
# Remote Access Tutorial using ...

## ZyXEL OTP Two-Way Factor Token,
## ZyWALL 35-70 VPN Router,
## ZyWALL VPN Client,
## Authenex Radius ASAS Server

Tutorial written by:

Writer: ZyXEL Engineering Team

Company: www.zyxel.com

# Table of contents

# 1 Disclaimer

*This tutorial is provided in this format for your convenience only. It is important to state that TheGreenBow has NO legal right over the content and instructions to configure either product listed in this document. This document is basically a copy of a ZyXEL web page called: "How to configure the VPN client (GreenBow) with OTP authentication over ZyWALL 35?" that you can google easily here: http://www.google.com/search?q=How+to+configure+the+VPN+client(GreenBow)+with+OTP+authentication+over+ZyWALL+35%3F.*

*Certification of the overall remote access architecture containing OTP Two-Way Factor token, Authenex Radius Server and ZyWALL 35 VPN Router has NOT been processed by TheGreenBow. However, ZyXELL did certify it. In any case, if you detect any errors in this tutorial (HowTo), we apologize to you in advance and would like you to post a request to our techsupport so we can take the appropriate action.*

# 2 Introduction

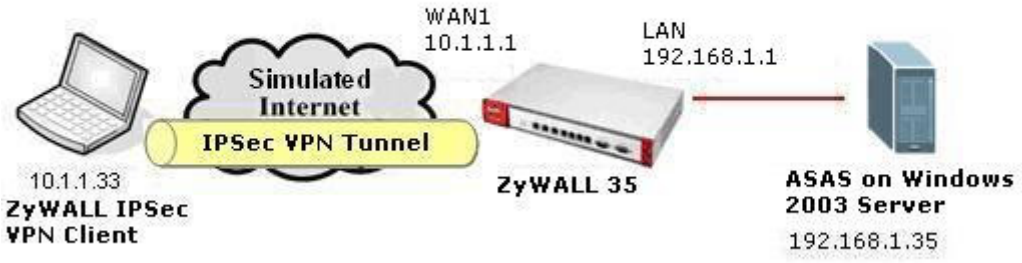
## 2.1 What is the problem?

How to configure the ZyWALL VPN Client software with OTP Authentication with RADIUS Server if the IPSec VPN gateway is a ZyNOS-based appliance (e.g. ZyWALL 35 or ZyWALL 70)?

## 2.2 Network topology

In this tutorial, we evaluated by using the ZyWALL Starter Kit which only comes with two ZyWALL OTP tokens. The ESN numbers are 73010234 and 73010235. We will create a new user Rex in order to login to ZyWALL with OTP.

For this tutorial, we'll use a ZyWALL 35 VPN Router and Authenex ASAS Radius Server.




## 2.3 OTP Token, Radius Server and VPN Router product info

It is critical that users find all necessary information about products used in the tutorial. All product info, User Guide and knowledge base can be found there.

| | |
|---|---|
| ZyWALL OTP tokens | http://www.zyxel.com/web/product_family_detail.php?PC1indexflag=20040908175941&CategoryGroupNo=96C9CDE6-F2AA-4D84-9D62-311A7CCD996C&display=7999 |
| ZyWALL 35 | http://www.zyxel.com/web/product_family_detail.php?PC1indexflag=20040908175941&display=6244&CategoryGroupNo=53C4D3B9-98B3-4F1F-A7B2-BED2BBA2A7CA |
| ZyWALL 70 | http://www.zyxel.com/web/product_family_detail.php?PC1indexflag=20040908175941&display=6244&CategoryGroupNo=53C4D3B9-98B3-4F1F-A7B2-BED2BBA2A7CA |
| ZyWALL VPN Client Software | http://www.zyxel.com/web/product_family_detail.php?PC1indexflag=20040908175941&CategoryGroupNo=288CE451-0F22-461F-B312-7CF3C12AAFF8&display=6244 |
| Authenex ASAS Radius server | http://www.authenex.com/authenex-products/asas-system.html |

# 3 Solution with OTP, Radius Server and VPN Router configuration

## 3.1 Quick step by step

In the following tutorial, we will employ the ZyXEL Two-Way Factor Authentication solution (ZyWALL OTP pack) to enhance password security by using the IPSec VPN application provided by ZyWALL 35.

In order to use this application, you are required to configure your ZyWALL and ASAS according to the following steps:

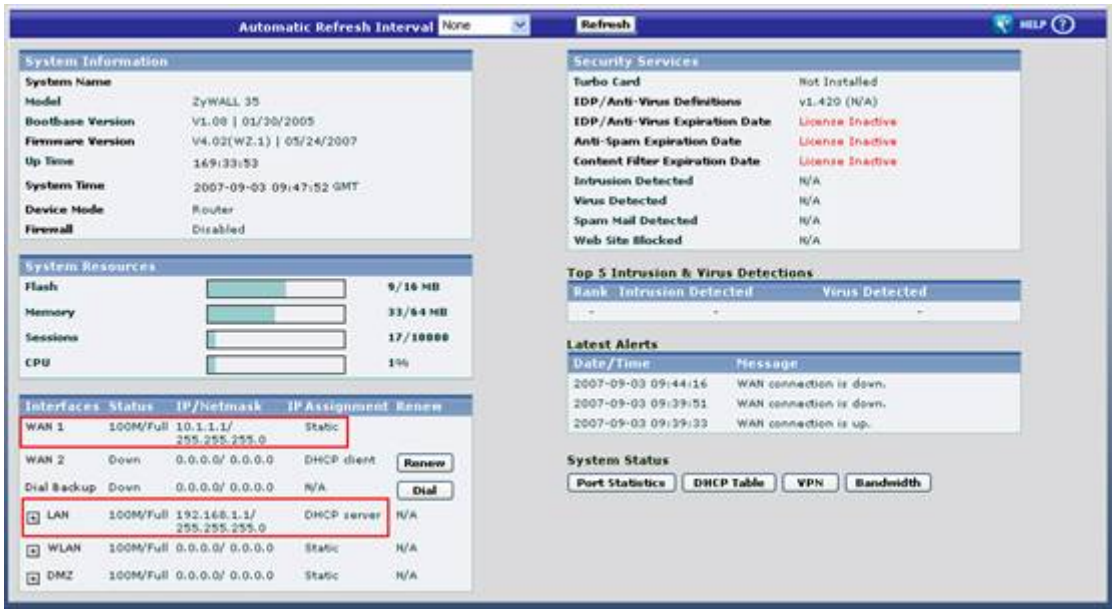
1. Install the ASAS authentication server on a computer. (Note: Please refer to the ASAS installation guide in Chapter 2 or the installation documentation in electronic format comes with the ZyXEL OTP Pack installation CD.)
2. Create a user account on the ASAS server.
3. Import each token's database file from the ZyXEL OTP installation CD over into the ASAS authentication server.
4. Assign the users to the OTP tokens over the administration interface in the ASAS server.
5. Configure the ASAS as a RADIUS server in the ZyWALL administration GUI Security > Auth Server > RADIUS
6. Give the OTP tokens away to the users who will remote login into the ZyWALL.

Note: ZyWALL OTP pack is a stand-alone product, which is not bundled with the ZyWALL series.

## 3.2 ZyWALL 35 VPN Router Configuration

### STEP 1: Configure Network Setting on the ZyWALL 35

Lunch a web browser window and logon into the ZyWALL35's web configurator. Configure the LAN and WAN interfaces according to your application scenario and network topology you plan.




## STEP 2: Configure the External Authentication Server

1) Click Security > Auth Server from the left panel and navigate to the RADIUS setting page.

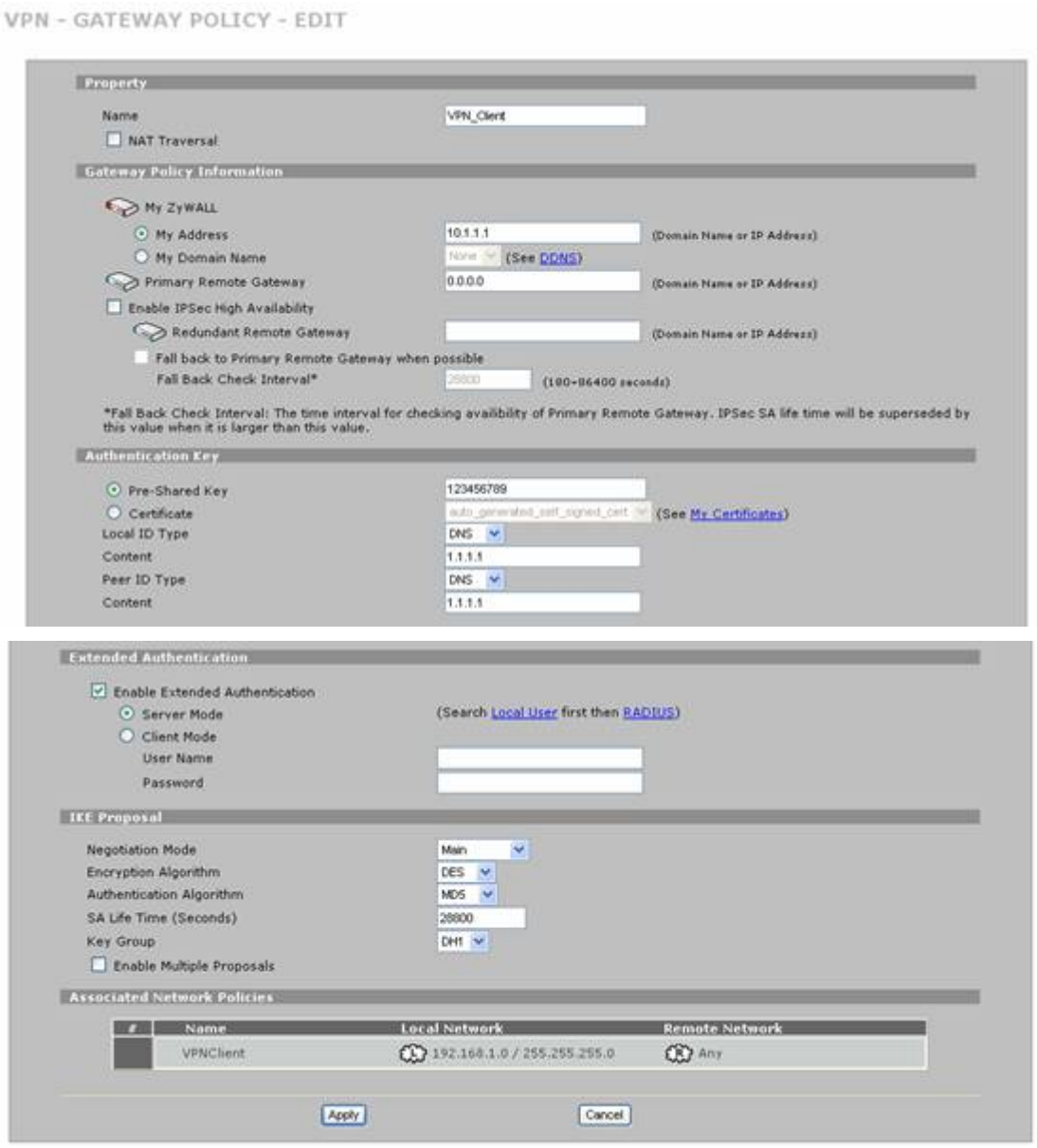
2) Enter the ASAS Server IP address in the Server IP Address and the Shared Secret in Key.


## STEP 3: Configuring the IPSec VPN Gateway (Phase 1) on the ZyWALL 35

Navigate to Security > VPN > and click Add in order to add a new IPSec VPN Gateway for VPN Client.

We will assign 0.0.0.0 for the Secure Gateway Address since we don't know the IP address of the remote client. 0.0.0.0 represents for any IP address will be accepted.

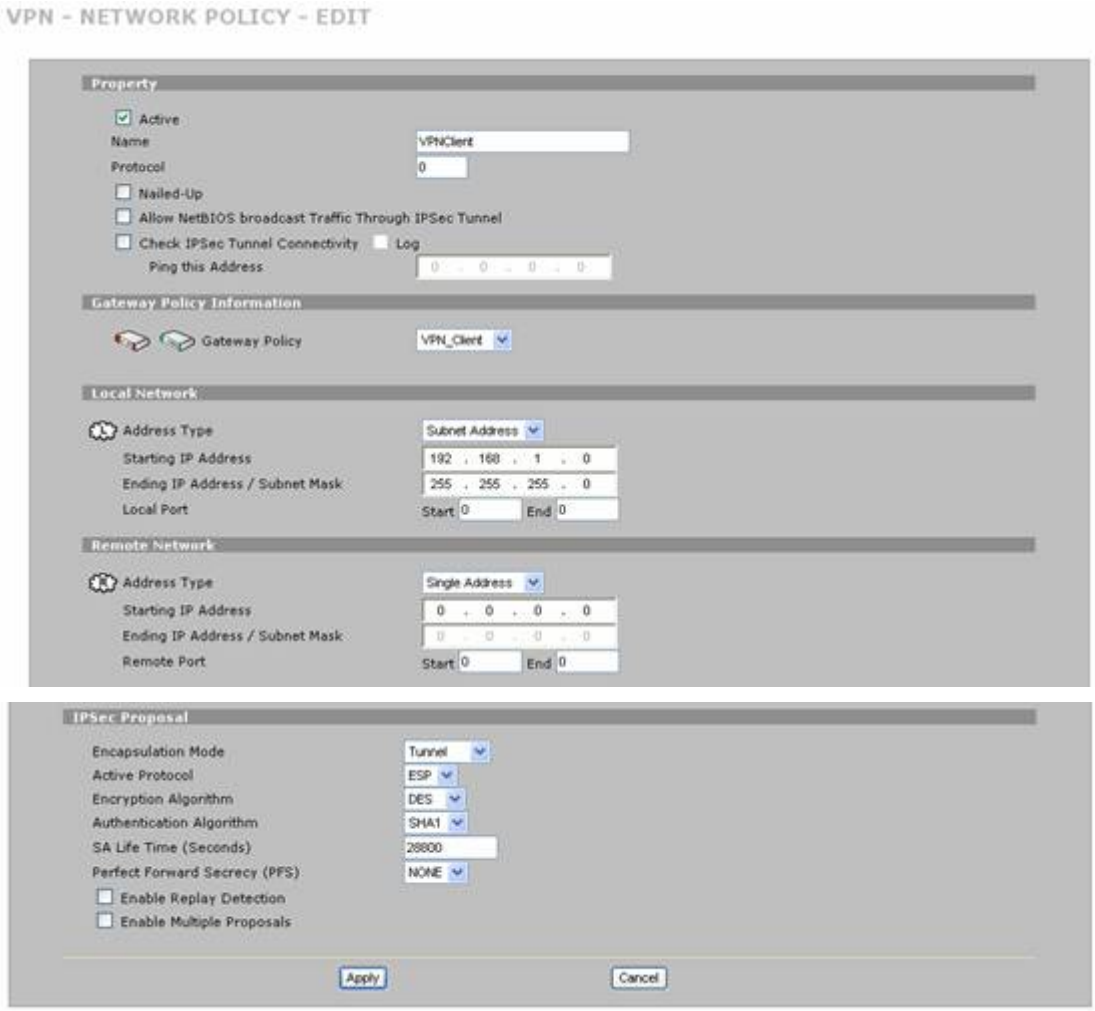
Check the Enable Extended Authentication checkbox.




## STEP 4: Configuring the IPSec VPN Connection (Phase2) on the ZyWALL

Navigate to Security > VPN, and click Add in order to create a new IPSec VPN Connection for the remote VPN client.

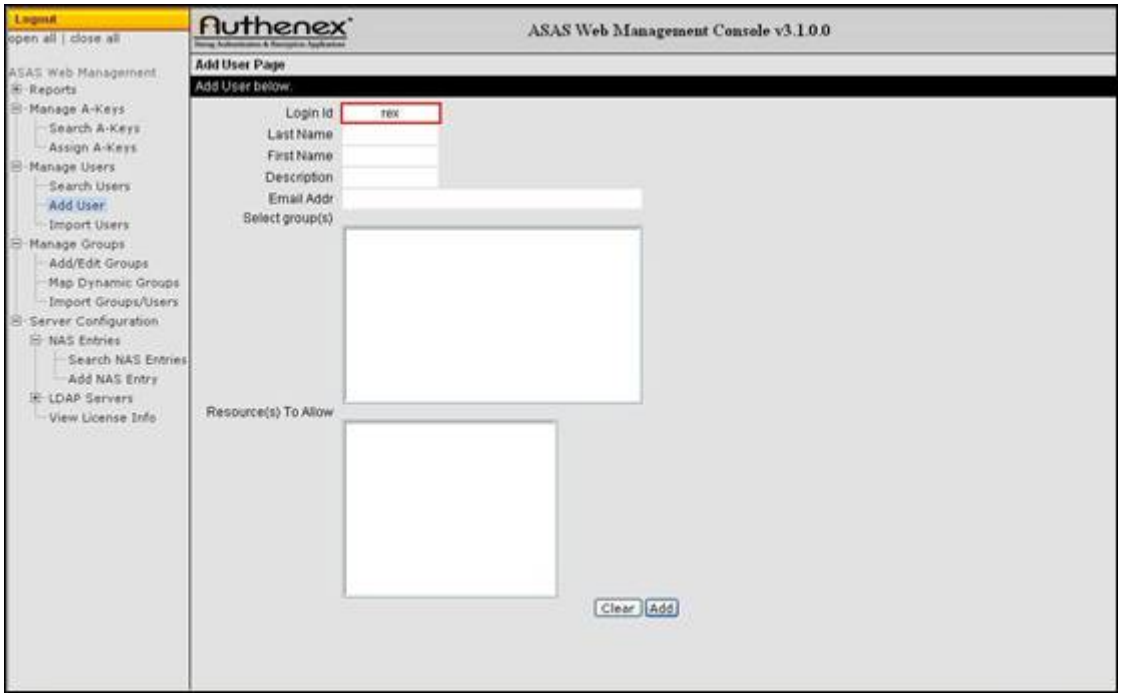
We will assign 0.0.0.0 for the Secure Gateway Address since we don't know the IP address of the remote client. 0.0.0.0 represents for any IP address will be accepted.




## 3.3 ASAS Radius Server Configuration

### STEP 1: Create a User Account on ASAS

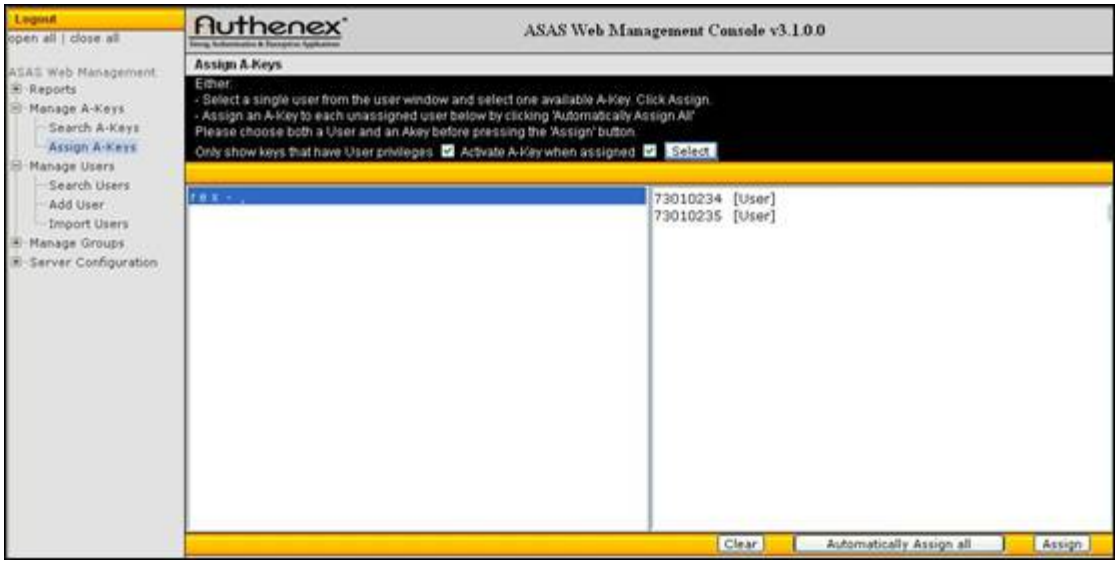
1) Login to the ASAS server as an administrator and create a new user via Manage Users > Add User.
2) Fill in the user name in the Login ID field.
3) Click the Add button in order to complete the configuration in this step.




## STEP 2: Assign an ZyWALL OTP Token to the New User

1) Navigate to Manage A-Keys > Assign A-Keys in order to assign the specific ZyWALL OTP Token to the newly created user.

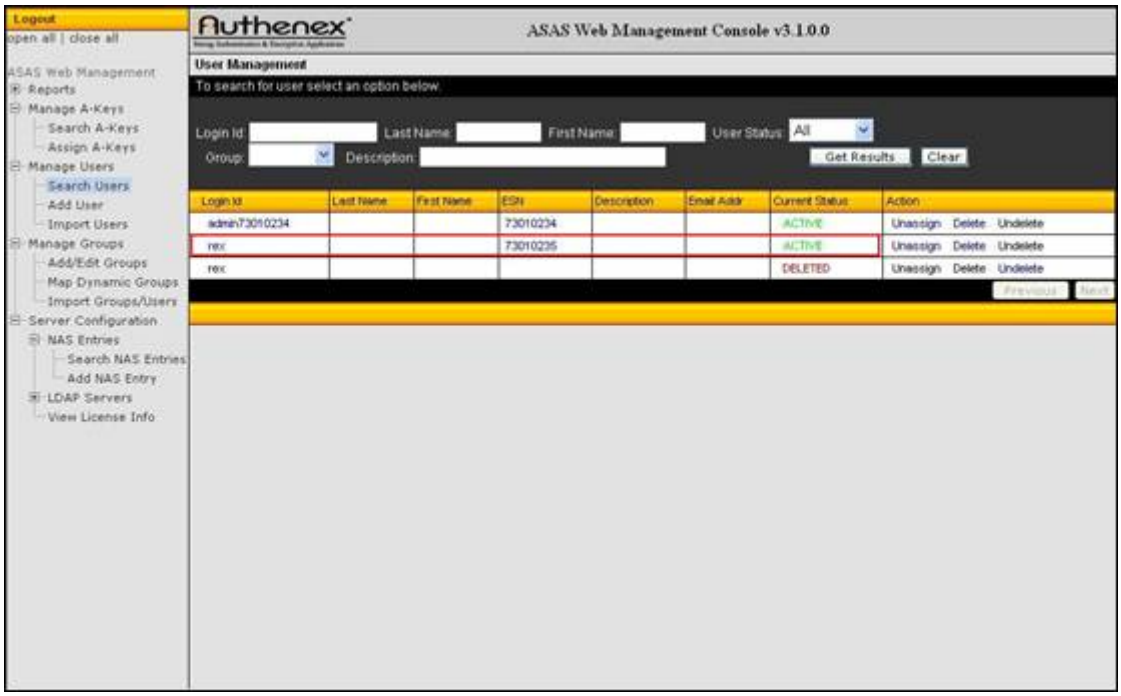
2) Pick up a ZyWALL OTP token that is available from the right panel and click the Assign button to complete the authentication key assignment.




## STEP 3: Verify that the A-Key is properly Assigned to the User

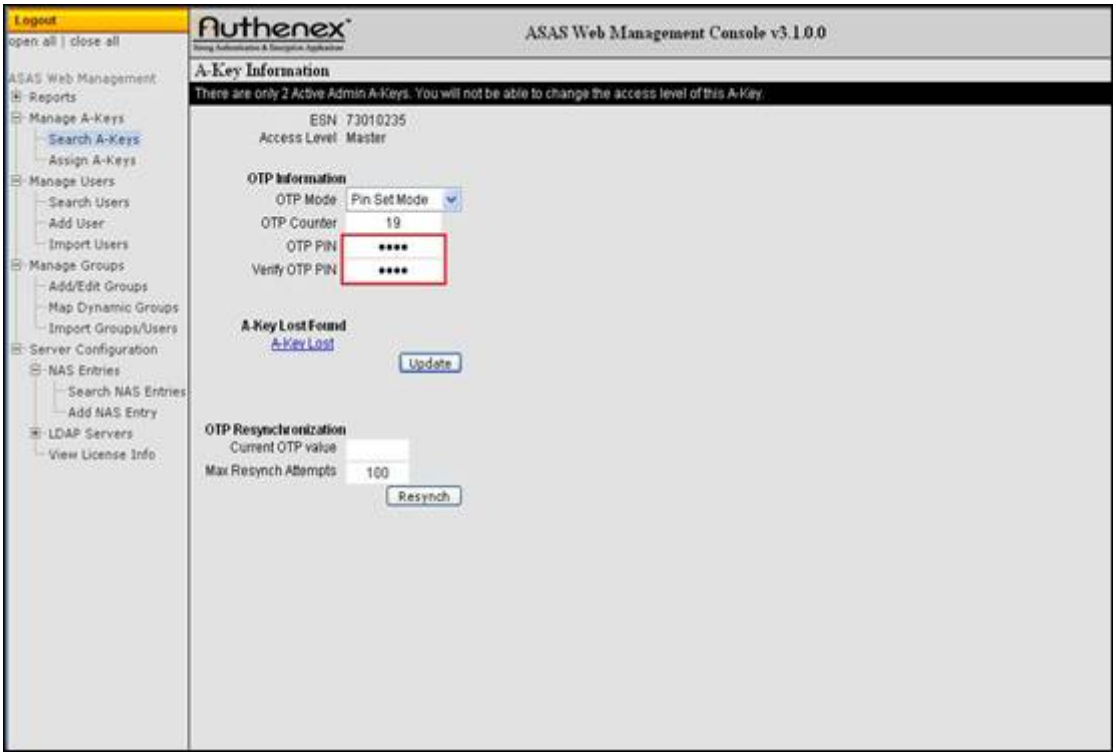
1) Navigate to Manage Users > Search Users page; leave the input fields empty and click the Get Results button in order to retrieve the user & A-Key binding list.

2) Ensure the ZyWALL OTP token is correctly assigned to the user account you created.



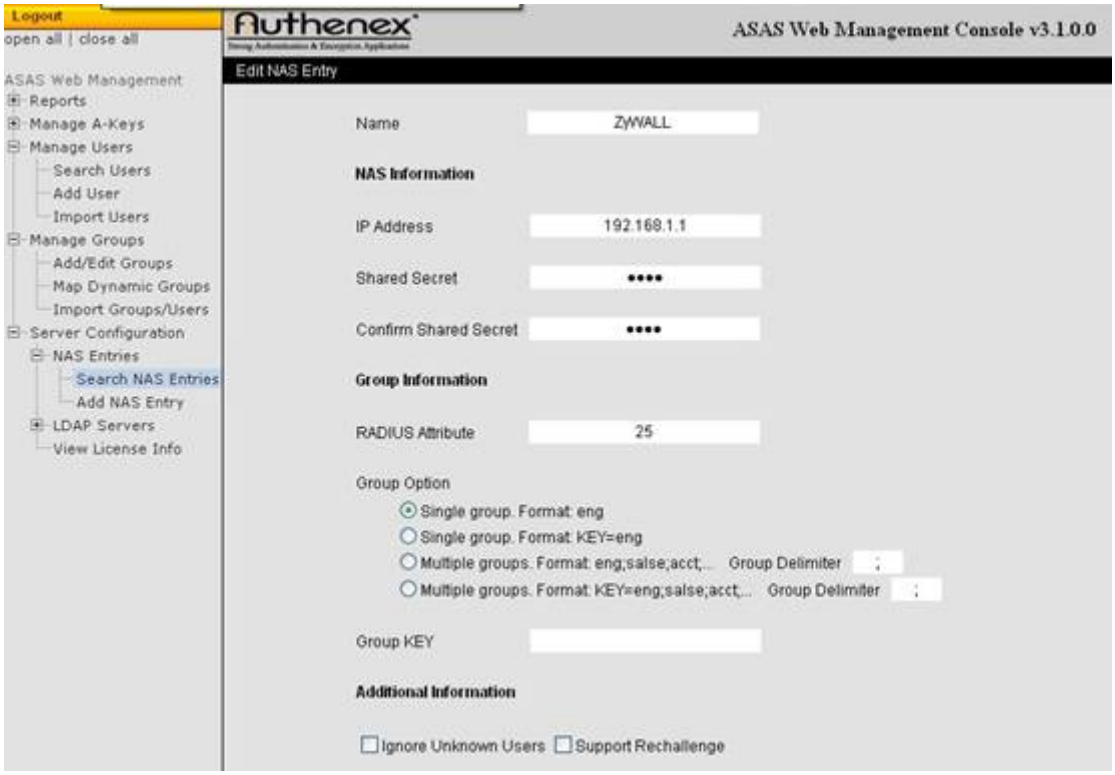

## STEP 4: Update the OPT PIN

1) Navigate to Manage A-Keys > Search A-Keys; leave the ESN field empty and click the Search button in order to browse the entire ZyWALL OTP token list.
2) In the search result page, pick up the ZyWALL OTP token you want to update the PIN code of.
3) Select PIN Set Mode from the OPT Mode dropdown list.
4) Enter the password in the OTP PIN text field with 4-24 alphanumeric characters length.
5) Re-enter the password in the Verify OTP PIN text field.




## STEP 5: Configure the NAS Devices

1) Click Server Configuration > NAS Entries > Add NAS Entry in order to specify which device will be given access to the authentication server.
2) Give the ZyWALL a name, specify the IP Address of the ZyWALL and the shared secret.
3) Click the Add button in order to finish the NAS Device configuration.

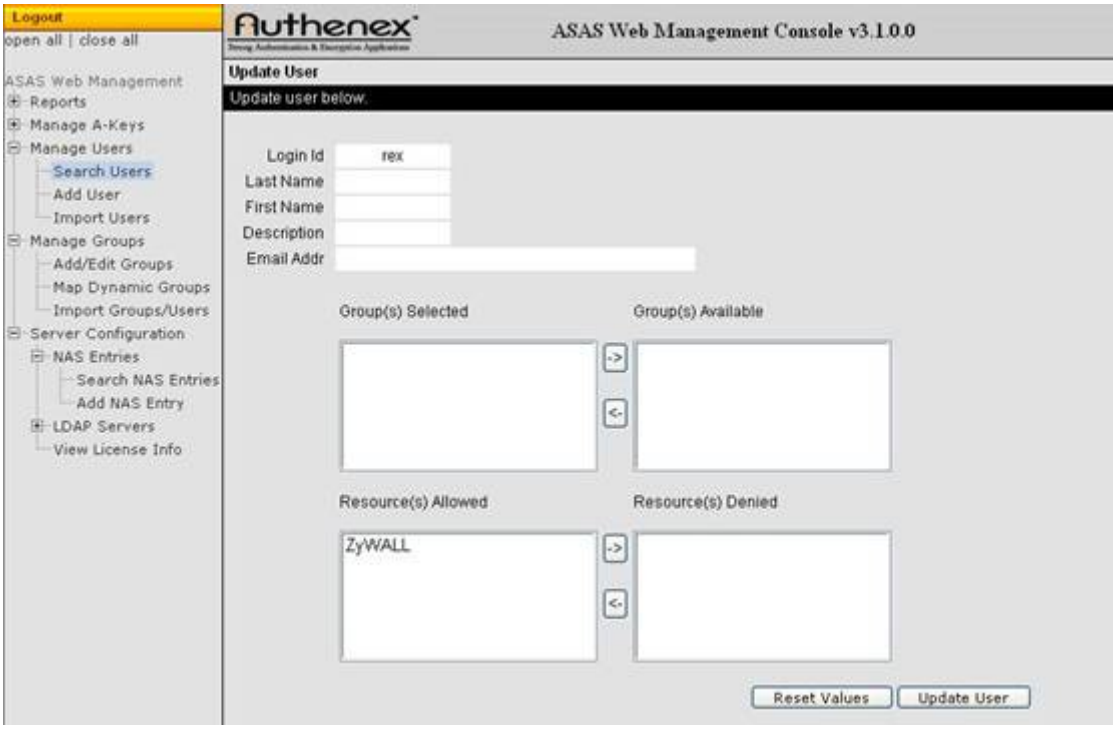



## STEP 6: Restart the ASAS Service

Select Start > Programs > Authenex > ASAS Server > Restart Services to reboot the ASAS Server and apply the configuration.

## STEP 7: Assign Resources to User

1) Click Manage Users > Search Users; leave all fields empty and click the Get Results button to retrieve the user account list.
2) Click on the user account you created first and the Update User page will appear.
3) Add the ZyWALL device to Resource(s) Allowed list.
4) Click the Update User button to complete the entire ASAS setting.




## 3.4 ZyWALL IPSec VPN Client Software configuration

### STEP 1: Configuring the VPN Gateway (Phase 1) on Client

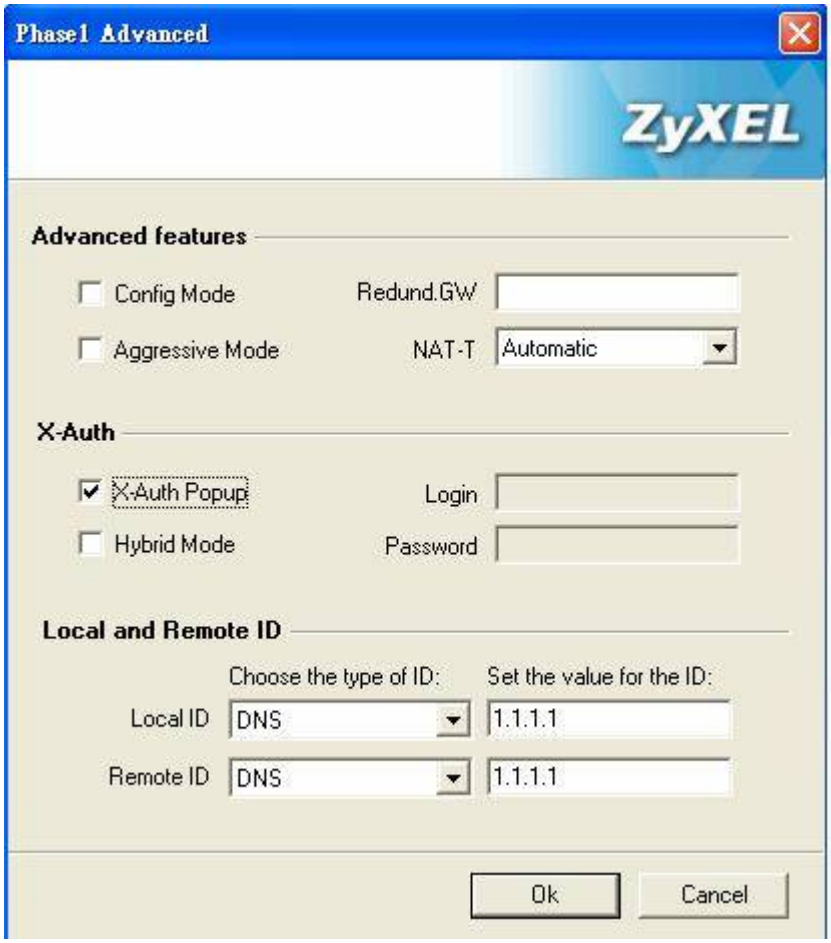
Launch the ZyWALL IPSec VPN Client and right click on Configuration and select New Phase1.

Enter the name and the IP address of Remote Gateway.

Enter the Pre-shared Key and ensure the number you just entered is matched with the one you entered on the ZyWALL in phase1 configuration. In this tutorial, we employ the Pre-shared key 123456789.

Confirming the encryption, authentication and key group to match the settings on ZyWALL.


Click the Advanced Settings... button and check the X-Auth checkbox to enable the extended authentication on VPN client. Ensure the Local and Remote ID are reflecting to the settings on ZyWALL.

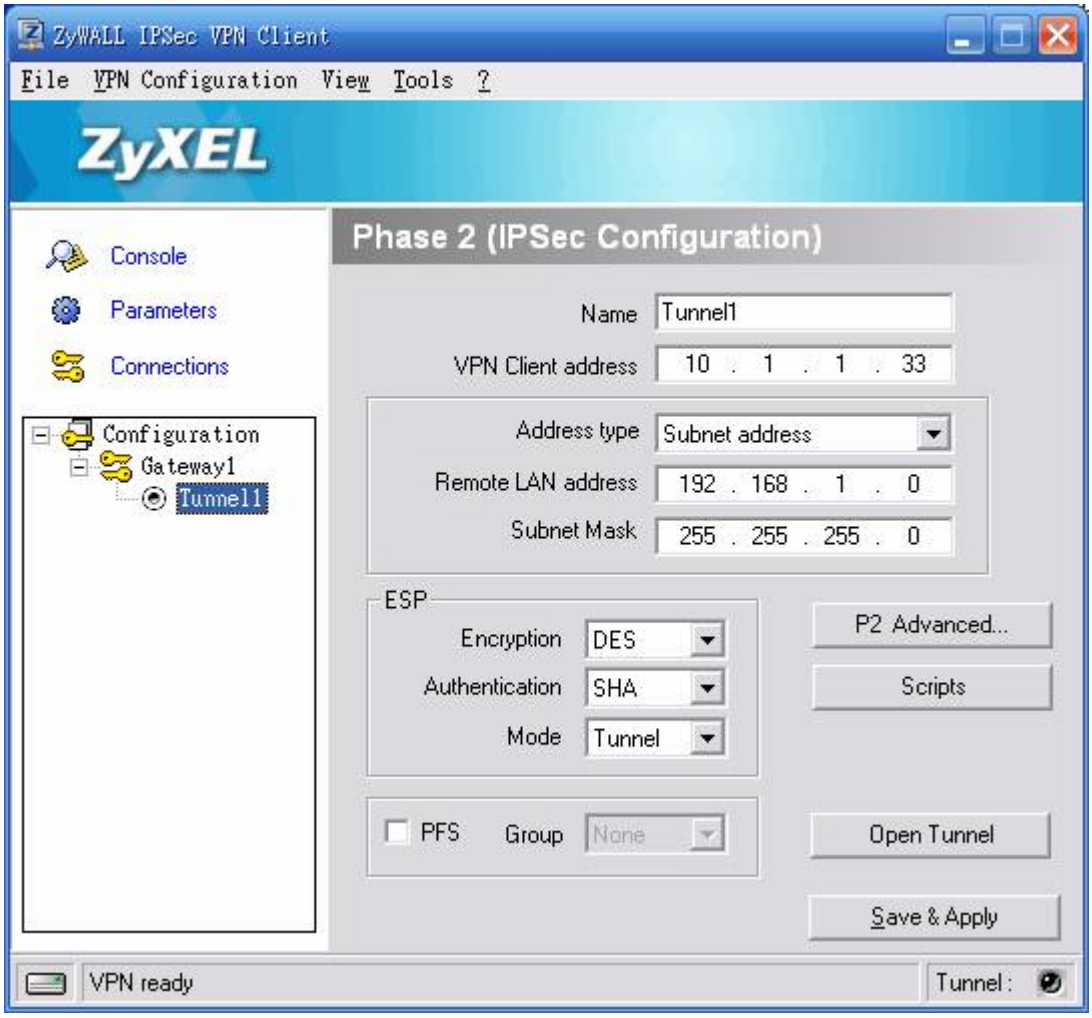



## STEP 2: Configuring the VPN Tunnel (Phase 2) on Client

Right click on the Gateway1 and select Add Phase 2 in order to create a new tunnel.

Fill in all the required fields on this page, including Address type and all ESP fields. Ensure the encryption method, authentication method, and mode are matched with the settings on ZyWALL.

Click 'Save & Apply' in order to complete the setting.




## 3.5 Verify OTP via Login from the VPN Client

### STEP 1: IPSec VPN Tunnel Establishing

Launch the ZyWALL IPSec VPN client.

Right click the icon of VPN client from the system tray and select Connection Panel.

Click the Open button in advance to establish the VPN tunnel.


## STEP 2: User Authentication via OTP

Click on the Open button and the Authentication window pops up.

Enter the login name and password. The password here is the combination of OTP pin + OTP for which we already manipulated the OTP PIN as 1234 on the STEP 4 Update the OPT PIN in the ASAS Server Configuration session.


Once the OTP works correctly, you will see the welcome message pop-up as on the following screenshot.

Once the OTP works correctly, the IPSec VPN tunnel will be opened.


ZyWALL IPSec VPN Client
ZyXEL
Gateway1-Tunnel1
Tunnel opened.
Gateway1-Tunnel1
Close
opened
Close

# 4 Contacts

Technical support at http://www.zyxel.com/web/support_feedback.php or support@thegreenbow.com