External Authentication with SonicWALL® SSL VPN

Authenticating Users Using SecurAccess Server by SecurEnvoy

Contact information		
SecurEnvoy	www.securenvoy.com	0845 2600010
	1210 Parkview Arlington Business Park Theale Reading RG7 4TY	
Phil Underwood	Punderwood@securenvoy.com	

SonicWALL® SSLVPN Integration Guide

This document describes how to integrate a SonicWALL® SSL VPN installed with SecurEnvoy two-factor Authentication solution called 'SecurAccess'.

SonicWALL® SSL VPN provides - Secure Application Access to the internal corporate network.

SecurAccess provides two-factor, strong authentication for remote Access solutions (such as SonicWALL ®), without the complication of deploying hardware tokens or smartcards.
Two-Factor authentication is provided by the use of (your PIN and your Phone to receive the one time passcode)

SecurAccess is designed as an easy to deploy and use technology. It integrates directly into any LDAP directory server such as Microsoft's Active Directory and negates the need for additional User Security databases. SecurAccess authentication server is directly integrated with LDAP or Active Directory in real time.

SecurEnvoy Security Server can be configured in such a way that it can use the existing Microsoft password. Utilising the Windows password as the PIN, allows the User to enter their UserID, Windows password and One Time Passcode received upon their mobile phone. This authentication request is passed to the SecurEnvoy Security Server via the RADIUS protocol, where it carries out a Two-Factor authentication. It provides a seemless login into the corporate network environment by the remote User entering three pieces of information. SecurEnvoy utilises a web GUI for configuration, whereas the SonicWALL® Server environment uses a GUI application. All notes within this integration guide refer to this type of approach.

The equipment used for the integration process is listed below:

SonicWALL® SSL VPN
SonicWALL software release v4

Microsoft (for installation of SecurEnvoy Security Server)
Windows 2003 server
IIS installed with SSL certificate (required for management and remote administration)
Access to Active Directory with an Administrator Account

SecurEnvoy
SecurAccess software release v5.1.500

Index

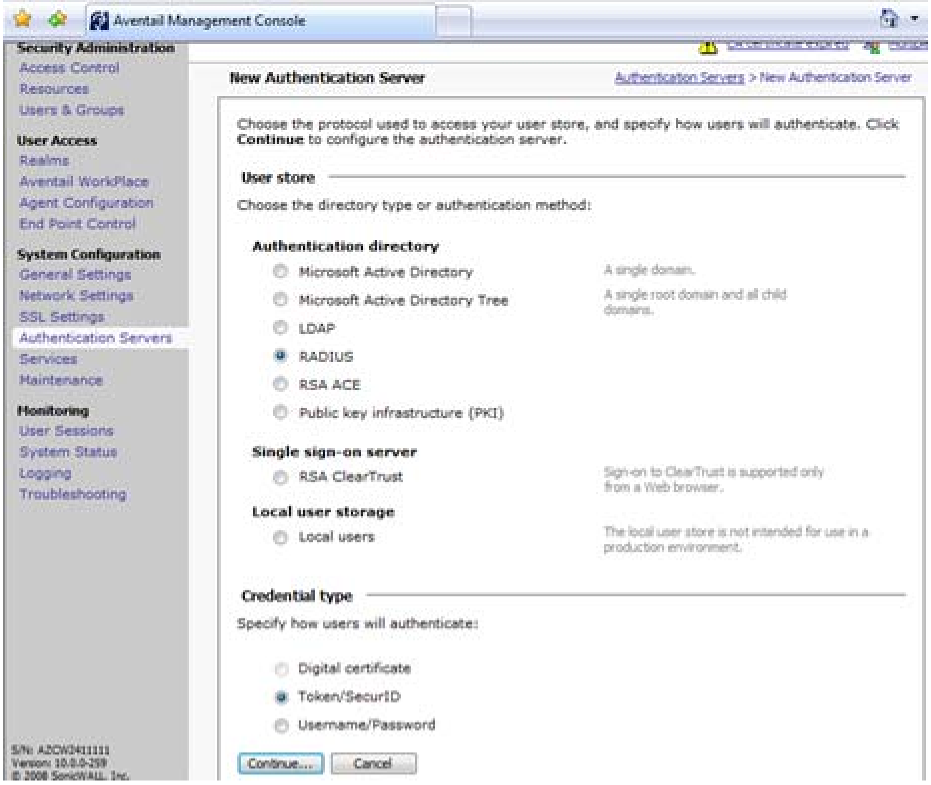
1.0 Pre Requisites

It is assumed that the SonicWALL® is setup and operational. An existing Domain user can authenticate using a Domain password and access applications. All communications are over HTTPS (port 443) for client browser and SonicWALL® SSL VPN.
Securenvoy Security Server has a suitable account created that has read and write privileges to the Active Directory, if firewalls are between the SecurEnvoy Security server, Active Directory servers, and the SonicWALL® SSL VPN, additional open ports will be required.
NOTE: SecurEnvoy requires LDAP connectivity either over port 389 or 636 to the Active Directory servers and port 1645 or 1812 for RADIUS communication from the SonicWALL® SSL VPN.

2.0 Configuration of SonicWALL

Within the SonicWALL® Aventail SSL VPN GUI

a) Navigate to Authentication servers
b) Select New
c) Enter details for a Radius server (SecurEnvoy)
d) Set credential type to Token/SecurID
e) Click "Continue"



New Authentication Server

Choose the protocol used to access your user store, and specify how users will authenticate. Click **Continue** to configure the authentication server.

User store

Choose the directory type or authentication method:

Authentication directory

○ Microsoft Active Directory — A single domain.
○ Microsoft Active Directory Tree — A single root domain and all child domains.
○ LDAP
● RADIUS
○ RSA ACE
○ Public key infrastructure (PKI)

Single sign-on server

○ RSA ClearTrust — Sign-on to ClearTrust is supported only from a Web browser.

Local user storage

○ Local users — The local user store is not intended for use in a production environment.

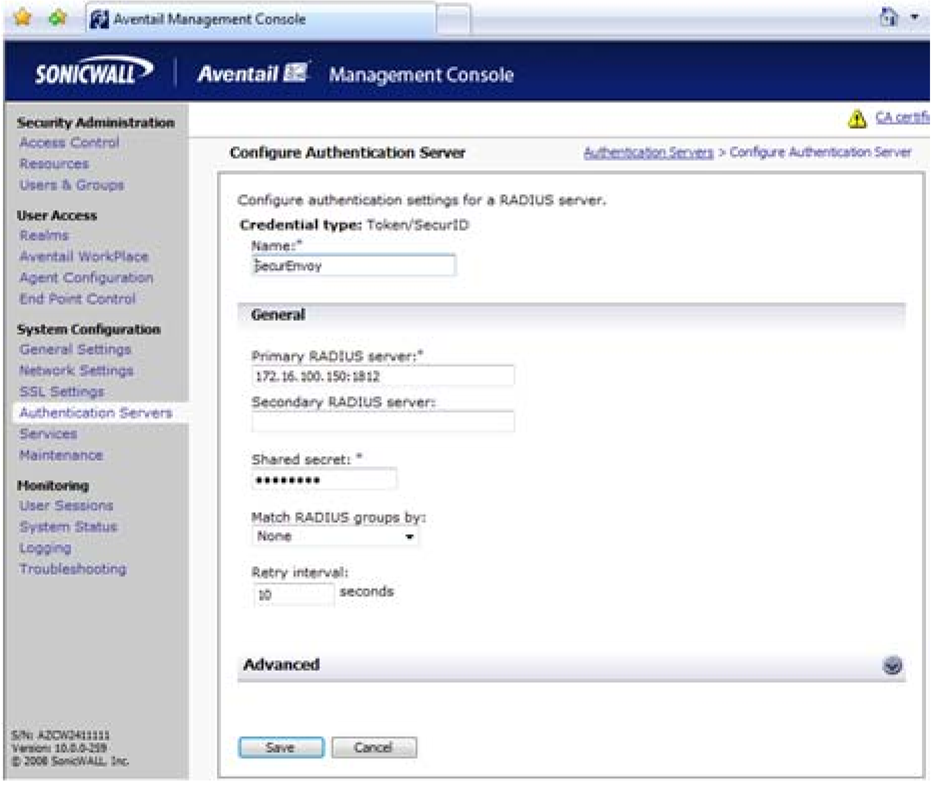
Credential type

Specify how users will authenticate:

○ Digital certificate
● Token/SecurID
○ Username/Password

Select Configure Authentication server

a) Enter details for SecurEnvoy server
   Name, IP Address and Port, shared secret
b) Set retry to 10 seconds



Configure Authentication Server

Configure authentication settings for a RADIUS server.

Credential type: Token/SecurID

Name:* SecurEnvoy

General

Primary RADIUS server:* 172.16.100.150:1812

Secondary RADIUS server:

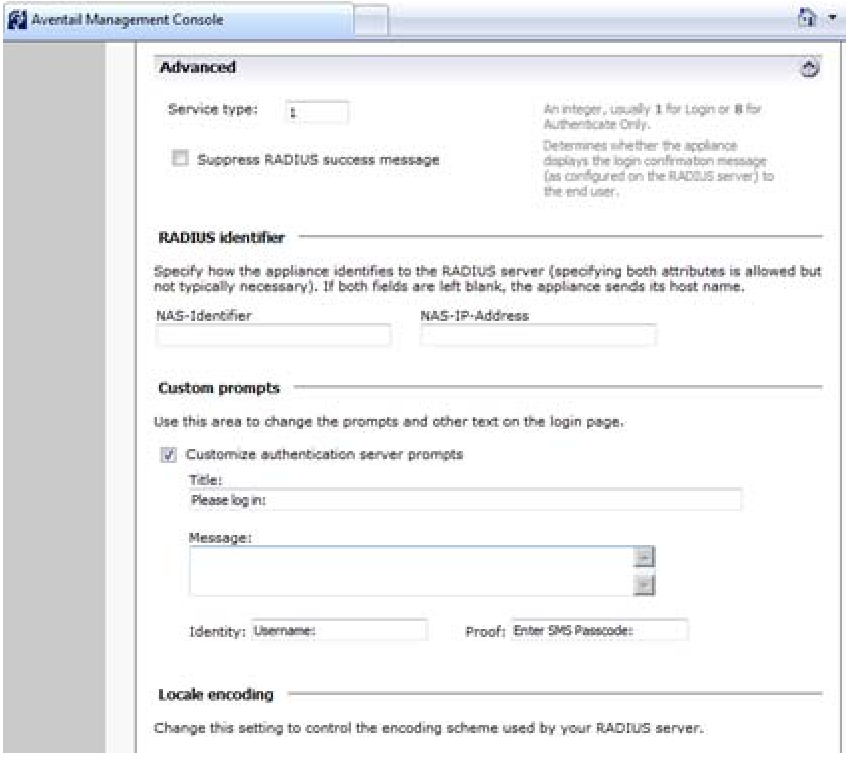
Shared secret: * ••••••••

Match RADIUS groups by: None

Retry interval: 10 seconds

Advanced

c) Select “Advanced”
d) Select “Customize authentication server prompts, with identity = “Username” and Proof = “Enter SMS Passcode”



Advanced

Service type: 1

An integer, usually 1 for Login or 8 for Authenticate Only.

□ Suppress RADIUS success message

Determines whether the appliance displays the login confirmation message (as configured on the RADIUS server) to the end user.

RADIUS identifier

Specify how the appliance identifies to the RADIUS server (specifying both attributes is allowed but not typically necessary). If both fields are left blank, the appliance sends its host name.

NAS-Identifier

NAS-IP-Address

Custom prompts

Use this area to change the prompts and other text on the login page.

☑ Customize authentication server prompts

Title: Please log in:

Message:

Identity: Username:

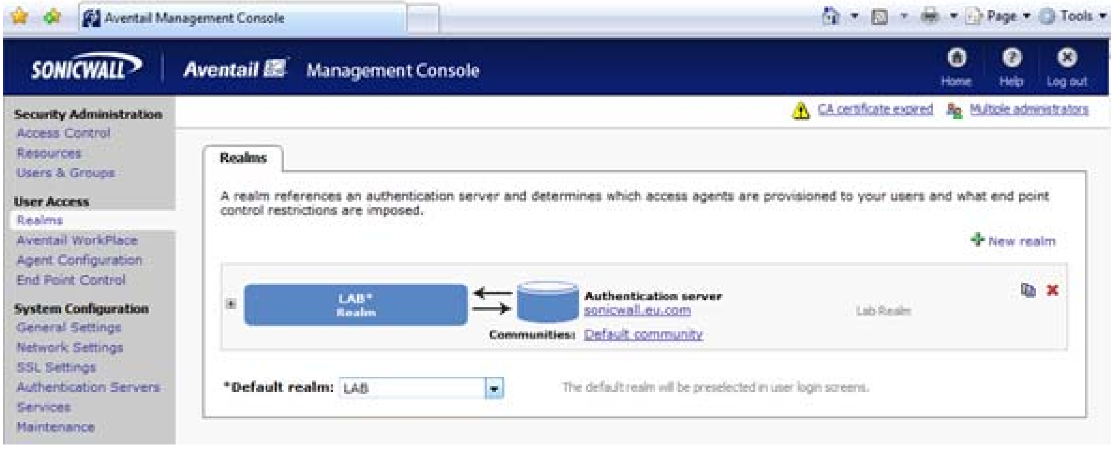
Proof: Enter SMS Passcode:

Locale encoding

Change this setting to control the encoding scheme used by your RADIUS server.

Navigate to User Access and select Realms

Click “New realm”



A realm references an authentication server and determines which access agents are provisioned to your users and what end point control restrictions are imposed.

LAB* Realm

Authentication server: sonicwall.eu.com

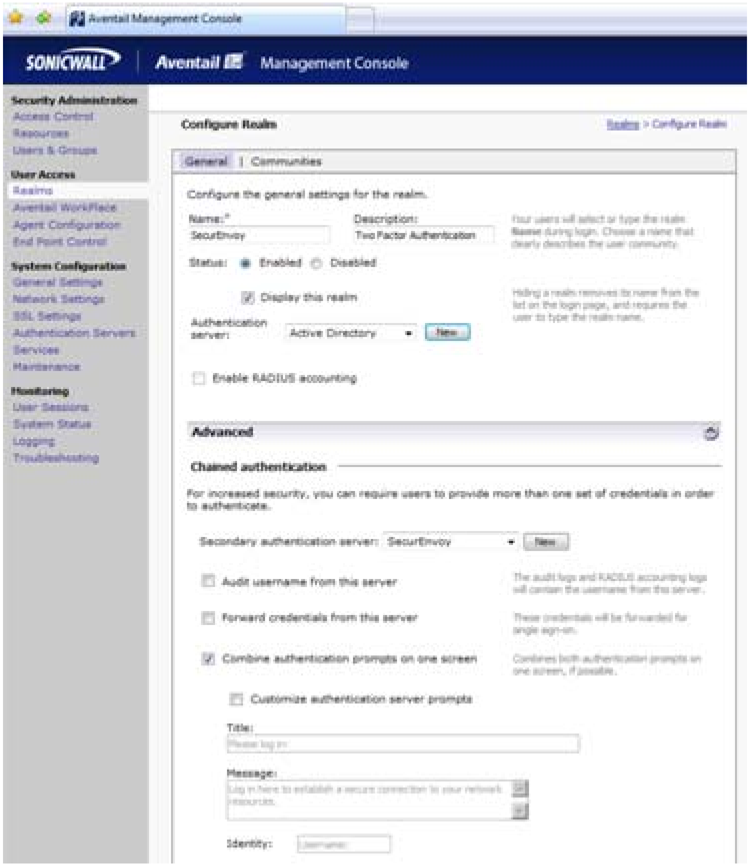
Communities: Default community

Lab Realm

*Default realm: LAB

The default realm will be preselected in user login screens.

a) Enter name information for the new realm
b) Select Active Directory as the authentication server
c) Select Advanced
d) Select SecurEnvoy for secondary authentication server
e) Select “Combine authentication prompts on one screen”



Configure Realm

Configure the general settings for the realm.

Name:* SecurEnvoy

Description: Two Factor Authentication

Your users will select or type the realm Name during login. Choose a name that clearly describes the user community.

Status: ● Enabled ○ Disabled

☑ Display this realm

Hiding a realm removes its name from the list on the login page, and requires the user to type the realm name.

Authentication server: Active Directory

□ Enable RADIUS accounting

Advanced

Chained authentication

For increased security, you can require users to provide more than one set of credentials in order to authenticate.

Secondary authentication server: SecurEnvoy

□ Audit username from this server

The audit logs and RADIUS accounting logs will contain the username from this server.

□ Forward credentials from this server

These credentials will be forwarded for single sign-on.

☑ Combine authentication prompts on one screen

Combines both authentication prompts on one screen, if possible.

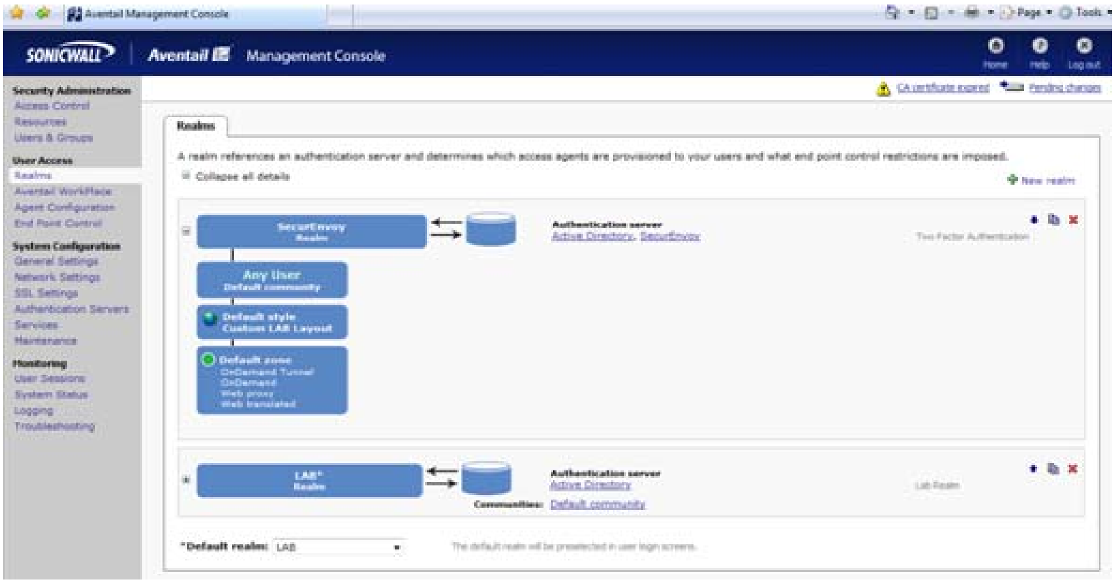
□ Customize authentication server prompts

Title: Please log in

Message: Log in here to establish a secure connection to your network resources.

Identity: Username

The new realm will now be displayed



A realm references an authentication server and determines which access agents are provisioned to your users and what end point control restrictions are imposed.

Collapse all details

SecurEnvoy Realm — Authentication server: Active Directory, SecurEnvoy — Two Factor Authentication

Any User Default community

Default style Custom LAB Layout

Default zone OnDemand Tunnel OnDemand Web proxy Web translated

LAB* Realm — Authentication server: Active Directory — Communities: Default community — Lab Realm

*Default realm: LAB

The default realm will be preselected in user login screens.

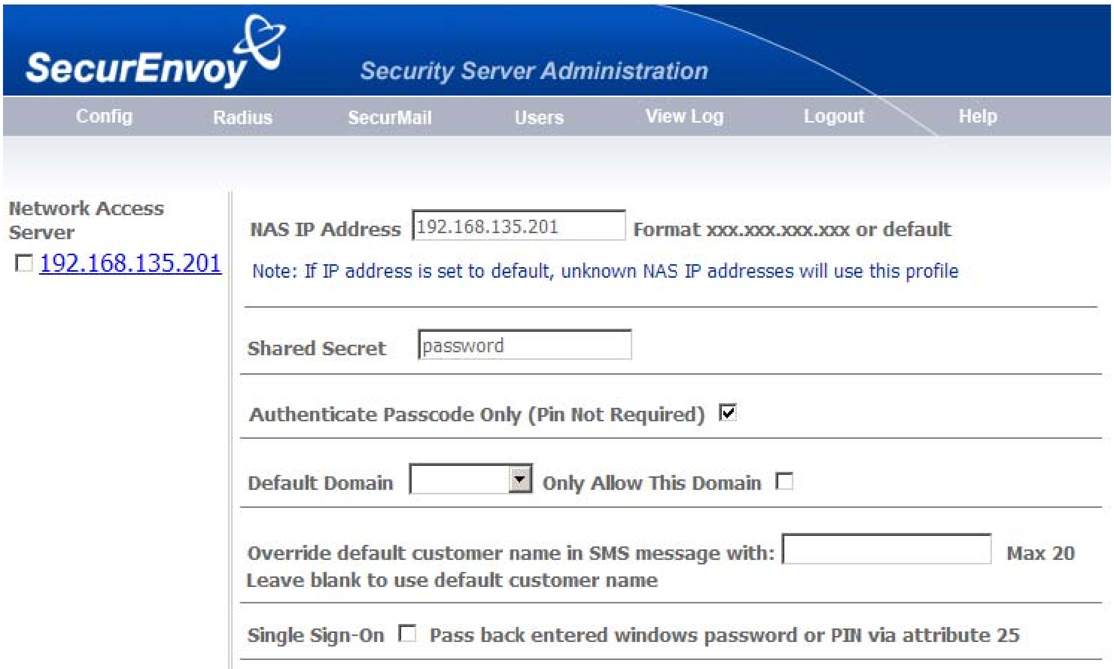
3.0 Configuration of SecurEnvoy

To help facilitate an easy to use environment, SecurEnvoy can utilise the existing Microsoft password as the PIN. This allows the users to only remember their Domain password. SecurEnvoy supplies the second factor of authentication, which is the dynamic one time passcode (OTP) which is sent to the user’s mobile phone.

Launch the SecurEnvoy admin interface, by executing the Local Security Server Administration link on the SecurEnvoy Security Server.

Click the **“Radius”** Button

Enter IP address and Shared secret for each SonicWALL® SSL VPN appliance that wishes to use **SecurEnvoy** Two-Factor authentication.



Network Access Server

□ 192.168.135.201

NAS IP Address 192.168.135.201 Format xxx.xxx.xxx.xxx or default

Note: If IP address is set to default, unknown NAS IP addresses will use this profile

Shared Secret password

Authenticate Passcode Only (Pin Not Required) ☑

Default Domain Only Allow This Domain □

Override default customer name in SMS message with: Max 20
Leave blank to use default customer name

Single Sign-On □ Pass back entered windows password or PIN via attribute 25

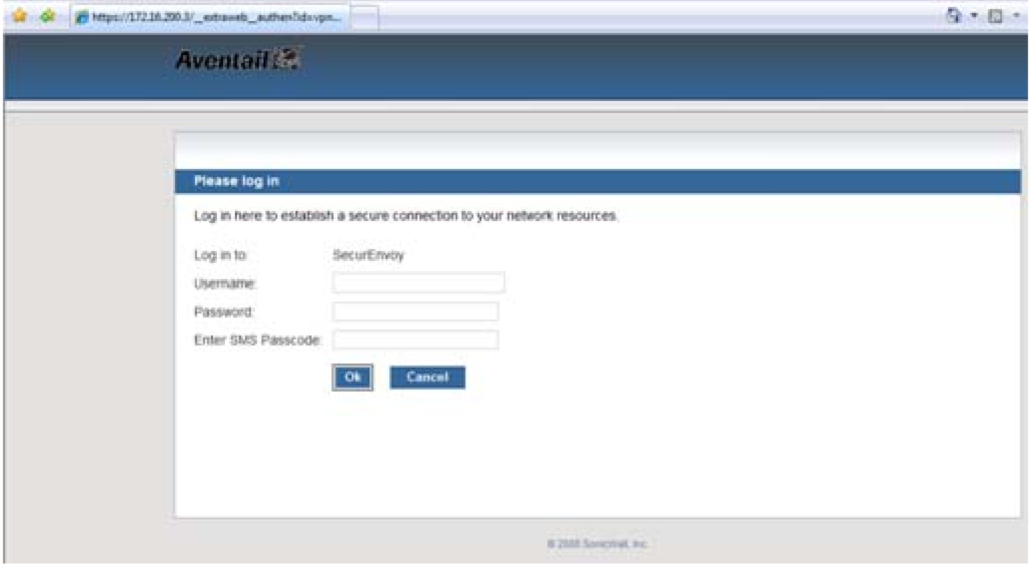
Click checkbox “Authenticate Passcode Only (PIN Not Required)

Click **“Update”** to confirm settings.

Click **“Logout”** when finished. This will log out of the Administrative session.

4.0 Test Logon

Open a browser and navigate to the logon page



https://172.16.200.3/__extraweb__authen?ids=vpn...

Please log in

Log in here to establish a secure connection to your network resources.

Log in to: SecurEnvoy

Username:

Password:

Enter SMS Passcode:

© 2008 SonicWall, Inc.