b>	<b>Required Patches</b>
Windows 98 (SE) and Windows ME	
Windows NT 4.0	Service Pack 5 or higher
Windows 2000	
Windows XP	
Windows CE 3.0 and above	(i.e. PocketPC 2002 )
Windows CE net 4.2 and above	(i.e. Windows Mobile 2003 for PocketPC)
Linux	(kernel 2.4.2 and higher) (i.e. RedHat or SuSE v8.0 and above)

## Agent Host Configuration

---

To facilitate communication between the NCP Secure Server and the RSA Authentication Manager / RSA SecurID Appliance, an Agent Host record must be added to the RSA Authentication Manager database. The Agent Host record identifies the NCP Secure Server within its database and contains information about communication and encryption.

To create the Agent Host record, you will need the following information.

- Hostname
- IP Addresses for all network interfaces
- RADIUS Secret

When adding the Agent Host Record, you should configure the NCP Secure Server as a Communications Server. This setting is used by the RSA Authentication Manager to determine how communication with the NCP Secure Server will occur.

---

 **Note: Hostnames within the RSA Authentication Manager / RSA SecurID Appliance must resolve to valid IP addresses on the local network.**

---

Please refer to the appropriate RSA Security documentation for additional information about Creating, Modifying and Managing Agent Host records.

# Partner Authentication Agent Configuration

## Before You Begin

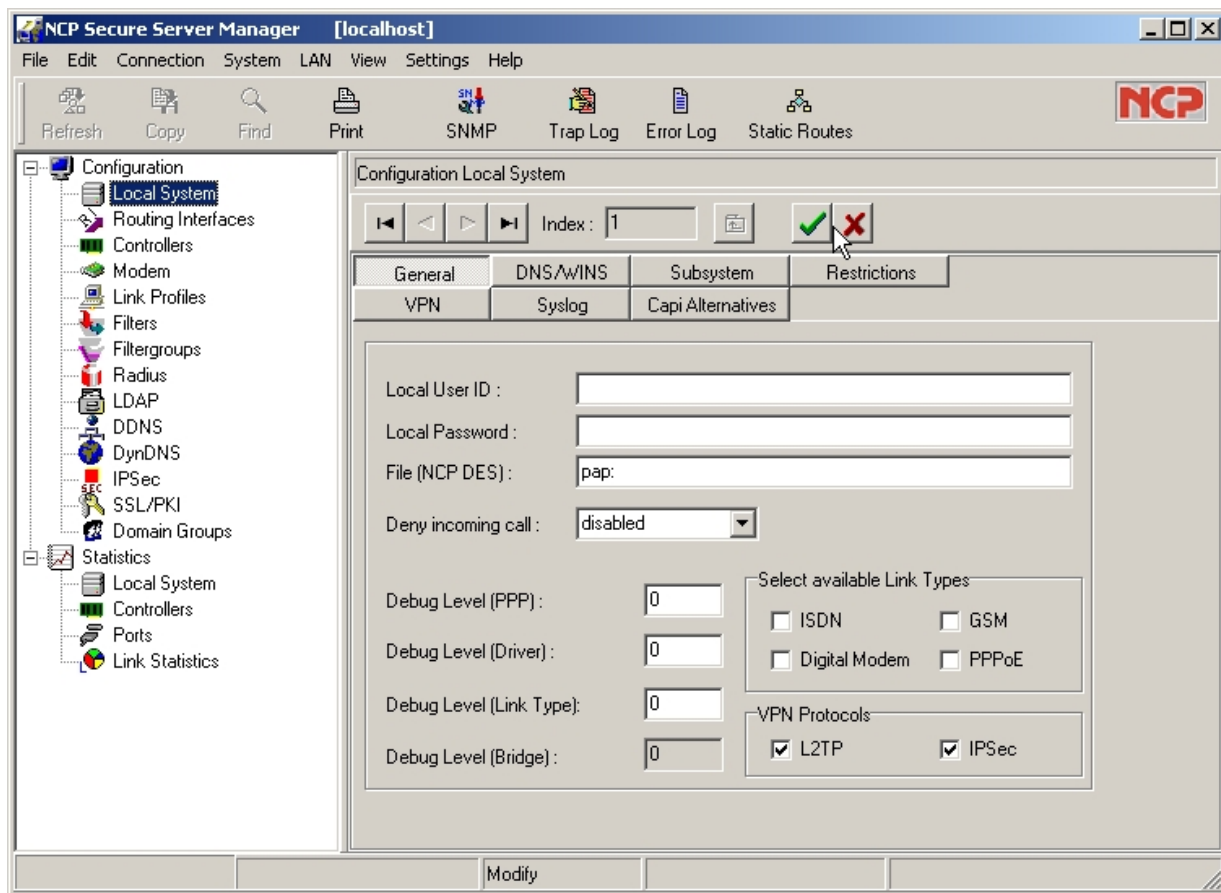
This section provides instructions for integrating the partners' product with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All vendor products/components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

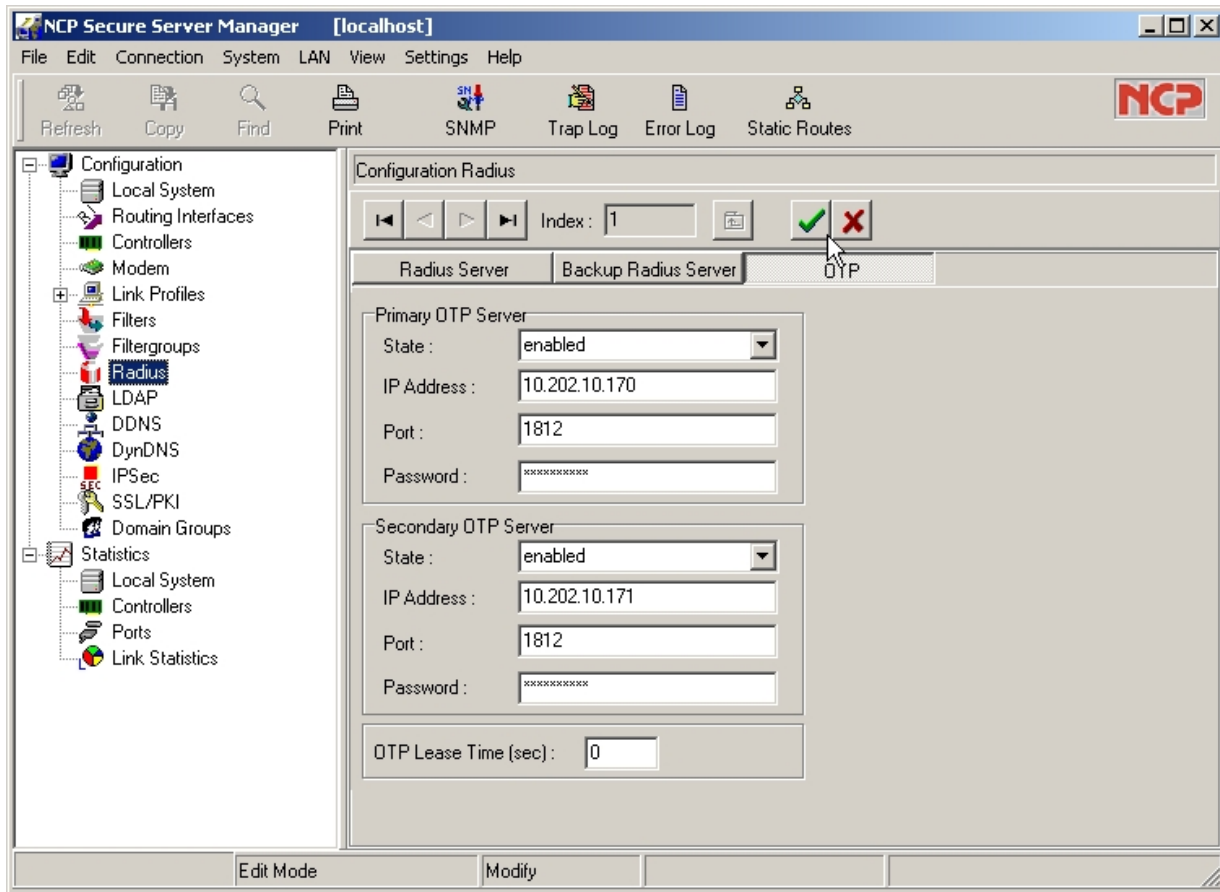
## Documenting the Solution

The Secure Server is going to be the Authentication Agent. The Client is going to attempt to establish a connection and during the authentication phase using the RSA SecurID pass authentication credentials to the Secure Server. The Secure Server in turn has to pass these credentials to the RSA Authentication Manager. In order to do this, the Secure Server needs to be aware of the use of the RSA Authentication Manager. The first step to do is to define the use of PAP when relaying the credentials to the RSA Authentication Manager.



Simply enter in the value "pap:" (without the quotation marks), as shown in the screenshot above, in the field for **File (NCP DES)**. This configures the Secure Server to pass the information on to the RSA Authentication Manager using PAP instead of CHAP (the latter not supported by the RSA Authentication Manager)

Next step is to define the use of the RSA Authentication Manager. This is done by configuring the use of an OTP (One Time Password) service, in the RADIUS section of the configuration. Two OTP servers or RSA Authentication Managers can be defined here, a primary one, and a secondary one in the event the primary cannot be reached. See screenshot below.



**State:** The state of the OTP Server can be switched to active or inactive. It must be switched to active when the used in combination with the RSA Authentication Manager.

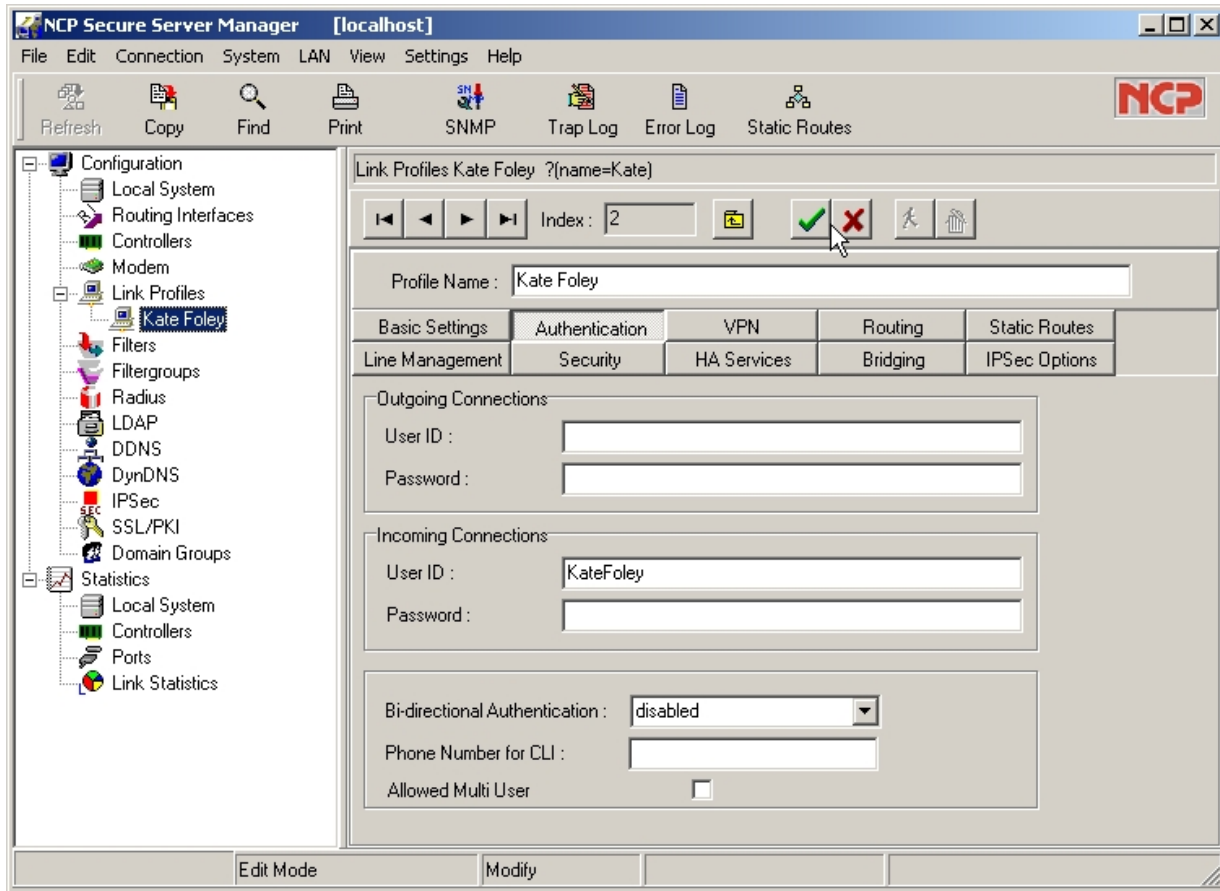
**IP Address:** The IP address of the RSA Authentication Manager

**Port:** The port that the RSA Authentication Manager's RADIUS service is listening on; default 1812.

**Password:** This is the Password or Encryption Key (see Agent Host configuration) needed for this Agent Host to communicate with the RSA Authentication Manager: see the RADIUS Secret earlier on in this document. This value must match, and is case sensitive.

## Configuring a user on the Secure Server

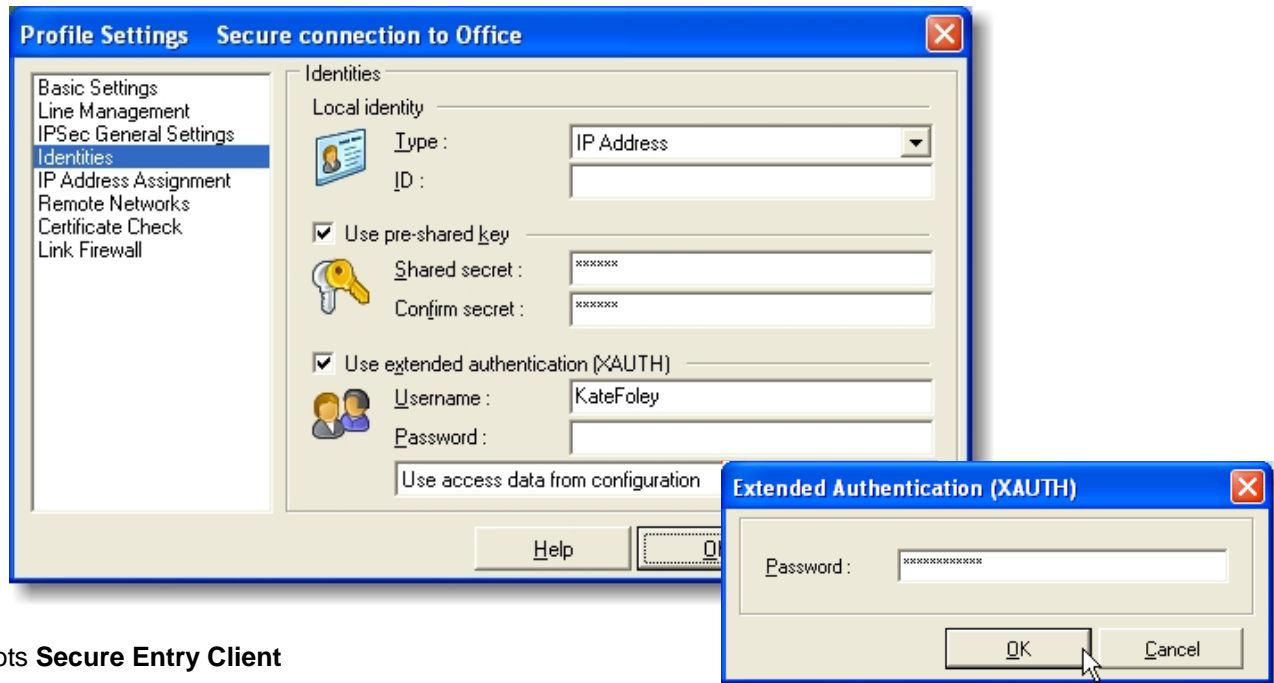
The configuration of a user proceeds just as any other configuration, with the only difference being that the Password field is left blank. The Secure Server will then automatically query configured RADIUS/OTP services to validate the User ID and Passcode/Tokencode the client presents.



Please refer to the appropriate NCP Secure Server/Users documentation for additional information about Creating, Modifying and Managing Link Profiles/Users

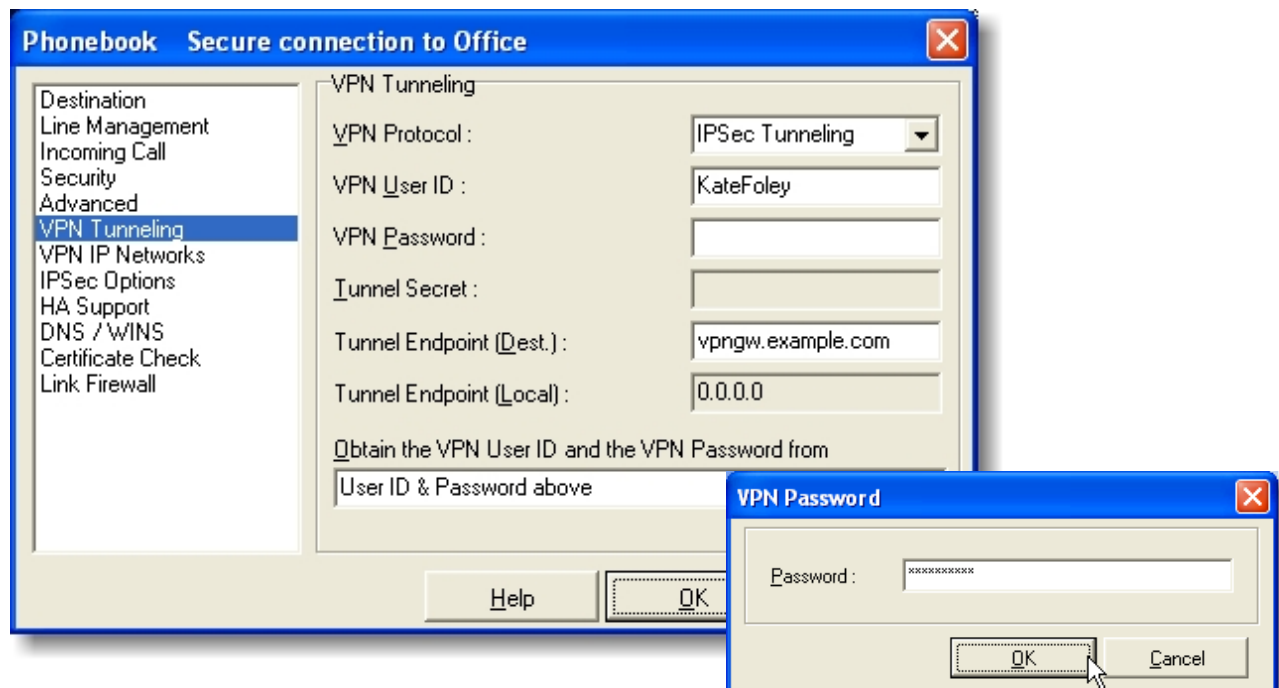
## Configuring the Secure Clients

In order to use the Secure Clients (Enterprise or Entry) in combination with the RSA SecurID, one simply needs to leave the password fields empty. The rest of the configuration is the same as any other configuration; please see appropriate documentation regarding the setup. By leaving the value for the passwords blank, one is prompted for the password prior to setting up a connection. This then is the opportunity to enter in the Passcode/Tokencode that will be relayed to the RSA Authentication Manager by the Secure Server.



Screenshots **Secure Entry Client**

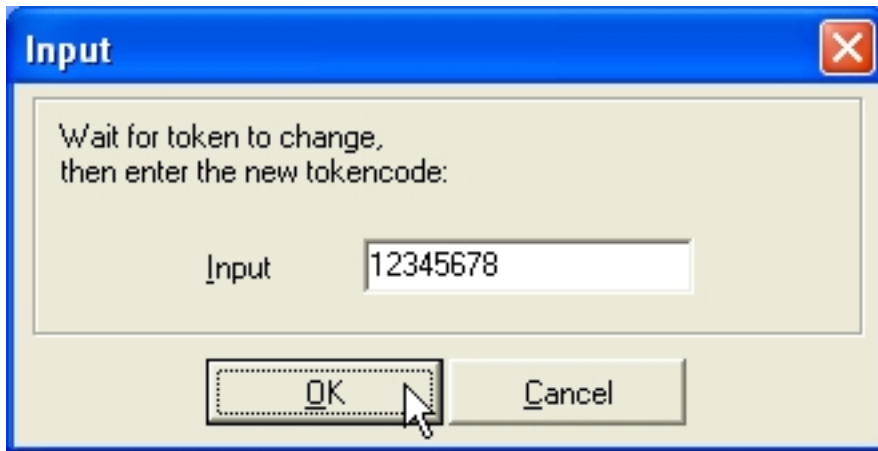
 **Note:** The (XAUTH) Password field has been left blank in the Profile Settings.



Screenshots **Secure Enterprise Client**

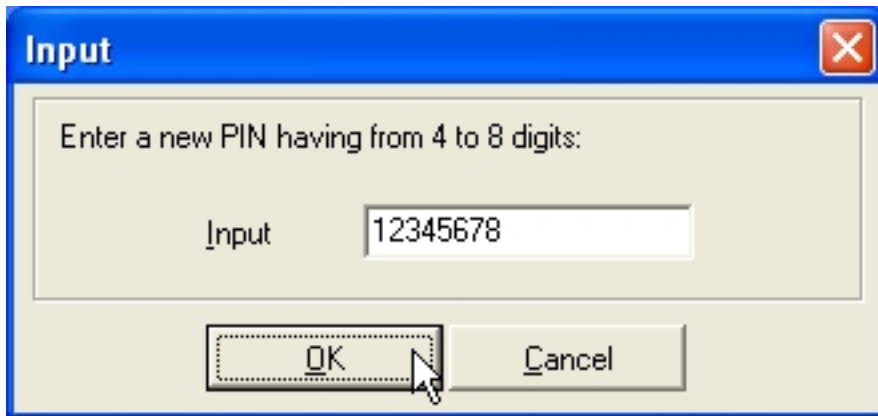
 **Note:** The VPN Password field has been left blank in the Phonebook entry.

Next Tokencode:



An "Input" dialog box with a blue title bar and a close button (X) in the top right corner. The main area contains the text "Wait for token to change, then enter the new tokencode:". Below this text is a text input field with the value "12345678". At the bottom of the dialog are two buttons: "OK" and "Cancel". A mouse cursor is hovering over the "OK" button.

NEW PIN:



An "Input" dialog box with a blue title bar and a close button (X) in the top right corner. The main area contains the text "Enter a new PIN having from 4 to 8 digits:". Below this text is a text input field with the value "12345678". At the bottom of the dialog are two buttons: "OK" and "Cancel". A mouse cursor is hovering over the "OK" button.

# Certification Checklist

Date Tested: August 25, 2005

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	6.0	Windows 2000 Advanced Server
Secure Server	6.09	Windows 2000
Secure Entry Client	8.21	Windows XP
Secure Enterprise Client	8.11	Linux

Mandatory Functionality			
RSA Native Protocol		RADIUS Protocol	
<b>New PIN Mode</b>			
Force Authentication After New PIN	N/A	Force Authentication After New PIN	✓
System Generated PIN	N/A	System Generated PIN	✓
User Defined (4-8 Alphanumeric)	N/A	User Defined (4-8 Alphanumeric)	✓
User Defined (5-7 Numeric)	N/A	User Defined (5-7 Numeric)	✓
User Selectable	N/A	User Selectable	✓
Deny 4 and 8 Digit PIN	N/A	Deny 4 and 8 Digit PIN	✓
Deny Alphanumeric PIN	N/A	Deny Alphanumeric PIN	✓
<b>PASSCODE</b>			
16 Digit PASSCODE	N/A	16 Digit PASSCODE	✓
4 Digit Password	N/A	4 Digit Password	✓
<b>Next Tokencode Mode</b>			
Next Tokencode Mode	N/A	Next Tokencode Mode	✓
<b>Load Balancing / Reliability Testing</b>			
Failover (3-10 Replicas)	N/A	Failover	✓
Name Locking Enabled	N/A	Name Locking Enabled	
No RSA Authentication Manager	N/A	No RSA Authentication Manager	✓
<b>Additional Functionality</b>			
<b>RSA Software Token API Functionality</b>			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
User Selectable	N/A	User Selectable	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A
<b>Domain Credential Functionality</b>			
Determine Cached Credential State	N/A	Determine Cached Credential State	
Set Domain Credential	N/A	Set Domain Credential	
Retrieve Domain Credential	N/A	Retrieve Domain Credential	

SWA / PAR

✓ = Pass ✗ = Fail N/A = Non-Available Function

## Known Issues

---

There are no known issues, please contact [info@ncp.de](mailto:info@ncp.de) if you have a question or query.