NCP engineering GmbH
NCP Secure Communication Products

RSA SecurID Ready Implementation Guide

Last Modified: January 15, 2014

Partner Information

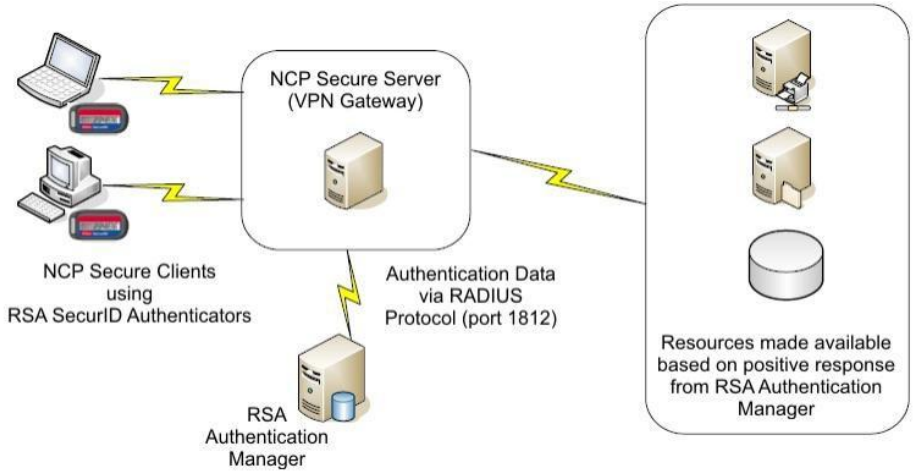
Product Information	
Partner Name	NCP engineering GmbH
Web Site	www.ncp-e.com
Product Name	NCP Secure Communication Products
Version & Platform	NCP Secure Enterprise Client v9.32 NCP Secure Enterprise Server v8.11 NCP Secure Entry Client v9.32
Product Description	**NCP Secure Enterprise Servers** represent 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. **NCP Secure Enterprise Client** 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. **NCP Secure Entry Client** 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.

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.

RSA Authentication Manager supported features NCP Secure Enterprise Server v8.11	
RSA SecurID Authentication via Native RSA SecurID Protocol	No
RSA SecurID Authentication via RADIUS Protocol	Yes
On-Demand Authentication via Native SecurID Protocol	No
On-Demand Authentication via RADIUS Protocol	Yes
Risk-Based Authentication	No
Risk-Based Authentication with Single Sign-On	No
RSA Authentication Manager Replica Support	No
Secondary RADIUS Server Support	Yes
RSA SecurID Software Token Automation	No
RSA SecurID SD800 Token Automation	No
RSA SecurID Protection of Administrative Interface	No



Authentication Agent Configuration

Authentication Agents are records in the RSA Authentication Manager database that contain information about the systems for which RSA SecurID authentication is provided. All RSA SecurID-enabled systems require corresponding Authentication Agents. Authentication Agents are managed using the RSA Security Console.

The following information is required to create an Authentication Agent:

- Hostname
- IP Addresses for network interfaces

Set the Agent Type to "Standard Agent" when adding the Authentication Agent. This setting is used by the RSA Authentication Manager to determine how communication with NCP Secure Server will occur.

A RADIUS client that corresponds to the Authentication Agent must be created in the RSA Authentication Manager in order for NCP Secure Server to communicate with RSA Authentication Manager. RADIUS clients are managed using the RSA Security Console.

The following information is required to create a RADIUS client:

- Hostname
- IP Addresses for network interfaces
- RADIUS Secret

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 documentation for additional information about creating, modifying and managing Authentication Agents and RADIUS clients.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the NCP Secure Communication Products with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

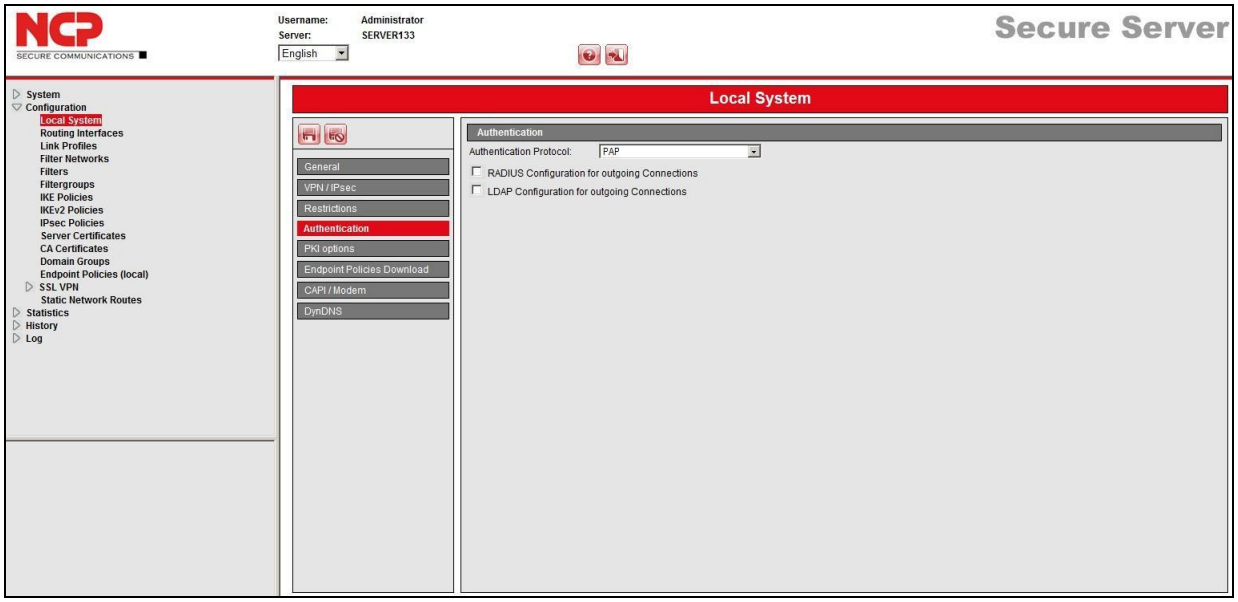
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All Secure Communications Products components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

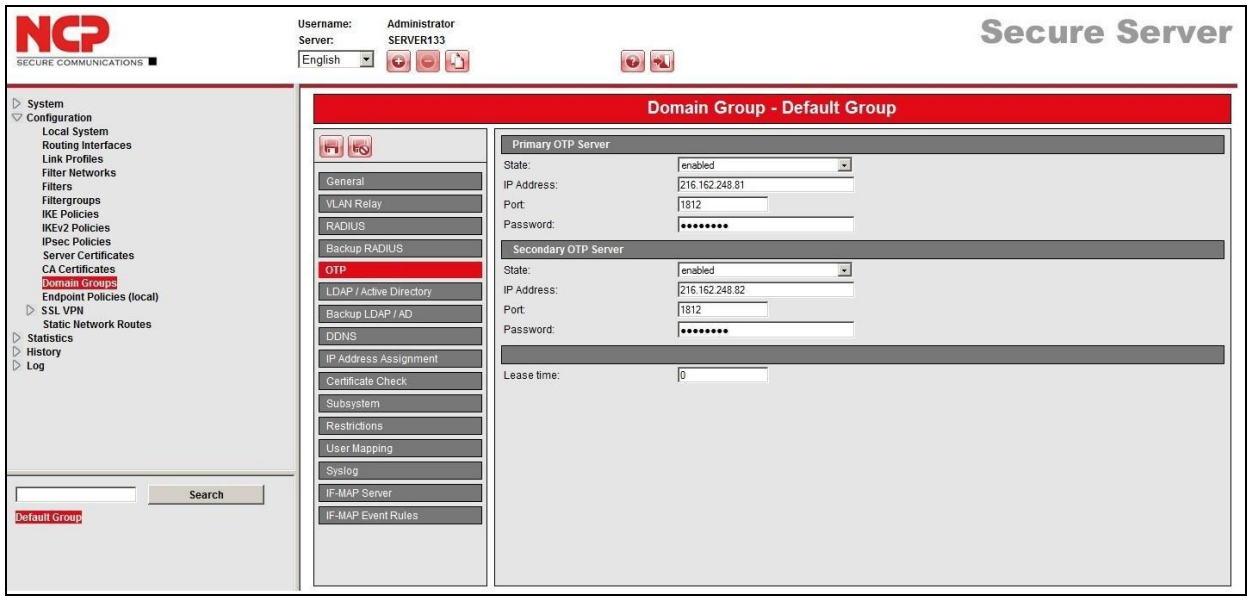
Documenting the Solution

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.

1. Define the use of PAP when relaying the credentials to the RSA Authentication Manager. Select the value **PAP**, in the field for Authentication Protocol. This configures the Secure Server to pass the information on to the RSA Authentication Manager using PAP instead of CHAP.



2. Next 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.



3. Complete the **State**, **IP Address**, **Port**, and **Password** fields.

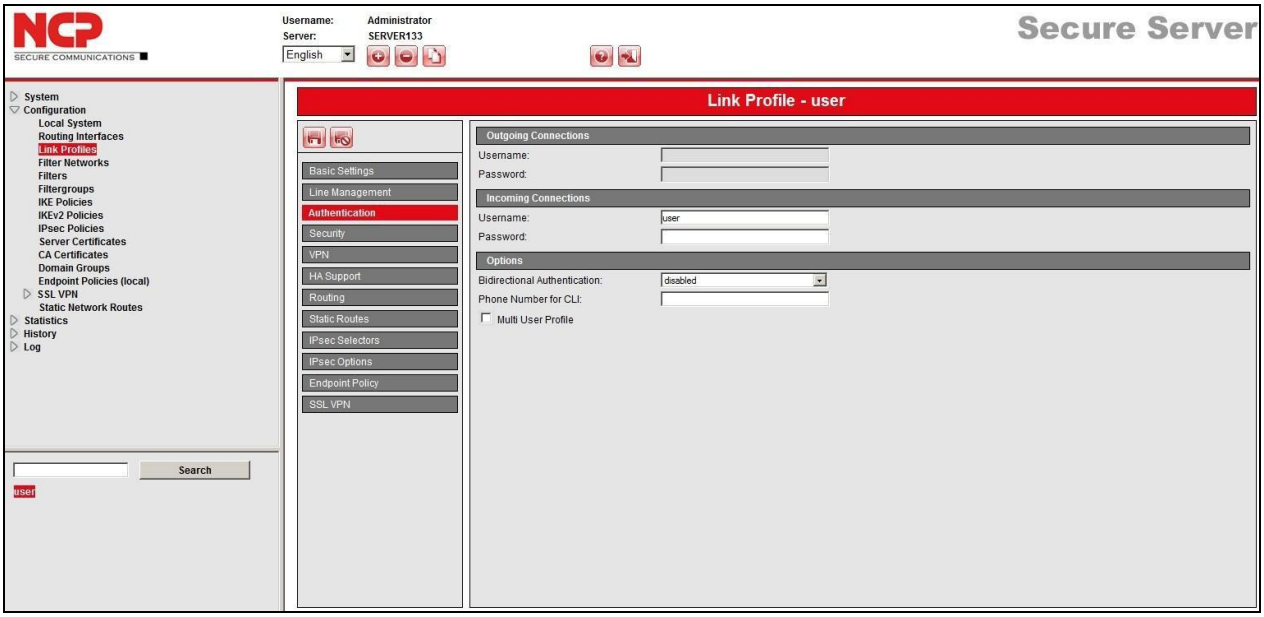
State: The state of the OTP Server can be switched to active or inactive. It must be switched to active when the used in combination with the RSA Authentication Manager.

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 Authentication Agent 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 in 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.

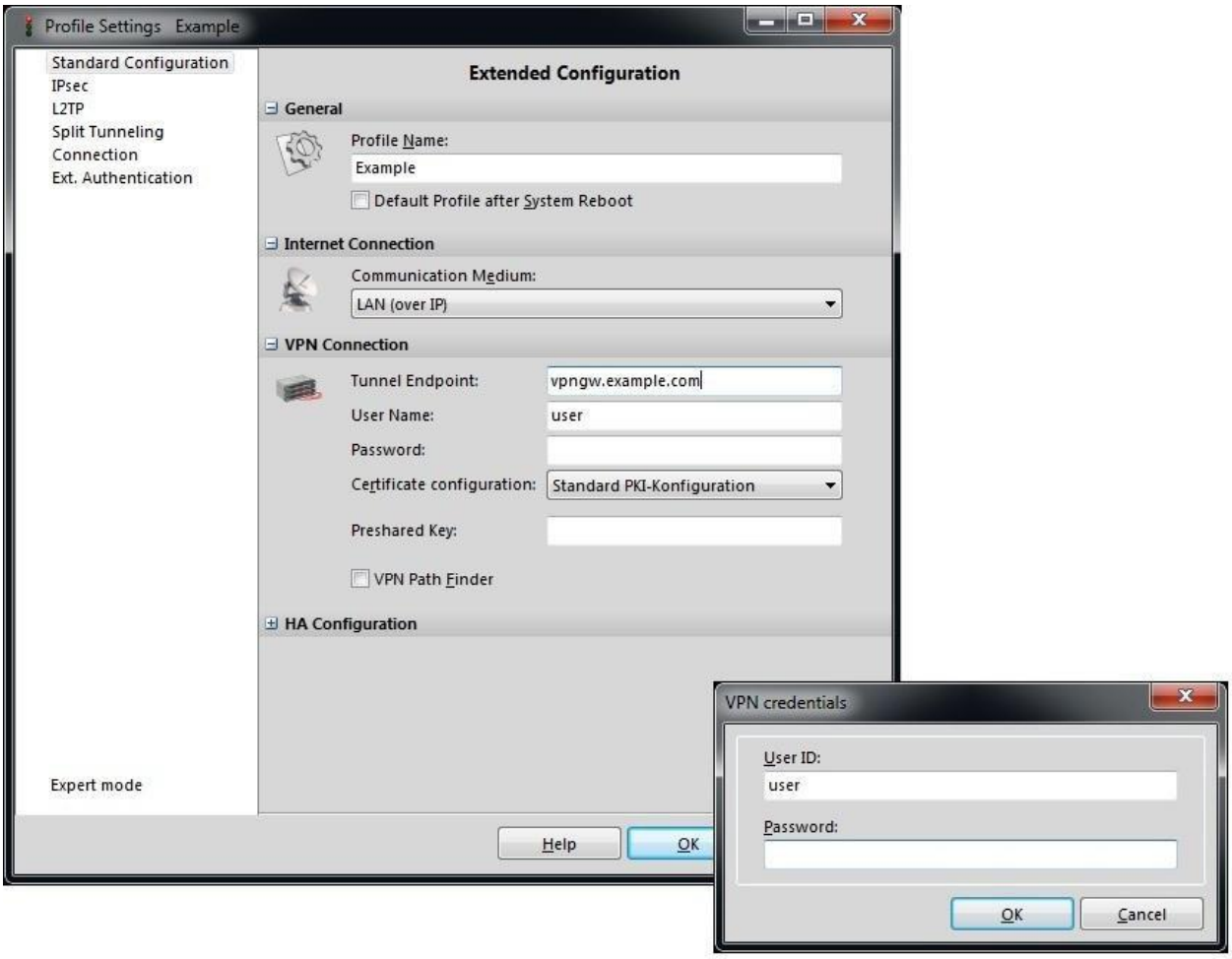


Note: Refer to the appropriate NCP Secure Server documentation for additional information about Creating, Modifying and Managing Link Profiles/Users.

Configuring the Secure Clients

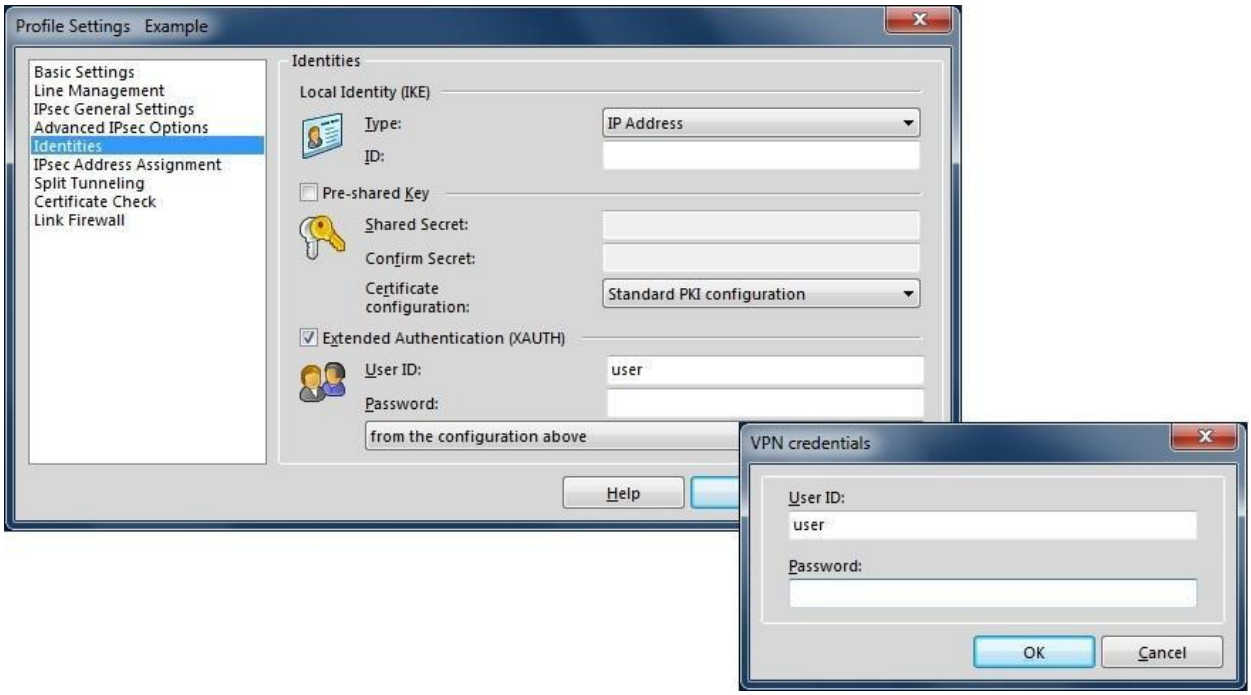
In order to use the Secure Clients (Enterprise or Entry) in combination with the RSA SecurID, one simply needs to leave the password fields empty. The rest of the configuration is the same as any other configuration; please see appropriate documentation regarding the setup. By leaving the value for the 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.

NCP Secure Enterprise Client



Note: The VPN Password field has been left blank in the Profile Settings.

NCP Secure Entry Client

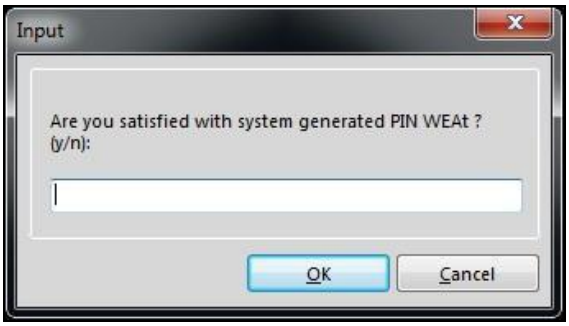


Note: The (XAUTH) Password field has been left blank in the Profile Settings.

RSA SecurID Login Screens

User-defined New PIN:

System-generated New PIN:



Next Tokencode:

Certification Checklist for RSA Authentication Manager

Date Tested: January 15, 2014

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.0	Virtual Appliance
Secure Server	8.11	Windows Server 2008 R2
Secure Entry Client	9.32	Windows 7
Secure Enterprise Client	9.32	Windows 7

Mandatory Functionality			
RSA Native Protocol		**RADIUS Protocol**	
New PIN Mode			
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)	✓
Deny 4 and 8 Digit PIN	N/A	Deny 4 and 8 Digit PIN	✓
Deny Alphanumeric PIN	N/A	Deny Alphanumeric PIN	✓
Deny PIN Reuse	N/A	Deny PIN Reuse	✓
Passcode			
16-Digit Passcode	N/A	16-Digit Passcode	✓
4-Digit Fixed Passcode	N/A	4-Digit Fixed Passcode	✓
Next Tokencode Mode			
Next Tokencode Mode	N/A	Next Tokencode Mode	✓
On-Demand Authentication			
On-Demand Authentication	N/A	On-Demand Authentication	✓
On-Demand New PIN	N/A	On-Demand New PIN	✓
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	N/A	Failover	✓
No RSA Authentication Manager	N/A	No RSA Authentication Manager	✓

GLS / PAR

✓ = Pass ✗ = Fail N/A = Not Applicable to Integration