

IOLAN Secure User's Guide V5.0

Updated: July 2018
Revision: A.1-07-04-2018
Document Part: 5500431-10

Preface

Audience

This guide is for the networking professional managing your IOLAN. Before using this guide, you should be familiar with the concepts and terminology of Ethernet and local area networking.

Purpose

This guide provides the information that you need to configure and manage your Perle IOLAN Product. For Web Manager (GUI) users, this guide provides the navigation reference that can be used within web sessions for each feature.

Product installation information can be found in the IOLAN Hardware Installation Guide for your product model on our Perle website at www.perle.com and in the Quick Start Guide that came with your product.

Additional Documentation

Document	Description
IOLAN Hardware Installation Guide	Product specific hardware guide on how to install your IOLAN.
IOLAN Quick Start Guide	Product specific Quick Start Guide that came with your IOLAN.
IOLAN CLI (Command Reference Guide) Guide V5.0 and greater	Command reference guide using CLI commands to configure the IOLAN (this is an advanced way to configure the IOLAN)

Document Conventions

This document contains the following conventions:

Most text is presented in the typeface used in this paragraph. Other typefaces are used to help you identify certain types of information. The other typefaces are:

Note: *Means reader take note:* notes contain helpful suggestions.

Guide Updates

This guide may be updated from time to time and is available at no charge from the download area of Perle's web site at <https://www.perle.com/downloads/>

Licensing

All Perle software pre-installed in Perle Products or downloaded from any other source or media is governed by Perle's End User License Agreement. USING THIS PERLE PRODUCT CONSTITUTES ACCEPTANCE OF THIS AGREEMENT. Please review the country specific End User License Agreement located at the following location prior to usage;

<https://www.perle.com/EULA.shtml/>

<https://www.perle.com/EULA-Germany.shtml/>

You also agree that Perle may collect, use, or disclose customer information in the course of fulfilling its obligations under the End User License Agreement, and such collection, use, and disclosure will be in accordance with Perle's privacy policy available at <https://www.perle.com>

IF YOU DO NOT AGREE TO ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT, You have no right to use the Perle Software and You should return the purchased product to Perle or the applicable reseller or distributor from whom you obtained the product.

Copyright Statement

This document must not be reproduced in any way whatsoever, either printed or electronically, without the consent of:

Perle Systems Limited,
60 Renfrew Drive
Markham, ON
Canada
L3R 0E1

Perle reserves the right to make changes without further notice, to any products to improve reliability, function, or design.

Perle, the Perle logo, and IOLAN are trademarks of Perle Systems Limited.

Microsoft, Windows NT®/Windows 2000®/Windows Vista®/Windows Server 2003®/Windows 2003 R2®/Windows 2008®/Windows 2008 R2®/Windows XP®/Windows 7®/Windows 8®/Windows 8.1®/Windows Server 2012®/Windows Server 2012 R2® /Windows Server 2016® /Windows 10 and Internet Explorer® are trademarks of Microsoft Corporation.

Solaris® is a registered trademark of Sun Microsystems, Inc. in the USA and other countries.
Perle Systems Limited, 2005-2018.

FCC Note The IOLAN Device Server series has been found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions in this Guide, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his/her own expense.

EN 55022: 1998, Class A, Note

WARNING This is a Class A product. In a domestic environment this product may cause radio interference in which case the user maybe required to take adequate measures.

Caution: the IOLAN product is approved for commercial use only.

Publishing History

Date	Revision	Update Details
July 2018	A.07.04.2018	Initial release of the IOLAN SCG series.

Preface	2
Publishing History	4
About the IOLAN	5
Hardware Features	5
General Features	5
Secure Features	5
Security	6
Setting Up the Network.....	7
Methods of Configuring the IOLAN	7
Configuring an IP Address	7
DeviceManager	8
Installing the DeviceManager to your PC	8
WebManager	12
Logging in to the IOLAN using WebManager.....	13
EasyPort Web	15
Command Line Interface.....	15
Connecting through the Network.....	15
Connecting to the Console Port(s).....	16
DHCP/BOOTP	16
Using DHCP/BOOTP	16
SNMP.....	17
Connecting to the IOLAN Using SNMP	17
Using the SNMP MIB	19
Network Settings	20
IPv4 Settings.....	20
WLAN (only applies to certain models)	25
Client Mode	25
Soft-AP Mode.....	25
WWAN (only applies to certain models).....	31
Host Table	32
IP Filtering.....	32
Routes	32
DNS/WINS	33

RIP	34
Dynamic DNS.....	35
IPv6 Tunnels	38
Serial Ports.....	39
Console Management Profile	47
Trueport Profile.....	51
TCP Sockets Profile	56
UDP Sockets Profile	61
Terminal Profile	66
User Service Settings.....	69
Serial Tunneling Profile.....	79
Virtual Modem Profile.....	81
Modbus Gateway Profile	85
Power Management Profile.....	89
Remote Access (PPP) Profile.....	91
Remote Access (SLIP) Profile	99
Custom Application Profile	102
Remote Port Buffers	103
Serial Settings Advanced Parameters	104
Modem Parameters	106
Adding/Editing a Modem	106
Trueport Baud Rate Parameters	106
Setting Up Users	107
Adding/Editing Users	107
User Services Parameters	108
User Sessions.....	111
User Sessions Parameters	112
Serial Port Access	112
Authentication	113

Security Overview	113
Setting Primary and Secondary Authentication Methods.....	113
Local	114
RADIUS	115
KerberosLDAP/Microsoft Active Directory	116
TACACS+	118
Securid	119
NIS.....	120
NIS Authentication Parameters	120
Users Logging into the IOLAN Using SSH	120
Users Passing Through the IOLAN Using SSH (Dir/Sil)	120
SSL/TLS	122
Authentication Parameters.....	123
VPN.....	126
IPsec.....	127
L2TP/IPsec	130
Alerts	139
Email Alerts	139
Email Alert Parameters.....	139
Syslog Parameters.....	140
Management	141
SNMP Parameters.....	141
SNMP Trap Parameters	142
Custom App/Plugin	144
Custom App Parameters	144
Control RPS, IPSec, WLAN and WWAN.....	149
RPS Control.....	149
Plug Control.....	149
Serial Port Power Control	150
Power Plug Status	151
IPsec Tunnel Control	151
WLAN Control	151
WWAN Control.....	152
RADIUS External Parameters	162
Supported RADIUS Parameters	162
Applications	176

Dynamic DNS.....	176
Dynamic DNS Update	176
Using Dynamic DNS Behind a NAT Router.....	176
Power Management	177
Machine To Machine Connections.....	178
Creating User Sessions	179
Configuring Modbus.....	179
Configuring PPP Dial On Demand.....	182
Configuring a Virtual Private Network	185
Configuring HTTP Tunnels	192
Tunnel Relay.....	197
Virtual Modem Initialization Commands.....	1
TruePort.....	1
Modbus Remapping Feature.....	2
Data Logging Feature	3
Trueport Profile	3
TCP Socket Profile	3

About the IOLAN

The IOLAN is an Ethernet communications/terminal server that allows serial devices to be connected directly to your network. The IOLAN attaches to your network using TCP/UDP/IP and allows serial devices such as modems and terminals, or printers to access the LTE/WLAN/LAN. It also allows LTE/WLAN/ LAN devices to access devices or equipment attached to IOLAN serial ports.

The IOLAN can connect to a wide range of devices including:

- Terminals for multi-user UNIX systems
- Data acquisition equipment (manufacturing, laboratory, scanners, etc)
- Retail point-of-sale equipment (bar coding, registers, etc.)
- PC's using terminal emulation or SLIP/PPP protocols
- Configurable serial modems
- All types of serial printers

The performance and flexibility of the IOLAN allows you to use a wide range of high speed devices in complex application environments. The IOLAN products will work in any server environment.

Hardware Features

See the IOLAN Hardware Installation Guide that came with your model for more information.

General Features

This section highlights the software components you can expect to find in your IOLAN model.

Basic IOLAN software features are available on all IOLAN models.

- IPv6 support
- Support for TCP/IP and UDP protocols including telnet and raw connections
- Printer support via LPD and RCP
- Virtual modem emulation
- 'Fixed tty' support for several operating systems using Perle's TruePort utility
- DHCP/BOOTP for automated network-based setup
- Dynamic statistics and line status information for fast problem diagnosis
- Multi-session support when accessing the IOLAN from either the serial port or the network
- Modbus master/slave/gateway support
- An SDK (Software Development Kit) for custom programs and plugin support
- Ability to disable services (for example, Telnet, TruePort, Syslog, SNMP, Modbus, HTTP) for additional security
- Logging via syslog
- Ability to disable Ping responses

Secure Features

- External system authentication:
 - RADIUS
 - Kerberos
 - TACACS+
 - NIS
 - SecurID
- LDAP/Microsoft Active Directory
- Dynamic DNS with DYNDNS.org
- Domain Name Server (DNS) support
- WINS support for Windows® environments
- Remote access support including PPP, SLIP, and SLIP with VJ Compression
- Ability to remotely manage the Perle Remote Power Switch (RPS)
- Ability to cluster several IOLANs

-
- Email alert notification
 - PPP authentication via PAP /CHAP/ MSCHAP
 - CHAP(MD5) authentication support to TACACS+ servers
 - SSH connections (supported ciphers are Blowfish, 3DES, AES-CBC, AES-CTR, AES-GMC, CAST, Arcfour and ChaCha20-Poly1305)
 - SSL/TLS connections
 - RIP authentication (via password or MD5)
 - SNMP (versions 1, 2, 3, and 4 are supported)

Security

Security features will vary depending on your IOLAN model

- Supervisory and serial port password protection
- Ability to set serial port access rights
- Ability to assign users access level rights to control their access
- Trusted host filtering (IP filtering), allowing only those hosts that have been configured in the IOLAN access to the IOLAN
- Idle port timers, which close a connection that has not been active for a specified period of time
- Ability to individually disable network services that won't be used by the IOLANSSH client/server connections (SSH 1 and SSH 2)
- SSL/TLS client/server data encryption (TLSv1/1.1/1.2 and SSLv2)
- Ability to setup Virtual Private Networks
- Access to firewalled/NAT'ed devices via HTTP tunnels
- Wireless Security; WEP, WPA2-PSK & Enterprise (EAP, PEAP, LEAP), 802.11i
- Wireless cellular security using PAP or CHAP authentication
- Front panel keyboard lock

Setting Up the Network

The most important part of setting up the network is assigning an IP address to the IOLAN, whether this is a static IP address or enabling a DHCP/BOOTP-assigned IP address. You should also assign a name to the IOLAN, to make it easier to recognize. This section deals primarily with setting the IP address.

Methods of Configuring the IOLAN

There are two ways you can access the IOLAN, through the network or through the serial connection. If you are accessing the IOLAN through the network, the IOLAN must already have a known IP address configured; for information see [Configuring an IP Address](#).

Some of the IOLAN configuration methods have the capability of configuring an IP address, which is the first required configuration step for a new IOLAN. Once the IOLAN has been assigned an IP address, any of the configuration methods can be used to configure the IOLAN.

Configuring an IP Address

Following is a list of methods for setting the IOLAN IP address and a short explanation of when you would want to use that method:

- **DeviceManager**—Use this method when you can connect the IOLAN to the network and access the IOLAN from a Windows® PC. The DeviceManager is a Windows®-based application that can be used for IOLAN configuration and management. The DeviceManager can be used to assign an IP address and perform the complete configuration and management of the IOLAN. See [DeviceManager](#) for more information on using the DeviceManager.
- **WebManager**—Use this method when you have already set the IOLAN with an IP address. This method cannot be used to initially set an IP address on the IOLAN. See [Downloading the Configuration with WebManager](#) for more information on using the WebManager.
- **Direct Connection**—Use this method when you can connect to the IOLAN from a serial terminal or from a computer running terminal emulation software over a serial port. Using this method, you will need to configure and/or manage the IOLAN using the CLI.
- **DHCP/BOOTP**—Use this method when you have a BOOTP or DHCP server running and you can connect the IOLAN to your network. The IOLAN will automatically obtain an IP address from a local network DHCP/BOOTP server when this service is enabled (it is disabled by default). You can also configure certain IOLAN parameters that will be passed from the DHCP/BOOTP server to the IOLAN when it boots up. Other configurators such as DeviceManager or CLI can be used to set this option, and obtain the initial IP address.
- **ARP-Ping**—Use this method when you can connect the IOLAN to the network and want to assign a temporary IP address to the IOLAN by adding an ARP entry to your PC and then ping-ing it.
- **IPv6 Network**—When the IOLAN is connected to an IPv6 network, its local link address is determined using stateless auto configuration.

DeviceManager

The DeviceManager is a Windows®-based application that can be used to connect to the IOLAN to actively manage and configure it or can create new IOLAN configurations off-line. The DeviceManager can be run from Windows 2000®/Windows Vista®/Windows Server 2003®/Windows 2003 R2®/Windows 2008®/Windows 2008 R2®/Windows XP®/Windows 7®/Windows 8®/Windows 8.1®/ Windows Server 2012®/ Windows Server 2012® R2, Windows Server 2016® and Windows 10.

Device Manager Features

Some DeviceManager features are:

- The ability to download the same configuration file to several IOLANs in one operation.
- The ability to save a configuration file locally in text format, in addition to the binary format.
- The ability to create a configuration file without being connected to the IOLAN.
- The ability to open a session to the IOLAN and download a (saved) configuration file to it.
- The ability to download/upload keys/certificates to/from the IOLAN.
- The ability to download custom files, such as new terminal definitions and custom languages to the IOLAN.

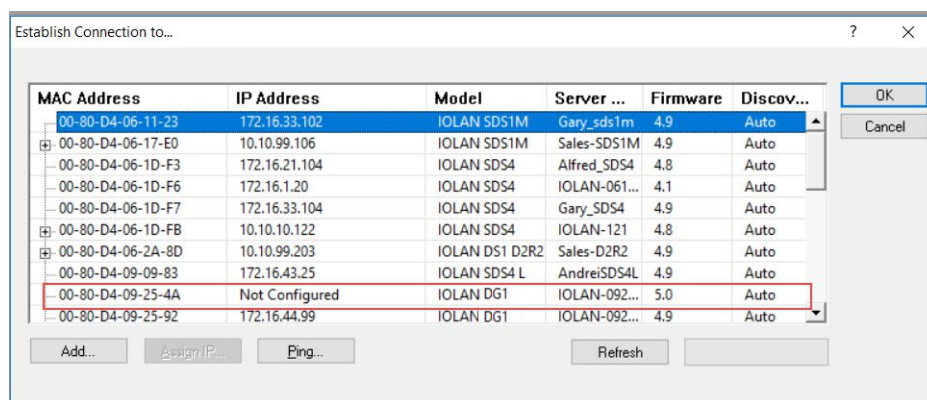
Installing the DeviceManager to your PC

Before you can use DeviceManager, you need to install it on your Windows operating system from the Perle website at www.perle.com. After the DeviceManager application is installed, select the Start icon, then scroll through the Applications and select the Perle Folder, then select the Perle Devicemanager application. When you launch the DeviceManager, it will scan the network for IOLANs. All discovered IOLANs will be displayed on the list along with their name and IP address. When a new IOLAN is discovered on the network, that has not yet been assigned an IP address, it will be displayed with an IP Address of **Not Configured**. If routers on the network have been setup to propagate multi-casts, DeviceManager will also be able to discover IOLANs in other networks. To configure the IP address, select the IOLAN and then select the **Assign IP** button.

Assigning a Temporary IP Address to a New IOLAN

A new IOLAN will show in the display list as **Not Configured**. You can temporarily assign an IP address to the IOLAN that is connected to your local network segment, for the purpose of connecting to it and downloading a configuration file (containing a permanent IP address). To temporarily assign an IP address to the IOLAN, do the following:

1. Select the **Refresh** button. The IOLAN will be displayed in the **IP Address** column as **Not Configured**.



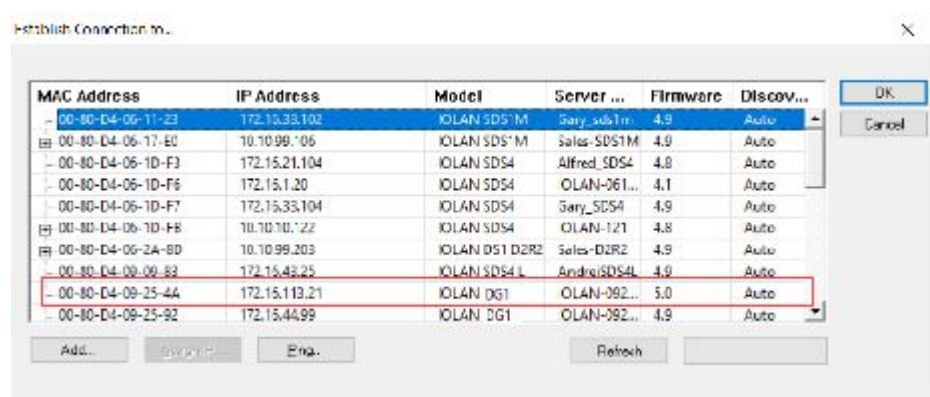
2. Type a valid temporary IP address into the address field or enable the **Have the IOLAN automatically get a temporary IP address**. If you enable the temporary IP address, the IOLAN will enable DHCP/BOOTP on your IOLAN and attempt to get an IP address from the DHCP/BOOTP server (this will permanently enable DHCP/BOOTP in your IOLAN's configuration, until you change it). If your network does not have a DHCP/BOOTP server, the IOLAN will temporarily assign an IP address of 192.168.1.124 with a subnet of 255.255.255.0 (this IP address is only assigned for the duration of the DeviceManager/IOLAN connection).
3. Select the **Assign IP** button.
4. After you configure the IP address, select the **Assign IP** button.

Starting a New Session

To start a new session and connect to the IOLAN using the DeviceManager:

Start the DeviceManager by selecting **Start, All Programs, Perle, DeviceManager, DeviceManager**.

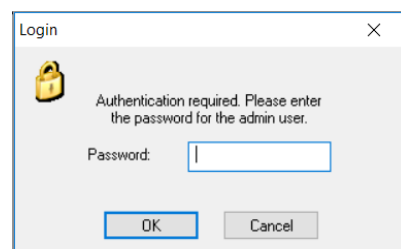
When the DeviceManager starts, it searches the network for IOLANs.



Note: If you are not seeing IPv6 addresses in the list (you must expand the entry).

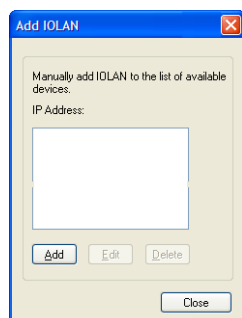
Logging into the IOLAN with DeviceManager

The refreshed list will now display the assigned IP address for the new IOLAN. To connect to the IOLAN, select the IOLAN entry and select **OK**. If this is the first time you are accessing the IOLAN, type in the factory default admin password, **superuser**, and select **OK**. The DeviceManager will display a window indicating that it is trying to authenticate and connect you to the IOLAN.

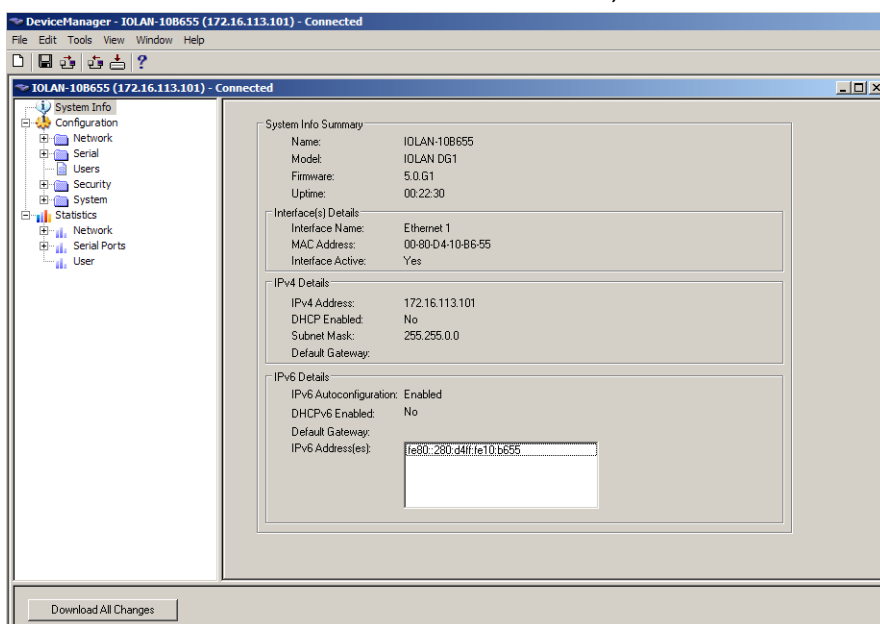


Adding/Deleting IOLANs Manually

To permanently add the IOLAN to the IOLAN list, select the **Add** button and type in the IPv4 or IPv6 address of the IOLAN. To permanently delete the IOLAN from the IOLAN list, select the IOLAN's IP address and select the **Delete** button.



If the authentication and connection are successful, the IOLAN's **Server Info** window is displayed.



If you cannot connect to the IOLAN, you can highlight the IOLAN and selecting the **Ping** button to verify that the DeviceManager can communicate with the IOLAN's IP Address. If the ping times out, then you might need to set up a Gateway in your IOLAN or verify that your network is communicating correctly. If your IOLAN is not in the local network and you do not have a multi-cast enabled router in your network and therefore the IOLAN is not displayed in the selectable list, but can be pinged from your PC, you can add it to the selectable list by selecting the **Add** button.

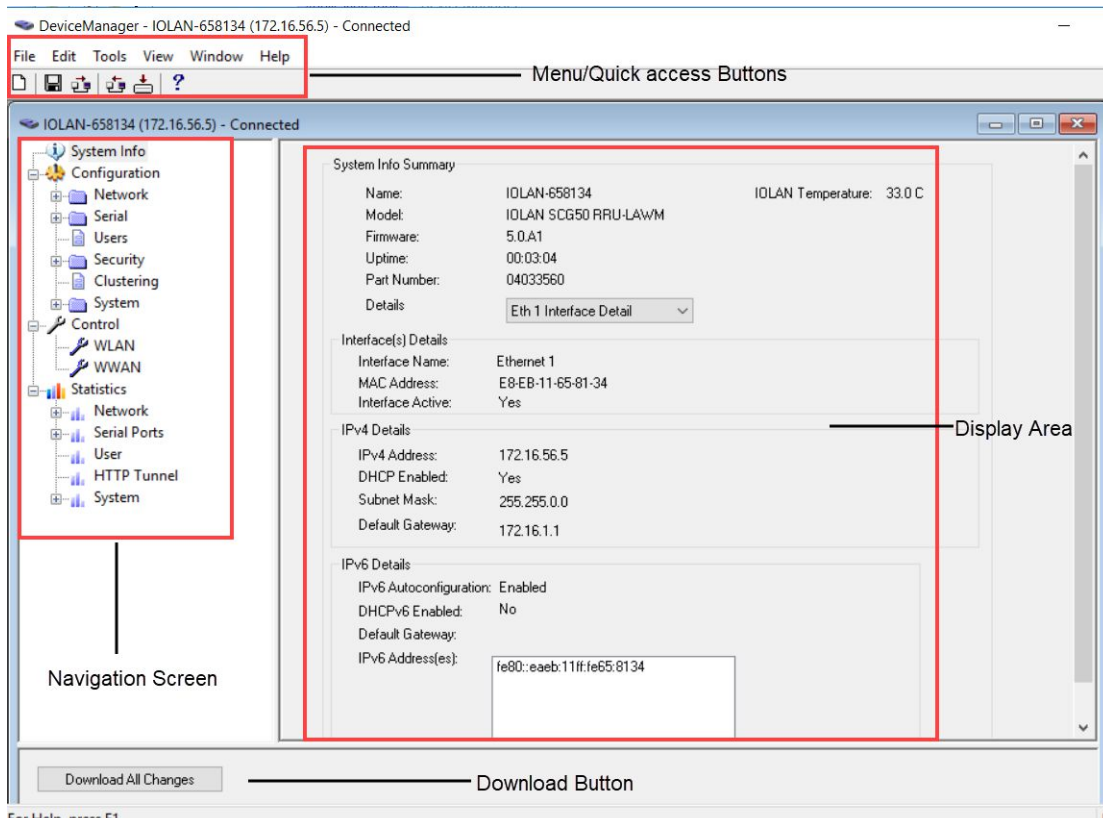
Note: The DeviceManager does not automatically update the IOLANs configuration. You must download the configuration changes to the IOLAN and then reboot the IOLAN to make the configuration changes take effect.

You are now ready to configure the IOLAN.

Navigating the DeviceManager

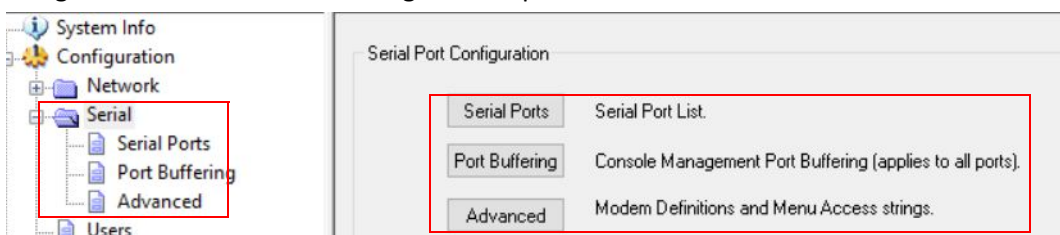
The DeviceManager has a navigation tree that you can use to access the available Configuration and Statistics pages in the display area. When you select an option in the navigation tree, you can often navigate the tabs or buttons in the display area to access the various configuration and statistics options.

Navigating the Options



The left-hand navigation tree allows you to quickly and easily navigate the various Configuration and Statistics pages of DeviceManager. Further navigation is available in the form of buttons and tabs in the display area of DeviceManager, depending on where you are in the navigation tree, as shown in the below.

Notice that when you expand a parent node in the tree (e.g., **Serial**), the tree displays the same options that appear as buttons in the display area, as shown below. This gives you the choice of using the navigation tree or buttons to navigate the options.

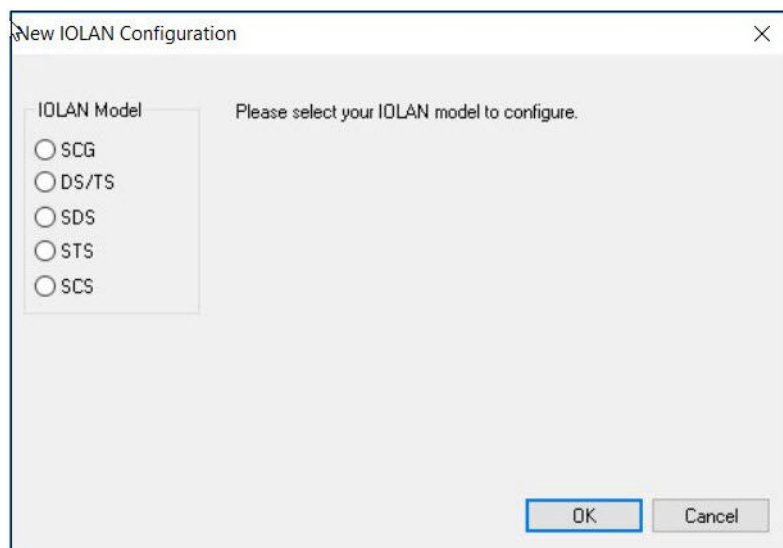


Downloading the Configuration with DeviceManager

When you have completed all your configuration changes, select the **Download All Changes** button to download the configuration to the IOLAN. You must reboot the IOLAN for your configuration changes to take effect.

Creating a New IOLAN Configuration in DeviceManager

In DeviceManager, when you select **File, New**, the New Configuration window is displayed.



Select the IOLAN model for which you want to create a new configuration file. Any configuration file created in this manner can only be save locally. To download a created configuration file, you must first connect to the IOLAN, import the created configuration file into DeviceManager (this is not available in WebManager), and then download the configuration file to the IOLAN and reboot it. Opening an Existing Configuration File

If you select the **File, Open**, a browse window is opened so you can select the configuration file you want to edit. IOLAN configuration files saved in the DeviceManager can be in the IOLAN-native binary format (.dme) or as a text file (.txt), which can be edited with a text editor. Either configuration version can be imported into the DeviceManager. IOLAN configuration files saved from WebManager can also be opened into DeviceManager.

Importing an Existing Configuration File

If you have a local, saved configuration file that you want to download to the IOLAN, you must first connect to the IOLAN that you want to download the configuration file to. Once you have successfully logged into the IOLAN, in DeviceManager select **Tools, Import Configuration from a File** and in WebManager select **Administration, Restore/Backup**. You need to download the file in DeviceManager and in both managers you need to reboot the IOLAN.

WebManager

Using the WebManager

The Perle WebManager is an embedded Web based application that provides an easy to use browser interface for managing the IOLAN. This interface provides the ability to configure and manage the IOLAN. This is accessible through any standard desktop web browser. You must have preconfigured a valid IP address on the IOLAN before connecting with the WebManager.

WebManager Features

Some Perle WebManager features are:

- The ability to downloading firmware to the IOLAN.
- The ability to reset serial ports.

-
- The ability to download/upload keys/certificates to/from the IOLAN.
 - The ability to download custom files, such as new terminal definitions and custom languages to the IOLAN
 - The ability to set the time and date

Logging in to the IOLAN using WebManager

WebManager can connect to IOLANs that already have an assigned IP address or wirelessly to an IOLAN with the wireless feature. See *WLAN (only applies to certain models)* settings in this guide for configuration options for Client or Soft AP mode.

To connect to the IOLAN, type the IP address of the IOLAN into the **Address bar** on your browser such as: `http://10.10.234.34`. (Your IOLAN IP address)

You will see the login screen. You will be prompted for the admin Password (the default is `superuser`).



If the authentication and connection are successful, the IOLAN's **Server Info** window is displayed.

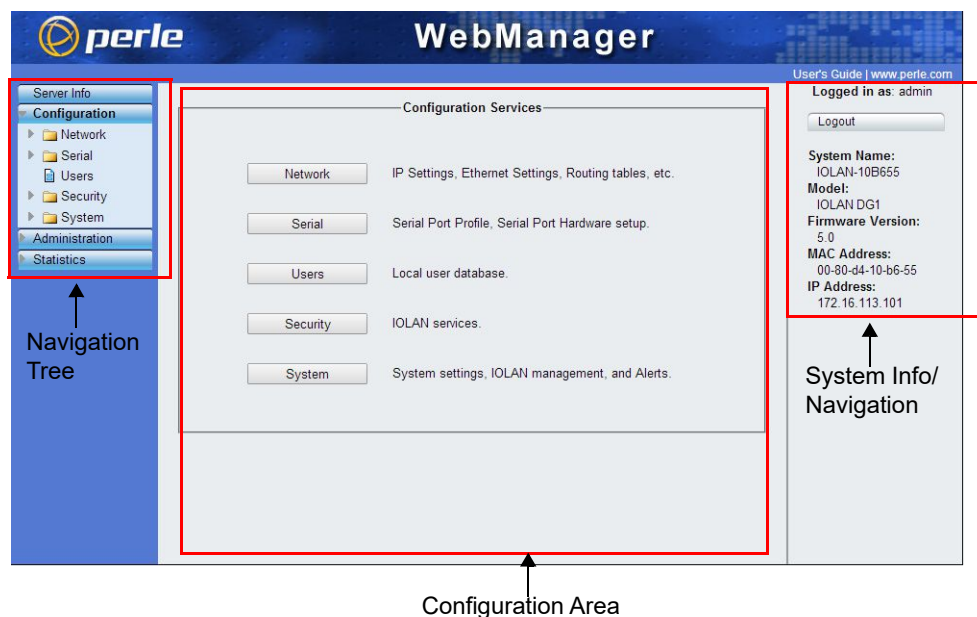
You are now ready to configure the IOLAN.

WebManager also launches EasyPort Web, which is a browser-based management tool that can be used to manage clustered IOLANs and Remote Power Switches (RPS). EasyPort Web can also be launched by any user who can connect to the IOLAN through a web browser.

Navigating the WebManager

The WebManager uses a expandable/collapsible buttons with folders and pages for the navigation tree. You can expand the buttons to view the folders and pages to see the available configuration options. When you access a configuration page, you can often navigate the tabs in the configuration area to access all of the configuration options.

When using WebManager, you are required to select the **Apply** button each time you make a change to a configuration window/tab.

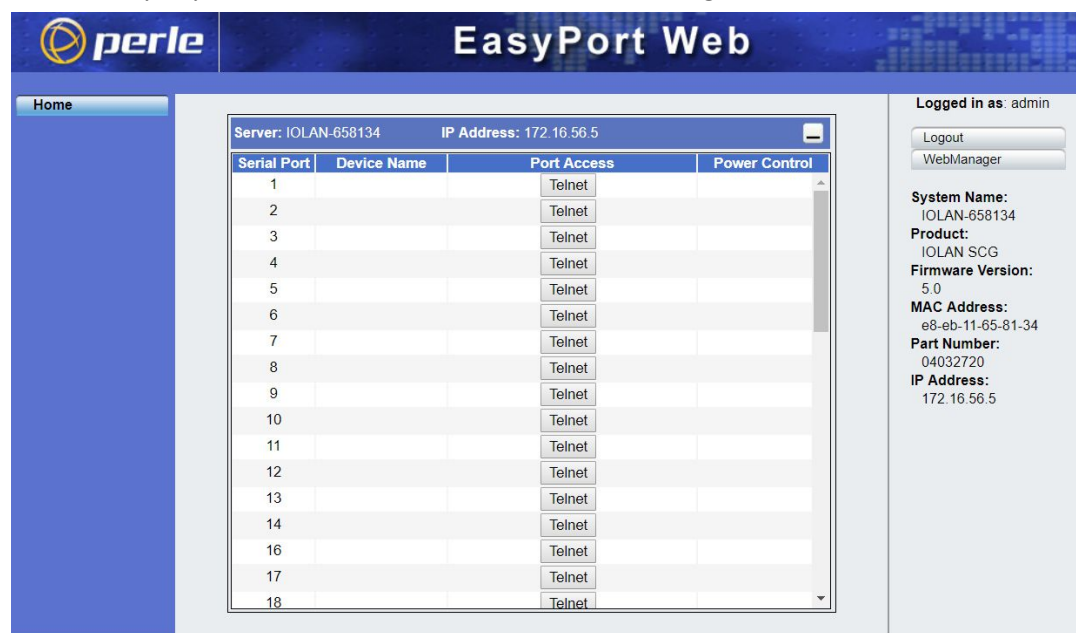


Downloading the Configuration with WebManager

The configuration is automatically downloaded when you select the apply button on each page. Most changes require a reboot of the IOLAN in order to take effect. Some changes such as serial port parameters can be made to take effect by simply resetting the serial port.

EasyPort Web

WebManager also launches EasyPort Web, which is a browser-based management tool that can be used to manage clustered IOLANs, Remote Power Switches (RPS), and power plugs. EasyPort Web can also be launched by any user who can connect to the IOLAN through a web browser.



Command Line Interface

The Command Line Interface (CLI) is a command line option for IOLAN configuration/management. See the *IOLAN Secure Command Line Interface Reference Guide V5.0* for a full breakdown of commands. The CLI is accessed by any application that supports a Telnet or SSH session to the IOLAN's IP address, such as Putty, SecureCRT, or you can connect directly to the admin console port.

After you have successfully logged in, you can start configuring/managing the IOLAN by typing in commands at the prompt. If you are not sure what commands are available, you can type a ? (question mark) at any time during a command to see your options.

Connecting through the Network

To connect to the IOLAN through the network to configure/manage it using the CLI, do the following:

1. Start a Telnet or SSH session to the IOLAN's IP address (IP address must be preconfigured).
2. You will get a **Login:** prompt. You can login as the admin user or as a user with Admin Level rights. If the login is successful, you will get a prompt that displays the IOLAN model and number of ports:

```
Login: admin
Password:
```

```
for exampleSCG32, DG1#
```

You will see a prompt that displays the model and number of serial ports on the IOLAN. You are now ready to start configuring/managing your IOLAN using the CLI.

See the *IOLAN Secure Command Line Interface Reference Guide V5.0* and greater for more information about using the CLI.

Connecting to the Console Port(s)

Depending on the model of IOLAN you purchased, connecting to the console port can be done in a variety of ways; using a DIP switch to set the port to Console mode, then connecting with a null modem serial cable, connecting to the IOLAN with the DB9 to RJ45 adapter that was shipped with your product or connecting to the standard Micro-B USB port via a USB cable to the front of the IOLAN. After you have established a connection to the IOLAN, you will get a **Login:** prompt. You can login as the admin user or as a user with Admin Level rights. If you are not sure what commands are available, you can type a ? (question mark) at any time during a command to see your options. See the **IOLAN Hardware Installation Guide** for your model to determine the method of connecting to your specific model.

DHCP/BOOTP

Connecting to the IOLAN Using DHCP/BOOTP

The IOLAN will automatically request an IP address from the DHCP/BOOTP server when the **Obtain IP address automatically using DHCP/BOOTP** parameter is enabled. By default, DHCP is disabled

Using DHCP/BOOTP

To use DHCP/BOOTP, edit the bootp file with IOLAN configuration parameters. You can use DHCP/BOOTP to perform the following actions on a single or multiple IOLANs on boot up:

- auto-configure with minimal information; for example, only an IP address
- auto-configure with basic setup information (IP address, subnet/prefix bits, etc.)
- download a new version of firmware
- download a full configuration file

DHCP/BOOTP is particularly useful for multiple installations: you can do all the IOLANs' configuration in one DHCP/BOOTP file, rather than configure each IOLAN manually. Another advantage of DHCP/BOOTP is that you can connect the IOLAN to the network, turn on its power and let autoconfiguration take place. All the configuration is carried out for you during the DHCP/BOOTP process.

DHCP Parameters

The following parameters can be set in the DHCP/BOOTP bootp file:

- **SW_FILE**—The full path, pre-fixed by hostname/IP address (IPv4 or IPv6), and file name of the firmware update.
- **CONFIG_FILE**—The full path, pre-fixed by hostname/IP address (IPv4 or IPv6), and file name of the configuration file.
- **GUI_ACCESS**—Access to the IOLAN from the HTTP or HTTPS WebManager. Values are **on** or **off**.
- **AUTH_TYPE**—The authentication method(s) employed by the IOLAN for all users. You can specify the primary and secondary authentication servers, separated by a comma. This uses the following numeric values for the authentication methods.
 - **0**—None (only valid for secondary authentication)
 - **1**—Local
 - **2**—RADIUS
 - **3**—Kerberos
 - **4**—LDAP/Microsoft Active Directory
 - **5**—TACACS+
 - **6**—SECURID
 - **7**—NIS

- **SECURITY**—Restricts IOLAN access to devices listed in the IOLANs host table. Values are **yes** or **no**.
- **TFTP_RETRY**—The number of TFTP retries before aborting. This is a numeric value, for example, 5.
- **TFTP_TMOUT**—The time, in seconds, before retrying a TFTP download/upload. This is a numeric value, for example, 3.
- **CUSTOM_LANG**—The full path, pre-fixed by a hostname/IP address (IPv4 or IPv6), and file name of a translated language file. For example,
192.101.34.211 /accounting/Iolan_ds_german.txt.
- **EXTRA_TERM1**—(**EXTRA_TERM2**, **EXTRA_TERM3**) The full path, pre-fixed by a hostname/IP address (IPv4 or IPv6), and file name of a termcap file for a specific terminal type.

Several IOLAN parameters can be configured through a DHCP/BOOTP server during the IOLAN boot up. This is particularly useful for configuring multiple IOLANs.

Using ARP-Ping

You can use the ARP-Ping (Address Resolution Protocol) method to temporarily assign an IP address and connect to your IOLAN to assign a permanent IP address. To use ARP-Ping to temporarily assign an IP address:

From a local UNIX/Linux host, type the following at the system command shell prompt:

```
arp -s a.b.c.d aa:bb:cc:dd:ee:ff
```

On a Windows® 2000 or newer system, type the following at the command prompt:

```
arp -s a.b.c.d aa-bb-cc-dd-ee-ff
```

(where **a.b.c.d** is the IPv4 address you want to temporarily assign to the IOLAN, and **aa:bb:cc:dd:ee:ff** is the Ethernet (MAC) address of IOLAN (found on the back of the unit).

Whether you use UNIX or Windows®, you are now ready to ping to the IOLAN. Here is a UNIX example of the sequence to use:

```
arp -s 192.168.209.8 00:80:d4:00:33:4e
ping 192.168.209.8
```

From the ping command issued in step 2, the IOLAN will pickup and use the IP address entered into the ARP table in step 1. You are now ready to configure the IOLAN.

Connecting to an IPv6 Network

The IOLAN has a factory default link local IPv6 address based upon its MAC Address.

For example:

For an IOLAN with a MAC Address of 00-80-D4-AB-CD-EF, the Link Local Address would be fe80::0280:D4ff:feAB:CDEF.

By default, the IOLAN will listen for IPV6 router advertisements to obtain additional IPV6 addresses. No configuration is required, however, you can manually configure IPV6 addresses and network settings; see [Connecting to an IPv6 Network](#) for more information on IPv6 configuration options.

SNMP

The IOLAN supports configuration and management through SNMP. SNMP Management tools (SNMP client/MIB browser software) can be used to set IOLAN configuration parameters and/or view IOLAN statistics.

Connecting to the IOLAN Using SNMP

Before you can connect to the IOLAN through an SNMP Management tool or MIB browser, you need to set the following components through another configuration method.

-
1. Configure a known IP address on the IOLAN.
 2. Configure a read-write user for SNMP version 3 or a community for SNMP version 1 or 2 on the IOLAN.
 3. Reboot the IOLAN to make sure the changes take effect.

To connect to the IOLAN through an SNMP Management tool or MIB browser, do the following:

1. From the Perle website, load the MIB, for your model, into your SNMP manager.

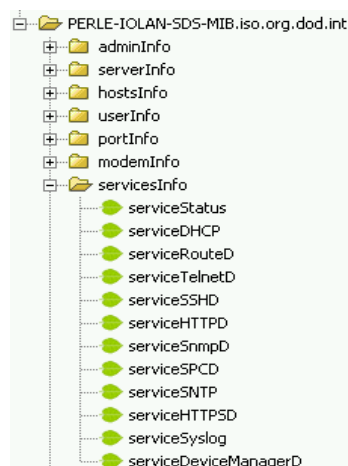
Note: You need to have the following MIBs installed in your SNMP manager (these are usually part of the standard SNMP client/MIB browser):

- SNMPv2-SMI
- SNMPv2-TC
- IPV6-TC

2. Verify that the read-write user for SNMP version 3 or a community for SNMP version 1 or 2 match the configuration on the IOLAN.
3. Type in the IOLAN's IP address and connect to the IOLAN.
4. You are now ready to start configuring the IOLAN using SNMP.

Using the SNMP MIB

After you have successfully connected to the IOLAN through your SNMP Management tool or MIB browser, expand the MIB folder to see the IOLAN's parameter folders. Below is an example of the configurable parameters under the **ServicesInfo** folder.



The first variable in each folder is the **Status** variable, for example, **serviceStatus**. When you perform a **GET** on this variable, one of the following values will be returned:

- **1**—Indicates that the container folder is active with no changes.
- **2**—Indicates that the container folder is active with change(s).

Once you have completed setting the variables in a folder, you will want to submit your changes to the IOLAN. To do this, set the **Status** variable to **4**. If you want to discard the changes, set the **Status** variable to **6**.

- **4**—Indicates that the changes in the container folder are to be submitted to the IOLAN.
- **6**—Indicates that the changes in the container folder are to be discarded.

If you want to save all the changes that have been submitted to the IOLAN, you need to expand the **adminInfo** container folder and **SET** the **adminFunction** to **1** to write to FLASH. To make the configuration changes take effect, **SET** the **adminFunction** to **3** to reboot the IOLAN.

To select a serial port profile in the WebManager, connect through the WebManager to the IOLAN you are configuring and select **Serial Port**, in the navigation pane. Highlight the serial port you want to configure and then select **Edit**.

Network Settings

The Network section is used to configure the parameters that identify the IOLAN within the network and how the IOLAN accesses hosts on the network. Select Network from the navigation tree on the left hand side.

- **IP Settings**—Configure IPv4, IPv6 settings, Default Gateway and Ethernet settings
- **WWAN** (wireless wide area network) —Configure WWAN settings
- **WLAN** (wireless local area network)—Configure WLAN settings
- **Advanced**—Configure Host table, IP Filtering, Routes, DNS/WINS, RIP, Dynamic DNS, IPv6 Tunnels.

IPv4 Settings

The parameters in IPv4 settings are used to access the IOLAN and how the IOLAN accesses the network. Select IPV4 from the Network Configuration screen and configure the parameters for your network.

System Name	The System Name is used for informational purposes by such tools as the DeviceManager and is also used in conjunction with the Domain field to construct a fully qualified domain name (FQDN).
Domain	This field is combined with the System Name to construct the fully qualified domain name (FQDN). For example, if the domain is mycompany.com and the Server Name is set to accounting , the FQDN would be accounting.mycompany.com .
Interface Name	Ethernet 1, Ethernet 2 or WLAN 0
Obtain IP Address automatically using DHCP/BOOTP	When enabled, the IOLAN will request an IP address from the DHCP/BOOTP server. By default, when this option is enabled, the IOLAN will also attempt to retrieve the DNS server, WINS server, and default gateway from the DHCP/BOOTP server. Default: Disabled
Use the following IP Address	Assign a specific IP address to the IOLAN. Field Format: IPv4 address
Ethernet 1	The IOLAN's unique IPv4 network Interface 1 IP address. Field Format: IPv4 address
Ethernet 2	The IOLAN's unique IPv4 network interface 1 IP address. Field Format: IPv4 address
WLAN 0	The IOLAN's unique IPv4 WLAN 0 network address. Field Format: IPv4 address
Subnet Mask	The network subnet mask. For example, 255.255.0.0.
Default Gateway	Specify the gateway IP address that will provide general access beyond the local network. Field Format: IPv4 address

Default Gateway Obtain Automatically	When DHCP/BOOTP is enabled, you can enable this option to have the IOLAN receive the Default Gateway IP address from the DHCP/BOOTP server. Default: Enabled
DNS Server	Specify the IP address of a DNS host in your network for host name resolution. Field Format: IPv4 or IPv6 address
DNS Server Obtain Automatically	When DHCP/BOOTP is enabled, you can enable this option to have the IOLAN receive the DNS IP address from the DHCP/BOOTP server. Default: Enabled
WINS Server	Specify the IP address of a WINS (Windows Internet Naming Service) host in your network for host resolution. Field Format: IPv4 address
WINS Server Obtain Automatically	When DHCP/BOOTP is enabled, you can enable this option to have the IOLAN receive the WINS IP address from the DHCP/BOOTP server. Default: Enabled

IPv6 Settings

Configure IPv6 settings when the IOLAN resides in an IPv6 network.

Ethernet 1	The IOLAN's unique IPv6 network Interface 1 IP address. Field Format: IPv6 address
Ethernet 2	The IOLAN's unique IPv6 network interface 1 IP address. Field Format: IPv6 address
WLAN 0	The IOLAN's unique IPv6 WLAN 0 network address. Field Format: IPv6 address
Obtain IPv6 Address(es) using	When enabled, you can configure the IOLAN to obtain the IPv6 address(es) using IPv6 Autoconfiguration or a DHCPv6 server. Default: Enabled
IPv6 Autoconfiguration	When enabled, the IOLAN will send out a Router Solicitation message. If a Router Advertisement message is received, the IOLAN will configure the IPv6 address(es) and configuration parameters based on the information contained in the advertisement. If no Router Advertisement message is received, the IOLAN will attempt to connect to a DHCPv6 server to obtain IPv6 addresses and other configuration parameters. Default: Enabled
DHCPv6	When enabled, requests IPv6 address(es) and configuration information from the DHCPv6 server. Default: Disabled
Custom IPv6 Address List	Displays the list of custom configured IPv6 addresses.

Default Gateway	Specify the gateway IP address that will provide general access beyond the local network. Field Format: IPv6 address
DNS Server	Specify the IPv6 address of a DNS host in your network for host name resolution. Field Format: IPv6 address
DNS Server Obtain Automatically	When DHCPv6 is enabled, you can enable this option to have the IOLAN receive the DNS IP address from the DHCPv6 server. Default: Enabled
DHCPv6 Settings IPv6 Address(es)	When enabled, the IOLAN will accept IPv6 address(es) from the DHCPv6 server. Default: Disabled
DHCPv6 Settings Network Prefix	When enabled, the IOLAN will accept the network prefix from the DHCPv6 server. Default: Disabled

Adding/Editing a Custom IPv6 Address

You can choose one of the following:

Enter the IPv6 network prefix:

Create a unique IPv6 address on the network When enabled, the IOLAN will derive an IPv6 address from the entered network prefix and the IOLAN's MAC address.
Default: Enabled

Network Prefix Specify the IPv6 network prefix.
Default: Enabled

Network Subnet Bits Specify the number of bits in the Network prefix which will be used to specify the subnet.
Range: 0-64
Default: 64

Enter the complete IPv6 address:

Use the following IPv6 address Enable this option when you want to enter a specific IPv6 address.
Default: Disabled

IPv6 Address Specify the complete IPv6 address.
Field Format: IPv6 address

IPv6 Address IPv6 Prefix Bits Specify the network prefix bits for the IPv6 address.
Range: 0-128
Default: 64

Advanced Network Settings

The **Advanced** tab configures DNS update, MTU size, IPv6 Advertising Router settings, and the Ethernet interface parameters.

Configure the parameters in the **Advanced** tab only if:

- you have already set up Dynamic DNS with DynDNS.com
- you want to specify the line speed and duplex for your Ethernet interface
- if you want the IOLAN to act as an IPv6 Advertising Router

Register Address in DNS	<p>When this parameter is set, the IOLAN will provide the DHCP/DHCPv6 server with a fully qualified domain name (FQDN), so that the DHCP/DHCPv6 server can update the network's DNS server with the newly assigned IP address.</p> <p>Default: Disabled</p>
Domain Prefix	<p>(Dual Interface models only) A domain prefix to uniquely identify the interface to the DNS when the IOLAN has more than one Ethernet interface. The FQDN that is sent to the DNS will be one of the following formats, depending on what is configured in the System Settings section on the IPv4 Settings tab:</p> <ul style="list-style-type: none">• <i><Server Name>.<Domain Prefix>.<Domain Name></i>• <i><Server Name>.<Domain Prefix></i> <p>Field Format: Maximum 8 alphanumeric characters</p>
Maximum Transmission Unit (MTU)	<p>The Maximum Transmission Unit (MTU) size of an IP frame that will be sent over the network. If your IOLAN has more than one interface each interface can be set separately, however only one MTU size can be set for both IPv4 or IPv6 frames.</p> <p>MTU IPv4: 68-1500 bytes</p> <p>MTU IPv6: 68-1500 bytes</p>
Enable Active Standby	<p>Active Standby permits the grouping of Ethernet LAN connections to provide for link failover. Both Ethernet connections will have the same Ethernet MAC address. Active standby refers to the process by which a failure of one interface can be automatically overcome by having its traffic routed to the other interface.</p> <p>Default: Disabled</p>
Monitoring Interval	<p>(Only applies to IOLANs with two Ethernet interfaces)</p> <p>The interval in which the active interface is checked to see if it is still communicating.</p> <p>Default: 100 ms</p>
Recovery Delay	<p>(Only applies to IOLANs with two Ethernet interfaces)</p> <p>The time that the IOLAN will wait to make the secondary interface (Ethernet 2) active after it has been detected as up.</p> <p>Default: 200 ms</p>
Disable IP Forwarding between Ethernet Interfaces	<p>(Only applies to IOLANs with two Ethernet interfaces)</p> <p>When enabled, no IP traffic will be forwarded between Ethernet interfaces.</p> <p>Default: Disabled</p>

Enable IPv6 Router Advertisement	<p>When enabled, the IOLAN will periodically send IPV6 Router Advertisement messages and respond to Router Solicitation messages. The Router Advertisement message can be configured to contain any of the following information:</p> <ul style="list-style-type: none"> • DHCPv6—Use the DHCPv6 server to obtain additional IPV6 address(es) and configuration parameters. • DHCPv6 Configuration Options—Use DHCPv6 server to obtain additional configuration parameters. • Network Prefixes—Advertise the selected custom configured network prefixes. <p>Default: Disabled</p>
Advertise DHCPv6	<p>When enabled, the Router Advertisement message indicates to use the DHCPv6 server for obtaining additional IPv6 addresses and configuration parameters.</p> <p>Default: Disabled</p>
Advertise DHCPv6 Configuration Options	<p>When enabled, the Router Advertisement message indicates to use the DHCPv6 server to obtain additional configuration parameters.</p> <p>Default: Disabled</p>
Advertise the following Network Prefix(es)	<p>The network prefix of the IPV6 addresses created in the IPv6 Settings tab in the Custom IPv6 Address List are included in the Router Advertisement message. You can choose to enabled or disable specific network prefixes from being advertised to hosts.</p> <p>Default: Enabled</p>
Media Type	<p>Select the type of hardware media.</p> <p>Options:</p> <ul style="list-style-type: none"> • Auto • RJ45 • SFP <p>Default: Auto</p>
Interface 1 Hardware Speed and Duplex	<p>Define the Ethernet connection speed.</p> <p>Data Options:</p> <ul style="list-style-type: none"> • Auto—automatically detects the Ethernet interface speed and duplex • 10 Mbps Half Duplex • 10 Mbps Full Duplex • 100 Mbps Half Duplex • 100 Mbps Full Duplex • 1000 Mbps Full Duplex <p>Default: Auto</p>
Interface 2 Hardware Speed and Duplex	<p>Define the Ethernet connection speed.</p> <p>Data Options:</p> <ul style="list-style-type: none"> • Auto—automatically detects the Ethernet interface speed and duplex • 10 Mbps Half Duplex • 10 Mbps Full Duplex • 100 Mbps Half Duplex • 100 Mbps Full Duplex • 1000 Mbps Full Duplex <p>Default: Auto</p>

SGMII Support

Enable SGMII support on the SFP transceiver port.

Default: Disable

WLAN (only applies to certain models)

The IOLAN can operate in two wireless modes. The WLAN can be disabled.

- Client Mode
- Soft-AP Mode

Client Mode

In Client mode the IOLAN can connect wirelessly to an Access Point (AP) wireless network. The IOLAN is preconfigure to run in Client mode. The IOLAN supports up to 8 client profiles for connecting to different Access Points (AP's).

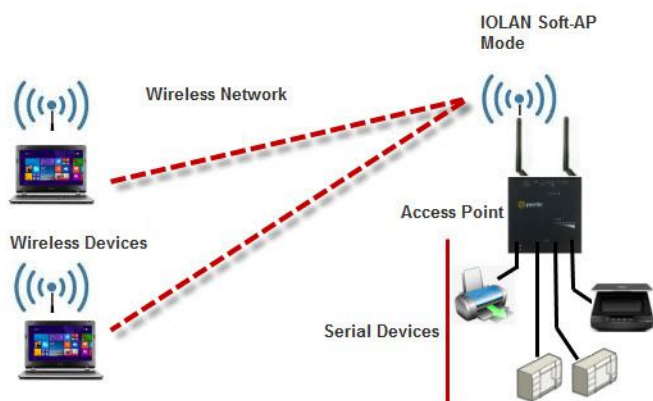
IOLAN in Client Mode



Soft-AP Mode

In Soft-AP Mode, the IOLAN acts as an Access Point for wireless clients. Up to 6 wireless clients can connect to the IOLAN.

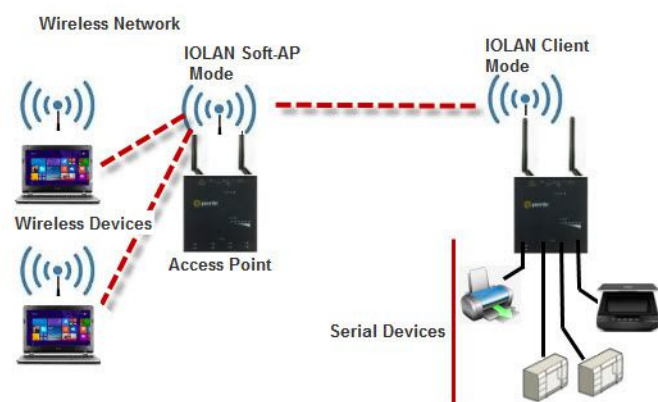
IOLAN in Soft-AP Mode



Back to Back IOLANs

In Back to Back Mode, one IOLAN is configured in Soft-AP Mode (AP) and the second IOLAN is configured in Client Mode. Selecting the WLAN tab will allow you to:

Back to Back IOLANs (one in Soft-AP Mode and the other in Client Mode)



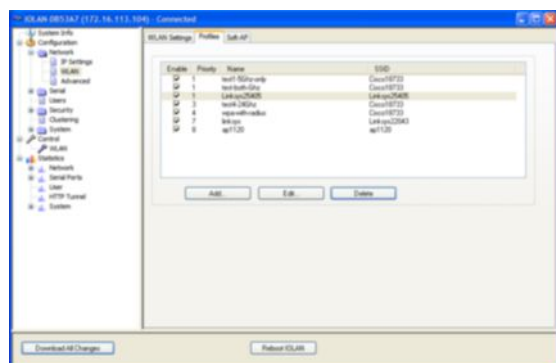
- set the WLAN parameters
- add/edit and delete profiles
- configure Soft-AP mode

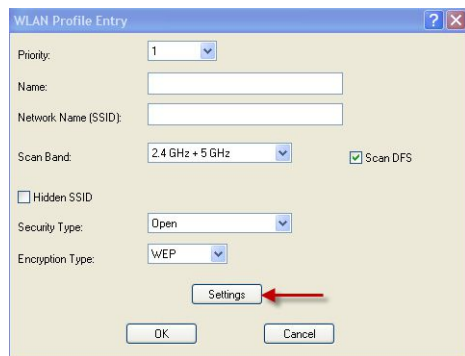
Region	Select your wireless region. Values: eu, japan, us-canada Default: us-canada
Mode	Specify the mode of operation for the IOLAN's WLAN operation. Client: The IOLAN's wireless interface is used to connect to an AP (Access Point). Soft-AP: The IOLAN's wireless interface acts as an AP (Access Point) allowing wireless clients to connect. Disabled: The IOLAN's wireless capabilities are disabled. When disabled, the external WPS button will have no effect on the mode of the IOLAN. Default: Client
Radio Band	The IOLAN can operate over 2.4GHz or 5GHz. To support connections to both bands use 2.4+5. Values: 2.4, 5, 2.4+5 Default: 2.4+5 (dual-band)
WPS Enabled (in client mode)	By default WPS (Wireless Protected Setup) mode is enabled to allow the IOLAN to easily connect to any routers/Access Points that are in the network and configured for WPS mode. The IOLAN will scan for 120 seconds to find the closest AP that is currently in WPS mode. The IOLAN will exchange credentials with that AP and then create an internal wireless profile (association) and then the IOLAN will exit WPS mode. Values: on or off Default: on
WPS Enabled (in Soft-AP mode)	The WPS button can be used in Soft-AP mode to facilitate the connection of wireless clients

-
- Passive Scan Only** In passive scan mode the IOLAN will scan all channels and listen for beacons being sent by the AP's on these channels. In active scan mode, the IOLAN actively seeks out AP's by sending out probes on these channels to accelerate their discovery. Active scan mode can be disabled by setting the Passive Scanning Only Mode to On.
Values: on or off
Default: off
- Roaming Enabled** This setting allows you to roam (reconnect) to a different wireless router/AP (with the same SSID) if there is a significant difference in the signal strength.
Values: on or off
Default: on
- Roaming Decision** When roaming, the IOLAN will be constantly scanning in the background to determine if there is a better AP to connect to within the ESSID network. Since this background scanning can have an effect on performance, it will normally do slow scans when the signal is strong and faster scans when the signal is weaker.
Values: Balanced, Optimize Bandwidth, Optimize Distance
Default: Balanced
- Out of Range Scan Interval** Specify the out of range scan interval for fast roaming scans.
Values: 0-65535 seconds
Default: 30 seconds
- In Range Scan Interval** Specify the in range scan interval for slow roaming scans.
Values: 0-65535 seconds
Default: 300 seconds
- Antenna Rx Diversity/MRC** The IOLAN uses these techniques to optimize receive signals on it's wireless antennas. (supported on models with 2 antennas)
2.4-GHz supports MRC (Maximal-Ratio Combining)
5-GHz supports Diversity Capable
Default: on

WLAN Profiles

A WLAN profile defines all the settings necessary to establish a wireless connection with an Access Point. You can defined up to 8 client profiles on the IOLAN. Associations with AP's in WPS mode will be automatically added by the IOLAN as profile (priority 1).





- Connect Priority** The connect priority order (1 being the highest) in which the IOLAN will attempt an association with AP's that match the SSID in the profile. If there are duplicate priority entries in the table, the IOLAN will connect to the duplicate entry with the most optimal AP based on signal strength and security type.
Values: 1-8
Default: 1
- Profile Name** Enter the name for this profile.
Values: 1-32 characters, no spaces allowed
- Network Name (SSID)** Specify an SSID (network name).
Values: max of 32 characters (no spaces allow)
Default: none or auto-created SSID
- Radio Band** The IOLAN can operate over 2.4GHz or 5GHz. To support connections to both bands use 2.4+5.
Values: 2.4, 5, 2.4+5
Default: 2.4+5 (dual-band)
- Scan DFS Channel** The IOLAN supports DFS. When connected to an AP that is using Dynamic Frequency Selection, it will respond to the specific protocol requests. When scanning channels for AP's the IOLAN provides the option of skipping the DFS protected channels.
Values: off or on
Default: on (applies to 5GHz mode only)
- Hidden SSID** If this profile is defined to connect to an AP that has a hidden SSID then this option must be enabled. This will force the IOLAN to send a directed probe to this AP with the specified SSID in order to discover it and determine the channel that it is using.
Values: off or on
Default: off

Security

Depending on the security type selected, some encryption types, authentication methods and authentication methods may not be supported. See table below for valid combinations.

	Security Type	Open	Shared	WPA- Personal	WPA2- Personal	WPA2- Enterprise	WPA- Enterprise	802.1
Encryption Type	WEP	•	•					•
	NONE	•						
	AES			•	•	•	•	
	TKIP			•	•	•	•	
	Security Keys	•	•	•	•			
Authentication Method	EAP-TLS					•	•	•
	PEAP					•	•	•
	LEAP					•	•	•
	EAP-TTLS					•	•	•
	Username					•	•	•
	Password					•	•	•
Authentication Protocol	CHAP					•	•	•
	MSCHAP2					•	•	•
	EAP-MSCHAPV2					•	•	•
	MSCHAP2					•	•	•
	EAP-MSCHAPV2					•	•	•
	EAP-MD5					•	•	•
	EAP-GTC					•	•	•
	EAP-MD5					•	•	•
	EAP-MD5					•	•	•
	Validate Sever Certificate					•	•	•
	Roaming Identify					•	•	•

Wepkey 1-4

Enter a wep key.

Values: (5 or 13 characters) or (10 or 26 hexadecimal digits)

TX-key index

Select the TX key index to use.

Values: 1-4.

Username

Specify a username to identify the IOLAN to the Radius server.

Values: max of 254 characters

Default: none

Password

Specify a password to identify the IOLAN to the Radius server.

Values: max of 128 characters

Default: none

Validate server certificate

Enable this option if you want the Radius server to validate that the IOLAN's server's certificate has been signed by a SSL/TLS certificate authority (CA). If you enable this option, you need to download an SSL/TLS certificate authority (CA) list file to the IOLAN.

Values: yes or no

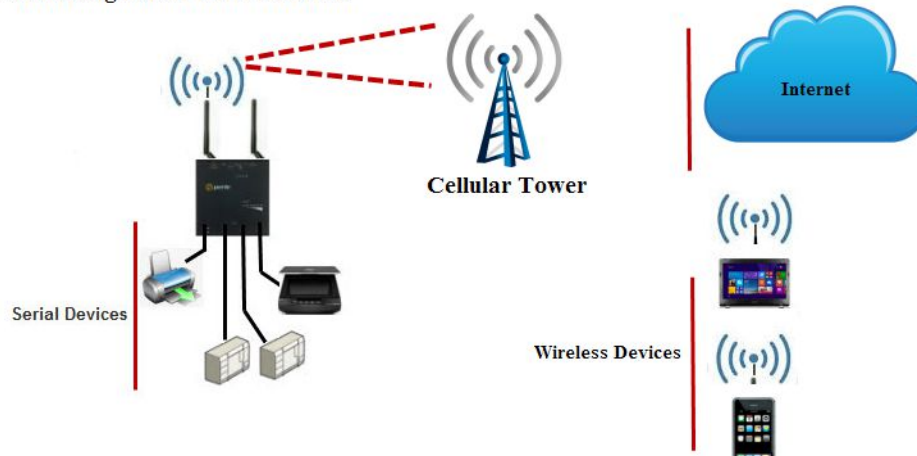
Default: no

Soft-AP Mode Parameters

SSID (network address)	Specify an SSID (network name). Values: max of 32 characters (no spaces allow) Default: none or auto-created SSID
Channel Number	Enter the channel number the IOLAN will use to connect to the AP. Values: (1-11) 2.4GHz (36,40,44,48) 5GHz Default: Selecting a channel number between 1-11 will use 2.4GHz band and selecting channels 38, 40, 44 and 48 will use 5GHz band.
Security type in Soft AP mode	In Soft-AP Mode, the IOLAN supports wpa-personal and wpa2-personal encryption. wpa-personal: tkip, aes Default: aes wpa2-personal: tkip, aes Default: aes
Security Key in Soft AP mode	Specify a security key for this connection. Value: 64 hexadecimal digits or as a passphrase of 8-63 printable ascii characters
IP address	Enter an IPv4 address for the IOLAN on this WLAN. Default: 192.168.0.1
Network mask	Enter the IOLAN's subnet mask. For example 255.255.0.0
Enable DHCP Server	This DHCP server can be used to give IP addresses to clients connecting on this wireless network. Value: off or on Default: on
DHCP IP address	Enter the start IPv4 address of the DHCP pool. Value: IP address Default: 192.168.0.100
DHCP subnet mask	Enter the IOLAN's subnet mask. For example 255.255.0.0

WWAN (only applies to certain models)

Connecting to a WWAN Network



Enable	Selecting this option will enable your IOLAN to connect to your cellular network.
APN	<p>Enter the Access Point Name (APN). The APN will use this information to identify the packet data network (PDN) that mobile data devices want to communicate with. In addition to identifying a PDN, an APN may be used to define the type of service. It can assigned an IP address to the wireless device, which security methods should be used and how or if it should be connected to a customer private network.</p> <p>Examples of APNs:</p> <ul style="list-style-type: none">• three.co.uk• internet.t-mobile• m2minternet.apn
Authentication	<p>If required by your PDN, enter the authentication method to use.</p> <p>Data Options: None, PAP, CHAP</p> <p>Default: None</p>
Username	<p>If required, enter the username to use for this connection.</p> <p>Data options: 0-127 characters</p>
Password	<p>If required, enter the password to use for this connection.</p> <p>Data Options: 0-127 characters</p>
Pin	<p>Enter a Pin if your SIM card has a PIN enabled, this will allow you to connect to the SIM card.</p> <p>Note: The IOLAN does not have the capability to set a Pin number on your SIM card.</p> <p>Value: 8 characters</p>
Radio Access Technology	<p>Select the radio access technology you will use to connect to the network.</p> <p>Data Options: Auto, LTE, 3G, 2G</p> <p>Default: auto</p>

Obtain DNS servers from the network	<p>Allow the network to provide the IOLAN with the addresses of DNS servers on the network.</p> <p>Data Options: on or off</p> <p>Default: on</p>
--	---

Host Table

The Host table contains the list of hosts that will be accessed by an IP address or Fully Qualified Domain Name (FQDN) from the IOLAN. This table will contain a symbolic name for the host as well as its IP address or FQDN. When a host entry is required elsewhere in the configuration, the symbolic name will be used. You can configure up to 100 hosts using IPv4 or IPv6 internet addresses.

Host Name	<p>The name of the host. This is used only for the IOLAN configuration.</p> <p>Field Format: Up to 14 characters, no spaces.</p>
IP Address	<p>The host's IP address.</p> <p>Field Format: IPv4 or IPv6 address</p>
Fully Qualified Domain Name	<p>When you have DNS defined in the IOLAN, you can enter a DNS resolvable fully qualified domain name (note: FQDN's are excluded as accessible hosts when IP Filtering is enabled).</p> <p>Field Format: Maximum 254 alphanumeric characters</p>

IP Filtering

The IP Filtering Host table allows you to configure a table to customize how traffic to and from the IOLAN will be filtered.

IP Filtering	You can allow all IP traffic to and from the IOLAN. This is the default configuration.
Define traffic based on below criteria	<p>This is a security feature that allow you to defined traffic to/from hosts defined within the IOLAN Host table or IP traffic based on address ranges.</p> <p>IP Filtering on Host Table</p> <p>This is a security feature that allow you to defined traffic to/from hosts defined only within the IOLAN Host table.</p> <p>IP Filtering on Address Ranges</p> <p>This is a security feature that allows you to define IP address ranges for traffic to/from the IOLAN. The IOLAN will only accept data from or send data to hosts configured within these IPv4 address ranges. You can define up to 6 IP traffic to/from address ranges.</p>

Routes

Entering routes in the routing list enables the identification of gateways to be used for accessing specific hosts or external networks from the IOLAN's local network.

There are three types of routes:

- **Default**—A route that provides general access beyond your local network.
- **Host**—A route defined for accessing a specific host external to your local network.
- **Network**—A route defined for accessing a specific network external to your local network.

You can specify up to 49 routes on the IOLAN. Two types of gateways (method of accessing specific hosts or external networks) can be configured.

- **Host**—Specify a specific host that will provide access to the route destination.
- **Interface**—Specify the IPv6 tunnel, Remote Access (PPP)-defined serial port, or remote Access (SLIP)-defined serial port that will provide access to the route destination.

Adding/Editing Routes

From the **Route List** tab, if you select the **Add** or **Edit** button, you will be able to add a new or edit an existing route.

Type	Specify the type of route you want to configure. Data Options: <ul style="list-style-type: none"> • Host—A route defined for accessing a specific host external to your local network. • Network—A route defined for accessing a specific network external to your local network. • Default—A route which provides general access beyond your local network. Default: Default
IP Address	When the route Type is defined as Host , this field will contain the IP address of the host. If the route Type is defined as Network , the network portion of the IP address must be specified and the Host port of the address will be set to 0. Example: to access network 10.10.20, the address 10.10.20.0 would be specified in this field. Format: IPv4 or IPv6 address
IPv4 Subnet Mask	When the route is a Network route, you must specify the network's subnet mask.
IPv6 Prefix Bits	If the IP address is IPv6, then you must specify the network's prefix bits. Range: 0-128
Host	Select this option when a host is being used as the route gateway. Default: Enabled, None
Interface	The Interface list is comprised of configured IPv6 tunnels and serial ports defined for Remote Access (PPP) and Remote Access (SLIP) profiles. Select this option when you want to use the specified interface as the gateway to the destination. Field Option(s): IPv6 tunnels, Remote Access (PPP) and Remote Access (SLIP) serial ports Default: Disabled

DNS/WINS

You can configure WINS servers for PPP-client name resolution and DNS servers for PPP-client name resolution and IOLAN host name resolution.

You can configure up to four DNS and four WINS servers. If you specified a DNS and/or WINS server on the **Network, IP Settings** tabs (either IPv4 or IPv6), it will be automatically entered into the appropriate list. If the DNS and/or WINS server is provided by a DHCP server, these will NOT be viewable in the list, however, you can add DNS and/or WINS servers to supplement the DHCP supplied server.

Editing/Adding DNS/WINS Servers

DNS IP Address	You can configure up to four DNS servers. Field Format: IPv4 or IPv6 address
-----------------------	--

WINS IP Address	You can configure up to four WINS servers. Field Format: IPv4 address
------------------------	---

RIP

The Routing Information Protocol (RIP) is a routing protocol used with almost every TCP/IP implementation. Its function is to pass routing information from a router or gateway to a neighboring router(s) or gateway(s). RIP messages contain information about destinations which can be reached and the number of hops which are required. The hop-count is the basic metric of RIP and so RIP is referred to as a “distance vector protocol”. RIP messages are carried in UDP datagrams.

You can configure RIP to selectively advertise networks remotely connected via a SLIP/PPP link on the Ethernet connection, and pass RIP routing information to remotely connected clients. As this can be undesirable in some environments, this behavior can be configured and is defaulted to the non-routing behavior.

Transmission and reception of Routing Information Protocol (RIP) packets over PPP and SLIP connections can be configured on a per user basis or on a per serial port basis.

The **Routing** parameter can be configured:

- On the **Advanced** tab for Remote Access (PPP) and Remote Access (SLIP) profiles configured for a serial port to determine the exchange of RIP packets between the IOLAN and remotely connected users connected from the serial side.
- On the **Services** tab for each local user to determine the exchange of RIP packets between the IOLAN and remotely connected users connected from the serial side.
- By the RADIUS server for users authenticated by RADIUS, the RADIUS-defined **Framed-Routing** parameter determines the exchange of RIP packets.

There are four options for setting the **Routing** parameters:

- **None**—Routing information is not exchanged across the link. This is the default setting for a line and a locally defined user.
 - **Send**—Routing information is only transmitted to the remote user.
 - **Listen**—Routing information is only received from the remote user.
 - **Send and Listen**—Routing information is transmitted to and received from the remote user.
- The local **User Routing** parameter or RADIUS **Framed-Routing** parameter, if set, override the serial port **Routing** parameter for a connection.

Authentication Method	Specify the type of RIP authentication.
------------------------------	---

Data Options:

- **None**—No authentication for RIP.
- **Password**—Simple RIP password authentication.
- **MD5**—Use MD5 RIP authentication.

Default: None

Password	Specify the password that allows the router tables to be updated.
-----------------	---

Confirm Password	Retype in the password to verify that you typed in it correctly.
-------------------------	--

Dynamic DNS

Dynamic DNS Service providers enable users to access a server connected to the internet that has been assigned a dynamic IP address. The IOLAN product line has built-in support for the DynDNS.com service provider. Refer to www.DynDNS.com for information on setting up an account.

When the IOLAN is assigned a dynamic IP address, it will inform the DynDNS.com service provider of its new IP address. Users can then use DynDNS.com as a DNS service to get the IP address of the IOLAN. In order to take advantage of this service, the following steps need to be taken.

1. Create an account with DynDNS.com and configure the name your IOLAN will be known by on the internet (the **Host** name). For example, create a host name such as `yourcompanySCS.DynDNS.org`.
2. Enable the **Network Dynamic DNS** feature and configure the IOLAN's dynamic DNS parameters to match the **Host's** configuration on the DynDNS.com server. Every time the IOLAN gets assigned a new IP address, it will update DynDNS.com with the new IP address.
3. Users accessing the IOLAN via the internet can now access it via its fully qualified host name. For example, `telnet yourcompanySCS.DynDNS.org`.

Enable Dynamic DNS for the system	Enables/disables the dynamic DNS feature. When Dynamic DNS is enabled, the IOLAN will automatically update its IP address with DynDNS.org if it changes. Default: Disabled
Service Provider	DynDns.org
Registered Host Name	Specify the registered hostname with DynDNS.org that will be updated with the IOLAN's IP address should it change. Put in the full name; for example, <code>mydeviceserver.dyndns.org</code> .
User Name	Specify the user name used to access the account set up on the DynDNS.org server.
Password	Specify the password used to access the account set up on the DynDNS.org server.

Dynamic DNS Account Settings

Enter the information about your DynDNS.com account so the IOLAN can communicate IP address updates. These settings are global and apply to all Dynamic DNS settings.

System Type	Specify how your account IP address schema was set up with DynDNS.org. Refer to www.DynDNS.org for information about this parameter. Data Options: Dynamic, Static, Custom Default: Dynamic
Wildcard	Adds an alias to <code>*.yourcompanySCS.dyndns.org</code> pointing to the same IP address as entered for <code>yourcompanySCS.dyndns.org</code> .

Connection Method Specify how the IOLAN is going to connect to the DynDNS.org server.

Data Options:

- HTTP
- HTTP through Port 8245
- HTTPS—for a secure connection to the DynDNS server

Default: Disabled

HTTPS Configuration

Cipher Suite Button Launches the cipher information window so you can specify the type of encryption that will be used for data that is transferred between the DynDNS.org server and the IOLAN. You can specify up to five cipher groups.

Validation Criteria See Validation Criteria for more information.

Validation Criteria

If you choose to configure validation criteria, the information in the peer SSL/TLS certificate must match exactly the information configured in this window in order to pass peer authentication and create a valid SSL/TLS connection.

Note: Some combinations of cipher groups may not be available on some firmware versions.

Country	A country code; for example, US. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate. Data Options: 2 characters
State/Province	An entry for the state/province; for example, IL. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate. Data Options: Maximum 128 characters
Locality	An entry for the location; for example, Chicago. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate. Data Options: Maximum 128 characters
Organization	An entry for the organization; for example, Accounting. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate. Data Options: Maximum 64 characters
Organization Unit	An entry for the unit in the organization; for example, Payroll. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate. Data Options: Maximum 64 characters
Common Name	An entry for common name; for example, the host name or fully qualified domain name. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate. Data Options: Maximum 64 characters

Email

An entry for an email address; for example, acct@anycompany.com. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate.

Data Options: Maximum 64 characters

IPv6 Tunnels

IPv6 tunnels transport IPv6 data packets from one IPv6 network to another IPv6 network over an IPv4 network. In addition to creating the IPv6 tunnel, you must also create the route that will transport the data packets through the IPv4 network in the Route List (see route list more information).

Adding/Editing an IPv6 Tunnel

When you add/edit an IPv6 tunnel, you are determining how an IPv6 message will reach an IPv6 device through an IPv4 network.

Name	The name of the IPv6 tunnel. Field Format: Maximum 16 alphanumeric characters Default: ipv6_tunnel1
Mode	The method or protocol that is used to create the IPv6 tunnel. <ul style="list-style-type: none">• Manual—When enabled, the IOLAN will manually create the IPv6 tunnel to the specified Remote Host through the specified Interface.• 6to4—When enabled, the IOLAN will broadcast to the multi-cast address 192.88.99.1 through the specified Interface. When the closest 6to4 router responds, it will create the IPv6 tunnel, encapsulating and decapsulating IPv6 traffic sent to and from the IOLAN.• Teredo—When enabled, the Teredo protocol encapsulates the IPv6 packet as an IPv4 UDP message, allowing it to pass through most network address translator (NAT) boxes and create an IPv6 tunnel to the specified Remote Host (a Teredo server) through the specified Interface. Default: Manual
Remote Host	The IPv4 host that can access the IPv6 network when the Mode is Manual . The Teredo server when the Mode is Teredo . Default: None
Interface	The interface that the IOLAN is going to use to access the Remote Host. The list is comprised of the Ethernet interface(s) and serial ports configured for the Remote Access (PPP) or Remote Access (SLIP) profiles. Default: Ethernet 1

Serial Ports

Each IOLAN serial port can be connected to a serial device. As you select the different serial port profiles, a short description and a picture representing a typical application of the profile is displayed. Each serial port can then be configured according to a serial port profile that coincides with the serial device attached to that serial port and how the serial device is accessed/used.

When you select the **Serial (Ports)** navigation option, you will see a list with the number of serial ports on your IOLAN. To configure/change a serial port, select the **Edit** button. From the top of the screen select the Profile **Change** button, then select the appropriate profile for the serial port. Select **Apply** to save your changes. The serial port profile configuration options will be displayed.

Configuring Serial Ports

The Serial section is used to configure the serial ports on your IOLAN. The following configuration windows are available:

- **Serial Ports**—Configures the type of connection that the serial port is being used for. This is accomplished by selecting a connection profile and then configuring the applicable parameters for that profile. See [Serial Profiles](#) for more information
- **Port Buffering**—Configures serial port data buffering preferences. See [Port Buffering General Parameters](#) for more information.
- **Advanced**—Configures those parameters that are applicable to specific environments. You will find modem and TruePort configuration options, in addition to others, here. See [Serial Settings Advanced Parameters](#)
- **SSL/TLS**—Configure SSL/TLS encryption options for the serial port. See [SSL/TLS Settings](#)

Serial Profiles

Some serial profiles/parameters may not be available on some models of the IOLAN. IOLANs with USB only serial interfaces will support the Console Management, Trueport, TCP sockets and Custom App/Plugin profiles*.

The following are the serial profiles:

- ***Console Management**—The Console Management profile configures a serial port to provide network access to a console or administrative port. This profile sets up a serial port to support a TCP socket that listens for a Telnet or SSH connection from the network. See [Console Management General Parameters](#).
- ***TruePort**—The TruePort profile configures a serial port to connect network servers or workstations running the TruePort software to a serial device as a virtual COM port. This profile is ideal for connecting multiple serial ports to a network system or server. See [Trueport General Parameters](#).
- ***TCP Sockets**—The TCP Sockets profile configures a serial port to allow a serial device to communicate over a TCP network. The TCP connection can be configured to be initiated from the network, a serial device connected to the serial port, or both. This is sometimes referred to as a raw connection or a TCP raw connection. See [TCP Sockets General Parameters](#).
- **UDP Sockets**—The UDP Sockets profile configures a serial port to allow communication between the network and serial devices connected to the IOLAN using the UDP protocol. See [UDP Sockets General Parameters](#)
- **Terminal**—The Terminal profile configures a serial port to allow network access from a terminal connected to the IOLAN's serial port. This profile is used to access predefined hosts on the network from the terminal. See [Terminal Profile Parameters](#).
- **Printer**—The Printer profile configures a serial port to support a serial printer that can be accessed by the network.

-
- **Serial Tunneling**—The Serial Tunneling profile configures a serial port to establish a virtual link over the network to a serial port on another IOLAN. Both IOLAN serial ports must be configured for Serial Tunneling (typically one serial port is configured as a Tunnel Server and the other serial port as a Tunnel Client). See [Serial Tunneling General Parameters](#).
 - **Virtual Modem**—The Virtual Modem profile configures a serial port to simulate a modem. When the serial device connected to the IOLAN initiates a modem connection, the IOLAN starts up a TCP connection to the other IOLAN configured with a virtual Modem serial port or to a host running a TCP application.
 - **Modbus Gateway**—The Modbus Gateway profile configures a serial port to act as a Modbus Master Gateway or a Modbus Slave Gateway. See [Modbus General Parameters](#).
 - **Power Management**—The Power Management Profile configures a serial port to communicate with a Remote Power Switch's (RPS) administration port. This allows network access to the RPS and permits access to statistics and control of the RPS's power plugs.
 - **PPP**—The Remote Access (PPP) profile configures a serial port to allow a remote user to establish a PPP connection to the IOLAN's serial port. This is typically used with a modem for dial-in or dial-out access to the network.
 - **Slip**—The Remote Access (SLIP) Profile configures a serial port to allow a remote user to establish a SLIP connection to the IOLAN's serial port. This is typically used with a modem for dial-in and dial-out access to the network.
 - ***Custom Application/Plugin**—The Custom Application/Plugin profile configures a serial port to run a custom application or IOLAN plugin. After you download the custom application files and specify the application name and any parameters you want to pass to it, the IOLAN will execute the application when the serial port is started. See [Custom Application General Parameters](#).

Common Serial Port Profiles

There are several functions that are common to more than one profile. These functions are:

- **Hardware**—Configure the physical serial line parameters. See [Serial Port Hardware Parameters](#)
- **Email Alert**—[Email Alert](#)
- **Packet Forwarding**—Configure data packet parameters. [Packet Forwarding](#)
- **SSL/TLS**—Configure SSL/TLS encryption options for the serial port. See [SSL/TLS Settings](#)

Serial Port Hardware Parameters

The **Hardware** tab configures all the serial port hardware connection information. Your **Hardware** tab might display a subset of the parameters described, depending on the IOLAN model and supported hardware.

Serial Interface	Specifies the type of serial line that is being used with the IOLAN. Data Options: EIA-232, EIA-422, EIA-485, USB
Rolled (DTE)/Straight (DCE)	Specifies the type of serial cable that you will need to use when connecting to this RS232 serial port. Default: Straight

Speed	<p>Specifies the baud rate of the serial line; keep in mind that speed is affected by the length of the cable. You can also specify a custom baud rate. When you enter a custom baud rate, the IOLAN will calculate the closest baud rate available to the hardware. The exact baud rate calculated can be viewed in the Serial Ports statistics.</p> <p>Range: 300-230400, custom supports 300-1843200</p> <p>Default: 9600</p>
Data Bits	<p>Specifies the number of bits in a transmitted character.</p> <p>Default: 8</p> <p>(5 databits is only supported with 2 stop bit).</p>
Parity	<p>Specifies the type of parity being used for the data communication on the serial port. If you want to force a parity type, you can specify Mark for 1 or Space for 0.</p> <p>Data Options: Even, Odd, Mark, Space, None</p> <p>Default: None</p>
Stop Bits	<p>Specifies the number of stop bits that follow a byte.</p> <p>Data Options: 1, 2</p> <p>Default: 1</p>
Flow Control	<p>Defines whether the data flow is handled by the software (Soft), hardware (Hard), Both, or None. If you are using SLIP, set to Hard only. If you are using PPP, set to either Soft or Hard (Hard is recommended). If you select Soft with PPP, you must set the ACCM parameter when you configure PPP for the Serial Port.</p> <p>Data Options: Soft, Hard, Both, None</p> <p>Default: None</p>
Enable RTS-Toggle	<p>Configure the Toggle RTS Feature if your application needs for RTS to be raised during character transmission.</p> <p>Initial delay: configure the time (in ms) between the time the RTS signal is raised and the start of character transmission. This delay only applies if this port is not running hardware flow control. If hardware flow control is used, the transmission will occur as soon as CTS is raised by the modem.</p> <p>Final delay: configure the time (in ms) between the time of character transmission and when RTS is dropped.</p> <p>Initial delay range: 0-1000 ms</p> <p>Final delay range: 0-1000 ms</p> <p>Default: Off</p>
Enable Inbound Flow Control	<p>Determines if input flow control is to be used.</p> <p>Default: Enabled</p>
Enable Outbound Flow Control	<p>Determines if output flow control is to be used.</p> <p>Default: Enabled</p>

Monitor DSR	Specifies whether the EIA-232 signal DSR (Data Set Ready) should be monitored. This is used with modems or any device that sends a DSR signal. When it is monitored and the IOLAN detects a DSR signal, the serial port profile is started. If both Monitor DCD and Monitor DSR are enabled, both signals must be detected before the serial port profile is started. Default: Disabled
Monitor DCD	Specifies whether the EIA-232 signal DCD (Data Carrier Detect) should be monitored. This is used with modems or any other device that sends a DCD signal. When it is monitored and the IOLAN detects a DCD signal, the serial port profile is started. If both Monitor DCD and Monitor DSR are enabled, both signals must be detected before the serial port profile is started. Default: Disabled
Discard Characters Received with Errors	When enabled, the IOLAN will discard characters received with a parity of framing error. Default: Disabled
Enable Echo Suppression	This parameter applies only to EIA-485 Half Duplex mode. All characters will be echoed to the user and transmitted across the serial ports. Some EIA-485 applications require local echo to be enabled in order to monitor the loopback data to determine that line contention has occurred. If your application cannot handle loopback data, echo suppression should be enabled. Default: Disabled
Enable Line Termination	Used with EIA-422 and EIA-485 (on IOLAN models that support this option), specifies whether or not the line is terminated; use this option when the serial port is connected to a device at the end of the serial network. Line termination should only be used if the serial port is the end point in a network. Default: Disabled

Copying a Serial Port

Once you configure a serial port, you can copy the serial port settings to other serial ports of the same type by selecting **Copy**, then select the Serial Port(s) to copy to current configuration, select the **Ok** button, then the **Apply** button.

Resetting a Serial Port

To reset a serial port from the WebManager, select **Administration, Serial Port(s), Reset**.

Email Alert

Email notification can be set at the Server and/or serial port levels. You can set unique email notifications for each serial port because the person who administers the IOLAN might not be the same person who administers the serial device(s) attached to the IOLAN port. Therefore, email notification can be sent to the proper person(s) responsible for the hardware.

The following event triggers an email notification on the **Serial Port** for the specified **Level**:

- DSR signal loss, Warning Level

Enable Port Email Alert	Enable/disable email alert settings for this serial port. Default: Disabled
--------------------------------	---

Use System Email Alert Settings	Determines whether you want the Serial Port to inherit the Email Alert settings from the System Email Alert configuration. If this is enabled, System and Serial Port notification events will have the same Email Alert setting. Default: Enabled
Level	Choose the event level that triggers an email notification. Data Options: Emergency, Alert, Critical, Error, Warning, Notice, Info, Debug Default: Emergency
Use System Setting	By default, the fields are populated with the "global email" parameters. If you wish to override a field you must uncheck this field.
To	An email address or list of email addresses that will receive the email notification.
Subject	A text string, which can contain spaces, that will display in the Subject field of the email notification.
From	The field can contain an email address that might identify the IOLAN name or some other value.
Reply to	The email address to whom all replies to the email notification should go.

Packet Forwarding

The **Packet Forwarding** tab can be used to control/define how and when serial port data packets are sent from the IOLAN to the network.

Minimize Latency	This option ensures that all application data is immediately forwarded to the serial device and that every character received from the device is immediately sent on the network. Select this option for timing-sensitive applications. Default: Enabled
Optimize Network Throughput	This option provides optimal network usage while ensuring that the application performance is not compromised. Select this option when you want to minimize overall packet count, such as when the connection is over a WAN. Default: Disabled
Prevent Message Fragmentation	This option detects the message, packet, or data blocking characteristics of the serial data and preserves it throughout the communication. Select this option for message-based applications or serial devices that are sensitive to inter-character delays within these messages. Default: Disabled
Delay Between Messages	The minimum time, in milliseconds, between messages that must pass before the data is forwarded by the IOLAN. Range: 0-65535 Default: 250 ms

Custom Packet Forwarding	<p>This option allows you to define the packet forwarding rules based on the packet definition or the frame definition.</p> <p>Default: Disabled</p>
Packet Definition	<p>When enabled, this group of parameters allows you to set a variety of packet definition options. The first criteria that is met causes the packet to be transmitted. For example, if you set a Force Transmit Timer of 1000 ms and a Packet Size of 100 bytes, whichever criteria is met first is what will cause the packet to be transmitted.</p> <p>Default: Enabled</p>
Packet Size	<p>The number of bytes that must be received from the serial port before the packet is transmitted to the network. A value of zero (0) ignores this parameter.</p> <p>Range: 0-1024 bytes</p> <p>Default: 0</p>
Idle Time	<p>The amount of time, in milliseconds, that must elapse between characters before the packet is transmitted to the network. A value of zero (0) ignores this parameter.</p> <p>Range: 0-65535 ms</p> <p>Default: 0</p>
End Trigger1 Character	<p>When enabled, specifies the character that when received will define when the packet is ready for transmission. The actual transmission of the packet is based on the Trigger Forwarding Rule.</p> <p>Range: hexadecimal 0-FF</p> <p>Default: 0</p>
End Trigger2 Character	<p>When enabled, creates a sequence of characters that must be received to specify when the packet is ready for transmission (if the End Trigger1 character is not immediately followed by the End Trigger2 character, the IOLAN waits for another End Trigger1 character to start the End Trigger1/End Trigger2 character sequence). The actual transmission of the packet is based on the Trigger Forwarding Rule.</p> <p>Range: hexadecimal 0-FF</p> <p>Default: 0</p>
Frame Definition	<p>When enabled, this group of parameters allows you to control the frame that is transmitted by defining the start and end of frame character(s). If the internal buffer (1024 bytes) is full before the EOF character(s) are received, the packet will be transmitted and the EOF character(s) search will continue.</p> <p>Default: Disabled</p>
SOF1 Character	<p>When enabled, the Start of Frame character defines the first character of the frame, any character(s) received before the Start of Frame character is ignored.</p> <p>Range: hexadecimal 0-FF</p> <p>Default: 0</p>

SOF2 Character	<p>When enabled, creates a sequence of characters that must be received to create the start of the frame (if the SOF1 character is not immediately followed by the SOF2 character, the IOLAN waits for another SOF1 character to start the SOF1/SOF2 character sequence).</p> <p>Range: hexadecimal 0-FF</p> <p>Default: 0</p>
Transmit SOF Character(s)	<p>When enabled, the SOF1 or SOF1/SOF2 characters will be transmitted with the frame. If not enabled, the SOF1 or SOF1/SOF2 characters will be stripped from the transmission.</p> <p>Default: Disabled</p>
EOF1 Character	<p>Specifies the End of Frame character, which defines when the frame is ready to be transmitted. The actual transmission of the frame is based on the Trigger Forwarding Rule.</p> <p>Range: hexadecimal 0-FF</p> <p>Default: 0</p>
EOF2 Character	<p>When enabled, creates a sequence of characters that must be received to define the end of the frame (if the EOF1 character is not immediately followed by the EOF2 character, the IOLAN waits for another EOF1 character to start the EOF1/EOF2 character sequence), which defines when the frame is ready to be transmitted. The actual transmission of the frame is based on the Trigger Forwarding Rule.</p> <p>Range: hexadecimal 0-FF</p> <p>Default: 0</p>
Trigger Forwarding Rule	<p>Determines what is included in the Frame (based on the EOF1 or EOF1/EOF2) or Packet (based on Trigger1 or Trigger1/Trigger2). Choose one of the following options:</p> <ul style="list-style-type: none"> • Strip-Trigger—Strips out the EOF1, EOF1/EOF2, Trigger1, or Trigger1/Trigger2, depending on your settings. • Trigger—Includes the EOF1, EOF1/EOF2, Trigger1, or Trigger1/Trigger2, depending on your settings. • Trigger+1—Includes the EOF1, EOF1/EOF2, Trigger1, or Trigger1/Trigger2, depending on your settings, plus the first byte that follows the trigger. • Trigger+2—Includes the EOF1, EOF1/EOF2, Trigger1, or Trigger1/Trigger2, depending on your settings, plus the next two bytes received after the trigger. <p>Default: Trigger</p>

SSL/TLS Settings

You can create an encrypted connection using SSL/TLS for the following profiles: **TruePort**, **TCP Sockets**, **Terminal** (the user's **Service** must be set to **SSL_Raw**), **Serial Tunneling**, **Virtual Modem**, and **Modbus**. When you enable this feature, it will automatically use the global SSL/TLS settings (configured on **Security, SSL/TLS**), although you can configure unique SSL/TLS settings for the serial port.

When configuring SSL/TLS, the following configuration options are available:

- You can set up the IOLAN to act as an SSL/TLS client or server.
- There is an extensive selection of SSL/TLS ciphers that you can configure for your SSL/TLS connection; see [Valid SSL/TLS Ciphers](#) for a list of SSL/TLS ciphers.

-
- You can enable peer certificate validation, for which you must supply the validation criteria that was used when creating the peer certificate (this is case sensitive, so keep that in mind when enabling and configuring this option).

Note: Some combinations of cipher groups are not available on FIPS firmware versions.

See: [Network Filtering](#) for information about SSL/TLS support documents.

Validation Criteria

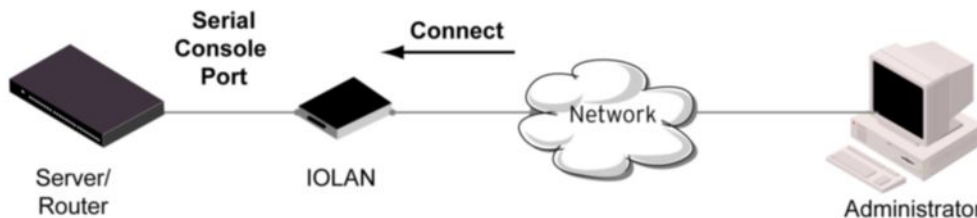
If you choose to configure validation criteria, the information in the peer SSL/TLS certificate must match exactly the information configured in this window in order to pass peer authentication and create a valid SSL/TLS connection.

Country	A country code; for example, US. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate. Data Options: Two characters
State/Province	An entry for the state/province; for example, IL. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate. Data Options: Maximum 128 characters
Locality	An entry for the location; for example, Chicago. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate. Data Options: Maximum 128 characters
Organization	An entry for the organization; for example, Accounting. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate. Data Options: Maximum 64 characters
Organization Unit	An entry for the unit in the organization; for example, Payroll. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate. Data Options: Maximum 64 characters
Common Name	An entry for common name; for example, the host name or fully qualified domain name. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate. Data Options: Maximum 64 characters
Email	An entry for an email address; for example, acct@anycompany.com. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate. Data Options: Maximum 64 characters

Console Management Profile

The Console Management profile provides access through the network to a console or administrative port of a server or router attached to the IOLAN's serial port. This profile configures the IOLAN's serial port to set up a TCP socket that will listen for a Telnet or SSH connection from the network.

Use the Console Management profile when you are configuring users who need to access a serial console port from the network.



Console Management General Parameters

Select **Serial Port**, highlight the serial port you want to change, select **Edit** to configure how the serial port will be accessed by the user through the network, then **Apply**.

Protocol	<p>Specify the connection method that users will use to communicate with a serial device connected to the IOLAN through the network.</p> <p>Data Options: Telnet, SSH</p> <p>Default: Telnet</p>
Listen for connections on TCP Port	<p>The port number that the IOLAN will listen on for incoming TCP connections.</p> <p>Note: if more than one serial port has the same TCP port number assignment, this would create a hunt group scenario. However, all operating parameters for each serial port configuration need to be the same.</p> <p>Default: 10001, depending on the serial port number</p>
Enable IP Aliasing	<p>Enables/disables the ability to access a serial device connected to the serial port by an IP address (or host name that can be resolved to the Internet Address in a DNS network) instead of the IOLAN's IP address and port number.</p> <p>Default: Disabled</p>
IP address	<p>Users can access serial devices connected to the IOLAN through the network by the specified Internet Address (or host name that can be resolved to the Internet Address in a DNS network).</p> <p>Field Format: IPv4 or IPv6 Address</p>

Console Management Advanced Parameters

The **Console Management Advanced** tab configures serial port options that may be required by certain applications.

Authenticate User	Enables/disables login/password authentication for users connecting from the network. Default: Disabled
Enable TCP Keepalive	Enables a per-connection TCP keep-alive feature. After the configured number of seconds, the connection will send a gratuitous ACK to the network peer, thus either ensuring the connection stays active OR causing a dropped connection condition to be recognized. This parameter needs to be used in conjunction with Monitor Connection Status Interval parameter found in the Serial, Advanced, Advanced Settings tab. The interval specifies the inactivity period before "testing" the connection. It should be noted that if a network connection is accidentally dropped, it can take as long as the specified interval before anyone can reconnect to the serial port. Default: Disabled
Enable Message of the Day (MOTD)	Enables/disables the display of the message of the day. Default: Disabled
Enable Microsoft Special Administer Console (SAC) support	When enabled, a user can access SAC (the interface of the Microsoft Emergency Management Systems utility) through EasyPort Web when the IOLAN's serial port is connected to a Microsoft Server 2003 or Microsoft Server 2008 host. Default: Disabled
Multisessions	The number of extra network connections available on a serial port, in addition to the single session that is always available. Enabling multisessions will permit multiple users to monitor the same console port. The maximum number of multisessions would be 101 sessions. Each user monitoring the port can be assigned different privileges to this port. Default: 0
Session Timeout	Use this timer to forcibly close the session/connection when the Session Timeout expires. Default: 0 seconds so the port will never timeout Range: 0-4294967 seconds (about 49 days)
Idle Timer	Use this timer to close a connection because of inactivity. When the Idle Timeout expires, the IOLAN will end the connection. Range: 0-4294967 seconds (about 49 days) Default: 0 seconds so the port will never timeout

Break Handling	<p>Specifies how a break is interpreted.</p> <p>Data Range:</p> <ul style="list-style-type: none"> • None—The IOLAN ignores the break key completely and it is not passed through to the host. • Local—The IOLAN deals with the break locally. If the user is in a session, the break key has the same effect as a hot key. • Remote—When the break key is pressed, the IOLAN translates this into a telnet break signal which it sends to the host machine. • Break Interrupt—On some systems such as SunOS, XENIX, and AIX, a break received from the peripheral is not passed to the client properly. If the client wishes to make the break act like an interrupt key (for example, when the stty options <code>-ignbrk</code> and <code>brkintr</code> are set). <p>Default: None</p>
Session Strings	<p>Controls the sending of ASCII strings to serial devices at session start and session termination as follows;</p> <ul style="list-style-type: none"> • Send at Start - If configured, this string will be sent to the serial device on power-up of the IOLAN, or when a kill line command is issued on this serial port. If the "monitor DSR" or "monitor DCD" options are set, the string will also be sent when the monitored signal is raised. • Range: 0-127 alpha-numeric characters. Non printable ascii characters must be entered in this format <027>. The decimal numbers within the brackets must be 3 digits long (example 003 not 3). • Send at End - If configured, this string will be sent to the serial device when the TCP session on the LAN is terminated. If multi-host is configured, this string will only be send in listen mode to the serial device when all multi-host connections are terminated. • Range: 0-127 alpha-numeric characters. Non printable ascii characters must be entered in this format <027>. The decimal numbers within the brackets must be 3 digits long (example 003 not 3). • Delay after Send—If configured, a delay time is sent to the device. This delay can be used to provide the serial device with time to process the string before the session is initiated. <p>Range: 0-65535 ms Default: 10 ms</p>
Dial In	<p>If the console port is remote and will be dialing in via modem or ISDN TA, enable this parameter.</p> <p>Default: Disabled</p>
Dial out	<p>If you want the modem to dial a number when the serial port is started, enable this parameter.</p> <p>Default: Disabled</p>
Dial Timeout	<p>The number of seconds the IOLAN will wait to establish a connection to a remote modem.</p> <p>Range: 1-99 Default: 45 seconds</p>

Dial Retry	The number of times the IOLAN will attempt to re-establish a connection with a remote modem. Range: 0-99 Default: 2
Modem	The name of the predefined modem that is used on this port. If you are using a IOLAN with a built in modem port then select iolan_modem. See Adding/Editing a Modem
Phone	The phone number to use when Dial Out is enabled.

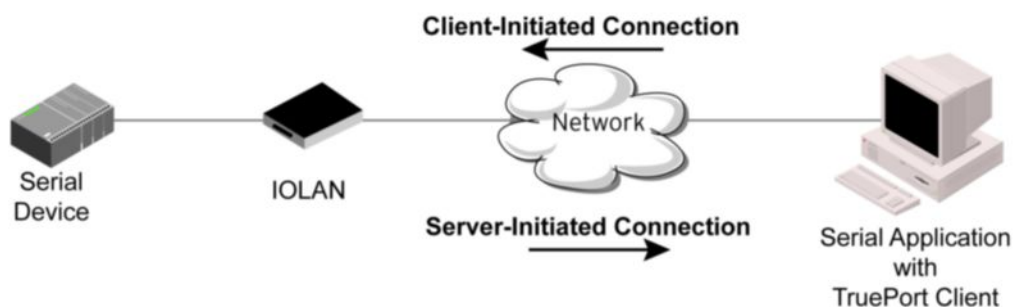
Trueport Profile

Trueport is a COM Port redirector that is supplied with the IOLAN. TruePort can be installed as a client on a Workstation or Server and supports a variety of operating systems. It, in conjunction with the IOLAN, emulates a local serial port (COM port), to the application, to provide connectivity to a remote serial device over the network. The TruePort profile operates in conjunction with the TruePort software.

Trueport can be run in two modes (these modes will be set on the client software when it is configured):

- **TruePort Full mode**—This mode allows complete device control and operates as if the device was directly connected to the Workstation/Server's local serial port. It provides a complete COM port interface between the attached serial device and the network. All serial controls, baud rate control, etc., are sent to the IOLAN and replicated on its associated serial port.
- **TruePort Lite mode**—This mode provides a simple raw data interface between the application and the remote serial port. Although the port will still operate as a COM port, control signals are ignored. In this mode, the serial communications parameters must be configured on the Trueport Profile.

See the *TruePort User's Guide* for more details about the TruePort client software



Trueport General Parameters

The **TruePort General** tab determines how the TruePort connection is initiated and then sets up the appropriate connection parameters.

Connect to Remote System (Server-Initiated Connection)	When enabled, the IOLAN initiates communication to the TruePort client. Default: Enabled
Host Name	The configured host that the IOLAN will connect to (must be running TruePort). Default: None
TCP Port	The TCP Port that the IOLAN will use to communicate through to the TruePort client. 10001 for serial port 1, then increments by one for each serial port
HTTP Tunnel	Specify the HTTP tunnel to be used for this connection.
Connect to Multiple Hosts	When enabled, the IOLAN will establish a connection to multiple clients (Hosts). When using the multiple hosts feature, all TruePort clients must be running in Lite mode. Default: Disabled

Send Name On Connect	When enabled, the port name will be sent to the host upon session initiation. This will be done before any other data is sent or received to/from the host. Default: Disabled
Define Additional Hosts Button	Select this button to define the hosts that this serial port will connect to. This button is also used to define the Primary/Backup host functionality. See Host Table for more information.
Listen for Connection (Client-Initiated Connection)	When enabled, the IOLAN will wait for connections to be initiated by the TruePort Client. Default: Disabled
TCP Port	The TCP Port that the IOLAN will use to communicate through to the TruePort client. Default: 10001 for serial port 1
Allow Multiple Hosts to connect	When this option is enabled, multiple hosts can connect to a serial device that is connected to this serial port. Note: These multiple clients (Hosts) need to be running TruePort in Lite mode. Default: Disabled

Adding/Editing Additional TruePort Hosts

You can define a list of hosts that the serial device will communicate to through TruePort Lite or a primary/backup host.

Define Additional hosts to connect to	When this option is enabled, you can define up to 49 hosts that the serial device connected to this serial port will attempt communicate to. With this mode of operation, the IOLAN will connect to multiple hosts simultaneously. Default: Enabled See Host Table for more information.
Define a primary host and a backup host to connection	When this option is enabled, you need to define a primary host that the serial device connected to this serial port will communicate to and a backup host, in the event that the IOLAN loses communication to the primary host. The IOLAN will first establish a connection to the primary host. Should the connection to the primary host be lost (or never established), the IOLAN will establish a connection the backup host. Once connected to the backup, the IOLAN will attempt to re-establish a connection to the Primary host, once this is successfully done, it gracefully shuts down the backup connection. Default: Disabled
Primary Host	Specify a preconfigured host that the serial device will communicate to through the IOLAN. Default: None
TCP Port	Specify the TCP port that the IOLAN will use to communicate to the Primary Host . Default: 0
Backup Host	Specify a preconfigured host that the serial device will communicate to through the IOLAN if the IOLAN cannot communicate with the Primary Host . Default: None

TCP Port	Specify the TCP port that the IOLAN will use to communicate to the Backup Host . Default: 10000
-----------------	--

Adding/Editing a Multi-host Entry

When you select the **Add** or **Edit** button, the Host Entry window appears. The hosts in the multi-host list must already be defined. If you add a host that was defined with its fully qualified domain name (FQDN), it must be resolvable by your configured DNS server.

Host	Specify the preconfigured host that will be in the multi-host list. Default: None
-------------	---

TCP Port	Specify the TCP port that the IOLAN will use to communicate to the Primary Host . Default: 1000 + serial port number -1
-----------------	--

Trueport Advanced Parameters

The **TruePort Advanced** tab determines how the TruePort connection is initiated and then sets up the appropriate connection parameters.

Signals high when not under TruePort client control	<p>This option has the following impact based on the state of the TruePort connection:</p> <ul style="list-style-type: none">• TruePort Lite Mode—When enabled, the EIA-232 signals remain active before, during, and after the TruePort connection is established. When disabled, the EIA-232 signals remain inactive during and after the Trueport connection is established.• TruePort Full Mode—When enabled, the EIA-232 signals remain active before and after the TruePort connection and the TruePort client will control the state of the signals during the established TruePort connection. When disabled, the EIA-232 signals remain inactive before and after the TruePort connection and the TruePort client will control the state of the signals during the established TruePort connection. <p>Default: Enabled</p>
--	--

Enable Message the Day (MOTD)	Enables/disables the display of the message of the day. Default: Disabled
--------------------------------------	---

Enable TCP Keepalive	<p>Enables a per-connection TCP keep-alive feature. After the configured number of seconds, the connection will send a gratuitous ACK to the network peer, thus either ensuring the connection stays active OR causing a dropped connection condition to be recognized.</p> <p>This parameter needs to be used in conjunction with Monitor Connection Status Interval parameter found in the Serial, Advanced, Advanced Settings tab. The interval specifies the inactivity period before "testing" the connection.</p> <p>Note: If a network connection is accidentally dropped, it can take as long as the specified interval before anyone can reconnect to the serial port.</p> <p>Default: Disabled</p>
-----------------------------	---

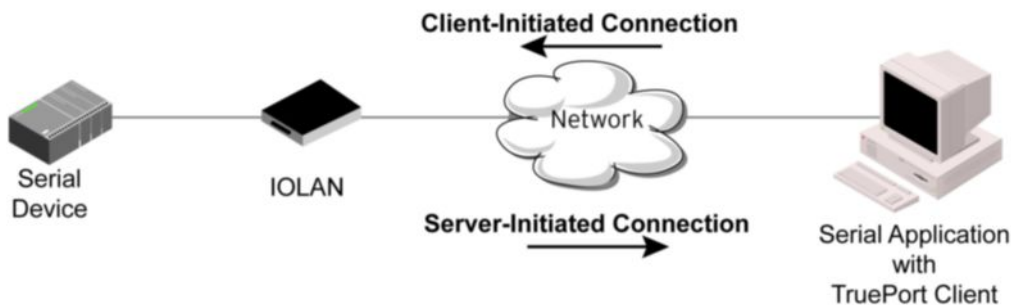
Enable Data Logging (Trueport Lite Mode)	<p>When enabled, serial data will be buffered if the TCP connection is lost. When Logging the TCP connection is re-established, the buffered serial data will be sent to its destination. If using the Trueport profile, data logging is only supported in Lite Mode. If the data buffer is filled, incoming serial data will overwrite the oldest data.</p> <p>The minimum data buffer size is 1 KB. The maximum data buffer size is 2000 KB for DS1/TS2/STS8D</p> <p>Values: 1-2000 KB (DS1/TS2/STS8D) - Default 4 KB</p> <p>Default: Disabled</p> <p>Note: A kill line or a reboot of the IOLAN causes all buffered data to be lost</p> <p>Some profile features are not compatible with the data logging feature. See the Data Logging Feature.</p> <p>To change the default data logging buffer size see Serial Settings Advanced Parameters.</p>
Idle Timeout	<p>Use this timer to close a connection because of inactivity. When the Idle Timeout expires, the IOLAN will end the connection.</p> <p>Range: 0-4294967 seconds (about 49 days)</p> <p>Default: 0 seconds so the port will never timeout</p>
Session Timeout	<p>Use this timer to forcibly close the session/connection when the Session Timeout expires.</p> <p>Default: 0 seconds so the port will never timeout</p> <p>Range: 0-4294967 seconds (about 49 days)</p>
Session Strings	<p>Controls the sending of ASCII strings to serial device at session start as follows;</p> <ul style="list-style-type: none"> • Send at Start—If configured, this string will be sent to the serial device on power-up of the IOLAN, or when a kill line command is issued on this serial port. If the "monitor DSR" or "monitor DCD" options are set, the string will also be sent when the monitored signal is raised. • Range: 0-127 alpha-numeric characters • Range: hexadecimal 0-FF • Delay after Send - If configured, will inset a delay after the string is sent to the device. This delay can be used to provide the serial device with time to process the string before the session is initiated. <p>Range: 0-65535 ms</p> <p>Default: 10 ms</p>
Dial in	<p>If the device is remote and will be dialing in via modem or ISDN TA, enable this parameter.</p> <p>Default: Disabled</p>
Dial out	<p>If you want the modem to dial a number when the serial port is started, enable this parameter.</p> <p>Default: Disabled</p>

Dial Timeout	The number of seconds the IOLAN will wait to establish a connection to a remote modem. Range: 1-99 Default: 45 seconds
Dial Retry	The number of times the IOLAN will attempt to re-establish a connection with a remote modem. Range: 0-99 Default: 2
Modem	The name of the predefined modem that is used on this port. If you are using a IOLAN SCG with a built in modem then select iolan_modem. See Adding/Editing a Modem
Phone	The phone number to use when Dial Out is enabled.

TCP Sockets Profile

The TCP Socket profile allows for a serial device to communicate over a TCP network. The TCP connection can be initiated from a host on the network and/or a serial device. This is typically used with an application on a Workstation or Server that communicates to a device using a specific TCP socket. This is often referred to as a RAW connection.

The TCP Sockets profile permits a raw connection to be established in either direction, meaning that the connection can be initiated by either the Workstation/Server or the IOLAN.



TCP Sockets General Parameters

Listen for Connection When enabled, the IOLAN listens for a connection to be established by the Workstation/Server on the network.

Default: Enabled

TCP Port The TCP port that the IOLAN will use to listen for incoming connections.

Default: 10000 plus the serial port number, so serial port 5 would have a default of 10005

HTTP Tunnel Specify the HTTP tunnel to be used for this connection.

Allow Multiple Hosts to Connect When this option is enabled, multiple hosts can connect to the serial device that is connected to this serial port.

Default: Disabled

Enable IP Aliasing Enables/disables the ability to access a serial device connected to the serial port by an IP address (or host name that can be resolved to the Internet Address in a DNS network) instead of the IOLAN's IP address and port number.

Default: Disabled

IP Address Users can access serial devices connected to the IOLAN through the network by the specified Internet Address (or host name that can be resolved to the Internet Address in a DNS network).

Field Format: IPv4 or IPv6 Address

Connect To When enabled, the IOLAN initiates communication to the Workstation/Server.

Default: Disabled

Host Name	The name (resolvable via DNS) or IP address of the configured host the IOLAN will connect to.
TCP Port	The TCP Port that the IOLAN will use to communicate to the client. Default: 0
Connect to Multiple Hosts	When enabled, allows a serial device connected to this serial port to communicate to multiple hosts. Default: Disabled
Define Additional Hosts Button	Select this button to define the hosts that this serial port will connect to. This button is also used to define the Primary/Backup host functionality.
Initiate Connection Automatically	If the serial port hardware parameters have been setup to monitor DSR or DCD, the host session will be started once the signals are detected. If no hardware signals are being monitored, the IOLAN will initiate the session immediately after being powered up. Default: Enabled
When any data is received	Initiates a connection to the specified host when any data is received on the serial port. Default: Disabled
When <hexadecimal value> is received	Initiates a connection to the specified host only when the specified character is received on the serial port. Default: Disabled
Send Name On Connect	When enabled, the port name will be sent to the host upon session initiation. This will be done before any other data is sent or received to/from the host Default: Disabled
Permit Connections in Both Directions	When this option is enabled, the connection can be initiated by either the IOLAN or a host. Default: Disabled

Adding/Editing Additional Hosts

You can define a list of hosts that the serial device will communicate to or a primary/backup host.

Define additional hosts to connect to	When this option is enabled, you can define up to 49 hosts that the serial device connected to this serial port will attempt communicate to. With this mode of operation, the IOLAN will connect to multiple hosts simultaneously. Default: Enabled
--	---

Define a primary host and a backup host to connect to	<p>When this option is enabled, you need to define a primary host that the serial device connected to this serial port will communicate to and a backup host, in the event that the IOLAN loses communication to the primary host. The IOLAN will first establish a connection to the primary host. Should the connection to the primary host be lost (or never established), the IOLAN will establish a connection to the backup host. Once connected to the backup, the IOLAN will attempt to re-establish a connection to the Primary host, once this is successfully done, it gracefully shuts down the backup connection.</p> <p>Default: Disabled</p>
Primary Host	<p>Specify a pre-configured host that the serial device will communicate to through the IOLAN.</p> <p>Default: None</p>
TCP Port	<p>Specify the TCP port that the IOLAN will use to communicate to the Primary Host.</p> <p>Default: 0</p>
Backup Host	<p>Specify a preconfigured host that the serial device will communicate to through the IOLAN if the IOLAN cannot communicate with the Primary Host.</p> <p>Default: None</p>
TCP Port	<p>Specify the TCP port that the IOLAN will use to communicate to the Backup Host.</p> <p>Default: 10000</p>

Adding/Editing a Multi-host Entry

When you select the **Add** or **Edit** button, the Host Entry window appears. The hosts in the multi-host list must already be defined (see Host Table to learn how to create a host). If you add a host that was defined with its fully qualified domain name (FQDN), it must be resolvable by your configured DNS server. Configure the following parameters:

Host	<p>Specify the preconfigured host that will be in the multi-host list.</p> <p>Default: None</p>
TCP Port	<p>Specify the TCP port that the IOLAN will use to communicate to the Host.</p> <p>Default: 0</p>

TCP Sockets Advanced Parameters

Authenticate User	<p>Enables/disables login/password authentication for users connecting from the network.</p> <p>Default: Disabled</p>
Enable TCP Keepalive	<p>Enables a per-connection TCP keep-alive feature. After the configured number of seconds, the connection will send a gratuitous ACK to the network peer, thus either ensuring the connection stays active OR causing a dropped connection condition to be recognized.</p> <p>This parameter needs to be used in conjunction with Monitor Connection Status Interval parameter found in the Serial, Advanced, Advanced Settings tab. The interval specifies the inactivity period before "testing" the connection.</p> <p>Default: Disabled</p>

Enable Message of the Day (MOTD)	<p>Enables/disables the display of the message of the day.</p> <p>Default: Disabled</p>
Enable Data Logging	<p>When enabled, serial data will be buffered if the TCP connection is lost. When Logging the TCP connection is re-established, the buffered serial data will be sent to its destination. If using the Trueport profile, data logging is only supported in Lite Mode.</p> <p>The minimum data buffer size for all models is 1 KB. The maximum data buffer size is 2000 KB for DS1/TS2/STS8D, all other models are 4000 KB.</p> <p>If the data buffer is filled, incoming serial data will overwrite the oldest data.</p> <p>Values: 1-2000 KB (DS1/TS2/STS8D) - Default 4 KB</p> <p>Values: 1-4000 KB (all other models) - Default 256 KB</p> <p>Default: Disabled</p> <p>Note: A kill line or a reboot of the IOLAN causes all buffered data to be lost. Some profile features are not compatible with the data logging feature. See Data Logging Feature</p>
Idle Timeout	<p>Use this timer to close a connection because of inactivity. When the Idle Timeout expires, the IOLAN will end the connection.</p> <p>Range: 0-4294967 seconds (about 49 days)</p> <p>Default: 0 seconds so the port will never timeout</p>
Session Timeout	<p>Use this timer to forcibly close the session/connection when the Session Timeout expires.</p> <p>Default: 0 seconds so the port will never timeout</p> <p>Range: 0-4294967 seconds (about 49 days)</p>
Session Strings	<p>Controls the sending of ASCII strings to serial devices at session start and session termination as follows;</p> <ul style="list-style-type: none"> • Send at Start - If configured, this string will be sent to the serial device on power-up of the IOLAN, or when a kill line command is issued on this serial port. If the "monitor DSR" or "monitor DCD" options are set, the string will also be sent when the monitored signal is raised. • Range: 0-127 alpha-numeric characters. Non printable ascii characters must be entered in this format <027>. The decimal numbers within the brackets must be 3 digits long (example 003 not 3). • Send at End - If configured, this string will be sent to the serial device when the TCP session on the LAN is terminated. If multi-host is configured, this string will only be send in listen mode to the serial device when all multi-host connections are terminated. • Range: 0-127 alpha-numeric characters. Non printable ascii characters must be entered in this format <027>. The decimal numbers within the brackets must be 3 digits long (example 003 not 3). • Delay after Send—If configured, a delay time is sent to the device. This delay can be used to provide the serial device with time to process the string before the session is initiated. <p>Range: 0-65535 ms</p> <p>Default: 10 ms</p>

Dial in	If the device is remote and will be dialing in via modem or ISDN TA, enable this parameter. Default: Disabled
Dial out	If you want the modem to dial a number when the serial port is started, enable this parameter. Default: Disabled
Dial Timeout	The number of seconds the IOLAN will wait to establish a connection to a remote modem. Range: 1-99 Default: 45 seconds
Dial Retry	The number of times the IOLAN will attempt to re-establish a connection with a remote modem. Range: 0-99 Default: 2
Modem	The name of the predefined modem that is used on this port. If you are using a IOLAN SCG with a built in modem then select iolan_modem. See Adding/Editing a Modem
Phone	The phone number to use when Dial Out is enabled.

UDP Sockets Profile

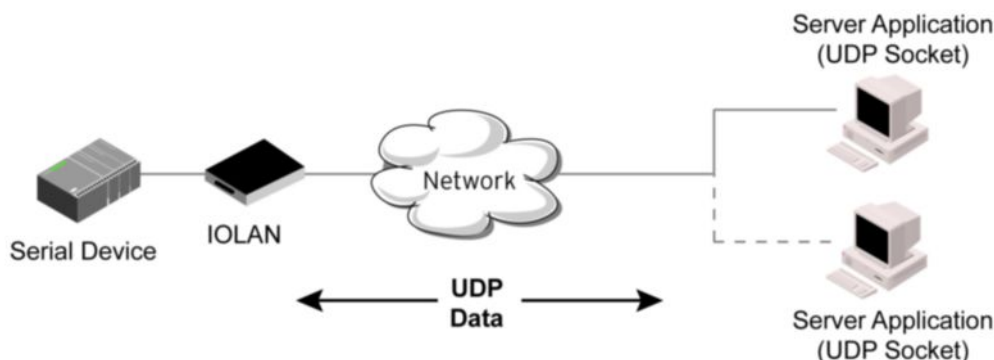
The UDP profile configures a serial port to send or receive data to/from the LAN using the UDP protocol. When you configure UDP, you are setting up a range of IP addresses and the port numbers that you will use to send UDP data to or receive UDP data from.

When you configure UDP for **LAN to Serial**, the following options are available:

To send to a single IP address, leave the **End IP Address** field at its default value (0.0.0.0).

The IP address can be auto learned if both start/end IP address are left blank/default.

If the **Start IP Address** field is set to 255.255.255.255 and the **End IP Address** is left at its default value (0.0.0.0), the IOLAN will accept UDP packets from any source address.



Four individual entries are provided to allow you greater flexibility to specify how data will be forwarded to/from the serial device. All four entries support the same configuration parameters. You can configure one or more of the entries as needed.

The first thing you need to configure for an entry is the “**Direction**” of the data flow. The following options are available;

- **Disabled** - UDP service not enabled.
- **LAN to Serial** - This setting will allow UDP data to be received from one or more hosts on the LAN and forwarded to the serial device attached to this serial port.
- **Serial to LAN** - This setting will allow data originating from the serial device attached to this serial port to be sent to one or more hosts on the LAN using UDP datagrams.
- **Both** - Allows for data to flow from the serial device to the LAN and from the LAN to the serial device.

The role of each of the configurable parameters in an entry depends on the “**Direction**” selected.

When the direction is “**LAN to Serial**” the role of the additional parameters is as follow;

- **Start IP Address** - This is the IP address of the host from which the UDP data will originate. If the data will originate from a number of hosts, this becomes the starting IP address of a range.
- **End IP Address** - If you wish to receive data only from the single host defined by "Start IP address", leave this entry as is (0.0.0.0). If you wish to accept data from a number of hosts, this address will represent the upper end of a range starting from "Start IP address". Only data originating from this range will be forwarded to the serial port.
- **UDP port** - This is the UDP port from which the data will originate. There are three options for this parameter.
- **Auto Learn** - The first UDP message received will be used to define which UDP port we are going to accept UDP data from. Once learned, only data from this UDP port will be accepted. The data must also originate from a host which is in the IP range defined for this entry.
- **Any Port** - Any UDP port will be accepted as long as the data originates from a host in the IP range defined for this entry.

- **Port** - Only data originating from the UDP port configured here as well as originating from a host in the IP range defined for this entry will be accepted.

When the direction is "**Serial to LAN**" the role of the additional parameters is as follow;

- **Start IP Address** - This is the IP address of the host to which the serial data will be sent using UDP datagrams. If the serial data is to be sent to more than one host, this becomes the starting IP address of a range.
- **End IP Address** - If you wish to send serial data to a single host, leave this entry as is (0.0.0.0). If you wish to send the serial data to a number of hosts, this address will represent the upper end of a range starting from "Start IP Address".
- **UDP port** - This is the UDP port to which the serial data will be forwarded. For a direction of "Serial to LAN", you must specify the port to be used.

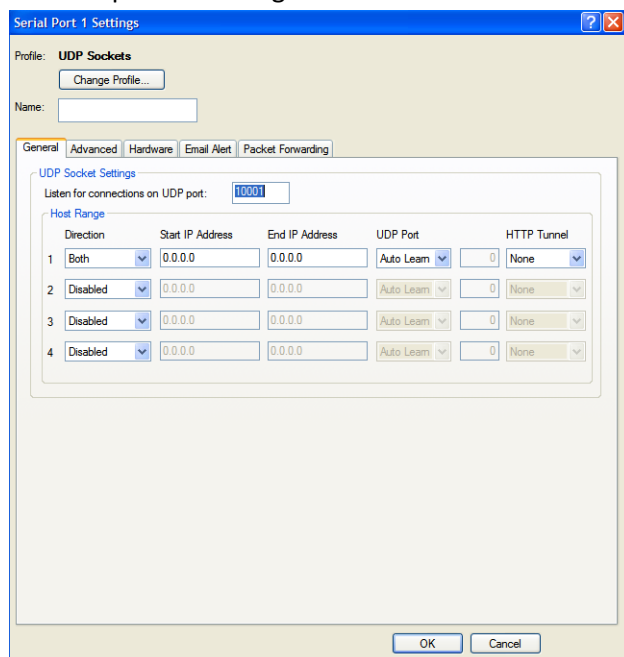
When the direction is "**Both**" the role of the additional parameters is as follow;

- **Start IP Address** - This is the IP address of the host to which the serial data will be sent using UDP datagrams. It is also the IP address of the host from which UDP data coming from the LAN will be accepted from. If the data is to be sent to or received from more than one host, this becomes the starting IP address of a range.
- **End IP Address** - If you wish to send serial data to a single host and only receive data from the single UDP host, leave this entry as is (0.0.0.0). If the data is to be sent to or received from more than one host, this address will represent the upper end of a range starting from "Start IP Address". Only data originating from this range will be forwarded to the serial port.
- **UDP Port** - This is the UDP port to which the serial data will be forwarded as well as the UDP port from which data originating on the LAN will be accepted from. For a direction of "Both", there are two valid option for the UDP Port as follows;
- **Auto Learn** - The first UDP message received will be used to define which port we are going to accept UDP data from. Once learned, only data from this UDP port will be accepted and serial data being forwarded to the LAN will be sent to this UDP port. Until the port is learned, data from the serial port intended to be sent to the LAN will be discarded.
- **Port** - Serial data being forwarded to the LAN from the serial device will sent to this UDP port. Only data originating from the UDP port configured here (as well as originating from a host in the IP range defined for this entry) will be forwarded to the serial device.

Special values for "**Start IP address**"

- **0.0.0.0** - This is the "auto learn IP address" value which is valid only in conjunction with the "LAN to Serial" setting. The first UDP packet received for this serial port will set the IP address from which we will accept future UDP packets to be forwarded to the serial port. For this setting, leave the "End IP Address" as 0.0.0.0.
- **255.255.255.255** - This selection is only valid in conjunction with the "LAN to Serial" setting. It will accept all UDP packets received for this serial port regardless of the originating IP address. For this setting, leave the "End IP Address" as 0.0.0.0.
- **Subnet directed broadcast** - You can use the "Start IP Address" field to enter a subnet directed broadcast address. This is done by specifying the subnet address with the host portion filled with 1s. For example, if you are on the subnet 172.16.x.x with a subnet mask of 255.255.254.0 than you would specify an IP address of 172.16.1.255 (all ones for host portion). For this setting, leave the "End IP Address" as 0.0.0.0. For any "LAN to Serial" ranges you have defined for this serial port, you must ensure that IP address of this IOLAN is not included in the range. If your IP address is within the range, you will receive the data you send via the subnet directed broadcasts as data coming in from the LAN.

An example UDP configuration is described based on the following window.



The UDP configuration window, taken from the DeviceManager, is configured to:

UDP Entry 1

All UDP data received from hosts that have an IP address that falls within the range of 172.16.1.25 to 172.16.1.50 and source UDP **Port** of 33010 will be sent to the serial device. The IOLAN will not send any data received on its serial port to the host range defined by this entry.

UDP Entry 2

All hosts that have an IP Address that falls within the range of 172.16.1.75 to 172.16.1.80 and who listen to UDP **Port** 33009 will receive UDP data from the serial device. No UDP data originating from the hosts defined by this entry will be forwarded to the serial device.

UDP Entry 3

All hosts that have an IP address that falls within the range of 172.16.1.1 to 172.16.1.20 and listen to **Port** 33001 will be sent the data from the serial device in UDP format. The serial device will only receive UDP data from the hosts in that range with a source UDP **Port** of 33001. The IOLAN will listen for data on the port value configured in the **Listen for connections on UDP port** parameter. (10001 in above example)

UDP Entry 4

This entry is disabled since **Direction** is set to **Disabled**.

UDP Sockets General Parameters

Listen for connections on UDP Port The IOLAN will listen for UDP packets on the specified port.
Default: 1000+<port-number> (for example, 10001 for serial port 1)

Direction	<p>The direction in which information is received or relayed:</p> <ul style="list-style-type: none"> • Disabled—UDP service not enabled. • LAN to Serial—This setting will allow UDP data to be received from one or more hosts on the LAN and forwarded to the serial device attached to this serial port. • Serial to LAN—This setting will allow data originating from the serial device attached to this serial port to be sent to one or more hosts on the LAN using UDP datagrams. • Both—Allows for data to flow from the serial device to the LAN and from the LAN to the serial device. <p>Default: Both for UDP 1 and Disabled for all other UDP ranges</p>
Start IP address	<p>The first host IP address in the range of IP addresses (for IPv4 or IPv6) that the IOLAN will listen for messages from and/or send messages to.</p> <p>Field Format: IPv4 or IPv6 address</p>
End IP address	<p>The last host IP address in the range of IP addresses (for IPv4, not supported for IPv6) that the IOLAN will listen for messages from and/or send messages to.</p> <p>Field Format: IPv4 address</p>
UDP Port	<p>Determines how the IOLAN's UDP port that will send/receive UDP messages is defined:</p> <ul style="list-style-type: none"> • Auto Learn—The IOLAN will only listen to the first port that it receives a UDP packet from. Applicable when Direction is set to LAN to Serial or Both. • Any Port—The IOLAN will receive messages from any port sending UDP packets. Applicable when Direction is set to LAN to Serial. • Port—The port that the IOLAN will use to relay messages to servers/hosts. This option works with any Direction except Disabled. The IOLAN will listen for UDP packets on the port configured by the Listen for connections on UDP port parameter. <p>Default: Auto Learn</p>
Port	<p>The UDP port to use.</p> <p>Default: 0 (zero)</p>
HTTP Tunnel	<p>Specify the HTTP tunnel to be used for this connection.</p>

UDP Sockets Advanced Parameters

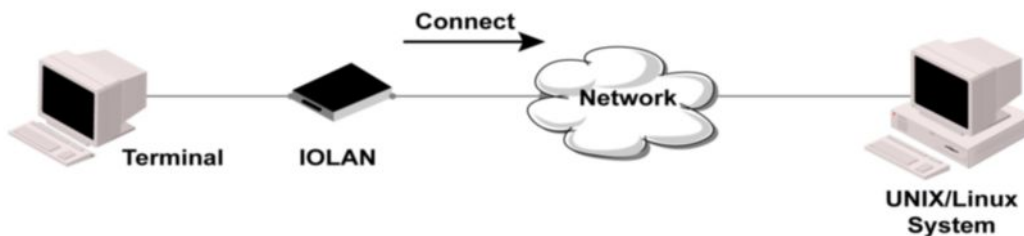
Session Strings	<p>Controls the sending of ASCII strings to serial devices at session start as follows;</p> <ul style="list-style-type: none"> • Send at Start—If configured, this string will be sent to the serial device on power-up of the IOLAN or when a kill line command is issued on this serial port. If the "monitor DSR" or "monitor DCD" options are set, the string will also be sent when the monitored signal is raised. • Range: 0-127 alpha-numeric characters • Range: hex 0-FF • Delay after Send—If configured, will inset a delay after the string is sent to the device. This delay can be used to provide the serial device with time to process the string before the session is initiated or terminated. • Default: 10 ms
------------------------	---

Terminal Profile

The Terminal profile allows network access from a terminal connected to the IOLAN's serial port. This profile is used to access pre-defined hosts on the network from the terminal.

This profile can be configured for users:

- who must be authenticated by the IOLAN first and then a connection to a host can be established.
- who are connecting through the serial port directly to a host.



Terminal Profile Parameters

Terminal Type	<p>Specifies the type of terminal connected to the line.</p> <p>Data Options:</p> <ul style="list-style-type: none">• Dumb• WYSE60• VT100• ANSI• TVI925• IBM3151TE• VT320 (specifically supporting VT320-7)• HP700 (specifically supporting HP700/44)• Term1, Term2, Term3 (user-defined terminals) <p>Default: Dumb</p>
Require Login	<p>When users access the IOLAN through the serial port, they must be authenticated, using either the local user database or an external authentication server.</p> <p>Default: Enabled</p>
User Service Settings Button	<p>After a user has been successfully authenticated, the IOLAN will connect to the specified host using the specified protocol according to:</p> <ul style="list-style-type: none">• the User Service parameter for locally configured users• the Default User Service parameter for users who are externally authenticated <p>TACACS+/RADIUS for externally authenticated users where the target host is passed to the IOLAN</p> <p>See User Services Parameters</p>
Connect to remote system	<p>When the serial port is started, the IOLAN will initiate a connection to the specified host using the specified protocol. With this option, user authentication will not be performed by the IOLAN.</p> <p>Default: Disabled</p>

Protocol	Specify the protocol that will be used to connect to the specified host. Data Options: Telnet, SSH, Rlogin Default: Telnet
Settings Button	Select this button to define the settings for the protocol that will be used to connect the user to the specified host.
Host Name	The name (resolvable via DNS) or IP address of the configured host the IOLAN will connect to.
TCP Port	The TCP Port that the IOLAN will use to connect to the host. Default: Telnet-23, SSH-22, Rlogin-513
Automatically	If the serial port hardware parameters have been setup to monitor DSR or DCD, the host session will be started once the signals are detected. If no hardware signals are being monitored, the IOLAN will initiate the session immediately after being powered up. Default: Enabled
When any data is received	Initiates a connection to the specified host when any data is received on the serial port. Default: Disabled
When <hexadecimal value> is received	Initiates a connection to the specified host only when the specified character is received on the serial port. Default: Disabled

Terminal Profile Advanced Parameters

Enable Message of the Day (MOTD)	Enables/disables the display of the message of the day. Default: Disabled
Reset Terminal on disconnect	When enabled, resets the terminal definition connected to the serial port when a user logs out. Default: Disabled
Allow Port Locking	When enabled, the user can lock his terminal with a password using the Hotkey Prefix (default Ctrl-a) ^a l (lowercase L). The IOLAN prompts the user for a password and a confirmation. Default: Disabled

Hotkey Prefix	<p>The prefix that a user types to lock a serial port or redraw the Menu.</p> <p>Data Range:</p> <ul style="list-style-type: none"> • ^a l—(Lowercase l) Locks the serial port until the user unlocks it. The user is prompted for a password (any password, excluding spaces) and locks the serial port. Next, the user must retype the password to unlock the serial port. • ^r—When you switch from a session back to the Menu, the screen may not be redrawn correctly. If this happens, use this command to redraw it properly. This is always Ctrl R, regardless of the Hotkey Prefix. <p>You can use the Hotkey Prefix key to lock a serial port only when the Allow Port Locking parameter is enabled.</p> <p>Default: hexadecimal 01 (Ctrl-a, ^a)</p>
Idle Timeout	<p>Use this timer to close a connection because of inactivity. When the Idle Timeout expires, the IOLAN will end the connection.</p> <p>Range: 0-4294967 seconds (about 49 days)</p> <p>Default: 0 seconds so the port will never timeout</p>
Session Timeout	<p>Use this timer to forcibly close the session/connection when the Session Timeout expires.</p> <p>Default: 0 seconds so the port will never timeout</p> <p>Range: 0-4294967 seconds (about 49 days)</p>
Session Strings	<p>Controls the sending of ASCII strings to serial device at session start as follows;</p> <p>Send at Start—If configured, this string will be sent to the serial device on power-up of the IOLAN, or when a kill line command is issued on this serial port. If the "monitor DSR" or "monitor DCD" options are set, the string will also be sent when the monitored signal is raised.</p> <p>Range: 0-127 alpha-numeric characters</p> <p>Range: hexadecimal 0-FF</p> <p>Delay after Send - If configured, will inset a delay after the string is sent to the device. This delay can be used to provide the serial device with time to process the string before the session is initiated.</p> <p>Range: 0-65535 ms</p> <p>Default: 10 ms</p>
Dial Timeout	<p>The number of seconds the IOLAN will wait to establish a connection to a remote modem.</p> <p>Range: 1-99</p> <p>Default: 45 seconds</p>
Dial Retry	<p>The number of times the IOLAN will attempt to re-establish a connection with a remote modem.</p> <p>Range: 0-99</p> <p>Default: 2</p>
Dial In	<p>If the device is remote and will be dialing in via modem or ISDN TA, enable this parameter.</p> <p>Default: Disabled</p>

Dial Out	If you want the modem to dial a number when the serial port is started, enable this parameter. Default: Disabled
Modem	The name of the predefined modem that is used on this line. If you are using a IOLAN SCG with a built in modem then select iolan_modem. See Adding/Editing a Modem
Phone	The phone number to use when Dial Out is enabled.

User Service Settings

Login Settings

These settings apply to users who are accessing the network from a terminal connected to the IOLAN's serial port. The Telnet, Rlogin, SSH, SLIP, PPP settings take effect when the connection method is defined in the user's profile (or are passed to the IOLAN by a RADIUS or TACACS+ server when those authentication methods are being used).

Limit Connection to User	Makes the serial port dedicated to the specified user. The user won't need to enter their login name - just their password.
Initial Mode	Specifies the initial interface a user navigates when logging into the serial port. Data Options: Command Line Default: Command Line
Terminal Pages	The number of video pages the terminal supports. Range: 1-7 Default: 5 pages

Telnet Settings

The Telnet settings apply when the **User Service** is set to **Telnet** or the Terminal profile specifies a **Telnet** connection to a host.

Terminal Type	Type of terminal attached to this serial port; for example, ANSI or WYSE60.
Local Echo	Toggles between local echo of entered characters and suppressing local echo. Local echo is used for normal processing, while suppressing the echo is convenient for entering text that should not be displayed on the screen, such as passwords. This parameter can be used only when Enable Line Mode is enabled. Default: Disabled
Enable Line Mode	When enabled, keyboard input is not sent to the remote host until Enter is pressed, otherwise input is sent every time a key is pressed. Default: Disabled
Map CR to CRLF	When enabled, maps carriage returns (CR) to carriage return line feed (CRLF). Default: Disabled

Interrupt	Defines the interrupt character. Typing the interrupt character interrupts the current process. This value is in hexadecimal. Default: 3 (ASCII value ^C)
Quit	Defines the quit character. Typing the quit character closes and exits the current telnet session. This value is in hexadecimal. Default: 1c (ASCII value FS)
EOF	Defines the end-of-file character. When Enable Line Mode is enabled, entering the EOF character as the first character on a line sends the character to the remote host. This value is in hexadecimal. Default: 4 (ASCII value ^D)
Erase	Defines the erase character. When Line Mode is Off , typing the erase character erases one character. This value is in hexadecimal. Default: 8 (ASCII value ^H)
Echo	Defines the echo character. When Line Mode is On , typing the echo character echoes the text locally and sends only completed lines to the host. This value is in hexadecimal. Default: 5 (ASCII value ^E)
Escape	Defines the escape character. Returns you to the command line mode. This value is in hexadecimal. Default: 1d (ASCII value GS)

Rlogin Settings

The Rlogin settings apply when the **User Service** is set to **Rlogin** or the Terminal profile has **Require Login** selected and specifies an **Rlogin** connection to a host.

Configure the following parameters:

Terminal Type Type of terminal attached to this serial port; for example, ANSI or WYSE60.

When **Connect to remote system** is selected, the Rlogin window requires the name of the user who is connecting to the host.

Terminal Type Type of terminal attached to this serial port; for example, ANSI or WYSE60.

User This name is passed on to the specified host for the Rlogin session, so that the user is only prompted for a password.

SSH Setting

The SSH settings apply when the **User Service** is set to **SSH** or the Terminal profile specifies an **SSH** connection to a host.

Note: Some combinations of cipher groups are not available on FIPS firmware versions.
SSH-1 protocol is not available on FIPS firmware versions.

Terminal Type Type of terminal attached to this serial port; for example, ANSI or WYSE60.

Verbose Mode	When enabled, displays debug messages on the terminal. Default: Disabled
Enable Compression	When enabled, requests compression of all data. Compression is desirable on modem lines and other slow connections, but will only slow down things on fast networks. Default: Disabled
Strict Host Key Checking	When enabled, a host public key (for each host you wish to ssh to) must be downloaded into the IOLAN. Default: Enabled
Auto Login	When enabled, creates an automatic SSH login, using the Name and Password values. Default: Disabled
Name	The name of the user logging into the SSH session. Field Format: Up to 20 alphanumeric characters, excluding spaces
Password	The user's password when Auto Login is enabled. Field Format: Up to 20 alphanumeric characters, excluding spaces
SSH1	When enabled, selects an SSH version 1 connection. Default: Enabled
SSH1 Cipher	Select the encryption method (cipher) that you want to use for your SSH version 1 connection: Data Options: <ul style="list-style-type: none">• 3DES• Blowfish Default: 3DES
SSH2	When enabled, selects an SSH version 2 connection. If both SSH 1 and SSH 2 are selected, the IOLAN will attempt to make an SSH 2 connection first. If that connection fails, it will attempt to connect to the specified host using SSH 1. Default: Enabled
SSH2 Cipher Opt1-5	When the order of negotiation for the encryption method (ciphers) that the IOLAN will use for the SSH version 2 connection: Data Options: <ul style="list-style-type: none">• 3DES• Blowfish• AES-CBC• AES-CTR• AES-GCM• Arcfour• CAST• ChaCha20-Poly1305

RSA	When enabled, an authentication method used by SSH version 1 and 2. Use RSA authentication for the SSH session. Default: Enabled
DSA	When enabled, an authentication method used by SSH version 2. Use DSA authentication for the SSH session. Default: Enabled
Keyboard Authentication	When enabled, the user types in a password for authentication. Default: Enabled

SLIP Settings

The SLIP settings apply when the **User Service** is set to **SLIP**.

Local IP Address	The IPv4 address of the IOLAN end of the SLIP link. For routing to work you must enter an IP address in this field. Choose an address that is part of the same network or subnetwork as the remote end; for example, if the remote end is address 192.101.34.146, your local IP address can be 192.101.34.145. Do not use the IOLAN's (main) IP address in this field; if you do so, routing will not take place correctly.
Remote IP Address	The IPv4 address of the remote end of the SLIP link. Choose an address that is part of the same network or subnetwork as the IOLAN. If your user is authenticated by the IOLAN, this remote IP address will be overridden if you have set a Framed IP Address for the user. If your user is authenticated by RADIUS <i>and</i> the RADIUS parameter Framed-Address is set in the RADIUS file, the IOLAN will use the value in the RADIUS file in preference to the value configured here.
Subnet Mask	The network subnet mask. For example, 255.255.0.0. If your user is authenticated by RADIUS <i>and</i> the RADIUS parameter Framed-Netmask is set in the RADIUS file, the IOLAN will use the value in the RADIUS file in preference to the value configured here.
MTU	The Maximum Transmission Unit (MTU) parameter restricts the size of individual SLIP packets being sent by the IOLAN. Enter a value between 256 and 1006 bytes; for example, 512. The default value is 256 . If your user is authenticated by the IOLAN, this MTU value will be overridden when you have set a Framed MTU value for the user. If your user is authenticated by RADIUS <i>and</i> the RADIUS parameter Framed-MTU is set in the RADIUS file, the IOLAN will use the value in the RADIUS file in preference to the value configured here. Default: 256

Routing	<p>Determine the routing mode (RIP, Routing Information Protocol) used on the SLIP interface as one of the following options:</p> <ul style="list-style-type: none"> • None—Disables RIP over the SLIP interface. • Send—Sends RIP over the SLIP interface. • Listen—Listens for RIP over the SLIP interface. • Send and Listen—Sends RIP and listens for RIP over the SLIP interface. <p>This is the same function as the Framed-Routing attribute for RADIUS authenticated users.</p> <p>Default: None</p>
VJ Compression	<p>When enabled, Van Jacobson compression is used on this link. When enabled, C-SLIP, or compressed SLIP, is used. When disabled, plain SLIP is used. C-SLIP greatly improves the performance of interactive traffic, such as Telnet or Rlogin.</p> <p>If your user is authenticated by the IOLAN, this VJ compression value will be overridden if you have set a Framed Compression value for a user. If your user is authenticated by RADIUS <i>and</i> the RADIUS parameter Framed-Compression is set in the RADIUS file, the IOLAN will use the value in the RADIUS file in preference to the value configured here.</p> <p>Default: Enabled</p>

PPP Settings

The PPP settings apply when the **User Service** is set to **PPP**.

IPv4 Local IP Address	<p>The IPv4 IP address of the IOLAN end of the PPP link. For routing to work, you must enter a local IP address. Choose an address that is part of the same network or subnetwork as the remote end; for example, if the remote end is address 192.101.34.146, your local IP address can be 192.101.34.145. Do not use the IOLAN's (main) IP address in this field; if you do so, routing will not take place correctly.</p>
IPv4 Remote IP Address	<p>The IPv4 IP address of the remote end of the PPP link. Choose an address that is part of the same network or subnetwork as the IOLAN. If you set the PPP parameter IP Address Negotiation to On, the IOLAN will ignore the remote IP address value you enter here and will allow the remote end to specify its IP address. If your user is authenticated by RADIUS <i>and</i> the RADIUS parameter Framed-Address is set in the RADIUS file, the IOLAN will use the value in the RADIUS file in preference to the value configured here. The exception to this rule is a Framed-Address value in the RADIUS file of 255.255.255.254; this value allows the IOLAN to use the remote IP address value configured here.</p>
IPv4 Subnet Mask	<p>The network subnet mask. For example, 255.255.0.0. If your user is authenticated by RADIUS <i>and</i> the RADIUS parameter Framed-Netmask is set in the RADIUS file, the IOLAN will use the value in the RADIUS file in preference to the value configured here.</p>

IPv6 Local Interface Identifier	<p>The local IPv6 interface identifier of the IOLAN end of the PPP link. For routing to work, you must enter a local IP address. Choose an address that is part of the same network or subnetwork as the remote end. Do not use the IOLAN's (main) IP address in this field; if you do so, routing will not take place correctly.</p> <p>Field Format: The first 64 bits of the Interface Identifier must be zero, therefore, ::abcd:abcd:abcd:abcd is the expected format.</p>
IPv6 Remote Interface Identifier	<p>The remote IPv6 interface identifier of the remote end of the PPP link. Choose an address that is part of the same network or subnetwork as the IOLAN. If you enable Negotiate IP Address Automatically, the IOLAN will ignore the remote IP address value you enter here and will allow the remote end to specify its IP address. If your user is authenticated by RADIUS <i>and</i> the RADIUS parameter Framed-Interface-ID is set in the RADIUS file, the IOLAN will use the value in the RADIUS file in preference to the value configured here.</p> <p>Field Format: The first 64 bits of the Interface Identifier must be zero, therefore, ::abcd:abcd:abcd:abcd is the expected format.</p>
ACCM	<p>Specify the ACCM (Asynchronous Control Character Map) characters that should be escaped from the data stream.</p> <p>Field Format: This is entered as a 32-bit hexadecimal number with each bit specifying whether or not the corresponding character should be escaped. The bits are specified as the most significant bit first and are numbered 31-0. Thus if bit 17 is set, the 17th character should be escaped, that is, 0x11 (XON). The value 000a0000 will cause the control characters 0x11 (XON) and 0x13 (XOFF) to be escaped on the link, thus allowing the use of XON/XOFF (software) flow control. If you have selected Soft Flow Control on the Serial Port, you must enter a value of at least 000a0000 for the ACCM.</p> <p>Default: 00000000, which means no characters will be escaped</p>
MRU	<p>The Maximum Receive Unit (MRU) parameter specifies the maximum size of PPP packets that the IOLAN's port will accept. If your user is authenticated by the IOLAN, the MRU value will be overridden if you have set a MTU value for the user. If your user is authenticated by RADIUS <i>and</i> the RADIUS parameter Framed-MTU is set in the RADIUS file, the IOLAN will use the value in the RADIUS file in preference to the value configured here.</p> <p>Range: 64-1500 bytes</p> <p>Default: 1500</p>

Authentication	<p>The type of authentication that will be done on the link. You can use PAP or CHAP (MD5-CHAP, MS-CHAPv1 and MS-CHAPv2) to authenticate a user or client on the IOLAN. When setting either PAP and CHAP, make sure the IOLAN and the PPP peer, have the same setting. For example, if the IOLAN is set to PAP, but the remote end is set to CHAP, the connection will be refused.</p> <p>Data Options:</p> <p>None—no authentication will be performed.</p> <p>PAP—is a one time challenge of a client/device requiring that it respond with a valid username and password. A timer operates during which successful authentication must take place. If the timer expires before the remote end has been authenticated successfully, the link will be terminated.</p> <p>CHAP—challenges a client/device at regular intervals to validate itself with a username and a response, based on a hash of the secret (password). A timer operates during which successful authentication must take place. If the timer expires before the remote end has been authenticated successfully, the link will be terminated. MD5-CHAP and Microsoft MS-CHAPv1/MS-CHAPv2 are supported. The IOLAN will attempt MS-CHAPv2 with MPPC compression, but will negotiate to the variation of CHAP, compression and encryption that the remote peer wants to use.</p> <p>Default: CHAP</p>
User	<p>Complete this field only if you have specified PAP or CHAP (security protocols) in the Authentication field, <i>and</i></p> <ul style="list-style-type: none"> • you wish to dedicate this line to a single remote user, who will be authenticated by the IOLAN, <i>or</i> • you are using the IOLAN as a router (back-to-back with another IOLAN). <p>When Connect is set to Dial Out or both Dial In/Dial Out are enabled, the User is the name the remote device will use to authenticate a port on this IOLAN. The remote device will only authenticate your IOLAN's port when PAP or CHAP are operating. You can enter a maximum of sixteen alphanumeric characters; for example, tracy201. When connecting together two networks, enter a dummy user name; for example, DS_HQ.</p> <p>Note If you want a reasonable level of security, the user name and password should not be similar to a user name or password used regularly to login to the IOLAN. External authentication can not be used for this user.</p> <p>Field Format: You can enter a maximum of 254 alphanumeric characters</p>
Password	<p>Complete this field only if you have specified PAP or CHAP (security protocols) in the Security field and:</p> <ul style="list-style-type: none"> • you wish to dedicate this serial port to a single remote user, who will be authenticated by the IOLAN, <i>or</i> • you are using the IOLAN as a router (back-to-back with another IOLAN) <p>Password means the following:</p> <ul style="list-style-type: none"> • When PAP is specified, this is the password the remote device will use to authenticate the port on this IOLAN. • When CHAP is specified, this is the secret (password) known to both ends of the link upon which responses to challenges shall be based. <p>Field Format: You can enter a maximum of 16 alphanumeric characters.</p>

Remote User	<p>Complete this field only if you have specified PAP or CHAP (security protocols) in the Security field, <i>and</i></p> <ul style="list-style-type: none"> • you wish to dedicate this line to a single remote user, who will be authenticated by the IOLAN, <i>or</i> • you are using the IOLAN as a router (back-to-back with another IOLAN) <p>When Dial In or Dial In/Dial Out is enabled, the Remote User is the name the IOLAN will use to authenticate the port on the remote device. Your IOLAN will only authenticate the port on the remote device when PAP or CHAP are operating. When connecting together two networks, enter a dummy user name; for example, DS_SALES.</p> <p>Note: If you want a reasonable level of security, the user name and password should not be similar to a user name or password used regularly to login to the IOLAN. This option does not work with external authentication.</p> <p>Field Format: You can enter a maximum of 254 alphanumeric characters.</p>
Remote Password	<p>Complete this field only if you have specified PAP or CHAP (security protocols) in the Security field, <i>and</i></p> <ul style="list-style-type: none"> • you wish to dedicate this serial port to a single remote user, and this user will be authenticated by the IOLAN, <i>or</i> • you are using the IOLAN as a router (back-to-back with another IOLAN) <p>Remote password means the following:</p> <ul style="list-style-type: none"> • When PAP is specified, this is the password the IOLAN will use to authenticate the remote device. • When CHAP is specified, this is the secret (password) known to both ends of the link upon which responses to challenges will be based. <p>Remote Password is the opposite of the parameter Password. Your IOLAN will only authenticate the remote device when PAP or CHAP is operating.</p> <p>Field Format: You can enter a maximum of 16 alphanumeric characters.</p>
Routing	<p>Determines the routing mode (RIP, Routing Information Protocol) used on the PPP interface. This is the same function as the Framed-Routing attribute for RADIUS authenticated users.</p> <p>Data Options:</p> <ul style="list-style-type: none"> • None—Disables RIP over the PPP interface. • Send—Sends RIP over the PPP interface. • Listen—Listens for RIP over the PPP interface. • Send and Listen—Sends RIP and listens for RIP over the PPP interface. <p>Default: None</p>
Configure Req. Timeout	<p>The maximum time, in seconds, that LCP (Link Control Protocol) will wait before it considers a <code>configure request</code> packet to have been lost.</p> <p>Range: 1-255</p> <p>Default: 3 seconds</p>
Configure Req. Retries	<p>The maximum number of times a <code>configure request</code> packet will be re-sent before the link is terminated.</p> <p>Range: 0-255</p> <p>Default: 10 seconds</p>

Terminate Req. Timeout	<p>The maximum time, in seconds, that LCP (Link Control Protocol) will wait before it considers a <code>terminate request</code> packet to have been lost.</p> <p>Range: 1-255</p> <p>Default: 3 seconds</p>
Terminate Req. Retries	<p>The maximum number of times a <code>terminate request</code> packet will be re-sent before the link is terminated.</p> <p>Range: 0-255</p> <p>Default: 2 seconds</p>
Configure NAK Retries	<p>The maximum number of times a <code>configure NAK</code> packet will be re-sent before the link is terminated.</p> <p>Range: 0-255</p> <p>Default: 10 seconds</p>
Authentication Timeout	<p>The timeout, in minutes, during which successful PAP or CHAP authentication must take place (when PAP or CHAP are specified). If the timer expires before the remote end has been authenticated successfully, the link will be terminated.</p> <p>Range: 1-255</p> <p>Default: 1 minute</p>
Roaming Callback	<p>A user can enter a telephone number that the IOLAN will use to callback him/her. This feature is particularly useful for a mobile user. Roaming callback can only work when the User Enable Callback parameter is enabled. Enable Roaming Callback therefore overrides (fixed) User Enable Callback. To use Enable Roaming Callback, the remote end must be a Microsoft Windows OS that supports Microsoft's Callback Control Protocol (CBCP). The user is allowed 30 seconds to enter a telephone number after which the IOLAN ends the call.</p> <p>Default: Disabled</p>
Challenge Interval	<p>The interval, in minutes, for which the IOLAN will issue a CHAP re-challenge to the remote end. During CHAP authentication, an initial CHAP challenge takes place, and is unrelated to CHAP re-challenges. The initial challenge takes place even if re-challenges are disabled. Some PPP client software does <i>not</i> work with CHAP re-challenges, so you might want to leave the parameter disabled in the IOLAN.</p> <p>Range: 0-255</p> <p>Default: 0 (zero), meaning CHAP re-challenge is disabled</p>
Address/Control Compression	<p>This determines whether compression of the PPP Address and Control fields take place on the link. For most applications this should be enabled.</p> <p>Default: Enabled</p>
Protocol Compression	<p>This determines whether compression of the PPP Protocol field takes place on this link.</p> <p>Default: Enabled</p>

VJ Compression	<p>When enabled, Van Jacobson Compression is used on this link. If your user is authenticated by the IOLAN, this VJ compression value will be overridden if you have enabled the User, Enable VJ Compression parameter. If the user is authenticated by RADIUS <i>and</i> the RADIUS parameter Framed-Compression is set in the RADIUS file, the IOLAN will use the value in the RADIUS file in preference to the value configured here.</p> <p>Default: Enabled</p>
Magic Negotiation	<p>Determines if a line is looping back. If enabled (On), random numbers are sent on the link. The random numbers should be different, unless the link loops back.</p> <p>Default: Disabled</p>
IP Address Negotiation	<p>Specifies whether or not IP address negotiation will take place. IP address negotiation is where the IOLAN allows the remote end to specify its IP address. When On, the IP address specified by the remote end will be used in preference to the Remote IP Address set for a Serial Port. When Off, the Remote IP Address set for the Serial Port will be used.</p> <p>Default: Disabled</p>
Dynamic DNS Button	<p>Launches the Dynamic DNS window when IP Address Negotiation is enabled, which can then update the DNS server with the IP address that is negotiated and accepted for the PPP session.</p>

Printer Parameters

MAP CR to CR/LF	<p>Defines the default end-of-line terminator as CR/LF (ASCII carriage-return line-feed) when enabled.</p> <p>Default: Disabled</p>
------------------------	--

Printer Advanced Parameters

Session Strings	<p>Controls the sending of ASCII strings to serial device at session start as follows;</p> <ul style="list-style-type: none"> • Send at Start—If configured, this string will be sent to the serial device on power-up of the IOLAN, or when a kill line command is issued on this serial port. If the "monitor DSR" or "monitor DCD" options are set, the string will also be sent when the monitored signal is raised. • Range: 0-127 alpha-numeric characters • Range: hexadecimal 0-FF • Delay after Send - If configured, will inset a delay after the string is sent to the device. This delay can be used to provide the serial device with time to process the string before the session is initiated. <p>Default: 10 ms</p>
------------------------	---

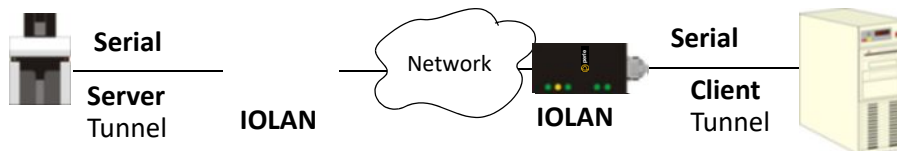
Serial Tunneling Profile

The Serial Tunneling profile allows two IOLANs to be connected back-to-back over the network to establish a virtual link between two serial ports based on RFC 2217.

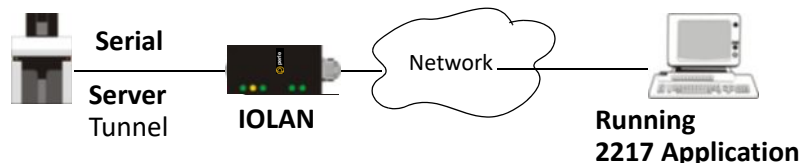
The serial device that initiates the connection is the **Tunnel Client** and the destination is the **Tunnel Server**, although once the serial communication tunnel has been successfully established, communication can go both ways.



A more detailed implementation of the Serial Tunneling profile is as follows:



The **Server Tunnel** will also support Telnet Com Port Control protocol as detailed in RFC 2217.



The IOLAN serial port signals will also follow the signals on the other serial port. If one serial port receives DSR then it will raise DTR on the other serial port. If one serial port receives CTS then it will raise RTS on the other serial port. The CD signal is ignored.

Serial Tunneling General Parameters

Act as Tunnel Server The IOLAN will listen for an incoming connection request on the specified **Internet Address** on the specified **TCP Port**.
Default: Enabled

Listen for connection on TCP Port The TCP port that the IOLAN will listen for incoming connection on.
Default: 10000+serial port number; so serial port 5 is 10005.

Act as Tunnel Client The IOLAN will initiate the connection the Tunnel Server.
Default: Disabled

Establish connection to Host Name A preconfigured host name that is associated with the IP address of the Tunnel Server.

Establish connection to TCP Port	The TCP port that the IOLAN will use to connect to the Tunnel Server. Default: 10000+serial port number; so serial port 1 is 10001.
HTTP Tunnel	Specify the HTTP tunnel to be used for this connection.
Enable TCP Keepalive	Enables a per-connection TCP keep-alive feature. After the configured number of seconds, the connection will send a gratuitous ACK to the network peer, thus either ensuring the connection stays active OR causing a dropped connection condition to be recognized. This parameter needs to be used in conjunction with Monitor Connection Status Interval parameter found in the Serial, Advanced, Advanced Settings tab. The interval specifies the inactivity period before "testing" the connection. Default: Disabled

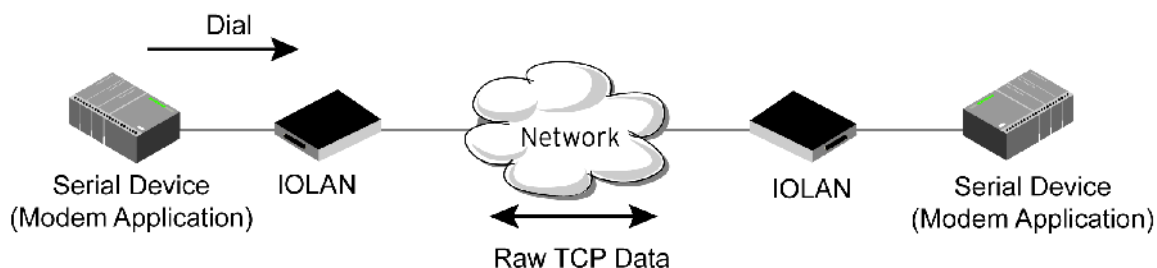
Serial Tunneling Advanced Parameters

Break Length	When the IOLAN receives a command from its peer to issue a break signal, this parameter defines the length of time the break condition will be asserted on the serial port Default: 1000ms (1 second)
Delay After Break	This parameter defines the delay between the termination of a break condition and the time data will be sent out the serial port. Default: 0ms (no delay).
Session Strings	Controls the sending of ASCII strings to serial devices at session start and session termination as follows; <ul style="list-style-type: none"> • Send at Start—If configured, this string will be sent to the serial device on power-up of the IOLAN or when a kill line command is issued on this serial port. If the "monitor DSR" or "monitor DCD" options are set, the string will also be sent when the monitored signal is raised. • Range: 0-127 alpha-numeric characters • Range: hexadecimal 0-FF • Send at End—If configured, this string will be sent to the serial device when the TCP session on the LAN is terminated. If multi-host is configured, this string will only be sent in listen mode to the serial device when all multi-host connections are terminated. • Range: 0-127 alpha-numeric characters • Range: hexadecimal 0-FF • Delay after Send—If configured, will insert a delay after the string is sent to the device. This delay can be used to provide the serial device with time to process the string before the session is initiated or terminated. Default: 10 ms

Virtual Modem Profile

Virtual Modem (Vmodem) is a feature of the IOLAN that provides a modem interface to a serial device. It will respond to AT commands and provide signals in the same way that a serially attached modem would. This feature is typically used when you are replacing dial-up modems with the IOLAN in order to provide Ethernet network connectivity.

The serial port will behave in exactly the same fashion as it would if it were connected to a modem. Using AT commands, it can configure the modem and then issue a dial-out request (ATDT). The IOLAN will then translate the dial request into a TCP connection and data will begin to flow in both directions. The connection can be terminated by “hanging” up the phone line. You can also manually start a connection by typing `ATD<ip_address>,<port_number>` and end the connection by typing `+++ATH`. The *ip_address* can be in IPv4 or IPv6 formats and is the IP address of the receiver. For example, `ATD123.34.23.43,10001` or you can use `ATD12303402304310001`, without any punctuation (although you do need to add zeros where there are not three digits present, so that the IP address is 12 digits long).



Virtual Modem General Parameters

Listen on TCP Port	The IOLAN TCP port that the IOLAN will listen on. Default: 10000 + serial port number (for example, serial port 12 defaults to 10012)
Connect Automatically At Startup	When enabled, automatically establishes the virtual modem connection when the serial port becomes active. Default: Enabled
Host Name	The preconfigured target host name.
TCP Port	The port number the target host is listening on for messages. Default: 0 (zero)
HTTP Tunnel	Specify the HTTP tunnel to be used for this connection.
Connect Manually Via AT Command	When enabled, the virtual modem requires an AT command before it establishes a connection. Specify this option when your modem application sends a phone number or other AT command to a modem. The serial device can supply an IP address directly or it can provide a phone number that will be translated into an IP address by the IOLAN using the mapping table. Default: Disabled

Phone Number to Host Mapping Button	When your modem application provides a phone number in an AT command string, you can map that phone number to the destination host.
Send Connection Status As	When enabled, the connection success/failure indication strings are sent to the connected device, otherwise these indications are suppressed. This option also determines the format of the connection status results that are generated by the virtual modem. Default: Enabled
Verbose Strings	When enabled, the connection status is sent by text strings to the connected device. Default: Disabled
Success String	String that is sent to the serial device when a connection succeeds. Default: CONNECT <speed>, for example, CONNECT 9600
Failure String	String that is sent to the serial device when a connection fails. Default: NO CARRIER
Numeric Codes	When enabled, the connection status is sent to the connected device using the following numeric codes: <ul style="list-style-type: none"> • 0 OK • 1 CONNECTED • 2 RING • 3 NO CARRIER • 4 ERROR • 6 INTERFACE DOWN • 7 CONNECTION REFUSED • 8 NO LISTENER Default: Enabled

Virtual Modem Advanced Parameters

Echo characters in command mode	When enabled, echoes back characters that are typed in (equivalent to ATE0/ATE1 commands). Default: Disabled
DTR Signal Always On	Specify this option to make the DTR signal always act as a DTR signal. Default: Enabled
DTR Signal Acts as DCD	Specify this option to make the DTR signal always act as a DCD signal. Default: Disabled
DTR Signal Acts as RI	Specify this option to make the DTR signal always act as a RI signal. Default: Disabled
RTS Signal Always On	Specify this option to make the RTS signal always act as a RTS signal. Default: Enabled

RTS Signal Acts as DCD	Specify this option to make the RTS signal always act as a DCD signal. Default: Disabled
RTS Signal Acts as RI	Specify this option to make the RTS signal always act as a RI signal. Default: Disabled
DCD Signal Always On	When you configure the DTR or RTS signal pin to act as a DCD signal, enable this option to make the DCD signal always stay on. Default: Enabled
DCD Signal On when host connection established	When you configure the DTR or RTS signal pin to act as a DCD signal, enable this option to make the DCD signal active only during active communication. Default: Disabled
Additional modem initialization	You can specify additional virtual modem commands that will affect how virtual modem starts. The following commands are supported: ATQn, ATVn, ATEn, +++ATH, ATA, ATIO, ATIS, ATSO, AT&Z1, AT&Sn, AT&Rn, AT&Cn, AT&F, ATS2, ATS12, ATO (ATD with no phone number), and ATDS1.
Enable Message of the Day (MOTD)	When enabled, displays the Message of the Day (MOTD) when a successful virtual modem connection is made. Default: Disabled
Enable TCP Keepalive	Enables a per-connection TCP keepalive feature. After the configured number of seconds, the connection will send a gratuitous ACK to the network peer, thus either ensuring the connection stays active OR causing a dropped connection condition to be recognized. This parameter needs to be used in conjunction with Monitor Connection Status Interval parameter found in the Serial, Advanced, Advanced Settings tab. The interval specifies the inactivity period before "testing" the connection. Default: Disabled
AT Command Response Delay	The amount of time, in milliseconds, before an AT response is sent to the requesting device. Default: 250 ms
Session Strings	Controls the sending of ASCII strings to serial devices at session start as follows; <ul style="list-style-type: none"> • Send at Start—If configured, this string will be sent to the serial device on power-up of the IOLAN or when a kill line command is issued on this serial port. If the “monitor DSR” or “monitor DCD” options are set, the string will also be sent when the monitored signal is raised. • Range: 0-127 alpha-numeric characters • Range: hex 0-FF • Delay after Send—If configured, will inset a delay after the string is sent to the device. This delay can be used to provide the serial device with time to process the string before the session is initiated or terminated. Default: 10 ms

Phone Number to Host Mapping

If your modem application dials using a phone number, you can add an entry in the Phone Number to Host Mapping window that can be accessed by all serial ports configured as Virtual Modem. You need to

enter the phone number sent by your modem application and the IOLAN IP address and TCP Port that will be receiving the “call”. The IOLAN supports up to 48 entries.

Virtual Modem Phone Number Entry

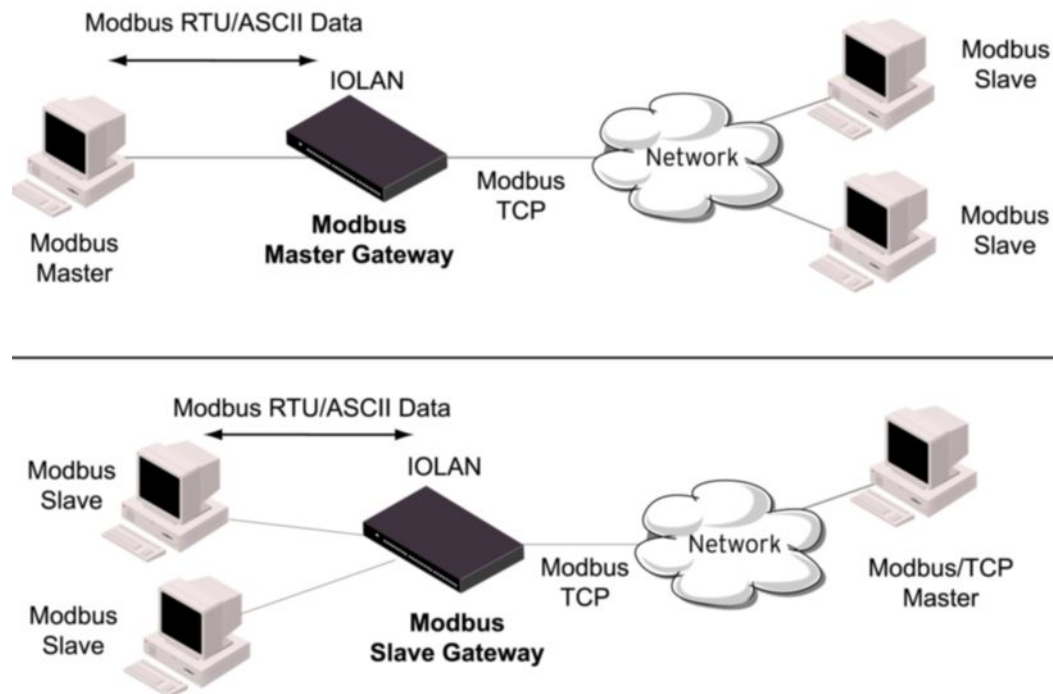
Create an entry in the Phone Number to Host Mapping window.

Phone Number	Specify the phone number your modem application sends to the modem. Note: The IOLAN does not validate the phone number, so it must be entered in the exact way the application will send it. For example, if you enter 555-1212 in this table and the application sends 5551212, the IOLAN will not match the two numbers. Spaces will be ignored.
Host IP Address	Specify the IP address of the IOLAN that is receiving the virtual modem connection. Field Format: IPv4 or IPv6 address
Host Name	Specify the host name (from the host table) of the IOLAN that is receiving the virtual modem connection. See Host Table or more information.
TCP Port	Specify the TCP Port on the IOLAN that is set to receive the virtual modem connection. Default: 0
HTTP Tunnel	Specify the HTTP tunnel to be used for this connection.

Modbus Gateway Profile

The Modbus Gateway profile configures a serial port to act as a Modbus Master Gateway or a Modbus Slave Gateway.

Modbus General Parameters



Modbus	<p>Specify how the Modbus Gateway is defined on the serial port.</p> <p>Data Options:</p> <ul style="list-style-type: none">• Modbus Master—Typically, the Modbus Master is connected to the Serial Port and is communicating to Modbus Slaves on the network.• Modbus Slave—Typically, the Modbus Master is accessing the IOLAN through the network to communicated to Modbus Slaves connected to the IOLAN's Serial Ports. <p>Default: Modbus Master Gateway</p>
Destination Slave IP Mappings Button	<p>Select this button to launch the Destination Slave IP Settings window, where you can configure the TCP/Ethernet Modbus Slaves that the Modbus Master on the Serial Port will communicate with.</p>
Advanced Slave Settings Button	<p>Select this button to configure global Modbus Slave settings.</p>
UID Range	<p>You can specify a range of UIDs (1-247), in addition to individual UIDs.</p> <p>Field Format: Comma delimited; for example, 2-35, 50, 100-103</p>
IP Address	<p>Set the IP address to be used for this serial port when using IP Aliasing feature.</p>

Modbus/RTU	Select this option when the Modbus/RTU protocol is being used for communication between the Modbus Master and Slave. Default: Enabled
Modbus/ASCII	Select this option when Modbus/ASCII protocol is being used for communication between the Modbus Master and Slave. Default: Disabled
Append CR/LF	When Modbus/ASCII is selected, adds a CR/LF to the end of the transmission; most Modbus devices require this option. Default: Enabled

Modbus Advanced Parameters

Idle Timeout	Use this timer to close a connection because of inactivity. When the Idle Timeout expires, the IOLAN will end the connection. Range: 0-4294967 seconds (about 49 days) Default: 0 (zero), which does not timeout, so the connection is permanently open.
Enable Modbus Exceptions	When enabled, an exception message is generated and sent to the initiating Modbus device when any of the following conditions are encountered: there is an invalid UID, the UID is not configured in the Gateway, there is no free network connection, there is an invalid message, or the target device is not answering the connection attempt. Default: Enabled
Character Timeout	Used in conjunction with the Modbus RTU protocol, specifies how long to wait, in milliseconds, after a character to determine the end of frame. Range: 10-10000 Default: 30 ms
Message Timeout	Time to wait, in milliseconds, for a response message from a Modbus TCP or serial slave (depending if the Modbus Gateway is a Master Gateway or Slave Gateway, respectively) before sending a Modbus exception. Range: 10-10000 Default: 1000 ms
Session Strings	Controls the sending of ASCII strings to serial devices at session start as follows; <ul style="list-style-type: none"> • Send at Start—If configured, this string will be sent to the serial device on power-up of the IOLAN or when a kill line command is issued on this serial port. If the “monitor DSR” or “monitor DCD” options are set, the string will also be sent when the monitored signal is raised. • Range: 0-127 alpha-numeric characters • Range: hex 0-FF • Delay after Send—If configured, will inset a delay after the string is sent to the device. This delay can be used to provide the serial device with time to process the string before the session is initiated or terminated. Default: 10 ms

Adding/Editing Modbus Slave IP Parameters

UID Start	<p>When Destination is set to Host and you have sequential Modbus Slave IP addresses (for example, 10.10.10.1, 10.10.10.2, 10.10.10.3, etc.), you can specify a UID range (not supported with IPv6 addresses) and the IOLAN will automatically increment the last digit of the configured IP address. Therefore, you can specify a UID range of 1-100, and the IOLAN will route Master Modbus messages to all Modbus Slaves with IP addresses of 10.10.10.1 - 10.10.10.100.</p> <p>Range: 1-247 Default: 0 (zero)</p>
UID End	<p>When Destination is set to Host and you have sequential Modbus Slave IP addresses (for example, 10.10.10.1, 10.10.10.2, 10.10.10.3, etc.), you can specify a UID range (not supported with IPv6 addresses) and the IOLAN will automatically increment the last digit of the configured IP address. Therefore, you can specify a UID range of 1-100, and the IOLAN will route Master Modbus messages to all Modbus Slaves with IP addresses of 10.10.10.1 - 10.10.10.100.</p> <p>Range: 1-247 Default: 0 (zero)</p>
Type	<p>Specify the configuration of the Modbus Slaves on the network.</p> <p>Data Options:</p> <ul style="list-style-type: none">• Host—The IP address is used for the first UID specified in the range. The last octet in the IPv4 address is then incremented for subsequent UID's in that range.• Gateway—The Modbus Master Gateway will use the same IP address when connecting to all the remote Modbus slaves in the specified UID range. <p>Default: Host</p>
Start IP Address	<p>The IP address of the TCP/Ethernet Modbus Slave.</p> <p>Field Format: IPv4 or IPv6 address</p>
End IP Address	<p>Displays the ending IP address of the TCP/Ethernet Modbus Slaves, based on the Start IP address and the UID range (not supported for IPv6 addresses).</p> <p>Field Format: IPv4 address</p>
HTTP Tunnel	<p>Specify the HTTP tunnel to be used for this connection.</p>
Protocol	<p>Specify the protocol that is used between the Modbus Master and Modbus Slave(s).</p> <p>Data Options: TCP or UDP Default: TCP</p>
UDP/TCP Port	<p>The destination port of the remote Modbus TCP Slave that the IOLAN will connect to.</p> <p>Range: 0-65535 Default: 502</p>

Modbus Slave Advanced Parameters

TCP/UDP Port	The network port number that the Slave Gateway will listen on for both TCP and UDP messages. Default: 502
Next Request Delay	A delay, in milliseconds, to allow serial slave(s) to re-enable receivers before issuing next Modbus Master request. Range: 0-1000 Default: 50 ms
Enable Serial Modbus Broadcasts	When enabled, a UID of 0 (zero) indicates that the message will be broadcast to all Modbus Slaves. Default: Disabled
Request Queuing	When enabled, allows multiple, simultaneous messages to be queued and processed in order of reception. Default: Enabled
Embedded	When this option is selected, the address of the slave Modbus device is embedded in the message header. Default: Enabled
Remapped	Used for single device/port operation. Older Modbus devices may not include a UID in their transmission header. When this option is selected, you can specify the UID that will be inserted into the message header for the Modbus slave device. This feature supersedes the Broadcast feature. Default: Disabled
Remap UID	Specify the UID that will be inserted into the message header for the Slave Modbus serial device. Range: 1-247 Default: 1
Enable IP Aliasing	The ability to access a serial device connected to the serial port by an IP address (or host name that can be resolved to the Internet Address in a DNS network) instead of the IOLAN's IP address and port number. Default: Disabled Remap: UID
Enable SSL/TLS using global settings	When enabled, Modbus Slave Gateway messages to remote TCP Modbus Masters are encrypted via SSL/TLS. Default: Disabled

Power Management Profile

The Power Management profile applies when there is a Perle Remote Power Switch (RPS) connected to the serial port. This profile is used to configure the RPS. See [RPS Control](#) for information on how to actively management the RPS.

The Power Management profile configures a serial port to communicate with a Remote Power Switch's (RPS) administration port. This allows network access to the RPS and permits access to statistics and control of the RPS's power plugs.

Power Management General Parameters

RPS Name	Specify a name for the RPS.
RPS Model	Specify the RPS model. Data Options: RSP820, RPS830, RPS1620, RPS1630 Default: RSP820
Edit button	Highlight a plug and then select the Edit button to configure the plug.

Power Management Advanced Parameters

Session Strings	Controls the sending of ASCII strings to serial devices at session start as follows; <ul style="list-style-type: none">• Send at Start—If configured, this string will be sent to the serial device on power-up of the IOLAN or when a kill line command is issued on this serial port. If the “monitor DSR” or “monitor DCD” options are set, the string will also be sent when the monitored signal is raised.• Range: 0-127 alpha-numeric characters• Range: hex 0-FF• Delay after Send—If configured, will inset a delay after the string is sent to the device. This delay can be used to provide the serial device with time to process the string before the session is initiated or terminated. Default: 10 ms
------------------------	--

Editing Power Management Plug Settings

Name	Specify a name for the plug to make it easier to recognize and manage.
Power up Interval	Specify the amount of time, in seconds, that the RPS will wait before powering up a plug. This can be useful if you have peripherals that need to be started in a specific order. Data Options: .5, 1, 2, 5, 15, 30, 60, 120, 180, 300 Default: .5 seconds
Default State	Sets the default state of the plug. Data Options: On, Off Default: Off

Associated Port **When** a server or router has its console port connected to one of the serial ports on this IOLAN and that server/router is also powered by this RPS, the server/router serial port number should be entered here. This will give you direct access to some RPS commands when managing that server or router (using Telnet or SSH).

Monitoring Power Plugs

Monitor Host This is the host which is to be monitored via PINGs. If the host stops responding to the PINGs, the power on this plug will be cycled in an attempt to recover the host.

Default: None

Ping

- Interval -Specify the frequency (in minutes) at which the configured host will be PING'ed.

Default - 15 minutes

- Timeout - Specify the length of time (in seconds) to wait for a reply

Default - 60 seconds

- Retries - Specify the number of times to re-try the PING when the host does not reply. This is in addition to the original PING request.

Default - 2

Wait before cycling power Enables a delay before cycling the power on the plug. This delay allows for the sending of notification(s) of the impending power cycle. Notifications can be sent to a user on the console port of the host being monitored and/or via email. This gives system administrators the time to take appropriate action.

Default: Disabled

- **Delay**—Specify a delay (in minutes) before cycling the power on the plug.

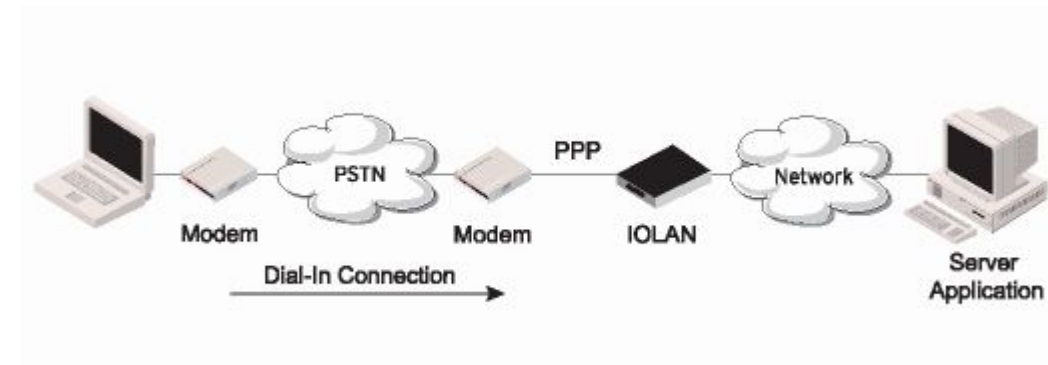
Default: 5 Minutes

Send Notification—Specify the desired notification to be sent advising of the impending power cycle.

- **By Email**—Send an email. Details configured in “Email Alert” tab.
- **To Serial Port**—Send a message to the serial port associated with this power plug. This is usually the console port on the host being monitored.

Remote Access (PPP) Profile

The **Remote Access (PPP)** profile configures a serial port to allow a remote user to establish a PPP connection to the IOLAN's serial port. This is typically used with a modem for dial-in or dial-out access to the network.



There are two options for PPP user authentication:

1. You can configure a specific user/password and a specific remote user/password per a serial port.
2. You can create a secrets file with multiple users and their passwords that will globally authenticate users on all serial ports.
3. You can use configure PPP authentication in the configuration or in the secrets file, but not both.
4. If you want to use a secrets file, you must download the secrets file to the IOLAN for CHAP or PAP authentication; the files must be downloaded to the IOLAN using the names `chap-secrets` and `pap-secrets`, respectively. The file can be downloaded to the IOLAN under the **Custom Files** option by selecting the **Download Other File**

parameter.

In the **Remote Access (PPP)** profile, you must also specify the **Authentication** option as **PAP** or **CHAP** on the **Authentication** tab, but must leave the **User**, **Password**, **Remote User**, and **Remote Password** fields blank.

An example of the CHAP secrets file follows:

```
# Secrets for authentication using CHAP
# client      server      secret                                acceptable local IP
addresses
  barney      fred        flintstone1234567890                192.168.43.1
  fred        barney      wilma                                192.168.43.2
```

An example of the PAP secret file follows:

```
# Secrets for authentication using PAP
# client      server      secret                                acceptable local IP
addresses
  barney      *          flintstone1234567890
  fred        *          wilma
```

Remote Access (PPP) General Parameters

IPv4 Local IP Address	The IPv4 IP address of the IOLAN end of the PPP link. For routing to work, you must enter a local IP address. Choose an address that is part of the same network or subnetwork as the remote end; for example, if the remote end is address 192.101.34.146, your local IP address can be 192.101.34.145. Do not use the IOLAN's (main) IP address in this field; if you do so, routing will not take place correctly.
IPv4 Remote IP Address	The IPv4 IP address of the remote end of the PPP link. Choose an address that is part of the same network or subnetwork as the IOLAN. If you set the PPP parameter IP Address Negotiation to On, the IOLAN will ignore the remote IP address value you enter here and will allow the remote end to specify its IP address. If your user is authenticated by RADIUS <i>and</i> the RADIUS parameter Framed-Address is set in the RADIUS file, the IOLAN will use the value in the RADIUS file in preference to the value configured here. The exception to this rule is a Framed-Address value in the RADIUS file of 255.255.255.254 ; this value allows the IOLAN to use the remote IP address value configured here.
IPv4 Subnet Mask	The network subnet mask. For example, 255.255.0.0. If your user is authenticated by RADIUS and the RADIUS parameter Framed-Netmask is set in the RADIUS file, the IOLAN will use the value in the RADIUS file in preference to the value configured here.
Enable IP Address Negotiation	Specifies whether or not IP address negotiation will take place. IP address negotiation is where the IOLAN allows the remote end to specify its IP address. When On , the IP address specified by the remote end will be used in preference to the Remote IP Address set for a Serial Port . When Off , the Remote IP Address set for the Serial Port will be used. Default: Disabled
Dynamic DNS Button	Launches the Dynamic DNS window when IP Address Negotiation is enabled, which can then update the DNS server with the IP address that is negotiated and accepted for the PPP session.
IPv6 Local Interface Identifier	The local IPv6 interface identifier of the IOLAN end of the PPP link. For routing to work, you must enter a local IP address. Choose an address that is part of the same network or subnetwork as the remote end. Do not use the IOLAN's (main) IP address in this field; if you do so, routing will not take place correctly. Field Format: The first 64 bits of the Interface Identifier must be zero, therefore, ::abcd:abcd:abcd:abcd is the expected format.
IPv6 Remote Interface Identifier	The remote IPv6 interface identifier of the remote end of the PPP link. Choose an address that is part of the same network or subnetwork as the IOLAN. If you enable Negotiate IP Address Automatically , the IOLAN will ignore the remote IP address value you enter here and will allow the remote end to specify its IP address. If your user is authenticated by RADIUS <i>and</i> the RADIUS parameter Framed-Interface-ID is set in the RADIUS file, the IOLAN will use the value in the RADIUS file in preference to the value configured here. Field Format: The first 64 bits of the Interface Identifier must be zero, therefore, ::abcd:abcd:abcd:abcd is the expected format.

IPv6 Global Network Prefix	You can optionally specify an IPv6 global network prefix that the IOLAN will advertise to the device at the other end of the PPP link. Default: 0:0:0:0
-----------------------------------	---

IPv6 Prefix Bits	Specify the prefix bits for the IPv6 global network prefix. Default: 64
-------------------------	---

Dynamic DNS

Dynamic DNS can be enabled and configured on a serial port level. If you enable Dynamic DNS and leave the parameters blank, the Dynamic DNS system parameters will be used (**Network, Advanced, Dynamic DNS** tab).

Dynamic DNS General ParametersAuthentication Parameters

Enable Dynamic DNS for this Serial Port	Enables/disables the ability to register a new IP address with the DNS server. Default: Disabled
--	--

Host	Specify the host name that will be updated with the PPP session's IP address on the DNS server.
-------------	---

User Name	Specify the user name used to access the DNS server.
------------------	--

Password	Specify the password used to access the DNS server.
-----------------	---

Account Settings Button	Select this button to configure the Dynamic DNS DynDNS.org account information.
--------------------------------	---

Authentication	The type of authentication that will be done on the link. You can use PAP or CHAP (MD5-CHAP, MS-CHAPv1 and MS-CHAPv2) to authenticate a user or client on the IOLAN. When setting either PAP and CHAP, make sure the IOLAN and the PPP peer, have the same setting. For example, if the IOLAN is set to PAP, but the remote end is set to CHAP, the connection will be refused.
-----------------------	---

Data Options:

None — no authentication will be performed.

PAP — is a one time challenge of a client/device requiring that it respond with a valid username and password. A timer operates during which successful authentication must take place. If the timer expires before the remote end has been authenticated successfully, the link will be terminated.

CHAP — challenges a client/device at regular intervals to validate itself with a username and a response, based on a hash of the secret (password). A timer operates during which successful authentication must take place. If the timer expires before the remote end has been authenticated successfully, the link will be terminated. MD5-CHAP and Microsoft MS-CHAPv1/MS-CHAPv2 are supported. The IOLAN will attempt MS-CHAPv2 with MPPC compression, but will negotiate to the variation of CHAP, compression and encryption that the remote peer wants to use.

Default: CHAP

User	<p>Complete this field only if you have specified PAP or CHAP (security protocols) in the Authentication field, <i>and</i></p> <ul style="list-style-type: none"> • you wish to dedicate this line to a single remote user, who will be authenticated by the IOLAN, or • you are using the IOLAN as a router (back-to-back with another IOLAN). <p>When Connect is set to Dial Out or both Dial In/Dial Out are enabled, the User is the name the remote device will use to authenticate a port on this IOLAN. The remote device will only authenticate your IOLAN's port when PAP or CHAP are operating. You can enter a maximum of sixteen alphanumeric characters; for example, tracy201. When connecting together two networks, enter a dummy user name; for example, DS_HQ.</p> <p>Note: If you want a reasonable level of security, the user name and password should not be similar to a user name or password used regularly to login to the IOLAN. External authentication can not be used for this user.</p> <p>Field Format: You can enter a maximum of 254 alphanumeric characters.</p>
Password	<p>Complete this field only if you have specified PAP or CHAP (security protocols) in the Security field and:</p> <ul style="list-style-type: none"> • you wish to dedicate this serial port to a single remote user, who will be authenticated by the IOLAN, or • you are using the IOLAN as a router (back-to-back with another IOLAN) <p>Password means the following:</p> <ul style="list-style-type: none"> • When PAP is specified, this is the password the remote device will use to authenticate the port on this IOLAN. • When CHAP is specified, this is the secret (password) known to both ends of the link upon which responses to challenges shall be based. <p>Field Format: You can enter a maximum of 16 alphanumeric characters.</p>
Remote User	<p>Complete this field only if you have specified PAP or CHAP (security protocols) in the Security field, <i>and</i></p> <ul style="list-style-type: none"> • you wish to dedicate this line to a single remote user, who will be authenticated by the IOLAN, or • you are using the IOLAN as a router (back-to-back with another IOLAN) <p>When Dial In or Dial In/Dial Out is enabled, the Remote User is the name the IOLAN will use to authenticate the port on the remote device. Your IOLAN will only authenticate the port on the remote device when PAP or CHAP are operating. When connecting together two networks, enter a dummy user name; for example, DS_SALES.</p> <p>Note If you want a reasonable level of security, the user name and password should not be similar to a user name or password used regularly to login to the IOLAN. This option does not work with external authentication.</p> <p>Field Format: You can enter a maximum of 254 alphanumeric characters.</p>

Remote Password	<p>Complete this field only if you have specified PAP or CHAP (security protocols) in the Security field, <i>and</i></p> <ul style="list-style-type: none"> • you wish to dedicate this serial port to a single remote user, and this user will be authenticated by the IOLAN, or • you are using the IOLAN as a router (back-to-back with another IOLAN) <p>Remote password means the following:</p> <ul style="list-style-type: none"> • When PAP is specified, this is the password the IOLAN will use to authenticate the remote device. • When CHAP is specified, this is the secret (password) known to both ends of the link upon which responses to challenges will be based. <p>Remote Password is the opposite of the parameter Password. Your IOLAN will only authenticate the remote device when PAP or CHAP is operating.</p> <p>Field Format: You can enter a maximum of 16 alphanumeric characters.</p>
Authentication Timeout	<p>The timeout, in minutes, during which successful PAP or CHAP authentication must take place (when PAP or CHAP are specified). If the timer expires before the remote end has been authenticated successfully, the link will be terminated.</p> <p>Range: 1-255</p> <p>Default: 1 minute</p>
CHAP Challenge Interval	<p>The interval, in minutes, for which the IOLAN will issue a CHAP re-challenge to the remote end. During CHAP authentication, an initial CHAP challenge takes place, and is unrelated to CHAP re-challenges. The initial challenge takes place even if re-challenges are disabled. Some PPP client software does <i>not</i> work with CHAP re-challenges, so you might want to leave the parameter disabled in the IOLAN.</p> <p>Range: 0-255</p> <p>Default: 0 (zero), meaning CHAP re-challenge is disabled</p>
Enable Roaming Callback	<p>A user can enter a telephone number that the IOLAN will use to callback him/her. This feature is particularly useful for a mobile user. Roaming callback can only work when the User Enable Callback parameter is enabled. Enable Roaming Callback therefore overrides (fixed) User Enable Callback. To use Enable Roaming Callback, the remote end must be a Microsoft Windows OS that supports Microsoft's Callback Control Protocol (CBCP). The user is allowed 30 seconds to enter a telephone number after which the IOLAN ends the call.</p> <p>Default: Disabled</p>

Remote Access (PPP) Advanced Tab

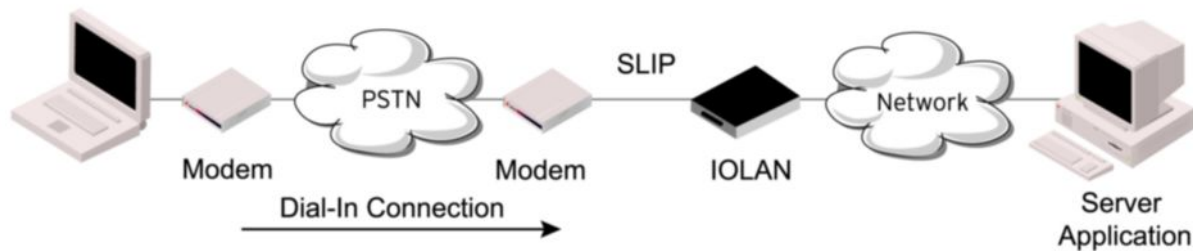
Routing	<p>Determines the routing mode (RIP, Routing Information Protocol) used on the PPP interface. This is the same function as the Framed-Routing attribute for RADIUS authenticated users.</p> <p>Data Options:</p> <ul style="list-style-type: none">• None—Disables RIP over the PPP interface.• Send—Sends RIP over the PPP interface.• Listen—Listens for RIP over the PPP interface.• Send and Listen—Sends RIP and listens for RIP over the PPP interface. <p>Default: None</p>
ACCM	<p>Specifies the ACCM (Asynchronous Control Character Map) characters that should be escaped from the data stream.</p> <p>Field Format: This is entered as a 32-bit hexadecimal number with each bit specifying whether or not the corresponding character should be escaped. The bits are specified as the most significant bit first and are numbered 31-0. Thus if bit 17 is set, the 17th character should be escaped, that is, 0x11 (XON). The value 000a0000 will cause the control characters 0x11 (XON) and 0x13 (XOFF) to be escaped on the link, thus allowing the use of XON/XOFF (software) flow control. If you have selected Soft Flow Control on the Serial Port, you must enter a value of at least 000a0000 for the ACCM.</p> <p>Default: 00000000, which means no characters will be escaped</p>
MRU	<p>The Maximum Receive Unit (MRU) parameter specifies the maximum size of PPP packets that the IOLAN's port will accept. If your user is authenticated by the IOLAN, the MRU value will be overridden if you have set a MTU value for the user. If your user is authenticated by RADIUS <i>and</i> the RADIUS parameter Framed-MTU is set in the RADIUS file, the IOLAN will use the value in the RADIUS file in preference to the value configured here.</p> <p>Range: 64-1500 bytes Default: 1500</p>
Configure Request Timeout	<p>The maximum time, in seconds, that LCP (Link Control Protocol) will wait before it considers a <code>configure request</code> packet to have been lost.</p> <p>Range: 1-255 Default: 3 seconds</p>
Configure Request Retries	<p>The maximum number of times a <code>configure request</code> packet will be re-sent before the link is terminated.</p> <p>Range: 0-255 Default: 10 seconds</p>
Terminate Request Timeout	<p>The maximum time, in seconds, that LCP (Link Control Protocol) will wait before it considers a <code>terminate request</code> packet to have been lost.</p> <p>Range: 1-255 Default: 3 seconds</p>

Terminate Request Retries	The maximum number of times a terminate request packet will be re-sent before the link is terminated. Range: 0-255 Default: 2 seconds
PPP echo request timeout	The maximum time, in seconds, between sending an echo request packet if no response is received from the remote host. Range: 0-255 Default: 30 seconds
PPP echo retry	The maximum number of times an echo request packet will be re-sent before the link is terminated. Range: 0-255 Default: 3
Configure NAK Retries	The maximum number of times a configure NAK packet will be re-sent before the link is terminated. Range: 0-255 Default: 10 seconds
Enable Address/Control Compression	This determines whether compression of the PPP Address and Control fields take place on the link. For most applications this should be enabled. Default: Enabled
Enable Protocol Compression	This determines whether compression of the PPP Protocol field takes place on this link. Default: Enabled
Enable VJ Compression	When enabled, Van Jacobson Compression is used on this link. If your user is authenticated by the IOLAN, this VJ compression value will be overridden if you have enabled the User, Enable VJ Compression parameter. If the user is authenticated by RADIUS <i>and</i> the RADIUS parameter Framed-Compression is set in the RADIUS file, the IOLAN will use the value in the RADIUS file in preference to the value configured here. Default: Enabled
Enable Magic Negotiation	Determines if a line is looping back. If enabled (On), random numbers are sent on the link. The random numbers should be different, unless the link loops back. Default: Disabled
Idle Timeout	Use this timer to close a connection because of inactivity. When the Idle Timeout expires, the IOLAN will end the connection. Range: 0-4294967 seconds (about 49 days) Default: 0 (zero), which does not timeout, so the connection is permanently open.
Direct Connect	Specify this option when a modem is not connected to this serial port. Default: Enabled
Dial In	If the device is remote and will be dialing in via modem or ISDN TA, enable this parameter. Default: Disabled

Dial Out	If you want the modem to dial a number when the serial port is started, enable this parameter. Default: Disabled
Dial In/Out	Enable this option when you want the serial port to do either of the following: <ul style="list-style-type: none">• accept a call from a modem or ISDN TA• dial a number when the serial port is started Default: Disabled
MS Direct Host	Specify this option when the serial port is connected to a Microsoft Guest device. Default: Enabled
MS Direct Guest	Enable this option when the serial port is connected to a Microsoft Host device. Default: Disabled
Dial Timeout	The number of seconds the IOLAN will wait to establish a connection to a remote modem. Range: 1-99 Default: 45 seconds
Dial Retry	The number of times the IOLAN will attempt to re-establish a connection with a remote modem. Range: 0-99 Default: 2
Modem	The name of the predefined modem that is used on this line.
Phone	The phone number to use when Dial Out is enabled.
Session Strings	Controls the sending of ASCII strings to serial device at session start as follows; <ul style="list-style-type: none">• Send at Start—If configured, this string will be sent to the serial device on power-up of the IOLAN, or when a kill line command is issued on this serial port. If the "monitor DSR" or "monitor DCD" options are set, the string will also be sent when the monitored signal is raised. Range: 0-127 alpha-numeric characters Range: hexadecimal 0-FF• Delay after Send - If configured, will inset a delay after the string is sent to the device. This delay can be used to provide the serial device with time to process the string before the session is initiated.• Range is 0-65535 ms Default: 10 ms

Remote Access (SLIP) Profile

The **Remote Access (SLIP)** profile configures a serial port to allow a remote user to establish a SLIP connection to the IOLAN's serial port. This is typically used with a modem for dial-in or dial-out access to the network.



Remote Access (SLIP) General Parameters

- Local IP Address** The IPv4 address of the IOLAN end of the SLIP link. For routing to work you must enter an IP address in this field. Choose an address that is part of the same network or subnetwork as the remote end; for example, if the remote end is address 192.101.34.146, your local IP address can be 192.101.34.145. Do not use the IOLAN's (main) IP address in this field; if you do so, routing will not take place correctly.
- Remote IP Address** The IPv4 address of the remote end of the SLIP link. Choose an address that is part of the same network or subnetwork as the IOLAN. If your user is authenticated by the IOLAN, this remote IP address will be overridden if you have set a **Framed IP Address** for the user. If your user is authenticated by RADIUS *and* the RADIUS parameter **Framed-Address** is set in the RADIUS file, the IOLAN will use the value in the RADIUS file in preference to the value configured here.
- Subnet Mask** The network subnet mask. For example, 255.255.0.0. If your user is authenticated by RADIUS *and* the RADIUS parameter **Framed-Netmask** is set in the RADIUS file, the IOLAN will use the value in the RADIUS file in preference to the value configured here.
- MTU** The Maximum Transmission Unit (MTU) parameter restricts the size of individual SLIP packets being sent by the IOLAN. Enter a value between 256 and 1006 bytes; for example, 512. The default value is **256**. If your user is authenticated by the IOLAN, this MTU value will be overridden when you have set a **Framed MTU** value for the user. If your user is authenticated by RADIUS *and* the RADIUS parameter **Framed-MTU** is set in the RADIUS file, the IOLAN will use the value in the RADIUS file in preference to the value configured here.
Default: 256

Routing	<p>Determines the routing mode (RIP, Routing Information Protocol) used on the SLIP interface as one of the following options:</p> <ul style="list-style-type: none"> • None—Disables RIP over the SLIP interface. • Send—Sends RIP over the SLIP interface. • Listen—Listens for RIP over the SLIP interface. • Send and Listen—Sends RIP and listens for RIP over the SLIP interface. <p>This is the same function as the Framed-Routing attribute for RADIUS authenticated users.</p> <p>Default: None</p>
Enable VJ Compression	<p>When enabled, Van Jacobson compression is used on this link. When enabled, C-SLIP, or compressed SLIP, is used. When disabled, plain SLIP is used. C-SLIP greatly improves the performance of interactive traffic, such as Telnet or Rlogin.</p> <p>If your user is authenticated by the IOLAN, this VJ compression value will be overridden if you have set a Framed Compression value for a user. If your user is authenticated by RADIUS <i>and</i> the RADIUS parameter Framed-Compression is set in the RADIUS file, the IOLAN will use the value in the RADIUS file in preference to the value configured here.</p> <p>Default: Enabled</p>
Session Strings	<p>Controls the sending of ASCII strings to serial device at session start as follows;</p> <ul style="list-style-type: none"> • Send at Start—If configured, this string will be sent to the serial device on power-up of the IOLAN, or when a kill line command is issued on this serial port. If the "monitor DSR" or "monitor DCD" options are set, the string will also be sent when the monitored signal is raised. • Range: 0-127 alpha-numeric characters • Range: hexadecimal 0-FF • Delay after Send - If configured, will inset a delay after the string is sent to the device. This delay can be used to provide the serial device with time to process the string before the session is initiated. • Range is 0-65535 ms <p>Default: 10 ms</p>
Dial Connect	<p>If the device is remote and will be dialing in via modem or ISDN TA, enable this parameter.</p> <p>Default: Disabled</p>
Dial In	<p>If the device is remote and will be dialing in via modem or ISDN TA, enable this parameter.</p> <p>Default: Disabled</p>
Dial Out	<p>If you want the modem to dial a number when the serial port is started, enable this parameter.</p> <p>Default: Disabled</p>

Dial In/Out	Enable this option when you want the serial port to do either of the following: <ul style="list-style-type: none">• accept a call from a modem or ISDN TA• dial a number when the serial port is started Default: Disabled
Dial Timeout	The number of seconds the IOLAN will wait to establish a connection to a remote modem. Range: 1-99 Default: 45 seconds
Dial Retry	The number of times the IOLAN will attempt to re-establish a connection with a remote modem. Range: 0-99 Default: 2
Modem	The name of the predefined modem that is used on this line.
Phone	The phone number to use when Dial Out is enabled.

Custom Application Profile

The **Custom App/Plugin** profile is used in conjunction with custom applications created for the IOLAN by using the Perle SDK. See the *SDK Programmer's Guide* (the SDK and guide are accessible via a request form located on the Perle website at for information about the functions that are supported.

You must download the program and any ancillary files to the IOLAN and set the serial port to the **Custom App/Plugin** profile to actually run a custom application. You must also specify the program executable and any parameters you want to pass to the program in the **Command Line** field. The custom application is automatically run when the serial port is started.

Custom Application General Parameters

Command Line The name of the SDK program executable that has been already been downloaded to the IOLAN, plus any parameters you want to pass to the program. Use the `shell` CLI command as described in the *SDK Programmer's Guide* to manage the files that you have downloaded to the IOLAN. For example, using sample outraw program, you would type:

```
outraw 192.168.2.1:10001 Acct:10001
```

if you were starting the application on a serial port.

Field Format: Maximum of 80 characters

Custom Application Advanced Parameters

Session Strings Controls the sending of ASCII strings to serial device at session start as follows;

- **Send at Start**—If configured, this string will be sent to the serial device on power-up of the IOLAN, or when a kill line command is issued on this serial port. If the "monitor DSR" or "monitor DCD" options are set, the string will also be sent when the monitored signal is raised.

Range: 0-127 alpha-numeric characters

Range: hexadecimal 0-FF

- **Delay after Send** - If configured, will inset a delay after the string is sent to the device. This delay can be used to provide the serial device with time to process the string before the session is initiated.

Range is 0-65535 ms

Default: 10 ms

To view the local port buffer for a particular serial port, you must:

Connect to the device on that serial port by Telnet or SSH.

The serial port(s) must be set to the **Console Management** profile

Once you have established a connection to a device, you can enter the **View Buffer String** at any time to switch the display to the content of the port buffer for that particular serial port.

To return to communicating to the device, press the **ESC** key and the communication session will continue from where you left off.

To navigate through the port buffer data, the following chart illustrates the keyboard keys or "hot keys" that can be used to view the port buffer data. Press the **ESC** key and to continue to communicate with the device on that particular serial port.

Keyboard	Buttons Hot Keys	Direction
----------	------------------	-----------

Page Up	<CTRL>B	Up
Page Down	<CTRL>F	Down
Home	<CTRL>T	Top of the buffer data (oldest data)
End	<CTRL>E	Bottom of the buffer (latest data)
ESC		Exit viewing port buffer data.

Remote Port Buffers

The Remote Port Buffering feature allows data received from serial ports on the IOLAN to be sent to a remote server on the LAN. The remote server, supporting Network File System (NFS), allows administrators to capture and analyze data and messages from the serial device connected to the IOLAN serial port. Remote Port Buffering data can be encrypted or raw and/or time stamped. The data is transmitted to an NFS server where a unique remote file is created for each serial port using the configured serial port **Name** for the file name. If the serial port **Name** parameter is left blank, the IOLAN will create unique files using the IOLAN's Ethernet MAC address and serial port number. It is recommended that a unique NFS directory and serial port **Name** be configured if multiple IOLANs use the same NFS host for Remote Port Buffering. The filenames will be created on the NFS host with a **.ENC** extension to indicate data encrypted files or **.DAT** for unencrypted files. If the data is encrypted, the Decoder utility application must be run on the NFS server to convert the encrypted data to a readable file for administrators to analyze. The Decoder Utility can be found on the Perle website (www.perle.com).

The data that is sent to the remote buffer file is appended to the end of the file (even through IOLAN reboots), so you will want to create a size limit on the file on your remote NFS host, to keep the buffer file size from becoming too large for your system.

Port Buffering General Parameters

Port buffering displays or logs data received on the IOLAN serial port.

Enable Local Port Buffering	Enables/disables local port buffering on the IOLAN. Default: Disabled
View Buffer String	The string used by a session connected to a serial port to display the port buffer for that particular serial port. Data Options: Up to an 8 character string. You can specify control (unprintable) codes by putting the decimal value in angle brackets < > (for example, Escape b is <027>b). Default: ~view
Enable Remote Port Buffering	Enables/disables port buffering on a remote system. When you enable this option, you have the ability to save the buffered data to a file(s) (one file is created for each serial port) and/or send it to the Syslog host for viewing on the Syslog host's monitor. Default: Disabled
NFS Host	The NFS host that the IOLAN will send data to for its Remote Port Buffering feature. The IOLAN will open a file on the NFS host for each serial port configured for Console Management , and will send serial port data to be written to that file(s). Default: None

NFS Directory	The directory and/or subdirectories where the Remote Port Buffering files will be created. For multiple IOLANs using the same NFS host, it is recommended that each IOLAN have its own unique directory to house the remote port log files. Default: /device_server/portlogs
Encrypt Data	Determines if the data sent to the NFS host is sent encrypted or in the clear across the LAN. NOTE: When NFS encryption is enabled, the Decoder utility software is required to be installed on the NFS host for decrypting the data to a readable format. Default: Disabled
Enable Port Buffering to Syslog	When enabled, buffered data is sent to the syslog host to be viewed on the host's monitor. Choose the event level that will be associated with the "port buffer data" in the syslog. Data Options: Emergency, Alert, Critical, Error, Warning, Notice, Info, Debug. Default Level: Info Default: Disabled
Add Time Stamp to Data	Enable/disable time stamping of the serial port buffer data. Default: Disabled
Enable Key Stroke Buffering	When enabled, key strokes that are sent from the network host to the serial device on the IOLAN's serial port are buffered. Default: Disabled

Serial Settings Advanced Parameters

Advanced serial port settings apply to all serial ports.

Process Break Signals	Enables/disables proprietary inband SSH break signal processing, the Telnet break signal, and the out-of-band break signals for TruePort. Default: Disabled
Flush Data Before Closing Serial Port	When enabled, deletes any pending outbound data when a port is closed. Default: Disabled

Deny Multiple Network Connections	<p>Allows only one network connection at a time per a serial port. Application accessing a serial port device across a network with get a connection (socket) refused until:</p> <ul style="list-style-type: none"> • All data from previous connections on that serial port has drained • There are no other connections • Up to a 1 second interconnection poll timer has expired <p>Enabling this feature automatically enables a TCP keep-alive mechanism which is used to detect when a session has abnormally terminated. The keep-alive is sent after 3 minutes of network connection idle time.</p> <p>Applications using this feature need to be aware that there can be some considerable delay between a network disconnection and the port being available for the next connection attempt, allowing any data sent on prior connections to be transmitted out of the serial port. Application network retry logic needs to accommodate this feature.</p> <p>Default: Disabled</p>
Enable Data Logging	<p>When enabled, serial data will be buffered if the TCP connection is lost. When Logging the TCP connection is re-established, the buffered serial data will be sent to its destination. If using the Trueport profile, data logging is only supported in Lite Mode.</p> <p>The minimum data buffer size for is 1 KB. The maximum data buffer size is 4000 KB.</p> <p>If the data buffer is filled, incoming serial data will overwrite the oldest data.</p> <p>Values: 1-4000 KB - Default 256 KB</p> <p>Default: Disabled</p> <p>Note: A kill line or a reboot of the IOLAN causes all buffered data to be lost</p>
Pre V4.3G Data Logging Mode	<p>Enable the logging feature previous to V4.3G software.</p> <p>Default: Disabled</p>
Serial Port Menu String	<p>When a user connects to the IOLAN through the network, the string used to access the Easy Port Access menu without disconnecting the network connection.</p> <p>Data Options: You can specify control (unprintable) codes by putting the decimal value in angle brackets < > (for example, ESC-b is <027>b).</p> <p>Default: ~menu</p>
Session Escape String	<p>When a user connects to the IOLAN through the network, the string is used to access the Reverse Session Menu.</p> <p>Data Options: You can specify control (unprintable) codes by putting the decimal value in angle brackets < > (for example, ESC-b is <027>b).</p> <p>Default: <026>s (Ctrl-z s)</p>
Power Management Menu String	<p>Users accessing the IOLAN through the network can enter the string to bring up the Power Bar Management menu.</p> <p>Data Options: You can specify control (unprintable) codes by putting the decimal value in angle brackets < > (for example, ESC-b is <027>b).</p> <p>Default: <016> (Ctrl-p)</p>

Monitor Connection Interval Status Specify how often, in seconds, the IOLAN will send a TCP keep-alive to services that support TCP keep-alive.
Default: 180 seconds

Retry Attempts The number of TCP keep-alive retries before the connection is closed.
Options: 1-32767

Modem Parameters

If your IOLAN contains an internal modem, a permanent modem string called **iolan_modem** exists permanently in your configuration.

You will need to configure a modem if you want to connect an external modem to one of your serial ports. Modems are usually configured for PPP/SLIP dial in/out connections, although some modems do support raw data communication. When you select the **Modems** tab, you will see any modems that have been configured and the **Add** button to add a new entry to the modem table.

Adding/Editing a Modem

You can add new modems or edit existing modems through the display window:

Name The name of the modem.
Restrictions: Do not use spaces.

Initialization String The initialization string of the modem; see your modem's documentation.

Trueport Baud Rate Parameters

The TruePort utility acts as a COM port redirector that allows applications to talk to serial devices across a network as though the serial devices were directly attached to the server.

Since some older applications may not support the higher baud rates that the IOLAN is capable of achieving, the baud rate can be mapped to a different value on the IOLAN. Through TruePort, you can map the baud rate of the host COM port to a higher baud rate for the serial line that connects the serial device and the IOLAN. See the [Trueport Profile](#) for more information about TruePort.

Actual Baud Rate The actual baud rate that runs between the IOLAN and the connected serial device.
Range: 300-230400, you can also specify a custom baud rate.



Setting Up Users

When you have a user who is accessing a device connected to a serial port from the network or who is accessing the network from a device connected to a serial port through the IOLAN or simply to manage the IOLAN; you can create a user account and configure the user's access privileges. Notice that if there is a Default user; the Default user's parameters are inherited by users logging into the IOLAN.

A user can even represent a device, like a barcode reader or a card swipe device, that you want to be authenticated.

When users are connecting to the IOLAN via serial ports, the user database can be used to:

- Have the user authenticated prior to establishing a connection to a network host.
- Establish a different connection type to the host specific to each user.
- Create a profile different from the Default user profile.

When users are connecting to the IOLAN from a network connection, the user database can be used to:

- Provide authentication on the IOLAN prior to establishing a serial connection via PPP or SLIP.
- Authenticate users prior to providing access to a serially attached console port (such as a Unix server or router).

Note: You do not need user accounts for users who are externally authenticated.

Adding/Editing Users

User Name	The name of the user. Restrictions: Do not use spaces.
Password	The password the user will need to enter to login to the IOLAN.
Confirm Password	Enter the user's password again to verify it is entered correctly.

Level	<p>The access that a user is allowed.</p> <p>Data Options:</p> <ul style="list-style-type: none"> • Admin—The admin level user has total access to the IOLAN. You can create more than one admin user account but we recommend that you only have one. They can monitor and configure the IOLAN. Users configured with this level can access the unit either via serial Terminal Profile connection or via a network originated Telnet or SSH connection to the IOLAN. • Normal—The Normal level user has limited access to the IOLAN. Limited CLI commands and Menu access are available with the ability to configure the user's own configuration settings. Users configured with this level can access the unit either via serial Terminal Profile connection or via a network originated Telnet or SSH connection to the IOLAN. • Restricted—The Restricted level user can only access predefined sessions or access the Easy Port Access menu. Users configured with this level will be restricted to pre-defined sessions or limited CLI commands when connecting through the serial port via the Terminal Profile. The CLI commands are limited to those used for initiating a session. If connection to the IOLAN is done with Telnet or SSH from the network, the user will be presented with the Easy Port Access menu. • Menu—The menu level user will only be able to access predefined sessions when connecting through a serial port with the Terminal Profile or will be limited to the EASY Port Access menu when connecting from the network. The Easy Port Web Access allows the user to connect to the accessible line without disconnecting their initial connection to the IOLAN. Menu users do not have access to CLI commands. <p>When the admin user logs into the IOLAN, the prompt ends with a #, whereas all other users' prompts ends with a \$ or €, depending on the character set.</p> <p>Default: Normal</p>
--------------	---

Note:	<p>A technique for giving a serially attach user (dial-in or terminal attached), the same menus as one that is network connected is to do the following:</p> <ol style="list-style-type: none"> 1. Define the serial port with a Terminal Profile using telnet protocol with a direct connection to Host IP address 127.0.0.0 (local loop back). 2. When the user connects to that serial port a Telnet session will be established to the IOLAN and the user will appear to have connected from the network.
--------------	---

User Services Parameters

The **Services** tab configures the connection parameters for a user. Any connection parameters configured in this window will override the serial port connection parameters.

When a **Terminal** profile is set for the serial port and **Require Login** has been selected, user's accessing the IOLAN through the serial port will be authenticated. Once authentication is successful, the **Service** specified here is started. For example, if the **Service Telnet** is specified, the IOLAN will start a Telnet connection to the specified **Host IP/TCP Port** after the user is successfully authenticated (logs in successfully).

Within the **Terminal** profile, there are a number of settings that apply to possible **Services**. Once it is known which user is connected, and which service is to be used, then the settings from both the **Terminal** profile and the user are used. User parameters take precedence over serial port parameters.

Service	<p>Used in conjunction with the Terminal Profile. After the user has successfully been authenticated, the specified service is started.</p> <p>Data Options: DSPrompt, Telnet, SSH, RLogin, SLIP, PPP, TCP Clear, TCP Raw, SSL Raw</p> <p>Default: DSPrompt</p>
Host IP	<p>For outbound User Services such as Telnet or TCP Clear, SSH and Rlogin, this is the target host name or IP address. If no IP address or host name is specified, the Host IP value in the Default User configuration will be used.</p> <p>Default: 0.0.0.0</p>
TCP Port	<p>When the User Service is Telnet, or TCP Clear, or SSH, this is the target port number. The default value will change based on the type of Service selected; the most common known port numbers are used as the default values.</p>
IPv4 Address	<p>Used for User Service PPP or SLIP, sets the IP address of the remote user. Enter the address in dot decimal notation as follows:</p> <p>n.n.n.n—(where n is a number) Enter the IP address of your choice. This IP address will then be used in preference to the Remote IP Address set for a line.</p> <p>The following IP addresses have a special meaning:</p> <p>255.255.255.254—The IOLAN will use the Remote IP Address set in the PPP settings for the serial port that this user is connecting to.</p> <p>255.255.255.255—When the User Service is PPP, the IOLAN will allow the remote machine to specify its IP address (overriding the IP address negotiation value configured in the PPP settings).</p> <p>255.255.255.255—When the User Service is SLIP, the IOLAN will use the Remote IP Address set for the line (no negotiation).</p> <p>Default: 255.255.255.254</p>
IPv4 Subnet Mask	<p>If the remote user is on a subnet, enter the network's subnet mask. For example, a subnet mask of 255.255.0.0.</p>
IPv6 Interface Identifier	<p>Used for User Service PPP, sets the IPv6 address of the remote user. Enter the address in IPv6 format.</p> <p>Field Format: The first 64 bits of the Interface Identifier must be zero, therefore, ::abcd:abcd:abcd:abcd is the expected format.</p>
MTU	<p>Used for User Service PPP or SLIP, specifies the maximum size of packets, in bytes, being transferred across the link. On noisy links it might be preferable to fragment large packets being transferred over the link, since there will be a quicker recovery from errors.</p> <p>Data Options:</p> <p>PPP—MTU will be the maximum size of packets that the IOLAN will negotiate for this port. This value is negotiated between the two ends of the link.</p> <p>SLIP—MTU will be the maximum size of packets being sent by the IOLAN.</p> <p>The User MTU value will override the MTU/MRU values set for a Serial Port.</p> <p>Range: PPP: 64-1500 bytes, SLIP: 256-1006 bytes</p> <p>Default: PPP is 1500 bytes, SLIP is 256 bytes</p>

Routing	<p>Determines the routing mode used for RIP packets on the PPP and SLIP interfaces. Values are:</p> <ul style="list-style-type: none"> • None—RIP packets are neither received nor sent by the IOLAN. • Send—RIP packets can only be sent by the IOLAN. • Listen—RIP packets can only be received by the IOLAN. • Send and Listen—RIP packets are sent and received by the IOLAN. <p>Default: None</p>
Enable VJ Compression	<p>Used for User Service PPP or SLIP, determines whether Van Jacobsen Compression is used on the link. VJ compression is a means of reducing the standard TCP/IP header from 40 octets to approximately 5 octets. This gives a significant performance improvement, particularly when interactive applications are being used. For example, when the user is typing, a single character can be transmitted and thus have the overhead of the full TCP/IP header. VJ Compression has minimal effect on other types of links, such as FTP, where the packets are much larger. The User VJ Compression option will override the VJ Compression value set for a Serial Port.</p> <p>Default: Disabled</p>

User Service Advanced Parameters

The **Advanced** tab is used to configure those parameters that control the user session; this includes session length, language, the hotkey used for switching between sessions, access to clustered ports, etc.

Idle Timeout	<p>The amount of time, in seconds, before the IOLAN closes a connection due to inactivity. The default value is 0 (zero), meaning that the Idle Timer will not expire (the connection is open permanently). The User Idle Timeout will override all other Serial Port Idle Timeout parameters.</p> <p>Range: 0-4294967</p> <p>Default: 0</p>
Session Timeout	<p>The amount of time, in seconds, before the IOLAN forcibly closes a user's session (connection). The default value is 0 (zero), meaning that the session timer will not expire (the session is open permanently, or until the user logs out). The User Session Timeout will override all other Serial Port Session Timeout parameters.</p> <p>Range: 0-4294967</p> <p>Default: 0</p>
Enable Callback	<p>When enabled, enter a phone number for the IOLAN to call the user back (the Enable Callback parameter is unrelated to the Serial Port Remote Access (PPP) profile Dial parameter).</p> <p>Note: the IOLAN will allow callback only when a user is authenticated. If the protocol over the link does not provide authentication, there will be no callback. Therefore, when the Serial Port profile is set to Remote Access (PPP), you must use either PAP or CHAP, because these protocols provide authentication.</p> <p>The IOLAN supports another type of callback, Roaming Callback, which is configurable when the Serial Port profile is set to Remote Access (PPP).</p> <p>Default: Disabled</p>

Phone Number	<p>The phone number the IOLAN will dial to callback the user (you must have set Enable Callback enabled).</p> <p>Restrictions: Enter the number without spaces.</p>
Language	<p>You can specify whether a user will use English or Custom Language as the language that appears in the CLI. The IOLAN supports one custom language that must be downloaded to the IOLAN.</p> <p>Default: English</p>
Hotkey Prefix	<p>The prefix that a user types to control the current session.</p> <p>Data Options:</p> <ul style="list-style-type: none"> • ^a number—To switch from one session to another, press ^a (Ctrl-a) and then the required session number. For example, ^a 2 would switch you to session 2. Pressing ^a 0 will return you to the IOLAN Menu. • ^a n—Display the next session. The current session will remain active. The lowest numbered active session will be displayed. • ^a p—Display the previous session. The current session will remain active. The highest numbered active session will be displayed. • ^a m—To exit a session and return to the IOLAN. You will be returned to the menu. The session will be left running. • ^a l—(Lowercase l) Locks the serial port until the user unlocks it. The user is prompted for a password (any password, excluding spaces) and the serial port is locked. The user must retype the password to unlock the serial port. • ^r—When you switch from a session back to the Menu, the screen may not be redrawn correctly. If this happens, use this command to redraw it properly. This is always Ctrl R, regardless of the Hotkey Prefix. <p>The User Hotkey Prefix value overrides the Serial Port Hotkey Prefix value. You can use the Hotkey Prefix keys to lock a serial port only when the serial port's Allow Port Locking parameter is enabled.</p> <p>Default: Hex 01 (Ctrl-a or ^a)</p>

User Sessions

The **Sessions** tab is used to configure specific connections for users who are accessing the network through the IOLAN's serial port.

Users who have successfully logged into the IOLAN (**User Service** set to **DSprompt**) can start up to four login sessions on network hosts. These users start sessions through the EasyPortMenu option **Sessions**. Multiple sessions can be run simultaneously to the same host or to different hosts. Users can switch between different sessions and also between sessions and the IOLAN using **Hotkey** commands (see [Hotkey Prefix](#)) for a list of commands.

Users with **Admin** or **Normal** privileges can define new sessions and use them to connect to Network hosts; they can even configure them to start automatically on login to the IOLAN. **Restricted** and **Menu** users can only start sessions predefined for them in their user configuration.

User Sessions Parameters

Predefined Outbound Sessions 1, 2, 3, 4 You can configure up to four (4) sessions that the user can select from to connect to a specific host after that user has successfully logged into the IOLAN (used only on serial ports configured for the **Terminal** profile).

Data Options:

- **None**—No connection is configured for this session.
- **Telnet**—For information on the Telnet connection window, see [Telnet Settings](#).
- **Rlogin**—For information on the Rlogin connection see RLogin [Rlogin Settings](#).
- **SSH**—For information on the SSH connection window, see [SSH Setting](#).

Default: None

Telnet SSH, Rlogin Settings Button

Select this button to configure the connection parameters for this session.

Connect

Automatically

Specify whether or not the session(s) will start automatically when the user logs into the IOLAN.

Default: Disabled

Host

The host that the user will connect to in this predefined session.

Default: None

TCP Port

The TCP port that the IOLAN will use to connect to the host in this predefined session.

Default: Telnet-23, SSH-22, Rlogin-513

Serial Port Access

The **Serial Port Access** tab controls the user's read/write access on any given IOLAN serial port. This pertains to users that are connecting from the network to a serial over a Console Management type session. This can be useful when you have multiple users connecting to the same serial device and you wish to control the viewing and/or the write to and from the device. See the **Multisessions** and **User Authentication** parameters in the [Console Management Advanced Parameters](#) for the serial port settings.

Serial Port Access

Specifies the user access rights to each IOLAN serial port device. There can be multiple users connected to a particular serial device and these settings determine the rights of this user for any of the listed serial ports.

Data Options:

- **Read/Write**—The user has read and write access to the serial port.
- **Read In**—The User will see data going to the serial port, from all network-connected users that have write privileges to this serial port.
- **Read Out**—The user will have access to all data originating from the serial device.

Users can read data going in both directions by selecting both the **Read In** and **Read Out** options.

Default: Read/Write

Authentication

Users can be authentication by the IOLAN. or through an external authentication server.

Authentication is different from authorization, which can restrict a user's access to the network (although this can be done through the concept of creating sessions for a user. Authentication ensures that the user is defined within the authentication database—with the exception of using the **Guest** authentication option under **Local Authentication**, which can accept any user ID as long as the user knows the configured password.

For external authentication, the IOLAN supports RADIUS, Kerberos, LDAP/Microsoft Active Directory, TACACS+, SecurID, and NIS. You can specify a primary authentication method and a secondary authentication method. If the primary authentication method fails (cannot connect to the server or authentication fails), the secondary authentication method is tried (unless you enable the **Only Use as backup** option, in which case the secondary authentication method will be tried only when the IOLAN cannot communicate with the primary authentication host). This allows you to specify two different authentication methods. If you do specify two different authentication methods, the user will be prompted for his/her username once, but will be prompted for a password for each authentication method tried. For example, user Alfred's user ID is maintained in the secondary authentication database, therefore, he will be prompted for his password twice, because he is not in the primary authentication database. Unlike the other external authentication methods, RADIUS and TACACS+ can also send back **Serial Port** and **User** parameters that are used for the duration of the connection. Therefore, any parameters configured by RADIUS or TACACS+ will override the same parameters configured in the IOLAN. See [Appendix RADIUS External Parameters](#) for more information.

Security Overview

The Security group includes the following configuration options:

- **Authentication**—When a serial port is configured for the Console Management or TCP Sockets profile, the user can be authenticated either locally in the IOLAN user profile or externally. This option configures the external authentication server. See *Setting Primary and Secondary Authentication Methods* for more information.
- **SSH**—This configuration window configures the SSH server in the IOLAN. See [NIS Authentication Parameters](#) for more information.
- **SSL/TLS**—This configuration window configures global SSL/TLS settings, which can be overridden on the serial port level. See [SSL/TLS](#) for more information.
- **VPN**—This configuration window configures the Virtual Personal Network (VPN) IPsec and L2TP/IPsec tunnel parameters. See [VPN Authentication Parameters](#) for more information.
- **HTTP Tunnel**—This configuration window configures the Http Tunneling parameters. See [Configuring a HTTP Tunnel](#) for more information.
- **Services**—This configuration window is used to enable/disable client and daemon services that run in the IOLAN. See [Enable/Disable Services](#) for more information.

In the Authentication window, you can select up to two methods of authentication made up of external authentication options and/or the local user database.

Setting Primary and Secondary Authentication Methods

Primary Authentication Method	The first authentication method that the IOLAN attempts. Data Options: Local, RADIUS, Kerberos, LDAP/Microsoft Active directory, TACACS+, SecurID, NIS Default: Local
--------------------------------------	---

Secondary Authentication Method	<p>If the Primary Authentication Method fails, the next authentication method that the IOLAN attempts. You can choose to use authentication methods in combination. For example, you can specify the Primary Authentication Method as Local and the Secondary Authentication Method as RADIUS. Therefore, some users can be defined in the IOLAN (Local) others in RADIUS.</p> <p>Data Options: None, Local, RADIUS, Kerberos, LDAP/Microsoft Active Directory, TACACS+, SecurID, NIS</p> <p>Default: None</p>
Only use as backup	<p>The secondary authentication method will be tried only when the IOLAN cannot communicate with the primary authentication host.</p> <p>Default: Disabled</p>
Only authenticate admin user in the local database	<p>When enabled, the IOLAN will only authenticate the admin user in the local user database, regardless of any external authentication methods configured. When disabled, a user called admin must exist when only external authentication methods are configured, or you will not be able to access the IOLAN as the admin user, except through the console port.</p> <p>Default: Enabled</p>

Local

When **Local** authentication is selected, the user must either be configured in the IOLAN's **User List** or you must enable **Guest** users.

Local Authentication Parameter

Enable Guest Mode	<p>Allow users who are not defined in the Users database to log into the IOLAN with any user ID and the specified password. Guest users inherit their settings from the Default User's configuration.</p> <p>Default: Disabled</p>
Guest Password	<p>The password that Guest users must use to log into the IOLAN.</p>
Confirm Password	<p>Type the Guest Password in again to verify that it is correct.</p>
Enable Login Once	<p>When this option is selected, only one user with the same username can be signed in at one time. Should the same user with the same username attempt to sign in again, their first session will be terminated and they will gain entry to their new session.</p>
Enable Password Rules	<p>When this option is selected, the following password rules will apply. The password must be 8 characters long and contain at least one number.</p>
Enable Account Lockout	<p>When this option is selected, the IOLAN's internal local user database will provide a 10 second delay after each invalid attempt. If 5 invalid attempts are made within 1 minute the user will be locked out from further attempts for 5 minutes.</p>

RADIUS

Radius is an authentication method that the IOLAN supports that can send back **User** information; see [Supported RADIUS Parameters](#) for more information on the **User** parameters that can be sent back by RADIUS.

Radius Authentication Parameters

First Authentication Host	Name of the primary RADIUS authentication host. Default: None
Second Authentication Host	Name of the secondary RADIUS authentication host, should the first RADIUS host fail to respond. Default: None
Secret	The secret (password) shared between the IOLAN and the RADIUS authentication host.
Authentication Port	The port that the RADIUS host listens to for authentication requests. Default: 1812
Enable Accounting	Enables/disables RADIUS accounting. Default: Disabled
First Accounting Host	Name of the primary RADIUS accounting host. Default: None
Second Accounting Host	Name of the secondary RADIUS accounting host. Default: None
Secret	The secret (password) shared between the IOLAN and the RADIUS accounting host.
Account Port	The port that the RADIUS host listens to for accounting requests. Default: 1813
Enable Accounting Authenticator	Enables/disables whether or not the IOLAN validates the RADIUS accounting response. Default: Enabled
Retry	The number of times the IOLAN tries to connect to the RADIUS server before erring out. Range: 0-255 Default: 5
Timeout	The time, in seconds, that the IOLAN waits to receive a reply after sending out a request to a RADIUS accounting or authentication host. If no reply is received before the timeout period expires, the IOLAN will retry the same host up to and including the number of retry attempts. Range: 1-255 Default: 3 seconds

Attribute Field Descriptions

NAS-Identifier	This is the string that identifies the Network Address Server (NAS) that is originating the Access-Request to authenticate a user. Field Format: Maximum 31 characters, including spaces
Automatically determine NAS-IP-Address	When enabled, the IOLAN will send the IOLAN's Ethernet 1 IPv4 address to the RADIUS server. Default: Enabled
Use the following NAS-IP-Address	When enabled, the IOLAN will send the specified IPv4 address to the RADIUS server. Default: Disabled
IP Address	The IPv4 address that the IOLAN will send to the RADIUS server. Default: 0.0.0.0
Automatically determine NAS-IPv6-Address	When enabled, the IOLAN will send the IOLAN's IPv6 address to the RADIUS server. Default: Enabled
Use the following NAS-IPv6-Address	When enabled, the IOLAN will send the specified IPv6 address to the RADIUS server. Default: Disabled
IPv6 Address	The IPv6 address that the IOLAN will send to the RADIUS server. Field Format: IPv6 address

KerberosLDAP/Microsoft Active Directory

Realm	The Kerberos realm is the Kerberos host domain name, in upper-case letters.
KDC Domain	The name of a host running the KDC (Key Distribution Center) for the specified realm. The host name that you specify must either be defined in the IOLAN's Host Table before the last reboot or be resolved by DNS.
KDC Port	Kerberos server listens to for authentication requests. Default: 88

LDAP (Lightweight Directory Access Protocol) is an application protocol for querying and modifying directory services running over TCP/IP. It is also used as a method of authenticating users. Microsoft Active Directory is an LDAP like directory service. It can be used for authenticating users in a similar fashion to LDAP. In this manual, the use of LDAP is synonymous with Microsoft Active Directory.

LDAP/Microsoft Active Directory Authentication Parameters

If you are using LDAP or Microsoft Active

Host Name	The name or IP address of the LDAP/Microsoft Active Directory host. If you use a host name, that host must either have been defined in the IOLAN's Host Table before the last reboot or be resolved by DNS. If you are using TLS , you must enter the same string you used to create the LDAP certificate that resides on your LDAP/Microsoft Active Directory server.
Port	The port that the LDAP/Microsoft Active Directory host listens to for authentication requests. Default: 389
Base	The domain component (dc) that is the starting point for the search for user authentication. You can enter up to 128 characters for the base.
User Attribute	<p>This defines the name of the attribute used to communicate the user name to the server.</p> <p>Options:</p> <ul style="list-style-type: none">• OpenLDAP(uid)—Chose this option if you are using an OpenLDAP server. The user attribute on this server is "uid".• Microsoft Active Directory(sAMAccountName)—Chose this option if your LDAP server is a Microsoft Active Directory server. The user attribute on this server is "sAMAccountName".• Other—If you are running something other than a OpenLDAP or Microsoft Active Directory server, you will have to find out from your system administrator what the user attribute is and enter it in this field. <p>Default: OpenLDAP(uid)</p>
Encrypt Passwords Using MD5 digest	<p>Checking this parameter will cause the IOLAN to encrypt the password using MD5 digest before sending it to server. If this option is not checked, the password is sent to the server in the clear.</p> <p>Default: Disabled</p>
Authenticate IOLAN with LDAP server	<p>This option will cause the Terminal Server to authenticate with the LDAP server before the user authentication takes place. The user name/password to use for this authentication is configured below.</p> <p>Default: Disabled</p>
Name	The user name associated with the IOLAN.
Append Base to Name	<p>When checked, this causes the domain component configured in the "base" parameter to be appended to the user name. This allows for a fully qualified name to be used when authenticating the IOLAN.</p> <p>Default: Enabled but if the base parameter is not configured, it does not modify the name.</p>
Confirm	<p>You must enter the exact same value as the password field. Since the password is not echoed, this ensures that the field was entered correctly.</p> <p>Default: Blank</p>

Enable TLS	Enables/disables the Transport Layer Security (TLS) with the LDAP/Microsoft Active Directory host. Default: Disabled.
-------------------	---

TLS Port	Specify the port number that LDAP/Microsoft Active Directory will use for TLS . Default: 636
-----------------	---

Directory with **TLS**, you need to download a CA list to the IOLAN that includes the certificate authority (CA) that signed the LDAP certificate on the LDAP host by selecting **Tools, Advanced, Keys and Certificates**. See [Network Filtering](#) for more information on the LDAP certificate.

TACACS+

TACACS+ is an authentication method that the IOLAN supports that can send back **User** information; see for more information on the **User** parameters that can be sent back by TACACS+.

TACACS+ Authentication Parameters

Authentication/Authorization Primary Host	The primary TACACS+ host that is used for authentication. Default: None
--	---

Authentication/Authorization Secondary Host	The secondary TACACS+ host that is used for authentication, should the primary TACACS+ host fail to respond. Default: None
--	--

Authentication/Authorization Port	The port number that TACACS+ listens to for authentication requests. Default: 49
--	--

Authentication/Authorization Secret	The TACACS+ shared secret is used to encrypt/decrypt TACACS+ packets in communications between two devices. The shared secret may be any alphanumeric string. Each shared secret must be configured on both client and server sides.
--	--

Enable Authorization	Enables authorization on the TACACS+ host, meaning that IOLAN-specific parameters set in the TACACS+ configuration file can be passed to the IOLAN after authentication. Default: Disabled
-----------------------------	--

Enable Accounting	Enables/disables TACACS+ accounting. Default: Disabled
--------------------------	--

Accounting Primary Host	The primary TACACS+ host that is used for accounting. Default: None
--------------------------------	---

Accounting Secondary Host	The secondary TACACS+ host that is used for accounting, should the primary accounting TACACS+ host fail to respond. Default: None
----------------------------------	---

Accounting Port	The port number that TACACS+ listens to for accounting requests. Default: 49
Accounting Secret	The TACACS+ shared secret is used to encrypt/decrypt TACACS+ packets in communications between two devices. The shared secret may be any alphanumeric string. Each shared secret must be configured on both client and server sides.
Use Alternate Service Names	The TACACS+ service name for Telnet or SSH is normally "raccess". The service name for Web Manager or Device Manager is "EXEC". In some cases, these service names conflicted with services used by Cisco devices. If this is the case, checking this field will cause the service name for Telnet or SSH to be "perlecli" and the service name for Web Manager or Device Manager to be "perleweb".

Securid

Securid Authentication Parameters***Securid Reset Node***

Primary/Master Host	The first SecurID server that is tried for user authentication. Default: None
Replica/Slave Host	If the first SecurID server does not respond to an authentication request, this is the next SecurID server that is tried for user authentication. Default: None
UDP Port	The port number that SecurID listens to for authentication requests. Default: 5500
Encryption Type	The type of encryption that will be used for SecurID server communication. Data Options: DES, SDI Default: SDI
Legacy	If you are running SecurID 3.x or 4.x, you need to run in Legacy Mode . If you are running SecurID 5.x or above, do not select Legacy Mode . Default: Disabled

If you need to reset the SecurID secret, select **Administration, Reset, Securid Secret**.

NIS

NIS Authentication Parameters

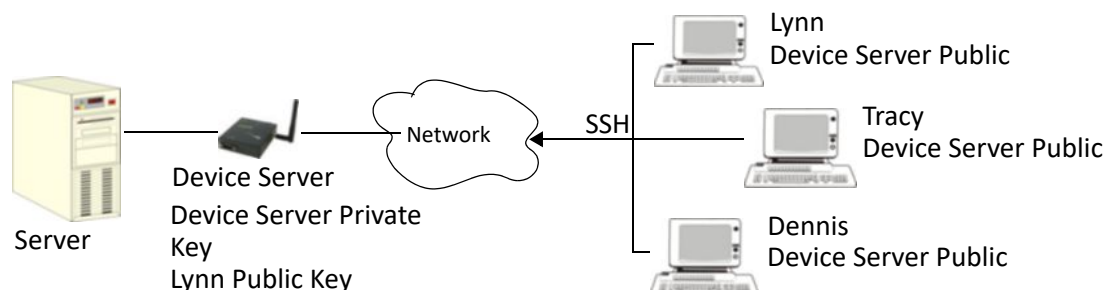
NIS Domain	The NIS domain name.
Primary NIS Host	The primary NIS host that is used for authentication. Default: None
Secondary NIS Host	The secondary NIS host that is used for authentication, should the primary NIS host fail to respond. Default: None

The IOLAN contains SSH Server software that you need to configure if the IOLAN is going to be accessed via SSH. If you specify more than one **Authentication** method and/or **Cipher**, the IOLAN will negotiate with the client and use the first authentication method and cipher that is compatible with both systems. When you are using the SSH connection protocol, keys need to be distributed to all users and the IOLAN. Below are a couple of example scenarios for key/certificate distribution.

Users Logging into the IOLAN Using SSH

This scenario applies to serial ports configured for **Console Management** using the SSH protocol. In the following example, users are connecting to the IOLAN via SSH from the LAN. Therefore, the following keys need to be exchanged:

- Upload the IOLAN **SSH Public Key** to each user's host machine who is connecting and logging into the IOLAN using SSH.
- Download the SSH Public Key from each user's host machine who is connecting and logging into the IOLAN using SSH.

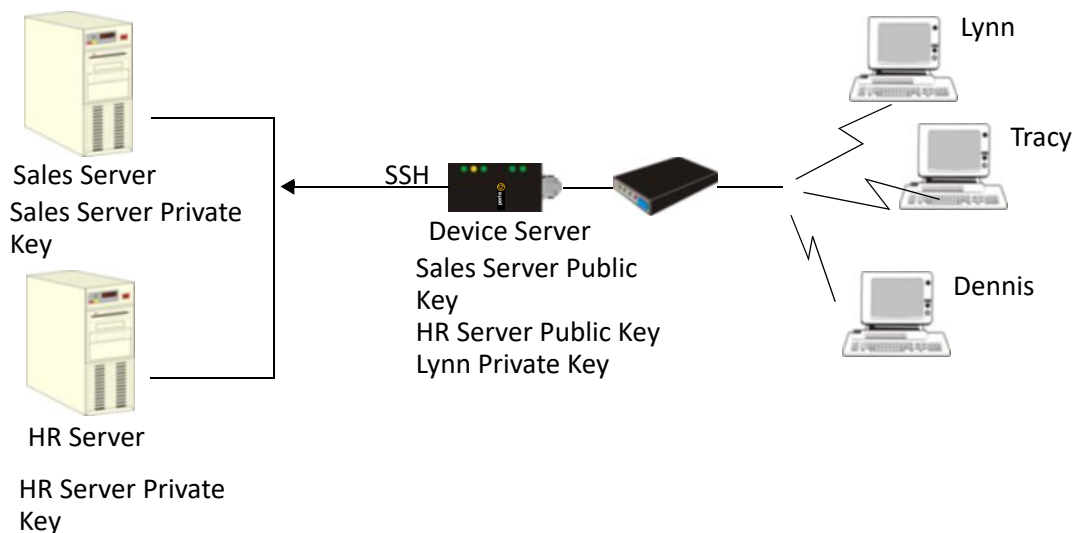


Users Passing Through the IOLAN Using SSH (Dir/Sil)

This scenario applies to serial ports configured for the **Terminal** profile and are required to login to the IOLAN. The user's service is set to the SSH protocol, therefore, users first log into the IOLAN and then are connected to a specified host (configured for the user when **User Service SSH** is selected) through an SSH connection. Lynn and Tracy automatically connect to the HR Server and Dennis automatically connects to the Development Server via SSH through the IOLAN. All the SSH negotiation is being done between the IOLAN and the target servers, therefore, the following keys need to be exchanged:

- Download the **SSH Host Public Key** to the IOLAN for each of the hosts that the IOLAN is connecting to.
- Download the **SSH User Private Key** for each user whose **User Service** is set to **SSH**.

- Copy the SSH User Public Key to the host that the user is connecting to (this is done outside the scope of the IOLAN).



Allow SSH-1 Protocol Allows the user's client to negotiate an SSH-1 connection, in addition to SSH-2.
Default: Disabled

RSA When a client SSH session requests RSA authentication, the IOLAN's SSH server will authenticate the user via RSA.
Default: Enabled

DSA When a client SSH session requests DSA authentication, the IOLAN's SSH server will authenticate the user via DSA.
Default: Enabled

Keyboard-Interactive The user types in a password for authentication.
Default: Enabled

Password The user types in a password for authentication.
Default: Enabled

3DES The IOLAN SSH server's 3DES encryption is enabled/disabled.
Default: Enabled

CAST The IOLAN SSH server's CAST encryption is enabled/disabled.
Default: Enabled

Blowfish The IOLAN SSH server's Blowfish encryption is enabled/disabled.
Default: Enabled

Arcfour The IOLAN SSH server's Arcfour encryption is enabled/disabled.
Default: Enabled

AES-CBC The IOLAN SSH server's AES-CBC encryption is enabled/disabled.
Default: Enabled

AES-CTR	The IOLAN SSH server's AES-CTR encryption is enabled/disabled. Default: Enabled
AES-GCM	The IOLAN SSH server's AES-GCM encryption is enabled/disabled. Default: Enabled
ChaCha20-Poly1305	The IOLAN SSH server's ChaCha20-Poly1305 encryption is enabled/disabled. Default: Enabled
Break String	The break string used for inband SSH break signal processing. A break signal is generated on a specific serial port only when the server's break option is enabled and the user currently connected using reverse SSH has typed the break string exactly. Field Format: maximum 8 characters Default: ~break, where ~ is tilde
Enable Verbose Output	Displays debug messages on the terminal. Default: Disabled
Allow Compression	Requests compression of all data. Compression is desirable on modem lines and other slow connections, but will only degrade data transmission speeds on faster networks. Default: Disabled
Login Timeout	Set the time to wait for the SSH client to complete the login. If the timer expires before the login is completed, the session is terminated. Default: 120 seconds Values: 1-600 seconds

SSL/TLS

When SSL/TLS is configured, data is encrypted between the IOLAN and the host/device (which must also support SSL/TLS). When you configure the **SSL/TLS** settings in the **System** section, you are configuring the default global SSL/TLS settings; you are not configuring an SSL/TLS server.

You can create an encrypted connection using SSL/TLS for the following profiles: **TruePort**, **TCP Sockets**, **Terminal** (the user's **Service** must be set to **SSL_Raw**), **Serial Tunneling**, **Virtual Modem**, and **Modbus**.

When configuring SSL/TLS, the following configuration options are available:

- You can set up the IOLAN to act as an SSL/TLS client or server.
- There is an extensive selection of SSL/TLS ciphers that you can configure for your SSL/TLS connection; see **appendix on ciphers** for a list of SSL/TLS ciphers.

Note: Some combinations of cipher groups are not available on FIPS firmware versions.

You can enable peer certificate validation, for which you must supply the validation criteria that was used when creating the peer certificate (this is case sensitive).

Note: See [Network Filtering](#) for information about SSL/TLS support documents.

Authentication Parameters

SSL/TLS Version	<p>Specify whether you want to use:</p> <ul style="list-style-type: none">• Any—The IOLAN will try a TLSv1 connection first. If that fails, it will try an SSLv3 connection. If that fails, it will try an SSLv2 connection.• SSLv3—The connection will use only SSLv3.• TLSv1—The connection will use only TLSv1.• TLSv1.1—The connection will use only TLSv1.1.• TLSv1.2—The connection will use only TLSv1.2. <p>Default: Any</p>
SSL/TLS Type	<p>Specify whether the IOLAN serial port will act as an SSL/TLS client or server.</p> <p>Default: Client</p>
Cipher Suite Button	<p>Select this button to specify SSL/TLS connection ciphers.</p>
Validate Peer Certificate	<p>Enable this option when you want the Validation Criteria to match the Peer Certificate for authentication to pass. If you enable this option, you need to download an SSL/TLS certificate authority (CA) list file to the IOLAN.</p> <p>Default: Disabled</p>
Validation Criteria Button	<p>Select this button to create peer certificate validation criteria that must be met for a valid SSL/TLS connection.</p>
SSL Certificate Passphrase	<p>This is the SSL/TLS passphrase used to generate an encrypted RSA/DSA private key. This private key and passphrase are required for both HTTPS and SSL/TLS connections, unless an unencrypted private key was generated, then the SSL passphrase is not required. Make sure that you download the SSL private key and certificate if you are using the secure HTTP option (HTTPS) or SSL/TLS. If both RSA and DSA private keys are downloaded to the IOLAN, they need to be generated using the same SSL passphrase for both to work.</p>

Cipher Suite Field Descriptions

The SSL/TLS cipher suite is used to encrypt data between the IOLAN and the client. You can specify up to five cipher groups.

Note: Some combinations of cipher groups may not be available on some firmware versions.

Adding/Editing a Cipher

See [Valid SSL/TLS Ciphers](#) for a list of valid SSL/TLS ciphers.

SSL Authentication Parameters

Encryption	<p>Select the type of encryption that will be used for the SSL connection.</p> <p>Data Options:</p> <ul style="list-style-type: none">• Any—Will use the first encryption format that can be negotiated.• AES• 3DES• DES• ARCFOUR• ARCTWO• AES-GCM <p>Default: Any</p>
Min Key Size	<p>The minimum key size value that will be used for the specified encryption type.</p> <p>Data Options: 40, 56, 64, 128, 168, 256</p> <p>Default: 40</p>
Max Key Size	<p>The maximum key size value that will be used for the specified encryption type.</p> <p>Data Options: 40, 56, 64, 128, 168, 256</p> <p>Default: 256</p>
Key Exchange	<p>The type of key to exchange for the encryption format.</p> <p>Data Options:</p> <ul style="list-style-type: none">• Any—Any key exchange that is valid is used (this does not, however, include ADH keys).• RSA—This is an RSA key exchange using an RSA key and certificate.• EDH-RSA—This is an EDH key exchange using an RSA key and certificate.• EDH-DSS—This is an EDH key exchange using a DSA key and certificate.• ADH—This is an anonymous key exchange which does not require a private key or certificate. Choose this key if you do not want to authenticate the peer device, but you want the data encrypted on the SSL/TLS connection.• ECDH-ECDSA—This is an ECDH key exchange using a ECDSA key and certificate. <p>Default: Any</p>
HMAC	<p>Select the key-hashing for message authentication method for your encryption type.</p> <p>Data Options:</p> <ul style="list-style-type: none">• Any• MD5• SHA1• SHA256• SHA384 <p>Default: Any</p>

Validation Criteria Field Descriptions

If you choose to configure validation criteria, then the information in the peer SSL/TLS certificate must match exactly the information configured in this window in order to pass peer authentication and create a valid SSL/TLS connection.

Country	A country code; for example, US. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate. Data Options: Two characters
State/Province	An entry for the state/province; for example, IL. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate. Data Options: Maximum 128 characters
Locality	An entry for the location; for example, Chicago. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate. Data Options: Maximum 128 characters
Organization	An entry for the organization; for example, Accounting. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate. Data Options: Maximum 64 characters
Organization Unit	An entry for the unit in the organization; for example, Payroll. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate. Data Options: Maximum 64 characters
Common Name	An entry for common name; for example, the host name or fully qualified domain name. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate. Data Options: Maximum 64 characters
Email	An entry for an email address; for example, acct@anycompany.com. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate. Data Options: Maximum 64 characters

VPN

A Virtual Private Network (VPN) creates a secure, dedicated communications network tunnelled through another network.

You can configure the IOLAN for:

- a host-to-host Virtual Private Network (VPN) connection
- a host-to-network VPN connection
- a network-to-network VPN connection
- or host/network-to-IOLAN VPN connection (allowing serial devices connected to the IOLAN to communicate data to a host/network).

In addition to being able to configure up to 64 IPsec tunnels, you can configure an L2TP/IPsec tunnel that will allow hosts to create a VPN tunnel to the IOLAN. The L2TP/IPsec VPN protocol is required by the Windows XP® operating system. Later versions of Windows® may support both VPN protocols, however check with the Windows® documentation that came with your Windows® pc.

Note: Before you enable/configure any VPN tunnels, you should configure any exceptions or you might not be able to access the IOLAN except through a VPN tunnel or the console port. See [L2TP/IPsec Exceptions](#) for more information about exceptions.

Note: If you are configuring IPsec and/or L2TP/IPsec, you must also enable the IPsec service found in **Security, Services** navigation tree.

The information in this section applies only to setting up IPsec VPN tunnels, not L2TP/IPsec VPN tunnels. The IOLAN can be configured as a VPN gateway using the IPsec protocol. You can configure the VPN connection using two IOLANs as the local and remote VPN gateways or the IOLAN as the local VPN gateway and a host/server running the VPN software as the remote VPN gateway.

If the VPN tunnel is being configured for an IPv6 network that is going through a router(s), the router(s) must have manual IPv6 address entry capability.

VPN servers/clients can support various VPN parameters. However, the following parameters are REQUIRED to be set to the following values to support a VPN tunnel between the IOLAN and a VPN server/client:

```
perfect forward secrecy: no
protocol: ESP
mode: tunnel (not transport)
opportunistic encryption: no
aggressive mode: no
```

IKE Phase 1 Proposals

The following IKE Phase 1 proposals are supported by the IOLAN VPN gateway:

- **Ciphers**—3DES, AES
- **Hashes**—MD5, SHA1
- **Diffie-Hellman Groups**—2 (MODP1024), 5 (MODP1536), 14 (MODP2048), 15 (MODP3072), 16 (MODP4096), 17 (MODP6144), 18 (MODP8192)

ESP Phase 2 Proposals

The following ESP Phase 2 proposals are supported by the IOLAN VPN gateway:

- **Ciphers**—3DES, AES
- **Authentication Algorithms**—MD5, SHA1, SHA2

IPsec

When an IPsec tunnel becomes active, you are requiring that all access to the IOLAN go through the configured IPsec tunnel(s), so you must configure any exceptions first see ([L2TP/IPsec Exceptions](#)). for more information on exceptions) or you will not be able to access the IOLAN through the network unless you are configured to go through the IPsec tunnel (you can still access the IOLAN through the Console port).

Adding/Editing the IPsec Tunnel

When you select the **Add** button or select an IPsec tunnel and select the **Edit** button, the following window is displayed:

Name	Provide a name for the IPsec VPN tunnel to make it easy to identify. Text Characteristics: Maximum of 16 characters, spaces not allowed
Authentication Method	<p>Specify the authentication method that will be used between VPN peers to authenticate the VPN tunnel.</p> <p>Data Options:</p> <ul style="list-style-type: none">• Shared Secret—A text-based secret that is used to authenticate the IPsec tunnel (case sensitive). This applies to all VPN tunnels (IPsec and L2TP/IPsec).• RSA Signature—RSA signatures are used to authenticate the IPsec tunnel. When using this authentication method, you must download the IPsec RSA public key to the IOLAN and upload the IPsec RSA public key from the IOLAN to the VPN gateway.• X.509 Certificate—X.509 certificates are used to authenticate the IPsec tunnel. When using this authentication method, you must include the signing authority's certificate information in the SSL/TLS CA list and download it to the IOLAN. <p>Default: Shared Secret</p>
Secret/Remote Validation Criteria Button	<p>Shared Secret—Specify the text-based secret that is used to authenticate the IPsec tunnel (case sensitive). This applies to all VPN tunnels (IPsec and L2TP/IPsec).</p> <p>X.509 Certificate—Specify the remote X.509 certificate validation criteria that must match for successful authentication (case sensitive). Note that all validation criteria must be configured to match the X.509 certificate. If using an asterisk (*) for wildcard matching, the Boot Action must be set to Add (Listen).</p> <p>See Shared Secret Field Description for more information.</p> <p>See Remote Validation Criteria Field Descriptions or more information on the X.509 certificate validation criteria.</p>
Local Device	<p>When the VPN tunnel is established, one side of the tunnel is designated as Right and the other as Left. You are configuring the IOLAN-side of the VPN tunnel.</p> <p>Data Options: Left, Right</p> <p>Default: Left</p>
Local IP Address	<p>The IP address of the IOLAN. You can specify <code>%defaultroute</code> when the IP address of the IOLAN is not always known (for example, when it gets its IP address from DHCP). When <code>%defaultroute</code> is used, a default gateway must be configured in the route table (Network, Advanced, Route List tab).</p> <p>Field Format: IPv4 address, IPv6 address, FQDN, <code>%defaultroute</code></p>

Local External IP Address	When NAT Traversal (NAT_T) is enabled, this is IOLAN's external IP address or FQDN. When the IOLAN is behind a NAT router, this will be its public IP address. Field Format: IPv4 address, IPv6 address, FQDN
Local Next Hop	The IP address of the router/gateway that will forward data packets to the remote VPN (if required). The router/gateway must reside on the same subnet at the IOLAN. Leave this parameter blank if you want to use the Default Gateway configured in the IOLAN. Field Format: IPv4 or IPv6 address
Local Host/Network Address	The IP address of a specific host, or the network address that the IOLAN will provide a VPN connection to. Field Format: IPv4 or IPv6 address
Local IPv4 Subnet Mask	The subnet mask of the local IPv4 network. Keep the default value when you are configuring a host-to-host VPN connection. Default: 255.255.255.255
Local IPv6 Prefix Bits	The prefix bits of the local IPv6 network. Keep the default value when you are configuring a host-to-host VPN connection. Default: 0
Remote IP Address	The IP address or FQDN of the remote VPN peer. If you want to accept a VPN connection from any VPN peer, you can enter %any in this field. Field Format: IPv4 address, IPv6 address, FQDN, %any
Remote External IP Address	When NAT Traversal (NAT_T) is enabled, the remote VPN's public external IP address or FQDN. Field Format: IPv4 address, IPv6 address, FQDN
Remote Next Hop	The IP address of the router/gateway that will forward data packets to the IOLAN (if required). The router/gateway must reside on the same subnet at the remote VPN. Field Format: IPv4 or IPv6 address
Remote Host/Network Address	The IP address of a specific host or the network address that the IOLAN will provide a VPN connection to. If the IPsec tunnel is listening for connections (Boot Action set to Add), and the field value is left at 0.0.0.0, any VPN peer with a private remote network/host that conforms to RFC 1918 (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) will be allowed to use this tunnel if it successfully authenticates. Field Format: IPv4 or IPv6 address
Remote IPv4 Subnet Mask	The subnet mask of the remote IPv4 network. Keep the default value when you are configuring a host-to-host VPN connection. Default: 255.255.255.255
Remote IPv6 Prefix Bits	The prefix bits of the remote IPv6 network. Keep the default value when you are configuring a host-to-host VPN connection. Default: 0

Boot Action	<p>Determines the state of the VPN network when the IOLAN is booted.</p> <p>Data Options:</p> <ul style="list-style-type: none"> • Start—Starts the VPN network, initiating communication to the remote VPN. • Add—Adds the VPN network, but doesn't initiate a connection to the remote VPN. • Ignore—Maintains the VPN network configuration, but the VPN network is not started and cannot be started through the IPsec command option. <p>When defining peer VPN gateways, one side should be defined as Start (initiate) and the other as Add (listen). It is invalid to define both gateways as Add. VPN connection time can take longer when both gateways are set to Start, as both sides will attempt to initiate the same VPN connection.</p> <p>Default: Start</p>
--------------------	--

Shared Secret Field Description

When the **Authentication Method** is set to **Shared Secret**, you can enter a secret that applies to all VPN tunnels (both the IPsec and L2TP/IPsec protocols) to successfully authenticate and create a valid connection.

Secret	<p>When the Authentication Method is set to Shared Secret, enter the case-sensitive secret word. This applies to all VPN tunnels (IPsec and L2TP/IPsec).</p> <p>Field Format: Maximum of 16 characters, spaces not allowed</p>
---------------	---

Remote Validation Criteria Field Descriptions

When the **Authentication Method** is set to **X.509 Certificate**, you can configure the remote validation criteria. The information in the remote X.509 certificate must match exactly the information configured in this window in order to successfully authenticate and create a valid connection. If using an asterisk(*) for wildcard matching the Boot Action must be set to **Add** (Listen).

IPsec Authentication Parameters

Country	<p>A country code; for example, US. This field is case sensitive in order to successfully match the information in the remote X.509 certificate.</p> <p>Data Options: Two characters, If using an asterisk (*) for wildcard matching, the Boot Action must be set to Add (Listen).</p>
State/Province	<p>An entry for the state/province; for example, IL. This field is case sensitive in order to successfully match the information in the remote X.509 certificate.</p> <p>Data Options: Maximum 128 characters, If using an asterisk (*) for wildcard matching, the Boot Action must be set to Add (Listen).</p>
Locality	<p>An entry for the location; for example, Chicago. This field is case sensitive in order to successfully match the information in the remote X.509 certificate.</p> <p>Data Options: Maximum 128 characters, If using an asterisk(*) for wildcard matching, the Boot Action must be set to Add (Listen).</p>
Organization	<p>An entry for the organization; for example, Accounting. This field is case sensitive in order to successfully match the information in the remote X.509 certificate.</p> <p>Data Options: Maximum 64 characters, If using an asterisk(*) for wildcard matching the Boot Action must be set to Add (Listen).</p>

Organization Unit	<p>An entry for the unit in the organization; for example, Payroll. This field is case sensitive in order to successfully match the information in the remote X.509 certificate.</p> <p>Data Options: Maximum 64 characters, If using an asterisk (*) for wildcard matching, the Boot Action must be set to Add (Listen).</p>
Common Name	<p>An entry for common name; for example, the host name or fully qualified domain name. This field is case sensitive in order to successfully match the information in the remote X.509 certificate.</p> <p>Data Options: Maximum 64 characters, If using an asterisk (*) for wildcard matching, the Boot Action must be set to Add (Listen).</p>
Email	<p>An entry for an email address; for example, acct@anycompany.com. This field is case sensitive in order to successfully match the information in the remote X.509 certificate.</p> <p>Data Options: Maximum 64 characters, If using an asterisk (*) for wildcard matching, the Boot Action must be set to Add (Listen).</p>

L2TP/IPsec

In order to create a VPN tunnel on Windows XP®, you must use the L2TP/IPsec protocol. When L2TP/IPsec is enabled, the IOLAN will listen for L2TP/IPsec VPN tunnel requests.

When you enable L2TP/IPsec, you are requiring that all access to the IOLAN go through the L2TP/IPsec tunnel, so you must configure any exceptions first see ([L2TP/IPsec Exceptions](#)) for more information on exceptions) or you will not be able to access the IOLAN through the network unless you are configured to go through the L2TP/IPsec tunnel (you can still access the IOLAN through the Console port).

L2TP/IPsec Authentication Parameters

Allow L2TP/IPsec connections	<p>When enabled, the IOLAN listens for L2TP/IPsec VPN tunnel connections. Note: to allow non-VPN tunnel connections to the IOLAN, you must create entries in the VPN Exceptions list.</p> <p>Default: Disabled</p>
Local IP Address	<p>If the IPsec local address is set to 0.0.0.0, the IOLAN will listen for L2TP/IPsec connections on (the IP address of) the network interface associated with (ie: on the same network as) the IOLAN's default gateway. If no default gateway exists, the IOLAN will not listen for L2TP/IPsec connections.</p> <p>Default: 0.0.0.0</p>
Authentication Method	<p>Specify the authentication method that will be used between VPN peers to authenticate the VPN tunnel.</p> <p>Data Options:</p> <ul style="list-style-type: none"> • Shared Secret—A text-based secret that is used to authenticate the IPsec tunnel (case sensitive). • X.509 Certificate—X.509 certificates are used to authenticate the IPsec tunnel. When using this authentication method, you must include the signing authority's certificate information in the SSL/TLS CA list and download it to the IOLAN. <p>Default: Shared Secret</p>

Remote Validation Criteria	<p>Shared Secret—Specify the text-based secret that is used to authenticate the IPsec tunnel (case sensitive). This applies to all VPN tunnels (IPsec and L2TP/IPsec).</p> <p>X.509 Certificate—Specify the remote X.509 certificate validation criteria that must match for successful authentication (case sensitive). Note that all validation criteria must be configured to match the X.509 certificate. If using an asterisk (*) for wildcard matching, the Boot Action must be set to Add (Listen).</p> <p>See Shared Secret Field Description for more information.</p> <p>See Remote Validation Criteria Field Descriptions or more information on the X.509 certificate validation criteria.</p>
IPv4 Local IP Address	<p>Specify the unique IPv4 address that hosts accessing the IOLAN through the L2TP tunnel will use.</p> <p>Field Format: IPv4 address</p>
IPv4 Remote IP Start Address	<p>Specify the first IPv4 address that can be assigned to incoming hosts through the L2TP tunnel.</p> <p>Field Format: IPv4 address</p>
IPv4 Remote IP End Address	<p>Specify the end range of the IPv4 addresses that can be assigned to incoming hosts through the L2TP tunnel.</p> <p>Field Format: IPv4 address</p>
Authentication	<p>Specify the authentication method that will be used for the L2TP tunnel.</p> <p>Data Options: CHAP, PAP, Both</p> <p>Default: Both</p>

L2TP/IPsec Exceptions

Exceptions allow specific hosts or any host in a network to access the IOLAN outside of a VPN tunnel. This is especially useful when allowing local network hosts access to the IOLAN when VPN tunnels have been configured for remote user security.

Adding/Editing a VPN Exception

IP Address	<p>The IP address of the host that will communicate with the IOLAN outside of the VPN tunnel.</p> <p>Field Format: IPv4 or IPv6 address</p>
Network	<p>The network address that will communicate with the IOLAN outside of the VPN tunnel.</p> <p>Field Format: IPv4 or IPv6 address</p>
IPv4 Subnet Mask	<p>The IPv4 subnet mask for the IPv4 network.</p> <p>Default: 0.0.0.0</p>
IPv6 Prefix Bits	<p>The IPv6 prefix bits for the IPv6 network.</p> <p>Range: 0-128</p> <p>Default: 0</p>

VPN Authentication Parameters

Use NAT Traversal (NAT_T) NAT Traversal should be enabled when the IOLAN is communicating through a router/gateway to a remote VPN that also has NAT Traversal enabled.
Default: Enabled

HTTP Tunneling

A HTTP tunnel is a firewall-safe communication channel between two IOLAN's. HTTP tunnels can transport arbitrary TCP/IP or UDP/IP data for applications such as Telnet/SSH or any other TCP application and most UDP applications.

You can configure the IOLAN for:

- a serial-to-serial HTTP tunnel connection
- a serial-to-host HTTP tunnel connection
- a host-to-host HTTP tunnel connection
- Tunnel Relay connection

See [Configuring a HTTP Tunnel](#) for more information on setup requirements for these scenarios.

The information in this section applies only to setting up HTTP tunnels.

A minimum of two IOLAN's must be configured to create a communication channel. One IOLAN must be configured as the listener and the other IOLAN must be configured as the connecting IOLAN.

Configuring a HTTP Tunnel

Name	Provide a name for this tunnel. This name must match the tunnel name on the tunnel peer IOLAN DS.
Connect to	Provide the Host name or IP address of the listening IOLAN.
Proxy Settings	If a proxy server is being used, allows for the configuration of proxy specific parameters.
Listen for Connections	Listen for connection requests generated from the connecting IOLAN.
Restrict to IP	Only accept connection requests from this IP address
Shared Secret	If a secret is defined, then both sides of the tunnel must set the same secret. A secret is used to ensure that the Tunnel is being established with the correct peer.
HTTPS	When enabled, secure access mode (HTTPS) will be used to establish the tunnel.
Restrict Access to this IOLAN only	If enabled, tunnel connections will only be allowed to access local devices (serial ports) on this IOLAN. Connection requests going to external IP hosts on the local LAN will be not allowed.

Note: HTTPS mode requires that the **SSL Passphrase** is already defined in the IOLAN configuration and the SSL/TLS certificate/private key and CA list must have already been downloaded to the IOLAN.

Configuring HTTP Tunnel Proxy

Proxy servers are used in larger companies and organizations. Ask your network administrator if you need to configure a Proxy server.

Use HTTP Proxy Enables the Proxy parameters.

Host/IP The Host name or IP address of the Proxy server.

Port The HTTP/HTTPS port number of the Proxy server. Default: 8080.

Username The "username" which will be used by the Terminal Server to authenticate with the proxy server (if authentication is required by the proxy server).

Password The "password" which will be used by the Terminal Server to authenticate with the proxy server (if authentication is required by the proxy server).

Domain This field is only used if authentication is needed with the proxy server. If the proxy server does not expect this field, it can be left blank.

Note: We support the following types of authentication; Local Windows account authentication (clear text, SPA) and Digest authentication (MD5).
Ensure that your Proxy Server does not restrict HTTP-CONNECT messages to port 443 and allows HTTP-CONNECT messages on Port 80

Configuring HTTP Tunnel Proxy Advanced

Keepalive Interval The number of seconds between sending keep-alives for HTTP connections. Keep-alives are used to prevent idle connections from closing. In most cases this value does not need to be changed.
Default: 30 seconds

Maximum Connection Age The maximum amount of time an HTTP connection will stay open in minutes. In most cases this value does not need to be changed.
Default: 1440 mins. (1 day).

Configuring HTTP Tunnel Destination

Configure the following parameters if host access via a tunnel is needed. Each entry in the list box defines the application and port numbers an external client will use to access the destination host or application.

Tunnel Select the HTTP tunnel to use for this connection

Destination The address of an external host on the peer IOLAN's LAN. If the destination is a serial port on the Peer IOLAN or the peer IOLAN itself, select "Same as Tunnel".

Add new Services Select either predefined services or custom services.

Predefined Services Select the service or services required. For predefined services, you must specify an alias local IP address which will be used by the external host to access the service.

Custom Services	Selecting custom services allows you to enter in a custom application configuration. Select either TCP or UDP.
Local Port	The listening TCP/IP or UDP/IP port. This is the port the local host will be using.
Destination Port	The port number used by the destination host or destination application.
Local IP Alias	Users can access the HTTP tunnel through this IP address. Typically this field is only needed if the IOLAN has a listener on the same local TCP port. If not entered, the IP address of the IOLAN is used.
Limited access to attached serial devices only	Limit Access To Serially Attached Devices Only Allow only attached serial devices to connect to this destination.
Add button	Acts like an “apply” button.
Delete button	Highlight an HTTP Tunnel Destination entry and select the Delete button to remove the entry from the list.

Note: When HTTP tunneling is used TCP and UDP ports 50,000 and above are reserved and should not be configured by the user.

Network Services

Services and Daemons are based on your IOLAN model. Network services can be enabled and disabled.

Enable/Disable Services

Telnet Server	Telnet daemon process in the IOLAN listening on TCP port 23. Default: Enabled
TruePort Full Mode	The TruePort daemon process in the IOLAN that supports TruePort Full Mode on UDP port 668. You can still communicate with the IOLAN in Lite Mode when this service is disabled. Default: Enabled
Syslog Client	Syslog client process in the IOLAN. Default: Enabled
Modbus	Modbus daemon process in the IOLAN listening on port 502. Default: Enabled
SNMP	SNMP daemon process in the IOLAN listening on UDP port 161 and sending traps on UDP port 162. Default: Enabled
DeviceManager	DeviceManager daemon process in the IOLAN. If you disable this service, you will not be able to connect to the IOLAN with the DeviceManager application. The DeviceManager listens on port 33812 and sends on port 33813. Default: Enabled

WebManager (HTTP)	WebManager daemon process in the IOLAN listening on port 80. Default: Enabled
WebManager (HTTPS)	Secure WebManager daemon process in the IOLAN listening on port 443. Default: Enabled If you are using the WebManager in secure mode (HTTPS), you need to download the SSL/TLS private key and certificate to the IOLAN. You also need to set the SSL Passphrase parameter with the same password that was used to generate the key. See ESP Phase 2 Proposals for more information.
SSH Server	SSH daemon process in the IOLAN listening on TCP port 22. Default: Enabled
NTP/SNTP Client	Simple Network Time Protocol client process in the IOLAN. NTP/SNTP client listens on UDP port 123. Default: Enabled
Dynamic Routing (RIP)	Dynamic Routing daemon process in the IOLAN listening on port 520/521. Default: Enabled
IPsec	IPsec daemon process in the IOLAN listening and sending on UDP port 500. Default: Disabled

Note: TCP ports 2601, 2602 and 2603 are used internally by the IOLAN.

Network Filtering

Allow Ping Responses By default the IOLAN will respond to pings.
Default: Enabled

Keys and Certificates

When you are using SSH, SSL/TLS, LDAP/Microsoft Active Directory, or HTTPS, you will need to install keys and/or certificates or get server keys in order to make those options work properly. All certificates need to be created and all keys need to be generated outside of the IOLAN, with the exception of the IOLAN SSH Public keys, which already exist in the IOLAN SSH keys must be generated using the OpenSSH format.

Certificate Authorities (CAs) such as Verisign, COST, GTE CyberTrust, etc. can issue certificates. Or, you can create a RSA or DSA self-signed certificate using a utility such as OpenSSL.

To download or keys, a certificate, or a CA list or to upload the IOLAN public SSH key, select **Administration, Keys and Certificates**.

Keys and Certificate Parameters

Key / Certificate	<p>Select the key or certificate that you want to download to the IOLAN or upload the Management Module's SSH Public Key.</p> <p>Data Options:</p> <ul style="list-style-type: none">• Upload Server SSH Public Key, used for SSH management access• Download SSH User Public Key, used for SSH management access• Download SSL/TLS Private Key, required if using HTTPS and/or SSL/TLS• Download SSH Host Public Key, required if using SSH• Download SSL/TLS Private Key, required if using SSL/TLS• Download SSL/TLS Certificate, required if using HTTPS and/or SSL/TLS• Upload IPsec RSA Public Key, required if using X.509 certification authentication for an IPsec tunnel• Download IPsec RSA Public Key, required if using X.509 certification authentication for an IPsec tunnel• Download SSL/TLS CA, required if using LDAP/Microsoft Active Directory with TLS, SSL/TLS, and/or X.509 certificate authentication for an IPsec tunnel• Download NTP/SNTP Keys File, required if using NTP/SNTP server authentication
File Name	The file that you are going to download/upload to/from the IOLAN via TFTP.
Key Type	<p>Specify the type of authentication that will be used for the SSH session. The following list details the keys that support each key type.</p> <p>Data Options:</p> <ul style="list-style-type: none">• RSA—Server SSH Public Key, SSH User Public Key, SSH User Private Key, SSH Host Public Key• DSA—Server SSH Public Key, SSH User Public Key, SSH User Private Key, SSH Host Public Key
User Name	The name of the user for whom you are downloading the SSH User Public or Private Key to the IOLAN.
Host Name	The name of the host for which you are downloading the SSH Host Public or Private Key to the IOLAN.
IPsec Tunnel Name	Select the IPsec tunnel that the RSA public key is being used to authenticate.

Clustering

Clustering is a way to provide access to the serial ports of many IOLANs through a single IP address. The IP address that will be used to access all clustered serial ports will be that of the Master IOLAN in the cluster. All other IOLANs in the cluster will be referred to as Slave IOLANs. Users can also access slave serial ports using EasyPort Web; EasyPort Web is automatically launched when a user types in the IP address of the Master IOLAN in a web browser. If the user has Admin privileges, the WebManager will first be displayed with an option to proceed to EasyPort Web.

The **Clustering Slave List** window displays the slave IOLAN entries and the number of ports on those slave IOLANs.

Note: No special configuration is required on the Slave IOLANs to enable this functionality.

Adding Clustering Slaves

When you add a clustering slave IOLAN entry, you are adding the IOLAN that users will access through this master IOLAN.

Clustering Parameters

Server Name	Specify a name for the slave IOLAN in the clustering group. This name does not have to correspond to the proper host name, as it is just used within the IOLAN. Field Format: Maximum 15 alphanumeric characters, including spaces
IP Address	Specify the IP address of the slave IOLAN in the clustering group. Field Format: IPv4
Number of Ports	Specify the number of ports in the Slave IOLAN that you are adding to the clustering group. Data Options: 1, 2, 4, 8, 16, 24, 36, 48 Default: 1
Starting Slave TCP Port	Specify the first TCP Port number (as specified in the slave IOLAN's serial port configuration) on the slave host. Default: 10001, and increments by one for each serial port
Starting Master TCP Port	Specify the TCP port number you want to map the first slave IOLAN DS Port number to. This number should not be a port number that is already in use by the master IOLAN. Default: 1024, and then increments by one for each new slave entry
Protocol	Specify the protocol that will be used to access the slave IOLAN port. Data Options: SSH, Telnet Field Format: Telnet

Advanced Clustering Slave Options

The **Advanced** button provides a means of configuring each individual serial port's name, connection protocol, and port association in the clustered IOLAN slave. The **Clustering Slave Settings** window displays each clustered serial port slave entry, you need to select the **Edit** button to configure the individual serial port settings.

If you select the **Retrieve Port Names** button, the DeviceManager will connect to the clustering slave IOLAN and download all the serial port names--you can change the names and other settings when you select the **Edit** button.

Editing Clustering Slave Settings

Port Name	Specify a name for the port. Default: A combination of the port number, the @ symbol, and the IP address; for example, <code>port1@172.22.23.101</code> .
Slave TCP Port	Specify the TCP Port number configured on the Slave IOLAN that is associated to the port number you are configuring. Range: 1-99999
Master TCP Port	Specify the TCP port number you want to map to the Slave IOLAN TCP Port. User's will use this TCP port number to access the Slave IOLAN's port. Default: 1024, and then increments by one for each new slave entry
Protocol	Specify the protocol that will be used to access the port. Data Options: SSH, Telnet Default: Telnet

Alerts

This chapter describes the alerts (email and syslog) that can be configured for the IOLAN and the advanced options (SNMP, time, custom applications/plugins, and other miscellaneous configuration options) that you will want to look at to see if they are required for your implementation.

Email Alerts

Email notification can be set at the Server and/or Line levels. You can set email notification at these levels because it is possible that the person who administers the IOLAN might not be the same person who administers the serial device(s) attached to the IOLAN port. Therefore, email notification can be sent to the proper person(s) responsible for the hardware.

Email notification requires an SMTP host that is accessible by the IOLAN to process the email messages sent by the IOLAN. When you enable email notification at the Server level, you can also use those settings at the serial port level, or you can configure email notification specifically for each serial port. When you choose an event **Level**, you are selecting the lowest notification level; for example, if you select **Level Error**, you will get notifications for all events that trigger **Error**, **Critical**, **Alert**, and **Emergency** messages. The level order, from most inclusive to least inclusive, is as follows: Debug, Info, Notice, Warning, Error, Critical, Alert, Emergency.

The following events trigger an email notification on the **System** for the specified **Level**:

- Reboot, Alert Level
- IOLAN System Failure, Error Level
- Authentication Failure, Notice Level
- Successful Login, Downloads (all), Configuration Save Commands, Info Level

Email Alert Parameters

Enable Email Alert	Enables/disables a global email alerts setting. Even if this option is disabled, you can still configure individual serial port email alerts. When this option is enabled, individual serial ports can inherit these email alerts settings. Default: Disabled
Level	Choose the event level that triggers an email notification. Data Options: Emergency, Alert, Critical, Error, Warning, Notice, Info, Debug Default: Emergency
To	An email address or list of email addresses that will receive the email notification.
Subject	A text string, which can contain spaces, that will display in the Subject field of the email notification.
From	This field can contain an email address that might identify the IOLAN name or some other value.
Reply To	The email address to whom all replies to the email notification should go.
Outgoing Mail Server	The SMTP host (email server) that will process the email notification request. This can be either a host name defined in the IOLAN host table or the SMTP host IP address.
HTTP Tunnel	Specify the HTTP tunnel to be used for this connection.

Username	If your mail server requires you to authenticate with it before it will accept email messages, use this field to configure the authorized user name. Maximum size of user name is 64 characters.
Password	Enter the password associated with the user configured in “Username”. Maximum size of password is 64 characters.
Encryption	Choose the type of encryption. Valid options are: None - All information is sent in the clear SSL - Select this if your email server requires SSL TLS - Select this if your email server requires TLS
Verify Peer Certificate	When checked this will enable the validation of the certificate presented by the email server. To validate the certificate, you will need to download the appropriate CA list into the IOLAN. If the certificate is not found to be valid, the communication with the email server will be terminated. No authentication will take place and the email message will not be forwarded to the email server. If this option is not checked, the certificate validation will still be attempted but if it fails, a syslog message will be generated but the authentication and forwarding of the email will still take place. Default: Enabled if SSL or TLS encryption is selected. Disabled if no encryption is selected.
TCP Port	This is the TCP port used to communicate with the email server. Default: 25 for non-SSL, 465 if SSL/TLS is used
NTLM Domain	This field is only used if SPA authentication is performed with the email server. It may or may not be required. If the email server does not expect this field, it can be left blank.

Syslog

The IOLAN can be configured to send system log messages to a syslog daemon running on a remote host if the **Syslog** service is activated. You can configure a primary and secondary host for the syslog information and specify the level for which you want syslog information sent.

Note: You must ensure that the **Syslog Client** service in the **Security, Services** window is enabled (by default it is enabled) for these settings to work.

Syslog Parameters

Primary Host	The first preconfigured host that the IOLAN will attempt to send system log messages to; messages will be displayed on the host’s monitor. Default: None
Secondary Host	If configured, the IOLAN will attempt to send system log messages to this syslog host as well as the primary syslog host defined. Messages will be displayed on the host’s monitor. Default: None

HTTP Tunnel	Specify the HTTP tunnel to be used for this connection.
Level	Choose the event level that triggers a syslog entry. Data Options: Emergency, Alert, Critical, Error, Warning, Notice, Info, Debug Default: Emergency

Management

If you are using SNMP to manage/configure the IOLAN, or to view statistics or traps, you must set up a User in SNMP version 3 or a Community in SNMP version 1,2 to allow your SNMP manager to connect to the IOLAN; this can be done in the DeviceManager, WebManager and CLI. You must then load the perle-sds.MIB (found on the Perle website at www.perle.com) file into your SNMP manager before you connect to the IOLAN.

Note: Ensure that the **SNMP** service found in the **Security, Services** page is enabled (by default it is enabled).

SNMP Parameters

Contact	The name and contact information of the person who manages this SMNP node.
Location	The physical location of the SNMP node.
Community	The name of the group that devices and management stations running SNMP belong to. Community only applies to SNMP v1 and v2c.
Internet Address	The IP address of the SNMP manager that will send requests to the IOLAN. If the address is 0.0.0.0, any SNMP manager with the Community name can access the IOLAN. If you specify a network address, for example 172.16.0.0, any SNMP manager within the local network with the Community name can access the IOLAN. Field Format: IPv4 or IPv6 address
Permissions	Permits the IOLAN to respond to SNMP requests. Data Options: <ul style="list-style-type: none"> • None—There is no response to requests from SNMP. • Readonly—Responds only to Read requests from SNMP. • Readwrite—Responds to both Read and Write requests from SNMP. Default: None
V3 Read-write User	This user can view and edit SNMP variables.
V3 Read-Write Security Level	Select the security level for the Read-Writer user. This must match the configuration set up in the SNMP manager. Data Options: <ul style="list-style-type: none"> • None—No security is used. • Auth—User authentication is used. • Auth/Priv—User authentication and privacy (encryption) settings are used. Default: None

V3 Read-Write Auth Algorithm	Specify the authentication algorithm that will be used for the read-write user. Data Options: MD5, SHA Default: MD5
V3 Read-Write Auth Password	Type in the read-write user's authentication password.
V3 Read-Write Confirm Password	Retype the user's authentication password.
V3 Read-Write Privacy Algorithm	Specify the read-write user's privacy algorithm (encryption). Data Options: DES, AES Default: DES
V3 Read-Write Privacy Password	Type in the read-write user's privacy password.
V3 Read-Write Confirm Password	Retype the privacy password.
V3 Read-Only User	This user can only read SNMP variables.
V3 Read-Only Security Level	Select the security level for the Read-Only user. This must match the configuration set up in the SNMP manager. Data Options: <ul style="list-style-type: none"> • None—No security is used. • Auth—User authentication is used. • Auth/Priv—User authentication and privacy (encryption) settings are used. Default: None
V3 Read-Only Auth Algorithm	Specify the authentication algorithm that will be used for the read-only user. Data Options: MD5, SHA Default: MD5
V3 Read-Only Auth Password	Type in the read-only user's authentication password.
V3 Read-Only Confirm Password	Retype the user's authentication password.
V3 Read-Only Privacy Algorithm	Specify the read-only user's privacy algorithm (encryption). Data Options: DES, AES Default: DES
V3 Read-Only Privacy Password	Type in the read-only user's privacy password.
V3 Read-Only Confirm Password	Retype the privacy password.

SNMP Trap Parameters

Trap checkbox	Check this box to enable the entry of the trap information.
----------------------	---

IP Address	<p>The IP address of the SNMP manager(s) that will receive messages from the IOLAN.</p> <p>Field Format: IPv4 or IPv6 address</p>
Trap Version	<p>Select the version of trap you want the IOLAN to send. Valid options are v1, v2c or v3.</p> <p>Default: v1</p>
Trap Type	<p>Select between Trap and Inform. Inform requires the host receiving the trap to acknowledge the receipt of the trap.</p>
Community	<p>The name of the group that devices and management stations running SNMP belong to. Community only applies to SNMP v1 and v2c</p>
HTTP Tunnel	<p>Specify the HTTP tunnel to be used for this connection.</p>
Timeout	<p>This is only used for Inform traps. Select the number of seconds to wait for the acknowledgment of the trap.</p> <p>Default: 1 second</p>
Retries	
V3 Trap User	<p>This field identifies the system sending the traps to the host receiving the traps. Same user name is used for all traps sent by this system.</p>
V3 Trap Security Level	<p>Select the security level for the V3 traps. This must match the configuration set up in the SNMP manager.</p> <p>Data Options:</p> <ul style="list-style-type: none"> • None—No security is used. • Auth—Trap authentication is used. • Auth/Priv—Trap authentication and privacy (encryption) settings are used. <p>Default: None</p>
V3 Trap Auth Algorithm	<p>Specify the authentication algorithm that will be used for the read-only user.</p> <p>Data Options: MD5, SHA</p> <p>Default: MD5</p>
V3 Trap Auth Password	<p>Type in the password associated with traps sent from this host.</p>
V3 Trap Confirm Password	<p>Re-enter the password associated with traps sent from this host.</p>
V3 Trap Privacy Algorithm	<p>Specify the privacy algorithm (encryption) which will be used with traps.</p> <p>Data Options: DES, AES</p> <p>Default: DES</p>
V3 Trap Privacy Password	<p>Type in the password associated with the encryption method being used for traps.</p>
V3 Trap Confirm Password	<p>Re-type the password associated with the encryption method being used for traps.</p>

V3 EngineID	This is the current engine ID. The Engine ID is a string which uniquely identifies this SNMP agent.
V3 Use Default EngineID	When this field is selected, the firmware will use the default Engine ID. The default Engine ID is the MAC address of the Ethernet interface to ensure that the Engine ID is unique to this agent.
V3 Create EngineID Using String	The string entered in this field will be combined with the defined string in hex of 800007AE04 to form the Engine ID. Ensure each string is unique for each IOLAN on your network.

Custom App/Plugin

You can create custom applications for the IOLAN by using the Perle SDK. See the *SDK Programmer's Guide* (the SDK and guide are accessible via a request form located on the Perle website at www.perle.com/supportfiles/SDK_Request.shtml) for information about the functions that are supported. You must download the program and any ancillary files to the IOLAN and set the **Serial Port Profile** to **Custom App/Plugin** to run a custom application. You must also specify the program executable in the **Command Line** parameter.

A custom application or plugin can be run on the serial port. In this situation, the application will start once the serial port is activated and operate solely on the context of that serial port and any network communications related to that serial port. You could run a different custom application on each serial port. The serial port custom application or plugin is configured by specifying the **Custom App/Plugin** profile for the serial port.

The system level custom application or plugin will begin execution immediately following the system startup. It runs on the context of the whole system and can access network communications as well as any or all serial ports.

Custom App Parameters

Command Line	<p>The name of the application that has been already been downloaded to the IOLAN, plus any parameters you want to pass to the program. For example, using sample <code>outraw</code> program (this is sample program supplied with the SDK), you would type:</p> <pre>outraw -s 0 192.168.2.1:10001 Acct:10001</pre> <p>if you were starting the application on the Server (notice the <code>-s 0</code> parameter specifies serial port 1 to this particular application).</p> <p>Field Format: Maximum of 80 characters</p>
---------------------	---

Front Panel (only applies to certain models)

Customize status menu order	Allows the user to choose what statuses are displayed on the front panel display and in what auto scrolling order.
Enable status auto-scroll	<p>When enabled, the auto scroll feature on the front panel will scroll using the idle timeout and scroll delay options.</p> <p>Default: Enabled</p>

Idle Timeout	The time the front panel display will wait before auto scrolling after no key has been pressed on the front panel display. Default: 300 seconds
Scroll Delay	The length of time each status is displayed for. Default: 5 seconds
Custom Text	Custom text may be entered here and is displayed on the front panel display. Default: Perle Systems Ltd. IOLAN SCG
Keypad Locked	When the keypad has been locked, there is no access from the front panel display.
Enable Pin	When a pin is enabled, the user will be prompted to enter this pin when accessing the Configuration and Administration menus on the front panel display.
Pin	A minimum password of 6 numbers must be entered.

Hardware (only applies to certain models)

When connected to an IOLAN, the current hardware installed will be displayed. For off-line configurations, you will be able to select your model type, number of port cards and serial interface on each of the port cards (RS232 or USB).

Advanced Options

Review the configuration options in the Advanced page to determine if any of them apply to your implementation.

Login Settings

Use System Name in Prompts Displays the **System Name** field value instead of default product name. When enabled, the **Server Name** is displayed in the IOLAN login prompt, CLI prompt, and WebManager login screen.
Default: Disabled

Display Login Banner This parameter concerns the banner information (product name/software version). This banner information is presented to a user with a login prompt. For security reasons, you can turn off the display of this information.
Default: Disabled

Use Custom Login Prompt When set, and a custom language file is in use, the login prompt and password prompt will use the string defined in the language file as the login prompt and password prompt instead of the default prompt,
login:
password:
Default: Disabled

Bypass Login Password	When set, authorized users who do not have a password set, with the exception of the admin user, WILL NOT be prompted for a password at login with Local Authentication . Default: Disabled
Use a Generic WebManager Login Screen	When set, and the user connects to the IOLAN using WebManager, the WebManager login screen that is displayed is generic — the Perle banner, IOLAN model name, and firmware version are not displayed to the user. Default: Disabled
Password Retry Limit	The number of attempts a user is allowed to enter a password for a serial port connection from the network, before the connection is terminated and the user has to attempt to login again. For users logging into the serial port, if this limit is exceeded, the serial port is disabled for 5 minutes. A user with Admin level rights can restart the serial port, bypassing the timeout, by issuing a kill on the disabled serial port. Default: 3
EasyPort Web	Select Java if communication is via port 23(Telnet) or port 22(SSH) and the IOLAN is not restricted by a firewall. Select Javascript if you need to communicate through a firewall on port 8080 using EasyPort Web.
Disable Caching	When this option is selected, the Web Manager will no longer cache web pages. Default: Caching

Bootup Files

You must have a SFTP/TFTP server running on any host that you are downloading files from. When you specify the file path, the path must be relative to the default path set in your SFTP/TFTP server software.

Bootup File Parameters

Firmware Host	The host name or IP address of the server that contains the firmware file. If you use a host name, it must exist in the IOLAN's host table or be resolved by DNS. Field Format: Resolvable host name, IPv4 address, IPv6 address
Firmware File	The path and file name, relative to the default path of your TFTP server software, of the update software for the IOLAN that will be loaded when the IOLAN is rebooted.
Firmware, Use SFTP	Check this box if you wish to use SFTP (Secure File Transfer Protocol) instead of TFTP (Trivial File Transfer Protocol). The IOLAN will use the SFTP server information entered under the SFTP tab.
Configuration Host	The host name or IP address of the server that contains the configuration file. If you use a host name, it must exist in the IOLAN's host table or be resolved by DNS. Field Format: Resolvable host name, IPv4 address, IPv6 address

Configuration File	The path and file name, relative to the default path of your TFTP server software, of the configuration file for the IOLAN that will be loaded when the IOLAN is rebooted.
---------------------------	--

Configuration, Use SFTP	Check this box if you wish to use SFTP (Secure File Transfer Protocol) instead of TFTP (Trivial File Transfer Protocol). The IOLAN will use the SFTP server information entered under the SFTP tab.
--------------------------------	---

Message of the Day (MOTD)

The message of the day is displayed when users log into the IOLAN through a telnet, a SSH session or through WebManager/EasyPort Web.

There are two ways to retrieve the message of the day to be displayed to users when they log into the IOLAN:

- The message of the day file is retrieved from a SFTP/TFTP server every time a user logs into the IOLAN. You must have a SFTP/TFTP server running on any host that you are uploading or downloading files to/from when using TFTP. When you specify the file path, the path must be relative to the default path set in your SFTP/TFTP server software.
- The message of the day file is downloaded to the IOLAN and retrieved locally every time a user logs into the IOLAN. You can download an MOTD file to the IOLAN in the DeviceManager by selecting **Tools, Advanced, Custom Files** and then selecting the **Download Other File** option and browse to the MOTD file. In WebManager, select **Administration, Custom Files** and select the **Other File** option and browse to the MOTD file. After the MOTD is downloaded to the IOLAN, you must specify the MOTD file name in the **Filename** field to access it as the message of the day (no **SFTP/FTP Host** parameter is required when the file is internal).

MOTD Parameters

TFTP Host	The host that the IOLAN will be getting the Message of the Day file from. Field Format: Resolvable host name, IPv4 address, IPv6 address.
------------------	---

Filename	The path and file name, relative to the default path of your TFTP server software, of the file that contains a string that is displayed when a user connects to the IOLAN. The IOLAN will look for the file internally (it must already be downloaded), if only the file is specified (no TFTP host) or the file cannot be found on the specified TFTP host.
-----------------	--

HTTP Tunnel	Specify the HTTP tunnel to be used for this connection.
--------------------	---

Use SFTP	Check this box if you wish to use SFTP (Secure File Transfer Protocol) instead of TFTP (Trivial File Transfer Protocol). The IOLAN will use the SFTP server information entered under the SFTP tab.
-----------------	---

Display MOTD in WebManager/ EasyPort Web	When enabled, displays the Message of the Day to users who are logging into WebManager or EasyPort Web. Default: Disabled
---	---

TFTP

You must have a TFTP server running on any host that you are uploading or downloading files to/from.

Note: TFTP file transfers send via UDP packets. When the packet delivery is interrupted for any reason and a timeout occurs, that packet is resent if the retry count allows it. Therefore, if a very large file is being transferred and is interrupted, the entire file is not resent, just the part of the file that was not received.

TFTP Parameters

Retry	The number of times the IOLAN will retry to transmit a TPFT packet to/from a host when no response is received. A value of 0 (zero) means that the IOLAN will not attempt a retry should TFTP fail. Range: 0-5 Default: 5
Timeout	The time, in seconds, that the IOLAN will wait for a successful transmit or receipt of TFTP packets before retrying a TFTP transfer. Range: 3-10 Default: 3 seconds
FTP Host	Select the host entry from the IOLANs host table which corresponds to the FTP server.
HTTP Tunnel	Specify the HTTP tunnel to be used for this connection.

Control RPS, IPsec, WLAN and WWAN

The Control section appears when the IOLAN is connected to a Remote Power Switch and/or, an IPsec tunnel is configured or you have configured a WLAN/WWAN interface.

RPS Control

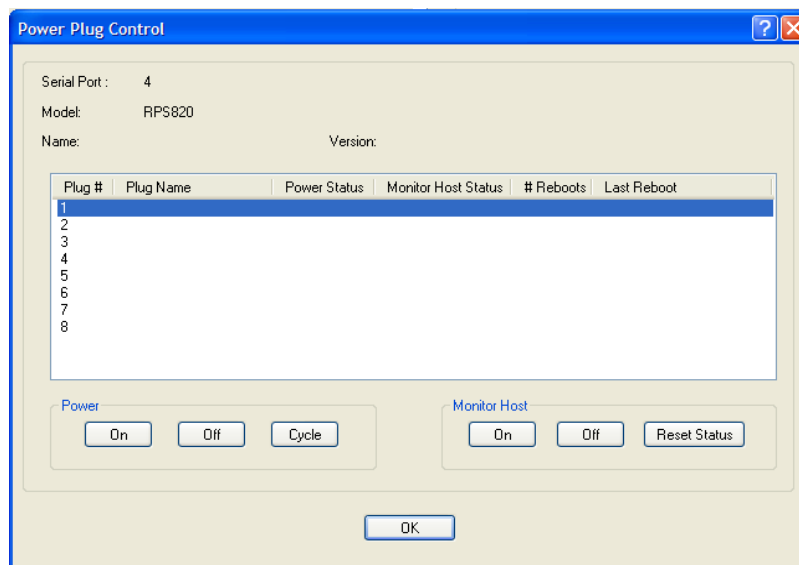
When a Remote Power Switch's (RPS) console port is attached to the IOLAN's serial port and the serial port is configured for the Power Management profile, you will be able to control the RPS's power plugs either universally or individually (power on/off the whole RPS or individual plugs).

The following buttons are available:

- | | |
|-------------------------------|--|
| On | Turns all the RPS plugs on. |
| Off | Turns all the RPS plugs off. |
| Cycle | Turns all the RPS plugs off and then on. |
| Reset to Default State | Resets all the RPS plugs to the default state as configured in the Power Management profile settings. |
| Plug Control | Displays a window that allows you to manage the individual plugs on the RPS. |

Plug Control

When you select the **Plug Control** button, you can power on/off individual plugs.



The "**Power Status**" field above can contain the following values;

- **On** - Power is currently being applied to the plug.
- **Off** - Power is currently not being applied to the plug.

The "**Monitor Host Status**" field above can contain the following values;

- **Disabled** - Feature is currently disabled.
- **Discovering** - Host has never responded to a PING. After a PING response is received once, the status will not return to "discovering until a reboot is performed or a "kill line" is issued on this port.

- **Waiting reboot**- Monitored host has not responded to all PING retries. It is now marked as needing a reboot and is executing the “delay before reboot” (if configured).
- **Rebooting**- The monitor host has determined that the host is not responding and has initiated a “power cycle” on the plug in order to re-boot the host.
- **Monitoring**- The host is being monitored and is responding to PING requests.

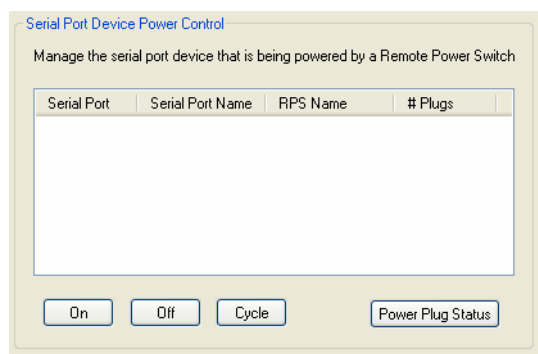
The “**# Reboots**” field above can contain the number of times that this power plug has been cycled due to a failure to respond to the PINGs.

The “**Last Reboot**” field above can contain the date and time of the last reboot to take place due to a failure to respond to the PINGs.

Power	Controls the power state of the plug as follows; On Button - Turns the selected plug on. Off Button - Turns the selected plug off. Cycle Button - Turns the selected plug off and then on.
Monitor Host	If host monitoring has been enabled on this plug, these buttons control the state of the feature as follows; On Button - Enables the host monitor function. Off Button - Disables the host monitor function. Reset Statistics Button - Resets the “# reboots” and “Last Reboot” fields
OK	Closes the window.

Serial Port Power Control

The **Serial Port Power Control** window allows you to manage the power plugs that have been associated with the serial devices connected to the IOLAN.



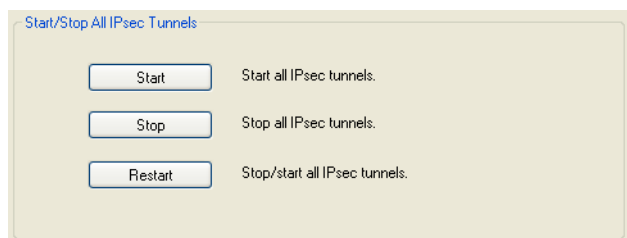
On	Turns the selected plug on.
Off	Turns the selected plug off.
Cycle	Turns the selected plug off and then on.
Power Plug Status	Displays a window that provides the plug status for every plug associated with the serial port.

Power Plug Status

This **Power Plug Status** window displays the status of all the plugs associated with a serial port. Select **OK** to close this window.

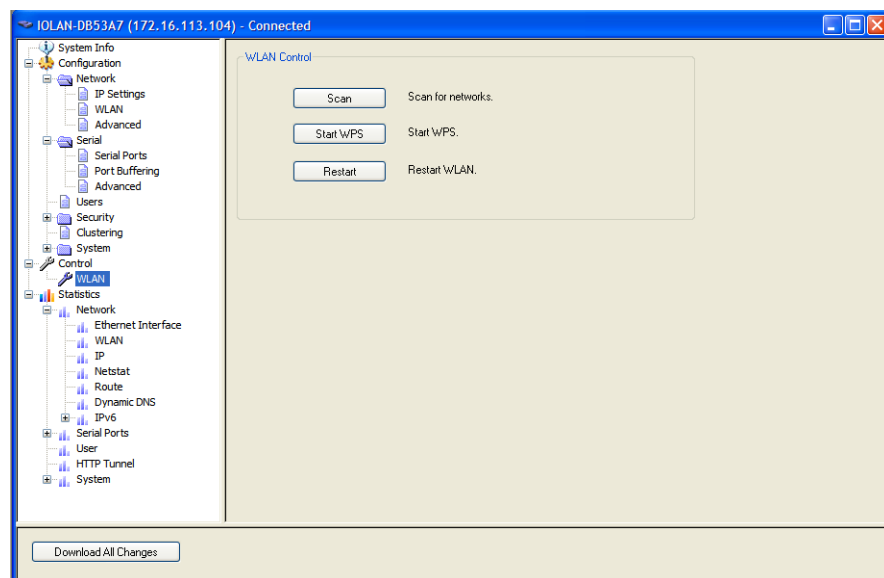
IPsec Tunnel Control

You can start, stop, and restart all the IPsec tunnels. When you start the IPsec tunnels, the **Boot Action** configured for each IPsec tunnel is what determines its state.:



- | | |
|----------------|--|
| Start | Starts all IPsec VPN tunnels. |
| Stop | Stops all IPsec VPN tunnels. |
| Restart | Stops and then starts all IPsec VPN tunnels. |

WLAN Control



Scan

Scan The IOLAN will scan the network for any broadcasting AP with the same SSID and security type.

Profile	<p>The configured Profile names are shown on a list (up to 8 profiles). Profiles will be matched to a broadcasting AP with the same SSID and security type. Matching profiles will be displayed at the top of the list and when highlighted will have the Connect Button highlighted in order to connect. Profiles without a matching AP and disabled profiles will not be on this list.</p> <p>Note: Open-WEP, Shared-WEP or 802.1x-WEP security will be matched as equivalent.</p>
SSID	Name or the network name assigned to the IOLAN when in Soft-AP mode.
Signal	Displays the wireless signal strength.
RSSI	A measurement of the power level of the received radio signal (in dBm) of the currently associated AP averaged over time. Values less than or equal to -95 dBm have no signal strength. Values greater than or equal to -35 dBm are at 100 percent signal strength.
BSSID	Shows whether the IOLAN is connected to this BSSID (Access Point's MAC Address).
Channel	Displays the channel number that the IOLAN is using to connect to the AP. Value: (1-11 channels use 2.4GHz) and (36, 40, 44, 48 channels use 5GHz).
Network type scan	The network type displayed will be Infrastructure or Ad Hoc. The IOLAN cannot connect to Ad Hoc networks.
Security	Displays the security type used for this connection between the IOLAN and the AP.
<i>Start WPS</i>	
Start WPS	The IOLAN will scan (120 seconds) all networks to find the closest AP that is currently in WPS mode. The IOLAN will exchange credentials with that AP and then create an internal wireless profile (association) and will then exit WPS mode.
<i>Restart WLAN</i>	
Restart	All WLANs will be stopped and any new configured WLAN parameters will be applied before the WLANs are restarted.

WWAN Control

Restart WWAN

Restart	Restart the WWAN connection.
----------------	------------------------------

Symmetric Key File

This section defines the layout of the NTP/SNTP Symmetric Key file that must be downloaded to the IOLAN in order to use NTP/SNTP server authentication feature. Each line of the NTP/SNTP symmetric key file consists of three fields: a key ID in the range 1 to 65,534, inclusive, a key type and a message digest key consisting of a printable ASCII string equal to or less than 20 characters or a 40 character hex digit string.

Table 0–1

key ID	key type	message digest key	
1	MD5	CeR{+'9LRTY:a0=P?GOA	ascii string
2	MD5	POE)+'9KRMYP0-PZOQ	ascii string
3	MD5	E)+'9KRRTS {+'9LRTpp	ascii string
4	MD5	ECeE)+'9KRDSRuurQPiw	ascii string
5	SHA1	0e9e44502940294fa788aafaac34ccb126347d34	hex digit string
6	SHA1	f4e9e4454e9e4450294faccb126309ff4ccb1200	hex digit string
7	SHA1	e9e44502949e4450294ccb12634e9e447d3489	hex digit string
8	SHA1	40294fa7894faccb126502944fac4e9e788aafaa	hex digit string

Note: 1-10 key ID entries are allowed in this NTP/SNTP key file. Both MD5 and SHA1 are supported. Key ID 0 is excluded.

Administration

This chapter addresses the functions that the admin user or a user with Admin Level privileges might do. This chapter uses the DeviceManager as the configuration method described in most administrative functions. As a general rule, administrative functions are accessed from the menu bar in the DeviceManager and under the **Administration** option in the WebManager's navigation tree.

Saving Configuration Files

When you connect to the IOLAN using either DeviceManager or WebManager, the IOLAN's active configuration file is loaded into the configurator. To save a backup of the configuration file locally, do the following:

In DeviceManager:

1. From the menu bar, select **File, Save As**.
2. In the Save As dialog box, specify a name and format for the file. Notice that you can save the file as either a **.dme** or a **.txt** file. Either file format can be imported into the DeviceManager and downloaded to the IOLAN in the future. The **.dme** is a binary file and the **.txt** file is a text file that can be viewed in any text editor.
3. Select **Save**.
4. In WebManager:
5. In the navigation tree, select the **Administration** option.
6. In the configuration area, select the **Backup/Restore** button.
7. Select the tab corresponding to the transfer method you wish to use. The options are;
 - Web - Uses HTTP to transfer the data
 - TFTP - Uses Trivial File Transfer Protocol to transfer the data
 - SFTP - Uses Secure File Transfer Protocol to transfer the data.

Note: For both TFTP or SFTP, you must have a host on your network which will act as the TFTP or SFTP Server. HTTP does not require any other host.

1. In the Backup group box, select the format (**Binary** or **Text**) in which you want to save the file. Either file format can be imported into the DeviceManager and downloaded to the IOLAN in the future.
2. Select the **Backup Configuration** button.

Downloading Configuration Files

You can download a configuration file to the IOLAN by doing the following:

In DeviceManager:

1. Connect to the IOLAN to retrieve the current configuration file.
2. Open the configuration file you want to download to the IOLAN by selecting **File, Import Configuration from a File** and then browsing to the configuration file. This will replace the retrieved configuration file.
3. Select **Tools, Download Configuration to IOLAN** or select the **Download All Changes** button.
4. Reboot the IOLAN.
5. In WebManager:
6. In the navigation tree, select the **Administration** option.
7. In the configuration area, select the **Backup/Restore** button.
8. Select the tab corresponding to the transfer method you wish to use. The options are;
 - Web - Uses HTTP to transfer the data
 - TFTP - Uses Trivial File Transfer Protocol to transfer the data

- SFTP - Uses Secure File Transfer Protocol to transfer the data.
9. In the Restore group box, browse to the configuration file that you want to download to the IOLAN.
 10. Select the **Restore Configuration** button.
 11. Reboot the IOLAN.

Note: For both TFTP or SFTP, you must have a host on your network which will act as the TFTP or SFTP Server. HTTP does not require any other host.

Downloading Configuration Files to Multiple IOLANs

You can download a configuration file to multiple IOLANs at the same time by doing the following in DeviceManager. DeviceManager is the only configurator that does this function:

1. Select **Tools, Download Configuration to Multiple IOLANs**.
2. Specify the IOLANs that you want to download the configuration to, then enter the following information for each IOLAN that you want to configure with the same configuration file.

IP Address	Enter the IP address of the IOLAN that you want to download the configuration to. Field Format: IPv4 or IPv6 address
Server Name	The name of the IOLAN. The IOLAN name that you put in this field is passed into the configuration before it is downloaded to the IOLAN and cannot be left blank.
Password	Enter the admin user password for the IOLAN.
Reboot Server	Determines whether or not the IOLAN is rebooted after it has received the new configuration. The new configuration definitions will not go into effect until the IOLAN is rebooted.

3. Select **Add** to add the IOLAN to the download list. You can also select on the IOLAN entry and edit any information and then select **Update** to make the edits permanent.
4. Select the **Download>** button to start the download process. A status window will display with the configuration download status.

Uploading Configuration Files

When you upload a configuration to the DeviceManager, you are uploading the IOLAN's working configuration file. In most other configurators (the exception being SNMP), you are always seeing the working configuration file.

In DeviceManager, select **Tools, Upload Configuration from IOLAN**. The working configuration file will automatically be loaded into the DeviceManager.

Specifying a Custom Factory Default Configuration

When you receive the IOLAN, it comes with a factory default configuration that the IOLAN can be reset to at any time. Administrators might find it useful to customize the factory default configuration file, so that if the IOLAN gets reset to its factory defaults, it will be reset to defaults that the Administrator specified. There are two ways you can set the custom factory default configuration:

- **Download a file to the IOLAN**—You can download a custom factory default file to the IOLAN using any of the configuration methods. In DeviceManager, you must connect to the IOLAN and then select **Tools, Advanced, Custom Files, Custom Factory Default Configuration** and then specify the file. In WebManager, you must connect to the IOLAN and then select **Administration, Reset, Factory Defaults, Set Current Configuration as Factory Default**.

- **Download the current configuration to the IOLAN**—You can specify the configuration that you are working with/on as the custom factory default configuration using any of the configuration methods (you must be connected to the IOLAN). In DeviceManager, select **Tools, Advanced, Set Factory Default to IOLAN**. In WebManager, select **Administration, Reset, Factory Defaults, Get and Set Factory Default Configuration File**.

Using the IOLAN reset button (only applies to certain models)

This inset reset button allows you to reset the IOLAN, reset the IOLAN to its Perle or custom factory default configuration or reset the IOLAN to the Perle factory default settings. The Power/Ready LED color and the resetting of the IOLAN default configuration vary depending on how long you press and hold the RESET button, as shown in the table below.

When you press and hold the RESET button for...	LED color	IOLAN System Status
Less than 3 seconds	Blinking amber	Reboots. All configuration and files will remain the same.
Between 3 and 10 seconds	Blinking amber, then turns solid amber when you release the RESET button	Reboots and resets the configuration to the factory default (either the Perle or custom default configuration). All configuration, user IDs, passwords and security certificates are deleted.
Over 10 seconds	Blinking amber, then turns solid amber when you release the RESET button	Reboots and resets the configuration to the Perle factory default configuration. All configuration, user IDs, passwords and security certificates are deleted, even if a custom default configuration has been defined.

Downloading IOLAN Firmware

To upgrade the IOLAN firmware (software):

- In DeviceManager, select **Tools, Advanced, Download Firmware to IOLAN**. You can browse to the firmware location. Once the firmware download is complete, you will be prompted to reboot the IOLAN. You can choose to reboot the IOLAN at another time by selecting **Tools, Reset, Reboot IOLAN**.
- In WebManager, under the **Administration** option, select **Update Firmware**. Either browse to the firmware file and then select the **Upload** button or configure the TFTP or SFTP server and select the **Upload** button. Note: If you use the TFTP or SFTP option, the specified TFTP or SFTP server must be on the same subnet as the IOLAN.

Upgrading the firmware does not affect the IOLAN's configuration file or downloaded custom files.

Setting the IOLAN's Date and Time

When you set the IOLAN's time, the connection method and time zone settings can affect the actual internal clock time that is being set. For example, if you are connecting to the IOLAN through the DeviceManager and your PC's time zone is set to Pacific Standard Time (GMT -8:00) and the IOLAN's time zone is set to Eastern Standard Time (GMT -5:00), the IOLAN's time is actually three hours ahead of your PC's time. Therefore, if you set the IOLAN's time to 2:30 pm in the DeviceManager, the IOLAN's actual internal clock time is 5:30 pm. This is the only configuration method that interprets the time and converts it between time zones, as necessary.

All other configuration methods set the IOLAN's internal clock time to the time specified, with no interpretation.

To set the IOLAN's system clock in DeviceManager, select **Tools, Advanced, Set Unit Time/Date** and in WebManager select **Administration, Date/Time**. The Set Date/Time window is displayed.

Configure the following parameters:

Date	The IOLAN's date. The format of the IOLAN's date is dependent on the Windows operating system and regional settings.
Time	The IOLAN's internal clock time, based on your PC's time zone. For example, if your PC's time zone is set to Pacific Standard Time (GMT -8:00) and the IOLAN's time zone is set to Eastern Standard Time (GMT -5:00), the IOLAN's time is three hours ahead of your PC's time. If you set the IOLAN's time to 2:30 pm, the IOLAN's actual internal clock time is 5:30 pm.
Use the PCs Date/Time	When enabled, sets the IOLAN's time to the PCs time. Default: Enabled This option is unique to the DeviceManager.

Rebooting the IOLAN

When you download any file (configuration, keys, certificates, firmware, etc.) to the IOLAN, you must reboot the IOLAN for it to take effect by selecting **Tools, Reset, Reboot Server** in DeviceManager and **Administration, Reboot Unit** in WebManager.

Resetting Serial Port Statistics

You can reset the IOLAN's serial port/s statistics back to zero.

Resetting the IOLAN to Factory Defaults using the WebManager

You can reset the IOLAN to its factory default configuration by selecting **Administration, Reset, Factory Defaults** in WebManager. The IOLAN will automatically reboot itself with the Perle factory default or custom factory default configuration.

Resetting the SecurID Node Secret

If you are using SecurID external authentication, you can select **Tools, Reset, Reset SecurID Node Secret** in DeviceManager and **Administration, Reset, SecurID Secret** in WebManager to reset the node secret. You do not need to reboot the IOLAN for this to take effect, it works instantly.

Language Support

Two language files, in addition to English, are supplied on the Perle website, French and German. You can use any of these language files to create a translation into a language of your choice. You can download the language file (whether the language is supplied or translated) into the IOLAN and select the **Language** option of **Custom Language** or **Customlang** (custom language), making the CLI field labels display in the desired language.

You can view the CLI in one other language only (as well as English). If you download another language file, this new language will replace the first language you downloaded.

You can revert to English at any time; the English language is stored permanently in the IOLAN and is not overwritten by your new language. Each user logged into the IOLAN can operate in either English or the downloaded language.

Loading a Supplied Language

This section describes how to download a language file using the CLI, since it is the least intuitive method. French and German language files can be downloaded from the Perle website.

To load one of the supplied languages into the IOLAN, so the CLI fields appear in another language, do the following:

1. Copy the language file to a host machine on the network; place it in the main file system or on the main hard drive.
2. Either use the TFTP/SFTP defaults in the IOLAN or, configure as necessary, TFTP/SFTP in the IOLAN.
3. In the CLI of the IOLAN, enter the host IP address and file name; for example,
4. Netload customlang 172.16.4.1 /temp/Iolan_ds_French.txt
5. Snetload customlang 172.16.4.1 /temp/Iolan_ds_French.txt
6. The IOLAN will download the language file via TFTP or SFTP.
7. In DeviceManager select **Tools, Advanced, Custom Files** and then select **Download Custom Language File** and browse to the language file. In WebManager select **Administration, Custom Files** and then specify the **Custom Language File** option and browse to the language file.
8. To set an individual user to the new language, go to the **Users** menu and, in the **Language** field select **Customlang**. In the CLI (only) you can set individual users or all users to the new language; see the **set user *** command.
9. The user will see the change of language when he/she logs out (**Main Menu, Sessions Menu, Logout**) and logs back into the IOLAN. If, as Admin user, you change your language setting to **Customlang**, you will see the text menus display in the new language when you save and exit the **Change User** form. Users with **Level Normal** can also change their display language.

Note: If you download a new software version, you can continue to use your language unchanged; however, we recommend translating the new strings, which will be added to the end of the language file. A **Reset to Factory Defaults** will reload the **Customlang** as English.

On successful download, the **Customlang** in the IOLAN will be overwritten by the new language.

Translation Guidance

To help you with your translation, of supplied ASCII text language files we offer the following guidance:

- The IOLAN will support languages other than English (and the supplied German and French languages). The English language file, **english.txt**, displays the character length of each line at the beginning of the line. If a translated line goes over that character length, it will be displayed truncated in the CLI.
- Translate line for line, do not omit lines if you do not know the translation; leave the original untranslated text in place. Also, you must maintain the same sequential order of lines. It is a good practice to translate the file using a text editor that displays line numbers, so you can periodically verify that the line sequence has not changed from the original file (by comparing it to the original file).
- Keep all translations in quotes, otherwise the line will not display properly.
- Each line must end with a carriage return.
- If a line contains only numbers, for example 38400, leave that line in place, unchanged (unless you are using a different alphabet).

Updating Language Files

Updated language files can be found on the Perle website at www.perle.com.

Note: The upgrade of your software (firmware) will not change the display of the language in the CLI.

If you are already using one of the supplied languages, French or German, you probably want to update the language file in the IOLAN. Until you update the IOLAN with the new language file, new text strings will appear in English.

If you are already using a language translated from an earlier version, you probably want to amend your translation. When a language file is updated, we will try to maintain the following convention:

- New text strings will be added to the bottom of the file (not inserted into the body of the existing file).
- Existing text strings, if altered, will be altered in sequence; that is, in their current position in the file.
- The existing sequence of lines will be unchanged.
- Until you have the changes translated, new text strings will appear in the CLI in English.

Downloading Terminal Definitions

All terminal types can be used on the IOLAN. Some terminal types which are not already defined in the IOLAN, however, are unable to use Full Screen mode (menus) and may not be able to page through sessions properly. When installed, the IOLAN has several defined terminal types—Dumb, WYSE60, VT100, ANSI, TVI925, IBM3151, VT320-7, and HP700/44.

If you are not using, or cannot emulate, any of these terminal types, you can add up to three additional terminal definitions to the IOLAN. The terminal definitions can be downloaded from a TCP/IP host.

To download terminal definitions, follow these steps:

1. Decide which TCP/IP host you are going to use. It must be a machine with enabled.
2. Configure SFTP/TFTP in the IOLAN as necessary.
3. Select **Tools, Advanced, Custom Files** from the menu bar in DeviceManager and **Administration, Custom Files** in WebManager.
4. From the **File Type** drop-down, select **Download Terminal Definition**. Select the terminal definition option **1, 2, or 3** and then browse to the terminal definition file that is being downloaded to the IOLAN.
5. In the **Terminal** profile, select the **Terminal Type Termx** that you custom defined.

Creating Terminal Definition Files

To create new terminal definition files, you need to copy and edit the information from the terminfo database.

1. On a UNIX host, change directory to `/usr/lib/terminfo/x` (where **x** is the first letter of the required terminal type). For a Wyse60, for example, you would enter the command `cd /usr/lib/terminfo/w`.
2. The termcap files are compiled, so use the command `infocmp termfile` to read the required file (for example: `infocmp wy60`).
3. Check the file for the attribute `xmc#n` (where **n** is greater than or equal to 1). This attribute will corrupt menu and form displays making the terminal type unsuitable for using Menu mode.
4. If the terminal definition is suitable, change to a directory of your choice.
5. Rename and copy the file to the directory specified at step 4. using the command `infocmp termfile > termn` where **n** is greater than or equal to 1; (for example, `infocmp wy50 > term1`). Make sure the file has global read and execute permission for its entire path.
6. Edit the file to include the following capabilities in this format:

```
term=
acsc=
bold=
civis=
clear=
cnorm=
cup=
rev=
rmacs=
rmso=
smacs=
smso=
page=
circ=
```

For example:

```
term=AT386 | at386| 386AT |386at |at/386 console
acsc=jYk?lZm@qDtCu4x3
bold=\E[1m
civis=
clear=\E[2J\E[H
cnorm=
cup=\E[%i%p1%02d;%p2%02dH
rev=\E4A
rmacs=\E[10m
rmso=\E[m
smacs=\E[12m
smso=\E[7m
page=
circ=n
```

Note: As you can see from the example, capabilities which are not defined in the terminfo file must still be included (albeit with no value). Each entry has an 80 character limit.

On some versions of UNIX, some of the capabilities are appended with a millisecond delay (of the form `$<n>`). These are ignored by the IOLAN and can be left out.

The ‘acsc’ capability, if defined, contains a list of character pairs. These pairs map the characters used by the terminal for graphics characters to those of the standard (VT100) character set.

Include only the following character pairs:

jx, kx, lx, mx, qx, tx, ux and xx

(where *x* must be substituted by the character used by the terminal). These are the box-drawing characters used to display the forms and menus of Menu mode. They must be entered in this order.

The last two capabilities will not be found in the terminfo file. In the **page** field you must enter the escape sequence used by the terminal to change screens. The **circ** field defines whether the terminal can use **previous page** and **next page** control sequences. It must be set to **y** or **n**. These capabilities can be found in the documentation supplied with the terminal.

Resetting Configuration Parameters

You can reset the IOLAN to its factory default settings (this will reset it to the Perle factory default or custom factory default settings, depending on what has been configured) through any of the following methods:

You can push in the reset button on the IOLAN hardware for three to ten seconds (pushing it in and then quickly releasing will just reboot the IOLAN). See the IOLAN Hardware Installation Guide to determine the location of the reset button.

- DeviceManager, select **Tools, Reset, Reset to Factory Defaults**
- CLI, at the command line type, `reset factory`
- WebManager, select **Administration, Reset, Factory Default**, and then select the **Reset to Factory Defaults** button
- Menu, select **Network Configuration, Reset to Factory Defaults**
- SNMP, in the **adminInfo** folder, set the **adminFunction** variable to **2**

Lost admin Password

If the admin user password is lost, there are only two possible ways to recover it:

- reset the IOLAN to the factory defaults
- have another user that has **Admin** level rights, if one is already configured, reset the admin password.

SD Flash (applies to some models)

Using the WebManager, you are able to perform these functions on the integrated SD flash. You must provide your own SD flash card.

- Copy - copy firmware and config between the IOLAN and SD flash
- Delete - Delete files and directories in the SD flash
- Dir - list the files and directories on the SD flash
- Mkdir - make a directory on the SD flash
- Format - format the SD flash (removes all files and directories)

RADIUS External Parameters

Although RADIUS can be used strictly for external authentication, it can also be used to configure line and user parameters. Therefore, when a user is being authenticated using RADIUS, it is possible that the user's configuration is a compilation of the parameters passed back from RADIUS, the IOLAN parameters if the user has also been set up as a local user in the IOLAN, and the Default User's parameters for any parameters that have not been set by either RADIUS or the user's local configuration.

Supported RADIUS Parameters

This section describes the attributes which will be accepted by the IOLAN from a RADIUS server in response to an successful authentication request.

Table 0–1

Type	Name		Description
1	User-Name	Request	The name of the user to be authenticated.
2	User-Password	Request	The password of the user to be authenticated.
4	NAS-IP-Address	Response	The IOLAN's IPV4 address.
5	NAS-Port	Response	If the user is connected to a physical port then the port number of the port is sent. If the user is connected to the IOLAN itself then a port number of 0 is sent.
6	Service-Type	Response	Indicates the service to use to connect the user to the IOLAN. A value of 6 indicates administrative access to the IOLAN. Supported values are: <ul style="list-style-type: none">• 1—Login• 3—Callback-Login Equivalent to the IOLAN User Service set by Type 15, Login-Service.• 2—Framed• 4—Callback-Framed Equivalent to the IOLAN User Service set by Type 7, Framed-Protocol.• 7—NAS prompt• 9—Callback NAS-prompt Equivalent to IOLAN User Service DSLogin.• 6—Administrative User• 11—Callback Administrative User Equivalent to IOLAN User Service DSLogin and the User gets Admin privileges.

Table 0–1

Type	Name		Description
7	Framed-Protocol	Response	The link layer protocol to be used by this user. Determines the User Service when Service-Type is set to Framed or Callback-Framed. Supported values are: <ul style="list-style-type: none">• 1—PPP• 2—SLIP
8	Framed-IP-Address	Response	The IP Address to be assigned to this user for PPP or SLIP.
9	Framed-IP-Netmask	Response	The subnet to be assigned to this user for PPP or SLIP.
12	Framed-MTU	Response	Attribute indicates the Maximum Transmission Unit (MTU) to be configured for the user, when it is not negotiated by some other means such as PPP.
13	Framed-Compression	Response	Indicates a compression protocol to be used for the PPP or SLIP link. Supported value is: <ul style="list-style-type: none">• 1—Van Jacobson TCP/IP compression.
14	Login-Host	Response	Indicates the host with which the user can connect to when the Service-Type is set to 1 (Login) or 3 (Callback-Login).
15	Login-Service	Response	Indicates the IOLAN User Service to use to connect the user a host. Supported values are: <ul style="list-style-type: none">• 0—Telnet• 1—Rlogin• 2—TCP Clear• 5—SSH• 6—SSL Raw
16	Login-TCP-Port	Response	Indicates the TCP port with which the user is to be connected when the Service-Type is set to 1 (Login) or 3 (Callback-Login).
19	Callback-Number	Response	Specifies the callback phone number. This is the same implementation as 20 (Callback-ID), but takes precedence if 20 is set.
20	Callback-ID	Response	Specifies the callback phone number. This is the same implementation as 19 (Callback-Number), but 19 takes precedence if both are set.
22	Framed-Route	Response	When the PPP IPv4 interface comes up, the IOLAN will add routes to the user's PPP interface in the same order they were received

Table 0–1

Type	Name		Description
25	Class	Response	Received attributes are send in the Accounting Reply messages.
26	Vendor-Specific	Response	<p>Perle’s defined attributes for line access rights and user level. See Perle RADIUS Dictionary Example for an example of this file.</p> <p>Line Access Rights for port <i>n</i> (where <i>n</i> is the line number):</p> <p>Name: Perle-Line-Access-Port-<i>n</i></p> <p>Type: 100 + <i>n</i></p> <p>Data Type: Integer</p> <p>Value: Disabled (0), ReadWrite(1), ReadInput(2), ReadInputWrite (3), ReadOutput (4), ReadOutputWrite (5), ReadOutputInput (6), ReadOutputInputWrite (7)</p> <p>Name: Perle-User-Level</p> <p>Type: 100</p> <p>Data Type: Integer</p> <p>Value: Admin(1), Normal(2), Restricted(3), Menu(4)</p> <p>Name: Perle-Clustered-Port-Access</p> <p>Type: 99</p> <p>Data Type: Integer</p> <p>Value: Disabled(0), Enabled(1)</p>
27	Session-Timeout	Response	Maximum number of seconds the user will be allowed to stay logged on.
28	Idle-Timeout	Response	Use this timer to close a connection because of inactivity. When the Idle-Timeout expires, the IOLAN will end the connection. The maximum value is 4294967 seconds (about 49 days). A value of 0 (zero) means the Idle-Timeout will not expire, so the connection is permanently open.
31	Calling-Station-Id	Response	For reverse telnet and reverse ssh the IP address of the client will be sent. All other server type do not send this field.
32	NAS-Identifier	Response	If the identifier is configured then this field will be sent.
61	NAS-Port-Type	Response	For reverse telnet and reverse ssh connections, a type of Virtual (5) will be sent. For a PPP connection type a type of Async (0) will be sent. For all direct connect service types a type of Async (0) will be sent.

Table 0–1

Type	Name		Description
87	NAS-Port-Id	Response	<p>For sessions originating from the serial port: <line-name> or “SERIAL:xx”, where xx starts at serial port 1.</p> <p>For reverse Telnet and SSH Ethernet sessions: “ETH:REVSESS:xx”, where xx is the serial port being accesses, otherwise 00 for a ILOAN management session.</p> <p>For Device manager sessions: “DEVMGR”</p> <p>For HTTP sessions: “HTTP”</p>
95	NAS-IPv6-Address	Response	The IPv6 address of the IOLAN.
96	Framed-Interface-Id	Response	The remote IPv6 interface identifier for the remote end of the PPP link.
98	Login-IPv6-Host	Response 8	For LOGIN and CALLBACK service types, the IPv4 address of the login host is sent to the radius accounting host.
99	Framed-IPv6-Route	Response	When the PPP IPv6 interface comes up, the IOLAN will add routes to the user’s PPP interface in the same order they were received.

Accounting Message

This section describes the attributes which will be included by the IOLAN when sending an accounting message to the RADIUS server.

Type	Name	Description
1	User-Name	The name of the user to be authenticated.
4	NAS-IP-Address	IP Address of IOLAN LAN interface.
5	NAS-Port	If the user is connected to a physical port then the port number of the port is sent. If the user is connected to the IOLAN itself then a port number of 0 is sent.

Type	Name	Description
6	Service-Type	<p>Indicates the service to use to connect the user to the IOLAN. A value of 6 indicates administrative access to the IOLAN. Supported values are:</p> <ul style="list-style-type: none"> • 1—Login • 3—Callback-Login <p>Equivalent to the IOLAN User Service set by Type 15, Login-Service.</p> <ul style="list-style-type: none"> • 2—Framed • 4—Callback-Framed <p>Equivalent to the IOLAN User Service set by Type 7, Framed-Protocol.</p> <ul style="list-style-type: none"> • 7—NAS prompt • 9—Callback NAS-prompt <p>Equivalent to IOLAN User Service DSPrompt.</p> <ul style="list-style-type: none"> • 6—Administrative User • 11—Callback Administrative User <p>Equivalent to IOLAN User Service DSPrompt and the User gets Admin privileges.</p>
14	Login-IP-Host	For LOGIN and CALLBACK service types, the IPv4 address of the login host is sent to the radius accounting host.
31	Calling-Station-Id	For reverse telnet and reverse ssh the IP address of the client will be sent. All other server type do not send this field.
32	NAS-Identifier	If the identifier is configured then this field will be sent.
40	Acct-Status-Type	Indicates if this is the beginning or end of a session. Supported values are: 1 = Start 2 =Stop.
42	Acct-Input-Octets	Number of bytes which were received from the user during this session.
43	Acct-Output-Octets	Number of bytes where were transmitted to the user during this session.
44	Acct-Session-ID	A string which identifies the session. The same string must be used in the start and stop messages.
45	Acct-Authentic	Indicates how the user was authenticated. Supported values are: 1 = Local 2 = RADIUS.
46	Acct-Session-Time	Number of seconds for which the user has been connected to a specific session.
47	Acct-Input-Packets	Number of packets which were received from the user during this session.
48	Acct-Output-Packets	Number of packets which were transmitted to the user during this session.

Type	Name	Description
49	Acct-Terminate-Cause	Indicates how the session was terminated: Supported values include: 1 = User Request 2= Lost Carrier 3=Lost Service 4= Idle Timeout 5= Session Timeout 14 = Port Suspended 16 = Callback.
61	NAS-Port-Type	For reverse telnet and reverse ssh connections, a type of Virtual (5) will be sent. For a PPP connection type a type of Async (0) will be sent. For all direct connect service types a type of Async (0) will be sent.
77	Connect-Info	.For reverse telnet, reverse ssh and direct serial connections the serial port baud rate is send to the radius accounting server.
87	NAS-Port-Id	For sessions originating from the serial port: <line-name> or “SERIAL:xx”, where xx starts at serial port 1. For reverse Telnet and SSH Ethernet sessions: “ETH:REVSESS:xx”, where xx is the serial port being accesses, otherwise 00 for a ILOAN management session. For Device manager sessions: “DEVMGR” For HTTP sessions: “HTTP”
95	NAS-IPv6-Address	The IPv6 address of the IOLAN
98	Login-IPv6-Host	For LOGIN and CALLBACK service types, the IPv4 address of the login host is sent to the radius accounting host.

Mapped RADIUS Parameters to IOLAN Parameters

When authentication is being done by RADIUS, there are several **Serial Port** and **User** parameters that can be set by the RADIUS server. Any parameters sent by that RADIUS server that are not supported by the IOLAN are discarded. Below is a list of the RADIUS parameters and their IOLAN parameters:

RADIUS Parameter	IOLAN Parameter
Service-Type	This has no IOLAN field, although it needs to be set to Framed-User in the RADIUS server if the port is set for PPP or SLIP. For a Console Management profile set the RADIUS Service-Type to NAS prompt.
Framed-Protocol	Set to SLIP or PPP service.

Framed-Address	Remote IP Address field under either SLIP or PPP. <i>Caution:</i> the exception to the above rule is a Framed-Address value of 255.255.255.254. When this value is specified in the RADIUS file, the unit will use the Remote IP address configured for a PPP line in the IOLAN.
Framed-Netmask	IPv4 Subnet Mask field under either SLIP or PPP .
Framed-Compression	VJ Compression field under either SLIP or PPP .
Framed-MTU	MTU field under SLIP . MRU field under PPP .
Idle-Timeout	Idle Timeout under the serial port Advanced settings.
Login-Service	Corresponds to one of the following User Service parameters: Telnet , Rlogin , TCP Clear , SSH , or SSL Raw .
Session-Timeout	Session Timeout under the serial port Advanced settings.
Callback-Number	Combination of the Enable Callback and Phone Number fields under User , Advanced settings.
Callback-ID	Combination of the Enable Callback and Phone Number fields under User , Advanced settings.

Perle RADIUS Dictionary Example

The IOLAN has defined Vendor Specific RADIUS attributes in order for the RADIUS server to be configured to support the IOLAN features of Line Access Rights and User Level. These attributes have been defined in [Supported RADIUS Parameters](#) to allow the RADIUS server to be configured for RADIUS users to have this level of configuration.

See below for an example of the Perle defined attributes for the RADIUS server for a 4-port IOLAN (although the dictionary can contain 48 ports, even if they are not all defined):

```
# Perle dictionary.
#
#       Perle Systems Ltd.
#       http://www.perle.com/
#
#       Enable by putting the line "$INCLUDE dictionary.perle" into
#       the main dictionary file.
#
# Version:  1.30   21-May-2008   Add attribute for clustered port access
# Version:  1.20   30-Nov-2005   Add new line access right values for ports
#                               up to 49.
# Version:  1.10   11-Nov-2003   Add new line access right values
# Version:  1.00   17-Jul-2003   original release for vendor specific field
support
#
```

```
VENDOR   Perle           1966
```

```
#   Perle Extensions
```

ATTRIBUTE	Perle-Clustered-Port-Access	99	integer	Perle
ATTRIBUTE	Perle-User-Level	100	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-1	101	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-2	102	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-3	103	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-4	104	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-5	105	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-6	106	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-7	107	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-8	108	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-9	109	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-10	110	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-11	111	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-12	112	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-13	113	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-14	114	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-15	115	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-16	116	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-17	117	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-18	118	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-19	119	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-20	120	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-21	121	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-22	122	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-23	123	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-24	124	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-25	125	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-26	126	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-27	127	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-28	128	integer	Perle

ATTRIBUTE	Perle-Line-Access-Port-29	129	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-30	130	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-31	131	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-32	132	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-33	133	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-34	134	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-35	135	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-36	136	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-37	137	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-38	138	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-39	139	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-40	140	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-41	141	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-42	142	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-43	143	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-44	144	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-45	145	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-46	146	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-47	147	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-48	148	integer	Perle
ATTRIBUTE	Perle-Line-Access-Port-49	149	integer	Perle

Perle Clustered Port Access Values

VALUE	Perle-Clustered-Port-Access	Disabled	0
VALUE	Perle-Clustered-Port-Access	Enabled	1

Perle User Level Values

VALUE	Perle-User-Level	Admin	1
VALUE	Perle-User-Level	Normal	2
VALUE	Perle-User-Level	Restricted	3
VALUE	Perle-User-Level	Menu	4

Perle Line Access Right Values

VALUE	Perle-Line-Access-Port-1	Disabled	0
VALUE	Perle-Line-Access-Port-1	Read-Write	1
VALUE	Perle-Line-Access-Port-1	Read-Input	2
VALUE	Perle-Line-Access-Port-1	Read-Input-Write	3
VALUE	Perle-Line-Access-Port-1	Read-Output	4
VALUE	Perle-Line-Access-Port-1	Read-Output-Write	5
VALUE	Perle-Line-Access-Port-1	Read-Output-Input	6
VALUE	Perle-Line-Access-Port-1	Read-Output-Input-Write	7
VALUE	Perle-Line-Access-Port-2	Disabled	0
VALUE	Perle-Line-Access-Port-2	Read-Write	1
VALUE	Perle-Line-Access-Port-2	Read-Input	2
VALUE	Perle-Line-Access-Port-2	Read-Input-Write	3
VALUE	Perle-Line-Access-Port-2	Read-Output	4
VALUE	Perle-Line-Access-Port-2	Read-Output-Write	5
VALUE	Perle-Line-Access-Port-2	Read-Output-Input	6
VALUE	Perle-Line-Access-Port-2	Read-Output-Input-Write	7
VALUE	Perle-Line-Access-Port-3	Disabled	0
VALUE	Perle-Line-Access-Port-3	Read-Write	1
VALUE	Perle-Line-Access-Port-3	Read-Input	2
VALUE	Perle-Line-Access-Port-3	Read-Input-Write	3
VALUE	Perle-Line-Access-Port-3	Read-Output	4
VALUE	Perle-Line-Access-Port-3	Read-Output-Write	5

VALUE	Perle-Line-Access-Port-3	Read-Output-Input	6
VALUE	Perle-Line-Access-Port-3	Read-Output-Input-Write	7
VALUE	Perle-Line-Access-Port-4	Disabled	0
VALUE	Perle-Line-Access-Port-4	Read-Write	1
VALUE	Perle-Line-Access-Port-4	Read-Input	2
VALUE	Perle-Line-Access-Port-4	Read-Input-Write	3
VALUE	Perle-Line-Access-Port-4	Read-Output	4
VALUE	Perle-Line-Access-Port-4	Read-Output-Write	5
VALUE	Perle-Line-Access-Port-4	Read-Output-Input	6
VALUE	Perle-Line-Access-Port-4	Read-Output-Input-Write	7

...

TACACS+

Although TACACS+ can be used strictly for external authentication, it can also be used to configure Serial Port and User parameters. Therefore, when a user is being authenticated using TACACS+, it is possible that the user's configuration is a compilation of the parameters passed back from the TACACS+ authentication server, the User's IOLAN parameters if the user has also been set up as a local user in the IOLAN, and the Default User's parameters for any parameters that have not been set by either TACACS+ or the User's local configuration.

User and Serial Port parameters can be passed to the IOLAN after authentication for users accessing the IOLAN from the serial side and users accessing the IOLAN from the Ethernet side connections.

Accessing the IOLAN Through a Serial Port Users

This section describes the attributes which will be accepted by the IOLAN from a TACACS+ server in response to an authentication request for Direct Users.

Name	Value(s)	Description
priv-lvl	12-15 (Admin) 8-11 (Normal) 4-7 (Restricted) 0-3 (Menu)	The IOLAN privilege level.
Perle_User_Service	0 (Telnet) 1 (Rlogin) 2 (TCP_Clear) 3 (SLIP) 4 (PPP) 5 (SSH) 6 (SSL_Raw)	Corresponds to the User Service setting in the IOLAN. If no value is specified, DSPrompt is the default User Service.
service = telnet		Settings when Perle_User_Service is set to 0.
{		
addr =	IPv4 or IPv6 address	
port =	TCP port number	
}		

Name	Value(s)	Description
service = rlogin { addr = }	IPv4 or IPv6 address	Settings when Perle_User_Service is set to 1.
service = tcp_clear { addr = port = }	IPv4 or IPv6 address TCP port number	Settings when Perle_User_Service is set to 2.
service = slip { routing = addr = }	true (Send and Listen) false (None) IPv4 or IPv6 address	Settings when Perle_User_Service is set to 3.
service = ppp { routing = addr = port = ppp-vj-slot-compression callback-dialstring }	true (Send and Listen) false (None) IPv4 or IPv6 address TCP port number true or false phone number, no punctuation	Settings when Perle_User_Service is set to 4.
service = ssh { addr = port = }	IPv4 or IPv6 address TCP port number	Settings when Perle_User_Service is set to 5.
service = ssl_raw { addr = port = }	IPv4 or IPv6 address TCP port number	Settings when Perle_User_Service is set to 6.

Accessing the IOLAN Through a Serial Port User Example Settings

The following example shows the parameters that can be set for users who are accessing the IOLAN from the serial side. These settings should be included in the TACACS+ user configuration file.

```
Service = EXEC
{
priv-lvl = x                # x = 12-15 (Admin)
                           # x = 8-11  (Normal)
                           # x = 4-7   (Restricted)
                           # x = 0-3   (Menu)

timeout=x                   # x = session timeout in minutes

idletime=x                  # x = Idle timeout in minutes

Perle_User_Service = x      # x = 0 Telnet
                           # x = 1 Rlogin
                           # x = 2 TCP_Clear
                           # x = 3 SLIP
                           # x = 4 PPP
                           # x = 5 SSH
                           # x = 6 SSL_RAW
                           # If not specified, command prompt
}

# Depending on what Perle_User_Service is set to

service = telnet
{
addr = x.x.x.x             # ipv4 or ipv6 addr
port = x                   # tcp_port #
}

service = rlogin
{
addr = x.x.x.x             # ipv4 or ipv6 addr
}

service = tcp_clear
{
addr = x.x.x.x             # ipv4 or ipv6 addr
port = x                   # tcp_port #
}

service = slip
{
routing=x                  # x = true (Send and Listen)
                           # x = false (None)
addr = x.x.x.x             # ipv4 addr
}
```

```

service = ppp
{
routing=x          # x = true (Send and Listen)
                  # x = false (None)
addr = x.x.x.x     # ipv4 or ipv6 addr
ppp-vj-slot-compression = x # x =true or false
callback-dialstring = x # x = number to callback on
}

service = ssh
{
addr = x.x.x.x     # ipv4 or ipv6 addr
port = x           # tcp_port #
}

service = ssl_raw
{
addr = x.x.x.x     # ipv4 or ipv6 addr
port = x           # tcp_port #
}

```

Accessing the IOLAN from the Network Users

This section describes the attributes which will be accepted by the IOLAN from a TACACS+ server in response to an authentication request for Reverse Users. The TACACS+ **service** needs to be set to **EXEC/raccess** or just **raccess** on the well known port.

Name	Value(s)	Description
priv-lvl	12-15 (Admin) 8-11 (Normal) 4-7 (Restricted) 0-3 (Menu)	The IOLAN privilege level.
Perle_Line_Access_#	# = port number 0 (Disabled) 1 (ReadWrite) 2 (ReadInput) 3 (ReadInputWrite) 4 (ReadOuptut) 5 (ReadOutputWrite) 6 (ReadOutputInput) 7 (ReadOuputWrite)	For the specified line, provides the User's Line Access rights.
timeout	0-4294967	Session timeout in minutes.
idletime	0-4294967	Idle timeout in minutes.
Perle_Clustered_Port_Access	0 (Disabled) 1 (Enabled)	Control access to clustered ports.

Accessing the IOLAN from the Network User Example Settings

The following example shows the parameters that can be set for users who are accessing the IOLAN from the Ethernet side. These settings should be included in the TACACS+ user configuration file.

```
# Settings for telnet/SSH access
service = raccess
{
priv-lvl = x          # x = 12-15 (Admin)
                      # x = 8-11 (Normal)
                      # x = 4-7 (Restricted)
                      # x = 0-3 (Menu)

Perle_Line_Access_i=x # i = port number
                      # x = 0 (Disabled)
                      # x = 1 (Read/Write)
                      # x = 2 (Read Input)
                      # x = 3 (Read Input/Write)
                      # x = 4 (Read Output)
                      # x = 5 (Read Output/Write)
                      # x = 6 (Read Output/Input)
                      # x = 7 (Read Output/Write)

timeout=x             # x = session timeout in minutes

idletime=x            # x = Idle timeout in minutes

Perle_Clustered_Port_Access=x # x = 0 (Disabled)
                              # x = 1 (Enabled)
}
```

Note: Users who are accessing the IOLAN through WebManager or DeviceManager and are being authenticated by TACACS+ must have the Admin privilege level and the TACACS+ service level must be set to EXEC.

```
# Settings for WebManager and DeviceManager access
service=EXEC
{
priv-lvl = 12          # x = 12-15 (Admin)

Perle_Line_Access_i=x # i = port number
                      # x = 0 (Disabled)
                      # x = 1 (Read/Write)
                      # x = 2 (Read Input)
                      # x = 3 (Read Input/Write)
                      # x = 4 (Read Output)
                      # x = 5 (Read Output/Write)
                      # x = 6 (Read Output/Input)
                      # x = 7 (Read Output/Write)

Perle_Clustered_Port_Access = 1 # enable clustered port access
}
```

Applications

This chapter provides examples of how to integrate the IOLAN within different network environments or applications. Each scenario provides an example of a typical setup and describes the configuration steps to achieve the IOLAN functionality feature.

Dynamic DNS

Dynamic DNS Service providers enable users to access a server connected to the internet that has been assigned a dynamic IP address. The IOLAN product line has built-in support for the DynDNS.com service provider. When the IOLAN is assigned a dynamic IP address, it will inform the DynDNS.com service provider of its new IP address. Users may then use DynDNS.com as a DNS service to get the IP address of the IOLAN. In order to take advantage of this service the following steps need to be taken.

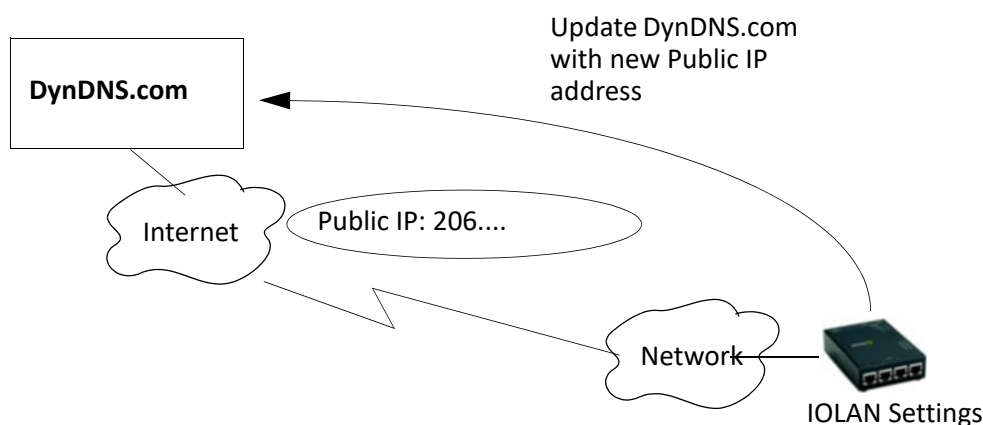
1. Create an account with DynDNS.com and configure the name your IOLAN will be known by on the internet (the **Host** name). For example, create a host name such as `yourcompanySCS.DynDNS.org`.
2. Enable the **Server Dynamic DNS** feature and configure the IOLAN's dynamic DNS parameters to match the **Host**'s configuration on the DynDNS.com server. Every time the IOLAN gets assigned a new IP address, it will update DynDNS.com with the new IP address.
3. Users accessing the IOLAN via the internet can now access it via its fully qualified host name. For example, `telnet yourcompanySCS.DynDNS.org`.

Dynamic DNS Update

When the **Server Dynamic DNS** feature is enabled and the DynDNS.com account information configured, the IOLAN will automatically update the DynDNS.com server with the public IP address assigned by the internet service provider (ISP). In the example below, an public IP address of 206.xx.xx.xx is assigned to the IOLAN by the ISP. The ISP should also provide the following:

- The IOLAN will need to have the Default Gateway configured so IP packets can be routed to the internet.
- You will also need to verify that a valid DNS entry (in the Network settings) has been created, since the DynDNS.com server is accessed via its Domain Name or URL.

If the internet service provider changes the IOLAN's IP address and Dynamic DNS is enabled and properly configured, the IOLAN will automatically send an update message to DynDNS.com to update it with the newly assigned IP address.

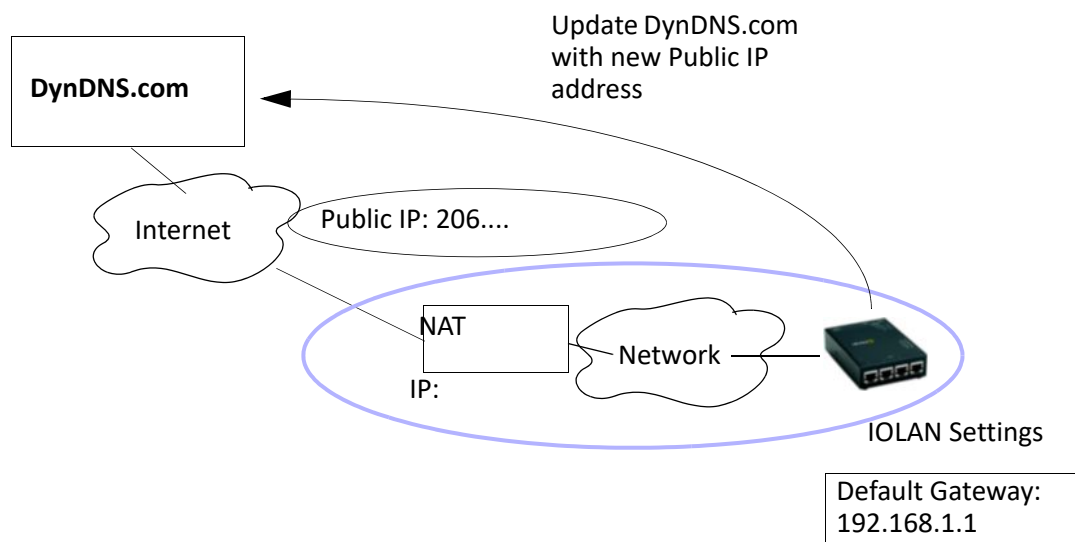


Using Dynamic DNS Behind a NAT Router

If the IOLAN is installed on a private network and has access to the internet via a router that performs NAT (Network Address Translation), this feature will still operate correctly. The IOLAN determines its internet

facing (public) IP address by sending a special request to the DynDNS.com server. This is the IP address that is used to update the DynDNS.com server. If setting up this type of configuration, verify that:

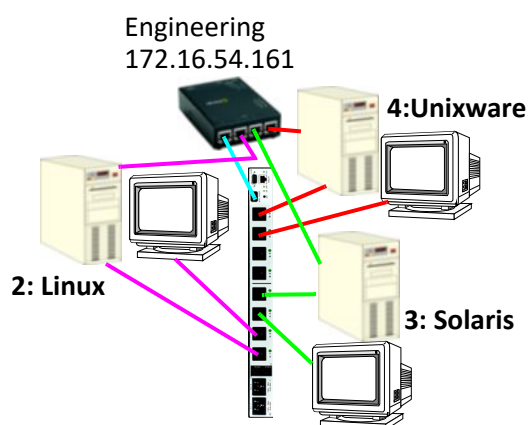
- The NAT router is identified on the IOLAN as the Default Gateway.
- A valid DNS server is defined in the IOLAN's network settings.
- You may need to setup Port Forwarding on the router to ensure that IP packets for sessions initiated on the internet can be routed to IOLAN.



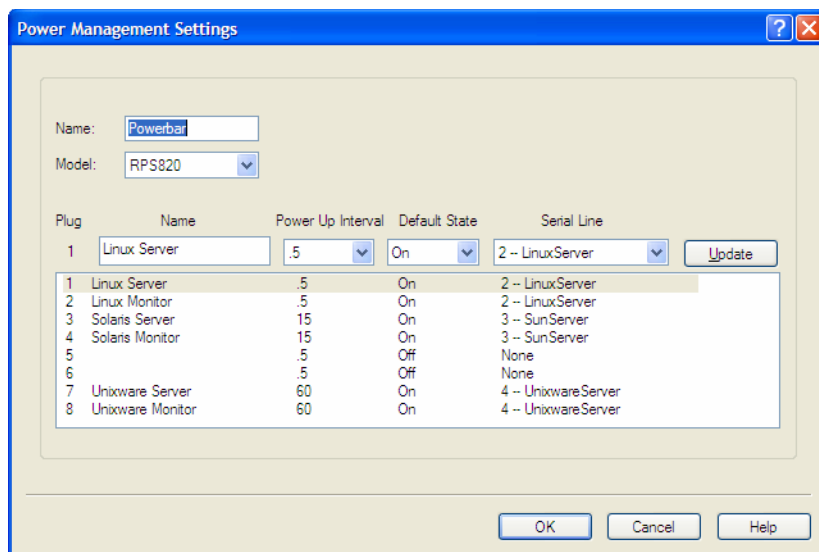
Power Management

If you have purchased a Perle RPS (Remote Power Switch) and have it connected to a IOLAN's serial port, you can manage the plugs on the RPS through the DeviceManager, CLI, or the WebManager's EasyPort Web.

In the following example, in the following scenario, the Perle RPS is connected to serial port 1 and there are various other Unix servers connected to the other serial ports. Each Unix server and its monitor is plugged into the RPS so that they can be managed through the power switch if, for example, the server should become remotely inaccessible.



The **Line** settings for serial line 1 are set to **Service Power Management**. The Power Management settings are configured to reflect the device (by device name) plugged into each RPS plug and its associated serial line (this allows a user to connect directly to a port and manage the power for all the devices associated with that port).



Any user can access and control all plugs in the RPS. If a user accesses the IOLAN through WebManager by typing the IOLAN's IP address into a web browser and entering their User Name and Password. The Admin user and users who have admin level rights will access the WebManager and can launch EasyPort Web by selecting the EasyPort Web button in the navigation pane. All other users will automatically get EasyPort Web as shown:

Manage Remote Power Switch

RPS Name: Powerbar Model: RPS820 Version 2.3.1

Device Name	Power Plug	Control			Status
Linux Server	1	On	Off	Cycle	OFF
Linux Monitor	2	On	Off	Cycle	ON
Solaris Server	3	On	Off	Cycle	ON
Solaris Monitor	4	On	Off	Cycle	ON
	5	On	Off	Cycle	OFF
	6	On	Off	Cycle	ON
Unixware Server	7	On	Off	Cycle	ON
Unixware Monitor	8	On	Off	Cycle	ON
All		On	Off	Cycle	Refresh
Reset to Default State					

From EasyPort Web, a user can either manage the entire RPS unit by selecting the Manage RPS button for Serial Port 1:

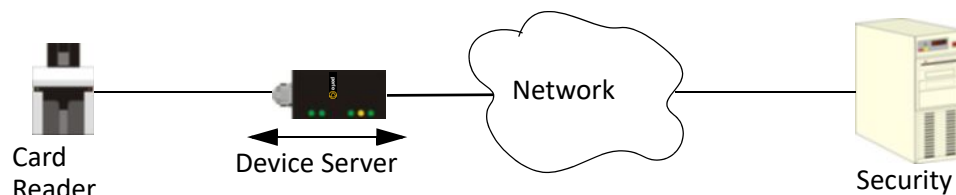
Or a user can manage the plugs associated with a serial line by selecting on the Device Power button for that serial.

Device Power Control			
Device Name: LinuxServer Serial Port #2 On Off Cycle			
Plug Name	Power Plug	Power Switch	
Linux Server	1	Powerbar	
Linux Monitor	2	Powerbar	

Machine To Machine Connections

If you are using the IOLAN to connect two hosts, allowing data to flow freely between them, you just need to configure the **Server** and the **Line** (no **User** required). In the following example, the serial device is a security Card Reader that needs to transmit and receive information to/from a host on the network that

maintains the Card Reader's application every time an employee uses an access card to attempt to gain entry to the company.



After configuring the **Server** parameters (**Server Name**, **IP Address**, **Ethernet** and **Serial** interfaces, etc.), the **Line Service** is set to **Sil Raw**, which creates an automatic, continuous connection between the Card Reader and its associated application on the Security host (through the IOLAN), by specifying the Security host name (which must already be configured in the IOLAN's Host Table) and TCP/IP port number. Therefore, the Card Reader can make a request to the Security host card reader application for employee verification, also logging access time, employee name, etc., and the Security host application can send back a code that does or does not unlock the door.

Creating User Sessions

Sessions are defined for users who are coming in through a serial device and are connecting to a host on the LAN.

Users who have successfully logged into the IOLAN (**User Service** set to **DSprompt**) can start up to four login sessions on LAN hosts. These users start sessions through the Menu option **Sessions**.

Multiple sessions can be run simultaneously on the same host or on different hosts. Users can switch between different sessions and also between sessions and the IOLAN using hotkey commands.

Users with **Admin** or **Normal** privileges can define new sessions and connect through them, even configure them to start automatically on login to the IOLAN. **Restricted** and **Menu** users can only start sessions pre-defined for them by the Admin user.

Users can be configured to have access to a specific port and access modes for this port, such as **Read/Write (RW)**, **Read Input (RI)**, **Read Output** and **Read Both (RI & RO)**.

Configuring Modbus

This sections provides a brief overview of the steps required to configure the IOLAN for your Modbus environment.

Configuring a Master Gateway

To configure a Master Gateway (Modbus Master connected to the serial side of the IOLAN), do the following:

1. Set the serial port that is connected to the serial Modbus Master to the **Modbus Gateway** profile.
2. In the **Modbus Gateway** profile on the **General** tab, set the **Mode** to **Modbus Master**.
3. Still on the **General** tab, select the **Destination Slave IP Mappings** button to map the Modbus Slave's IP addresses and their UIDs that the serial Modbus Master will attempt to communicate with.
4. For specialized configuration options, select the **Advanced** tab and configure as required.

Configuring a Slave Gateway

To configure a Slave Gateway (Modbus Master resides on the TCP/Ethernet network), do the following:

1. Set the serial port that is connected to the serial Modbus Slave(s) to the **Modbus Gateway** profile.
2. In the **Modbus Gateway** profile on the **General** tab, set the **Mode** to **Modbus Slave**.

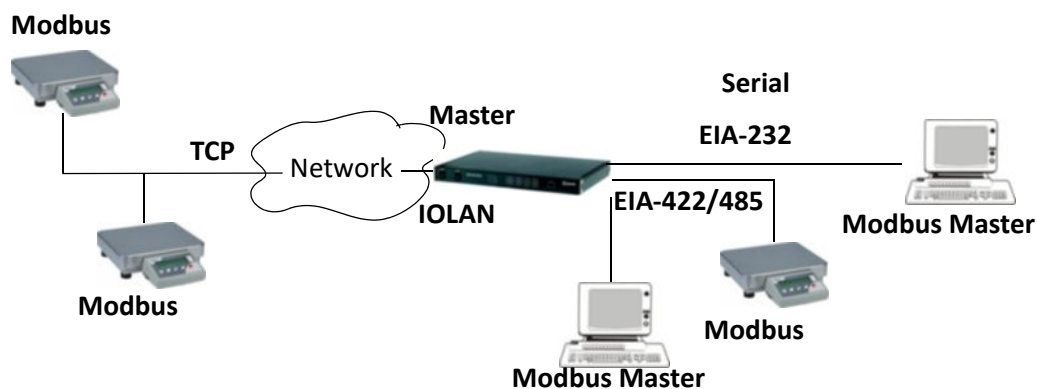
3. Still on the **General** tab, specify the Modbus Slave UIDs that the TCP Modbus Master will attempt to communicate with.
4. Still on the **General** tab, select the **Advanced Slave Settings** button to configure global Slave Gateway settings.
5. For specialized configuration options, select the **Advanced** tab and configure as required.

Modbus Gateway Settings

The scenarios in this section are used to illustrate how the IOLAN's Modbus Gateway settings are incorporated into a Modbus device environment. Depending on how your Modbus Master or Slave devices are distributed, the IOLAN can act as both a Slave and Master Gateway(s) on a multiport IOLAN or as either a Slave or Master Gateway on a single port IOLAN.

Modbus Master Gateway

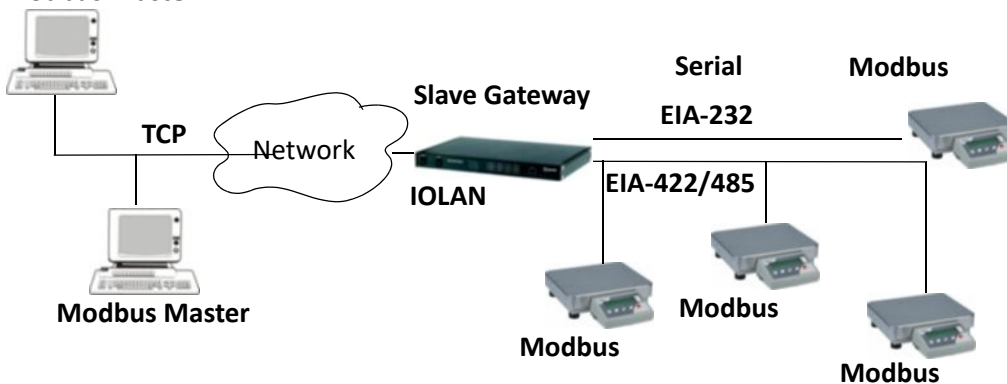
The IOLAN acts as a Master Gateway when the Modbus Master is connected to a serial port on the IOLAN. Each Modbus Master can communicate to UIDs 1-247.



Modbus Slave Gateway

The IOLAN acts as a Slave Gateway when the Modbus Master resides on the TCP/Ethernet network and the Modbus Slaves are connected to the serial ports on the IOLAN. Note: The IOLAN provides a single gateway to the network-attached Modbus Masters. This means that all Modbus Slaves attached to the IOLAN's serial ports must have a unique UID. Multiple Masters on the network can communicate with these Modbus Slaves. Note: If a transaction is in progress to a Modbus Slave, other requests to that same device will be queued until that transaction is complete.

Modbus Master



Modbus Serial Port Settings

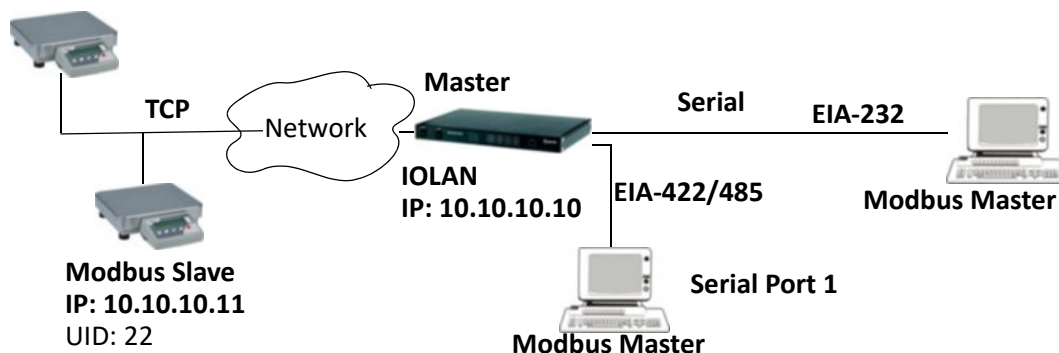
Modbus Master Settings

When the Modbus Masters is attached to the IOLAN's serial port, configure that serial port to the **Modbus Gateway** profile acting as a Modbus Master. You must configure the Modbus TCP Slaves on the TCP/Ethernet side so the IOLAN can properly route messages, using the Modbus Slave's UIDs, to the appropriate TCP-attached devices.

Modbus Slave

IP: 10.10.10.12

UID: 23



To configure the Modbus Master on serial port 1, do the following:

1. Select the **Modbus Gateway** profile for serial port 1.
2. On the **General** tab, enable the **Modbus Master** parameter.
3. Select the **Destination Slave IP Mappings** button and select the **Add** button in the **Destination Slave IP Mappings** window.
4. Configure the **Destination Slave IP Mappings** window as follows

The dialog box titled "Destination Modbus Slave IP Settings" contains the following fields and options:

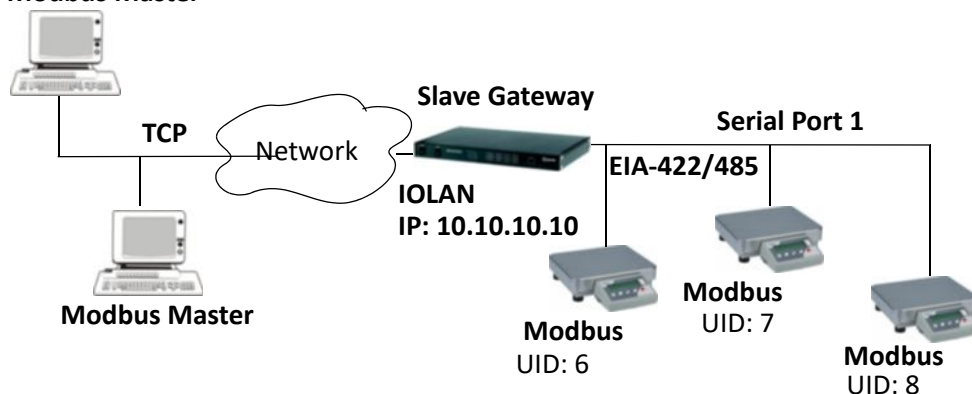
- UID: Start: 22, End: 23
- Destination Type: ☒ Host, ☐ Gateway
- IP Address: Start: 10.10.10.11, End: 10.10.10.12
- Protocol: ☒ TCP, ☐ UDP
- UDP/TCP Port: 502
- Buttons: OK, Cancel

The IOLAN will send a request and expect a response from the Modbus Slave with an IP Address of 10.10.10.11 on Port 502 with UID 22 and from the Modbus Slave with an IP Address of 10.10.10.12 on Port 502 with UID 23 (remember when **Type** is set to **Host**, the IOLAN increments the last octet of the IP address for each UID specified in the range).

Modbus Slave Settings

When you have Modbus Slaves on the serial side of the IOLAN, configure the serial port to the **Modbus Gateway** profile acting as a Modbus Slave. There is only one Slave Gateway in the IOLAN, so all Modbus serial Slaves must be configured uniquely for that one Slave Gateway; all serial Modbus Slaves must have unique UIDs, even if they reside on different serial ports, because they all must be configured to communicate through the one Slave Gateway.

Modbus Master



To configure the Modbus Gateway on serial port 1, do the following:

1. Select the **Modbus Gateway** profile for serial port 1.
2. On the **General** tab, enable the **Modbus Slave** parameter.
3. On the **General** tab, specify the **UID Range** as 6–8 as shown below:

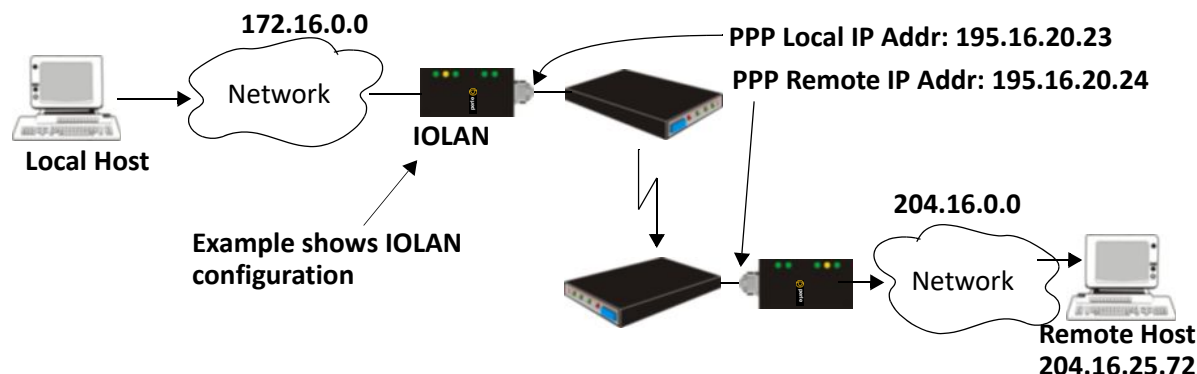
Select the **Advanced Slave Settings** button to verify that the default settings are acceptable.

The screenshot shows the 'Serial Port 1 Settings' window. The 'Profile' is set to 'Modbus Gateway'. The 'Name' field is empty. The 'General' tab is selected. Under 'Modbus Gateway Settings', the 'Mode' is set to 'Modbus Slave' (indicated by a radio button). The 'UID Range' is set to '6-8'. The 'Advanced Slave Settings...' button is visible. Under 'Protocol', 'Modbus/RTU' is selected (indicated by a radio button), and 'Append CR/LF' is unchecked.

Configuring PPP Dial On Demand

The IOLAN can be configured to access remote networks via modems connected to the serial interface of the IOLAN. By configuring the IOLAN for the **Remote Access (PPP)** profile, data that is destined for the

remote network will initiate a modem connection to the remote network to route the data to its appropriate destination.



If you want to configure a serial port to use PPP dial on demand, do the following:

1. Create an entry for the modem and its initialization string (**Serial, Advanced, Modems** tab).
2. Set the serial port to **Remote Access (PPP)**.
3. In **Remote Access (PPP)**, select the **Advanced** tab. Enable the **Connect** option and select **Dial Out**. Set the **Modem** parameter to the modem you just added. Enter the **Phone** number that the modem will be calling.
4. Still on the **Advanced** tab, set the **Idle Timeout** parameter to a value that is *not* zero (setting this value to zero creates a permanent connection).
5. On the **General** tab, enter one of the following:
 - A **Local** and/or **Remote IPv4 Address**
 - A **Local** and/or **Remote IPv6 Interface Identifier**

Note: .that this IP address or interface identifier should be on its own unique network; that is not part of the local or remote networks.

In this example, the local network has an IPv4 address of 172.16.0.0/16 and the remote network has an IPv4 address of 204.16.0.0/16, so we arbitrarily assigned the PPP **IPv4 Local IP Address** as 195.16.20.23 and the PPP **IPv4 Remote IP Address** as 195.16.20.24.

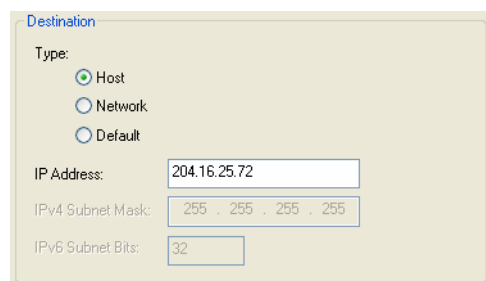
PPP Settings

IPv4 Local IP Address:	195 . 16 . 20 . 23
IPv4 Remote IP Address:	195 . 16 . 20 . 24
IPv4 Subnet Mask:	255 . 255 . 255 . 0

Next you need to create a gateway and destination route entry. Select **Network, Advanced**, and the **Route List** tab.

For the destination, if you want the connection to be able to reach any host in the remote network, set the **Type** to **Network** and specify the network IP address and subnet/prefix bits; if you want the connection to go directly to a specific remote host, set the **Type** to **Host** and specify the host's IP address.

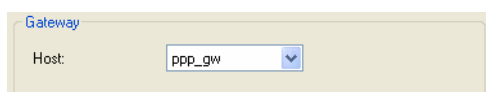
We want a specific host to be the destination, so we configured the **Type** as **Host**:



The Destination configuration window shows the following settings:

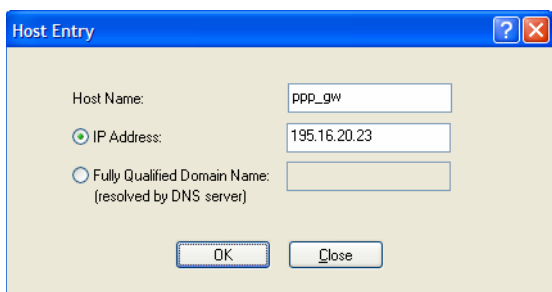
- Type: ☒ Host, ☐ Network, ☐ Default
- IP Address: 204.16.25.72
- IPv4 Subnet Mask: 255 . 255 . 255 . 255
- IPv6 Subnet Bits: 32

We also need to create a **Gateway** entry using the same PPP IPv4 local IP address. Any traffic that goes through the gateway will automatically cause PPP to dial out:



The Gateway configuration window shows the following setting:

- Host: ppp_gw



The Host Entry configuration window shows the following settings:

- Host Name: ppp_gw
- ☒ IP Address: 195.16.20.23
- ☐ Fully Qualified Domain Name: (resolved by DNS server)
- Buttons: OK, Close

Setting Up Printers

The IOLAN can communicate with printers on its serial ports using LPD and RCP protocols, as well as print handling software using TCP/IP.

Remote Printing Using LPD

When setting up a serial line that access a printer using LPD, do the following:

1. Set the serial port to **Printer** and configure the **Speed, Flow Control, Stop Bits, Parity, and Bits** parameters so that they match the printer's port settings.
2. Save your settings and restart the serial port.
3. Verify that LPD has been configured on the network host. To configure LPD on the network host, you need to know the name or IP address of the IOLAN and the print queue, either `raw_p<port_number>` for a raw data connection or `ascii_p<portnumber>` for an ASCII character connection. If you want to direct output to a hunt group, omit the port number(s). For example: `raw_p` or `ascii_p`. You can optionally append `_d` or `_f` to the queue name to add a `<control d>` or `<form feed>` to the end of the print job.
4. To execute a print job on a UNIX Linux system, use the following syntax:
5. `lp -d raw_p<port_number> <filename>`

Remote Printing Using RCP

When setting up a serial port that accesses a printer using RCP, do the following:

1. Set the serial port to **Printer** and configure the **Speed, Flow Control, Stop Bits, Parity, and Bits** parameters so that they match the printer's port settings.
2. Save your settings and restart the serial port.
3. To execute a print job, use either of the following syntaxes:
4. `rnp <filename> <ip_address>:<line_name>`

or

```
rnp <filename> <IOLAN_Name><line_name>
```

where `<#>` is the IOLAN serial port number.

Remote Printing Using Host-Based Print Handling Software

Printers connected to the IOLAN can be accessed by TCP/IP hosts using print handling software.

1. Set the serial port to **TCP Sockets**. Enable the **Listen for connection option**. On the **Hardware** tab, configure the **Speed, Flow Control, Stop Bits, Parity, and Bits** parameters so that they match the printer's port settings.
2. Save your settings and restart the serial port.
3. The print handling software needs to know the **Name** of the IOLAN and the **TCP Port** number assigned to the printer serial port.

Configuring a Virtual Private Network

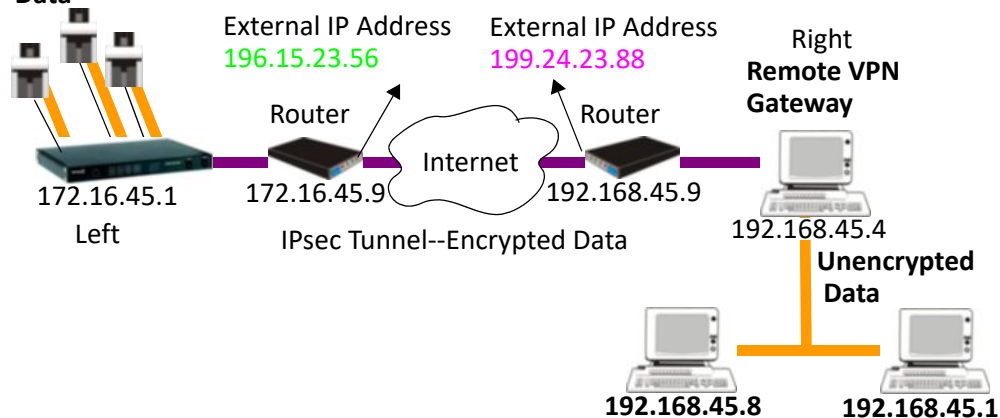
You can configure the IOLAN to act as a Virtual Private Network (VPN) gateway using the IPsec protocol. Any of the following scenarios can be configured using one IOLAN and a host/server running IPsec software or two IOLANs, each acting as the VPN gateway. All the examples have **NAT Traversal (NAT_T)** enabled, since both VPN gateways are running through routers.

IOLAN-to-Host/Network

The following example shows how to configure an IPsec tunnel between serial devices connected to the IOLAN and a host/network. **NAT Traversal (NAT_T)** is enabled in this example (on both sides) because the VPN tunnel is going private network to public network to private network. This example uses an RSA

signature for the authentication method, so the steps required to configure the authentication are in this example.

Unencrypted Data



Configure the IPsec tunnel in the IOLAN:

1. Use a utility (for example, Openswan's newhostkey/showhostkey utilities) to generate the RSA signature public key for the Remote VPN gateway. Copy the public key portion to a file using the following format:

```
<description>=<keydata>
```

or just

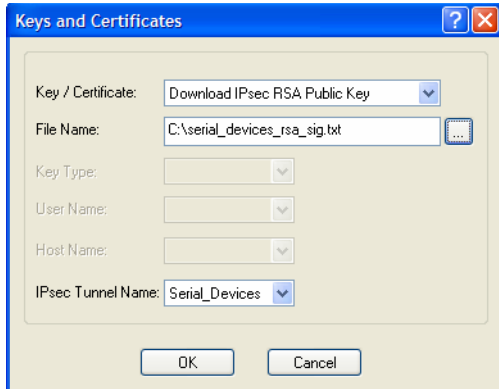
```
<keydata>
```

For example:

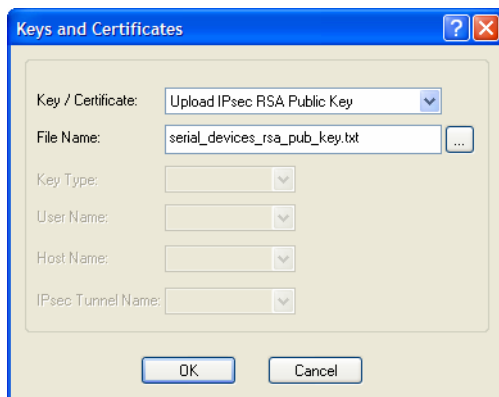
```
# RSA 1024 bits   scs48_vpn   Tue Jan  3 15:29:33 2006
leftrsasigkey=0sAQOEmzSTdNv1ZUJW9UmPtUY84gM5AGEAOq9gUwFqnOUSeSfnuXlxPe+Mc
+ufXYvglvxyYZ0XhdIh1FwFeeIQLyRvD447mjrIMFjJfheMUTHgOZhvWSE18ZfGEXNOo7yagZq
Lzjxu9XJIA2SAGV+/LL3epPqW2fV5ORxVrf7uWn7I5FQ==
```

Note that the pound sign (#) indicates a comment line and all characters in that line are ignored. The key value itself should not have an carriage returns.

2. In the DeviceManager, select **Tools, Advanced, Keys and Certificates**. In the WebManager, select **Tools, Administration, Keys/Certificates**. Download the RSA signature public file (for the Remote VPN Gateway) to the DeviceManager, specifying the IPsec tunnel it's for:



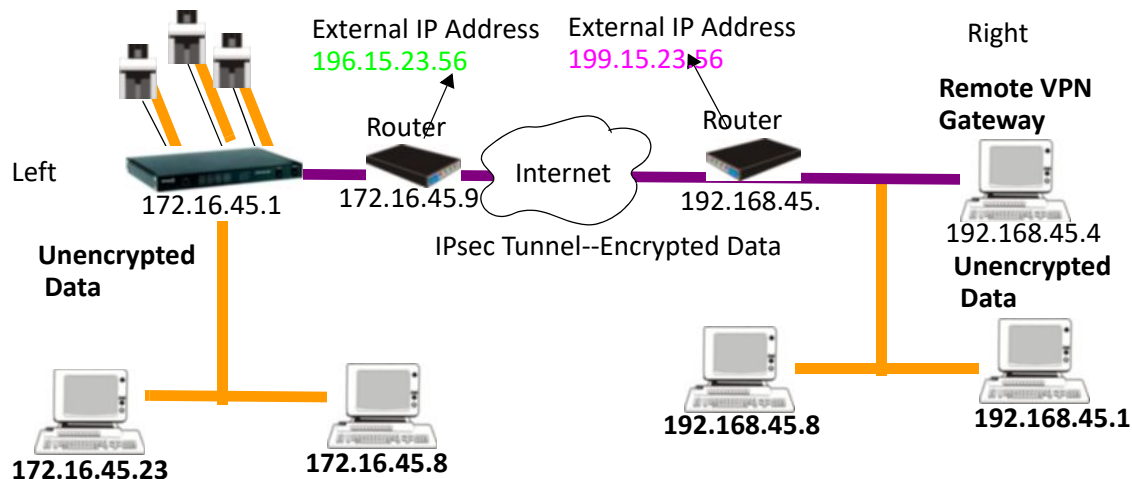
In the same **Keys and Certificates** window, upload the IOLAN's RSA signature public key:



Install the IOLAN's public key in the remote VPN gateway for the Serial_Devices IPsec tunnel. Enable the **IPsec** service found in **Security, Services**.

Network-to-Network

The following examples shows how to configure a network-to-network IPsec tunnel. This example uses the X.509 Certificate authentication method, so it includes the configuration requirements for the X.509 certificate. **NAT Traversal (NAT_T)** is enabled in this example (on both sides) because the VPN tunnel is going private network to public network to private network. Notice also that the serial devices connected to the IOLAN can be accessed by the VPN tunnel, since they are included in the network configuration as part of the **172.16.45.0** subnetwork.



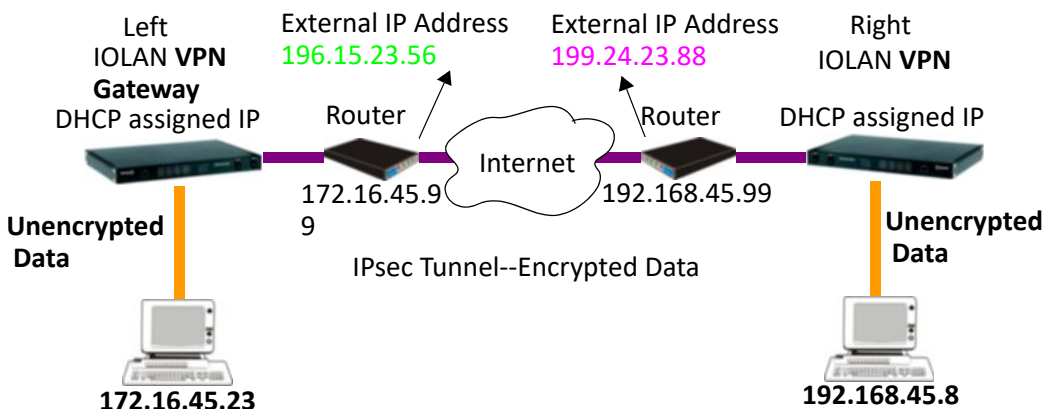
1. Configure the IPsec tunnel in the IOLAN.

The screenshot shows the 'IPsec Tunnel' configuration window. The 'Name' field is 'Net-to-Net'. The 'Authentication Method' is 'X.509 Certificate'. The 'Secret' field is empty. The 'Local Device (IOLAN)' is set to 'Left'. The 'Local' configuration section includes: IP Address: 172.16.45.1, External IP Address: 196.15.23.56, Next Hop: 172.16.45.99, Host/Network Address: 172.16.45.0, IPv4 Subnet Mask: 255 . 255 . 255 . 0, and IPv6 Subnet Bits: 0. The 'Remote' configuration section includes: IP Address: 199.15.23.56, External IP Address: (empty), Next Hop: 0.0.0.0, Host/Network Address: 192.168.45.0, IPv4 Subnet Mask: 255 . 255 . 255 . 0, and IPv6 Subnet Bits: 0. The 'Boot Action' is set to 'Start'. The 'OK' and 'Cancel' buttons are at the bottom.

2. Select the **Remote Validation Criteria** button and enable and populate the fields that are required for the remote X.509 certificate validation. If you just want to validate the X.509 certificate signer, you do not need to enable any of the remote validation criteria fields.
3. If the signer of the remote X.509 certificate has not already been included in the CA list file that has already been downloaded to the IOLAN, you need to add (append) the signer of the X.509 certificate to the CA list file and then download the file to the IOLAN by selecting **Tools, Advanced, Keys and Certificates**. In the **Keys and Certificates** window, select **Download SSL/TLS CA** and the file name and select **OK**. Note that this file must be a concatenation of all certificate signers required for any SSL/TLS, LDAP, SSH, and/or IPsec connections.
4. Enable the **IPsec** service found in **Security, Services**.

Host-to-Host

The following example shows how to configure two IOLANs to work as VPN gateways for a host-to-host IPsec tunnel. **NAT Traversal (NAT_T)** is enabled in this example (on both sides) because the VPN tunnel is going private network to public network to private network. In this example, both of the IOLAN VPN gateways have a DHCP assigned IP address.



1. The following window configures the Left IOLAN VPN Gateway.

The screenshot shows the 'IPsec Tunnel' configuration window. The 'Name' field is set to 'Right'. The 'Authentication Method' is 'Shared Secret'. The 'Secret' field is masked with dots. The 'Local Device (IOLAN)' is set to 'Right'. The 'Local' section has the following fields: 'IP Address' set to '%defaultroute', 'External IP Address' set to '199.24.23.88', 'Next Hop' set to '192.168.45.99', 'Host/Network Address' set to '192.168.45.87', 'IPv4 Subnet Mask' set to '255 . 255 . 255 . 255', and 'IPv6 Subnet Bits' set to '0'. The 'Remote' section has the following fields: 'IP Address' set to '%any', 'External IP Address' is empty, 'Next Hop' set to '0.0.0.0', 'Host/Network Address' set to '172.16.45.23', 'IPv4 Subnet Mask' set to '255 . 255 . 255 . 255', and 'IPv6 Subnet Bits' set to '0'. The 'Boot Action' is set to 'Add'. The 'OK' and 'Cancel' buttons are at the bottom.

`%defaultroute` is entered for the **Local IP Address** because the IP address is DHCP assigned and is therefore subject to change.

2. The following window configures the Right IOLAN VPN Gateway.

The image shows the 'IPsec Tunnel' configuration window. At the top, the 'Name' field is set to 'Right'. The 'Authentication Method' is set to 'Shared Secret', and the 'Secret' field contains five dots. The 'Local Device (IOLAN)' section has 'Right' selected with a radio button. Below this, there are two main sections: 'Local' and 'Remote'. The 'Local' section has fields for 'IP Address' (set to '%defaultroute'), 'External IP Address' (199.24.23.88), 'Next Hop' (192.168.45.99), 'Host/Network Address' (192.168.45.87), 'IPv4 Subnet Mask' (255 . 255 . 255 . 255), and 'IPv6 Subnet Bits' (0). The 'Remote' section has fields for 'IP Address' (set to '%any'), 'External IP Address' (empty), 'Next Hop' (0.0.0.0), 'Host/Network Address' (172.16.45.23), 'IPv4 Subnet Mask' (255 . 255 . 255 . 255), and 'IPv6 Subnet Bits' (0). At the bottom, the 'Boot Action' is set to 'Add'. There are 'OK' and 'Cancel' buttons at the bottom right.

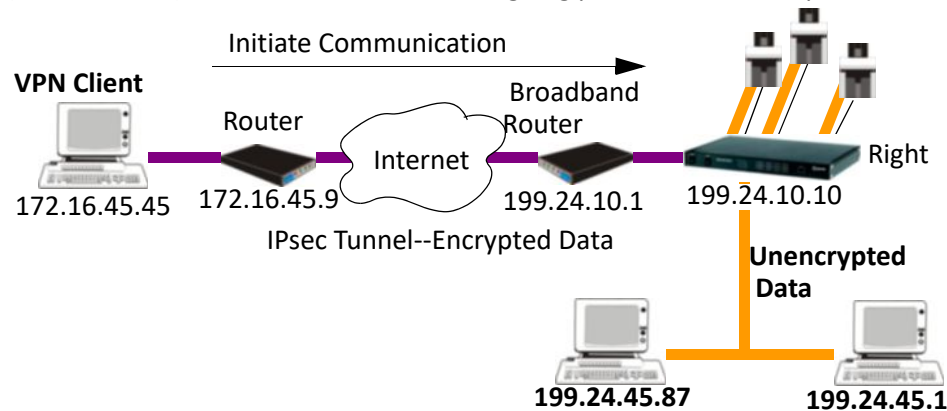
`%defaultroute` is entered for the **Local IP Address** because the IP address is DHCP assigned and is therefore subject to change.

`%any` is entered for the **Remote IP Address** to indicate that it will accept a VPN connection from any host/network; this is necessary because the Left IOLAN VPN gateway is DHCP assigned and cannot be known. Also note that **Boot Action** on the Left IOLAN VPN gateway is set to **Start**, meaning that it will try to initiate the VPN connection, while the **Boot Action** on the Right IOLAN VPN gateway is set to **Add**, which will listen for a VPN connection request.

Enable the **IPsec** service found in **Security, Services**.

VPN Client-to-Network

The following example shows how to configure a VPN client-to-network IPsec tunnel. In this example, the IOLAN will accept VPN connections from multiple VPN clients on private networks that want to access the public **199.24.0.0** subnetwork through the VPN gateway. **NAT Traversal (NAT_T)** is disabled in this example (on both sides) because the VPN tunnel is going private network to public network.



Configure the IPsec tunnel in the IOLAN:

The screenshot shows the **IPsec Tunnel** configuration window. The **Name** field is set to **VPNClient-to-Net**. The **Authentication Method** is set to **Shared Secret**, and the **Secret** field is masked with dots. The **Local Device (IOLAN)** is set to **Right**. The **Local** section shows: **IP Address** (199.24.10.10), **External IP Address** (blank), **Next Hop** (199.24.10.1), **Host/Network Address** (199.24.0.0), **IPv4 Subnet Mask** (255.255.0.0), and **IPv6 Subnet Bits** (0). The **Remote** section shows: **IP Address** (%any), **External IP Address** (blank), **Next Hop** (0.0.0.0), **Host/Network Address** (0.0.0.0), **IPv4 Subnet Mask** (255.255.255.255), and **IPv6 Subnet Bits** (0). The **Boot Action** is set to **Add**. The **OK** and **Cancel** buttons are at the bottom.

The **Remote IP Address** field is set to **any** to allow any VPN client to communicate in the IPsec tunnel that can validate the **Secret**. Also, the **Remote Host/Network** field is configured for **0.0.0.0** to allow any remote peer private IP address (RFC 1918—10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) access to the IPsec tunnel. Lastly, the **Boot Action** is set to **Add** to listen for an IPsec tunnel connection.

Configuring HTTP Tunnels

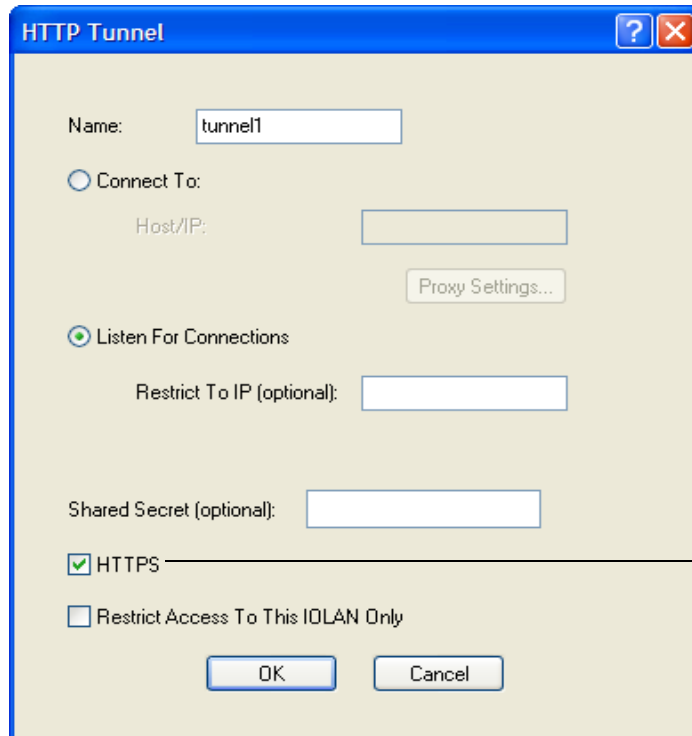
Note: When HTTP tunneling is used TCP and UDP ports 50000 and above are reserved and should not be configured by the user.

Serial-to Serial

The following example will demonstrate how to set up a serial device (VT100 Terminal) to serial device (Linux host, console port) connection via an HTTPS tunnel. HTTPS will be used because data security is required. Because IOLAN 1 is behind the firewall, it will need to initiate the HTTP tunnel connection.

See parameters for

Configure a “Listen for connection” HTTP tunnel on IOLAN 2



The screenshot shows the 'HTTP Tunnel' configuration window. It has a title bar with a question mark and a close button. The window contains the following fields and options:

- Name:** A text box containing 'tunnel1'.
- Connect To:** A radio button that is currently unselected.
- Host/IP:** A text box next to the 'Connect To' radio button.
- Proxy Settings...:** A button next to the 'Host/IP' text box.
- Listen For Connections:** A radio button that is currently selected.
- Restrict To IP (optional):** A text box next to the 'Listen For Connections' radio button.
- Shared Secret (optional):** A text box.
- HTTPS:** A checkbox that is checked.
- Restrict Access To This IOLAN Only:** An unchecked checkbox.
- OK** and **Cancel** buttons at the bottom.

Check HTTPS for secure tunnel connection. This must match configuration IOLAN 1

On IOLAN 1, under *Serial port configuration*, select serial ports and configure for Terminal profile.

Specify a terminal type

Protocol - Telnet

Add host IP address for IOLAN 2

TCP port number must match TCP port number on IOLAN 2

Select tunnel1

On IOLAN 2, under *serial port configuration*, select serial port and configure for Console Management profile.

Protocol - Telnet

TCP port number must match TCP port number on IOLAN 1

The setup for HTTP Tunnel serial-to-serial is now complete.

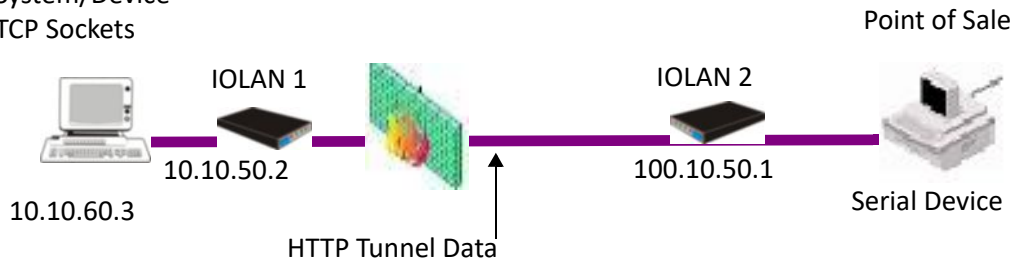
Serial-to Host

The following example will demonstrate how to setup a serial device (Point of Sale terminal) to an IP host (100.10.60.3) connection via an HTTP tunnel. Because IOLAN 1 is behind the firewall, it will need to initiate the tunnel connection to IOLAN 2. At the application level, the serial device will initiate the connection with the IP host.

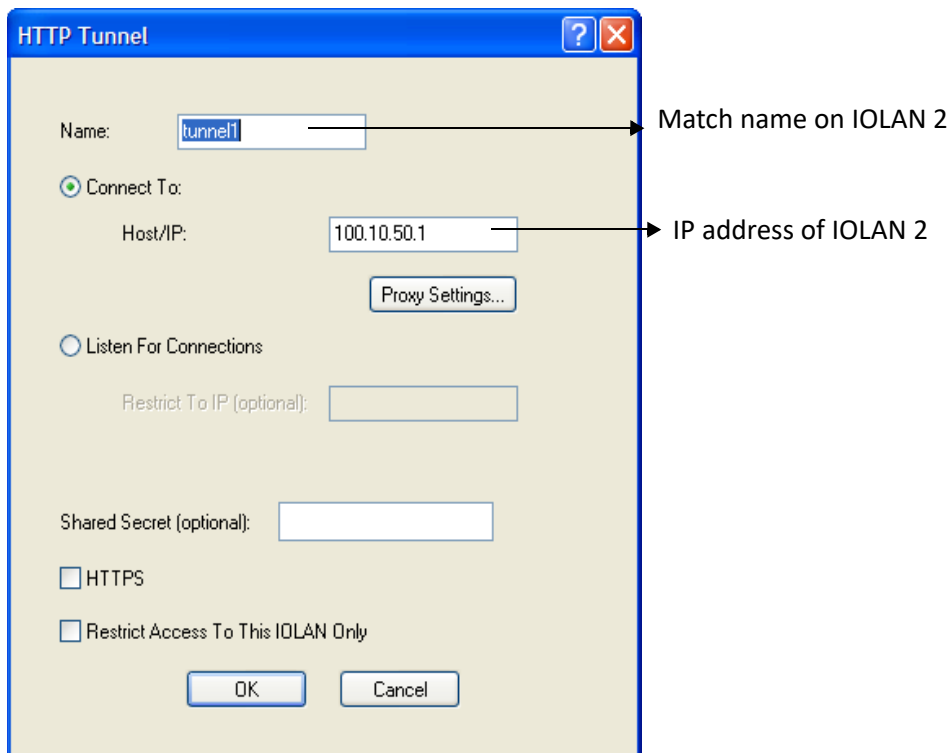
For more HTTP tunneling configuration parameters see [Configuring HTTP Tunnels](#).

System/Device

TCP Sockets



Configure a “connect to” HTTP tunnel on IOLAN 1.



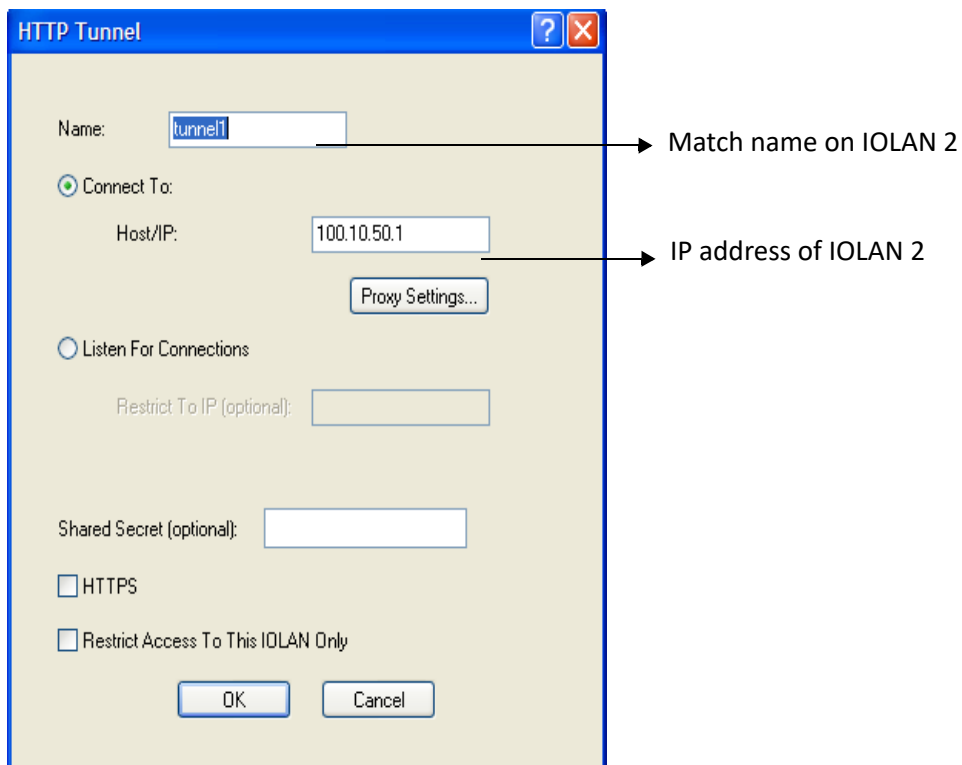
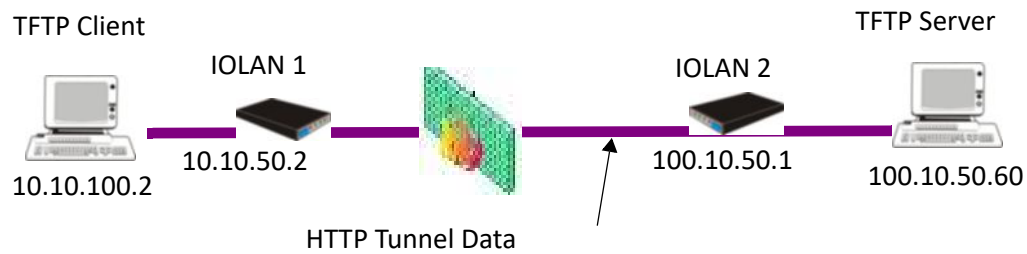
Configure a “Listen for connection” HTTP tunnel on IOLAN 2

Host-to Host

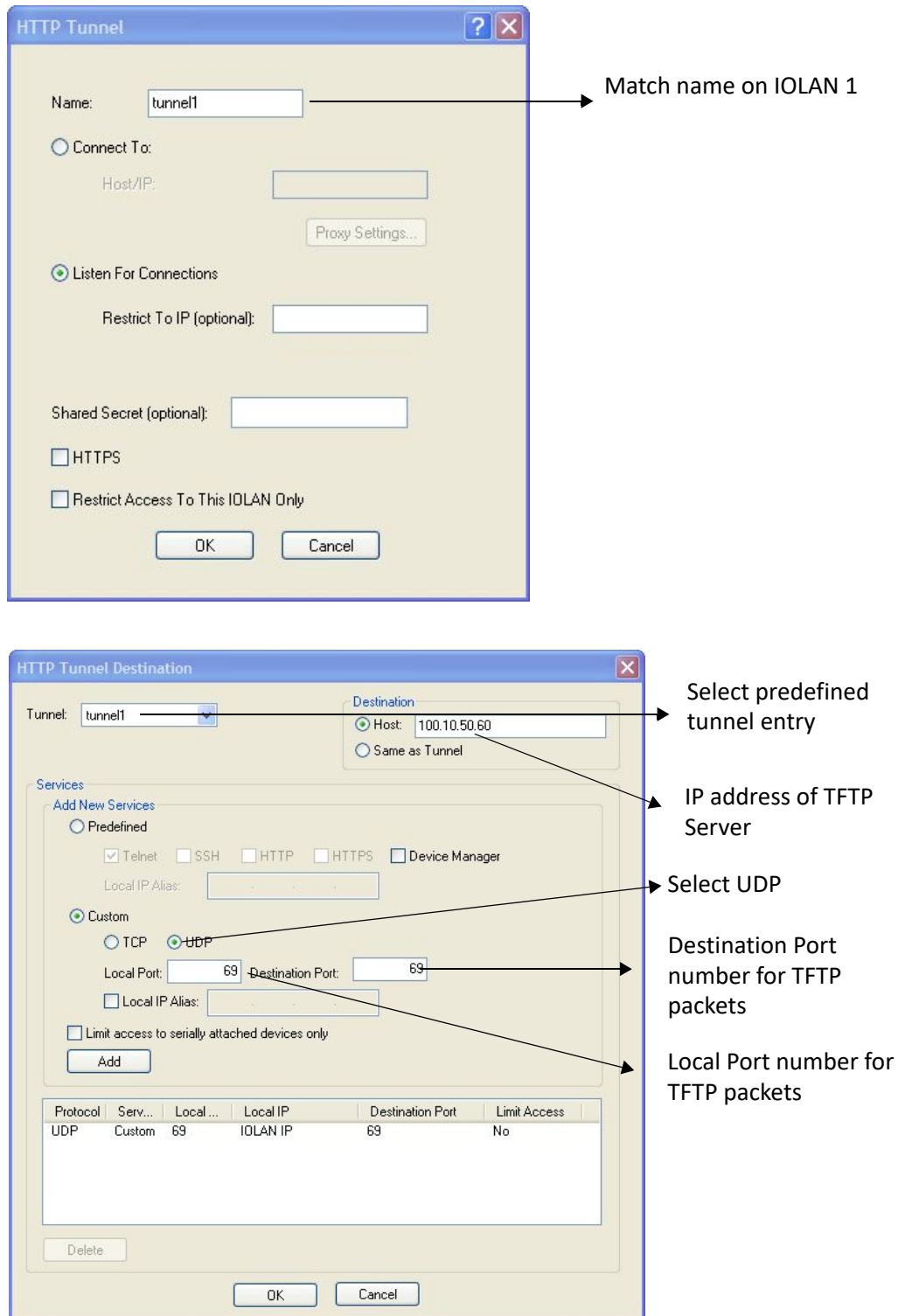
The following example will demonstrate how to setup an IP Host (10.10.100.2) to an IP Host (100.10.50.60) connection via an HTTP tunnel. In this example, the hosts are doing a TFTP transfer which uses the UDP protocol.

Because IOLAN 1 is behind the firewall, it will need to initiate the tunnel connection to IOLAN 2.

For more HTTP tunneling configuration parameters see [Configuring HTTP Tunnels](#).



Configure a "Listen for connection" HTTP tunnel.



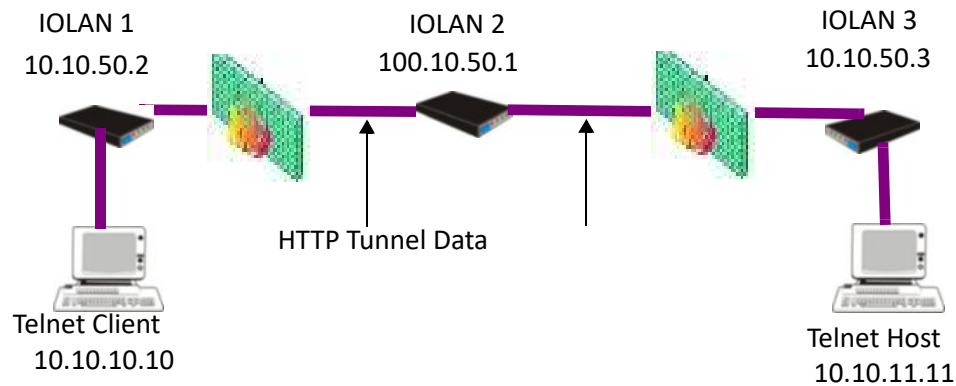
On IOLAN 1, under *HTTP Tunnel*, add a Tunnel destination.
The setup for HTTP Tunnel Host-to-Host is now complete.

Tunnel Relay

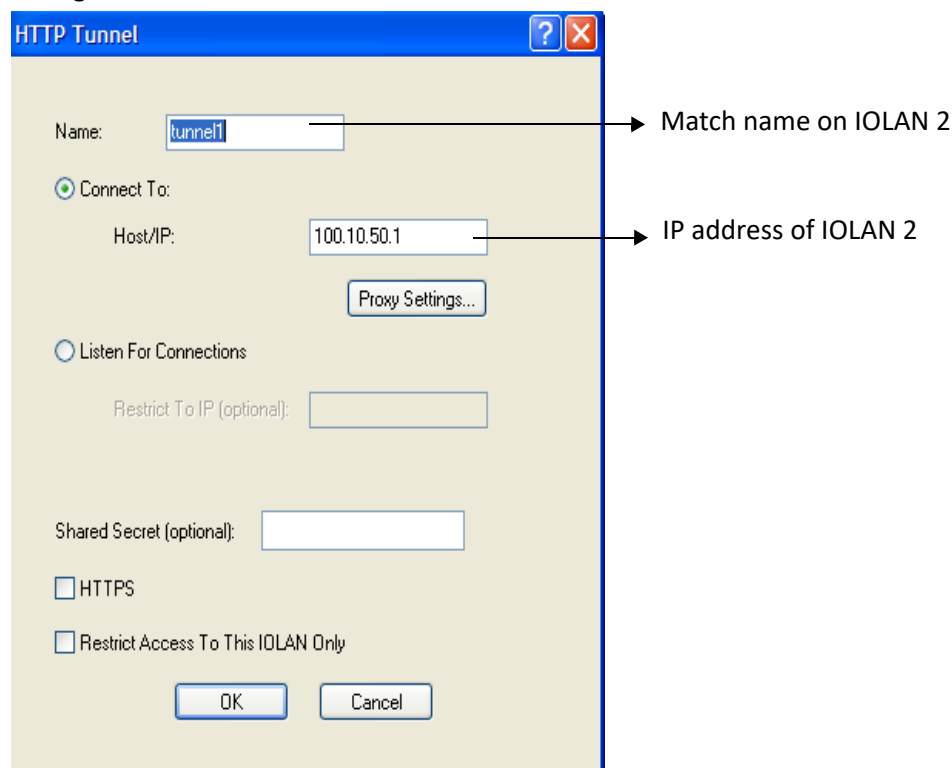
The following example will demonstrate how to setup an IP host (10.10.10.10) to an IP Host (10.10.11.11) connection using HTTP tunnels when both hosts are sitting behind a firewall. To do this, a third IOLAN which is not behind a firewall is required.

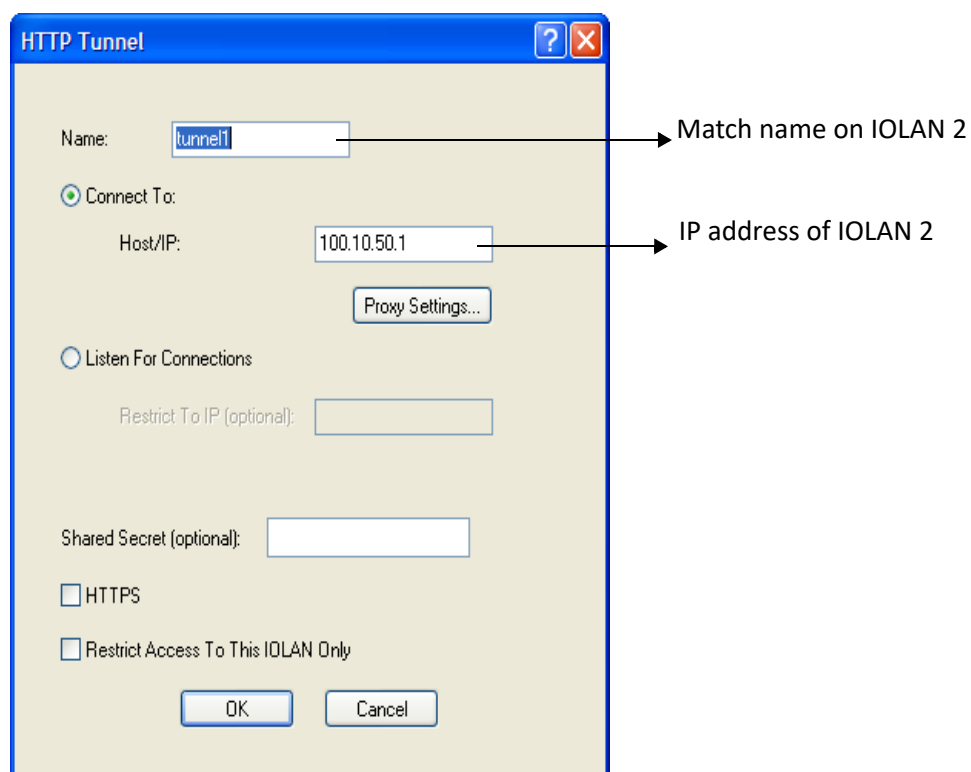
Because IOLAN 1 and IOLAN 3 are both behind a firewall, each will need to initiate a connection to IOLAN2 who is in the open.

For more Tunnel Relay configuration parameters see [Serial Tunneling General Parameters](#).

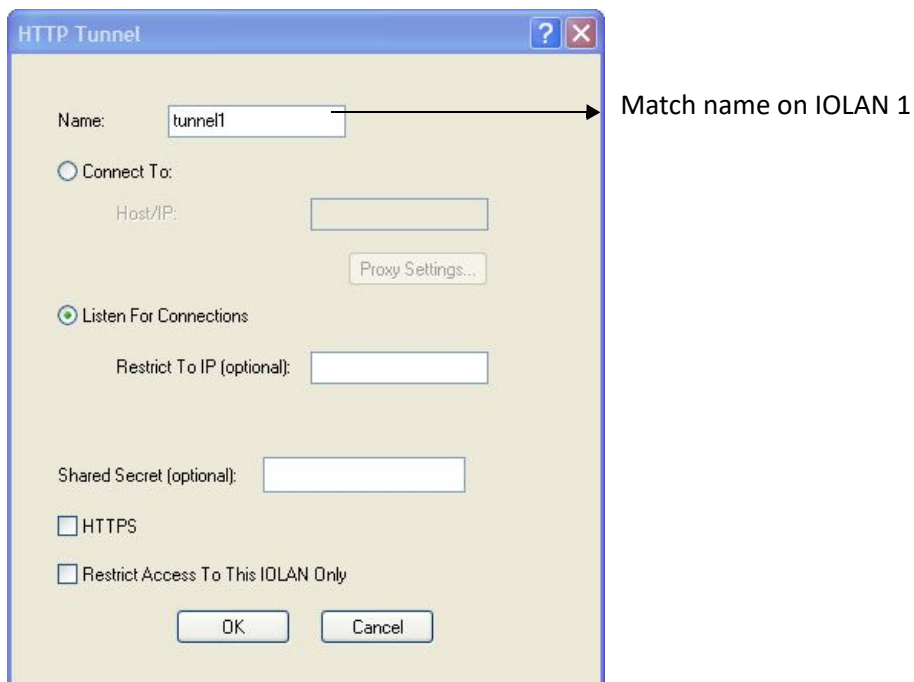


Configure a “connect to” HTTP tunnel on IOLAN 1.

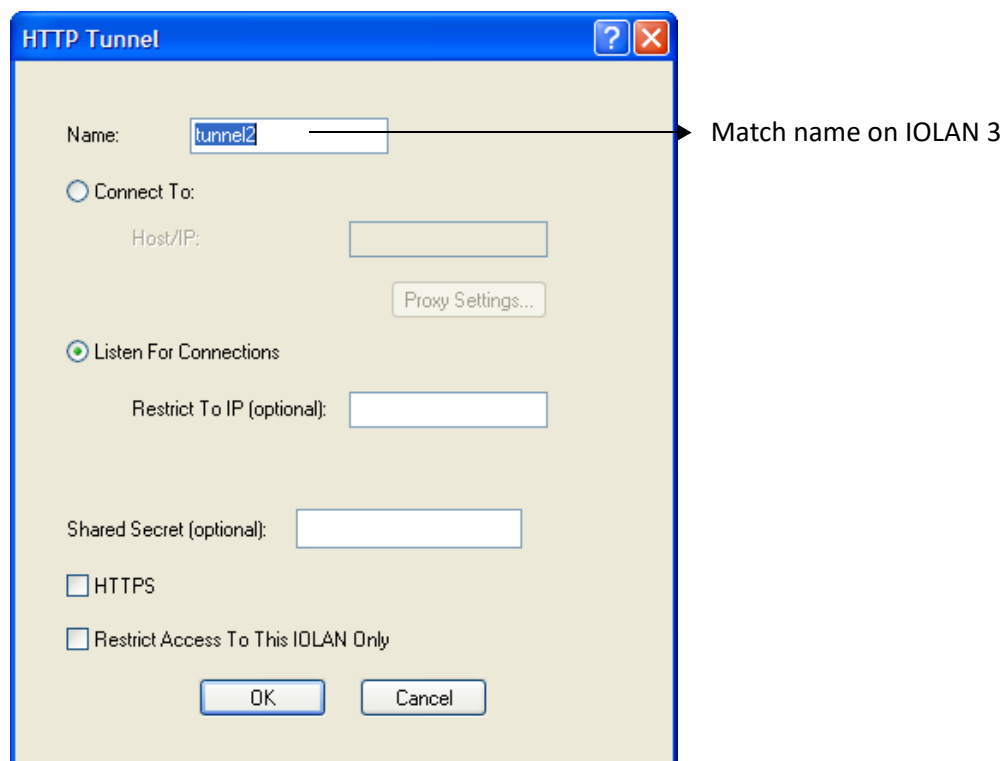




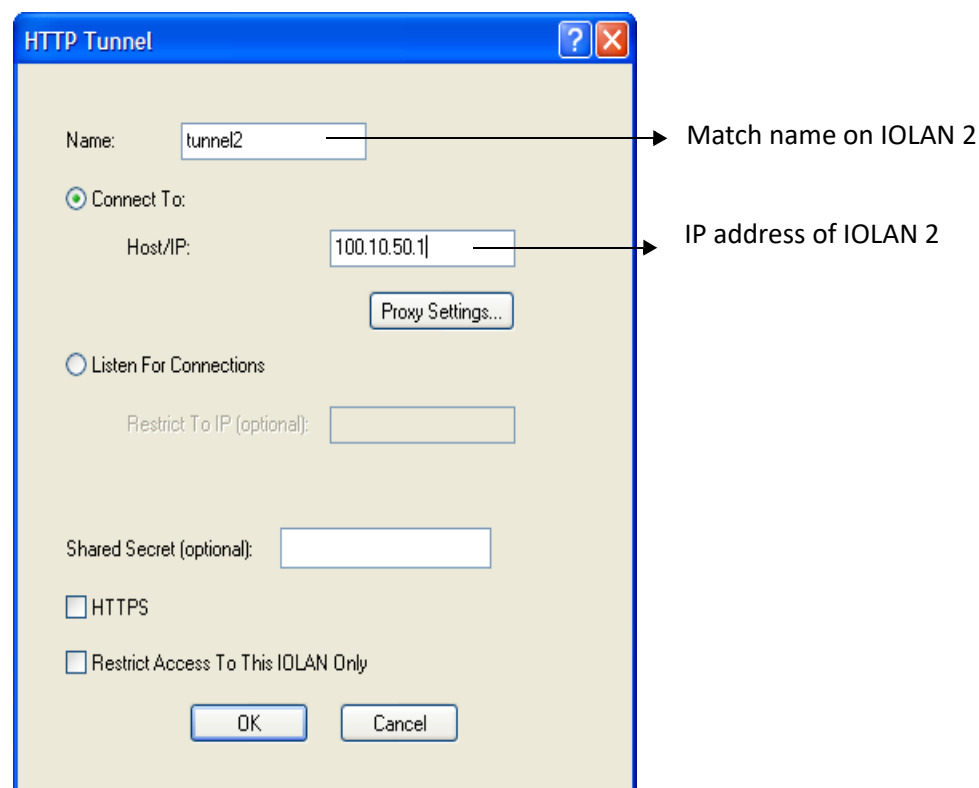
Configure a “Listen for connection” HTTP tunnel on IOLAN 2.



Configure a second “Listen for connection to IOLAN



Configure a “connect to” HTTP tunnel on IOLAN



On IOLAN 1, under *HTTP Tunnel*, add a Tunnel destination.

HTTP Tunnel Destination

Tunnel:

Destination: ☐ Host:
☒ Same as Tunnel

Services: ☐ Predefined
☐ Telnet ☐ SSH ☐ HTTP ☐ HTTPS ☐ Device Manager

Local IP Alias:

☒ Custom
☒ TCP ☐ UDP

Local Port: Destination Port:

☐ Local IP Alias:

☐ Limit access to serially attached devices only

Add

Protocol	Serv...	Local ...	Local IP	Destination Port	Limit Access
TCP	Custom	40002	IOLAN IP	40001	No

Delete

OK Cancel

Select tunnel1

Select Same as Tunnel

Select TCP

Destination port number to be used by IOLAN 1 for communications. Default starts at 40001.

This is the port number the telnet client will use.

On IOLAN 2, under *HTTP Tunnel*, add a Tunnel destination.

HTTP Tunnel Destination

Tunnel:

Destination: ☒ Host:
☐ Same as Tunnel

Services: ☐ Predefined
☒ Telnet ☐ SSH ☐ HTTP ☐ HTTPS ☐ Device Manager

Local IP Alias:

☒ Custom
☒ TCP ☐ UDP

Local Port: Destination Port:

☐ Local IP Alias:

☐ Limit access to serially attached devices only

Add

Protocol	Serv...	Local ...	Local IP	Destination Port	Limit Access
TCP	Custom	40001	IOLAN IP	23	No

Delete

OK Cancel

Select tunnel2

IP address of final destination Telnet host

Select TCP

Destination port set to 23 for Telnet protocol

Local port number to be used by IOLAN 2 for communications.

Note: This value must match destination port number on IOLAN 1

The setup for HTTP Tunnel Relay is now complete.

Valid SSL/TLS Ciphers

This appendix contains a table that shows valid SSL/TLS cipher combinations.

Note: Some combinations of cipher groups are not available on FIPS firmware versions.

Full Name	Key-Exchange	Auth	Encryption	Key-Size	HMAC
EDCHE-ECDSA-AES256-GCM-SHA384	Kx=ECDH	Au=ECDSA	Enc=AES-GCM	256	Mac=SHA384
ECDHE-ECDSA-AES256-SHA384	Kx=ECDH	Au=ECDSA	Enc=AES	256	Mac=SHA384
ECDHE-ECDSA-AES256-SHA	Kx=ECDH	Au=ECDSA	Enc=AES	256	Mac=SHA1
DHE-DSS-AES256-GCM-SHA384	Kx=DH	Au=DSS	Enc=AES-GCM	256	Mac=SHA384
DHE-RSA-AES256-GCM-SHA384	Kx=DH	RSA	Enc=AES-GCM	256	Mac=SHA384
DHE-RSA-AES256-SHA256	Kx=DH	RSA	Enc=AES	256	Mac=SHA256
AES256-GCM-SHA384	Kx=RSA	RSA	Enc=AES-GCM	256	Mac=SHA384
AES256-SHA256	Kx=RSA	RSA	Enc=AES	256	Mac=SHA256
DHE-DSS-AES256-SHA256	Kx=DH	DSS	Enc=AES	256	Mac=SHA256
DHE-RSA-AES256-SHA	Kx=DH	RSA	Enc=AES	256	Mac=SHA1
DHE-DSS-AES256-SHA	Kx=DH	DSS	Enc=AES	256	Mac=SHA1
ADH-AES256-GCM-SHA384	Kx=DH	None	Enc=AES-GCM	256	Mac=SHA384
ADH-AES256-SHA256	Kx=DH	None	Enc=AES	256	Mac=SHA256
ADH-AES256-SHA	Kx=DH	None	Enc=AES	256	SHA1
AES256-SHA	Kx=RSA	Au=RSA	Enc=AES	256	Mac=SHA1
ECDHE-RSA-AES128-GCM-SHA256	Kx=ECDH	Au=RSA	Enc=AES-GCM	128	Mac=SHA256
ECDHE-ECDSA-AES128-GCM-SHA256	Kx=ECDH	Au=ECDSA	Enc=AES-GCM	128	SHA256
ECDHE-ECDSA-AES128-SHA256	Kx=ECDH	Au=ECDSA	Enc=AES	128	SHA256
ECDHE-ECDSA-AES128-SHA	Kx=ECDH	Au=ECDSA	Enc=AES	128	SHA1
DHE-DSS-AES128-GCM-SHA256	Kx=DH	Au=DSS	Enc=AES-GCM	128	SHA256

Full Name	Key-Exchange	Auth	Encryption	Key-Size	HMAC
DHE-RSA-AES128-GCM-SHA256	Kx=DH	Au=RSA	Enc=AES-GCM	128	SHA256
DHE-RSA-AES128-SHA256	Kx=DH	Au=RSA	Enc=AES	128	SHA256
DHE-DSS-AES128-SHA256	Kx=DH	Au=DSS	Enc=AES	128	SHA256
DHE-RSA-AES128-SHA	Kx=DH	Au=RSA	Enc=AES	128	SHA1
DHE-DSS-AES128-SHA	Kx=DH	Au=DSS	Enc=AES	128	SHA1
ADH-AES128-SHA256	Kx=DH	Au=None	Enc=AES	128	SHA256
ADH-AES128-SHA	Kx=DH	Au=None	Enc=AES	128	SHA1
AES128-GCM-SHA256	Kx=RSA	Au=RSA	Enc=AES-GCM	128	SHA256
AES128-SHA256	Kx=RSA	Au=RSA	Enc=AES	128	SHA256
AES128-SHA	Kx=RSA	Au=RSA	Enc=AES	128	SHA1
RC2-CBC-MD5	Kx=RSA	Au=RSA	Enc=RC2	128	MD5
ADH-RC4-MD5	Kx=DH	Au=None	Enc=RC4	128	MD5
RC4-SHA	Kx=RSA	AU=RSA	Enc=RC4	128	SHA1
RC54-MD5	Kx=RSA	Au=RSA	Enc=RC4	128	MD5
ECDHE-ECDSA-DES-CBC3-SHA	Kx=ECDH	Au=ECDSA	Enc=3DES	168	SHA1
EDH-RSA-DES-CBC3-SHA	Kx=DH	Au=RSA	Enc=3DES	168	SHA1
EDH-DSS-DES-CBC3-SHA	Kx=DH	Au=DSS	Enc=3DES	168	SHA1
ADH-DES-CBC3-SHA	Kx=DH	Au=None	Enc=3DES	168	SHA1
DES-CBC3-SHA	Kx=RSA	Au=RSA	Enc=3DES	168	SHA1
DES-CBC3-MD5	Kx=RSA	Au=RSA	Enc=3DES	168	MD5
EDH-RSA-DES-CBC-SHA	Kx=DH	Au=RSA	Enc=DES	56	SHA1
EDH-DSS-DES-CBC-SHA	Kx=DH	Au=DSS	Enc=DES	56	SHA1
ADH-DES-CBC-SHA	Kx=DH	Au=None	Enc=DES	56	SHA1
DES-CBC-SHA	Kx=RSA	Au=RSA	Enc=DES	56	SHA1
EXP-EDH-RSA-DES-CBC-SHA	Kx=DH-512	Au=RSA	Enc=DES	40	SHA1
EXP-EDH-DSS-DES-CBC-SHA	Kx=DH-512	Au=DSS	Enc=DES	40	SHA1
EXP-DES-CBC-SHA	Kx=RSA-512	Au=RSA	Enc=DES	40	SHA1
EXP-RC2-CBC-MD5	Kx=RSA-512	Au=RSA	Enc=RC2	40	MD5

Full Name	Key-Exchange	Auth	Encryption	Key-Size	HMAC
EXP-ADH-DES-CBC-SHA	Kx=DH-512	Au=none	Enc=DES	40	SHA1
EXP-ADH-RC4-MD5	Kx=DH-512	Au=none	Enc=RC4	40	MD5
EXP-RC4-MD5	Kx=RSA-512	Au=RSA	Enc=RC4	40	MD5

Virtual Modem Initialization Commands

You can initialize the modem connection using any of the following commands:

Command	Description	Options
ATQn	Quiet mode. Determines if result codes will be sent to the connected terminal. Basic results codes are OK, CONNECT, RING, NO CARRIER, and ERROR. Setting quiet mode also suppresses the "RING" message for incoming calls.	n=0, result codes will be sent. (default) n=1, no result codes will be sent.
ATVn	Verbose mode. Determines if result codes are displayed as text or numeric values.	n=0, display as numeric values. n=1, display as text. (default)
ATEn	Echo mode. Determines whether characters sent from the serial device will be echoed back by the IOLAN when VModem is in "command" mode. Any AT commands not supported will return an "ok" if n=1.	n=0, disable echo. n=1, enable echo. (default)
+++ATH	Hang up. This command instructs the IOLAN to terminate the current session and go into "command" mode.	
ATA	Answer call. Instructs the VModem to accept connection requests. VModem will give the terminal up to 3 minutes to answer the call. If the ATA is not received within 3 minutes, all pending sync messages will be discarded.	
ATI0	Return the modem manufacturer name.	
ATI3	Return the modem model name.	
ATS0	Sets the value of the S0 register. The S0 register controls the "auto answer" behavior. In "manual" mode, the IOLAN will not accept incoming sessions until an ATA is issued by the serial device. In "auto answer" mode, the IOLAN will automatically accept an incoming connection request.	Register=0, sets "manual answer" mode Register=1-255, "auto answer" mode (default)
AT&Z1	Set command allows the user to store an IP address and port number or phone number to use when making a connection. The user will issue an ATDS1 to cause the IOLAN to initiate the connection.	

Command	Description	Options
AT&Sn	Sets the behavior of IOLAN's DTR signal. (DSR from a DCE perspective)	n=0, DTR signal always high. (default) n=2, DTR signal acts as DCD. n=3, DTR signal acts as RI.
AT&Rn	Sets the behavior of IOLAN's RTS signal. (CTS from a DCE perspective) If line is configured for hardware flow control, the RTS is used for this purpose and the setting of this command is ignored.	n=0, RTS always high. (default). n=3, RTS signal acts as DCD. n=4, RTS signal acts as RI.
AT&Cn	Sets the behaviour of the DCD signal.	n=0, DCD always on. n=1, DCD follows state of connection (off when no connection, on when TCP connection exists). (default)
AT&F	Sets the modem back to the factory defaults. This is a hard-coded default configuration which does not look at any user configuration.	
ATS2	Sets the value of the S2 register. The S2 register controls which character is used to enter "command" mode. (this is the potential replacement for the +++ (default) in front of the ATH command). This register will hold the hexadecimal value of the "escape" character. Any value > 27 will disable the ability to escape into "command" mode.	
ATS12	Sets the value of the S12 register. The S12 register controls the minimum length of idle time which must elapse between the receipt of the escape character and the A (first character of the ATH sequence). Units are 1/50th of a second. The default is 50 = 1 second.	
ATO	(ATD with no phone number) Establishes a connection using the IP and port specified in the telephone number field.	
ATDS1	Establishes a connection using the IP and port (or phone number) specified in the Phone Number field (stored by the AT&Z1 command).	

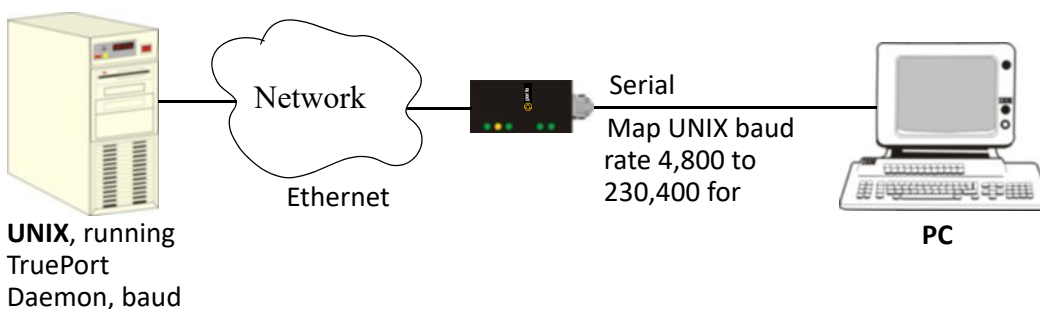
TruePort

This chapter provides information on TruePort and the Decoder utilities.

Trueport is a com port redirector utility for the IOLAN. It can be run in two modes:

- **TruePort Full mode**—This mode allows complete device control and operates exactly like a directly connected serial port. It provides a complete COM port interface between the attached serial device and the network.
- **TruePort Lite mode**—This mode provides a simple raw data interface between the device and the network. Although the port will still operate as a COM port, control signals are ignored. In this mode, the serial communications parameters must be configured on the IOLAN.

You use TruePort when you want to connect extra terminals to a server using the IOLAN rather than a multi-port serial card. TruePort is especially useful when you want to improve data security, as you can enable an SSL/TLS connection between the TruePort host port and the IOLAN. When run on UNIX, TruePort allows you to print directly from a terminal to an attached printer (transparent printing). You can also remap the slow baud rate of your UNIX server to a faster baud rate, as shown below.



Currently, TruePort is supported on Linux, Windows®, SCO®, Solaris®, and others. For a complete list of the supported operating systems, see the Perle website.

Decoder

If you are using **Port Buffering NFS Encryption**, you need to run the Decoder utility to view the port buffering logs. See the Readme file to install the Decoder utility on any of the following 32-bit platforms.

- Windows® 2000 and greater platform

Note: The Windows/DOS platform restricts the converted readable file to an 8.3 filename limitation.

- DOS
- Solaris x86
- Solaris Sparc 32-bit/64-bit
- Linux x86 v2.4.x

Modbus Remapping Feature

This appendix provides additional information about the Modbus Remapping feature.

Modbus Remapping Feature

The Modbus remapping feature allows a TCP Modbus Master to poll a Modbus slave device and have the IOLAN translate the UID to a different UID for the slave device. The Master UID has to be unique on the IOLAN. The Slave UID must be unique on each serial port. The translate rules are controlled by a file downloaded to the IOLAN.

The following procedure will allow you to use the Modbus remapping feature:

Create a configuration file

- The file must be called "modbus.remap"
- One translate rule per line
- The fields on a line are separated by a comma

Line format for one UID is:

- port, master_uid, slave_uid
- port: is the IOLAN port number that the slave is connected to
- master_uid: is the UID that the TCP Modbus Master uses
- slave_uid: is the UID that the Modbus slave uses

Line format for UID ranges is:

- port, master_start-master_end, slave_start-slave_end
- port: is the IOLAN port number that the slave is connected to
- master_start: is the first master UID in the range
- master_end: is the last master UID in the range
- slave_start: is the first slave UID in the range
- slave_end: is the last slave UID in the range

Configuring the Modbus UID Remapping Feature

1. On the serial port Modbus Gateway, configure Modbus slave. Configuration parameters such as "UID range" and UID Address Mode will be ignored in this mode of operation
 2. Download the "modbus_remap" file that you created to the IOLAN using:
 3. Device Manager: use "tools-advanced-custom files" dialog "download other file"
 4. Web Manager: use "administration-custom files" page "other file"
- CLI: use the command "netload customapp-file" command
 - See all network problems at a glance and take appropriate action

Data Logging Feature

This appendix provides additional information about the Data Logging Feature

Trueport Profile

The following features are not compatible when using the Data Logging feature.

- Allow Multiple Hosts to connect
- Connect to Multiple Hosts
- Monitor DSR or DCD
- Signals high when not under Trueport client control
- Message of the day
- Session timeout

TCP Socket Profile

The following features are not compatible when using the Data Logging feature.

- Allow Multiple Hosts to connect
- Connect to Multiple Hosts
- Monitor DSR or DCD
- Permit connections in both directions
- Authenticate user
- Message of the day
- Session timeout