



## External Authentication with Perle Device Server IOLAN SDS

## Authenticating Users Using SecurAccess Server by SecurEnvoy

<b>Contact information</b>		
SecurEnvoy Ltd	<a href="http://www.securenvoy.com">www.securenvoy.com</a>	0845 2600010
	1210 Parkview Arlington Business Park Theale Reading RG7 4TY	<a href="mailto:Sales@securenvoy.com">Sales@securenvoy.com</a>
Perle Systems Europe Ltd	<a href="http://www.perle.com">www.perle.com</a>	01932 268591
	Abbey House Wellington Way Brooklands Business Park Weybridge Surrey KT13 0TT	<a href="mailto:Sales@perle.com">Sales@perle.com</a>

This document describes how to integrate Perle IOLAN SDS Device Servers with SecurEnvoy two-factor Authentication solution called 'SecurAccess'

The Perle IOLAN SDS is an advanced device server for secure serial to Ethernet connectivity. Delivering high performance in a compact size, the IOLAN SDS offers robust security, flexibility and next generation IPV6 technology making it ideal for applications that require remote device/console management, data capture or monitoring

SecurAccess provides two-factor, strong authentication for remote Access solutions (such as VPN, Web or serial connections), without the complication of deploying hardware tokens or smartcards.

Two-Factor authentication is provided by the use of your PIN and your mobile Phone to receive a one time passcode.

SecurAccess is designed as an easy to deploy and use technology. It integrates directly into Microsoft's Active Directory and negates the need for additional User Security databases. SecurAccess consists of two core elements: a Radius Server and Authentication server. The Authentication server is directly integrated with LDAP or Active Directory in real time.

Perle IOLAN SDS can be configured in such a way that it can proxy the Authentication request of the users to an external directory (such as Radius). Hereby the Perle IOLAN SDS device can protect designated telnet/SSH or serial connections with a two factor authentication. All authentication requests are forwarded to the SecurEnvoy Authentication server. SecurEnvoy utilizes a web GUI for configuration, whereas the Perle IOLAN configuration is shown with a Device Manager GUI, the unit can also be configure through the command line. All notes within this integration guide refer to the Device Manager type of approach.

The equipment used for the integration process is listed below

**Perle  
IOLAN SDS 2**

2-port secure device server, software selectable, EIA-232/422/485 interface, 10/100 Network SSH, SSL, port buffers

Version 1.3 (build 10)

<http://www.perle.com/products/product.asp?pid=04030104&cat=C003>

**Microsoft**

Windows 2000 server SP4

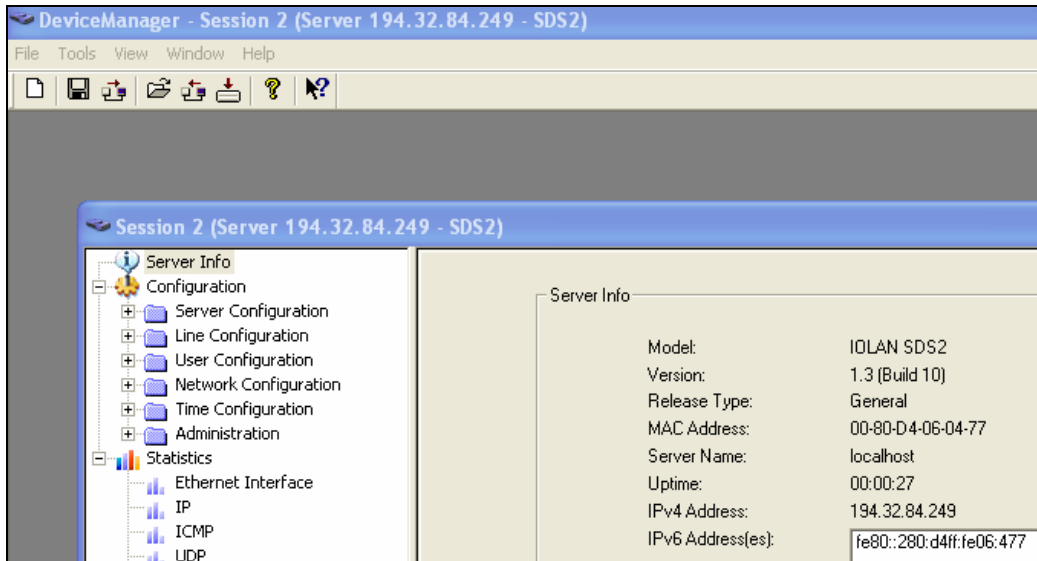
IIS installed with SSL certificate (required for management and remote administration)

Active Directory installed

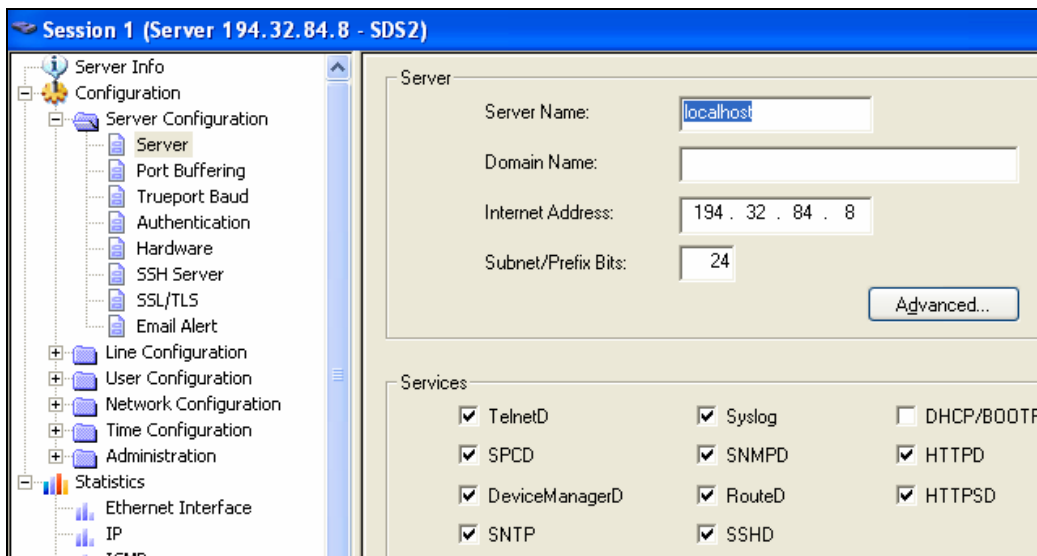
**SecurEnvoy**

SecurAccess software release v2.7 0100

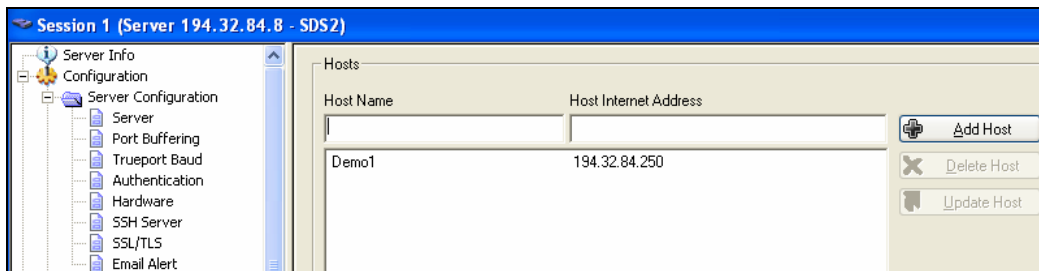
The Perle configuration is shown below, all screen shots show configuration via Perle's Device Manager Software, additional text has been added to help explain the configuration



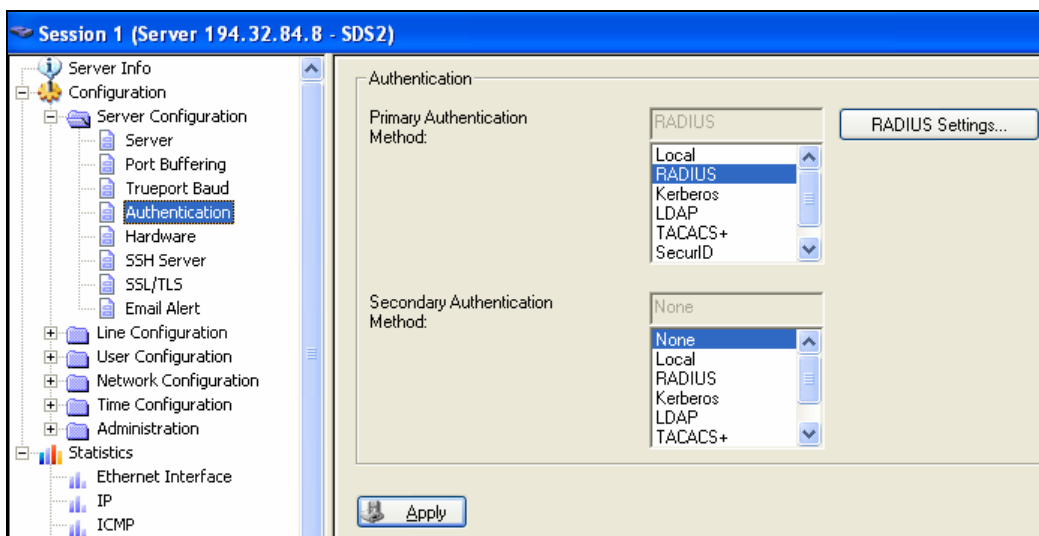
Open Device Manager Software. Device Manager will pick the unit off the local subnet by its MAC address. Double click on the unit and log into it with the password "superuser". You will now be presented with the screen above.



Select "Configuration" then "Server Configuration" then "Server". In this screen we set the IP address and disable DHCP by unchecking the box. Click "apply".



As we are adding a RADIUS, this has to go into a host table. Select "Network Configuration" then select "Hosts". Add the host name and the IP address, click "Add Host".



Set the Authentication. Under the "Server Configuration" menu, select "Authentication", then highlight "RADIUS" as the Primary Authentication method and select "RADIUS Settings..." If there is a secondary RADIUS then repeat these steps for that option as well.

### RADIUS Settings

**RADIUS Settings**

**Authentication Hosts**

First Authentication Host:  Secret:

Second Authentication Host:  Secret:

Authentication Port:

**Accounting**

Enable Accounting

First Accounting Host:  Secret:

Second Accounting Host:  Secret:

Account Port:

Enable Accounting Authenticator

**RADIUS Configuration**

Retry:  Timeout:

Select the RADIUS host you have just added, from the drop down box on "First Authentication Host". Add the "secret" that has been set on the RADIUS. Set the Authentication Port according to the RADIUS settings. If there is an accounting server then check the "Enable Accounting" box and fill in the details as per the Accounting Host. Change the RADIUS Configuration "Retry" settings from 5 to 2 and "Timeout" settings from 3 to 10.

### Session 1 (Server 194.32.84.8 - SDS2)

**Server Info**

- Configuration
  - Server Configuration
  - Line Configuration
    - Lines
    - Modems
  - User Configuration
  - Network Configuration
  - Time Configuration
  - Administration
- Statistics
  - Ethernet Interface
  - IP
  - ICMP
  - UDP
  - TCP
  - User
  - Netstat
  - Route
  - PPP Interface
  - SLIP Interface
  - Line

**Line 1**

Enable Line

Line Name:

Service:

DS Port:

Terminal Type:

**Hardware Settings**

Serial Interface:  Duplex:

Speed:  TX Driver Control:

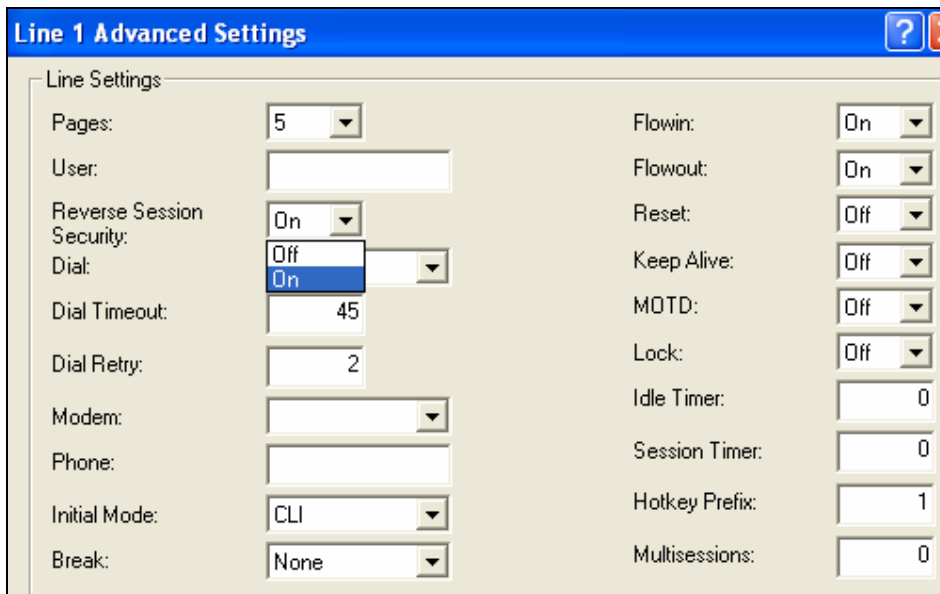
Bits:  Echo Suppression:

Parity:  Monitor DSR:

Stop Bits:  Monitor DCD:

Flow Control:

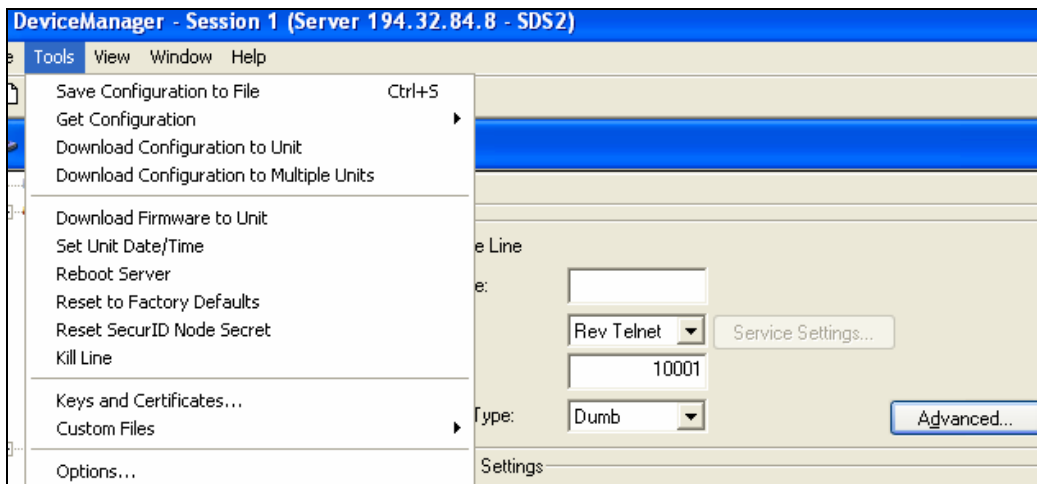
For console management, the port should be set for a reverse connection, in this instance the "Service" is set to "Rev Telnet". The "DS Port" is set to 10001- all other settings are unchanged. Confirm the device you are connecting to but these settings are correct for most devices. Click on the "Advanced..." tab.



The image shows the "Line 1 Advanced Settings" configuration window. The settings are as follows:

Setting	Value	Setting	Value
Pages:	5	Flowin:	On
User:		Flowout:	On
Reverse Session Security:	On	Reset:	Off
Dial:	On	Keep Alive:	Off
Dial Timeout:	45	MOTD:	Off
Dial Retry:	2	Lock:	Off
Modem:		Idle Timer:	0
Phone:		Session Timer:	0
Initial Mode:	CLI	Hotkey Prefix:	1
Break:	None	Multisessions:	0

In here, set the "Reverse Session Security" from "off" to "on" then click "OK".



The image shows the "DeviceManager - Session 1 (Server 194.32.84.8 - SDS2)" configuration window. The "Tools" menu is open, showing options like "Save Configuration to File", "Get Configuration", "Download Configuration to Unit", "Download Configuration to Multiple Units", "Download Firmware to Unit", "Set Unit Date/Time", "Reboot Server", "Reset to Factory Defaults", "Reset SecurID Node Secret", "Kill Line", "Keys and Certificates...", "Custom Files", and "Options...". The "Advanced..." button is visible in the bottom right corner.

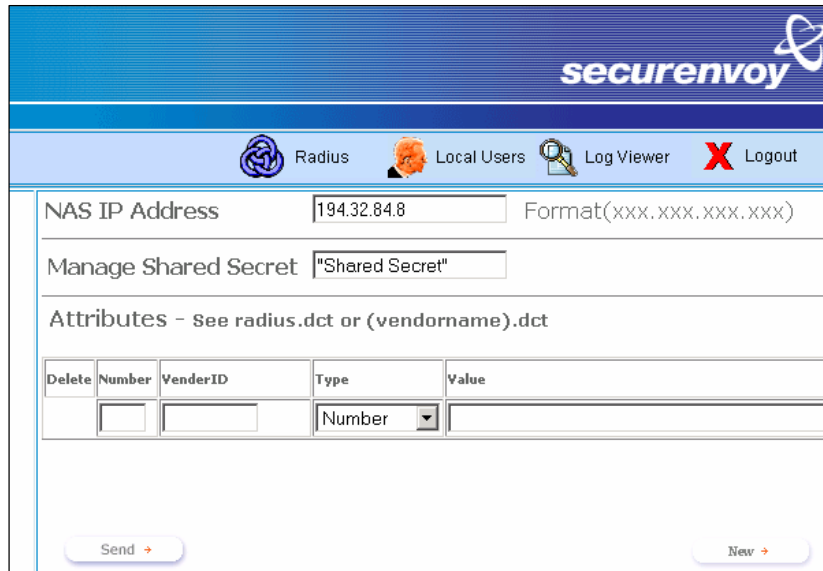
From the main tool bar menu, select "Tools" then "Download Configuration to Unit". This will send the config to the unit but it won't become active in the unit till the unit has been rebooted. Again go to "Tools" and select "Reboot Server". This will disconnect you from the unit and once the unit comes up, this config will be live in the unit.

## To set up Radius on SecurEnvoy SecurAccess

Launch local Security Server Administration - Select Radius

Enter NAS IP address; this will be the IP address of the Perle IOLAN SDS device server.

Enter "Radius Shared Secret" this must match what was entered within the Perle SDS config. Click "Send".



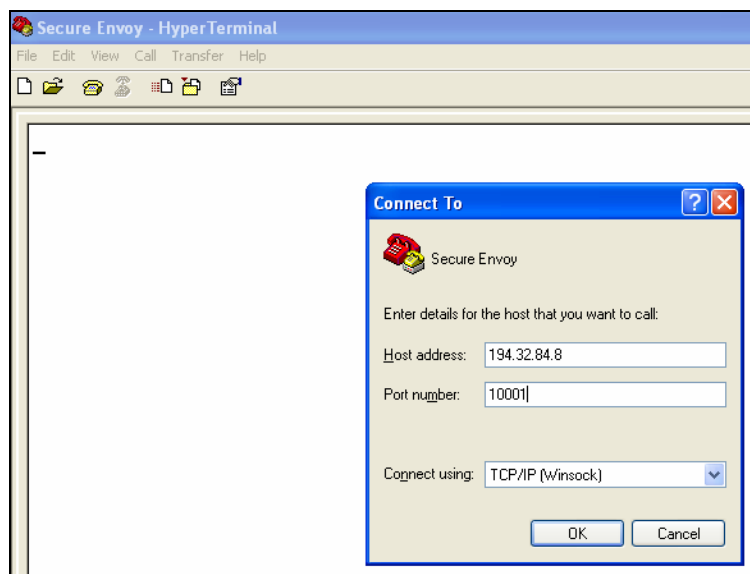
The screenshot shows the SecurEnvoy web interface for configuring the Radius server. The top navigation bar includes "Radius", "Local Users", "Log Viewer", and "Logout". The main configuration area contains the following fields:

- NAS IP Address: 194.32.84.8 (Format: xxx.xxx.xxx.xxx)
- Manage Shared Secret: "Shared Secret"
- Attributes - See radius.dct or (vendorname).dct

Delete	Number	VenderID	Type	Value
<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	Number	<input type="text"/>

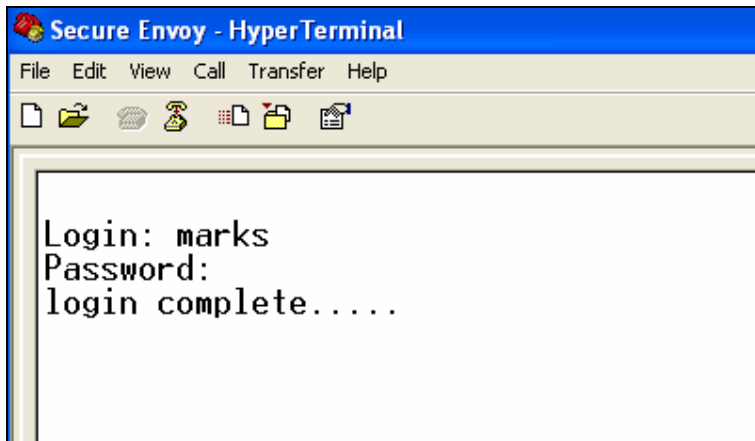
Buttons: "Send" and "New"

## Demonstrating the login using Hyper Terminal to a Microsoft Windows 2000 server serial port.



This is a set up for which we used Hyper Terminal to connect to a Windows 2000 Server. In the connection properties, we selected a TCP/IP connection.

This enabled us to be able to set the IP address of the Device Server and the Port number that the Windows Server was connected to.



We were prompted for a login. As the RADIUS configuration passed all Authentications to the SecurEnvoy security server, the login name is the user name that is configured within Microsoft Active Directory (shown here as "marks") and as Secure Envoy is the True Authentication method, the Password is the pin code set in SecurEnvoy, followed by the Passcode that had been sent via SMS to the users mobile phone. The "login complete...." was actually a message that was sent from the Windows Server, this was for demonstration purposes only.

This integration guide used Hyper Terminal; we also tested with Windows Telnet successfully. Any telnet package should work and the connection can be to any device with a console port, i.e. UNIX, Linux, SUN, PABX's, routers etc with all the security being handled from one central and trusted point.