NCP

SECURE COMMUNICATIONS

Connecting an iOS Device to a NCP Secure VPN Server

As of July 2011
version 1.0

Easy Guide

high security remote access

Network
Communications
Products engineering

USA:

NCP engineering, Inc.
444 Castro Street, Suite 711
Mountain View, CA 94041
Tel.: +1 (650) 316-6273
Fax: +1 (650) 251-4155

Germany:

NCP engineering GmbH
Dombuehler Str. 2
D-90449 Nuremberg
Tel.: +49 (911) 9968-0
Fax: +49 (911) 9968-299

Internet

http://www.ncp-e.com

Email

info@ncp-e.com

Support

NCP offers support for all international users by means of Fax and Email.

Email Addresses

helpdesk@ncp-e.com	(English)
support@ncp-e.com	(German)

Fax

+1 (650) 251-4155	(USA)
+49 (911) 9968-458	(Europe)

When submitting a support request, please include the following information:

- exact product name
- serial number
- version number
- an accurate description of your problem
- any error message(s)

Copyright

While considerable care has been taken in the preparation and publication of this manual, errors in content, typo-graphical or otherwise, may occur. If you have any comments or recommendations concerning the accuracy, then please contact NCP. 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 suitability of use for any particular purpose.
Furthermore, NCP reserves the right to revise this publication and to make amendments to the contents, at any time, without obligation to notify any person or entity of such revisions or changes. This manual is the sole property of NCP and may not be copied for resale, commercial distribution or translated to another language without the express written permission of NCP engineering GmbH.
All trademarks or registered trademarks appearing in this manual belong to their respective owners.

Contents

1. Introduction 4

2. Installation of the Secure VPN Server 4

2.1. Virtual VPN Network........ 4

2.2. Installing a Windows VPN Server........ 5

2.3. Installing a Linux VPN Server 5

3. First login to configuration web interface 5

4. Basic Configuration 6

5. Set up DNS Server and IP address pool........ 6

6. Creating a local IPsec Link Profile........ 8

7. Create connection on iOS Device........ 9

8. Active Directory Authentication with LDAP 10

1. Introduction

Welcome to the Easy Guide "Connecting an iOS Device to a NCP Secure VPN Server".

The Easy Guides are meant to provide an easy step by step installation guide to achieve a special VPN setup in less than 20 pages. If you need more information about how a VPN works or a more detailed description how to set a NCP Secure VPN Server up, please have a look at the Quick Configuration Guide for Secure VPN Server or the manual of the Secure VPN Server.

Please note that we also offer a wide range of easy to use VPN Clients for different operating systems (like Windows 7) and support the native IPsec client on iOS devices like the iPhone and iPad or the native L2TP over IPsec Client on Android devices. For more Information please visit us at http://www.ncp-e.com .

If you should encounter any error in this document, if you have any suggestions for improvement or if you have any trouble setting up the scenario, please send an email to easyguide@ncp-e.com.

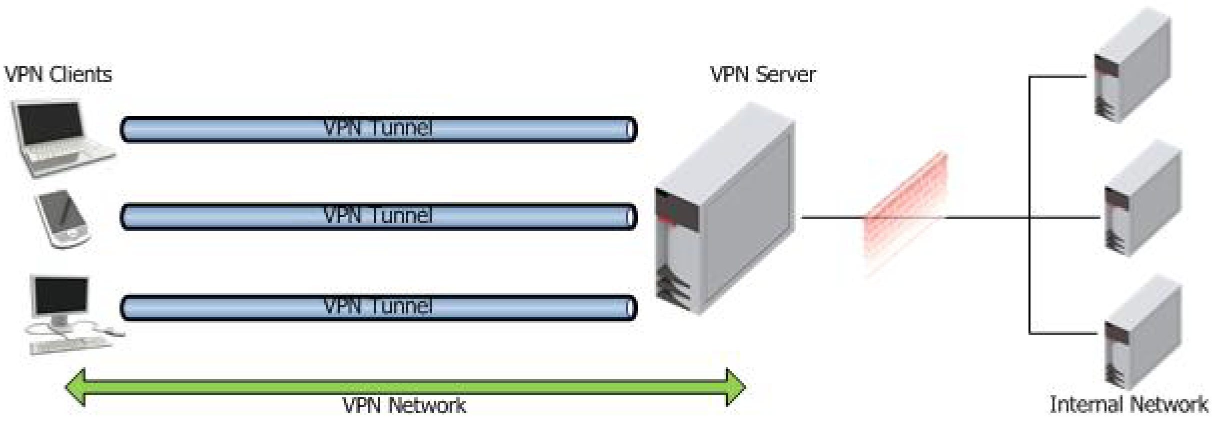
2. Installation of the Secure VPN Server

We provide a 30 day test version of the Secure VPN Server for Windows and Linux operating systems which is only limited to 5 concurrent connections.

To get a test version please write an email to sales@ncp-e.com or register on our web site at https://www.ncp-e.com/en/service/login/userregistration.html?no_cache=1

2.1. Virtual VPN Network

Upon installation each VPN server requests a virtual IP address. The virtual VPN network is shared between the VPN Server and the VPN Clients. Effectively the VPN Server acts as a router for the virtual network and thus the routes in your network have to be adopted accordingly.



Let's look at a practical example for this:

The virtual IP address of the server is set to 192.168.100.1 in a class c network (netmask 255.255.255.0). Each VPN Client will get an IP address from the same IP range. For example a VPN client will get the IP address 192.168.100.150.

If the VPN connection is established and your system tries to connect to your internal mail server that resides in a 192.168.200.x network, it will see an incoming connection request from the IP address 192.168.100.150. The mail server (or your central router) has to know where to route the 192.168.100.x network to and that is to the VPN Gateway respectively the internal IP address of the VPN Gateway on your LAN.

The VPN Server has to be reachable from the Internet for the following ports:
UDP 500 (IKE), UDP 4500 (NAT-T), IP Prot. 50 (ESP)

2.2. Installing a Windows VPN Server

The prerequisite for installing the VPN Server on a Windows system is the SNMP Service of Windows installed on that system. In Windows Server System starting from Windows 2008 you can find the SNMP Service in the list of Features that can be installed.

After installing the SNMP service start the installation package and select a user defined installation. You will be asked for the virtual IP address of the VPN Server (see section Virtual VPN Network). After a reboot the installation of the VPN server is complete.

2.3. Installing a Linux VPN Server

The installation package for Linux comes as an executable shell script installation. Just transfer the installation package to your Linux system, make the file executable and start the script as root. You will be guided through the installation by the script. Make sure to assign a proper virtual IP address to the server as described in the section "Virtual VPN Network".

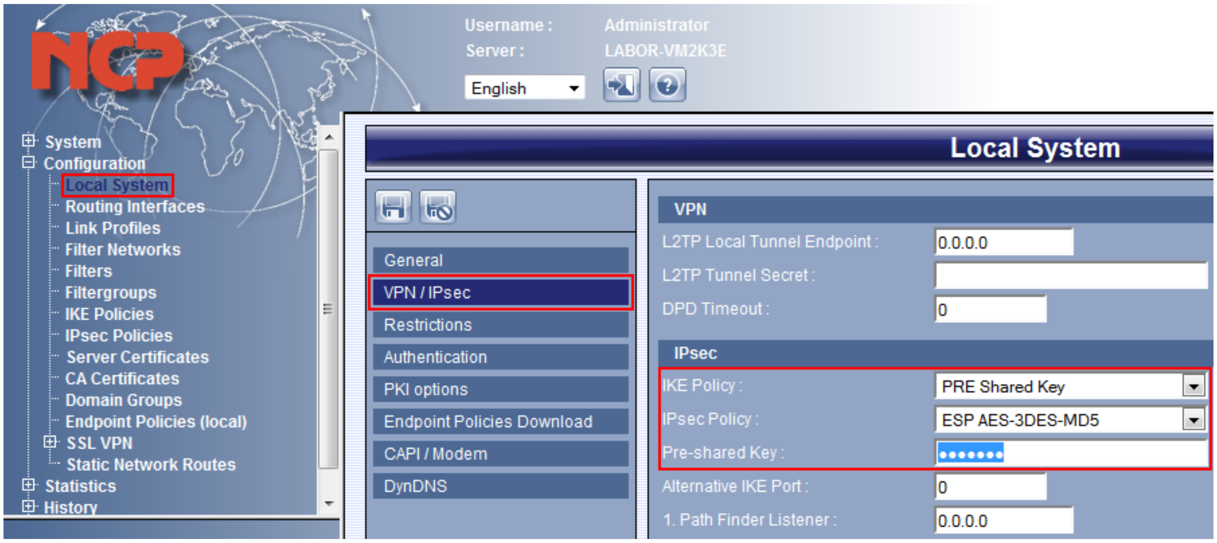
3. First login to configuration web interface

After installing the server in Windows or Linux you can access the web interface at https://<ipofserver>:20112.
A login page will be displayed where you will be asked to enter a login name and a password. Please login with "Administrator" and empty password. You will be prompted to enter and confirm a new password. As soon as you save the new password by clicking the save button, you will be forwarded to the NCP Secure VPN Server web Interface.

4. Basic Configuration

On the left side of the window you can see a tree menu. Please click on the menu item "Configuration" and the entry "Local System". On the right side of the screen you should see the "Local System" menu, which has its own list of categories. The category "General" is selected by default.

Please click on the "VPN/IPsec" category of the "Local System" menu. Go to the headline "IPsec". Activate the drop-down of the entry "IKE Policy" and select "PRE Shared Key". Now activate the drop-down of the entry "IPsec Policy" and select "ESP AES-3DES-MD5".
Additionally you have to enter a Pre-shared Key which later will be used by the the iOS Device.



Username : Administrator
Server : LABOR-VM2K3E
English

VPN

L2TP Local Tunnel Endpoint : 0.0.0.0
L2TP Tunnel Secret :
DPD Timeout : 0

IPsec

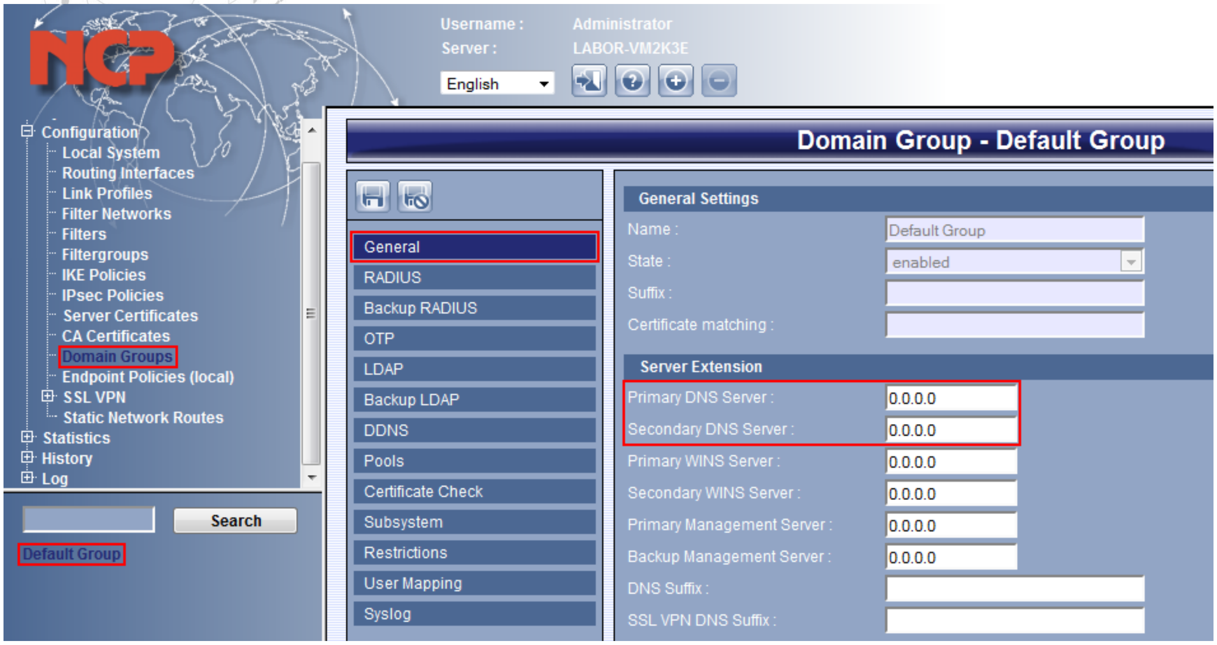
IKE Policy : PRE Shared Key
IPsec Policy : ESP AES-3DES-MD5
Pre-shared Key : •••••••
Alternative IKE Port : 0
1. Path Finder Listener : 0.0.0.0

Click on the save button above the "Local System" category list in order to save the changes.

5. Set up DNS Server and IP address pool

Now go back to the tree menu on the left side of the window and click on the entry "Domain Groups". On the right side of the screen you will not see any configuration options, since you have to choose a domain group first. You can see the existing groups in a list below the tree menu. Click on the entry "Default Group". You now have access to the settings of the Default Domain Group.

Again you have a separate list of categories. The category "General" is selected by default. Therein you should look for the headline "Server Extension" and the entries "Primary DNS Server" and "Secondary DNS Server". Enter the IP addresses of your primary and (if available) secondary DNS server here.



Username : Administrator
Server : LABOR-VM2K3E
English

Domain Group - Default Group

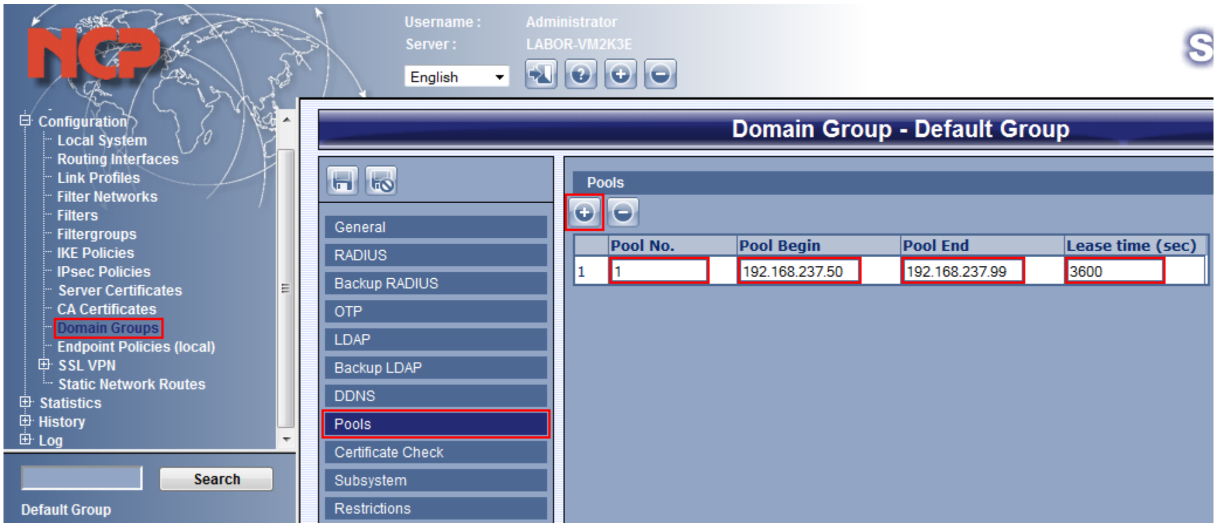
General Settings

Name : Default Group
State : enabled
Suffix :
Certificate matching :

Server Extension

Primary DNS Server : 0.0.0.0
Secondary DNS Server : 0.0.0.0
Primary WINS Server : 0.0.0.0
Secondary WINS Server : 0.0.0.0
Primary Management Server : 0.0.0.0
Backup Management Server : 0.0.0.0
DNS Suffix :
SSL VPN DNS Suffix :

Please click on the "Pools" category of the Default Domain Group. Click on the button with the plus symbol (+) in order to create a new IP address pool. Please assign 1 as "Pool No" and enter a Lease time of 3600.
The text boxes "Pool Begin" and "Pool End" have to be filled with the first, respectively the last IP address from the range of IP addresses from the virtual subnet that will be assigned to the clients (see 2.1 Virtual VPN Network).



Username : Administrator
Server : LABOR-VM2K3E
English

Domain Group - Default Group

Pools

	Pool No.	Pool Begin	Pool End	Lease time (sec)
1	1	192.168.237.50	192.168.237.99	3600

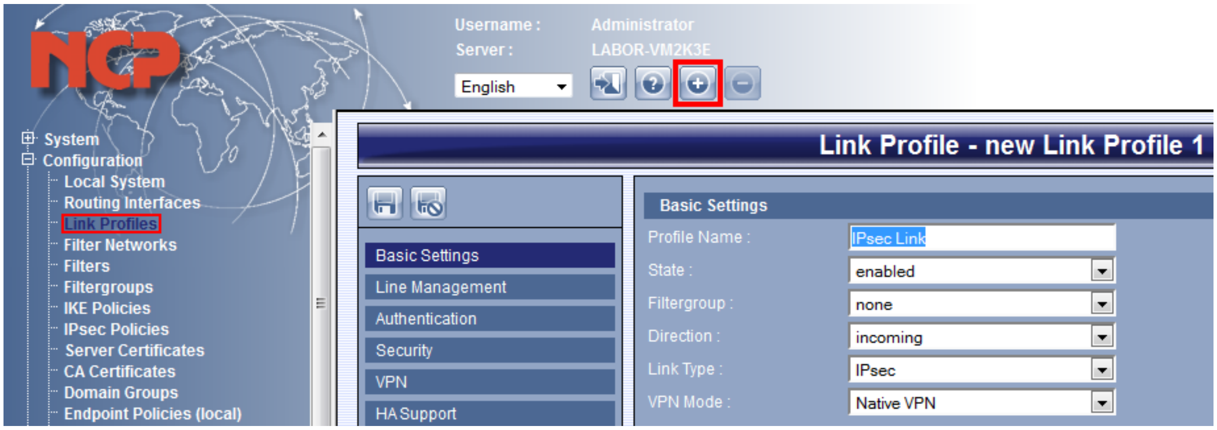
Click on the save button above the "Domain Group – Default Group" category list in order to save the changes you have made.

6. Creating a local IPsec Link Profile

To authenticate devices you can either create local profiles or use Active Directory with LDAP for authentication.

In this chapter we will describe the authentication with local profiles. If you want to do Active Directory authentication please have a look at chapter 8.

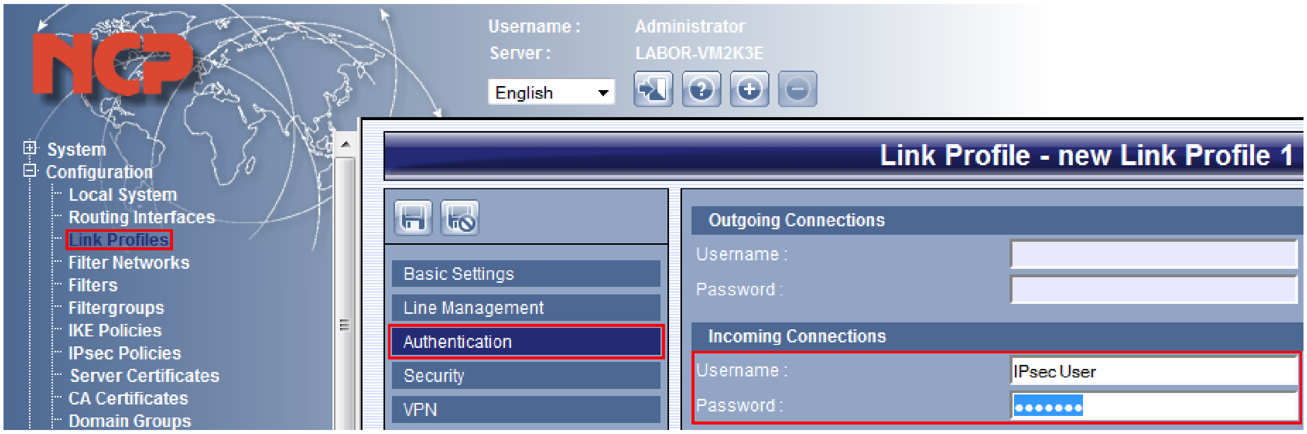
Click on the entry "Link Profiles" in the tree menu on the left side of the browser window. By default the list of link profiles is empty. To create a new profile, click on the "Add a list entry" button (+) in the center of the window, right below your login and server name. A new link profile has been created with the category "Basic Settings" selected by default. Enter a distinctive name into the "Profile Name" text box.


Username : Administrator
Server : LABOR-VM2K3E

Link Profile - new Link Profile 1

Basic Settings
Profile Name : IPsec Link
State : enabled
Filtergroup : none
Direction : incoming
Link Type : IPsec
VPN Mode : Native VPN

Now go to the category "Authentication" and enter a username and password for "Incoming Connections".

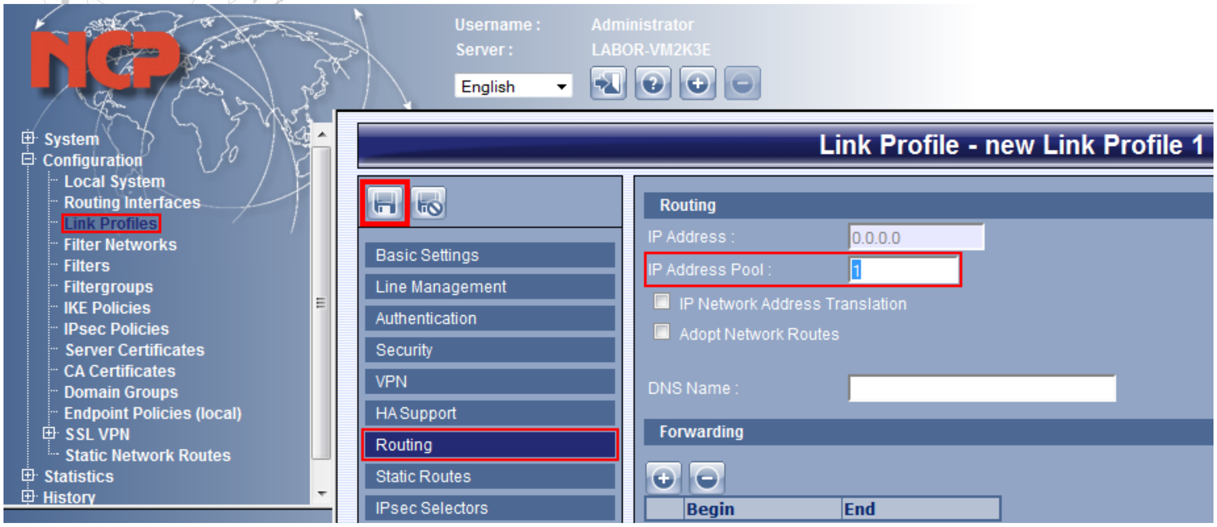

Username : Administrator
Server : LABOR-VM2K3E

Link Profile - new Link Profile 1

Outgoing Connections
Username :
Password :

Incoming Connections
Username : IPsec User
Password : •••••••

The next step is to go to the category "Routing" of the "Link Profile" menu. Enter the number you assigned to the IP Pool earlier to the text box labeled "IP Address Pool" (in our example this would be the number 1).



Username : Administrator
Server : LABOR-VM2K3E
English

Link Profile - new Link Profile 1

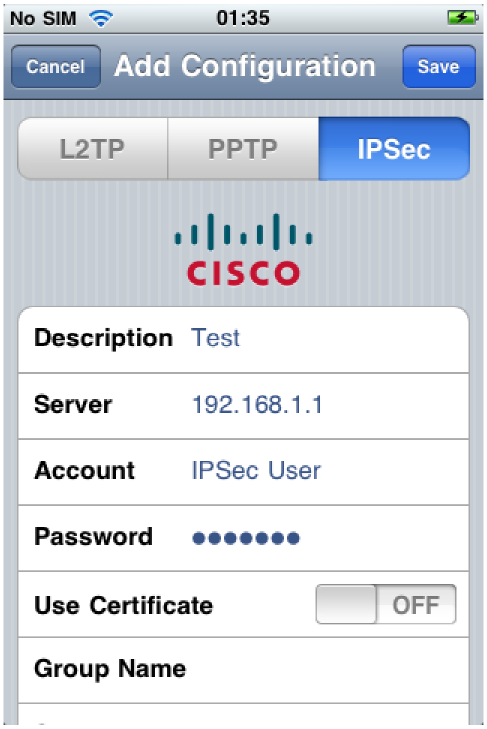
Routing

IP Address : 0.0.0.0
IP Address Pool : 1
□ IP Network Address Translation
□ Adopt Network Routes
DNS Name :

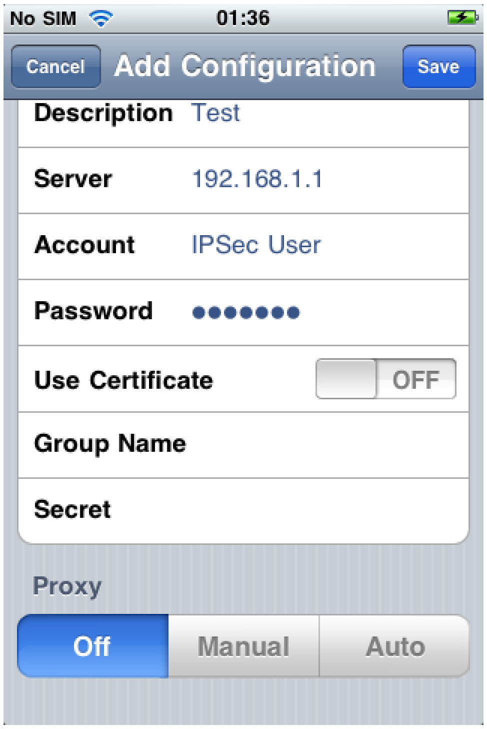
Click on the save button above the “Link Profiles” category list in order to save the changes you have made.

7. Create connection on iOS Device

Please add a new VPN connection on your iOS Device, enter any Description, the IP address where the VPN Server can be reached and the username and password you have entered in chapter 6. Additionally you will have to enter the pre-shared key you entered in chapter 4.



Description Test
Server 192.168.1.1
Account IPSec User
Password ●●●●●●●
Use Certificate OFF
Group Name



Description Test
Server 192.168.1.1
Account IPSec User
Password ●●●●●●●
Use Certificate OFF
Group Name
Secret
Proxy: [✓ Off] Manual Auto

8. Active Directory Authentication with LDAP

Instead of using locally configured profiles you can use your Active Directory for authentication.

Please go to the web interface of the Secure VPN Server again and select the entry “Domain Groups” in the tree menu and select the “Default Group”.
In the Default Group please select “LDAP / Active Directory”.
Enable the LDAP configuration and enter the IP address of your Active Directory server here. Optionally you can use the more secure LDAP over SSL here, but you will have to change the port to the standard port for LDAP over SSL (636) manually.

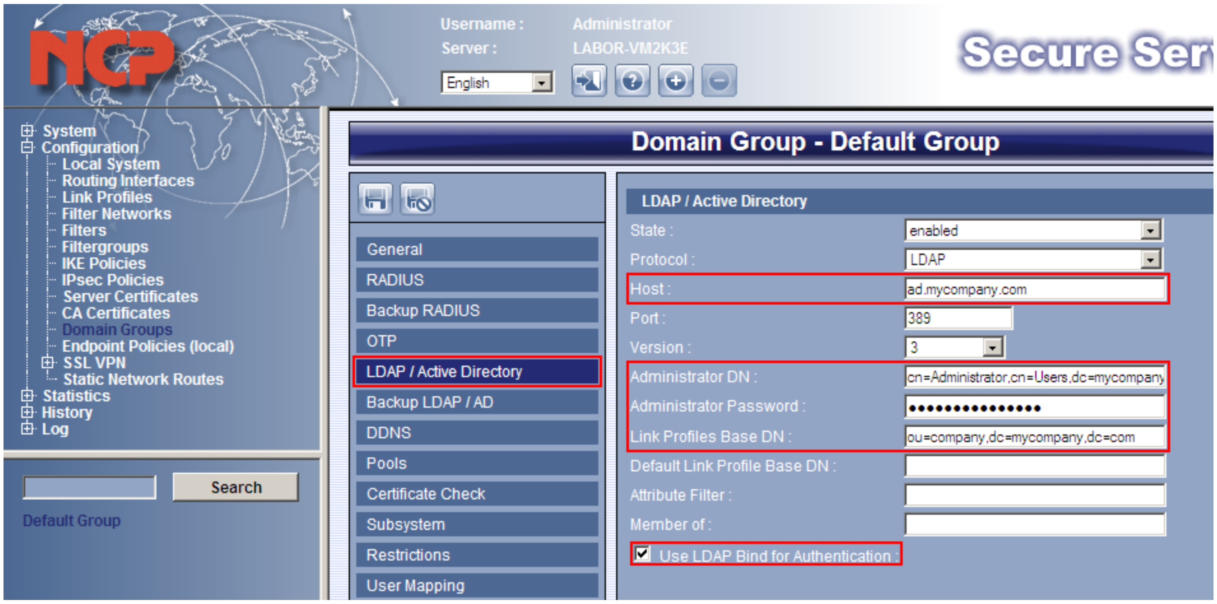
You will need an account that has at least read permissions to your directory service and enter the username in form of a fully qualified LDAP name and the password here.

In the field for “Link Profiles Base DN” you can specify in which Organizational Unit your users are located. The entry has to be in form of a fully qualified LDAP name again

Per default all users within the Group you specified in “Link Profiles Base DN” will have access to the VPN. It is possible to restrict access with two different settings on the LDAP configuration page.

The first possible restriction is the attribute filter. If you set the attribute filter to “(msNPAllowDialin=TRUE)” you only allow access for users that have the Active Directory setting “Allow Dialin” set.

You can also filter the users by Active Directory Group Membership. If you enter “cn=VPN Group, dc=myCompany, dc=com” in the field for “Member of” you only allow access to users that are members of the VPN Group.



Domain Group - Default Group

LDAP / Active Directory

State :	enabled
Protocol :	LDAP
Host :	ad.mycompany.com
Port :	389
Version :	3
Administrator DN :	cn=Administrator,cn=Users,dc=mycompany
Administrator Password :	•••••••••••••••
Link Profiles Base DN :	ou=company,dc=mycompany,dc=com
Default Link Profile Base DN :	
Attribute Filter :	
Member of :	

☑ Use LDAP Bind for Authentication :