



December 2016

Secure Device Servers - LES5011 to 5164
Secure Terminal Servers - LES6044 to 7244
Secure Console Servers - LES8084 to 8324

Secure Terminal Server Secure Console Server Secure Device Server User Guide

Version 4.8

5500183-48

CUSTOMER Order **toll-free** in the U.S 24 hours, 7 A.M. Monday to midnight Friday: **877-877-BBOX**
SUPPORT FREE technical support, 24 hours a day, 7 days a week: Call **724-746-5500** or fax **724-746-0746**
INFORMATION Mail order: **Black Box Corporation**, 1000 Park Drive, Lawrence, PA 15055-1018
Web site: **www.blackbox.com** * E-mail **info@blackbox.com**

Normas Oficiales Mexicanas (NOM) Electrical Safety Statement

INSTRUCCIONES DE SEGURIDAD

1. Todas las instrucciones de seguridad y operación deberán ser leídas antes de que el aparato eléctrico sea operado.
2. Las instrucciones de seguridad y operación deberán ser guardadas para referencia futura.
3. Todas las advertencias en el aparato eléctrico y en sus instrucciones de operación deben ser respetadas.
4. Todas las instrucciones de operación y uso deben ser seguidas.
5. El aparato eléctrico no deberá ser usado cerca del agua-por ejemplo, cerca de la tina de baño, lavabo, sótano mojado o cerca de una alberca, etc.
6. El aparato eléctrico debe ser usado únicamente con carritos o pedestales que sean recomendados por el fabricante.
7. El aparato eléctrico debe ser montado a la pared o al techo sólo como sea recomendado por el fabricante.
8. Servicio-El usuario no debe intentar dar servicio al equipo eléctrico más allá a lo descrito en las instrucciones de operación. Todo otro servicio deberá ser referido a personal de servicio calificado.
9. El aparato eléctrico debe ser situado de tal manera que su posición no interfiera su uso. La colocación del aparato eléctrico sobre una cama, sofá, alfombra o superficie similar puede bloquea la ventilación, no se debe colocar en libreros o gabinetes que impidan el flujo de aire por los orificios de ventilación.
10. El equipo eléctrico debe ser situado fuera del alcance de fuentes de calor como radiadores, registros de calor, estufas u otros aparatos (incluyendo amplificadores) que producen calor.
11. El aparato eléctrico deberá ser conectado a una fuente de poder sólo del tipo descrito en el instructivo de operación, o como se indique en el aparato.
12. Precaución debe ser tomada de tal manera que la tierra física y la polarización del equipo no sea eliminada.
13. Los cables de la fuente de poder deben ser guiados de tal manera que no sean pisados ni pellizcados por objetos colocados sobre o contra ellos, poniendo particular atención a los contactos y receptáculos donde salen del aparato.
14. El equipo eléctrico debe ser limpiado únicamente de acuerdo a las recomendaciones del fabricante.
15. En caso de existir, una antena externa deberá ser localizada lejos de las líneas de energía.
16. El cable de corriente deberá ser desconectado del cuando el equipo no sea usado por un largo periodo de tiempo.
17. Cuidado debe ser tomado de tal manera que objetos líquidos no sean derramados sobre la cubierta u orificios de ventilación.
18. Servicio por personal calificado deberá ser provisto cuando:
 - a. El cable de poder o el contacto ha sido dañado; u
 - b. Objetos han caído o líquido ha sido derramado dentro del aparato; o
 - c. El aparato ha sido expuesto a la lluvia; o
 - d. El aparato parece no operar normalmente o muestra un cambio en su desempeño; o
 - e. El aparato ha sido tirado o su cubierta ha sido dañada.

FCC Requirements for Telephone-Line Equipment

1. The Federal Communications Commission (FCC) has established rules which permit this device to be directly connected to the telephone network with standardized jacks. This equipment should not be used on party lines or coin lines.
2. If this device is malfunctioning, it may also be causing harm to the telephone network; this device should be disconnected until the source of the problem can be determined and until the repair has been made. If this is not done, the telephone company may temporarily disconnect service.
3. If you have problems with your telephone equipment after installing this device, disconnect this device from the line to see if it is causing the problem. If it is, contact your supplier or an authorized agent.
4. The telephone company may make changes in its technical operations and procedures. If any such changes affect the compatibility or use of this device, the telephone company is required to give adequate notice of the changes.
5. If the telephone company requests information on what equipment is connected to their lines, inform them of:
 - a. The telephone number that this unit is connected to.
 - b. The ringer equivalence number.
 - c. The USOC jack required: RJ-11C.
 - d. The FCC registration number.

Items (B) and (D) can be found on the unit's FCC label. The ringer equivalence number (REN) is used to determine how many devices can be connected to your telephone line. In most areas, the sum of the RENs of all devices on any one line should not exceed five. If too many devices are attached, they may not ring properly.

6. In the event of an equipment malfunction, all repairs should be performed by your supplier or an authorized agent. It is the responsibility of users requiring service to report the need for service to the supplier or to an authorized agent.

Certification Notice for Equipment Used in Canada

The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications-network protective, operation, and safety requirements. Industry Canada does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single-line individual service may be extended by means of a certified connector assembly (extension cord). The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized maintenance facility—in this case, Black Box. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

CAUTION: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

The LOAD NUMBER (LN) assigned to each terminal device denotes the percentage of the total load to be connected to a telephone loop which is used by the device, to prevent overloading.

The termination on a loop may consist of any combination of devices, subject only to the requirement that the total of the load numbers of all the devices does not exceed 100.

FEDERAL COMMUNICATIONS COMMISSION AND INDUSTRY CANADA RADIO FREQUENCY INTERFERENCE STATEMENTS

This equipment generates, uses, and can radiate radio-frequency energy, and if not installed and used properly, that is, in strict accordance with the manufacturer's instructions, may cause interference to radio communication. It has been tested and found to comply with the limits for a Class A computing device in accordance with the specifications in Subpart B of Part 15 of FCC rules, which are designed to provide reasonable protection against such interference when the equipment is operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user at his own expense will be required to take whatever measures may be necessary to correct the interference.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This digital apparatus does not exceed the Class A limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of Industry Canada.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Règlement sur le brouillage radioélectrique publié par le Industrie Canada.

Table of Contents

Preface	21
About This Book	21
Intended Audience	21
Documentation	21
Typeface Conventions	22
Online Help	22
Chapter 1 Introduction	23
About the Terminal Server	23
Terminal Server Models	23
Terminal Server Features	24
Hardware	24
.....	25
Software	26
Accessing the Terminal Server	26
General Features	26
Advanced Features	27
Security	27
Chapter 2 Hardware and Connectivity	28
Introduction	28
Terminal Server Components	28
What's Included	28
What You Need to Supply	28

Power Supply Specifications	29
Desktop Models	29
Power Over Ethernet (PoE) Models.....	29
Rack Mount Models.....	29
AC Power Requirements.....	29
Getting to Know Your Terminal Server	30
Overview.....	30
1-Port	31
2-Port	32
4-Port	32
Rack Mount	33
Console Port/LED View.....	33
Serial/Ethernet View.....	33
Console/Serial Switch	33
Console Mode	33
Serial Mode	34
Dedicated Console Port: Rack Mount Models	34
Powering Up the Terminal Server	34
Desktop/Rack Mount Models.....	34
Chapter 3 Configuration Methods	35
Introduction	35
Configuration Methods Overview.....	36
Configures an IP Address.....	36
Requires a Configured IP Address	36
Easy Config Wizard	37
DeviceManager.....	38
Overview.....	38
Access Platforms	38
Unique Features	38
Connecting to the Terminal Server Using DeviceManager	38
Using DeviceManager	40
Downloading Configuration	40
WebManager.....	41

Overview.....	41
Access Platforms	41
Features.....	41
Connecting to the Terminal Server Using WebManager	42
Using WebManager	43
Command Line Interface	44
Overview.....	44
Access Platforms	44
Features.....	44
Connecting to the Terminal Server Using the CLI.....	44
Through the Network.....	44
Through the Serial Port.....	45
Using the CLI	45
Menu.....	45
Overview.....	45
Access Platforms	45
Features.....	45
Connecting to the Terminal Server Using the Menu	45
Using the Menu.....	46
DHCP/BOOTP	47
Overview.....	47
Features.....	47
Connecting to the Terminal Server Using DHCP/BOOTP.....	47
Using DHCP/BOOTP.....	47
DHCP/BOOTP Parameters	48
SNMP.....	48
Overview.....	48
Access Platforms	48
Features.....	49
Connecting to the Terminal Server Using SNMP	49
Using the SNMP MIB	49
Chapter 4 Getting Started.....	50

Introduction	50
Easy Configuration Wizard	51
Setting Up the Network	52
Using DeviceManager	52
Using WebManager	53
Using a Direct Serial Connection to Specify an IP Address.....	53
Using a Direct Serial Connection to Enable BOOTP/DHCP	54
Using ARP-Ping	55
For an IPv6 Network	55
Setting Up the Serial Port(s)	56
Setting Up Users	58
Chapter 5 Using DeviceManager and WebManager.....	59
Introduction	59
Navigating DeviceManager/WebManager	59
DeviceManager	60
WebManager	61
EasyPort Web	61
Using DeviceManager to Connect to the Terminal Server	62
Starting a New Session.....	62
Assigning a Temporary IP Address to a New Terminal Server.....	63
Adding/Deleting Manual Terminal Servers	64
Logging in to the Terminal Server	64
Using WebManager to Connect to the Terminal Server	65
Logging into the Terminal Server	65
Configuration Files	66
Creating a New Terminal Server Configuration in DeviceManager ...	66
Opening an Existing Configuration File	66
Importing an Existing Configuration File	66
Managing the Terminal Server.....	66

Chapter 6 Network Settings	67
Introduction	67
IP Settings	67
IPv4 Settings	67
Overview	67
Field Descriptions	67
IPv6 Settings	69
Overview	69
Field Descriptions	69
Adding/Editing a Custom IPv6 Address	70
Advanced	71
Overview	71
Field Descriptions	71
Advanced	73
Host Table	73
Overview	73
Functionality	73
Field Descriptions	74
Adding/Editing a Host	74
IP Filtering	74
Overview	74
Functionality	75
Field Descriptions	75
Route List	75
Overview	75
Functionality	75
Field Descriptions	76
Adding/Editing Routes	77
DNS/WINS	78
Overview	78
Functionality	78
Field Descriptions	78
Editing/Adding DNS/WINS Servers	79
RIP	80
Overview	80
Functionality	80
Field Descriptions	81
Dynamic DNS	82
Overview	82
Functionality	82

Field Descriptions.....	82
Account Settings	83
Cipher Suite Field Descriptions.....	84
Adding/Editing a Cipher Suite	85
Validation Criteria Field Descriptions	86
IPv6 Tunnels	87
Overview	87
Field Descriptions.....	87
Adding/Editing an IPv6 Tunnel.....	88
Chapter 7 Configuring Users	89
Introduction	89
User Settings	90
Overview.....	90
Functionality	90
Adding/Editing Users	91
General Tab.....	91
Overview	91
Functionality	91
Field Descriptions.....	91
Services Tab	93
Overview	93
Functionality	93
Field Descriptions.....	93
Advanced Tab	95
Overview	95
Field Descriptions.....	95
Sessions Tab	97
Overview	97
Functionality	97
Field Descriptions.....	97
Serial Port Access Tab.....	99
Overview	99
Field Descriptions.....	99
Chapter 8 Configuring Serial Ports	100
Introduction	100
Serial Ports	100

Overview.....	100
Functionality	100
Editing a Serial Port	101
Copying a Serial Port	102
Resetting a Serial Port	103
Serial Port Profiles.....	103
Common Tabs.....	103
Overview	103
Hardware Tab Field Descriptions.....	104
Email Alert Tab Field Descriptions	106
Packet Forwarding Tab Field Descriptions	107
SSL/TLS Settings Tab Field Descriptions	110
Cipher Suite Field Descriptions.....	111
Adding/Editing a Cipher Suite	112
Validation Criteria Field Descriptions	113
Console Management Profile	114
Overview	114
Functionality	114
General Tab Field Descriptions.....	115
Advanced Tab Field Descriptions	116
COMredirect Profile.....	119
Overview	119
Functionality	119
General Tab Field Descriptions.....	119
Adding/Editing Additional COMredirect Hosts.....	121
Adding/Editing a Multihost Entry	122
.....	123
Advanced Tab Field Descriptions	123
TCP Sockets Profile	126
Overview	126
Functionality	126
General Tab Field Descriptions.....	126
Adding/Editing Additional Hosts	128
Adding/Editing a Multihost Entry	129
Advanced Tab Field Descriptions	130
UDP Sockets Profile	132
Overview	132
Functionality	132
General Tab Field Descriptions.....	135
Advanced Tab Field Descriptions	136
Terminal Profile	137
Overview	137
Functionality	137

General Tab Field Descriptions.....	137
Advanced Tab Field Descriptions	139
User Service Settings.....	142
Login Settings	142
Telnet Settings	142
Rlogin Settings	143
SSH Settings.....	144
SLIP Settings	146
PPP Settings.....	147
Printer Profile.....	153
Overview	153
General Tab Field Descriptions.....	153
Advanced Tab Field Descriptions	153
Serial Tunneling Profile	155
Overview	155
Functionality	155
General Tab Field Descriptions.....	156
Advanced Tab Field Descriptions	157
Virtual Modem Profile.....	158
Overview	158
Functionality	158
General Tab Field Descriptions.....	159
Advanced Tab Field Descriptions	160
Phone Number to Host Mapping.....	162
VModem Phone Number Entry	162
Modbus Gateway Profile.....	164
Overview	164
Functionality	164
General Tab Field Descriptions.....	165
Advanced Field Descriptions.....	166
Modbus Slave IP Settings Field Descriptions	167
Adding/Editing Modbus Slave IP Settings.....	168
Modbus Slave Advanced Settings Field Descriptions.....	169
Remote Access (PPP) Profile	170
Overview	170
Functionality	170
General Tab Field Descriptions.....	171
Dynamic DNS Field Descriptions	172
.....	173
Authentication Tab Field Descriptions.....	173
Advanced Tab Field Descriptions	176
Remote Access (SLIP) Profile	180
Overview	180
General Tab Field Descriptions.....	180

Advanced Tab Field Descriptions	181
Port Buffering.....	183
Overview.....	183
Functionality	183
Local Port Buffering.....	183
Remote Port Buffers.....	184
Field Definitions.....	184
Advanced.....	186
Advanced Serial Settings Tab	186
Overview	186
Field Descriptions.....	186
Modems Tab.....	187
Overview	187
Functionality	187
Adding/Editing a Modem	188
COMredirect Baud Rate Tab.....	188
Overview	188
Functionality	188
Field Definitions.....	189
Chapter 9 Configuring Security	190
Introduction	190
Authentication	191
Authentication	191
Local	192
Overview	192
Field Descriptions.....	192
RADIUS.....	193
Overview	193
General Field Descriptions.....	193
Attributes Field Descriptions	195
Kerberos.....	196
Field Descriptions.....	196
LDAP/Microsoft Active Directory	197
Overview	197
Field Descriptions.....	197
TACACS+	199
Overview	199

Field Descriptions.....	199
SecurID	200
Overview	200
Field Descriptions.....	200
NIS.....	201
Field Descriptions.....	201
SSH.....	202
Overview.....	202
Functionality	202
Users Logging into the Terminal Server Using SSH	202
Users Passing Through the Terminal Server Using SSH (Dir/Sil) ...	203
Field Descriptions	204
SSL/TLS	205
Overview.....	205
Functionality	205
Field Descriptions	206
Cipher Suite Field Descriptions.....	207
Adding/Editing a Cipher	207
Validation Criteria Field Descriptions	209
VPN.....	210
Overview.....	210
Functionality	210
IKE Phase 1 Proposals	210
ESP Phase 2 Proposals.....	211
IPsec	211
Field Descriptions.....	211
Adding/Editing the IPsec Tunnel.....	211
Shared Secret Field Description	214
Remote Validation Criteria Field Descriptions.....	215
L2TP/IPsec	216
Field Descriptions.....	216
Exceptions	217
Field Descriptions.....	217
Adding/Editing a VPN Exception.....	218
Advanced	218
Field Description	218
HTTP Tunneling	219
Overview.....	219

Functionality	219
Adding/Editing the HTTP Tunnel	219
Field Descriptions.....	219
Configuring HTTP Tunnels	220
Field Descriptions.....	220
Configuring HTTP Tunnel Proxy	221
Field Descriptions.....	221
Configuring HTTP Tunnel Proxy Advanced.....	222
Field Descriptions.....	222
Configuring HTTP Tunnel Destination	222
Field Descriptions.....	223
Services	225
Overview.....	225
Functionality	225
Field Descriptions	225
Keys and Certificates	227
Chapter 10 Configuring the Option Card	229
Introduction	229
Option Card Settings	229
Overview.....	229
Functionality	229
Configuring a Secure Console Server Modem Card	229
Chapter 11 Configuring Clustering.....	230
Introduction	230
Clustering Slave List	230
Overview.....	230
Adding Clustering Slaves	231
Overview	231
Field Descriptions.....	231
Advanced Clustering Slave Options.....	232
Overview	232
Editing Clustering Slave Settings	232

Chapter 12 Configuring the System	234
Introduction	234
Alerts	234
Email Alerts	234
Overview	234
Functionality	234
Field Descriptions	235
Syslog	236
Overview	236
Field Descriptions	236
Management	238
SNMP	238
Overview	238
Field Descriptions	238
SNMP TRAPS	240
Time	241
Overview	241
Functionality	241
Network Time Tab Field Descriptions	242
Time Zone/Summer Time Tab Field Descriptions	243
Advanced	244
Overview	244
Login Tab Field Descriptions	244
Bootup Files Tab Field Descriptions	246
Message of the Day (MOTD) Tab Field Descriptions	246
TFTP Tab Field Descriptions	247
SFTP Tab Field Descriptions	248
Console Port Tab Field Descriptions	249
Chapter 13 System Administration	250
Introduction	250
Managing Configuration Files	250
Saving Configuration Files	250
Downloading Configuration Files	250
Downloading Configuration Files to Multiple Terminal Servers	251
Uploading Configuration Files	251
Specifying a Custom Factory Default Configuration	252

Resetting to the Original Factory Default Configuration	252
Downloading Terminal Server Firmware	253
Setting the Terminal Server's Date and Time.....	253
Rebooting the Terminal Server.....	253
Resetting Serial Port Statistics.....	253
Resetting the Terminal Server to Factory Defaults	254
Resetting the SecurID Node Secret.....	254
Language Support	254
Loading a Supplied Language	254
Translation Guidance.....	255
Software Upgrades and Language Files	255
Downloading Terminal Definitions	256
Creating Terminal Definition Files	256
Resetting Configuration Parameters	258
Lost Admin Password	258
Chapter 14 Applications	259
Introduction	259
Configuring Modbus.....	259
Overview.....	259
Configuring a Master Gateway.....	259
Configuring a Slave Gateway.....	259
Modbus Gateway Settings.....	260
Modbus Master Gateway	260
Modbus Slave Gateway	260
Modbus Serial Port Settings.....	261
Modbus Master Settings	261
Modbus Slave Settings	262
Configuring PPP Dial On Demand.....	263
Setting Up Printers	265
Remote Printing Using LPD.....	265

Remote Printing Using RCP	265
Remote Printing Using Host-Based Print Handling Software	265
Configuring a Virtual Private Network	266
Terminal Server-to-Host/Network	266
Network-to-Network	269
Host-to-Host.....	270
VPN Client-to-Network	272
Configuring HTTP Tunnels	273
Serial-to Serial	273
Serial-to Host	275
Host-to Host.....	277
Tunnel Relay	280
Appendix 15 SSL/TLS Ciphers	284
Valid SSL/TLS Ciphers	284
Appendix A RADIUS and TACACS+	286
Introduction	286
RADIUS	286
Supported RADIUS Parameters	286
Accounting Message.....	290
Mapped RADIUS Parameters to Terminal Server Parameters	291
BLACK BOX® RADIUS Dictionary Example	293
TACACS+	295
Accessing the Terminal Server Through a Serial Port Users	295
Accessing the Terminal Server Through a Serial Port - Example ...	297
Accessing the Terminal Server from the Network	298
Accessing the Terminal Server from the Network- Example	299
Appendix B Setting Jumpers	300
Introduction	300
Terminal Server 1-Port DB25 Male/Female	300
Terminal Server 1-Port RJ45	301

PoE Device Server 1-Port	301
Terminal Server 1-Port DB9	302
Modem Device Server 1-Port	302
2-Port Terminal Server	303
4-Port Desktop Secure Terminal Server	304
Appendix C Accessories	305
Introduction	305
Installing a BLACK BOX® PCI Card	305
Appendix D Pinouts and Cabling Diagrams	308
Serial Pinouts	308
DB25 Male	308
DB25 Female	309
RJ45	310
DB9 Male	311
Power Over Ethernet Pinouts	311
EIA-232 Cabling Diagrams	312
Terminal DB25 Connector	312
DB25 Male	312
DB25 Female	312
RJ45	313
DB9 Male	313
Modem DB25 Connector	314
DB25 Male	314
RJ45	314
DB9 Male	315
Appendix E Virtual Modem AT Commands	316
Virtual Modem Initialization Commands	316
Appendix F Utilities	318
Introduction	318
COMredirect	318

Decoder.....	319
Appendix G Troubleshooting.....	320
Introduction	320
Hardware Troubleshooting	320
Communication Issues.....	321
DeviceManager Problems	321
Host Problems.....	321
RADIUS Authentication Problems.....	322
Login Problems	322
Problems with Terminals	323
Unknown IP Address	323
DHCP/BOOTP Problems.....	324
Callback Problems	324
Language Problems.....	324
Modem Problems	324
PPP Problems	325
Printing Problems	325
Long Reboot Cycle	325
SSL/TLS	326
IPv6 Issues	326
Appendix H Data Logging	327
Introduction	327
COMredirect Profile	327
TCP Socket Profile.....	327

Appendix I Modbus Remapping.....	328
Configuring the Modbus UID Translation Feature	328
Appendix J Symmetric Key File.....	330
Symmetric Key File.....	330
Glossary	331

Preface

About This Book

This guide provides the information you need to:

- configure the Terminal Server. Terminal Server is being used throughout this guide as a generic term to describe all Terminal Server, Secure Device Server, Secure Terminal Server and Secure Console Server models.
- incorporate the Terminal Server into your production environment.

Intended Audience

This guide is for administrators who will be configuring the Terminal Server.

Some prerequisite knowledge is needed to understand the concepts and examples in this guide:

- If you are using an external authentication application(s), working knowledge of the authentication application(s).
- Knowledge of SFTP/TFTP, the transfer protocol the Terminal Server uses.

Documentation

The following documentation is included on the Terminal Server installation CD:



- *BLACK BOX® 1-Port Quick Start Guide*
- *BLACK BOX® 2-4-Port Desktop Quick Start Guide*
- *BLACK BOX® Rack Mount Quick Start Guide*
- *BLACK BOX® Terminal Server, Secure Console Server, Secure Device Server User Guide*
- *BLACK BOX® Terminal Server, Secure Console Server, Secure Device Server Command Line Reference Guide*
- *BLACK BOX® COMredirect Windows User Guide*
- *BLACK BOX® COMredirect Linux User Guide*
- *BLACK BOX® COMredirect Solaris User Guide*
- *BLACK BOX® COMredirect Unixware User Guide*
- *BLACK BOX® COMredirect SCO Openserver 5 User Guide*
- *BLACK BOX® COMredirect SCO Openserver 6 User Guide*
- *BLACK BOX® COMredirect HP-UX User Guide*
- Online Help in the DeviceManager (automatically installed with the DeviceManager application)

Typeface 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:

Typeface Example	Usage
At the C: prompt, type: <code>add host</code>	This typeface is used for code examples and system-generated output. It can represent a line you type in, or a piece of your code, or an example of output.
Set the value to TRUE .	The typeface used for TRUE is also used when referring to an actual value or identifier that you should use or that is used in a code example.
<code>subscribe project subject</code> <code>run yourcode.exec</code>	The italicized portion of these examples shows the typeface used for variables that are placeholders for values you specify. This is found in regular text and in code examples as shown. Instead of entering <i>project</i> , you enter your own value, such as <code>stock_trader</code> , and for yourcode , enter the name of your program.
File, Save	This typeface and comma indicates a path you should follow through the menus. In this example, you select Save from the File menu.
<i>BLACK BOX® User Guide</i>	This typeface indicates a book or document title.
See <i>About the Terminal Server</i> for more information.	This indicates a cross-reference to another chapter or section that you can click on to jump to that section.

Online Help

Online help is provided in the DeviceManager. You can click on the What's This button ( or ) and then click on a field to get field-level help. Or, you can press the **F1** key to get window-level help. You can also get the *User Guide* online by selecting **Help, Help Topics**.

1 Introduction

About the Terminal Server

The Terminal Server is an Ethernet communications/terminal server that allows serial devices to be connected directly to LANs. The Terminal Server 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.)
- PCs using terminal emulation or SLIP/PPP
- Modems for remote access and Internet access
- ISDN adapters for branch remote access and Internet access
- All types of serial printers

The performance and flexibility of the Terminal Server allows you to use a wide range of high speed devices in complex application environments. The Terminal Server products will work in any server environment running TCP/UDP/IP.

Terminal Server Models

The Terminal Server comes in several different models to meet your network needs:

- **Terminal Server**—Offered as a 1-port unit (DB25M, DB25F, RJ45, and DB9M interfaces available), this model provides basic Terminal Server functionality and supports software configurable serial interface protocols EIA-232/422/485.
- **Secure Device Server**—This model is available in both desktop and rack mount configurations. Both models support software configurable serial interface protocols EIA-232/422/485. The Secure Device Server model has the advanced secure feature set in addition to the general Terminal Server functionality.
- **Secure Terminal Server**—This model comes in one desktop model and several rack mount configurations. All models support EIA-232 only. The Secure Terminal Server model has the advanced secure feature set in addition to the general Terminal Server functionality.
- **Secure Console Server**—This model comes in several rack mount configurations. All models support EIA-232 only and have an internal PCI card interface. The Secure Console Server model has the advanced secure feature set in addition to the general Terminal functionality.

See [Hardware](#) for information about the hardware specifications for your Terminal Server model.

See [Software](#) for a list of the basic and advanced software features.

Terminal Server Features

The Terminal Server is a communications server used for making serial network connections. It attaches to your TCP/IP network and allows serial devices such as modems, terminals, or printers to access the LAN. It also allows LAN devices to access devices or equipment attached to Terminal Server serial ports.

This section highlights the hardware and software components you can expect to find in your Terminal Server model.

Hardware

Hardware Features		BLACK BOX® Models						
		Desktop				Rack Mount		
		Terminal Server	Secure Device Server 1	Secure Device Server 2/4	Secure Terminal Server 4	Secure Device Server	Secure Console Server	Secure Terminal Server
Serial Connectors	DB25F	•	•					
	DB25M	•	•					
	RJ45	•	•	•	•	•	•	•
	DB9M	•	•					
Serial Interface	EIA-232	•	•	•	•	•	•	•
	EIA-422	•	•	•		•		
	EIA-485	•	•	•		•		
Serial Power In Pin	DB25F	•	•					
	DB25M	•	•					
	RJ45	•	•	•	•			
Serial Connectors	DB25F	•	•					
	DB25M	•	•					
	RJ45	•	•	•	•	•	•	•
	DB9M	•	•					
Serial Interface	EIA-232	•	•	•	•	•	•	•
	EIA-422	•	•	•		•		
	EIA-485	•	•	•		•		

Hardware Features		BLACK BOX® Models						
		Desktop				Rack Mount		
		Terminal Server	Secure Device Server 1	Secure Device Server 2/4	Secure Terminal Server 4	Secure Device Server	Secure Console Server	Secure Terminal Server
Serial Power In Pin	DB25F	•	•					
	DB25M	•	•					
	RJ45	•	•	•	•			
Serial Power Out Pin	DB25F		•					
	DB25M		•					
	RJ45		•	•	•			
Auto Sensing Ethernet Interface	10/100	•	•	•	•			
	10/100/1000					•	•	•
PCI Interface							•	
Power Supply	Power over Ethernet		•	•				
	External AC	•	•	•	•			
	Internal AC					•	•	•
Dedicated Console Port						•	•	•

Software

This section describes the supported software features available.

Accessing the Terminal Server

All Terminal Server models can be accessed through any of the following methods:

- Easy Config Wizard, an easy configuration wizard that allows you to quickly setup the Terminal Server in a Windows® environment
- DeviceManager, a fully functional Windows 2000®/Windows Server 2003®/Windows Server 2003 R2®/Windows XP®/Windows Vista®/Windows Server 2008®/Windows Server 2008 R2®/Windows 7®/Windows 8®/Windows 8.1®/Windows Server 2012® and Windows Server 2012 R2® configuration/management tool
- WebManager, a web browser (HTTP/HTTPS) option for configuring/managing the Terminal Server
- Menu, a window-oriented menu interface for configuration and user access
- CLI, a Command Line Interface option for configuration/management and user access
- SNMP, allowing remote configuration via SNMP as well as statistics gathering
- DHCP/BOOTP, a method of automatically updating the Terminal Server

General Features

Basic software features are available on all Terminal Server 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 the BLACK BOX® COMredirect utility.
- DHCP/BOOTP for automated network-based setup.
- Dynamic statistics and line status information for fast problem diagnosis.
- Multisession support when accessing the Terminal Server from either the serial port or the network.
- Modbus master/slave/gateway support.
- Ability to disable services (for example, Telnet, COMredirect, Syslog, SNMP, Modbus, HTTP) for additional security.
- Logging via Syslog.
- Ability to enable ping responses.

Advanced Features

Advanced software features can be found on all models except the Terminal Server model.

- External authentication using any of the following systems:
 - RADIUS
 - Kerberos
 - TACACS+
 - NIS
 - SecurID
 - LDAP/Microsoft Active Directory
- Support for TCP/IP and UDP protocols.
- 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 cluster several Terminal Servers.
- Email alert notification.
- PPP authentication via PAP/CHAP/MSCHAP.
- SSH connections (supported ciphers are Blowfish, 3DES, AES, CAST128, and Arcfour).
- SSL/TLS connections.
- Logging via Syslog.
- RIP authentication (via password or MD5).
- NTP/SNTP (versions 1, 2, 3, and 4 are supported).

Security

The Terminal Server security features can include (depending on your 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 Terminal Server access to the Terminal Server.
- 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 Terminal Server.
- SSH client/server connections (SSH 1 and SSH 2).
- SSL/TLS client/server data encryption (TLSv1 and SSLv2).
- Ability to setup Virtual Private Networks.
- Access to fire walled/Nated devices via HTTP tunnels.

2 Hardware and Connectivity

Introduction

This chapter describes how to physically set up your Terminal Server unit. It includes an overview of the Terminal Server hardware components and how to power up the Terminal Server to make sure it works correctly.

Terminal Server Components

What's Included

The following components are included with your product:

- Terminal Server unit
- External power supply (1-, 2-, and 4-port models only)
- A CD-ROM containing documentation, firmware, configuration software, COMredirect, etc.
- Terminal Server models that have an RJ45 serial connector(s) come with an RJ45→DB9F adapter

Added components for rack mount models:

- 3' CAT5 RJ45 Administration cable
- Rack mounting kit

What You Need to Supply

Before you can begin, you need to have the following:

- A serial cable(s) to connect serial devices to your Terminal Server unit
- An Ethernet CAT5 10/100/1000BASE-T cable to connect the Terminal Server unit to the network

Power Supply Specifications

Desktop Models

If you are providing a power supply for a desktop Terminal Server model, your power supply must meet the following requirements:

- Output between 9-30V DC.
- DC barrel connector: The cable attached to the power supply should be about 20AWG, length 6 feet approx. The barrel dimensions of the cable-plug are OD=5.5, ID=2.1, and length= 9.5mm, with a straight barrel, and positive polarity on the inside and negative polarity on the outside.
- Power can also be provided by:
 - Serial Port 1, pin 1 on the Terminal Server/Secure Terminal Server 1 port models
 - Serial Port 2, pin 1 on the Secure Device Server 2 port model
 - Serial Port 4, pin 1 on the Secure Device Server 4 port model

Power Over Ethernet (PoE) Models

The 1-port/4-port Secure Device Server models can be powered by PoE.

Note: If you are using the Power over Ethernet feature in conjunction with the serial power pinout, the power output is always 5 volts on the serial port, regardless of how the jumpers are set.

The Terminal Server SDS P model is considered a Powered Device (PD) and can accept power from an IEEE 802.3AF compliant Power Source Equipment (PSE) device. The Terminal Server PoE can receive up to 13W of power using one of the following methods to connect to a PSE:

- Using the two unused twisted pair wires (10/100Mb only).
- Using the two data pairs or "phantom power" method (100Mb).

Rack Mount Models

AC Power Requirements

AC power rack mount units come with standard power cords, specific to your country, that should be used to power the Terminal Server unit.

Getting to Know Your Terminal Server

This section describes the hardware components found on your Terminal Server unit.

Overview

All Terminal Servers have the same basic hardware components to allow you to connect to serial devices, connect to the network, monitor LAN and serial activity, and manage the unit. Below is a list of these components:

- **Serial Port(s)**—Connector(s) that will be used to connect to a serial device.
- **Activity**—This LED flashes to indicate LAN activity.
- **Link10/100**—This LED indicates the Ethernet connection speed for desktop models:
 - **Green**—10 Mbits
 - **Yellow**—100 Mbits
 - **Off**—no LAN connection
- **Link10/100/1000**—This LED indicates the Ethernet connection speed for rack mount models:
 - **Green**—10/100 Mbits
 - **Yellow**—1000 Mbits
 - **Off**—no LAN connection
- **Power/Ready**—This LED can cycle through several colors (yellow, green, red) during a boot process, but should complete with a green light. When the Terminal Server has completed the power up cycle, the LED will be steady green on rack mount modes. On desktop models, if the LED is green after power up but continues to cycle on and off (flashes green), this indicates that the console switch is in the **on** position. You can learn more about the Power/Ready LED in [Hardware Troubleshooting](#).

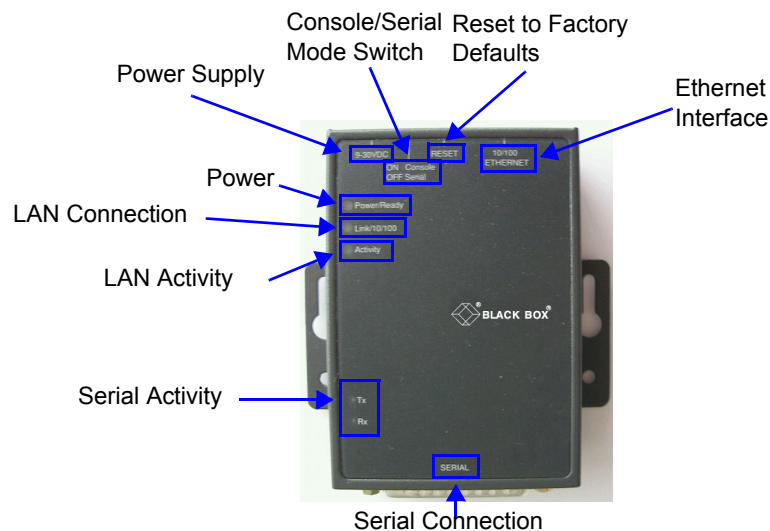
BLACK BOX®

Model	LED Label	Green light	Red light
Desktop	Power/Ready	<p>Solid — Indicates the Terminal Server has completed the power up cycle.</p> <p>Blinks — After power up, a blinking green light indicates that the console switch is in the on position.</p>	<p>Solid — Indicates the Terminal Server has a fatal error.</p> <p>Blinks — After power up, a blinking red means the Terminal Server has a critical error.</p> <p>See Hardware Troubleshooting for possible causes.</p>
Rack mount	System Ready	<p>Solid — Indicates the Terminal Server has completed the power up cycle.</p>	<p>Solid — Indicates the Terminal Server has a fatal error.</p> <p>Blinks — After power up, a blinking red means the Terminal Server has encountered a critical error.</p> <p>See Hardware Troubleshooting for possible causes.</p>

- **External Power Supply**—This can be an external AC/DC adaptor or AC power cord, depending on your Terminal Server model.
- **Console/Serial Switch**—Found on desktop models only (rack mount models have a dedicated console port), this switch determines whether port 1 functions as a serial port or a console port.
- **Reset**—The inset RESET button will reboot the Terminal Server if pushed in and released quickly. It will reset the Terminal Server to factory defaults if pushed in and held for more than three seconds. See [Resetting to the Original Factory Default Configuration](#) for more information.
- **Serial Activity**—
 - **Tx**—Flashes with transmit serial activity. There is a Tx LED for each serial port.
 - **Rx**—Flashes with receive serial activity. There is an Rx LED for each serial port.
- **Ethernet**—The Ethernet connector. Secure Console Server models have dual Ethernet.

1-Port

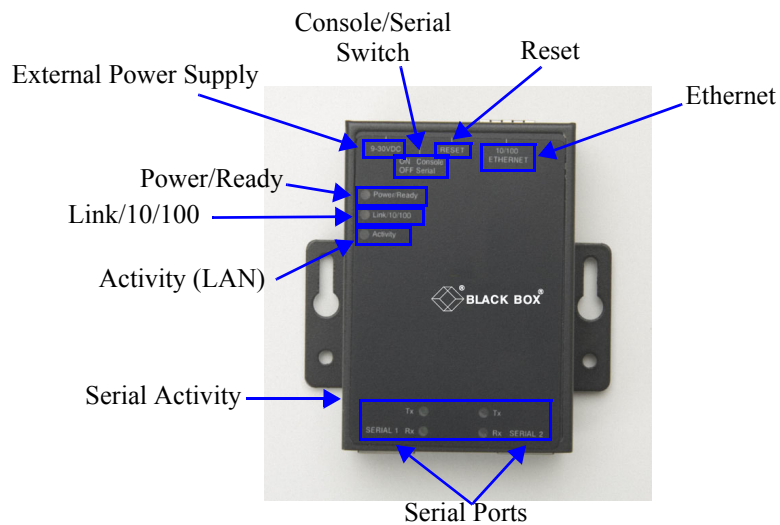
This section describes the components found on the Terminal Server 1-port models.



The 1-port Terminal Server has one serial connection that is one of the following connectors: DB25 male, DB25 female, RJ45, or DB9 male.

2-Port

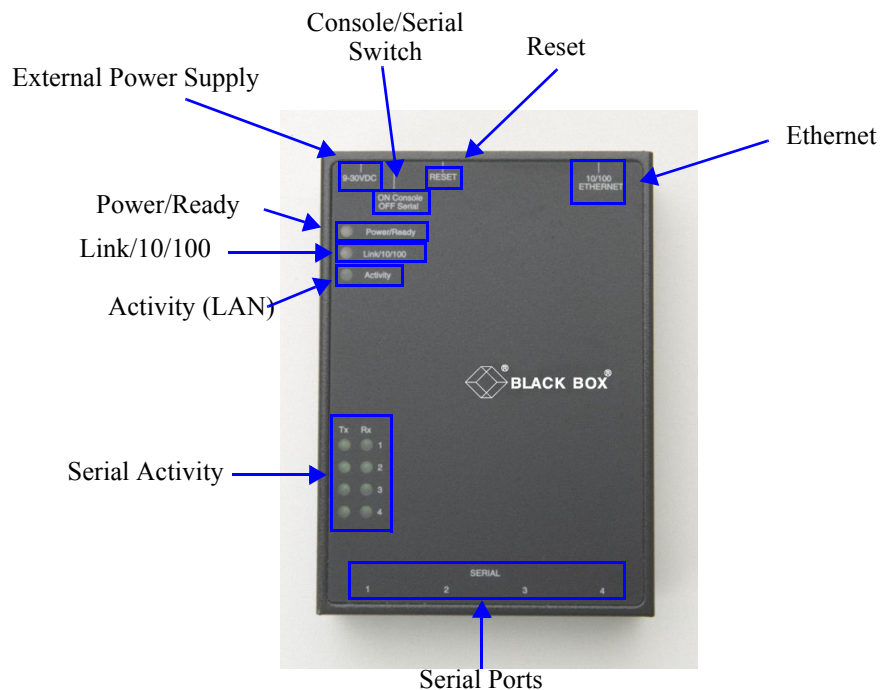
This section describes the components found on the Secure Device Server 2-port models.



The 2-port Secure Device Server has two RJ45 serial connections. The 2-port Terminal Server can support an 8-pin connector if there is no requirement for power in (pin 1) or power out (pin 10) pins.

4-Port

This section describes the components found on the Secure Device Server 4-port desktop models.

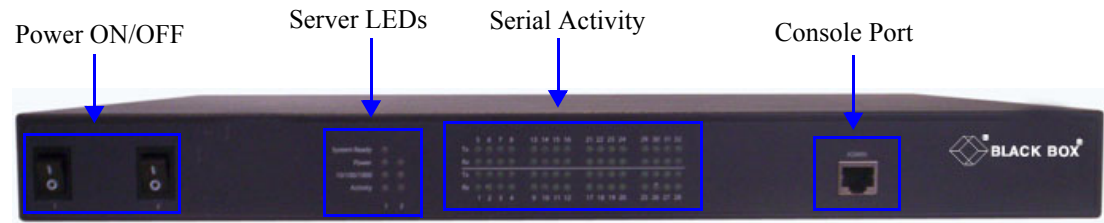


The 4-port Terminal Server model has four RJ45 serial connections.

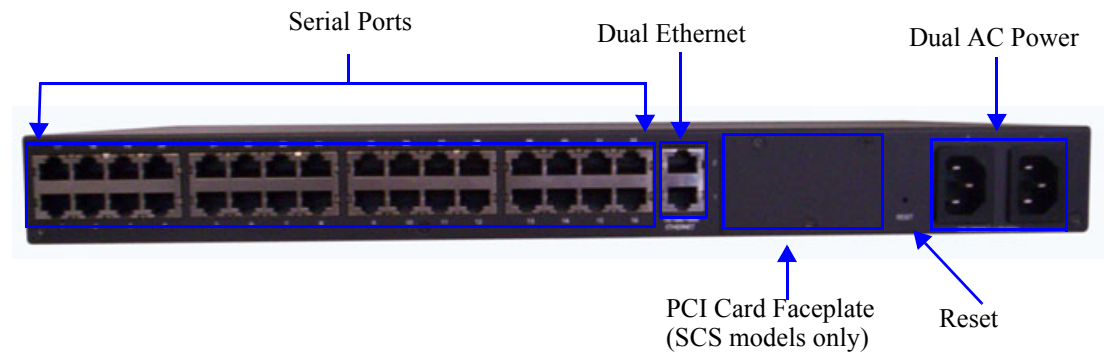
Rack Mount

This section describes the basic components of all rack mount Terminal Server models. This example uses a Secure Console Server with dual Ethernet and dual AC power.

Console Port/LED View

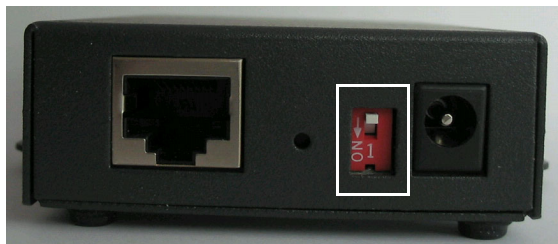


Serial/Ethernet View



Console/Serial Switch

Located at the back of the desktop models is a switch that controls whether serial port 1 is in Console or Serial mode.



Look at your model to verify the direction of the ON switch position. ON indicates that serial port 1 is in Console mode; otherwise serial port 1 is in Serial mode.

Console Mode

Console mode is used when you have a direct connection between a serial device (like a terminal or a PC) and the Terminal Server, accessed by the Admin user to configure/manage the Terminal Server. Console mode automatically sets serial port settings as:

- **Serial Interface** to **EIA-232**
- **Speed** to **9600**
- **Flow Control** to **No**
- **Bits** to **8**

- **Stop Bits** to 1
- **Parity** to None

Console mode also displays extra system messages.

Serial port 1 will ignore any **Serial Port** settings when in Console mode, so you need to turn Console mode off to use serial port 1 in your network.

Note: When the console switch is in the **on** position, the System/Ready LED will cycle on and off (flashes green).

Serial Mode

Serial mode is used when the Terminal Server acts as a communications server, or anytime you are not connecting directly to the Terminal Server to configure it. You can connect directly to the Terminal Server in Serial mode, but the Terminal Server will not display all the messages/information you will get in Console mode.

Dedicated Console Port: Rack Mount Models

The rack mount Terminal Server models have a dedicated Console port, located on the LED side of the Terminal Server. You can use the supplied Administration cable (with the supplied RJ45→DB9F adapter if needed) to connect a terminal to the Console/Admin port to view diagnostic information and/or configure the Terminal Server using the Menu or Command Line Interface (CLI). You can configure the baud rate and flow control of the dedicated Console port.

Powering Up the Terminal Server

Desktop/Rack Mount Models

To power up the Terminal Server, perform the following steps:

1. Rack Mount Models only: Using the rack mount brackets included with your Terminal Server, you can rack mount the Terminal Server from the front or the back of the chassis, depending on your environment. Make sure you don't block the Terminal Server's side air vents. Each Terminal Server is 1U in height, and does not require any extra space between units; therefore, you can rack mount up to five Terminal Servers in a 5U rack.
2. Plug the external power supply into the Terminal Server and then into the electrical outlet. Connect it to the PSE if you have a P series (Power over Ethernet) model.
3. Rack mount models only: Power on the Terminal Server unit using the Power ON/OFF switch.
4. You will see the LEDs cycle for several seconds and then remain a solid green, indicating that it is ready to configure/use.

Before you start to configure the Terminal Server, you should set the desktop Terminal Server jumpers if you want to terminate the line or use the power in pin feature (instead of an external power supply, if your desktop Terminal Server model supports it).

In some circumstances, the setting of jumpers may be required:

- Desktop models where EIA-422/485 line termination is required.

See *Appendix B, Setting Jumpers* to see how to set the jumpers for your Terminal Server desktop model.

3 Configuration Methods

Introduction

This chapter provides information about the different methods you can use to configure the Terminal Server. Before you can configure the Terminal Server, you must assign an IP address to the Terminal Server. See the [Chapter 4, Getting Started](#) to find out how to assign an IP address to the Terminal Server.

Once an IP address is assigned to the Terminal Server, you can use any of the configuration methods to:

- Configure users.
- Configure Terminal Server server parameters.
- Configure serial port parameters.
- Configure network parameters.
- Configure time parameters.
- Reboot the Terminal Server.
- View statistics while connected to the Terminal Server.

Configuration Methods Overview

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

Configures an IP Address

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

- **Easy Config Wizard**—The Easy Config Wizard is available from the CD ROM included with your Terminal Server. You can use the Easy Config Wizard to set the Terminal Servers IP address and configure serial ports. This configuration method would typically be used when:
 - All ports are to have the same configuration.
 - Only the most commonly used profiles are required.
 - Straightforward application with no advanced functionality required. Easy Config is installed on a Windows®-based PC with local network access to the Terminal Server.
- **DeviceManager**—Use this method when you can connect the Terminal Server to the network and access the Terminal Server from a Windows® PC. The DeviceManager is a Windows®-based application that can be used for Terminal Server configuration and management. The DeviceManager can be used to assign an IP address and perform the complete configuration and management of the Terminal Server.
- **Direct Connection**—Use this method when you can connect to the Terminal Server 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 Terminal Server using either the Menu or CLI.
- **DHCP/BOOTP**—Use this method when you have a BOOTP or DHCP server running and you can connect the Terminal Server to your network. The Terminal Server 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 Terminal Server parameters that will be passed from the DHCP/BOOTP server to the Terminal Server when it boots up. Other configurators such as DeviceManager, CLI, or Menu can be used to set this option, and obtain the initial IP address.
- **ARP-Ping**—Use this method when you can connect the Terminal Server to the network and want to assign a temporary IP address to the Terminal Server by specifying an ARP entry from your PC and then pinging it.
- **IPv6 Network**—When the Terminal Server is connected to an IPv6 network, its local link address is determined using stateless auto configuration.

Once an IP address has been assigned to the Terminal Server, in most cases, you can continue to use the same method if it is a configurator or you can switch to any other configuration method.

Requires a Configured IP Address

The following configuration methods require that an IP address already be assigned to the Terminal Server.

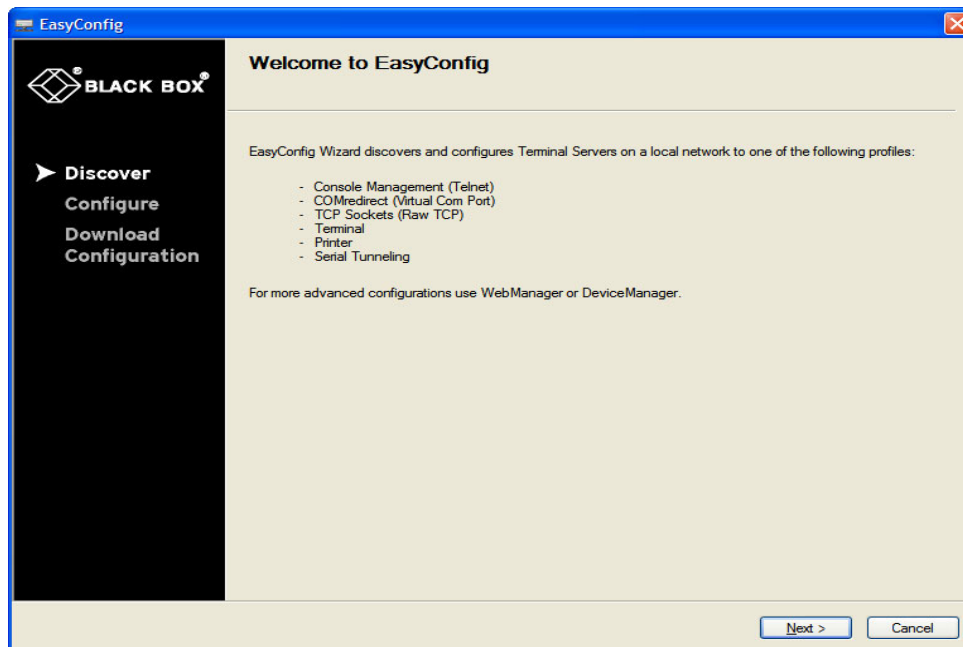
- **WebManager**—WebManager is a fully functional, browser-based configuration method.

Easy Config Wizard

The Easy Config Wizard is a configuration wizard that will configure all the serial ports on your Terminal Server to one of the following:

- Console Management
- COMredirect (Virtual COM Port)
- TCP Sockets (Raw TCP)
- Terminal
- Printer (not supported on Terminal Server 1 Port model)
- Serial Tunneling

You can launch the Easy Config Wizard from the installation CD-ROM.



The Easy Config Wizard has been designed to walk you through the configuration process for any of the available configuration options shown on the Welcome window.

DeviceManager

Overview

The DeviceManager is a Windows® -based application that can be used to connect to the Terminal Server to actively manage and configure it, or can create new Terminal Server configurations offline. See [Chapter 5, Using DeviceManager and WebManager](#) for information on configuring/managing the Terminal Server with DeviceManager.

Access Platforms

The DeviceManager can be run from Windows 2000®/Windows Server 2003®/Windows Server 2003 R2®/Windows XP®/Windows Vista®/Windows Server 2008®/Windows Server 2008 R2®/Windows 7®/Windows 8®/Windows 8.1®/Windows Server 2012®/Windows Server 2012 R2®.

DeviceManager can be installed from the product CD-ROM. Unless the Terminal Server has already been configured with a Gateway, DeviceManager can only access Terminal Servers in the local subnet. Only the admin user can manage or configure the Terminal Server via the DeviceManager.

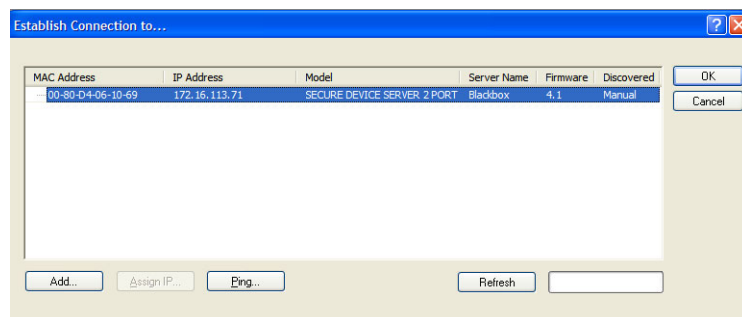
Unique Features

DeviceManager supports the following unique features:

- The ability to download the same configuration file to several Terminal Servers 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 Terminal Server.
- The ability to open a session to the Terminal Server and download a (saved) configuration file to it.
- The ability to download/upload keys/certificates to/from the Terminal Server.
- The ability to download custom files, such as new terminal definitions and a custom language files to the Terminal Server.

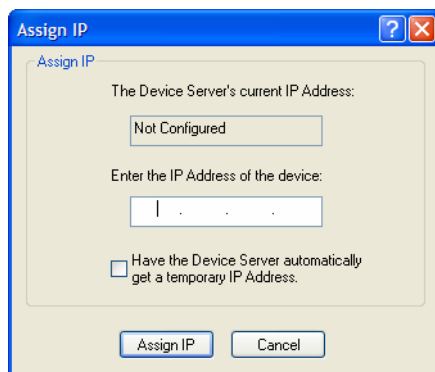
Connecting to the Terminal Server Using DeviceManager

Before you can use DeviceManager, you need to install it on your Windows® operating system from the Terminal Server CD-ROM. After the DeviceManager application is installed, click **Start, All Programs, Black Box, DeviceManager, DeviceManager** to start the application. When you launch the DeviceManager, it will scan the network for Terminal Servers or optionally can manually add your server's IP address:



All discovered Terminal Servers will be displayed on the list along with their name and IP address. When a new Terminal Server 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**. To configure the IP address, click on the Terminal Server and then click the **Assign IP** button. To Add, Edit or Delete manually configured servers, click on the **Add** button.

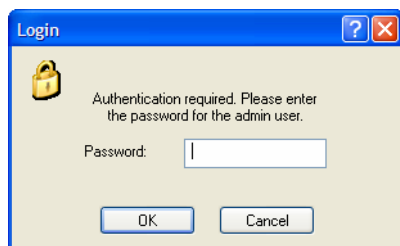


Choose the method you want to use to assign an IP address to the Terminal Server:

- Type in the IP address that you want to assign to this Terminal Server
- Enable the **Have the Terminal Server automatically get a temporary IP Address** option. This will turn on DHCP/BOOTP, so the Terminal Server will attempt to get its IP address from your DHCP/BOOTP server. If you do not have a DHCP/BOOTP server, DeviceManager will temporarily assign an IP address in the range of **169.254.0.1 - 169.254.255.255** that will be used only for the duration of the DeviceManager/Terminal Server communication.

After you configure the IP address, click the **Assign IP** button.

The refreshed list will now display the assigned IP address for the new Terminal Server. To connect to the Terminal Server, click the Terminal Server entry and click **OK**. You will be asked to supply the Admin password (the factory default password is **superuser**).

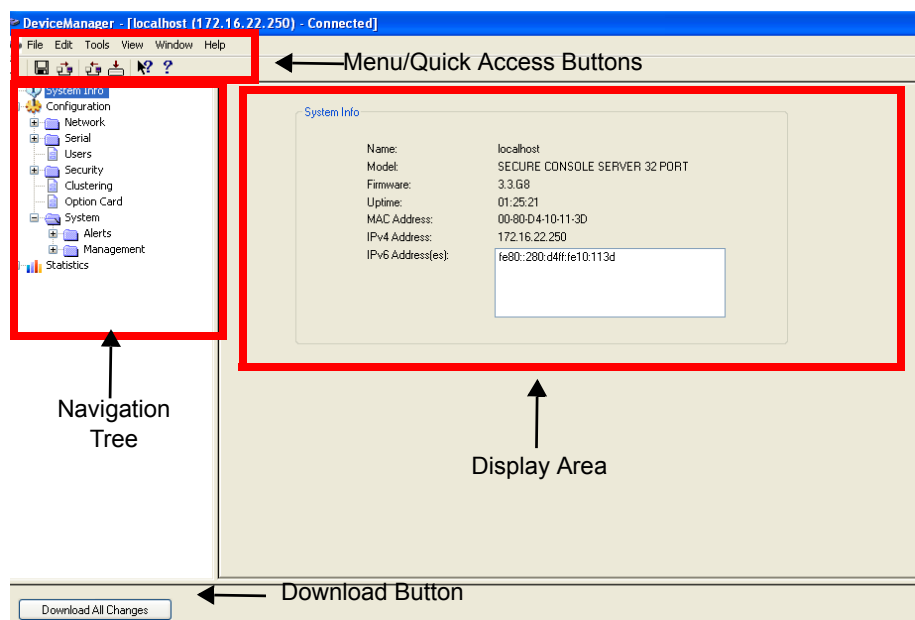


If you have a successful connection, the DeviceManager will retrieve the configuration and then display the Terminal Server's System Information and you can begin configuring the Terminal Server.

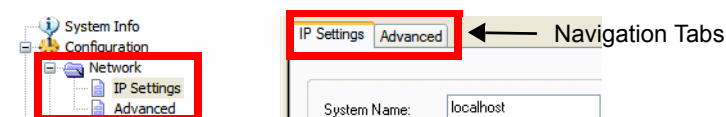
Note: The DeviceManager does not automatically update the Terminal Server's configuration. You must download the configuration changes to the Terminal Server and then reboot the Terminal Server to make the configuration changes take effect.

Using DeviceManager

After you have successfully connected to the Terminal Server, you will see the following window:



You navigate through the different configuration windows by selecting an option in the left-hand navigation tree. If you double-click on an option that is next to a folder, more navigation options are displayed:



The **Network** folder contains two configuration options, **IP Address** and **Advanced**. Notice that when the **IP Address** option is selected, there are more navigation options in the form of the tabs, **IP Settings** and **Advanced**.

Downloading Configuration

When you have completed all your configuration changes, click the **Download Changes** button to download the configuration to the Terminal Server. You must reboot the Terminal Server to make those configuration changes take effect.

WebManager

Overview

The WebManager is a web-browser based method of configuring/managing the Terminal Server. It follows the same design as the DeviceManager, so it is easy to switch between the WebManager and DeviceManager when configuring your Terminal Server. See [Chapter 5, Using DeviceManager and WebManager](#) for information on configuring/managing the Terminal Server with DeviceManager.

Access Platforms

You can access the Terminal Server through WebManager from any system that can run a web browser. WebManager can be accessed by the admin user or any user who has Admin Level privileges.

Features

WebManager supports the following unique features:

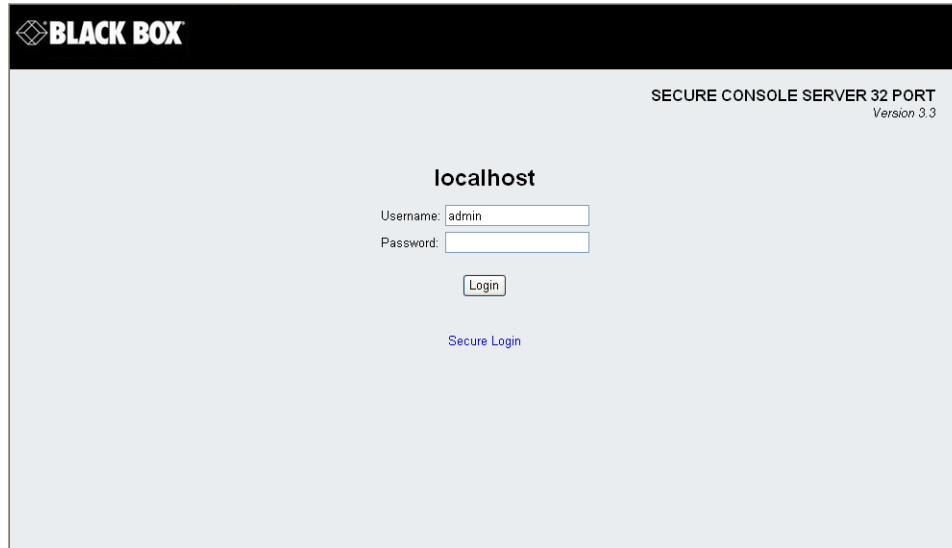
- The ability to open a session to the Terminal Server and download a (saved) configuration file to it.
- The ability to save a configuration file locally in text format, in addition to the binary format.
- The ability to download/upload keys/certificates to/from the Terminal Server.
- The ability to download custom files, such as new terminal definitions and a custom language files to the Terminal Server.
- From WebManager, you can launch EasyPort Web, which can be used to:
 - access clustered Terminal Servers
 - access ports configured with the Console Server profile and launch an SSH or Telnet session to those console ports

Connecting to the Terminal Server Using WebManager

Before you can connect to the Terminal Server using WebManager, the Terminal Server must already be configured with a known IP address; see [Setting Up the Network](#) to configure an IP address on your Terminal Server.

To connect to the Terminal Server through the WebManager:

1. Open your web browser and type in the IP address of the Terminal Server that you want to manage/configure and press **Enter**; for example: `http://123.123.123.123`.
2. If you successfully connect to the Terminal Server, a login screen will appear.



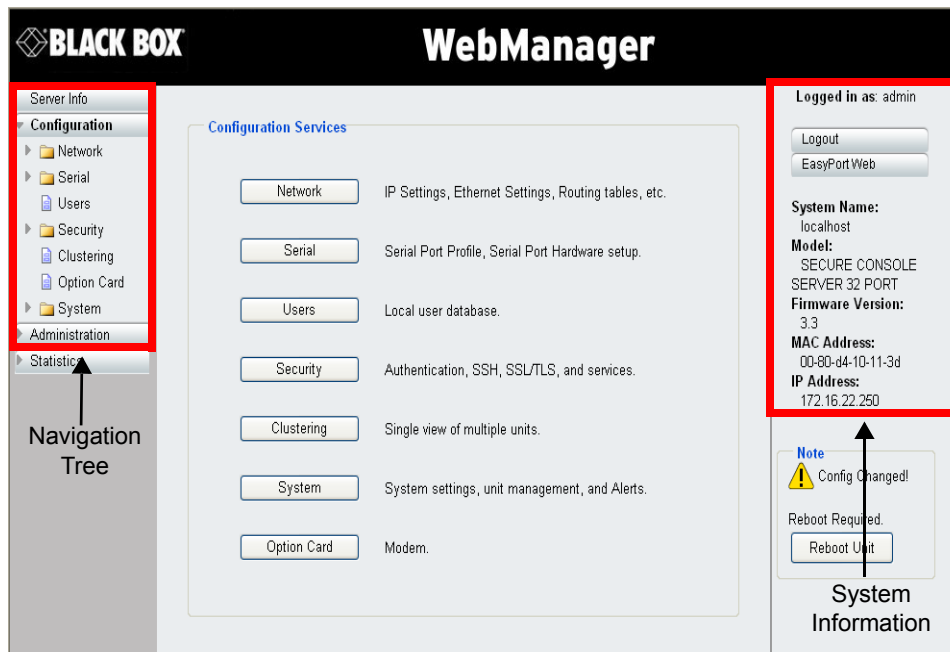
The screenshot shows a web browser window displaying the Black Box Secure Console Server login interface. At the top, there is a black header with the 'BLACK BOX' logo on the left and 'SECURE CONSOLE SERVER 32 PORT Version 3.3' on the right. The main content area has a light gray background. In the center, the word 'localhost' is displayed. Below it, there is a login form with two input fields: 'Username:' containing the text 'admin' and 'Password:'. Below these fields is a 'Login' button. At the bottom of the form area, there is a link labeled 'Secure Login'.

3. If you are accessing the Terminal Server in non-secure HTTP, just type in the Admin password (the factory default password is **superuser**). If the Terminal Server has already been configured for secure access mode (HTTPS), select the **For a Secure Login** link and then type in the username "admin" and the associated password.

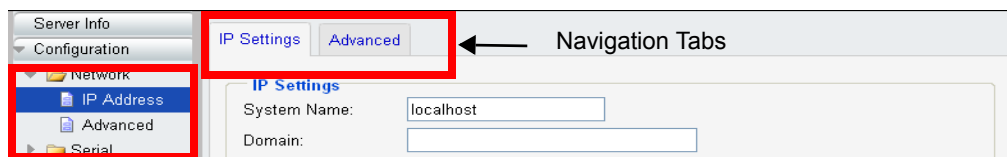
Note: The secure HTTP (HTTPS) mode requires that the **SSL Passphrase** is already defined in the Terminal Server configuration and the SSL/TLS certificate/private key and CA list must have already been downloaded to the Terminal Server; see [Keys and Certificates](#) for more information.

Using WebManager

After you have successfully logged into WebManager, you will see the following:



You navigate through the different configuration windows by selecting an option in the left-hand navigation tree. When you click on an option that is under a folder, more navigation options are displayed:



The **Network** folder contains two configuration options, **IP Address** and **Advanced**. Notice that when the **IP Address** option is selected, there are more navigation options in the form of the tabs, **IP Settings** and **Advanced**.

Remember that in the WebManager, it is necessary to press the **Apply** button to save your changes.

Command Line Interface

Overview

The Command Line Interface (CLI) is a command line option for Terminal Server configuration/management. See the *Command Line Interface Reference Guide* for a full breakdown of all the CLI commands and their functionality.

Access Platforms

The CLI is accessed by any application that supports a Telnet or SSH session to the Terminal Server's IP address, such as Putty, SecureCRT, or from a command prompt. You can also access the CLI from a dumb terminal or PC connected to a serial port.

Features

The CLI supports the following unique features:

- You can access the Terminal Server from any application that supports Telnet or SSH.
- Ability to clear the ARP table (cache).
- The ability to save a configuration file locally in text format, in addition to binary.

Connecting to the Terminal Server Using the CLI

There are two ways you can access the Terminal Server, through the network (Ethernet connection) or through the serial connection. If you are accessing the Terminal Server through the network, the Terminal Server must already have a known IP address configured; see [Using a Direct Serial Connection to Specify an IP Address](#) getting started for information on configuring an IP address.

Through the Network

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

1. Start a Telnet or SSH session to the Terminal Server's IP address; for example:

```
telnet 10.10.201.100
```

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 Terminal Server model and number of ports:

```
Login: admin
Password:
```

```
Secure Device Server 2 Port#
```

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

Through the Serial Port

To connect to the Terminal Server through the serial port to configure/manage it using the CLI (or Menu), see [Using a Direct Serial Connection to Specify an IP Address](#) .

After you have established a connection to the Terminal Server, 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 Terminal Server model and number of ports:

```
Login: admin
```

```
Password:
```

```
Secure Device Server 2 Port#
```

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

Using the CLI

After you have successfully logged in, you can start configuring/managing the Terminal Server 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.

See the *Command Line Interface Reference Guide* for more information about the CLI.

Menu

Overview

The Menu is a graphical representation of the CLI. You can look up Menu parameter explanations in the *Command Line Interface Reference Guide*. The only operations that the Menu does not support are the downloading and uploading of files to/from the Terminal Server.

Access Platforms

The Menu is accessed by any application that supports a Telnet or SSH session to the Terminal Server's IP address, such as Putty, SecureCRT, or from a command prompt. You can also access the Menu from a dumb terminal or PC connected to a serial port.

Features

The Menu supports the following unique features:

- You can access the Terminal Server from any application that supports Telnet or SSH.

Connecting to the Terminal Server Using the Menu

To connect the Terminal Server using the Menu, follow the directions for [Connecting to the Terminal Server Using the CLI](#) .

Using the Menu

After you have successfully logged in, type **screen** at the prompt and press **Enter**. You will be asked to enter a terminal type, and then you will see the following Menu:



To navigate through the Menu options, do the following:

1. Highlight a Menu option by using the keyboard up and down arrows to navigate the list.
2. When the Menu item you want to access is highlighted, press the **Enter** key to either get to the next list of options or to get the configuration screen, depending on what you select.
3. When you are done configuring parameters in a screen, press the **Enter** key and then the **Enter** key again to **Accept and exit the form**.
4. If you want to discard your changes, press the **Esc** key to exit a screen, at which point you will be prompted with **Changes will be lost, proceed? (y/n)**, type **y** to discard your changes or **n** to return to the screen so you can press **Enter** to submit your changes.
5. If there are a number of predefined options available for a field, you can scroll through those items by pressing the **Space Bar** or you can type **1** (lowercase L) to get a list of options, use the up/down arrows to highlight the option you want, and then press **Enter** to select it.

DHCP/BOOTP

Overview

Several Terminal Server parameters can be configured through a DHCP/BOOTP server during an Terminal Server bootup. This is particularly useful for configuring multiple Terminal Servers.

Not all configuration parameters are supported in the DHCP/BOOTP configuration (see [DHCP/BOOTP Parameters](#) for supported configuration parameters), so you will need to use another configuration method, such as DeviceManager, WebManager or CLI, to complete the configuration.

Features

DHCP/BOOTP supports the following unique features:

- DHCP/BOOTP can supply the Terminal Server's IP address.
- The DHCP/BOOTP server can configure certain server and user configuration parameters when the Terminal Server is booted.
- The DHCP/BOOTP server can auto-configure the Terminal Server with basic setup information (IP address, subnet/prefix bits, etc.)
- The DHCP/BOOTP server can download a new version of firmware when the Terminal Server is rebooted.
- The DHCP/BOOTP server can download a full configuration file when the Terminal Server is rebooted.

Connecting to the Terminal Server Using DHCP/BOOTP

The Terminal Server will automatically request an IP address from the DHCP/BOOTP server when the **Obtain IP address automatically using DHCP/BOOTP** parameter is enabled. To enable the **Obtain IP address automatically using DHCP/BOOTP** parameter, follow the directions in [Using a Direct Serial Connection to Enable BOOTP/DHCP](#).

Using DHCP/BOOTP

To use DHCP/BOOTP, edit the bootp file with Terminal Server configuration parameters. You can use DHCP/BOOTP to perform the following actions on a single or multiple Terminal Servers on bootup:

- 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 Terminal Servers' configuration in one DHCP/BOOTP file, rather than configure each Terminal Server manually. Another advantage of DHCP/BOOTP is that you can connect the Terminal Server 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/BOOTP 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 Terminal Server from the HTTP or HTTPS WebManager. Values are **on** or **off**.
- **AUTH_TYPE**—The authentication method(s) employed by the Terminal Server 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 Terminal Server access to devices listed in the Terminal Server's 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/bb_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.

SNMP

Overview

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

Before you can configure/manage the Terminal Server using SNMP, you need to set the Terminal Server IP address and configure a read-write user for SNMP version 3 or a community for SNMP version 1 or 2. You can use DeviceManager, CLI, or the Menu to set the IP address and user/community (don't forget to reboot the Terminal Server before connecting with the SNMP manager to make your changes take effect).

Access Platforms

You can access the Terminal Server SNMP MIB from any system that runs your SNMP client/MIB browser software.

Features

SNMP supports the following features:

- You can configure SNMP traps.
- Since not all versions of SNMP support secure communication, password parameters must be set using another configuration method.

Connecting to the Terminal Server Using SNMP

Before you can connect to the Terminal Server 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 Terminal Server.
2. Configure a read-write user for SNMP version 3 or a community for SNMP version 1 or 2 on the Terminal Server.
3. Reboot the Terminal Server to make sure the changes take effect.

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

1. Load the **blackbox-sds.MIB** file from the Terminal Server CD-ROM into your SNMP manager (this MIB works for all Secure Terminal Server, Secure Console Server, and Secure Device Server models).

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 Terminal Server.
3. Type in the Terminal Server's IP address and connect to the Terminal Server.

You are now ready to start configuring the Terminal Server using SNMP.

Using the SNMP MIB

After you have successfully connected to the Terminal Server through your SNMP Management tool or MIB browser, expand the **BLACKBOX-SECURE-DEVICE-SERVER-MIB** folder to see the Terminal Server's parameter folders. 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 Terminal Server. 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 Terminal Server.
- **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 Terminal Server, 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 Terminal Server.

4

Getting Started

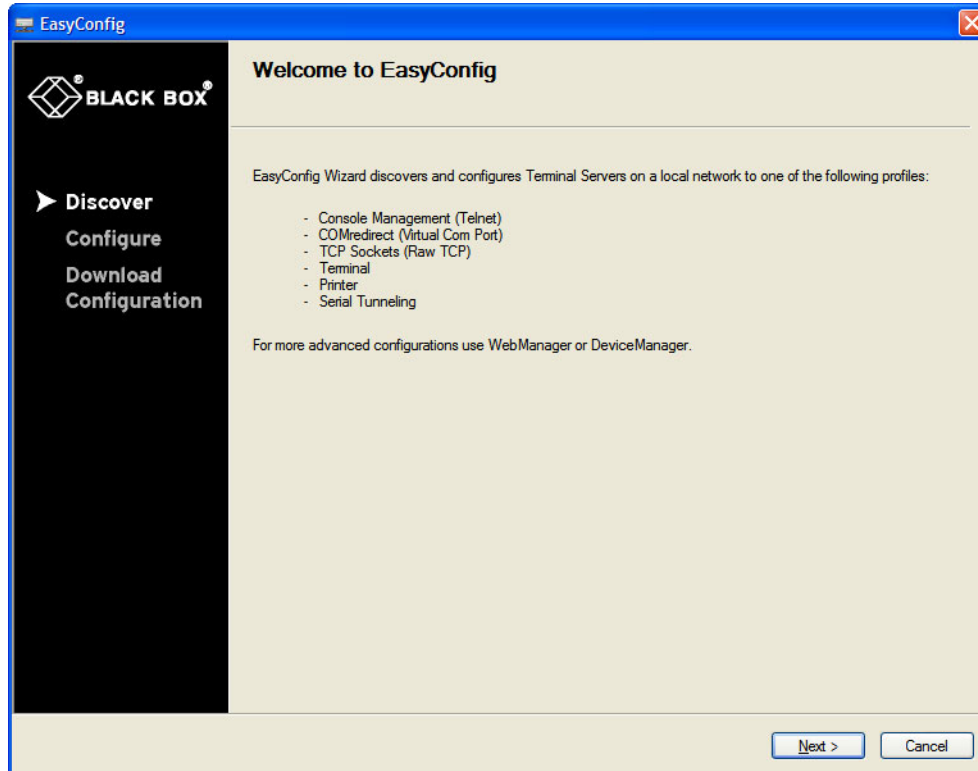
Introduction

There are several different configuration methods available to configure the Terminal Server (see [Chapter 3, Configuration Methods](#) for more information). This chapter describes the three main minimal configuration requirements for the Terminal Server through either Easy Config Wizard (cannot configure users using this method), DeviceManager, or WebManager:

1. **Setting up the network**—This minimally consists of configuring an IP address or enabling DHCP/BOOTP. Once the Terminal Server has an IP address, you can use any configuration method.
2. **Setting up the serial ports**—You will want to select the serial port profile that matches the serial port requirement/scenario for your serial device.
3. **Setting up users**—This is an optional step, which is only required when your implementation requires users to access the Terminal Server and you are not using external authentication.

Easy Configuration Wizard

The Easy Config Wizard quickly sets up the Terminal Server's network configuration and all serial ports to one of the following:



- **Console Management**—Allows users on the network to connect to a serial device that is connected to a serial port on the Terminal Server.
- **COMredirect (Virtual COM Port)**—Allows a networked system to communicate with your serial device through a virtual COM or TTY port, using the Black Box COMredirect software.
- **TCP Sockets (Raw TCP)**—Allows hosts on the network to communicate with a serial device that requires raw data throughput (such as a printer or card reader) connected to the Terminal Server serial port.
- **Terminal**—Allows a terminal device to connect to a specified host on the network through a serial port on the Terminal Server.
- **Printer**—Allows hosts on the network to talk to a printer using LPD connected to the Terminal Server.
- **Serial Tunneling**—Allows Terminal Servers on the network to establish a virtual link between their serial ports. Typically, one Terminal Server's serial port is configured as a Tunnel Server and the other Terminal Server's serial port is configured as a Tunnel Client.

Setting Up the Network

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

Using DeviceManager

To use the DeviceManager, you must first install it on a Windows® operating system. The DeviceManager is able to automatically discover all Terminal Servers on your local network, even if they have not yet been assigned an IP address. If routers on the network have been setup to propagate multicasts, DeviceManager will also be able to discover Terminal Servers in other networks. The DeviceManager installation wizard can be found on the CD-ROM included in the Terminal Server package.

1. Connect the Terminal Server to the network.
2. Power on the Terminal Server.
3. From the CD-ROM that was included in the Terminal Server packaging, select the DeviceManager link.
4. Click on the link under **Location** and click **Open** to automatically start the DeviceManager installation.
5. Install the DeviceManager by following the installation wizard. On the last window, check the **Yes, I want to launch DeviceManager now.** box and click the **Finish** button.
6. When you launch the DeviceManager, it will automatically scan the local network and display any Terminal Servers that it can find.
7. Any Terminal Server that does not have an IP address will be displayed as **Not Configured**, with the **Model** and **MAC Address** to identify the Terminal Server. Highlight the Terminal Server that you want to assign an IP address to and click the **Assign IP** button.
8. Choose the method you want to use to assign an IP address to the Terminal Server:
 - Type in the IP address that you want to assign to this Terminal Server.
 - Enable the **Have the Terminal Server automatically get a temporary IP address** option. This will turn on DHCP/BOOTP, so the Terminal Server will attempt to get its IP address from your DHCP/BOOTP server. If you don't have a DHCP/BOOTP server, DeviceManager will temporarily assign an IP address in the range of **169.254.0.1 - 169.254.255.255** that will be used only for the duration of the DeviceManager/Terminal Server communication.

Click the **Assign IP** button.

9. You are now ready to configure the Terminal Server. Double-click the Terminal Server you just configured IP address for to open a configuration session. Type **superuser** (the factory default Admin user password) in the Login window and click **OK**.
10. Expand the **Server Configuration** folder and select **Server**. Verify the IP address configuration. You should also enter a name in the **Server Name** field to make the Terminal Server easily identifiable.
11. To make your edits take effect, you need to download the new configuration file and then reboot the Terminal Server. Download the configuration file to the Terminal Server by selecting **Tools, Download Configuration to Unit** or click the **Download All Changes** button.
12. Reboot the Terminal Server by selecting **Tools, Reboot Server** or click the **Reboot** Terminal Server button.

For more information on configuring the Terminal Server using DeviceManager, see [Chapter 5, Using DeviceManager and WebManager](#).

Using WebManager

To use the WebManager as your configurator, you must first assign an IP address to the Terminal Server. You can use the Easy Config Wizard to assign an IP address to the Terminal Server or any of the other methods described in this section. Once the IP address is assigned to the Terminal Server, simply type the IP address into the **Address** field of your web browser and press the **Enter** key.

Using a Direct Serial Connection to Specify an IP Address

You can connect to the Terminal Server's serial console port using a PC with a terminal emulation package, such as HyperTerminal or a terminal.

1. Connect the Terminal Server to your PC or dumb terminal. Make sure the DIP switch is in Console mode (desktop models, this sets the Terminal Server serial port 1 to EIA-232) or that you are connected to the dedicated Console port (rack mount models). When connecting a terminal or PC directly (without modems), the EIA-232 signals need to be crossed over ('null modem' cable). For RJ45 models, the RJ45 to DB9F adaptor shipped with the unit will provide this crossover.
2. Using a PC emulation application, such as HyperTerminal, or from a dumb terminal, set the Port settings to 9600 Baud, 8 Data bits, No Parity, 1 Stop Bits, and No Hardware Flow control to connect to the Terminal Server. You can change these settings for future connections on the rack mount models (the Terminal Server must be rebooted for these changes to take place).
3. When prompted, type **admin** for the User and **superuser** for the Password. You should now see the a prompt that displays the model type and port number; for example, **Secure Console Server 16 port#**.
4. You are now logged into the Terminal Server and can set the IP address by typing from the command line using the Command Line Interface (CLI).

For single Ethernet connection models, type:

```
set server internet <ipv4address>
```

For dual Ethernet connection (Secure Console Server) models, type:

```
set server internet eth1 <ipv4address>
```

Where **ipv4address** is the IP Address being assigned to the Terminal Server.

5. Type the following command:

```
save
```
6. If you are going to use another configuration method, such as WebManager or DeviceManager, the Terminal Server will need to be re-booted first. On a desktop unit, change the DIP switch to the OFF (Serial) position before re-booting the Terminal Server. Plug the Terminal Server back in, automatically rebooting the Terminal Server in the process.
7. If you want to complete the configuration using a direct connection, see [Command Line Interface](#) and/or [Menu](#) . After you complete configuring the Terminal Server, it will need to be re-booted for the configuration to take effect. On a desktop unit, change the DIP switch to the OFF (Serial) position before re-booting the Terminal Server. Plug the Terminal Server back in, automatically rebooting the Terminal Server in the process.

Using a Direct Serial Connection to Enable BOOTP/DHCP

If you are using BOOTP, you need to add an entry in the BOOTP server for the Terminal Server that associates the MAC address (found on the back of the Terminal Server) and the IP address that you want to assign to the Terminal Server. After you have made the MAC address/IP address association for BOOTP, use the following directions for BOOTP or DHCP.

You can connect to the Terminal Server using a PC with a terminal emulation package, such as HyperTerminal or a dumb terminal.

1. Connect the Terminal Server to your PC or dumb terminal. Make sure the DIP switch is in Console mode (desktop models, this sets the Terminal Server serial port to EIA-232) or that you are connected to the dedicated Console port (rack mount models). When connecting a terminal or PC directly (without modems), the EIA-232 signals need to be crossed over ('null modem' cable). For RJ45 models, the RJ45 to DB9F adaptor shipped with the unit will provide this crossover.
2. Using a PC emulation application, such as HyperTerminal, or from a dumb terminal, set the Port settings to 9600 Baud, 8 Data bits, No Parity, 1 Stop Bits, and No Hardware Flow control to connect to the Terminal Server. You can change these settings for future connections on the rack mount models (the Terminal Server must be rebooted for these changes to take place).
3. When prompted, type **admin** for the User and **superuser** for the Password. You should now see the a prompt that displays the model type and port number; for example, **Secure Console Server 16 port#**.
4. You are now logged into the Terminal Server and can set the IP address by typing from the command line using the Command Line Interface (CLI). Type the following command:

```
set server internet dhcp/bootp on
```

5. Type the following command:

```
save
```

6. Type the following command:

```
reboot
```

7. When the Terminal Server reboots, it will automatically poll for an IP address from the DHCP/BOOTP server. If you have a Terminal Server with dual Ethernet, each Ethernet connection will automatically be assigned an IP address, you can access the Terminal Server through either IP address.
8. To view the DHCP/BOOTP assigned IP address, type the following command:

```
show interface ethernet
```

If for some reason it cannot obtain an IP address from your DHCP/BOOTP server, you will have to either reconnect to the Terminal Server on the console port and reboot it or push the Reset to Factory button to access the Terminal Server.

You are now ready to configure the Terminal Server. See [Chapter 3, Configuration Methods](#) for information on the different Terminal Server configuration methods.

Using ARP-Ping

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

1. 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 Terminal Server, and **aa:bb:cc:dd:ee:ff** is the Ethernet (MAC) address of Terminal Server (found on the back of the unit).

2. Whether you use UNIX or Windows®, you are now ready to ping to the Terminal Server. 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 Terminal Server will pickup and use the IP address entered into the ARP table in step 1. You are now ready to configure the Terminal Server. See [Chapter 3, Configuration Methods](#) for information on the different Terminal Server configuration methods.

For an IPv6 Network

The Terminal Server has a factory default link local IPv6 address that takes the following format:

Terminal Server MAC Address: 00-80-D4-AB-CD-EF

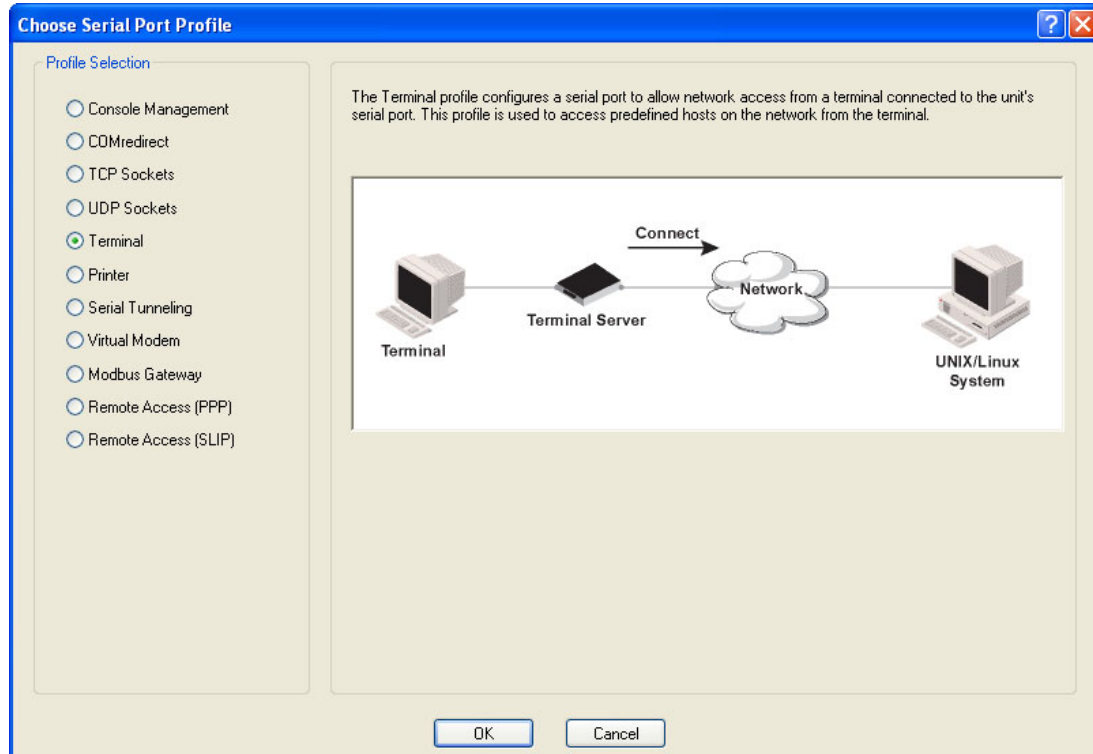
Link Local Address: fe80::0280:D4ff:feAB:CDEF

By default, the Terminal Server 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 [Chapter 6, Network Settings](#) for more information on IPv6 configuration options.

You are now ready to configure the Terminal Server. See [Chapter 3, Configuration Methods](#) for information on the different Terminal Server configuration methods.

Setting Up the Serial Port(s)

The DeviceManager and WebManager have the following serial port profiles that will simplify serial port setup:

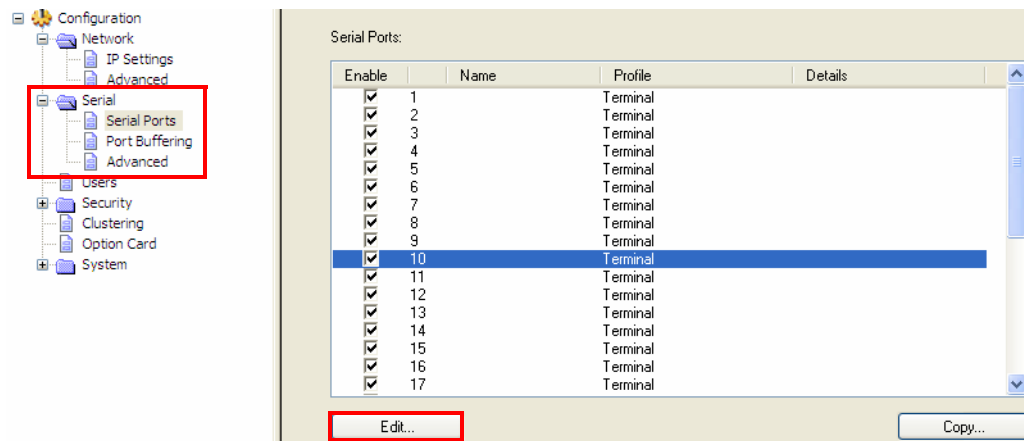


- **Console Management**—The Console Management profile configures a serial port to provide network access to a console or administrative port. This profile sets up a serial port to support a TCP socket that listens for a Telnet or SSH connection from the network.
- **COMredirect**—The COMredirect profile configures a serial port to connect network servers or workstations running the COMredirect 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.
- **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.
- **UDP Sockets**—The UDP Sockets profile configures a serial port to allow communication between the network and serial devices connected to the Terminal Server using the UDP protocol.
- **Terminal**—The Terminal profile configures a serial port to allow network access from a terminal connected to the Terminal Server's serial port. This profile is used to access predefined hosts on the network from the terminal.
- **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 Terminal Server. Both Terminal Server 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).

- **Virtual Modem**—The Virtual Modem (Vmodem) profile configures a serial port to simulate a modem. When the serial device connected to the Terminal Server initiates a modem connection, the Terminal Server starts up a TCP connection to another Terminal Server 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.
- **Remote Access (PPP)**—The Remote Access (PPP) profile configures a serial port to allow a remote user to establish a PPP connection to the Terminal Server's serial port. This is typically used with a modem for dial-in or dial-out access to the network.
- **Remote Access (SLIP)**—The Remote Access (SLIP) profile configures a serial port to allow a remote user to establish a SLIP connection to the Terminal Server's serial port. This is typically used with a modem for dial-in or dial-out access to the network.

Each serial port profile contains all the parameters that are required to completely configure the serial port scenario represented by the profile.

To select a serial port profile in the DeviceManager, connect through the DeviceManager to the Terminal Server you are configuring and select **Serial, Serial Ports** in the navigation pane. Highlight the serial port you want to configure and then click **Edit**.

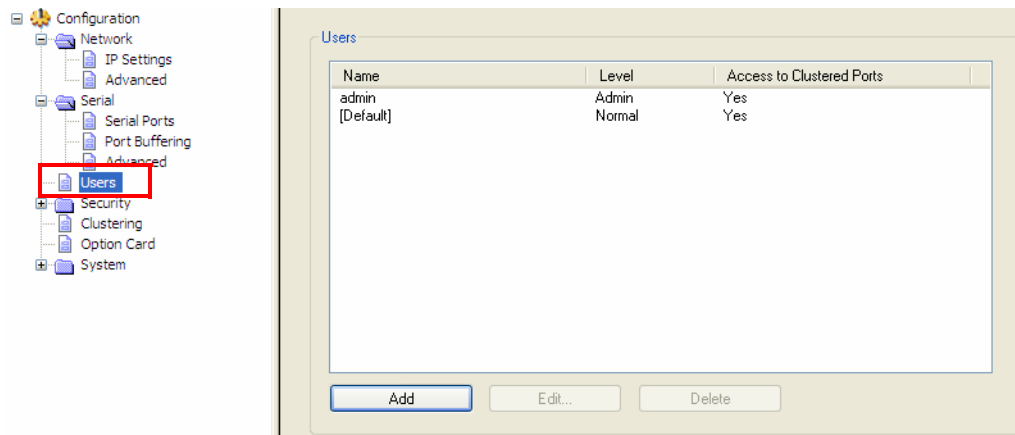


When the default serial port profile Terminal displays, click the **Change Profile** button and select the appropriate profile for the serial port. See [Chapter 8, Configuring Serial Ports](#) for more information on the serial port profiles and their configuration parameters.

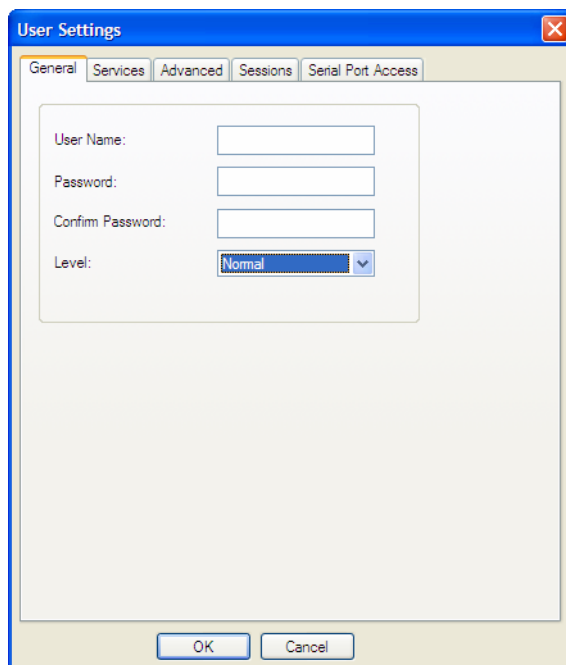
Setting Up Users

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 Terminal Server, you can create a user account and configure the user's access privileges. Notice that there is a Default user; the Default user's parameters are inherited by users logging into the Terminal Server who are being authenticated by an external authentication method (see [Authentication](#) for more information) or are accessing the Terminal Server as a Guest (see [Local](#) for more information).

To add a user account, click on the **Users** page in the navigation pane.



Click the **Add** button to create a user account.



To quickly add a user, fill out the field in the **General** tab and click **OK**.

See [Chapter 7, Configuring Users](#) for more information about the other user parameters you can configure.

5

Using DeviceManager and WebManager

Introduction

The DeviceManager and WebManager Terminal Server managers have been designed to be very similar to use. DeviceManager is a Windows®-based application and WebManager is a browser-based application. Both options use the Terminal Server's IP address to access the Terminal Server; the DeviceManager can be used to assign an IP address to a new Terminal Server and the WebManager requires that the Terminal Server already have an IP address before it can be used to configure the Terminal Server.

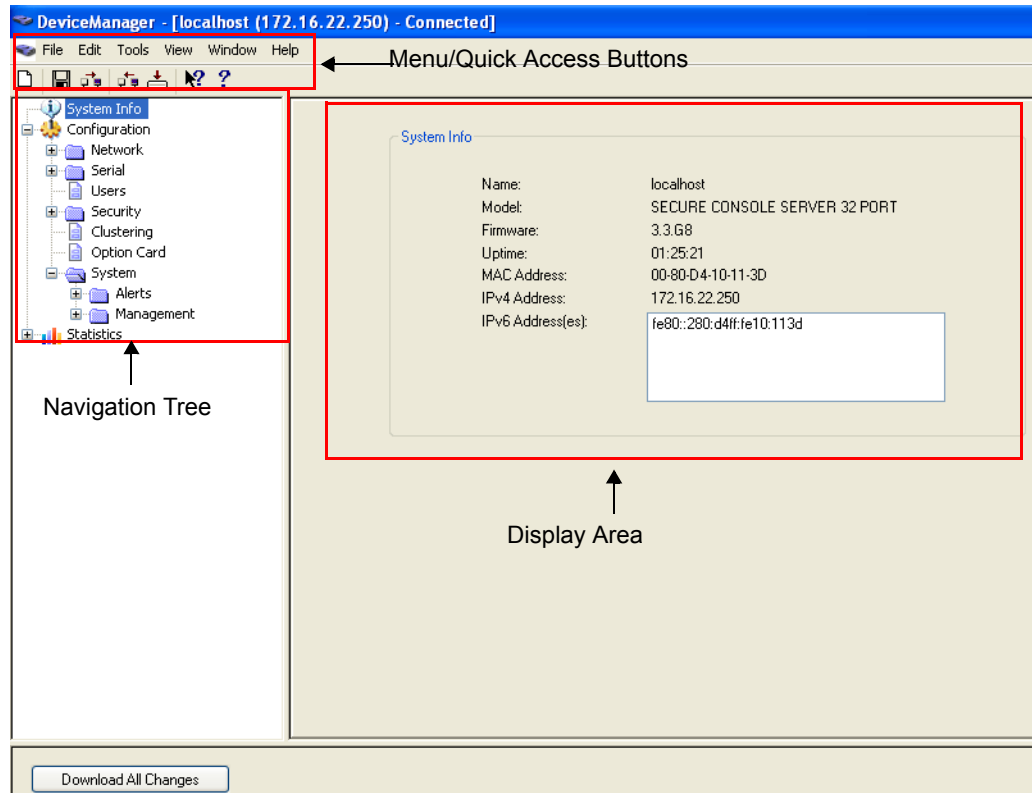
When using WebManager, you are required to click the **Apply** button each time you make a change to a configuration window/tab. In DeviceManager, you must download your configuration changes to the Terminal Server either periodically or after you are done with the configuration changes. From both managers you must reboot the Terminal Server in order for your configuration changes to take effect.

Navigating DeviceManager/WebManager

The DeviceManager and WebManager have very similar navigation methods. The left-hand side of the manager is the navigation tree and the center is the configuration area. The DeviceManager has menu and quick access buttons, whereas the WebManager has system information and some navigation options on the far right-hand side.

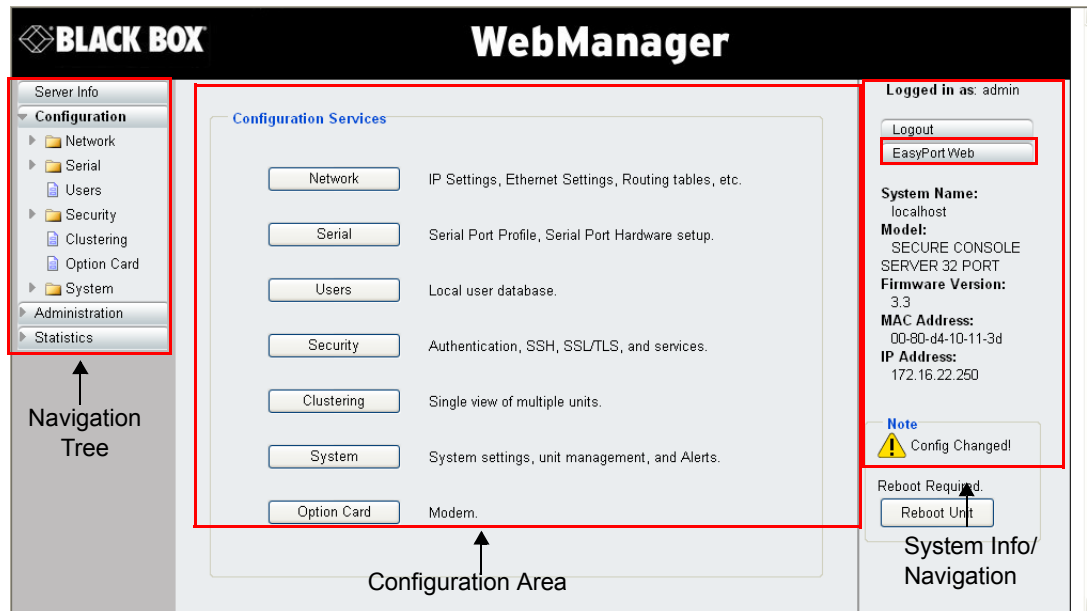
DeviceManager

The DeviceManager uses a folder/page navigation tree. You can expand the folders to see the available configuration pages. When you access a configuration page, you can often navigate the tabs in the configuration area to access all of the configuration options.



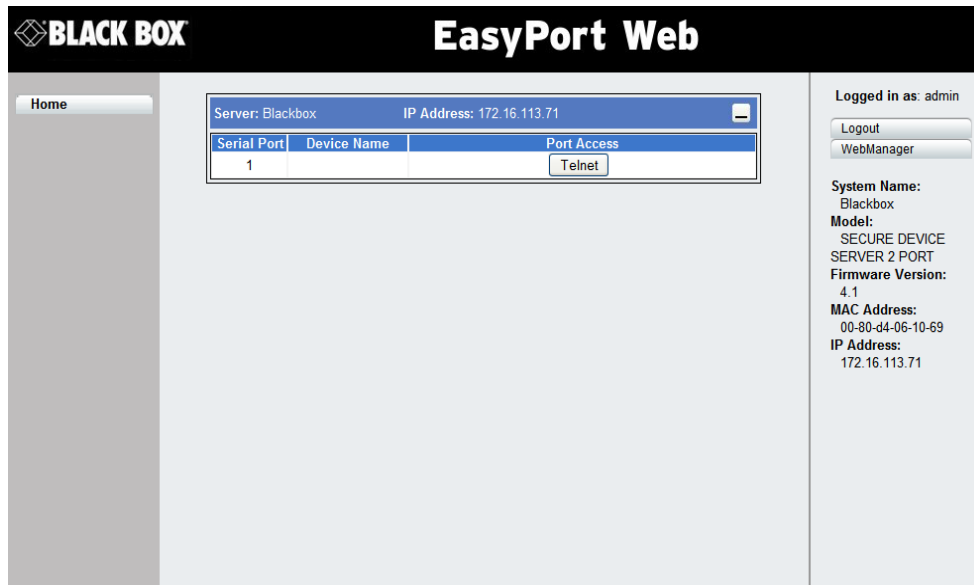
WebManager

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.



EasyPort Web

WebManager also launches EasyPort Web, which is a browser-based management tool that can be used to manage clustered Terminal Servers. EasyPort Web can also be launched by any user who can connect to the Terminal Server through a web browser.



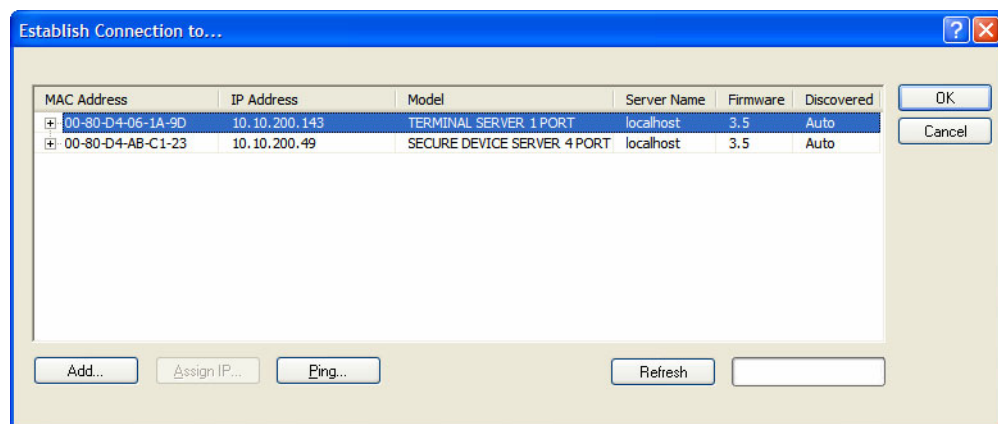
Using DeviceManager to Connect to the Terminal Server

DeviceManager can connect to existing Terminal Servers or assign an IP address to a new Terminal Server. Whenever you connect to a Terminal Server through the DeviceManager, you connect as the Admin user and must supply the password for the Admin user.

Starting a New Session

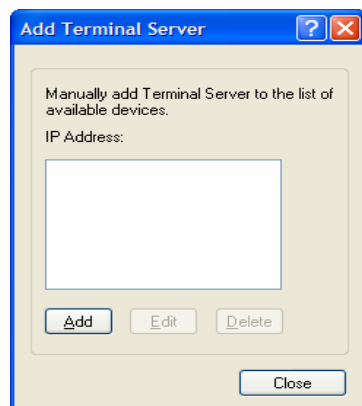
To start a new session and connect to the Terminal Server using the DeviceManager:

1. Start the DeviceManager by selecting **Start, All Programs, Black Box, DeviceManager, DeviceManager**.
2. When the DeviceManager starts, it searches the network for Terminal Servers.



Note: If you are not seeing IPv6 addresses in the list (you must expand the entry), see [IPv6 Issues](#) to find out how to install IPv6 support.

If your Terminal Server is not in the local network and you do not have a multicast enabled router in your network and therefore is not displayed in the selectable list, but can be pinged from your PC, you can add it to the selectable list by clicking the **Add** button.



Click the **Add** button and type in the Terminal Server's IP address; this field supports IPv4 and IPv6 addresses. Click the **Close** button when you have completed adding all the manual entries. Select the manually added server to connect to it.

Assigning a Temporary IP Address to a New Terminal Server

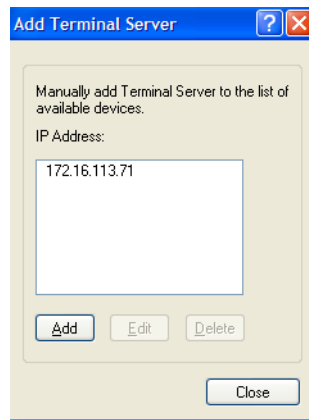
You can temporarily assign an IP address to the Terminal Server that is connected to your local network segment, for the purpose of connecting to it and downloading a configuration file (containing a permanent IP address). To temporarily assign an IP address to the Terminal Server, do the following:

1. Click the **Refresh** button. The Terminal Server will be displayed in the **IP Address** column as **Not Configured**.
2. Select the new Terminal Server and click the **Assign IP** button.
3. Type a valid temporary IP address into the address field or, in version 3.2 or higher, enable the **Have the Terminal Server automatically get a temporary IP address**. If you enable the temporary IP address, the Terminal Server will enable DHCP/BOOTP on your Terminal Server and attempt to get an IP address from the DHCP/BOOTP server (this will permanently enable DHCP/BOOTP in your Terminal Server's configuration, until you change it). If your network does not have a DHCP/BOOTP server, the Terminal Server will temporarily assign an IP address in the range of **169.254.0.1 - 169.254.255.255** (this IP address is only assigned for the duration of the DeviceManager/Terminal Server connection).
4. Click the **Assign IP** button.
5. Double-click the Terminal Server in the Terminal Server **List**. If this is the first time you are accessing the Terminal Server, type in the factory default Admin password, **superuser**, and click **OK**. The DeviceManager will display a window indicating that it is trying to authenticate and connect you on the Terminal Server.
6. If the authentication and connection are successful, the Server Info window is displayed. You are now ready to configure the Terminal Server. If authentication was unsuccessful, try to connect to the Terminal Server again; you probably mistyped the password for the Admin user.

For more information about managing a Terminal Server, see [Configuration Files](#) .

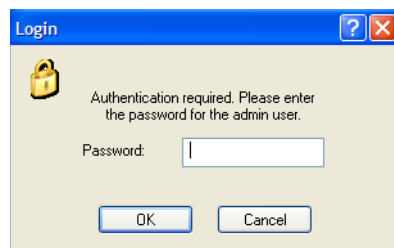
Adding/Deleting Manual Terminal Servers

To permanently add or delete a Terminal Server to/from the Terminal Server **List**, click the **Add** button

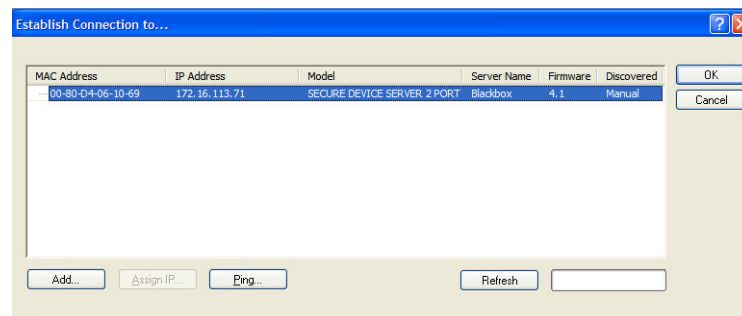


Logging in to the Terminal Server

To log in to a Terminal Server, double-click on the Terminal Server in the **Device Server List**. You will be prompted for the Admin Password (the default is **superuser**)



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

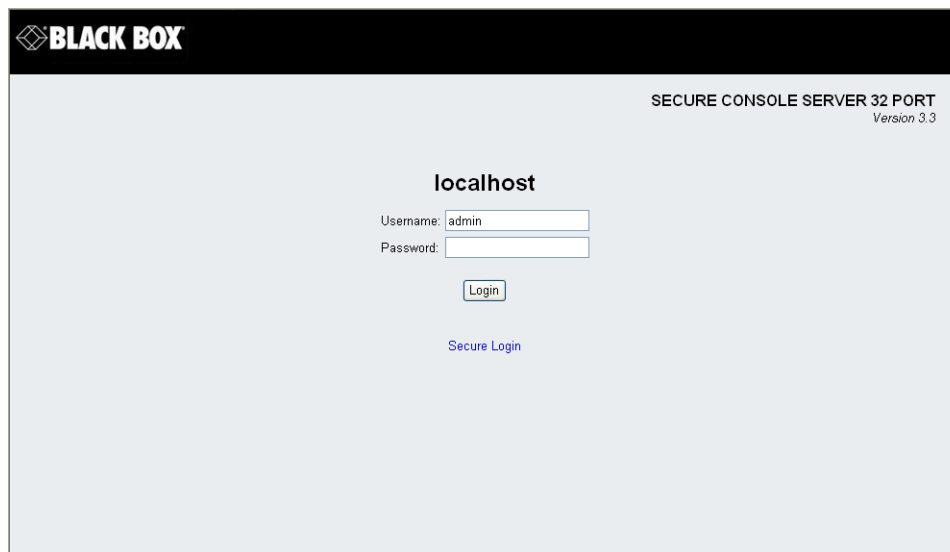


If you cannot connect to a Terminal Server, you can highlight the Terminal Server and click the **Ping** button to verify that the DeviceManager can communicate with the Terminal Server's IP Address. If the ping times out, then you might need to set up a Gateway in your Terminal Server or verify that your network is communicating correctly.

Using WebManager to Connect to the Terminal Server

WebManager can only connect to Terminal Servers that already have an assigned IP address. To connect to the Terminal Server, type the IP address of the Terminal Server into the **Address** field as such: **http://10.10.234.34**.

You will see the login screen.



BLACK BOX

SECURE CONSOLE SERVER 32 PORT
Version 3.3

localhost

Username:

Password:

[Secure Login](#)

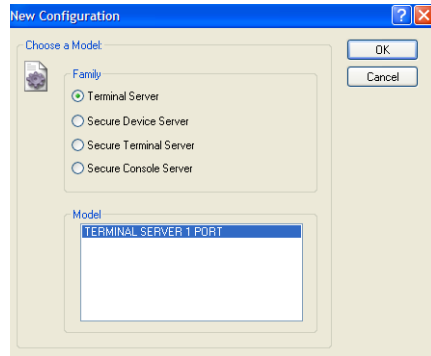
Logging into the Terminal Server

Type in the Admin password in the **Password** field and click the **Login** button. A user who does not have admin privileges can access EasyPort Web to access clustered serial ports by typing their user name and password on the login screen.

Configuration Files

Creating a New Terminal Server Configuration in DeviceManager

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



Select the Terminal Server 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 Terminal Server, import the created configuration file into DeviceManager (this is not available in WebManager), and then download the configuration file to the Terminal Server 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. Terminal Server configuration files saved in the DeviceManager can be in the Terminal Server-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. Terminal Server 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 Terminal Server, you must first connect to the Terminal Server that you want to download the configuration file to. Once you have successfully logged into the Terminal Server, 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 Terminal Server.

Managing the Terminal Server

Most of the management tasks, such as setting the time/date, downloading keys/certificates, downloading firmware, downloading custom files, resetting serial ports, etc., are found under the **Tools** menu option in the DeviceManager and under **Administration** in WebManager.

6 Network Settings

Introduction

The Network section is used to configure the parameters that identify the Terminal Server within the network and how the Terminal Server accesses hosts on the network.

The following configuration windows are available:

- **IP Settings**—This window configures the Terminal Server’s name, IP address, and Ethernet information. See [IP Settings](#) for more information.
- **Advanced**—This window configures hosts that the Terminal Server will be communicating with, routes, DNS/WINS servers, RIP, Dynamic DNS, and IPv6 Tunnels. See [Advanced](#) for more information on these options.

IP Settings

IPv4 Settings

Overview

The parameters in IPv4 settings are used to access the Terminal Server and are how the Terminal Server accesses the network.

Field Descriptions

The screenshot shows the 'IPv4 Settings' window with three tabs: 'IPv4 Settings' (selected), 'IPv6 Settings', and 'Advanced'. The window is divided into two main sections: 'System Settings' and 'IPv4 Configurations'. In 'System Settings', there is a 'System Name' field containing 'localhost' and a 'Domain' field. The 'IPv4 Configurations' section contains 'Ethernet Interface Settings' with two radio buttons: 'Obtain IP address automatically using DHCP/BOOTP' (unselected) and 'Use the following IP address:' (selected). Below these are fields for 'IP Address' and 'Subnet Mask', both set to '0 . 0 . 0 . 0'. At the bottom, there are fields for 'Default Gateway', 'DNS Server', and 'WINS Server', all currently empty.

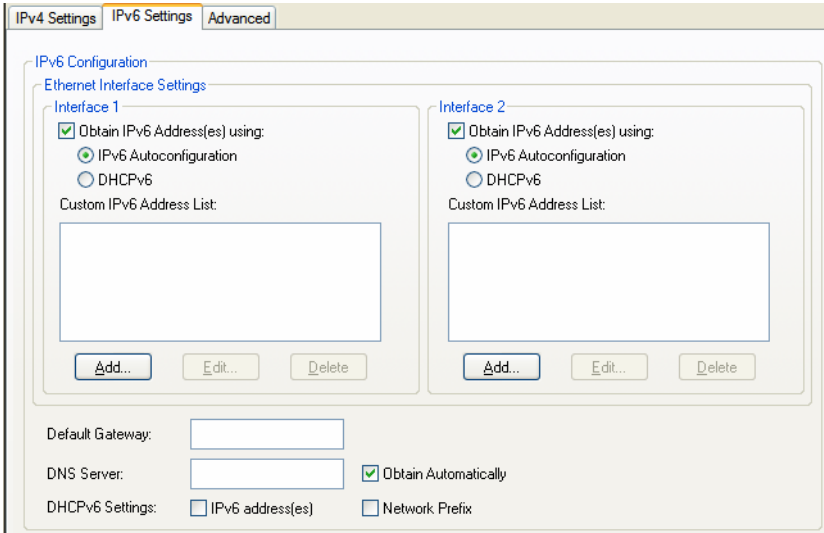
Configure the following parameters:

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). Default: localhost
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 .
Obtain IP Address automatically using DHCP/BOOTP	When enabled, the Terminal Server will request an IP address from the DHCP/BOOTP server. By default, when this option is enabled, the Terminal Server 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 Terminal Server. Field Format: IPv4 address
IP Address	The Terminal Server's unique IPv4 network IP 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 Terminal Server 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 address
DNS Server Obtain Automatically	When DHCP/BOOTP is enabled, you can enable this option to have the Terminal Server 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 Terminal Server receive the WINS IP address from the DHCP/BOOTP server. Default: Enabled

IPv6 Settings

Overview

Configure IPv6 settings when the Terminal Server resides in an IPv6 network.



Field Descriptions

Configure the appropriate parameters:

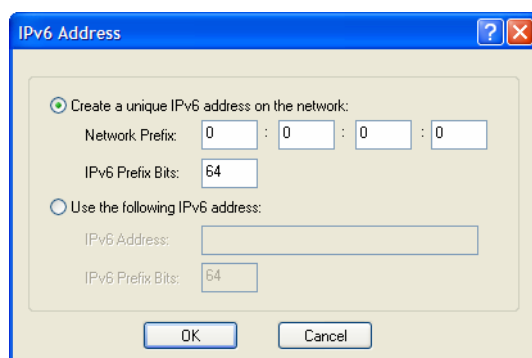
Obtain IPv6 Address(es) using	When enabled, you can configure the Terminal Server to obtain the IPv6 address(es) using IPv6 Autoconfiguration or a DHCPv6 server. Default: Enabled
IPv6 Autoconfiguration	When enabled, the Terminal Server will send out a Router Solicitation message. If a Router Advertisement message is received, the Terminal Server 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 Terminal Server 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.
Add Button	Adds a custom IPv6 address.
Edit Button	Edits an existing IPv6 address.
Delete Button	Deletes an IPv6 address from the Custom IPv6 address list.
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 Terminal Server receive the DNS IP address from the DHCPv6 server. Default: Enabled
DHCPv6 Settings IPv6 Address(es)	When enabled, the Terminal Server will accept IPv6 address(es) from the DHCPv6 server. Default: Disabled
DHCPv6 Settings Network Prefix	When enabled, the Terminal Server will accept the network prefix from the DHCPv6 server. Default: Disabled

Adding/Editing a Custom IPv6 Address

You can manually add one of the following:

- The IPv6 network prefix (and the Terminal Server will determine an IPv6 address based on the network prefix and the Terminal Server MAC address).
- The complete IPv6 address.



Configure the following parameters:

Create a unique IPv6 address on the network	When enabled, the Terminal Server will derive an IPv6 address from the entered network prefix and the Terminal Server's MAC address. Default: Enabled
Network Prefix	Specify the IPv6 network prefix. The Terminal Server will derive the complete IPv6 address from the entered network prefix and the Terminal Server's MAC address. Default: Enabled
Network Prefix IPv6 Prefix Bits	Specify the network prefix bits for the IPv6 address. Range: 0-64 Default: 64
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

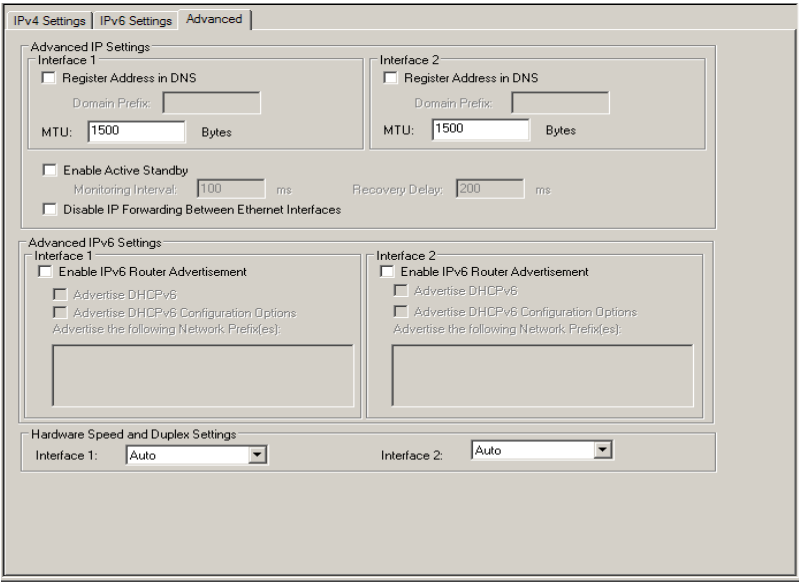
Overview

The **Advanced** tab configures Active Standby (Secure Console Server models only), DNS update, IPv6 Advertising Router settings, and the Ethernet interface(s) hardware speed and duplex.

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

- you have already set up Dynamic DNS with DynDNS.com
- you want to enable Active Standby (Secure Console Server models only)
- you want to specify the line speed and duplex
- you want the Terminal Server to act as an IPv6 Advertising Router

Field Descriptions



Configure the appropriate parameters:

Register Address in DNS When this parameter is set, the Terminal Server 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.
Default: Disabled

Maximum Transmission Unit (MTU) The Maximum Transmission Unit (MTU) size of an IP frame that will be sent over the network. If your Terminal Server has more than one Ethernet interface each interface can be set separately, however only one MTU size can be set for both IPV4 or IPV6 frames.
MTU IPV4: 68-1500 bytes
MTU IPV6: 68-1500 bytes

Domain Prefix	<p>(Secure Console Server models only) A domain prefix to uniquely identify the Ethernet interface to the DNS when the Terminal Server has two Ethernet interfaces. 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>
Enable Active Standby	<p>(Secure Console Server models only) 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>
Disable IP forwarding between Ethernet Interfaces	<p>SCS 8,16,32 models with two Ethernet Interfaces.</p> <p>When enabled, no IP traffic will be forwarded between Ethernet interfaces.</p> <p>Default: Disabled</p>
Monitoring Interval	<p>(Secure Console Server only) 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>(Secure Console Server only) The time that the Terminal Server will wait to make the secondary interface (Ethernet 2) active after it has been detected as up.</p> <p>Default: 200 ms</p>
Enable IPv6 Router Advertisement	<p>When enabled, the Terminal Server 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 enable or disable specific network prefixes from being advertised to hosts.</p> <p>Default: Enabled</p>

**Interface 1
Hardware Speed
and Duplex**

Define the Ethernet connection speed (desktop models can support up to 100 Mbps and rack models can support up to 1000 Mbps).

Data Options:

- **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**

Default: Auto

**Interface 2
Hardware Speed
and Duplex**

Define the Ethernet connection speed (available on Secure Console Server models only).

Data Options:

- **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**

Default: Auto

Advanced

Host Table

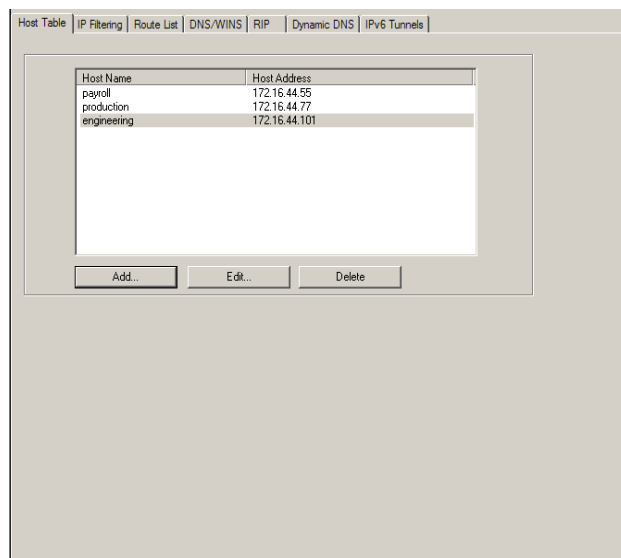
Overview

The Host table contains the list of hosts that will be accessed by an IP address or Fully Qualified Domain Name (FQDN) from the Terminal Server. 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.

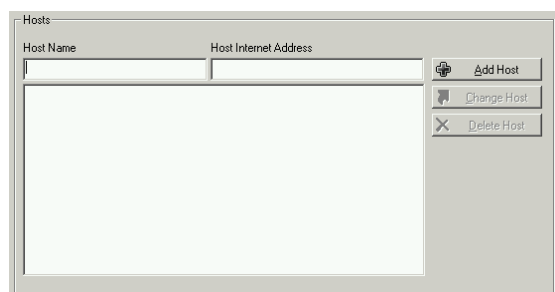
Functionality

You can configure up to 50 hosts using IPv4 or IPv6 internet addresses on desktop Terminal Server models; you can configure up to 100 hosts on rack mount Terminal Server models.

Field Descriptions



Adding/Editing a Host



Configure the appropriate parameters:

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

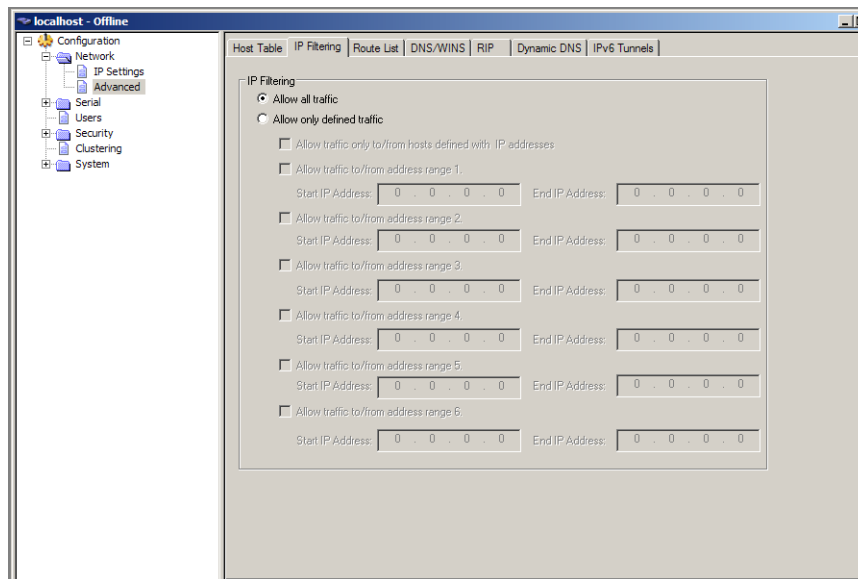
IP Filtering

Configure the appropriate parameters:

Overview

The IP Filtering Host table allows you to configure:

- any host to connect to the Terminal Server
- only hosts as defined in the Host Table and/or
- specify up to 6 IP address ranges



Functionality

You can specify up to 6 IP traffic to/from address ranges.

Field Descriptions

Configure the appropriate parameters

IP Filtering

Data Options:

Allow all traffic - Allows any host to connect to the Terminal Server.

Default: allow all ranges

IP Filtering on Host Allow only defined traffic to/from hosts defined with IP addresses - a security feature that when enabled, the Terminal Server will only accept data or send data to hosts configured in the Terminal Server's **Host Table**.

IP Filtering on Range

Allows traffic to/from address range - a security feature that when enabled, the Terminal Server will only accept data or send data to hosts configured with these address ranges.

Route List

Overview

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

Functionality

There are three types of routes:

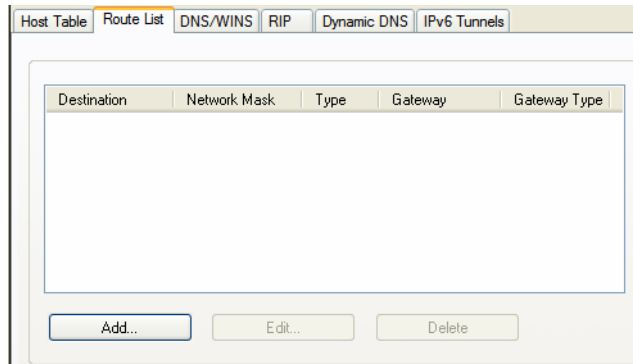
- **Default**—A route that provides general access beyond your local network.
- **Host**—A route defined for accessing a specific host external to your local network.
- **Network**—A route defined for accessing a specific network external to your local network.

You can specify up to 20 routes on desktop Terminal Server models; you can specify up to 49 routes on rack mount Terminal Server models.

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.

Field Descriptions



The following buttons are available on this window:

- | | |
|----------------------|--|
| Add Button | Adds a route to the Route List. |
| Edit Button | Changes an existing route in the Route List. |
| Delete Button | Deletes a route from the Route List. |

Adding/Editing Routes

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

Configure the appropriate parameters:

Type	<p>Specify the type of route you want to configure.</p> <p>Data Options:</p> <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. <p>Default: Default</p>
IP Address	<p>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.</p> <p>Format: IPv4 or IPv6 Address</p>
IPv4 Subnet Mask	<p>When the route is a Network route, you must specify the network's subnet mask.</p>
IPv6 Prefix Bits	<p>If the IP address is IPv6, then you must specify the network's prefix bits.</p> <p>Range: 0-128</p>
Host	<p>Select this option when a host is being used at the route gateway.</p> <p>Default: Enabled, None</p>

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

Overview

You can configure WINS servers for PPP-client name resolution and DNS servers for PPP-client name resolution and Terminal Server host name resolution (for example, when specifying **Bootup** file).

Functionality

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.

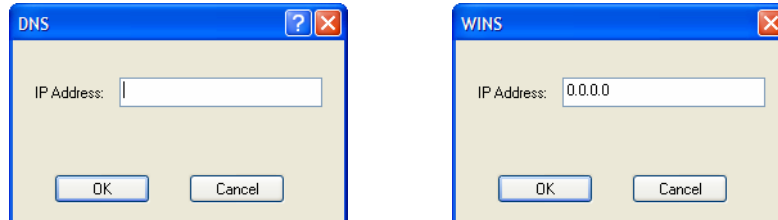
Field Descriptions

The following buttons are available on this window:

- Add DNS Button** Adds a DNS server.
- Edit DNS Button** Edits an existing DNS server.
- Delete DNS Button** Deletes a DNS server.
- Add WINS Button** Adds a WINS server.
- Edit WINS Button** Edits an existing WINS server.

Delete WINS Button Deletes a WINS server.

Editing/Adding DNS/WINS Servers



Configure the parameter:

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

Overview

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.

Functionality

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 Terminal Server 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 Terminal Server 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.

Field Descriptions

The screenshot shows the RIP configuration window. At the top, there are tabs: Host Table, Route List, DNS/WINS, RIP (selected), Dynamic DNS, and IPv6 Tunnels. Below the tabs, the 'Ethernet Mode' is set to 'None'. Under 'Authentication Method', 'None' is selected. Below that are fields for 'Password' and 'Confirm Password'. Under 'MD5', there is a table with columns: ID, Start Date, Start Time, End Date, End Time, Key, and Confirm Key. The table contains four rows, each with a checkbox, the value '0', and default date/time values (12/31/1969 and 7:00:00 PM).

Configure the appropriate parameters:

Ethernet Mode Enable/disable RIP (Routing Information Protocol) mode for the Ethernet interface.

Data Options:

- **None**—Disables RIP over the Ethernet interface.
- **Send**—Sends RIP over the Ethernet interface.
- **Listen**—Listens for RIP over the Ethernet interface.
- **Send and Listen**—Sends RIP and listens for RIP over the Ethernet interface.

Default: None

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.

ID The **MD5** identification key.

Start Date The start date that the MD5 key becomes valid. The date format is dependent on your system's settings.

Start Time The time that the MD5 key becomes valid. The time format is dependent on your system's settings.

End Date The last day that the MD5 key is valid. The date format is dependent on your system's settings.

End Time	The time that the MD5 key becomes invalid. The time format is dependent on your system's settings.
Key	The MD5 key that is being used by your routers.
Confirm Key	Retype the MD5 key that is being used by your routers to verify that it was typed correctly.

Dynamic DNS

Overview

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

Functionality

When the Terminal Server 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 Terminal Server. 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 Terminal Server 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 Terminal Server's dynamic DNS parameters to match the **Host**'s configuration on the DynDNS.com server. Every time the Terminal Server gets assigned a new IP address, it will update DynDNS.com with the new IP address.
3. Users accessing the Terminal Server via the internet can now access it via its fully qualified host name. For example, **telnet yourcompanySCS.DynDNS.org**.

Field Descriptions

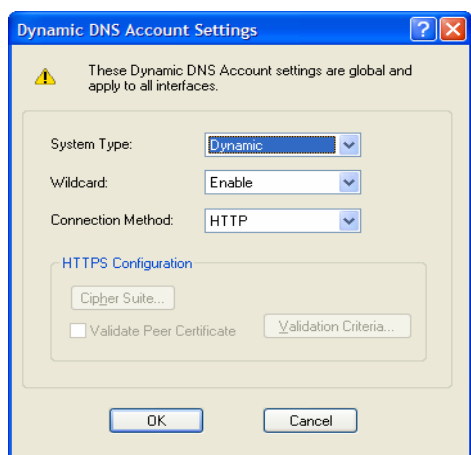
Configure the appropriate parameters:

Enable Dynamic DNS for the system	Enables/disables the dynamic DNS feature. When Dynamic DNS is enabled, the Terminal Server will automatically update its IP address with DynDNS.org if it changes. Default: Disabled
--	---

Host	Specify the registered hostname with DynDNS.org that will be updated with the Terminal Server's IP address should it change. Put in the full name; for example, myterminalserver.dyndns.org .
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.
Account Settings Button	Click this button to configure the Dynamic DNS DynDNS.org account information.

Account Settings

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



Configure the appropriate parameters:

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 *.yourcompanySCS.dyndns.org pointing to the same IP address as entered for yourcompanySCS.dyndns.org .
Connection Method	Specify how the Terminal Server is going to connect to the DynDNS.org server. Data Options: <ul style="list-style-type: none"> • HTTP • HTTP through Port 8245 • HTTPS—for a secure connection to the DynDNS server Default: Disabled
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 Terminal Server. See Cipher Suite Field Descriptions for more information.

Validate Peer Certificate

Enables/disables peer validation between the DynDNS.org server and the Terminal Server. This may be desirable, since the DynDNS user name and password are sent from the Terminal Server to the DynDNS server when the IP address needs to be updated and when an account refresh is performed. Account refreshes are done periodically to ensure that DynDNS accounts do not auto-delete should the IP address change infrequently. This parameter will only take effect if **HTTPS** is selected as the connection method.

Default: Disabled

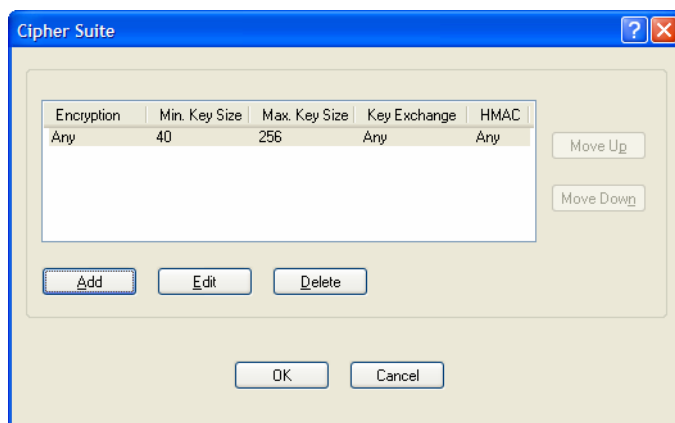
Validation Criteria Button

Launches the peer validation criteria window so you can specify the information used to validate the connection between the DynDNS.org server and the Terminal Server.

See [Validation Criteria Field Descriptions](#) for more information.

Cipher Suite Field Descriptions

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

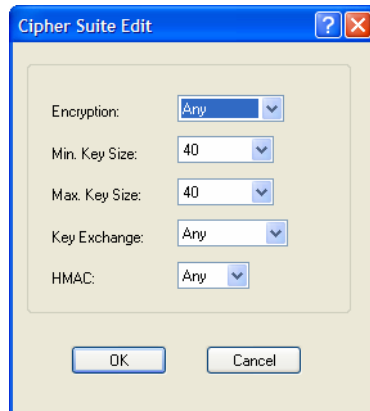


The following buttons are available on this window:

- Add Button** Adds a cipher to the cipher list.
- Edit Button** Edits a cipher in the cipher list.
- Delete Button** Deletes a cipher from the cipher list.
- Move Up Button** Moves a cipher up in preference in the cipher list.
- Move Down Button** Moves a cipher down in preference in the cipher list.

Adding/Editing a Cipher Suite

To see a list of valid cipher suite combinations, see [Appendix 15, SSL/TLS Ciphers](#).



Configure the following 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

The type of key to exchange for the encryption format.

Data Options:

- **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.

Default: Any

HMAC

Select the key-hashing for message authentication method for your encryption type.

Data Options:

- Any
- MD5
- SHA1
- SHA256
- SHA384

Default: Any

Validation Criteria Field Descriptions

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.

The screenshot shows a window titled "SSL Validation Criteria". Inside, there are seven rows, each with a checkbox and a text input field. The rows are labeled: "Country:", "State/Province:", "Locality:", "Organization:", "Organization Unit:", "Common Name:", and "Email:". At the bottom of the window are two buttons: "OK" and "Cancel".

Configure the following parameters:

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

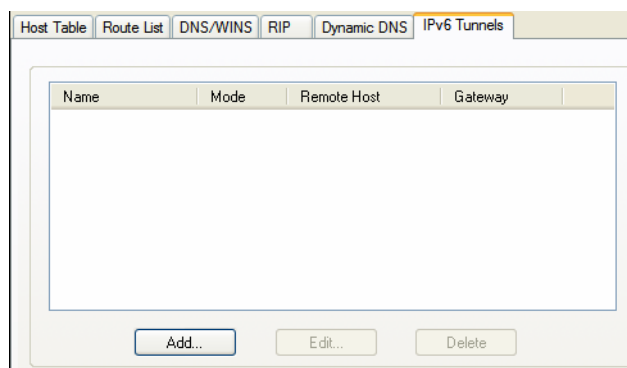
State/Province	An entry for the state/province; for example, IL. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate. Data Options: Maximum 128 characters
Locality	An entry for the location; for example, Chicago. This field is case sensitive in 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

IPv6 Tunnels

Overview

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 [IP Filtering](#) for more information).

Field Descriptions



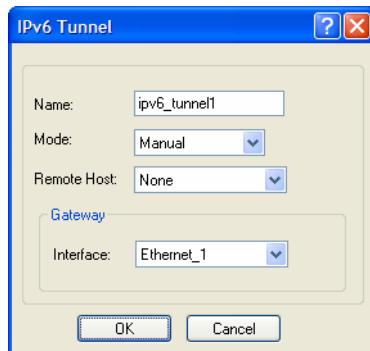
The following buttons are available:

Add Button Adds an IPv6 tunnel.

Edit Button	Edits an existing IPv6 tunnel.
Delete Button	Deletes an IPv6 tunnel. If a tunnel is associated with a route, it cannot be deleted until the route is either changed or deleted.

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.



Configure the following parameters:

Name	<p>The name of the IPv6 tunnel.</p> <p>Field Format: Maximum 16 alphanumeric characters</p> <p>Default: ipv6_tunnel1</p>
Mode	<p>The method or protocol that is used to create the IPv6 tunnel.</p> <ul style="list-style-type: none"> • Manual—When enabled, the Terminal Server will manually create the IPv6 tunnel to the specified Remote Host through the specified Interface. • 6to4—When enabled, the Terminal Server will broadcast to the multicast 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 Terminal Server. • 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. <p>Default: Manual</p>
Remote Host	<p>The IPv4 host that can access the IPv6 network when the Mode is Manual. The Teredo server when the Mode is Teredo.</p> <p>Default: None</p>
Interface	<p>The interface that the Terminal Server 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.</p> <p>Default: Ethernet 1</p>

7 Configuring Users

Introduction

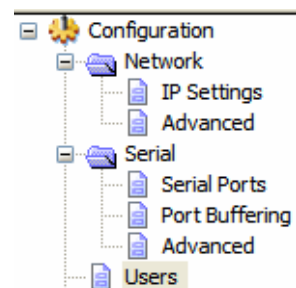
You can configure up to four users in the Terminal Server's local user database for all Terminal Server, Secure Device Server, and Secure Terminal Server 1-port to 4-port desktop models, in addition to the Admin user. You can configure up to 48 users in the Terminal Server's local user database for all Secure Terminal Servers, Secure Console Servers, and Secure Device Server rack mount models, in addition to the Admin user. 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 Terminal Server 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 Terminal Server from a network connection, the user database can be used to:

- Provide authentication on the Terminal Server 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.

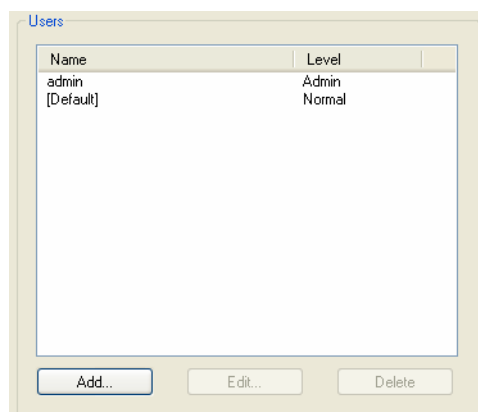
User Settings

Overview

The Users window allows you to add, edit, and delete users from the Terminal Server. **Note:** you can not delete the **admin** user.

Functionality

The Users window displays the users who have been configured. You can add users, edit existing users, or delete users from this window. See [Adding/Editing Users](#) for information on the parameters available when adding or editing a user.



Adding/Editing Users

General Tab

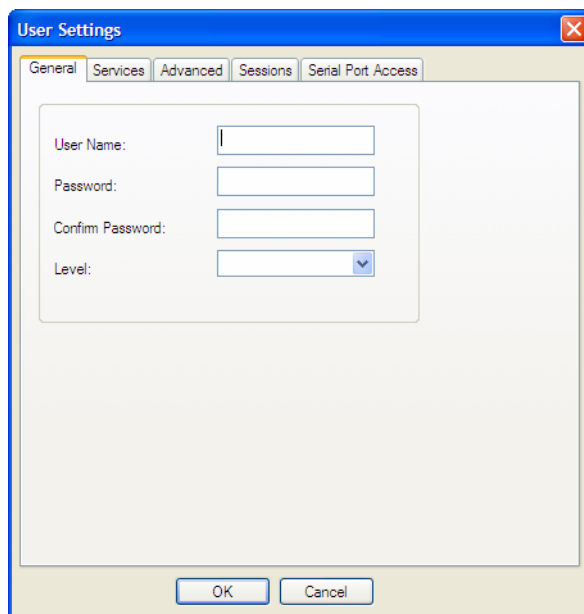
Overview

The General tab configures the basic user information.

Functionality

You must, minimally, provide a **User Name** and **Level** for a user.

Field Descriptions

The image shows a 'User Settings' dialog box with a blue title bar and a close button. It has five tabs: 'General' (selected), 'Services', 'Advanced', 'Sessions', and 'Serial Port Access'. The 'General' tab contains four input fields: 'User Name' (a text box), 'Password' (a text box), 'Confirm Password' (a text box), and 'Level' (a dropdown menu). At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Configure the following parameters:

- | | |
|-------------------------|---|
| 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 Terminal Server. |
| Confirm Password | Enter the user's password again to verify it is entered correctly. |

Level

The access that a user is allowed.

Data Options:

- **Admin**—The admin level user has total access to the Terminal Server. You can create more than one admin user account but we recommend that you only have one. They can monitor and configure the Terminal Server. 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 Terminal Server.
- **Normal**—The Normal level user has limited access to the Terminal Server. 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 Terminal Server.
- **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 Terminal Server 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 session 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 Access allows the user to connect to the accessible line without disconnecting their initial connection to the Terminal Server. Does not have any access to CLI commands.

When the Admin user logs into the Terminal Server, the prompt ends with a #, whereas all other users' prompts ends with a \$ or £, depending on the character set.

Default: Normal

Note: 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:

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 Terminal Server and the user will appear to have connected from the network.

Services Tab

Overview

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

Functionality

When a **Terminal** profile is set for the serial port and **Require Login** has been selected, user's accessing the Terminal Server 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 Terminal Server 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.

Field Descriptions

Configure the following parameters:

Service	Used in conjunction with the Terminal Profile . After the user has successfully been authenticated, the specified service is started. Data Options: DSPrompt, Telnet, SSH, RLogin, SLIP, PPP, TCP Raw, SSL Raw Default: DSPrompt
Host IP	For outbound User Services such as Telnet , SSH , 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. Default: 0.0.0.0

TCP Port	<p>When the User Service is Telnet, SSH, TCP Clear or SSL Raw, 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> <ul style="list-style-type: none"> • 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>The following IP addresses have a special meaning:</p> <ul style="list-style-type: none"> • 255.255.255.254—The Terminal Server will use the Remote IP Address set in the PPP settings for the serial port that this user is connecting to. • 255.255.255.255—When the User Service is PPP, the Terminal Server will allow the remote machine to specify its IP address (overriding the Remote IP Address configured in serial port PPP settings). When the User Service is SLIP, the Terminal Server will use the Remote IP Address set for the line (no negotiation). <p>Default: 255.255.255.254</p>
IPv4 Subnet Mask	<p>Used when the User Service is PPP or SLIP. Only used for IPv4. 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. The first 64 bits of the Interface must be zero.</p> <p>Field Format: 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> <ul style="list-style-type: none"> • PPP—MTU will be the maximum size of packets that the Terminal Server will negotiate for this port. This value is negotiated between the two ends of the link. • SLIP—MTU will be the maximum size of packets being sent by the Terminal Server. <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 for this user. Values are:</p> <ul style="list-style-type: none"> • None—RIP packets are neither received nor sent by the Terminal Server. • Send—RIP packets can only be sent by the Terminal Server. • Listen—RIP packets can only be received by the Terminal Server. • Send and Listen—RIP packets are sent and received by the Terminal Server. <p>Default: None</p>

Enable VJ Compression

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**.

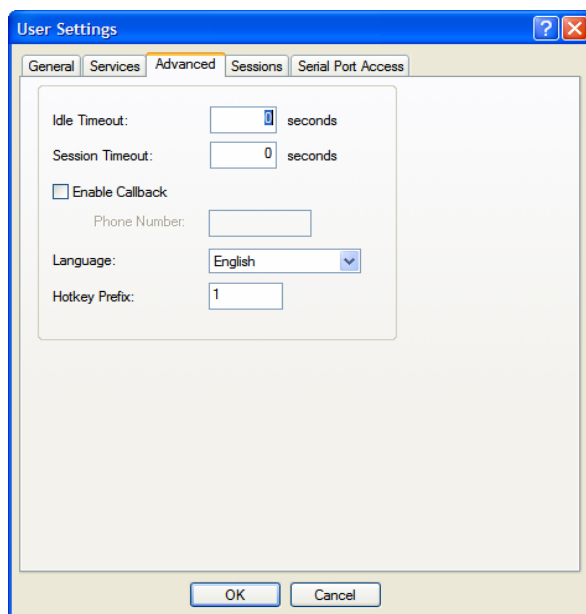
Default: Disabled

Advanced Tab

Overview

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.

Field Descriptions



Configure the following parameters:

Idle Timeout

The amount of time, in seconds, before the Terminal Server 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.

Range: 0-4294967

Default: 0

Session Timeout	<p>The amount of time, in seconds, before the Terminal Server 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 Terminal Server 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 Terminal Server 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 Terminal Server 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 Terminal Server 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 Menu, CLI, or WebManager. The Terminal Server supports one custom language that must be downloaded to the Terminal Server.</p> <p>Default: English</p> <p>See Language Support for more information about Custom Languages.</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 Terminal Server 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 Terminal Server. 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>

Sessions Tab

Overview

The Sessions tab is used to configure specific connections for users who are accessing the network through a Terminal Server serial port.

Functionality

Users who have successfully logged into the Terminal Server (**User Service** set to **DSprompt**) can start up to four login sessions on network hosts. These users start sessions through the Easy Port Menu 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 Terminal Server 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 Terminal Server. **Restricted** and **Menu** users can only start sessions predefined for them in their user configuration.

Field Descriptions

The screenshot shows the 'User Settings' dialog box with the 'Sessions' tab selected. The 'Predefined Outbound Sessions' section contains four session configurations:

- Session 1:** Protocol: Telnet, Host: None, TCP Port: 23. Includes a 'Telnet Settings...' button and an unchecked 'Connect Automatically' checkbox.
- Session 2:** Protocol: None, Host: None, TCP Port: 0. Includes an unchecked 'Connect Automatically' checkbox.
- Session 3:** Protocol: None, Host: None, TCP Port: 0. Includes an unchecked 'Connect Automatically' checkbox.
- Session 4:** Protocol: None, Host: None, TCP Port: 0. Includes an unchecked 'Connect Automatically' checkbox.

The dialog box has 'OK' and 'Cancel' buttons at the bottom.

Configure the following parameters:

Session 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 Terminal Server (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](#).
- **SSH**—For information on the SSH connection window, see [SSH Settings](#).
- **RLogin**—For information on the RLogin connection window, see [Rlogin Settings](#).

Default: None

Settings Button Click 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 Terminal Server.

Default: Disabled

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

Default: None

TCP Port The TCP port that the Terminal Server will use to connect to the host in this predefined session.

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

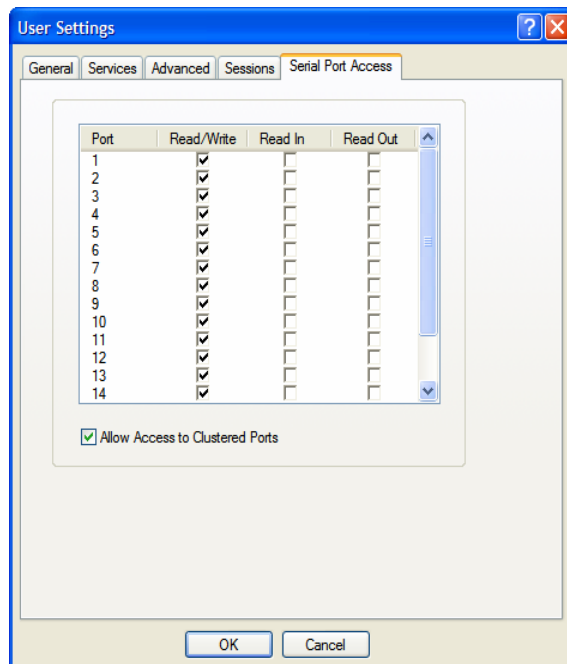
Serial Port Access Tab

Overview

The **Serial Port Access** tab controls the user's read/write access on any given Terminal Server 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 Profile* for the serial port settings.

Field Descriptions



Configure the following parameters:

Serial Port Access Specifies the user access rights to each Terminal Server 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

Allow Access to Clustered Ports

When enabled, allows the user access to Terminal Servers that have been configured in the clustering group.

Default: Enabled

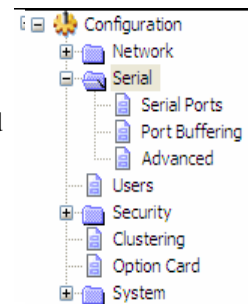
8

Configuring Serial Ports

Introduction

The Serial section is used to configure the serial ports on your Terminal Server. 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 Ports](#) for more information.
- **Port Buffering**—Configures serial port data buffering preferences. See [Port Buffering](#) for more information.
- **Advanced**—Configures those parameters that are applicable to specific environments. You will find modem and COMredirect configuration options, in addition to others, here. See [Advanced](#) for more information.



Serial Ports

Overview

Each Terminal Server serial port can be connected to serial device. 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.

Functionality

When you select the **Serial Ports** navigation option, you will see a list with the number of serial ports on your Terminal Server. As you configure the serial ports, the information for each serial port is displayed.

Serial Ports:

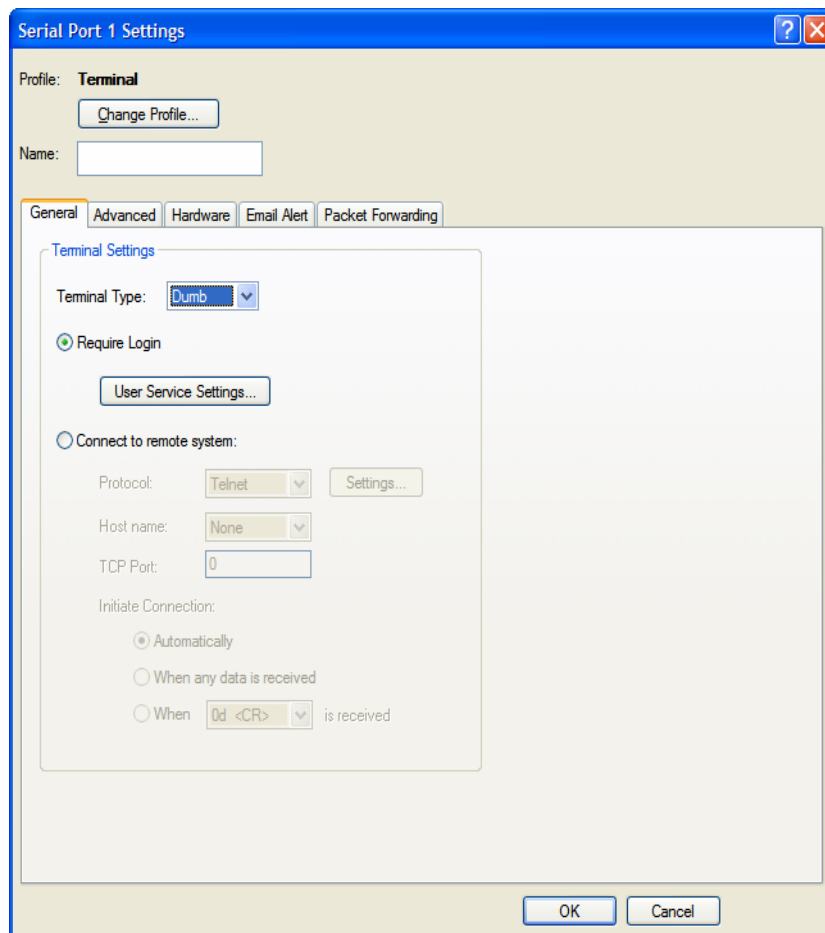
Enable		Name	Profile	Details
<input checked="" type="checkbox"/>	1	SUN Console Port	Console Management	Telnet - Listen: TCP 10001
<input checked="" type="checkbox"/>	2	Linux Console Port	Console Management	SSH - Listen: TCP 10002
<input type="checkbox"/>	3		Terminal	Login Required
<input type="checkbox"/>	4		PPP	

Edit... Copy...

To configure/change a serial port, click the **Edit** button.

Editing a Serial Port

In the **Serial Port Settings** window, click on a serial port and then click the **Edit** button, the following window is displayed:



The image shows a Windows-style dialog box titled "Serial Port 1 Settings". It has a blue title bar with a question mark icon and a close button. The main area is divided into several sections. At the top, it says "Profile: Terminal" with a "Change Profile..." button. Below that is a "Name:" text box. A tabbed interface is present with tabs for "General", "Advanced", "Hardware", "Email Alert", and "Packet Forwarding". The "General" tab is selected, showing "Terminal Settings". Inside this section, there is a "Terminal Type:" dropdown menu set to "Dumb". Below that is a "Require Login" radio button, which is selected, with a "User Service Settings..." button next to it. Underneath is a "Connect to remote system:" radio button, which is unselected. Below this are three fields: "Protocol:" with a dropdown set to "Telnet" and a "Settings..." button; "Host name:" with a dropdown set to "None"; and "TCP Port:" with a text box containing "0". At the bottom of the "Terminal Settings" section is the "Initiate Connection:" section with three radio buttons: "Automatically" (selected), "When any data is received", and "When 0d <CR> is received". The "0d <CR>" has a small dropdown arrow. At the very bottom of the dialog are "OK" and "Cancel" buttons.

Serial Port 1 Settings

Profile: **Terminal**
Change Profile...

Name:

General Advanced Hardware Email Alert Packet Forwarding

Terminal Settings

Terminal Type: Dumb

☒ Require Login
User Service Settings...

☐ Connect to remote system:

Protocol: Telnet Settings...

Host name: None

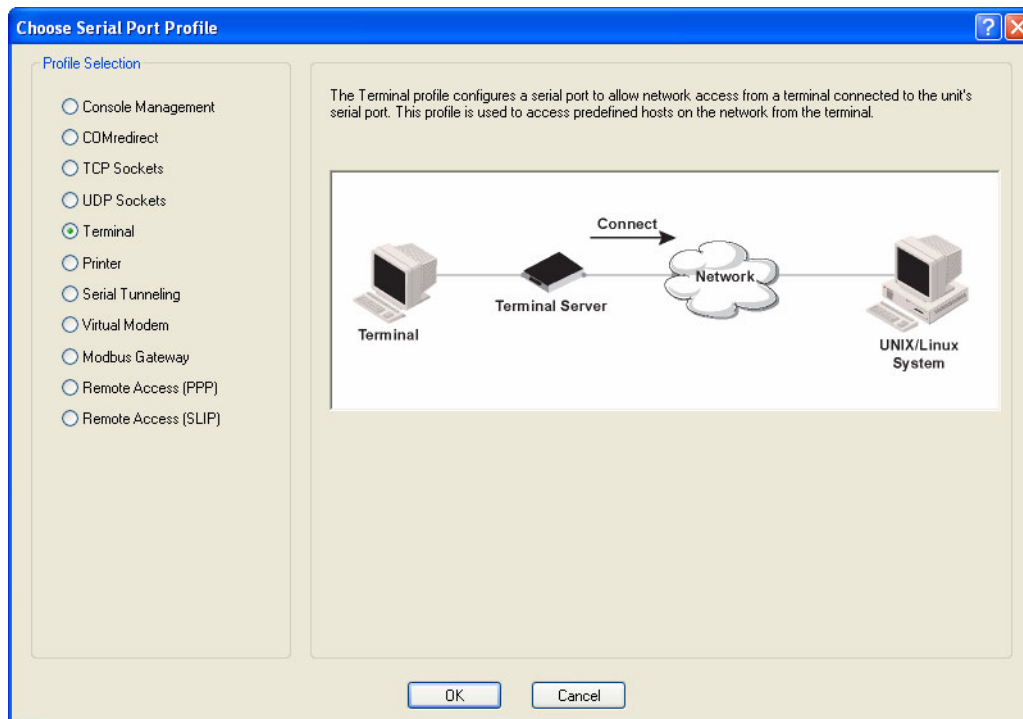
TCP Port: 0

Initiate Connection:

☒ Automatically
☐ When any data is received
☐ When 0d <CR> is received

OK Cancel

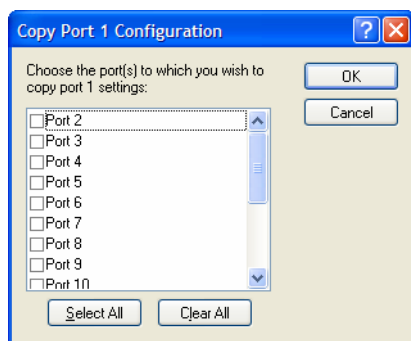
Click the **Change Profile** button to select a different serial port profile if you don't want the displayed profile:



As you select the different serial port profiles, a short description and a picture representing a typical application of the profile is displayed. When you have selected the appropriate profile for the serial port, click **OK** and those serial port profile configuration options will be displayed.

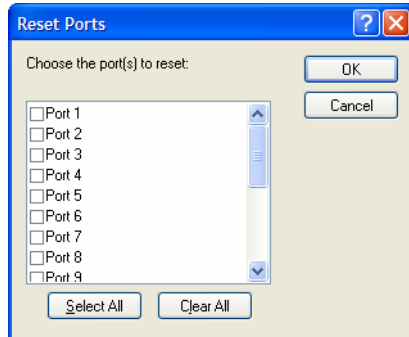
Copying a Serial Port

Once you configure a serial port, you can copy the serial port settings to other serial ports by selecting a serial port and then clicking the **Copy** button on the Serial Ports Settings window.



Resetting a Serial Port

When you change a serial port's configuration, you can download the configuration file to the Terminal Server and then reset a specific serial port(s) to see how you change affects the serial port's behavior. To reset a serial port, select **Tools, Reset, Serial Port(s)**.



Serial Port Profiles

Common Tabs

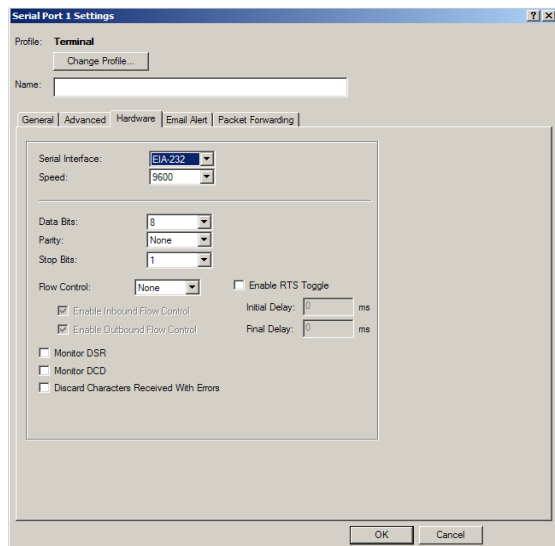
Overview

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

- **Hardware**—Configure the physical serial line parameters. See [Hardware Tab Field Descriptions](#).
- **Email Alert**—Configure email alerts for the serial line (these can also be configured globally for all lines under the **System** settings). See [Email Alert Tab Field Descriptions](#).
- **Packet Forwarding**—Configure data packet parameters. See [Packet Forwarding Tab Field Descriptions](#).
- **SSL/TLS**—Configure SSL/TLS encryption options for the serial port. See [SSL/TLS Settings Tab Field Descriptions](#).

Hardware Tab Field Descriptions

The **Hardware** tab configures the serial port hardware connection information. The window below shows a Secure Device Server 1-port model; your **Hardware** tab might display a subset of the parameters described.



Configure the following parameters:

- | | |
|-------------------------|--|
| Serial Interface | Specifies the type of serial line that is being used with the Terminal Server.
Data Options: EIA-232, EIA-422, or EIA-485. Secure Console Server/Secure Terminal Server models support only EIA-232.
Default: EIA-232 |
| Speed | 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 Terminal Server will calculate the closest baud rate available to the hardware. The exact baud rate calculated can be viewed in the Serial Ports statistics.
Range: 50-230400, custom supports 50-1843200
Default: 9600 |
| Data Bits | Specifies the number of bits in a transmitted character.
Default: 8 |
| Parity | 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.
Data Options: Even, Odd, Mark, Space, None
Default: None |
| Stop Bits | Specifies the number of stop bits that follow a byte.
Data Options: 1, 1.5, 2. 1.5 is only available on the 1-port and 2-port models, but not on the modem of the Secure Device Server1 Port model.
Default: 1 |

Duplex	Used with a EIA-485 serial interface, specify whether the serial port is Full Duplex (communication both ways at the same time) or Half Duplex (communication in one direction at a time). Default: Full
TX Driver Control	Used with a EIA-485 serial interface, if your application supports RTS (Request To Send), select this option. Otherwise, select Auto . Default: Auto
Flow Control	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 . Data Options: Soft, Hard, Both, None Default: None
Enable RTS Toggle	Configure the Toggle RTS Feature if your application needs for RTS to be raised during character transmission. 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. Final delay: configure the time (in ms) between the time of character transmission and when RTS is dropped. Initial delay range: 0-1000 ms Final delay range: 0-1000 ms Default: Off
Enable Inbound Flow Control	Determines if input flow control is to be used. Default: Enabled
Enable Outbound Flow Control	Determines if output flow control is to be used. Default: Enabled
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 Terminal Server detects a DSR signal, the line profile is started. If both Monitor DCD and Monitor DSR are enabled, both signals must be detected before the line 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 Terminal Server detects a DCD signal, the line profile is started. If both Monitor DCD and Monitor DSR are enabled, both signals must be detected before the line profile is started. Default: Disabled
Enable Line Termination	Used with EIA-422 and EIA-485 on Secure Device Server rack mount models, specifies whether or not the line is terminated. When termination is required, you need to terminate the line at both ends of the connection. 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

Discard Characters Received with Errors

When enabled, the Terminal Server will discard characters received with a parity or framing error.

Default: Disabled

Email Alert Tab Field Descriptions

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 Terminal Server might not be the same person who administers the serial device(s) attached to the Terminal Server 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

The screenshot shows the 'Email Alert' configuration window. At the top, there are tabs: 'General', 'Advanced', 'Hardware', 'Email Alert' (selected), and 'Packet Forwarding'. Below the tabs, the 'Enable Port Email Alert' checkbox is checked. The 'Level' section on the left has a tree view with 'Emergency' selected. The 'Addressing' section on the right has four fields: 'To:', 'Subject:', 'From:', and 'Reply To:'. Each field has a 'Use System Setting' checkbox checked.

Configure the following parameters:

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
The list above is in decreasing order of priority (Emergency being the highest and Debug being the lowest).

Default: Emergency

Use System Setting

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 will be the contents of the "from" field in the generated email.
Reply To	The email address to whom all replies to the email notification should go.

Packet Forwarding Tab Field Descriptions

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

General Advanced Hardware Email Alert **Packet Forwarding**

Define the conditions under which data received on the serial port will be forwarded to the network.

☒ Minimize Latency

☐ Optimize Network Throughput

☐ Prevent Message Fragmentation

Delay Between Messages: ms

☐ Custom Packet Forwarding

☒ Packet Definition

Packet Size:

Idle Time:

Force Transmit Timer:

☐ End Trigger1 Character:

☐ End Trigger2 Character:

☐ Frame Definition

SOF1 Character:

☐ SOF2 Character:

☒ Transmit SOF Character(s):

EOF1 Character:

☐ EOF2 Character:

Trigger Forwarding Rule:

Configure the following parameters:

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	<p>The minimum time, in milliseconds, between messages that must pass before the data is forwarded by the Terminal Server.</p> <p>Range: 0-65535</p> <p>Default: 250 ms</p>
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>
Enable Trigger1 Character	<p>When enabled, specifies the character that when received will define when the packet is ready for transmission. The transmission of the packet is based on the Trigger Forwarding Rule.</p> <p>Range: Hex 0-FF</p> <p>Default: 0</p>
Enable 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 Terminal Server waits for another End Trigger1 character to start the End Trigger1/End Trigger2 character sequence).</p> <p>Range: Hex 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: Hex 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 Terminal Server waits for another SOF1 character to start the SOF1/SOF2 character sequence).</p> <p>Range: Hex 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 transmission of the frame is based on the Trigger Forwarding Rule.</p> <p>Range: Hex 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 Terminal Server waits for another EOF1 character to start the EOF1/EOF2 character sequence), which defines when the frame is ready to be transmitted. The transmission of the frame is based on the Trigger Forwarding Rule.</p> <p>Range: Hex 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 Tab Field Descriptions

You can create an encrypted connection using SSL/TLS for any serial port profile that accesses the Terminal Server from the network. 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 Terminal Server 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 15, 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: See *Keys and Certificates* for information about SSL/TLS support documents.

Configure the following parameters:

- | | |
|----------------------------|---|
| Enable SSL/TLS | Activates the SSL/TLS settings for the serial port.
Default: Disabled |
| Use global settings | Uses the SSL/TLS settings configured in the Security section for the serial port.
Default: Enabled |
| SSL/TLS Version | Specify whether you want to use: <ul style="list-style-type: none"> • Any—The Terminal Server will try a TLSv1 connection first. If that fails, it will try an SSLv3 connection. If that fails, it will try all other connection methods. • 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. Default: Any |
| SSL/TLS Type | Specify whether the Terminal Server serial port will act as an SSL/TLS client or server.
Default: Client |
| Cipher Suite Button | Click this button to specify SSL/TLS connection ciphers.
See <i>Cipher Suite Field Descriptions</i> for more information. |

Validate Peer Certificate

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 Terminal Server.

Default: Disabled

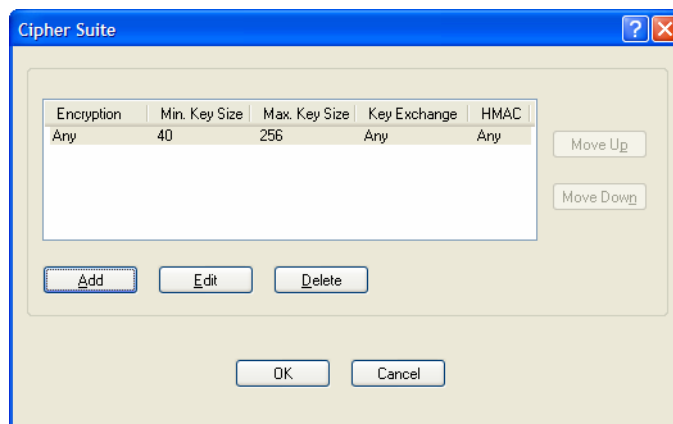
Validation Criteria Button

Click this button to create peer certificate validation criteria that must be met for a valid SSL/TLS connection.

See [Validation Criteria Field Descriptions](#) for more information.

Cipher Suite Field Descriptions

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



The following buttons are available on this window:

Add Button

Adds a cipher to the cipher list.

Edit Button

Edits a cipher in the cipher list.

Delete Button

Deletes a cipher from the cipher list.

Move Up Button

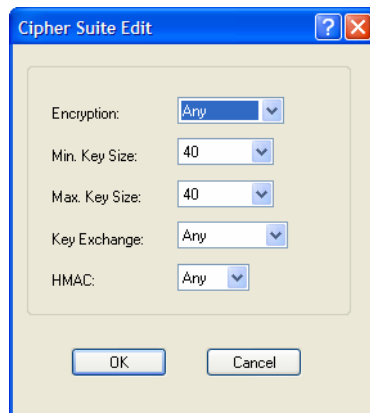
Moves a cipher up in preference in the cipher list.

Move Down Button

Moves a cipher down in preference in the cipher list.

Adding/Editing a Cipher Suite

To see a list of valid cipher suite combinations, see *Appendix 15, SSL/TLS Ciphers*.



Configure the following 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

The type of key to exchange for the encryption format.

Data Options:

- **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.

Default: Any

HMAC

Select the key-hashing for message authentication method for your encryption type.

Data Options:

- Any
- MD5
- SHA1
- SHA256
- SHA384

Default: Any

Validation Criteria Field Descriptions

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.

Configure the following parameters:

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

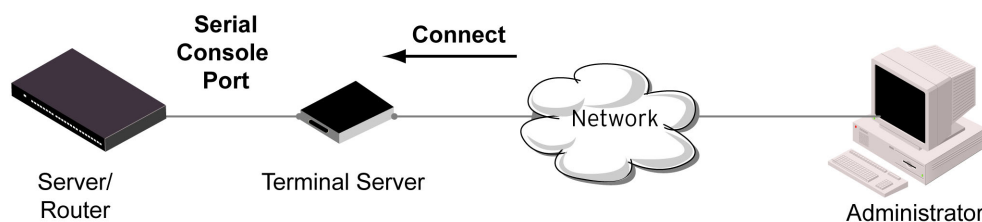
Console Management Profile

Overview

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

Functionality

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



General Tab Field Descriptions

The **Console Management General** tab configures how the serial port will be accessed by the user through the network.

Configure the following parameters:

Protocol	<p>Specify the connection method that users will use to communicate with a serial device connected to the Terminal Server 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 Terminal Server will listen on for incoming TCP connections.</p> <p>Note: if more then one serial port has the same TCP port number assignment, this would create a hunt group senario. 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 Terminal Server's IP address and port number.</p> <p>Default: Disabled</p>
IP Address	<p>Users can access serial devices connected to the Terminal Server 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>

Advanced Tab Field Descriptions

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

Configure the following parameters:

- | | |
|---|--|
| Authenticate User | Enables/disables login/password authentication for users connecting from the network.
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 determines how long the Terminal Server will wait during inactivity 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 Administrator Console (SAC) support | When enabled, a user can access SAC (the interface of the Microsoft Emergency Management Systems utility) through EasyPort Web when the Terminal Server's serial port is connected to a Microsoft Server 2003 or Microsoft Server 2008 host.
Default: Disabled |

Multisessions	<p>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. Each user monitoring the port can be assigned different privileges to this port.</p> <p>Range: Dependent on model:</p> <ul style="list-style-type: none"> • 1-port: 0-3 • 2-port: (4 x #-of-ports) -1 • Secure Terminal Servers/Secure Device Servers 4+ ports: (2 x #-of-ports) -1 • Secure Console Servers 4+ ports: (2 x (#-of-ports + 1)) -1 <p>Default: 0</p>
Idle Timeout	<p>Use this timer to close a connection because of inactivity. When the Idle Timeout expires, the Terminal Server 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>
Break Handling	<p>Specifies how a break is interpreted.</p> <p>Data Range:</p> <ul style="list-style-type: none"> • None—The Terminal Server ignores the break key completely and it is not passed through to the host. • Local—The Terminal Server 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 Terminal Server 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 -ignbrk and brkintr are set). <p>Default: None</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 Secure Terminal Server, 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>Range: 0-127 alpha-numeric characters. The decimal numbers within the brackets must be 3 digits long (example 003 not 3). To enter the < (less than symbol) precede the symbol with a \ (backslash symbol).</p> <ul style="list-style-type: none"> • 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 console port 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 Terminal Server will wait to establish a connection to a remote modem. Range: 1-99 Default: 45 seconds
Dial Retry	The number of times the Terminal Server 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.

COMredirect Profile

Overview

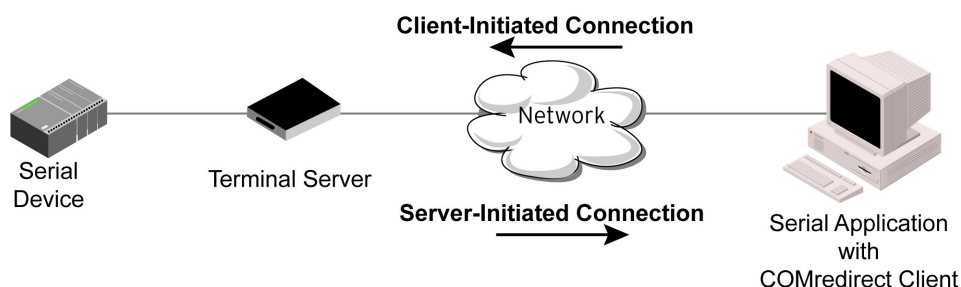
COMredirect is especially useful when you want to improve data security, as you can enable an SSL/TLS connection between the COMredirect host port and the Terminal Server. COMredirect is a COM Port redirector that is supplied with the Terminal Server. COMredirect can be installed as a client on a Workstation or Server and supports a variety of operating systems. It, in conjunction with the Terminal Server, COMredirect emulates a local serial port (COM port), to the application, to provide connectivity to a remote serial device over the network. The COMredirect profile operates in conjunction with the COMredirect software.

Functionality

COMredirect is a COM port redirector utility for the Terminal Server. It can be run in two modes (these modes will be set on the client software when it is configured):

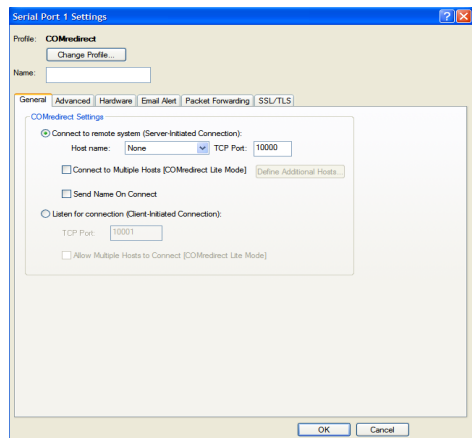
- **COMredirect Full mode**—This mode allows complete device control and operates as if the device was directly connected to the Workstation/Server's local serial port. It provides a complete COM port interface between the attached serial device and the network. All serial controls, baud rate control, etc., are sent to the Terminal Server and replicated on its associated serial port.
- **COMredirect 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 Terminal Server.

See the *COMredirect User Guide* for more details about the COMredirect client software.



General Tab Field Descriptions

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



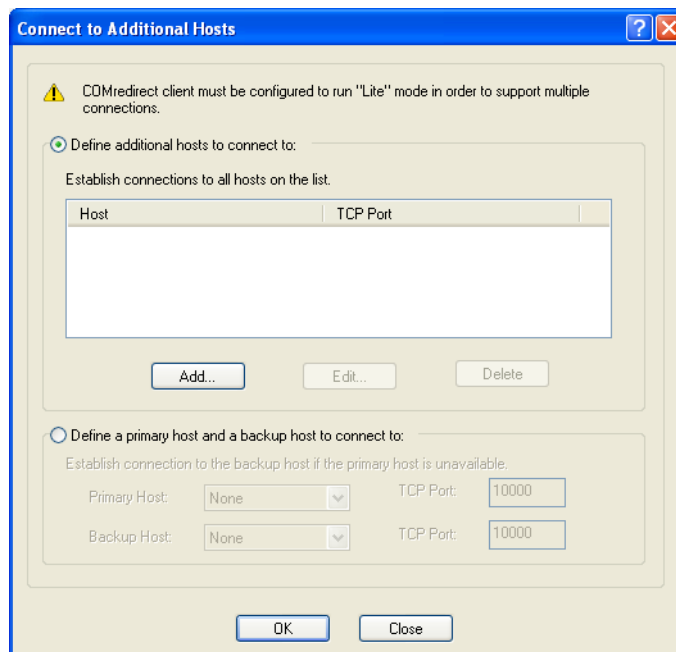
Configure the following parameters:

- | | |
|---------------------------------------|---|
| Connect to remote system | When enabled, the Terminal Server initiates communication to the COMredirect client.
Default: Enabled |
| Host Name | The configured host that the Terminal Server will connect to (must be running COMredirect).
Default: None |
| TCP Port | The TCP Port that the Terminal Server will use to communicate through to the COMredirect client.
Default: 10001 for serial port 1, then increments by one for each serial port |
| HTTP Tunnel | Specify the HTTP Tunnel that the Terminal Server will use for this connection. |
| Connect to Multiple Hosts | When enabled, the Terminal Server will establish a connection to multiple clients (Hosts). When using the multiple hosts feature, all COMredirect clients must be running in Lite mode.
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 an Internal IP Address in a DNS network). The Terminal Server can also be accessed by it's IP address and port number.
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 | Click 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 Adding/Editing Additional COMredirect Hosts for more information. |
| Listen for Connection | When enabled, the Terminal Server will wait for connections to be initiated by the COMredirect Client.
Default: Disabled |

TCP Port	The TCP Port that the Terminal Server will use to communicate through to the COMredirect client. Default: 10001 for serial port 1, then increments by one for each serial port
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 COMredirect in Lite mode. Default: Disabled

Adding/Editing Additional COMredirect Hosts

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



Configure the following parameters:

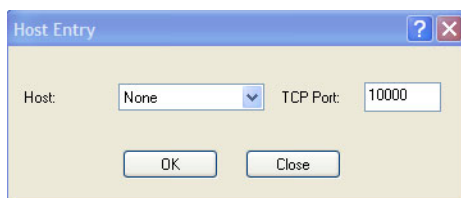
Define additional hosts to connect to	When this option is enabled, you can define up to 49 hosts that the serial device connected to this serial port will attempt communicate to. With this mode of operation, the Terminal Server will connect to multiple hosts simultaneously. Default: Enabled
Add Button	Click the Add button to add a host to the list of hosts that will be receiving communication from the serial device connected to the Terminal Server. See Adding/Editing a Multihost Entry for more information.
Edit Button	Highlight an existing host and click the Edit button to edit a host in the list of hosts that will be receiving communication from the serial device connected to the Terminal Server.
Delete Button	Highlight an existing host and click the Edit button to edit a host in the list of hosts that will be receiving communication from the serial device connected to the Terminal Server.

Define a primary host and backup...	<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 Terminal Server loses communication to the primary host. The Terminal Server will first establish a connection to the primary host. Should the connection to the primary host be lost (or never established), the Terminal Server will establish a connection the backup host. Once connected to the backup, the Terminal Server 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 preconfigured host that the serial device will communicate to through the Terminal Server.</p> <p>Default: None</p>
TCP Port	<p>Specify the TCP port that the Terminal Server 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 Terminal Server if the Terminal Server cannot communicate with the Primary Host.</p> <p>Default: None</p>
TCP Port	<p>Specify the TCP port that the Terminal Server will use to communicate to the Backup Host.</p> <p>Default: 10000</p>

Adding/Editing a Multihost Entry

When you click the **Add** or **Edit** button, the Host Entry window appears. The hosts in the multihost 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.

Configure the following parameters.

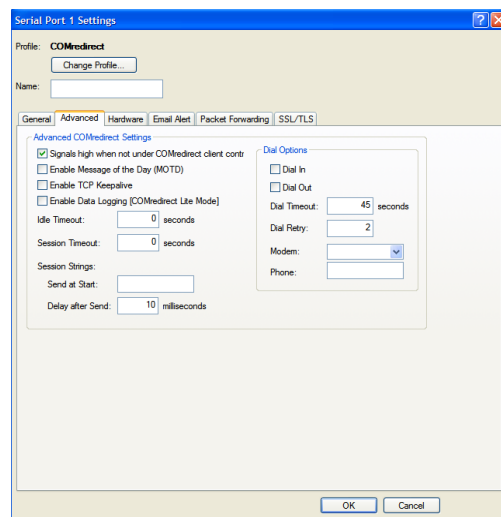


The image shows a 'Host Entry' dialog box with a title bar containing a question mark and a close button. Inside the dialog, there are two fields: 'Host' and 'TCP Port'. The 'Host' field is a dropdown menu currently showing 'None'. The 'TCP Port' field is a text box containing the value '10000'. At the bottom of the dialog, there are two buttons: 'OK' and 'Close'.

Host Name	Specify the preconfigured host that will be in the multihost list. Default: None
TCP Port	Specify the TCP port that the Terminal Server will use to communicate to the Primary Host . Default: 10000 + serial port number - 1 (so serial port 47 defaults to 10046)

Advanced Tab Field Descriptions

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



Configure the following parameters:

Signals high when...	<p>This option has the following impact based on the state of the COMredirect connection:</p> <ul style="list-style-type: none"> ● COMredirect Lite Mode—When enabled, the EIA-232 signals remain active before, during, and after the COMredirect connection is established. When disabled, the EIA-232 signals remain inactive during and after the COMredirect connection is established. ● COMredirect Full Mode—When enabled, the EIA-232 signals remain active before and after the COMredirect connection and the COMredirect client will control the state of the signals during the established COMredirect connection. When disabled, the EIA-232 signals remain inactive before and after the COMredirect connection and the COMredirect client will control the state of the signals during the established COMredirect connection. <p>Default: Enabled</p>
Enable Message of the Day (MOTD)	<p>Enables/disables the display of the message of the day.</p> <p>Default: Disabled</p>

Enable TCP Keepalive	<p>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.</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 determines how long the Terminal Server will wait during inactivity 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.</p> <p>Default: Disabled</p>
Enable Data Logging [COMredirect Lite Mode]	<p>When enabled, serial data will be buffered if the TCP connection is lost. When the TCP connection is re-established, the buffered serial data will be sent to its destination. Only valid in COMredirect Lite Mode. Not valid when using COMredirect in Full mode.</p> <p>The minimum data buffer size for all models is 1K. The maximum data buffer size is 2000 KB for the TS, all other models are 4000 KB. If the data buffer is filled, incoming serial data will overwrite the oldest data.</p> <p>Values: 1-2000 KB (TS) - Default is 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 Terminal Server causes all buffered data to be lost.</p> <p>Some profile features are not compatible with Data Logging. See Appendix H, Data Logging for the complete list.</p> <p>To change the default buffer size see Advanced Serial Settings Tab.</p>
Idle Timeout	<p>Use this timer to close a connection because of inactivity. When the Idle Timeout expires, the Terminal Server 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 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 Terminal Server 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>Range: 0-127 alpha-numeric characters</p> <p>Range: Hexadecimal 0-FF</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 or terminated. <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 Terminal Server will wait to establish a connection to a remote modem. Range: 1-99 Default: 45 seconds
Dial Retry	The number of times the Terminal Server 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.

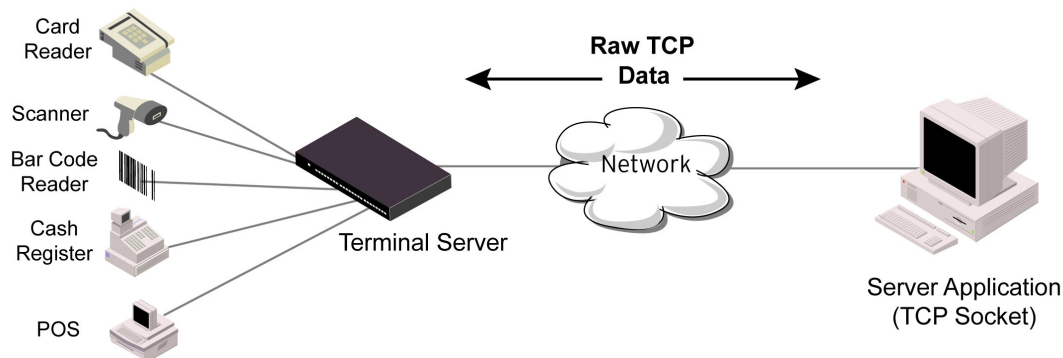
TCP Sockets Profile

Overview

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.

Functionality

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 Terminal Server.



General Tab Field Descriptions

Serial Port 1 Settings

Profile: **TCP Sockets**

Name:

General | Advanced | Hardware | Email Alert | Packet Forwarding | SSL/TLS

TCP Socket Settings

☒ Listen for connection:

TCP Port:

☐ Allow Multiple Hosts to Connect

☐ Enable IP Aliasing

IP Address:

☐ Connect to:

Host name: TCP Port:

☐ Connect to Multiple Hosts

Initiate Connection:

☒ Automatically

☐ When any data is received

☐ When is received

☐ Send Name On Connect

☐ Permit Connections in Both Directions

OK Cancel

Configure the following parameters:

Listen for Connection

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

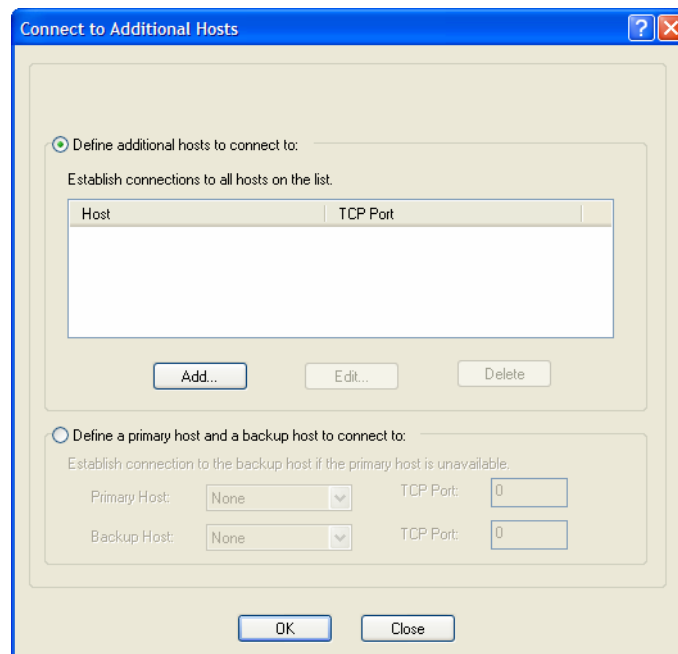
Default: Enabled

TCP Port	<p>The TCP port that the Terminal Server will use to listen for incoming connections.</p> <p>Default: 10000 plus the serial port number, so serial port 5 would have a default of 10005</p>
HTTP Tunnel	<p>Specific the HTTP tunnel to be used for this connection.</p>
Allow Multiple Hosts to Connect	<p>When enabled, the Terminal server will establish a connection to multiple clients (Hosts). When using the multiple hosts feature, all COMredirect clients must be running in Lite Mode.</p> <p>Default: Disabled</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 an Internal IP Address in a DNS network). The Terminal Server can also be accessed by it's IP address and port number.</p> <p>Default: Disabled</p>
IP Address	<p>Users can access serial devices connected to the Terminal Server 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>
Connect To	<p>When enabled, the Terminal Server initiates communication to the Workstation/Server.</p> <p>Default: Disabled</p>
Host Name	<p>The name (resolvable via DNS) or IP address of the configured host the Terminal Server will connect to.</p>
TCP Port	<p>The TCP Port that the Terminal Server will use to communicate to the client.</p> <p>Default: 0</p>
Connect to Multiple Hosts	<p>When enabled, allows a serial device connected to this serial port to communicate to multiple hosts.</p> <p>Default: Disabled</p>
Define Additional Hosts Button	<p>Click 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.</p>
Initiate Connection Automatically	<p>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 Terminal Server will initiate the session immediately after being powered up.</p> <p>Default: Enabled</p>
Initiate Connection When any data is received	<p>Initiates a connection to the specified host when any data is received on the serial port.</p> <p>Default: Disabled</p>
Initiate Connection When <hex value> is received	<p>Initiates a connection to the specified host only when the specified character is received on the serial port.</p> <p>Default: Disabled</p>

- 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, you can select box checkbox options "listen for connection" and "connect to".
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.



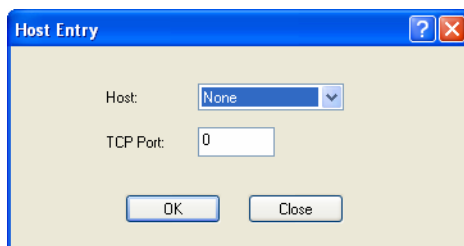
Configure the following parameters:

- 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 Terminal Server will connect to multiple hosts simultaneously.
Default: Enabled
- Add Button** Click the **Add** button to add a host to the list of hosts that will be receiving communication from the serial device connected to the Terminal Server.
- Edit Button** Highlight an existing host and click the **Edit** button to edit a host in the list of hosts that will be receiving communication from the serial device connected to the Terminal Server.
- Delete Button** Click the **Delete** button to delete a host to the list of hosts that will be receiving communication from the serial device connected to the Terminal Server.

Define a primary host and backup...	<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 Terminal Server loses communication to the primary host. The Terminal Server will first establish a connection to the primary host. Should the connection to the primary host be lost (or never established), the Terminal Server will establish a connection the backup host. Once connected to the backup, the Terminal Server 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 preconfigured host that the serial device will communicate to through the Terminal Server.</p> <p>Default: None</p>
TCP Port	<p>Specify the TCP port that the Terminal Server 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 Terminal Server if the Terminal Server cannot communicate with the Primary Host.</p> <p>Default: None</p>
TCP Port	<p>Specify the TCP port that the Terminal Server will use to communicate to the Backup Host.</p> <p>Default: 10000</p>

Adding/Editing a Multihost Entry

When you click the **Add** or **Edit** button, the Host Entry window appears. The hosts in the multihost 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 Name	<p>Specify the preconfigured host that will be in the multihost list.</p> <p>Default: None</p>
TCP Port	<p>Specify the TCP port that the Terminal Server will use to communicate to the Host.</p> <p>Default: 0</p>

Advanced Tab Field Descriptions

Configure the following parameters:

- Authenticate User** Enables/disables login/password authentication for users connecting from the network.
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 determines how long the Terminal Server will wait during inactivity 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 Data Logging** When enabled, serial data will be buffered if the TCP connection is lost. When the TCP connection is re-established, the buffered serial data will be sent to its destination.
 The minimum data buffer size for all models is 1K. The maximum data buffer size is 2000 KB for the TS, all other models are 4000 KB. If the data buffer is filled, incoming serial data will overwrite the oldest data.
Values: 1-2000 KB (TS) - Default is 4 KB
Values: 1-4000 KB (all other models) - Default 256 KB
Default: Disabled
Note: A kill line or a reboot of the Terminal Server causes all buffered data to be lost.
 Some profile features are not compatible with Data Logging. See [Appendix H, Data Logging](#) for the complete list.
 To change the default buffer size see [Advanced Serial Settings Tab](#).

Idle Timeout	<p>Use this timer to close a connection because of inactivity. When the Idle Timeout expires, the Terminal Server 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>
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>
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 Secure Terminal Server, 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 multihost is configured, this string will only be sent to the serial device when the profile is configured as a listen mode connection and after all multihost connections are terminated. 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.• Default: 10 ms
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 Terminal Server 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 Terminal Server will attempt to re-establish a connection with a remote modem.</p> <p>Range: 0-99</p> <p>Default: 2</p>
Modem	<p>The name of the predefined modem that is used on this line.</p>
Phone	<p>The phone number to use when Dial Out is enabled.</p>

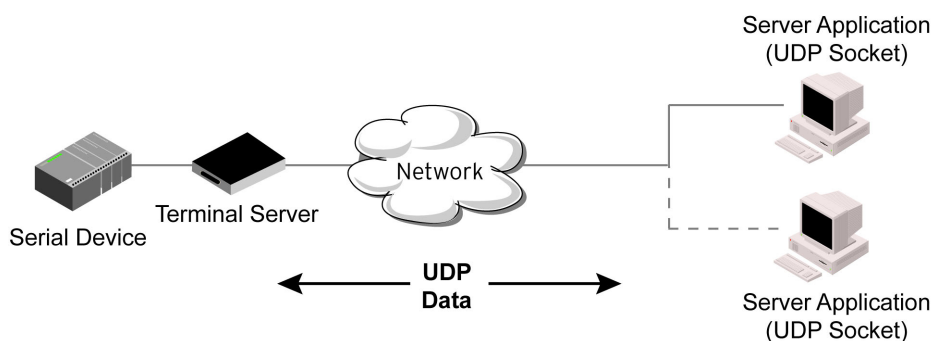
UDP Sockets Profile

Overview

The UDP profile configures a serial port to broadcast UDP data to systems and/or receive UDP data from systems.

Functionality

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 Terminal Server will accept UDP packets from any source address

Sample **UDP Sockets** configuration screen.

	Direction	Start IP Address	End IP Address	UDP Port
1	Both	0.0.0.0	0.0.0.0	Auto Learn
2	Disabled	0.0.0.0	0.0.0.0	Auto Learn
3	Disabled	0.0.0.0	0.0.0.0	Auto Learn
4	Disabled	0.0.0.0	0.0.0.0	Auto Learn

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 then 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 Terminal Server 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.

	Direction	Start IP Address	End IP Address	UDP Port
1	Both	172.16.1.1	172.16.1.25	33001
2	LAN to Serial	172.16.1.20	172.16.1.50	33010
3	Serial to LAN	172.16.1.75	172.16.1.80	33009
4	Disabled		0.0.0.0	0

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

- **UDP Entry 1**
All hosts that have an IP address that falls within the range of **172.16.1.1** to **172.16.1.25** 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 **Port 33001**. The Terminal Server will listen for data on the port value configured in the **Listen for connections on UDP port** parameter.
- **UDP Entry 2**
All UDP data received from hosts that have an IP address that falls within the range of **172.16.1.20** to **172.16.1.50** and **Port 33010** will be sent to the serial device. The Terminal Server will not send any data received on its serial port.
- **UDP Entry 3**
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 **Port 33009** will receive UDP data from the serial device. The Terminal Server will listen for messages on the port value configured in the **Listen for connections on UDP port** parameter. No UDP data will be sent to the serial device.
- **UDP Entry 4**
This entry is disabled since **Direction** is set to **Disabled**.

General Tab Field Descriptions

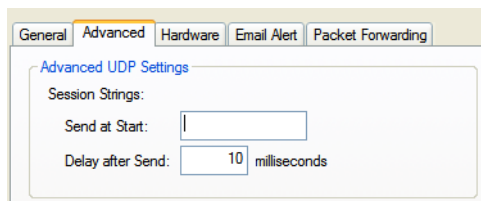
UDP Socket Settings				
Listen for connections on UDP port: 10001				
Host Range				
	Direction	Start IP Address	End IP Address	UDP Port
1	Both		0.0.0.0	Auto Learn
2	Disabled		0.0.0.0	Auto Learn
3	Disabled		0.0.0.0	Auto Learn
4	Disabled		0.0.0.0	Auto Learn

Configure the following parameters:

Listen for connections on UDP port	The Terminal Server will listen for UDP packets on the specified port. Default: 1000+<port-number> (for example, 10001 for serial port 1)
Direction	The direction in which information is received or relayed: <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. Default: Both for UDP 1 and Disabled for all other UDP ranges
Start IP Address	The first host IP address in the range of IP addresses (for IPv4 or IPv6) that the Secure Terminal Server will listen for messages from and/or send messages to. Field Format: IPv4 or IPv6 address
End IP Address	The last host IP address in the range of IP addresses (for IPv4, not supported for IPv6) that the Secure Terminal Server will listen for messages from and/or send messages to. Field Format: IPv4 address
UDP Port	Determines how the Terminal Server's UDP port that will send/receive UDP messages is defined: <ul style="list-style-type: none"> • Auto Learn—The Terminal Server 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 Terminal Server will receive messages from any port sending UDP packets. Applicable when Direction is set to LAN to Serial. • Port—The port that the Terminal Server will use to relay messages to servers/hosts. This option works with any Direction except Disabled. The Terminal Server will listen for UDP packets on the port configured by the Listen for connections on UDP port parameter. Default: Auto Learn
Port	The UDP port to use. Default: 0 (zero)

HTTP Tunnel Specify the HTTP Tunnel that the Terminal Server will use for this connection.

Advanced Tab Field Descriptions



This profile can be configured for users:

- Session Strings** Controls the sending of ASCII strings to serial devices at session start as follows;
- Send at Start**—If configured, this string will be sent to the serial device on power-up of the Terminal Server 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 or terminated.
Default: 10 ms

Terminal Profile

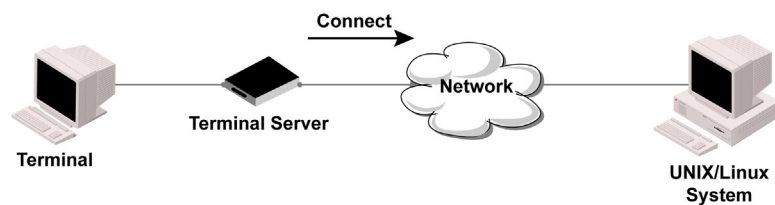
Overview

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

Functionality

This profile can be configured for users:

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



General Tab Field Descriptions

General Advanced Hardware Email Alert Packet Forwarding

Terminal Settings

Terminal Type: Dumb

☒ Require Login

User Service Settings...

☐ Connect to remote system:

Protocol: Telnet Settings...

Host name: None

TCP Port: 0

Initiate Connection:

☒ Automatically

☐ When any data is received

☐ When 0d <CR> is received

Configure the following 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 Terminal Server 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 Terminal Server 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 • TACACS+/RADIUS for externally authenticated users where the target host is passed to the Terminal Server <p>See User Service Settings for field descriptions of the various User Service Settings.</p>
Connect to Remote System	<p>When the serial port is started, the Terminal Server will initiate a connection to the specified host using the specified protocol. With this option, user authentication will not be performed by the Terminal Server.</p> <p>Default: Disabled</p>
Protocol	<p>Specify the protocol that will be used to connect to the specified host.</p> <p>Data Options: Telnet, SSH, Rlogin</p> <p>Default: Telnet</p>
Settings Button	<p>Click this button to define the settings for the protocol that will be used to connect the user to the specified host.</p>
Host Name	<p>The name (resolvable via DNS) or IP address of the configured host the Terminal Server will connect to.</p>
TCP Port	<p>The TCP Port that the Terminal Server will use to connect to the host.</p> <p>Default: Telnet-23, SSH-22, Rlogin-513</p>
Automatically	<p>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 Terminal Server will initiate the session immediately after being powered up.</p> <p>Default: Enabled</p>

When any data is received Initiates a connection to the specified host when any data is received on the serial port.

Default: Disabled

When <hex value> is received Initiates a connection to the specified host only when the specified character is received on the serial port.

Default: Disabled

Advanced Tab Field Descriptions

Serial Port 1 Settings

Profile: **Terminal**

Name:

General | **Advanced** | Hardware | Email Alert | Packet Forwarding

Advanced Terminal Settings

☐ Enable Message of the Day (MOTD)
☐ Reset Terminal on disconnect
☐ Allow Port Locking

Hotkey Prefix:
 Idle Timeout: seconds
 Session Timeout: seconds

Session Strings:
 Send at Start:
 Delay after Send: milliseconds

Dial Options
☐ Dial In
☐ Dial Out
 Dial Timeout: seconds
 Dial Retry:
 Modem:
 Phone:

Configure the following 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 Terminal Server 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: Hex 01 (Ctrl-a, ^a)</p>
Idle Timeout	<p>Use this timer to close a connection because of inactivity. When the Idle Timeout expires, the Terminal Server 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 Secure Terminal Server, 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>Range: 0-127 alpha-numeric characters. The decimal numbers within the brackets must be 3 digits long (example 003 not 3). To enter the < (less than symbol) precede the symbol with a \ (backslash symbol).</p> <ul style="list-style-type: none"> • 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 Timeout	<p>The number of seconds the Terminal Server 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 Terminal Server 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

User Service Settings

Login Settings

These settings apply to users who are accessing the network from a terminal connected to the Terminal Server'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 Terminal Server by a RADIUS or TACACS+ server when those authentication methods are being used).

Configure the following parameters:

- | | |
|---------------------------------|--|
| 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: Menu, 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. When the Terminal Server initiates a Telnet connection to a host, it is acting as a Telnet client.

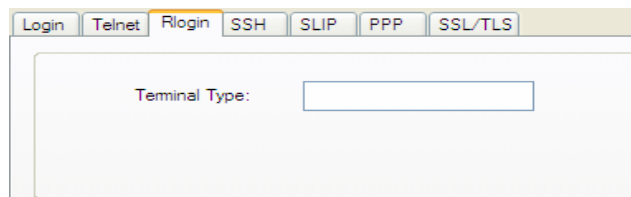
Configure the following parameters:

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

Enable 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.

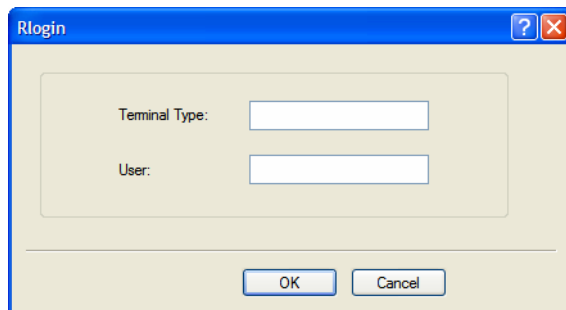


The screenshot shows a configuration window with tabs for Login, Telnet, Rlogin, SSH, SLIP, PPP, and SSL/TLS. The Rlogin tab is selected. Below the tabs is a large text area labeled "Terminal Type:" with an empty input box next to it.

Configure the following parameter:

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.

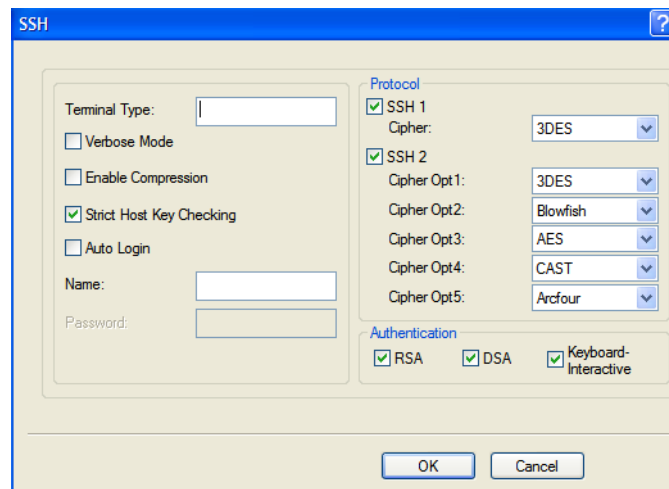


Configure the following parameters:

- 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 Settings

The SSH settings apply when the **User Service** is set to **SSH** or the Terminal profile specifies an **SSH** connection to a host. When the Terminal Server initiates a SSH connection to a host, it is acting as an SSH client.



Configure the following parameters:

- 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	<p>When enabled, a host public key (for each host you wish to ssh to) must be downloaded into the Terminal Server.</p> <p>Default: Enabled</p>
Auto Login	<p>When enabled, creates an automatic SSH login, using the Name and Password values.</p> <p>Default: Disabled</p>
Name	<p>The name of the user logging into the SSH session.</p> <p>Field Format: Up to 20 alphanumeric characters, excluding spaces</p>
Password	<p>The user's password when Auto Login is enabled.</p> <p>Field Format: Up to 20 alphanumeric characters, excluding spaces</p>
SSH1	<p>When enabled, selects an SSH version 1 connection.</p> <p>Default: Enabled</p>
SSH1 Cipher	<p>Select the encryption method (cipher) that you want to use for your SSH version 1 connection:</p> <p>Data Options:</p> <ul style="list-style-type: none">• 3DES• Blowfish <p>Default: 3DES</p>
SSH2	<p>When enabled, selects an SSH version 2 connection. If both SSH 1 and SSH 2 are selected, the Terminal Server 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.</p> <p>Default: Enabled</p>
SSH2 Ciphers Opt1-8	<p>Select the order of negotiation for the encryption method (ciphers) that the Terminal Server will use for the SSH version 2 connection:</p> <p>Data Options:</p> <ul style="list-style-type: none">• ChaCha20-Poly1305• AES-CTR• AES-GCM• AES-CBC• 3DES• Blowfish• CAST• ArcFour
RSA	<p>When enabled, an authentication method used by SSH version 1 and 2. Use RSA authentication for the SSH session.</p> <p>Default: Enabled</p>
DSA	<p>When enabled, an authentication method used by SSH version 2. Use DSA authentication for the SSH session.</p> <p>Default: Enabled</p>
Keyboard Authentication	<p>When enabled, the user types in a password for authentication.</p> <p>Default: Enabled</p>

SLIP Settings

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

The screenshot shows a configuration window with tabs for Login, Telnet, Rlogin, SSH, SLIP, PPP, and SSL/TLS. The SLIP tab is active. It contains the following fields:

- Local IP Address: 0 . 0 . 0 . 0
- Remote IP Address: 0 . 0 . 0 . 0
- Subnet Mask: 0 . 0 . 0 . 0
- MTU: 256
- Routing: None (dropdown menu)
- ☒ VJ Compression

Configure the following parameters:

- Local IP Address** The IPv4 address of the Terminal Server 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 Terminal Server'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 Terminal Server. If your user is authenticated by the Terminal Server, 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 Terminal Server 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 Terminal Server 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 Terminal Server. Enter a value between 256 and 1500 bytes; for example, 512. The default value is **256**. If your user is authenticated by the Terminal Server, 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 Terminal Server will use the value in the RADIUS file in preference to the value configured here.
Default: 256
- Routing** Determines the routing mode (RIP, Routing Information Protocol) used on the **SLIP** interface as one of the following options:
- **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.
- This is the same function as the **Framed-Routing** attribute for RADIUS authenticated users.
Default: None

VJ Compression

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.

If your user is authenticated by the Terminal Server, 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 *and* the RADIUS parameter **Framed-Compression** is set in the RADIUS file, the Terminal Server will use the value in the RADIUS file in preference to the value configured here.

Default: Enabled

PPP Settings

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

Configure the following parameters:

IPv4 Local IP Address

The IPV4 IP address of the Terminal Server 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 Terminal Server'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 Terminal Server. If you set the PPP parameter IP Address Negotiation to On, the Terminal Server 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 *and* the RADIUS parameter **Framed-Address** is set in the RADIUS file, the Terminal Server 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 Terminal Server 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 Terminal Server will use the value in the RADIUS file in preference to the value configured here.

IPv6 Local Interface Identifier	<p>The local IPv6 interface identifier of the Terminal Server 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 Terminal Server'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 Terminal Server. If you enable Negotiate IP Address Automatically, the Terminal Server 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 Terminal Server 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>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 Terminal Server's port will accept. If your user is authenticated by the Terminal Server, 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 Terminal Server 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 Terminal Server. When setting either PAP and CHAP, make sure the Terminal Server and the PPP peer, have the same setting. For example, if the Terminal Server 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 Terminal Server 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 Terminal Server, <i>or</i> • you are using the Terminal Server as a router (back-to-back with another Terminal Server). <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 Terminal Server. The remote device will only authenticate your Terminal Server'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 Terminal Server. 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 Terminal Server, <i>or</i> • you are using the Terminal Server as a router (back-to-back with another Terminal Server) <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 Terminal Server. <p>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> <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 Terminal Server, <i>or</i> • you are using the Terminal Server as a router (back-to-back with another Terminal Server) <p>When Dial In or Dial In/Dial Out is enabled, the Remote User is the name the Terminal Server will use to authenticate the port on the remote device. Your Terminal Server 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 Terminal Server. This option does not work with external authentication.</p> <p>Field Format: You can enter a maximum of 16 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 Terminal Server, <i>or</i> • you are using the Terminal Server as a router (back-to-back with another Terminal Server) <p>Remote password means the following:</p> <ul style="list-style-type: none"> • When PAP is specified, this is the password the Terminal Server 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 Terminal Server 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 configure request 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 configure request packet will be re-sent before the link is terminated.</p> <p>Range: 0-255</p> <p>Default: 10 seconds</p>

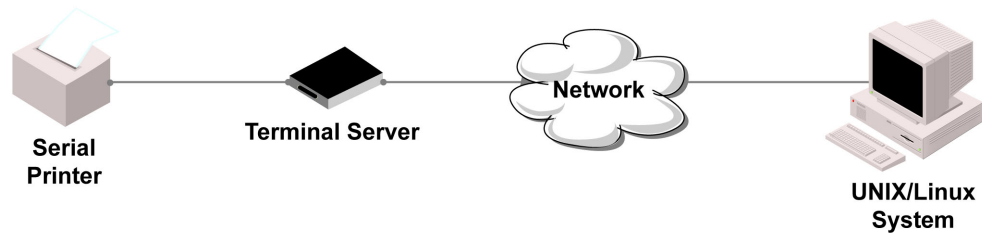
Terminate Req. Timeout	<p>The maximum time, in seconds, that LCP (Link Control Protocol) will wait before it considers a terminate request packet to have been lost.</p> <p>Range: 1-255</p> <p>Default: 3 seconds</p>
Terminate Req. Retries	<p>The maximum number of times a terminate request packet will 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 configure NAK 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 Terminal Server 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 Terminal Server ends the call.</p> <p>Default: Disabled</p>
Challenge Interval	<p>The interval, in minutes, for which the Terminal Server 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 Terminal Server.</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 Terminal Server, 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 Terminal Server will use the value in the RADIUS file in preference to the value configured here.</p> <p>Default: Enabled</p>

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
IP Address Negotiation	Specifies whether or not IP address negotiation will take place. IP address negotiation is where the Terminal Server 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.

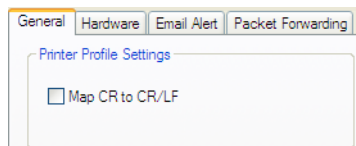
Printer Profile

Overview

The Printer profile allows for the serial port to be configured to support a serial printer device that can be accessed by the network.



General Tab Field Descriptions

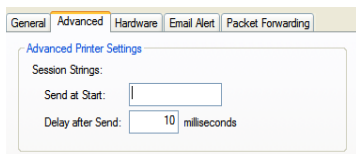


Configure the following parameter:

Map CR to CR/LF Defines the default end-of-line terminator as CR/LF (ASCII carriage-return line-feed) when enabled.

Default: Disabled

Advanced Tab Field Descriptions



Configure the following parameter:

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 Secure Terminal Server, 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. The decimal numbers within the brackets must be 3 digits long (example 003 not 3). To enter the < (less than symbol) precede the symbol with a \ (backslash symbol).

- **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.

Range: 0-65535 ms

Default: 10 ms

Serial Tunneling Profile

Overview

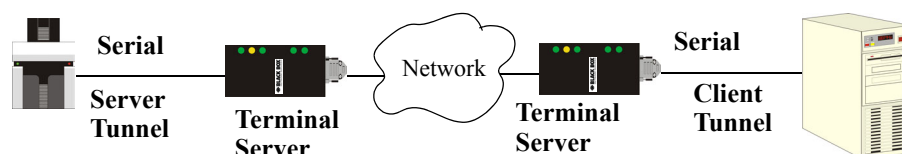
The Serial Tunneling profile allows two Terminal Servers to be connected back-to-back over the network to establish a virtual link between two serial ports based on RFC 2217.

Functionality

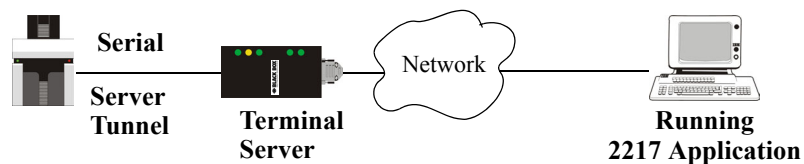
The serial device that initiates the connection is the **Tunnel Client** and the destination is the **Tunnel Server**, although once the serial communication tunnel has been successfully established, communication can go both ways.



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 Terminal Server 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.

General Tab Field Descriptions

Serial Port 2 Settings

Profile: **Serial Tunneling**
 Change Profile...

Name:

General | Advanced | Hardware | Email Alert | Packet Forwarding | SSL/TLS

Serial Tunneling Settings

A serial tunnel consists of two IOLANs connected over a TCP/IP network and creating a virtual link between two serial ports.

☒ **Act as Tunnel Server**
 Listen for connections on:
 TCP Port:

☐ **Act as Tunnel Client**
 Establish connection to:
 Host Name: TCP Port:

☐ **Enable TCP Keepalive**

Configure the following parameters:

Act As Tunnel Server	The Terminal Server will listen for an incoming connection request on the specified Internet Address on the specified TCP Port . Default: Enabled
TCP Port	The TCP port that the Terminal Server will listen for incoming connection on. Default: 10000+serial port number; so serial port 5 is 10005.
Act as Tunnel Client	The Terminal Server will initiate the connection the Tunnel Server. Default: Disabled
Host Name	A preconfigured host name that is associated with the IP address of the Tunnel Server.
TCP Port	The TCP port that the Terminal Server will use to connect to the Tunnel Server. Default: 10000+serial port number; so serial port 5 is 10005.
HTTP Tunnel	Specific the HTTP tunnel to be used for this connection.
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 determines how long the Terminal Server will wait during inactivity 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

Advanced Tab Field Descriptions

Advanced Serial Tunneling Settings

Break Length: milliseconds

Delay After Break: milliseconds

Session Strings:

Send at Start:

Send at End:

Delay after Send: milliseconds

Configure the following parameters:

- Break Length** When the Terminal Server 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;
- **Send at Start**—If configured, this string will be sent to the serial device on power-up of the Terminal Server 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 multihost is configured, this string will only be sent in listen mode to the serial device when all multihost 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

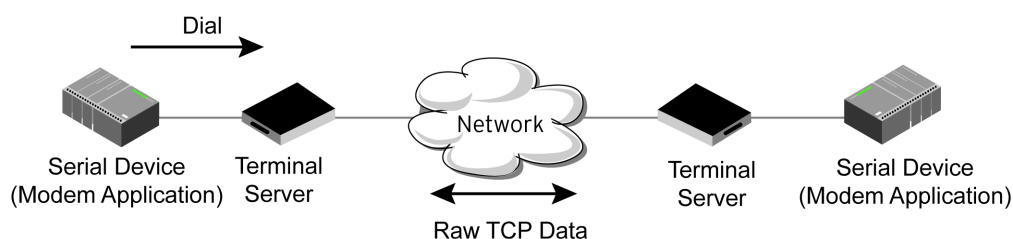
Overview

Virtual Modem (Vmodem) is a feature of the Terminal Server 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 Terminal Server in order to provide Ethernet network connectivity.

Functionality

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 the issue a dial-out request (ATDT). The Terminal Server 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 presents, so that the IP address is 12 digits long).



General Tab Field Descriptions

The screenshot shows the 'General' tab of the 'Virtual Modem Settings' window. It contains two main sections: 'Session Connection' and 'Connection Status'. In 'Session Connection', 'Listen on TCP Port' is 10001, 'Connect Automatically At Startup' is selected, 'Host Name' is 'None', and 'TCP Port' is 0. In 'Connection Status', 'Send Connection Status as' is checked, 'Verbose String' is selected, 'Success String' is 'CONNECT', and 'Failure String' is 'NO CARRIER'. There is also a 'Phone Number to Host Mapping...' button.

Configure the following parameters:

- Listen on TCP Port** The Terminal Server TCP port that the Terminal Server 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** Specific 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 Terminal Server 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.
 See [Phone Number to Host Mapping](#) for information about the window that appears when you click this button.
- 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 String	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 LISTNER Default: Enabled

Advanced Tab Field Descriptions

The screenshot shows the 'Advanced Virtual Modem Settings' window. The 'Advanced' tab is active. Under 'Modem Setup', 'Echo characters in command mode' is checked. The 'Hardware Signal Assignment' section has three columns: DTR Signal (radio buttons for Always On, Acts as DCD, Acts as RI), RTS Signal (radio buttons for Always On, Acts as DCD, Acts as RI), and DCD Signal (radio buttons for Always On, On when host connection established). The 'Additional modem initialization' field is empty. The 'Virtual Modem Features' section has 'Enable Message of the Day (MOTD)' and 'Enable TCP Keepalive' unchecked. 'AT Command Response Delay' is set to 250 milliseconds. 'Session Strings' has 'Send at Start' and 'Delay after Send' (set to 10 milliseconds) fields.

Configure the following 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	<p>You can specify additional virtual modem commands that will affect how virtual modem starts. The following commands are supported: ATQn, ATVn, ATEn, +++ATH, ATA, ATi0, ATi3, ATs0, AT&Z1, AT&Sn, AT&Rn, AT&Cn, AT&F, ATs2, ATs12, ATO (ATD with no phone number), and ATDS1.</p> <p>See <i>Appendix E, Virtual Modem AT Commands</i> for a more detailed explanation of the support initialization commands.</p>
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	<p>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.</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 determines how long the Terminal Server will wait during inactivity 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.</p> <p>Default: Disabled</p>
AT Command Response Delay	<p>The amount of time, in milliseconds, before an AT response is sent to the requesting device.</p> <p>Default: 250 ms</p>

Session Strings

Controls the sending of ASCII strings to serial devices at session start as follows;

- **Send at Start**—If configured, this string will be sent to the serial device on power-up of the Terminal Server 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 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 Terminal Server IP address and TCP Port that will be receiving the 'call.' 1-port models support up to 4 entries, all other desktop models support up to 8 entries, and rack-mount models support up to 48 entries.

The following buttons are available:

Add Button

Click the **Add** button to display a window that allows you to configure the phone number or AT command your modem application sends and the Terminal Server's IP address and TCP port number that is receiving the call.

Edit Button

Click on a phone number entry and click the **Edit** button to change any values configured for the phone number.

Delete Button

Click on a phone number entry and click the **Delete** button to remove it from the phone number list.

VModem Phone Number Entry

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

Configure the following parameters:

Phone Number

Specify the phone number your modem application sends to the modem. Note: The Terminal Server 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 Terminal Server will not match the two numbers. Spaces will be ignored.

Host IP Address	Specify the IP address of the Host that is receiving the virtual modem connection. Field Format: IPv4 or IPv6 address
Host	Specify the name of the Host that is receiving the virtual modem connection.
TCP Port	Specify the TCP Port on the Terminal Server that is set to receive the virtual modem connection. Default: 0

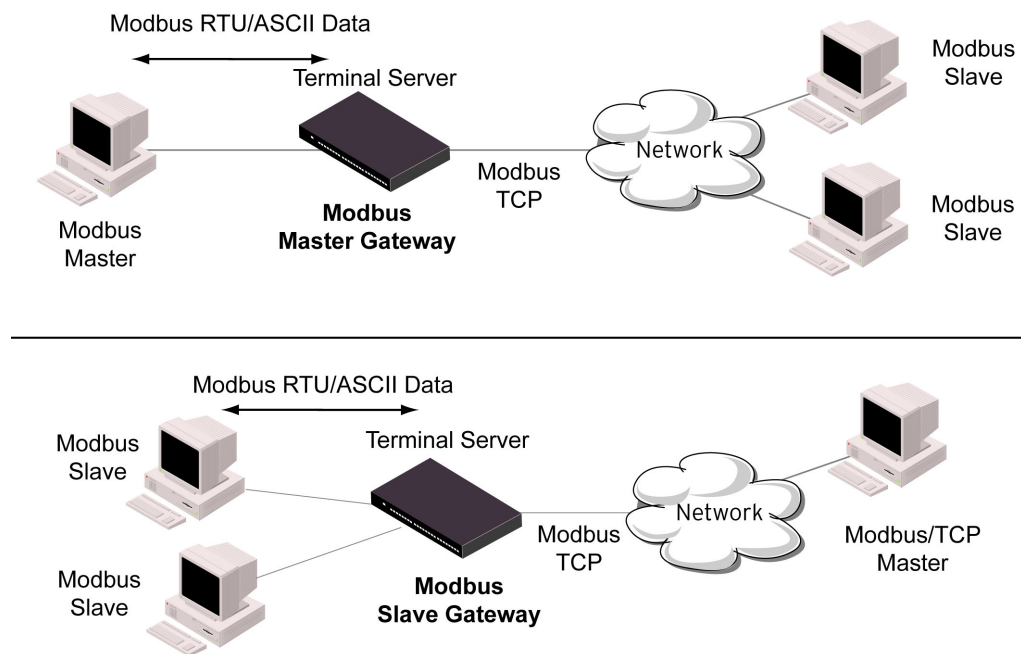
Modbus Gateway Profile

Overview

Each serial port can be configured as either a Modbus Master gateway or a Modbus Slave gateway, depending on your configuration and requirements.

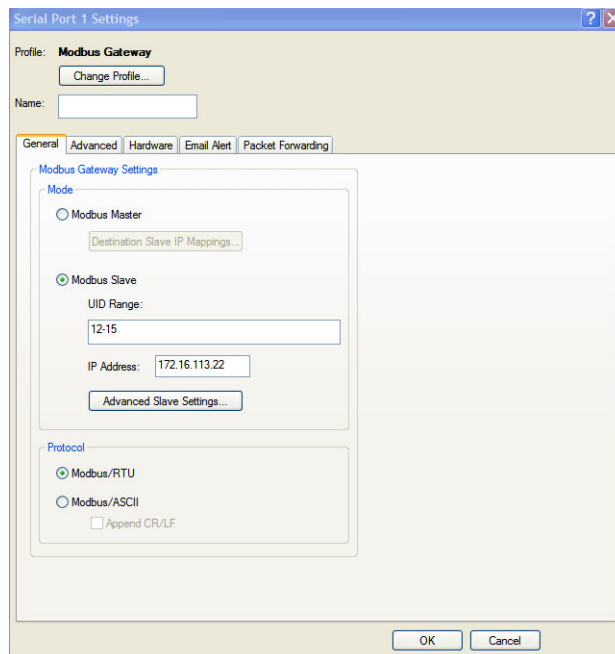
Functionality

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



General Tab Field Descriptions

Configure the following parameters:



Mode	<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 Terminal Server through the network to communicated to Modbus Slaves connected to the Terminal Server's Serial Ports. <p>Default: Modbus Master Gateway</p>
Destination Slave IP Mappings Button	Click 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.
Advanced Slave Settings Button	Click this button to configure global Modbus Slave settings.
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 the IP Aliasing feature.</p> <p>See Enable IP Aliasing for details about how to enable this feature.</p>
Modbus/RTU	<p>Select this option when the Modbus/RTU protocol is being used for communication between the Modbus Master and Slave.</p> <p>Default: Enabled</p>
Modbus/ASCII	<p>Select this option when Modbus/ASCII protocol is being used for communication between the Modbus Master and Slave.</p> <p>Default: Disabled</p>

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

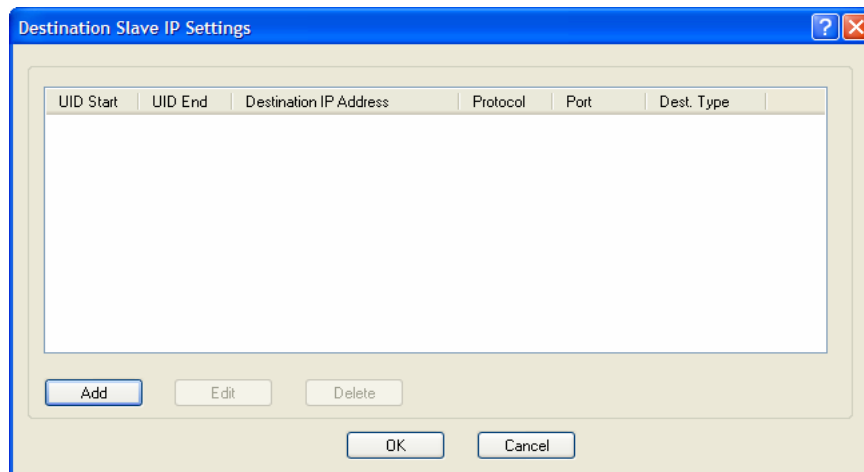
Advanced Field Descriptions

Configure the following parameters:

- Idle Timeout** Use this timer to close a connection because of inactivity. When the **Idle Timeout** expires, the Terminal Server 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** Click 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.
- 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;
- **Send at Start**—If configured, this string will be sent to the serial device on power-up of the Terminal Server 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 or terminated.
Default: 10 ms

Modbus Slave IP Settings Field Descriptions

This window is used to configure the Modbus Slaves.



The following buttons are available:

- | | |
|----------------------|---|
| Add Button | Adds an entry into the Modbus Destination Slave IP Settings table. |
| Edit Button | Edits an entry in the Modbus Destination Slave IP Settings table. |
| Delete Button | Deletes an entry from the Modbus Destination Slave IP Settings table. |

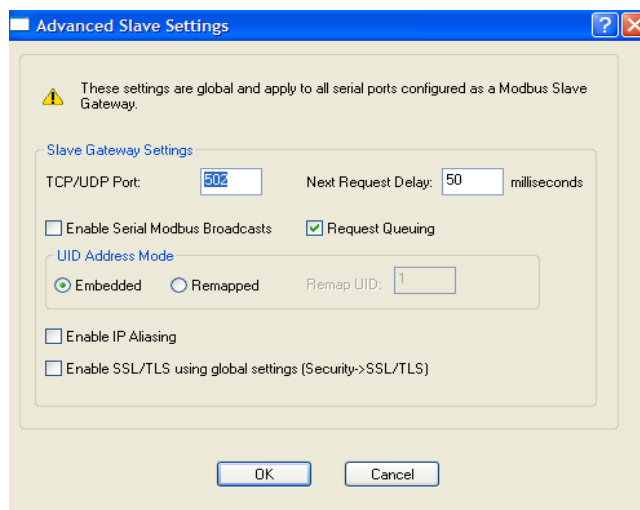
Adding/Editing Modbus Slave IP Settings

Configure the following 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 Terminal Server will automatically increment the last digit of the configured IP address. Therefore, you can specify a UID range of 1-100, and the Terminal Server 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</p> <p>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 Terminal Server will automatically increment the last digit of the configured IP address. Therefore, you can specify a UID range of 1-100, and the Terminal Server 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</p> <p>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	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). Field Format: IPv4 address
HTTP Tunnel	Specify the HTTP Tunnel that the Terminal Server will use for this connection.
Protocol	Specify the protocol that is used between the Modbus Master and Modbus Slave(s). Data Options: TCP or UDP Default: TCP
UDP/TCP Port	The destination port of the remote Modbus TCP Slave that the Terminal Server will connect to. Range: 0-65535 Default: 502

Modbus Slave Advanced Settings Field Descriptions



Configure the following parameters:

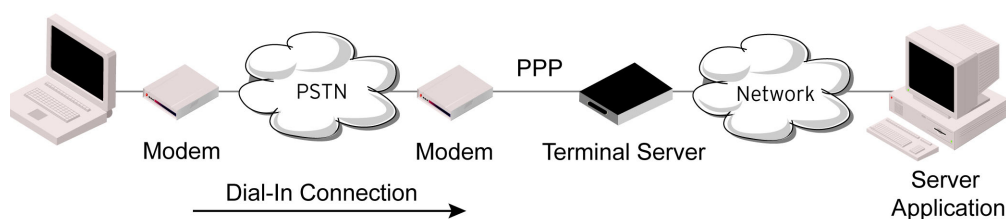
TCP/UDP Port	The network port number that the Slave Gateway will listen on for both TCP and UDP messages. Default: 502
Next Request Delay	A delay, in milliseconds, to allow serial slave(s) to re-enable receivers before issuing next Modbus Master request. Range: 0-1000 Default: 50 ms
Enable Serial Modbus 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

Enable IP Aliasing	When enabled, allows for multiple requests to serial slaves (from an Ethernet Master/s) to be processed simultaneously. Default: Off See IP Address for details about setting the IP address to be used with this serial port.
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 SSL/TLS using global settings	When enabled, Modbus Slave Gateway messages to remote TCP Modbus Masters are encrypted via SSL/TLS. Default: Disabled

Remote Access (PPP) Profile

Overview

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



Functionality

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.

You can use configure PPP authentication in the configuration or in the secrets file, but not both.

If you want to use a secrets file, you must download the secrets file to the Terminal Server for CHAP or PAP authentication; the files must be downloaded to the Terminal Server using the names

chap-secrets and **pap-secrets**, respectively. The file can be downloaded to the Terminal Server 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
```

General Tab Field Descriptions

The screenshot shows the 'General' tab of the 'PPP Settings' window. It contains the following fields and controls:

- IPv4 Local IP Address:** A text box with the value '0 . 0 . 0 . 0'.
- IPv4 Remote IP Address:** A text box with the value '0 . 0 . 0 . 0'.
- IPv4 Subnet Mask:** A text box with the value '0 . 0 . 0 . 0'.
- ☐ **Negotiate IP Address Automatically**
- Dynamic DNS...** button
- IPv6 Local Interface Identifier:** A text box with the value '::'.
- IPv6 Remote Interface Identifier:** A text box with the value '::'.
- IPv6 Global Network Prefix:** A text box with the value '0 : 0 : 0 : 0'.
- IPv6 Prefix Bits:** A text box with the value '64'.

Configure the following parameters:

IPv4 Local IP Address

The IPV4 IP address of the Terminal Server 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 Terminal Server'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 Terminal Server. If you set the PPP parameter IP Address Negotiation to On, the Terminal Server 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 and the RADIUS parameter **Framed-Address** is set in the RADIUS file, the Terminal Server 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 Terminal Server to use the remote IP address value configured here.

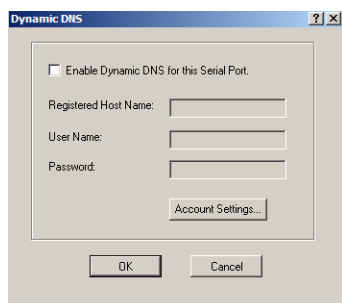
IPv4 Subnet Mask

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 Terminal Server will use the value in the RADIUS file in preference to the value configured here.

Negotiate IP Address Automatically	<p>Specifies whether or not IP address negotiation will take place. IP address negotiation is where the Terminal Server 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>
IPv6 Local Interface Identifier	<p>The local IPv6 interface identifier of the Terminal Server 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 Terminal Server'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 Terminal Server. If you enable Negotiate IP Address Automatically, the Terminal Server 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 Terminal Server 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>
IPv6 Global Network Prefix	<p>You can optionally specify an IPv6 global network prefix that the Terminal Server will advertise to the device at the other end of the PPP link.</p> <p>Default: 0:0:0:0</p>
IPv6 Prefix Bits	<p>Specify the prefix bits for the IPv6 global network prefix.</p> <p>Default: 64</p>

Dynamic DNS Field Descriptions

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).



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	Enables/disables the ability to register a new IP address with the DNS server. Default: Disabled

Authentication Tab Field Descriptions

The screenshot shows the 'Authentication' tab of a configuration window. It includes a dropdown menu for 'Authentication' set to 'CHAP', text input fields for 'User', 'Password', 'Remote User', and 'Remote Password', numeric input fields for 'Authentication Timeout' (1) and 'CHAP Challenge Interval' (0), and an unchecked checkbox for 'Enable Roaming Callback'.

Configure the following parameters:

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 Terminal Server. When setting either PAP and CHAP, make sure the Terminal Server and the PPP peer, have the same setting. For example, if the Terminal Server 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 Terminal Server 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 Terminal Server, <i>or</i>• you are using the Terminal Server as a router (back-to-back with another Terminal Server). <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 Terminal Server. The remote device will only authenticate your Terminal Server'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 Terminal Server. 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 Terminal Server, <i>or</i>• you are using the Terminal Server as a router (back-to-back with another Terminal Server) <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 Terminal Server. <p>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> <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 Terminal Server, <i>or</i>• you are using the Terminal Server as a router (back-to-back with another Terminal Server) <p>When Dial In or Dial In/Dial Out is enabled, the Remote User is the name the Terminal Server will use to authenticate the port on the remote device. Your Terminal Server 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 Terminal Server. This option does not work with external authentication.</p> <p>Field Format: You can enter a maximum of 16 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 Terminal Server, <i>or</i> • you are using the Terminal Server as a router (back-to-back with another Terminal Server) <p>Remote password means the following:</p> <ul style="list-style-type: none"> • When PAP is specified, this is the password the Terminal Server 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 Terminal Server 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 Terminal Server 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 Terminal Server.</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 Terminal Server 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 Terminal Server ends the call.</p> <p>Default: Disabled</p>

Advanced Tab Field Descriptions

Configure the following parameters:

- Routing** 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.
- Data Options
- **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.
- Default: None
- ACCM** Specifies the ACCM (Asynchronous Control Character Map) characters that should be escaped from the data stream.
- 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**.
- Default:** 00000000, which means no characters will be escaped
- MRU** The Maximum Receive Unit (MRU) parameter specifies the maximum size of PPP packets that the Terminal Server's port will accept. If your user is authenticated by the Terminal Server, the **MRU** value will be overridden if you have set a **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 Terminal Server will use the value in the RADIUS file in preference to the value configured here.
- Range:** 64-1500 bytes
- Default:** 1500

Configure Request Timeout	<p>The maximum time, in seconds, that LCP (Link Control Protocol) will wait before it considers a configure request packet to have been lost.</p> <p>Range: 1-255</p> <p>Default: 3 seconds</p>
Configure Request Retries	<p>The maximum number of times a configure request packet will be re-sent before the link is terminated.</p> <p>Range: 0-255</p> <p>Default: 10 seconds</p>
Terminate Request Timeout	<p>The maximum time, in seconds, that LCP (Link Control Protocol) will wait before it considers a terminate request packet to have been lost.</p> <p>Range: 1-255</p> <p>Default: 3 seconds</p>
Terminate Request Retries	<p>The maximum number of times a terminate request packet will be re-sent before the link is terminated.</p> <p>Range: 0-255</p> <p>Default: 2 seconds</p>
Echo Request Timeout	<p>The maximum time, in seconds, between sending an echo request packet if no response is received from the remote host.</p> <p>Range: 0-255</p> <p>Default: 30 seconds</p>
Echo Request Retries	<p>The maximum number of times an echo request packet will be re-sent before the link is terminated.</p> <p>Range: 0-255</p> <p>Default: 3</p>
Configure NAK Retries	<p>The maximum number of times a configure NAK packet will be re-sent before the link is terminated.</p> <p>Range: 0-255</p> <p>Default: 10 seconds</p>
Enable 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>
Enable Protocol Compression	<p>This determines whether compression of the PPP Protocol field takes place on this link.</p> <p>Default: Enabled</p>
Enable VJ Compression	<p>When enabled, Van Jacobson Compression is used on this link. If your user is authenticated by the Terminal Server, 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 Terminal Server will use the value in the RADIUS file in preference to the value configured here.</p> <p>Default: Enabled</p>

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 Terminal Server 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 Terminal Server will wait to establish a connection to a remote modem. Range: 1-99 Default: 45 seconds
Dial Retry	The number of times the Terminal Server 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;

- **Send at Start**—If configured, this string will be sent to the serial device on power-up of the Secure Terminal Server, 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. The decimal numbers within the brackets must be 3 digits long (example 003 not 3). To enter the < (less than symbol) precede the symbol with a \ (backslash symbol).

- **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.

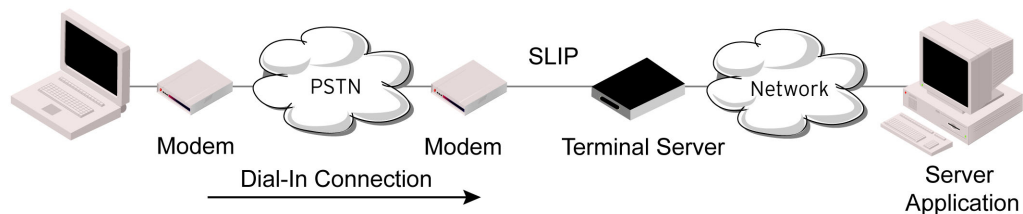
Range: 0-65535 ms

Default: 10 ms

Remote Access (SLIP) Profile

Overview

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



General Tab Field Descriptions

The screenshot shows a window titled 'SLIP Settings' with a 'General' tab selected. It contains three input fields for IP addresses and a subnet mask, each with a placeholder value of '0 . 0 . 0 . 0'.

Configure the following parameters:

- Local IP Address** The IPv4 address of the Terminal Server 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 Terminal Server'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 Terminal Server. If your user is authenticated by the Terminal Server, 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 Terminal Server 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 Terminal Server will use the value in the RADIUS file in preference to the value configured here.

Advanced Tab Field Descriptions

The screenshot shows the 'Advanced SLIP Settings' window. The 'Advanced' tab is active. The 'MTU' field is set to 256. The 'Routing' dropdown is set to 'None'. The 'VJ Compression' checkbox is checked. Under 'Session Strings', 'Send at Start' is empty and 'Delay after Send' is set to 10 milliseconds. The 'Dial Options' section has four radio buttons: 'Direct Connect' (selected), 'Dial In', 'Dial Out', and 'Dial In/Out'. The 'Dial Timeout' is set to 45 seconds and 'Dial Retry' is set to 2. There are also fields for 'Modem' and 'Phone'.

Configure the following parameters:

- MTU** The Maximum Transmission Unit (MTU) parameter restricts the size of individual SLIP packets being sent by the Terminal Server. Enter a value between 256 and 1500 bytes; for example, 512. The default value is **256**. If your user is authenticated by the Terminal Server, 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 Terminal Server will use the value in the RADIUS file in preference to the value configured here.
Default: 256
- Routing** Determines the routing mode (RIP, Routing Information Protocol) used on the **SLIP** interface as one of the following options:
- **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.
- This is the same function as the **Framed-Routing** attribute for RADIUS authenticated users.
Default: None
- VJ Compression** 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.
- If your user is authenticated by the Terminal Server, 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 *and* the RADIUS parameter **Framed-Compression** is set in the RADIUS file, the Terminal Server will use the value in the RADIUS file in preference to the value configured here.
Default: Enabled

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 Secure Terminal Server, 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. The decimal numbers within the brackets must be 3 digits long (example 003 not 3). To enter the < (less than symbol) precede the symbol with a \ (backslash symbol). • 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. Range: 0-65535 ms Default: 10 ms
Direct Connect	<p>If the device is remote and will be dialing in via modem or ISDN TA, enable this parameter. Default: Disabled</p>
Dial In	<p>If the device is remote and will be dialing in via modem or ISDN TA, enable this parameter. Default: Disabled</p>
Dial Out	<p>If you want the modem to dial a number when the serial port is started, enable this parameter. Default: Disabled</p>
Dial In/Out	<p>Enable this option when you want the serial port to do either of the following:</p> <ul style="list-style-type: none"> • accept a call from a modem or ISDN TA • dial a number when the serial port is started <p>Default: Disabled</p>
Dial Timeout	<p>The number of seconds the Terminal Server will wait to establish a connection to a remote modem. Range: 1-99 Default: 45 seconds</p>
Dial Retry	<p>The number of times the Terminal Server will attempt to re-establish a connection with a remote modem. Range: 0-99 Default: 2</p>
Modem	<p>The name of the predefined modem that is used on this line.</p>
Phone	<p>The phone number to use when Dial Out is enabled.</p>

Port Buffering

Overview

The Port Buffering feature allows data activity on the Terminal Server's serial ports to be held in memory for viewing at a later stage without affecting the normal operation of the serial ports.

Note: Port Buffering is only supported on serial port(s) configured for the **Console Management** profile.

Functionality

Port Buffering is required by system administrators to capture important information from devices attached to the Terminal Server. If a device (such as a Router) has a problem and sends a warning message out of its console port while no one is connected, the warning can be lost. With **Port Buffering** enabled, the messages will be captured in memory or in a file and can be viewed later to aid administrators in diagnosing and fixing problems.

Local Port Buffering

Port buffer information for the serial port can be viewed after successful connection to a device on a serial port. The user can toggle between communicating to the device on the serial port and viewing the port buffer data for that device by entering a the **View Buffer String** (default ~view). Local port buffering is limited to 256Kb and will be flushed after the Terminal Server reboots.

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

1. Connect to the device on that serial port by Telnet or SSH (the serial port(s) must be set to the **Console Management** profile to support this type of connection).
2. 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.
3. 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 Terminal Server 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 Terminal Server 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 Terminal Server will create unique files using the Terminal Server's Ethernet MAC address and serial port number. It is recommended that a unique NFS directory and serial port **Name** be configured if multiple Terminal Servers 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 your installation CDROM.

The data that is sent to the remote buffer file is appended to the end of the file (even through Terminal Server 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.

Field Definitions

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

Configure the following parameters:

Enable Local Buffering

Enables/disables local port buffering on the Terminal Server.
Default: Disabled

View Port Buffering String	<p>The string used by a session connected to a serial port to display the port buffer for that particular serial port.</p> <p>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).</p> <p>Default: ~view</p>
Enable Remote (NFS) Buffering	<p>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.</p> <p>Default: Disabled</p>
NFS Host	<p>The NFS host that the Terminal Server will send data to for its Remote Port Buffering feature. The Terminal Server 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).</p> <p>Default: None</p>
NFS Directory	<p>The directory and/or subdirectories where the Remote Port Buffering files will be created. For multiple Terminal Servers using the same NFS host, it is recommended that each Terminal Server have its own unique directory to house the remote port log files.</p> <p>Default: /device_server/portlogs</p>
Encrypt Data	<p>Determines if the data sent to the NFS host is sent encrypted or in the clear across the LAN.</p> <p>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. The Decoder utility software can be found on the installation CD-ROM.</p> <p>Default: Disabled</p>
Enable Port Buffering to Syslog	<p>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.</p> <p>Data Options: Emergency, Alert, Critical, Error, Warning, Notice, Info, Debug.</p> <p>Default Level: Info</p> <p>Default: Disabled</p>
Add Time Stamp to Data	<p>Enable/disable time stamping of the serial port buffer data.</p> <p>Default: Disabled</p>
Enable Key Stroke Buffering	<p>When enabled, key strokes that are sent from the network host to the serial device on the Terminal Server's serial port are buffered.</p> <p>Default: Disabled</p>

Advanced

Advanced Serial Settings Tab

Overview

Advanced serial port settings apply to all serial ports.

Field Descriptions

Configure the following parameters:

Process Break Signals	Enables/disables proprietary inband SSH break signal processing, the Telnet break signal, and the out-of-band break signals for COMredirect. 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 will 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>This also enables a per-connection TCP keepalive feature. After approximately 3 minutes of network connection idle time, 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 by all peer network connections.</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>

Data Logging Buffer Size	<p>The minimum data buffer size for all models is 1K. The maximum data buffer size is 2000 KB for the TS, all other models are 4000 KB. If the data buffer is filled, incoming serial data will overwrite the oldest data.</p> <p>Values: 1-2000 KB (TS) - Default 4 KB</p> <p>Values: 1-4000 KB (all other models) - Default 256 KB</p> <p>The Data Logging feature is a valid option for the COMredirect Profile and the TCP Sockets Profile</p>
Pre V4.3G Data Logging Mode	<p>Enable the data logging feature previous to V4.3G firmware.</p> <p>Default: Disabled</p>
Serial Port Menu String	<p>When a user connects to the Terminal Server through the network, the string used to access the Easy Port Access menu without disconnecting the network connection.</p> <p>Default: ~menu</p>
Session Escape String	<p>When a user connects to the Terminal Server 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>
Monitor Connection Status Interval	<p>Specify how often, in seconds, the Terminal Server will send a TCP keepalive to services that support TCP keepalive. This only applies to line service types that support the keepalive feature.</p> <p>Default: 180 seconds</p>
Retry Interval	<p>Sets the maximum time to wait for a response after sending a TCP keepalive message.</p> <p>Values: 1-32767 seconds</p> <p>Default: 5 seconds</p>
Retry Attempts	<p>The number of TCP keepalive retries before the connection is closed.</p> <p>Values: 1-32767</p> <p>Default: 5</p>

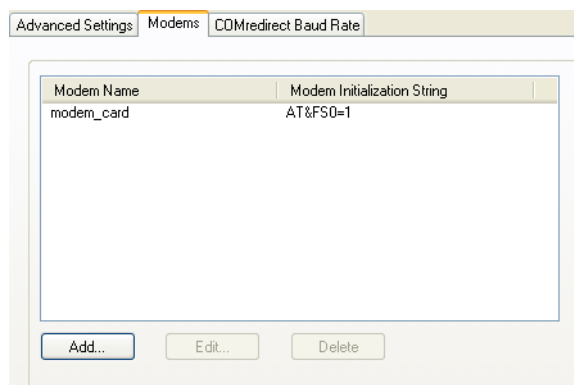
Modems Tab

Overview

You need to configure a modem if there is a modem connected to the Terminal Server. If your Terminal Server model contains an internal modem or a PCI slot (Secure Console Server models) for a modem card, a permanent modem string called **internal_modem** or Terminal Server **modem_card**, respectively, exists permanently in your configuration.

Functionality

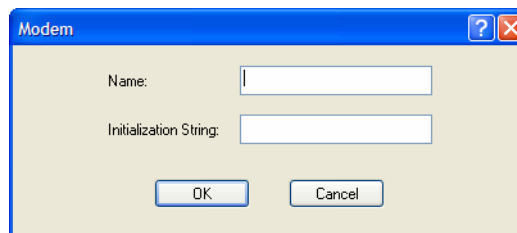
Modems are usually configured for PPP/SLIP dial in/out connections, although some modems do support raw data communication. When you click on the **Modems** tab, you will see the following:



If any modems have been configured, they will be displayed.

Adding/Editing a Modem

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



Configure the following parameters:

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

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

COMredirect Baud Rate Tab

Overview

The COMredirect 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.

Functionality

Since some older applications may not support the higher baud rates that the Terminal Server is capable of achieving, the baud rate can be mapped to a different value on the Terminal Server. Through COMredirect, you can remap the baud rate being specified by the Serial application to a different value on the physical serial port on the Terminal Server. See [COMredirect](#) for more information about the COMredirect utility.

Field Definitions

Advanced Settings Modems **COMredirect Baud Rate**

[Map COMredirect Baud](#)

Map your COMredirect baud rate (running on the application software) to the Actual baud rate (baud rate on the serial port).

COMredirect Baud	Actual Baud Rate
50	57600
75	75
110	115200
134	230400
150	150
200	200
300	300
600	600
1200	1200
1800	1800
2400	2400
4800	4800
9600	9600
19200	19200
38400	38400

Configure the following parameter:

Actual Baud Rate The actual baud rate that runs between the Terminal Server and the connected serial device. You can also specify a custom baud rate.

Range: 50 - 230400

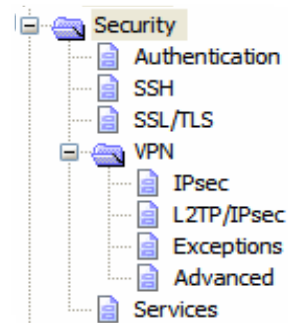
9

Configuring Security

Introduction

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 Terminal Server user profile or externally. This option configures the external authentication server. See [Authentication](#) for more information.
- **SSH**—This configuration window configures the SSH server in the Terminal Server. See [SSH](#) 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](#) for more information.
- **HTTP Tunnel**—This configuration window configures the Http Tunneling parameters. See [HTTP Tunneling](#) for more information.
- **Services**—This configuration window is used to enable/disable client and daemon services that run in the Terminal Server. See [Field Descriptions](#) for more information.



Authentication

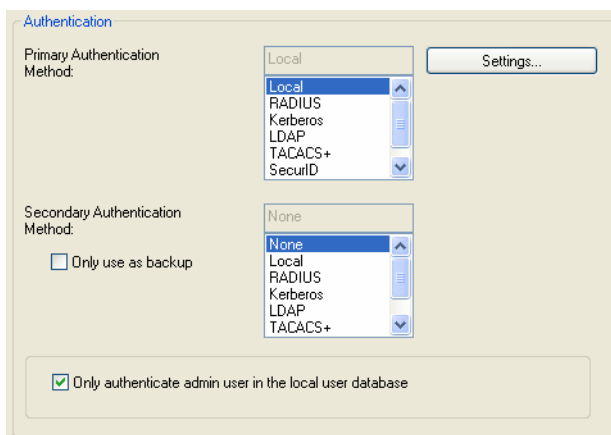
Authentication can be handled by the Terminal Server or through an external authentication server. Authentication is different from authorization, which can restrict a user's access to the network (although this can be done through the concept of creating sessions for a user, see [Sessions Tab](#) for more information). 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 Terminal Server supports RADIUS, Kerberos, LDAP, 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 Terminal Server 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 Terminal Server. See [Appendix A, RADIUS and TACACS+](#) for more information.

Authentication

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.



Configure the following parameters:

Primary Authentication Method

The first authentication method that the Terminal Server attempts.

Data Options: Local, RADIUS, Kerberos, LDAP/Microsoft Active directory, TACACS+, SecurID, NIS

Default: Local

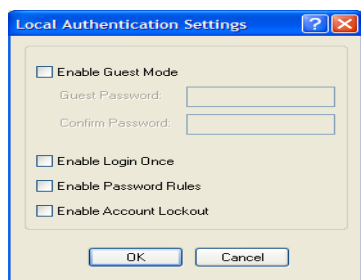
Secondary Authentication Method	<p>If the Primary Authentication Method fails, the next authentication method that the Terminal Server attempts. You can choose to use authentication methods in combination. For example, you can specify the Primary Authentication Method as Local and the Secondary Authentication Method as RADIUS. Therefore, some users can be defined in the Terminal Server (Local) others in RADIUS.</p> <p>Data Options: None, Local, RADIUS, Kerberos, LDAP/Microsoft Active Directory, TACACS+, SecurID, NIS</p> <p>Default: None</p>
Settings Button	Click this button to configure the authentication method.
Only use as backup	<p>The secondary authentication method will be tried only when the Terminal Server cannot communicate with the primary authentication host.</p> <p>Default: Disabled</p>
Only authenticate admin user in the local database	<p>When enabled, the Terminal Server 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 Terminal Server as the admin user, except through the console port.</p> <p>Default: Enabled</p>

Local

Overview

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

Field Descriptions



Configure the following parameters:

Enable Guest Mode	<p>Allow users who are not defined in the Users database to log into the Terminal Server 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	The password that Guest users must use to log into the Terminal Server.
Confirm Password	Type the Guest Password in again to verify that it is correct.

- Enable Login Once** 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.
- Enable Password Rules** When this option is selected, the following password rules will apply. The password must be 8 characters long and contain at least one number.
- Enable Account Lockout** When this option is selected, the Terminal Server's internal local user database will provide a 10 second delay after each valid attempt. If 5 invalid attempts are made within 10 minutes the user will be locked out from further attempts for 5 minutes.

RADIUS

Overview

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

General Field Descriptions

RADIUS Settings

Authentication Hosts

First Authentication Host: Secret:

Second Authentication Host: Secret:

Authentication Port:

Accounting

☐ Enable Accounting

First Accounting Host: Secret:

Second Accounting Host: Secret:

Account Port:

☒ Enable Accounting Authenticator

RADIUS Configuration

Retry: Timeout:

OK Cancel

Configure the following 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 Terminal Server 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 Terminal Server 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 Terminal Server validates the RADIUS accounting response. Default: Enabled
Retry	The number of times the Terminal Server tries to connect to the RADIUS server before erroring out. Range: 0-255 Default: 5
Timeout	The time, in seconds, that the Terminal Server 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 Terminal Server will retry the same host up to and including the number of retry attempts. Range: 1-255 Default: 3 seconds

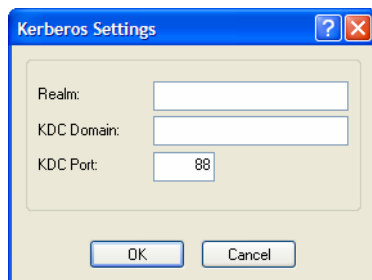
Attributes Field Descriptions

Configure the following parameters:

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 Terminal Server will send the Terminal Server's Ethernet 1 IPv4 address to the RADIUS server. Default: Enabled
Use the following NAS-IP-Address	When enabled, the Terminal Server will send the specified IPv4 address to the RADIUS server. Default: Disabled
IP Address	The IPv4 address that the Terminal Server will send to the RADIUS server. Default: 0.0.0.0
Automatically determine NAS-IPv6-Address	When enabled, the Terminal Server will send the Terminal Server's IPv6 address to the RADIUS server. Default: Enabled
Use the following NAS-IPv6-Address	When enabled, the Terminal Server will send the specified IPv6 address to the RADIUS server. Default: Disabled
IPv6 Address	The IPv6 address that the Terminal Server will send to the RADIUS server. Field Format: IPv6 address

Kerberos

Field Descriptions



Configure the following parameters:

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 Terminal Server's Host Table before the last reboot or be resolved by DNS.
KDC Port	The port that the Kerberos server listens to for authentication requests. Default: 88

LDAP/Microsoft Active Directory

Overview

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.

The following parameter need to be configured to use this feature.

Field Descriptions

The screenshot shows a window titled "LDAP/Active Directory Settings". It contains the following fields and controls:

- Host Name: [Text Field]
- Port: [389]
- Base: [Text Field]
- User Attribute:
 - ☒ OpenLDAP (uid)
 - ☐ Microsoft Active Directory (sAMAccountName)
 - ☐ Other: [Text Field]
- ☐ Encrypt Passwords Using MD5 Digest
- ☐ Authenticate Unit With LDAP Server
- Name: [Text Field]
- ☒ Append Base To Name
- Password: [Text Field]
- Confirm: [Text Field]
- ☐ Enable TLS
- TLS Port: [636]
- OK and Cancel buttons at the bottom.

Configure the following parameters.

- | | |
|-----------------------|---|
| 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 Terminal Server'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 | This defines the name of the attribute used to communicate the user name to the server.
Options: <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. Default: OpenLDAP(uid) |

Encrypt Passwords Using MD5 digest	Checking this parameter will cause the Terminal Server 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. Default: Disabled
Authenticate Terminal Server with LDAP server	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. Default: Disabled
Name	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 Terminal Server . Default: Enabled but if the base parameter is not configured, it does not modify the name.
Append Base to Name	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.
Confirm	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. Default: Blank
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

If you are using LDAP or Microsoft Active Directory with **TLS**, you need to download a CA list to the Terminal Server that includes the certificate authority (CA) that signed the LDAP certificate on the LDAP host by selecting **Tools, Advanced, Keys and Certificates**. See [Keys and Certificates](#) for more information on the LDAP certificate.

TACACS+

Overview

TACACS+ is an authentication method that the Terminal Server supports that can send back **User** information; see [TACACS+](#) for more information on the **User** parameters that can be sent back by TACACS+.

Field Descriptions

The screenshot shows a configuration window with two main sections: 'Authentication/Authorization' and 'Accounting'. In the 'Authentication/Authorization' section, 'Primary Host' and 'Secondary Host' are dropdown menus set to 'None', 'Port' is a text box containing '49', 'Secret' is an empty text box, and there is an unchecked checkbox for 'Enable Authorization'. The 'Accounting' section has an unchecked checkbox for 'Enable Accounting', followed by 'Primary Host' and 'Secondary Host' dropdown menus set to 'None', 'Port' is a text box containing '49', and 'Secret' is an empty text box. At the bottom of the window is an unchecked checkbox for 'Use Alternate Service Names'.

Configure the following 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 Terminal Server-specific parameters set in the TACACS+ configuration file can be passed to the Terminal Server after authentication. Default: Disabled
Enable Accounting	Enables/disables TACACS+ accounting. Default: Disabled

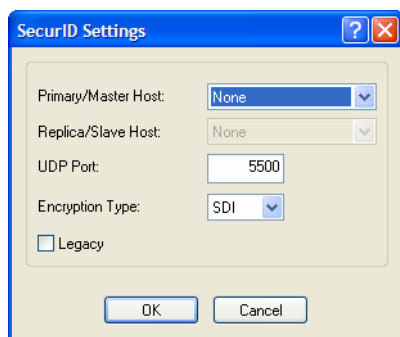
Accounting Primary Host	The primary TACACS+ host that is used for accounting. Default: None
Accounting Secondary Host	The secondary TACACS+ host that is used for accounting, should the primary accounting TACACS+ host fail to respond. Default: None
Accounting Port	The port number that TACACS+ listens 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 “admincli” and the service name for Web Manager or Device Manager to be “adminweb”.

SecurID

Overview

If you need to reset the SecurID secret, select **Tools, Reset, Reset SecurID Node Secret**.

Field Descriptions



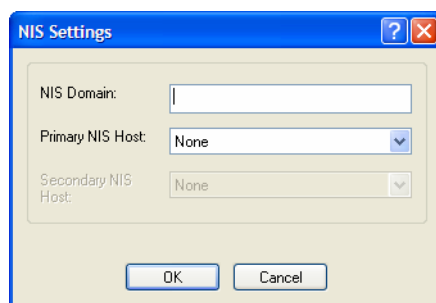
Configure the following parameters:

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

NIS

Field Descriptions



Configure the following 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

SSH

Overview

The Terminal Server contains SSH Server software that you need to configure if the Terminal Server is going to be accessed via SSH. If you specify more than one **Authentication** method and/or **Cipher**, the Terminal Server will negotiate with the client and use the first authentication method and cipher that is compatible with both systems.

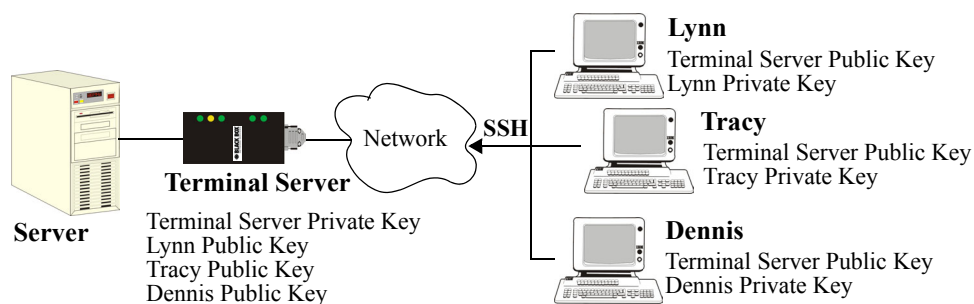
Functionality

When you are using the SSH connection protocol, keys need to be distributed to all users and the Terminal Server. Below are a couple of example scenarios for key/certificate distribution.

Users Logging into the Terminal Server 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 Terminal Server via SSH from the LAN. Therefore, the following keys need to be exchanged:

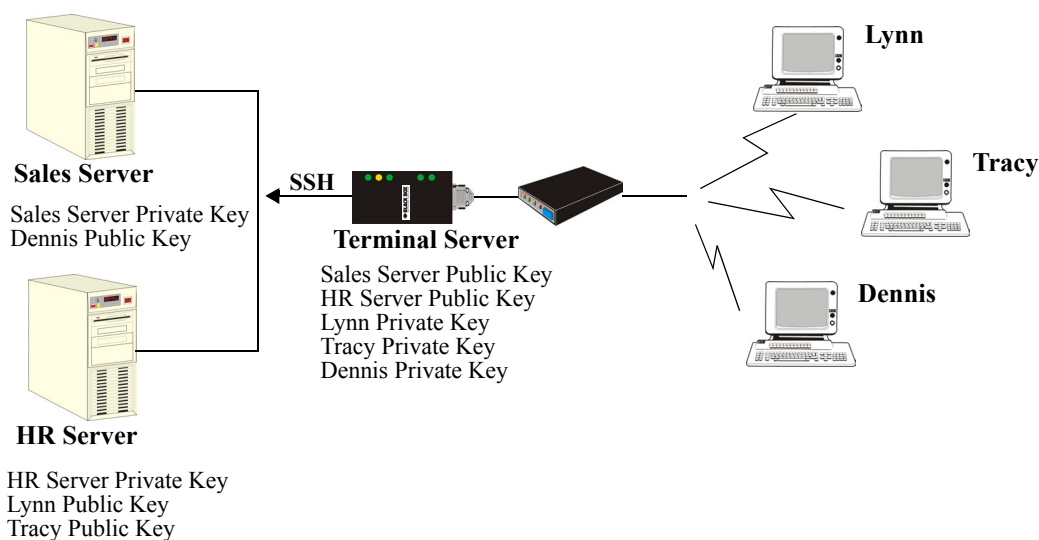
- Upload the Terminal Server **SSH Public Key** to each user's host machine who is connecting and logging into the Terminal Server using SSH.
- Download the SSH Public Key from each user's host machine who is connecting and logging into the Terminal Server using SSH.



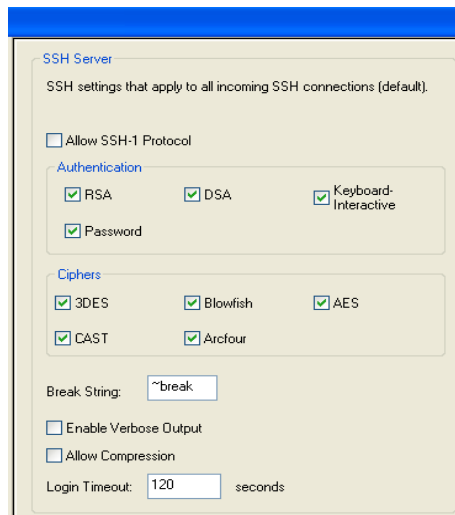
Users Passing Through the Terminal Server Using SSH (Dir/Sil)

This scenario applies to serial ports configured for the **Terminal** profile and are required to login to the Terminal Server. The user's service is set to the SSH protocol, therefore, users first log into the Terminal Server 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 Terminal Server. All the SSH negotiation is being done between the Terminal Server and the target servers, therefore, the following keys need to be exchanged:

- Download the **SSH Host Public Key** to the Terminal Server for each of the hosts that the Terminal Server 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 Terminal Server).



Field Descriptions



SSH Server
SSH settings that apply to all incoming SSH connections (default).

☐ Allow SSH-1 Protocol

Authentication

☒ RSA ☒ DSA ☒ Keyboard-Interactive
☒ Password

Ciphers

☒ 3DES ☒ Blowfish ☒ AES
☒ CAST ☒ Arcfour

Break String:

☐ Enable Verbose Output

☐ Allow Compression

Login Timeout: seconds

Configure the following parameters:

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 Terminal Server's SSH server will authenticate the user via RSA. Default: Enabled
DSA	When a client SSH session requests DSA authentication, the Terminal Server'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 Terminal Server SSH server's 3DES encryption is enabled/disabled. Default: Enabled
CAST	The Terminal Server SSH server's CAST encryption is enabled/disabled. Default: Enabled
Blowfish	The Terminal Server SSH server's Blowfish encryption is enabled/disabled. Default: Enabled
Arcfour	The Terminal Server SSH server's Arcfour encryption is enabled/disabled. Default: Enabled
AES-CBC	The Terminal Server SSH server's AES-CBC encryption is enabled/disabled. Default: Enabled

AES-CTR	The Terminal Server SSH server's AES-CTR encryption is enabled/disabled. Default: Enabled
AES-GCM	The Terminal Server SSH server's AES-GCM encryption is enabled/disabled. Default: Enabled
ChaCha20Poly1305	The Terminal Server SSH server's ChaCha20Poly1305 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 slow down things on fast networks. Default: Disabled
Login Timeout	Sets 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

Overview

When SSL/TLS is configured, data is encrypted between the Terminal Server 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.

Functionality

You can create an encrypted connection using SSL/TLS for the following profiles: **COMredirect**, **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 Terminal Server 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; [Appendix 15, 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).

Note: See [Keys and Certificates](#) for information about SSL/TLS support documents.

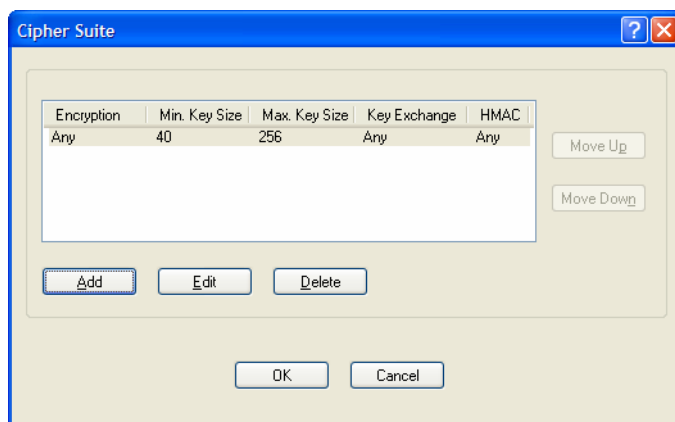
Field Descriptions

Configure the following parameters:

- | | |
|-----------------------------------|---|
| SSL/TLS Version | <p>Specify whether you want to use:</p> <ul style="list-style-type: none"> • Any—The Terminal Server will try a TLSv1 connection first. If that fails, it will try an SSLv3 connection. If that fails, it will try all other connection methods. • 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 Terminal Server serial port will act as an SSL/TLS client or server.</p> <p>Default: Client</p> |
| Cipher Suite Button | Click this button to specify SSL/TLS connection ciphers. |
| 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 Terminal Server.</p> <p>Default: Disabled</p> |
| Validation Criteria Button | Click this button to create peer certificate validation criteria that must be met for a valid SSL/TLS connection. |
| 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 Terminal Server, 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 Terminal Server and the client. You can specify up to five cipher groups.

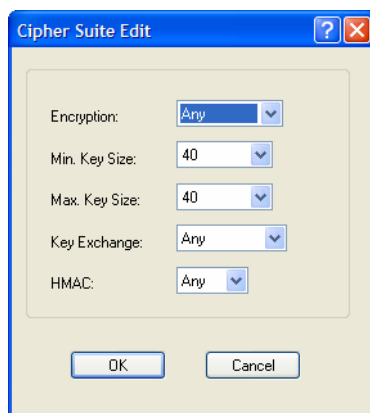


The following buttons are available on the Cipher Suite window:

- Add Button** Adds a cipher to the cipher list.
- Edit Button** Edits a cipher in the cipher list.
- Delete Button** Deletes a cipher from the cipher list.
- Move Up Button** Moves a cipher up in preference in the cipher list.
- Move Down Button** Moves a cipher down in preference in the cipher list.

Adding/Editing a Cipher

See [Appendix 15, SSL/TLS Ciphers](#) for a list of valid SSL/TLS ciphers.



Configure the following 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.

Configure the following parameters:

- | | |
|--------------------------|---|
| 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

Overview

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

You can configure the Terminal Server 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-Terminal Server VPN connection (allowing serial devices connected to the Terminal Server 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 Terminal Server. 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 Terminal Server except through a VPN tunnel or the console port. See [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.

Functionality

The information in this section applies only to setting up IPsec VPN tunnels, not L2TP/IPsec VPN tunnels.

The Terminal Server can be configured as a VPN gateway using the IPsec protocol. You can configure the VPN connection using two Terminal Servers as the local and remote VPN gateways or the Terminal Server 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, similar to what Windows Vista® provides.

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 Terminal Server 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 Terminal Server 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 Terminal Server 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 Terminal Server go through the configured IPsec tunnel(s), so you must configure any exceptions first (see [Exceptions](#) for more information on exceptions) or you will not be able to access the Terminal Server through the network unless you are configured to go through the IPsec tunnel (you can still access the Terminal Server through the Console port).

Field Descriptions

Name	Local IP Address	Local Host/Network	Remote IP Address	Remote Host/Network	Boot

The following buttons are available:

- Add Button** Click this button to add a new IPsec VPN tunnel.
- Edit Button** Select an existing IPsec VPN tunnel to edit the tunnel's parameters.
- Delete Button** Deletes a cipher from the cipher list.

Adding/Editing the IPsec Tunnel

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

Configure the following parameters:

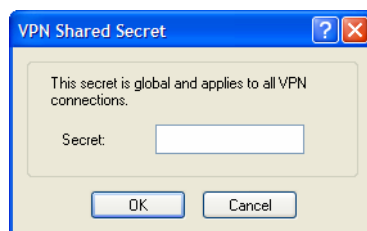
- | | |
|------------------------------|---|
| Name | Provide a name for the IPsec VPN tunnel to make it easy to identify.
Text Characteristics: Maximum of 16 characters, spaces not allowed |
| Authentication Method | Specify the authentication method that will be used between VPN peers to authenticate the VPN tunnel.
Data Options: <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 Terminal Server and upload the IPsec RSA public key from the Terminal Server 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 Terminal Server. Default: Shared Secret |

Secret/Remote Validation Criteria Button	<p>Depending on the Authentication Method:</p> <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. An asterisk (*) is valid as a wildcard.</p> <p>See Shared Secret Field Description for more information.</p> <p>See Remote Validation Criteria Field Descriptions for 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 Terminal Server-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 Terminal Server. You can specify %defaultroute when the IP address of the Terminal Server is not always known (for example, when it gets its IP address from DHCP). When %defaultroute 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, %defaultroute</p>
Local External IP Address	<p>When NAT Traversal (NAT_T) is enabled, this is Terminal Server's external IP address or FQDN. When the Terminal Server is behind a NAT router, this will be its public IP address.</p> <p>Field Format: IPv4 address, IPv6 address, FQDN</p>
Local Next Hop	<p>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 Terminal Server. Leave this parameter blank if you want to use the Default Gateway configured in the Terminal Server.</p> <p>Field Format: IPv4 or IPv6 address</p>
Local Host/Network Address	<p>The IP address of a specific host, or the network address that the Terminal Server will provide a VPN connection to.</p> <p>Field Format: IPv4 or IPv6 address</p>
Local IPv4 Subnet Mask	<p>The subnet mask of the local IPv4 network. Keep the default value when you are configuring a host-to-host VPN connection.</p> <p>Default: 255.255.255.255</p>
Local IPv6 Prefix Bits	<p>The prefix bits of the local IPv6 network. Keep the default value when you are configuring a host-to-host VPN connection.</p> <p>Default: 0</p>
Remote IP Address	<p>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.</p> <p>Field Format: IPv4 address, IPv6 address, FQDN, %any</p>
Remote External IP Address	<p>When NAT Traversal (NAT_T) is enabled, the remote VPN's public external IP address or FQDN.</p> <p>Field Format: IPv4 address, IPv6 address, FQDN</p>

Remote Next Hop	<p>The IP address of the router/gateway that will forward data packets to the Terminal Server (if required). The router/gateway must reside on the same subnet at the remote VPN.</p> <p>Field Format: IPv4 or IPv6 address</p>
Remote Host/Network Address	<p>The IP address of a specific host or the network address that the Terminal Server 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.</p> <p>Field Format: IPv4 or IPv6 address</p>
Remote IPv4 Subnet Mask	<p>The subnet mask of the remote IPv4 network. Keep the default value when you are configuring a host-to-host VPN connection.</p> <p>Default: 255.255.255.255</p>
Remote IPv6 Prefix Bits	<p>The prefix bits of the remote IPv6 network. Keep the default value when you are configuring a host-to-host VPN connection.</p> <p>Default: 0</p>
Boot Action	<p>Determines the state of the VPN network when the Terminal Server 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.



Configure the following parameter:

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).

The screenshot shows a window titled "IPsec Remote Validation Criteria". Inside, there are seven rows of configuration options, each consisting of a checkbox and a text input field:

- ☐ Country: [text input]
- ☐ State/Province: [text input]
- ☐ Locality: [text input]
- ☐ Organization: [text input]
- ☐ Organization Unit: [text input]
- ☐ Common Name: [text input]
- ☐ Email: [text input]

At the bottom of the window are two buttons: "OK" and "Cancel".

Configure the following 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, asterisk (*) works as a wildcard</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, asterisk (*) works as a wildcard</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, asterisk (*) works as a wildcard</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, asterisk (*) works as a wildcard</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, asterisk (*) works as a wildcard</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, asterisk (*) works as a wildcard. 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, asterisk (*) works as a wildcard</p> |

L2TP/IPsec

Many operating systems support L2TP/IPsec VPN tunnels, however, Windows XP® requires this VPN tunnel protocol. When L2TP/IPsec is enabled, the Terminal Server will listen for L2TP/IPsec VPN tunnel requests.

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

Field Descriptions

Configure the following parameters:

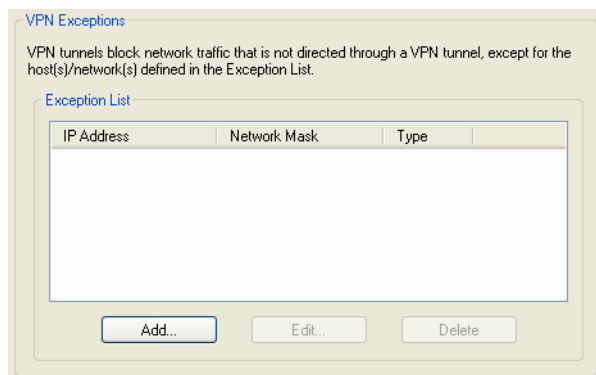
- | | |
|-------------------------------------|---|
| Allow L2TP/IPsec connections | When enabled, the Terminal Server listens for L2TP/IPsec VPN tunnel connections. Note: to allow non-VPN tunnel connections to the Terminal Server, you must create entries in the VPN Exceptions list.
Default: Disabled |
| Local IP Address | If the IPsec local address is set to 0.0.0.0, the Terminal Server will listen for L2TP/IPsec connections on (the IP address of) the network interface associated with (ie: on the same network as) the Terminal Server's default gateway. If no default gateway exists, the Terminal Server will not listen for L2TP/IPsec connections.
Default: 0.0.0.0 |
| Authentication Method | Specify the authentication method that will be used between VPN peers to authenticate the VPN tunnel.
Data Options: <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 Terminal Server. Default: Shared Secret |

Remote Validation Criteria	<p>Depending on the Authentication Method:</p> <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. An asterisk (*) is valid as a wildcard.</p> <p>See Shared Secret Field Description for more information.</p> <p>See Remote Validation Criteria Field Descriptions for more information on the X.509 certificate validation criteria.</p>
IPv4 Local IP Address	<p>If the IPsec local address is set to 0.0.0.0, the Terminal Server will listen for L2TP/IPsec connections on (the IP address of) the network interface associated with (ie: on the same network as) the Terminal Server's default gateway. If no default gateway exists, the Terminal Server will not listen for L2TP/IPsec connections.</p> <p>Default: 0.0.0.0</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>

Exceptions

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

Field Descriptions



The following buttons are available:

Add Button Click the **Add** button to add a VPN exception to the **Exception List**.

Edit Button	Highlight an Exception List entry and click the Edit button to change the entry.
Delete Button	Highlight an Exception List entry and click the Delete button to remove the entry from the list.

Adding/Editing a VPN Exception

The following parameters are available:

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

Advanced

Field Description

Configure the following parameter:

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

HTTP Tunneling

Overview

A HTTP tunnel is a firewall-safe communication channel between two Terminal Server'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 Terminal Server 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 HTTP Tunnels](#) for more information on setup requirements for these scenarios.

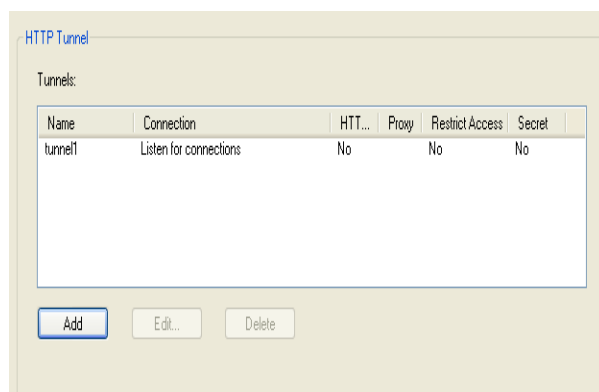
Functionality

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

A minimum of two Terminal Servers must be configured to create a communication channel. One Terminal Server must be configured as the listener and the other Terminal Server must be configured as the connecting Terminal Server.

Adding/Editing the HTTP Tunnel

Field Descriptions



The following buttons are available.

- | | |
|----------------------|--|
| Add Button | Click the Add button to add an HTTP Tunnel entry to the list. |
| Edit Button | Highlight an HTTP Tunnel entry and click the Edit button to change the entry. |
| Delete Button | Highlight an HTTP Tunnel entry and click the Delete button to remove the entry from the list. |

Configuring HTTP Tunnels

Field Descriptions

The following parameters are available for configurations.

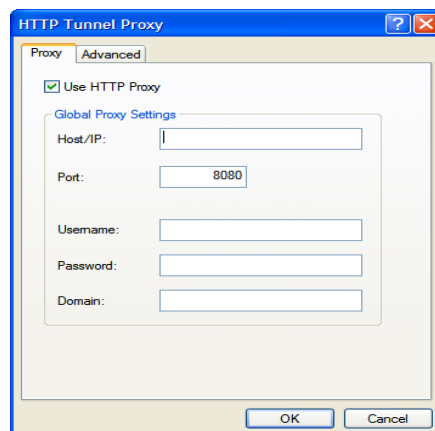
Name	Provide a name for this tunnel. This name must match the tunnel name on the tunnel peer Terminal Server.
Connect to	Provide the Host name or IP address of the listening Terminal Server.
Proxy Settings	If a proxy server is being used, configure the proxy specific parameters.
Listen for Connections	Listen for connection requests generated from the connecting Terminal Server.
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 Terminal Server only	If enabled, tunnel connections will only be allowed to access local devices (serial ports) on this Terminal Server . 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 Terminal Server configuration and the SSL/TLS certificate/private key and CA list must have already been downloaded to the Terminal Server; see [Keys and Certificates](#) for more information.

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.

Field Descriptions



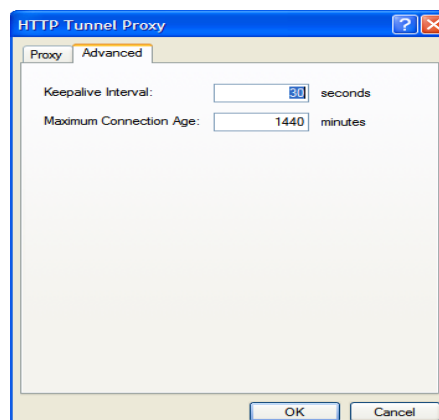
The following parameters are available for configuring the Proxy specific parameters:

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

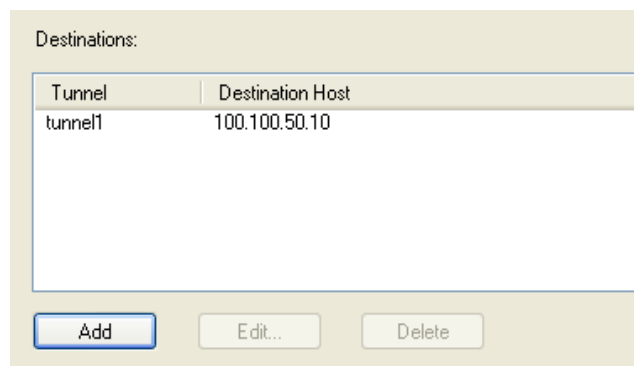
Field Descriptions



Configure the following parameters:

- Keepalive Interval** The number of seconds between sending keepalives for HTTP connections. Keepalives 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



The following buttons are available:

- Add Button** Click the **Add** button to add an HTTP Tunnel Destination entry to the list.
- Edit Button** Highlight an HTTP Tunnel Destination entry and click the **Edit** button to change the entry.
- Delete Button** Highlight an HTTP Tunnel Destination entry and click the **Delete** button to remove the entry from the list.

Field Descriptions

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 Terminal Server 's LAN. If the destination is a serial port on the Peer Terminal Server or the peer Terminal Server 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 Terminal Server has a listener on the same local TCP port. If not entered, the IP address of the Terminal Server is used.
Limited access to attached serial 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 click 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.

Services

Overview

Services are either daemon or client processes that run on the Terminal Server. You can disable any of the services for security reasons.

Functionality

If you disable any of the daemons, it can affect how the Terminal Server can be used or accessed. For example, if you disable WebManager (HTTPS and HTTP) services, you will not be able to access the Terminal Server with the WebManager. If you disable the DeviceManager service, the DeviceManager will not be able to connect to the Terminal Server. If you do not want to allow users to Telnet to the Terminal Server, you can disable the Telnet Server service; therefore, disabling daemons can also be used as an added security method for accessing the Terminal Server.

By default, all daemon and client applications are enabled, except IPsec, and running on the Terminal Server.

Field Descriptions

Network services that can be enabled/disabled to enhanced network security.

Network Services

- ☒ Telnet Server (listening on TCP port 23)
- ☒ TruePort Full Mode (listening on UDP port 668)
- ☒ Syslog Client (sends on UDP port 514)
- ☒ Modbus (default listening on UDP/TCP port 502)
- ☒ SNMP (listening on UDP port 161 and sending traps on UDP port 162)
- ☒ DeviceManager (listening on UDP port 33812 and sending on UDP port 33813)
- ☒ WebManager (HTTP) (listening on TCP port 80)
- ☒ WebManager (HTTPS) (listening on TCP port 443)
- ☒ SSH Server (listening on TCP port 22)
- ☒ NTP/SNTP Client (listening on UDP port 123)
- ☒ Dynamic Routing (RIP) (listening on UDP port 520/521)
- ☐ IPsec (listening and sending on UDP port 500)

Network Filtering

- ☒ Allow Ping Responses

Enable/disable the following options:

Telnet Server	Telnet daemon process in the Terminal Server listening on TCP port 23. Default: Enabled
COMredirect Full Mode	The COMredirect daemon process in the Secure Terminal Server supports COMredirect Full Mode on UDP port 668. You can still communicate with the Secure Terminal Server in Lite Mode when this service is disabled. Default: Enabled
Syslog Client	Syslog client process in the Terminal Server. Default: Enabled
Modbus	Modbus daemon process in the Terminal Server listening on port 502. Default: Enabled
SNMP	SNMP daemon process in the Terminal Server listening on port 161. Default: Enabled

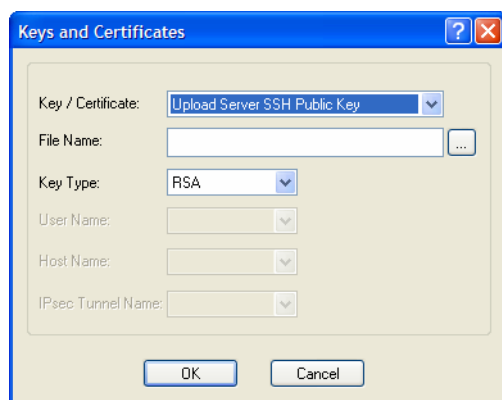
DeviceManager	<p>DeviceManager daemon process in the Terminal Server. If you disable this service, you will not be able to connect to the Terminal Server with the DeviceManager application. The DeviceManager listens on port 33812 and sends on port 33813.</p> <p>Default: Enabled</p>
WebManager (HTTP)	<p>WebManager daemon process in the Terminal Server listening on port 80.</p> <p>Default: Enabled</p>
WebManager (HTTPS)	<p>Secure WebManager daemon process in the Terminal Server listening on port 443.</p> <p>Default: Enabled</p> <p>If you are using the WebManager in secure mode (HTTPS), you need to download the SSL/TLS private key and certificate to the Terminal Server. You also need to set the SSL Passphrase parameter with the same password that was used to generate the key. See Keys and Certificates for more information.</p>
SSH Server	<p>SSH daemon process in the Terminal Server listening on TCP port 22.</p> <p>Default: Enabled</p>
NTP/SNTP Client	<p>Simple Network Time Protocol client process in the Terminal Server.</p> <p>Default: Enabled</p>
Dynamic Routing (RIP)	<p>Dynamic Routing daemon process in the Terminal Server listening on port 520.</p> <p>Default: Enabled</p>
IPsec	<p>IPsec daemon process in the Terminal Server listening and sending on UDP port 500.</p> <p>Default: Disabled</p>

Keys and Certificates

When you are using SSH, SSL/TLS, LDAP, 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 Terminal Server, with the exception of the Terminal Server SSH Public keys, which already exist in the Terminal Server. 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 Terminal Server public SSH key, select **Tools, Advanced, Keys and Certificates**.



The following fields are available:

- | | |
|--------------------------|--|
| Key / Certificate | <p>Select the key or certificate that you want to download to the Terminal Server or upload the Terminal Server SSH Public Key.</p> <p>Data Options:</p> <ul style="list-style-type: none"> ● Upload Server SSH Public Key, used for Console Management serial ports set to SSH connections ● Download SSH User Public Key, used for Console Management serial ports set to SSH connections ● Download SSH User Private Key, used for Terminal Server Users on serial ports set to the Terminal profile using SSH connections ● Download SSH Host Public Key, used for Terminal Server Users on serial ports set to the Terminal profile using SSH connections ● Download SSL/TLS Private Key, required if using HTTPS and/or SSL/TLS ● Download SSL/TLS Certificate, required if using HTTPS and/or SSL/TLS ● 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 ● Upload IPsec RSA Public Key, must be installed on the remote VPN gateway when the RSA Signature is the IPsec tunnel authentication method ● Download IPsec RSA Public Key, from the remote VPN gateway when RSA Signature is the IPsec tunnel authentication method ● 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 Terminal Server 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● **RSA1—SSH User Private Key, SSH Host Public Key <p>*RSA is used with SSH-2 **RSA1 is used with SSH-1</p>
User Name	The name of the user for whom you are downloading the SSH User Public or Private Key to the Terminal Server.
Host Name	The name of the host for which you are downloading the SSH Host Public or Private Key to the Terminal Server.
IPsec Tunnel Name	Select the IPsec tunnel that the RSA public key is being used to authenticate.

10 Configuring the Option Card

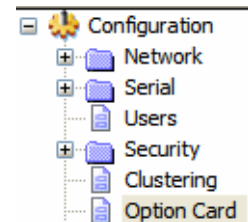
Introduction

Secure Console Server models have a built-in option card slot that supports a BLACK BOX[®] modem card (purchased separately).

Option Card Settings

Overview

The **Option Card** settings allow you to configure the option card slot for a BLACK BOX[®] modem card.



Functionality

The BLACK BOX[®] modem card slides into the PCI slot as described in [Installing a BLACK BOX[®] PCI Card](#).

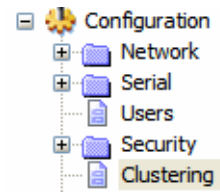
Configuring a Secure Console Server Modem Card

The Secure Console Server **Modem** card **Configure** button automatically takes you to the **PPP** serial port profile, although you can set and configure any serial port profile appropriate for modem use. See the [Chapter 8, Configuring Serial Ports](#) for information on the configuration options for the serial port profile that fits your modem usage.

11 Configuring Clustering

Introduction

Clustering is a way to provide access to the serial ports of many Terminal Servers through a single IP address.



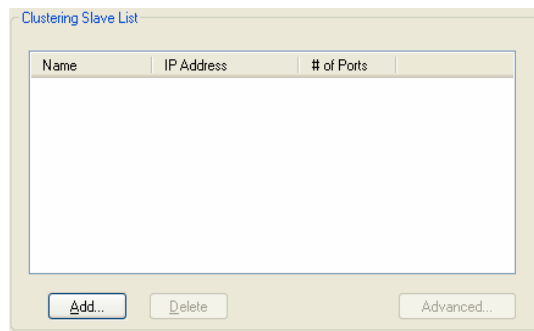
Clustering Slave List

Overview

The IP address that will be used to access all clustered serial ports will be that of the Master Terminal Server in the cluster. All other Terminal Servers in the cluster will be referred to as Slave Terminal Servers. 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 Terminal Server 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 Terminal Server entries and the number of ports on those slave Terminal Servers.

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



The following buttons are available:

- | | |
|----------------------|---|
| Add Button | Click this button to display a window to configure and add a new Slave Terminal Server's configuration to the clustering group.
See Adding Clustering Slaves for more information. |
| Delete Button | Select a Slave Terminal Server and click this button to delete it from the clustering group. |

Advanced Button Select a Slave Terminal Server and click this button to configure the individual Slave Terminal Server's serial ports.

See [Advanced Clustering Slave Options](#) for more information.

Adding Clustering Slaves

Overview

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

Field Descriptions

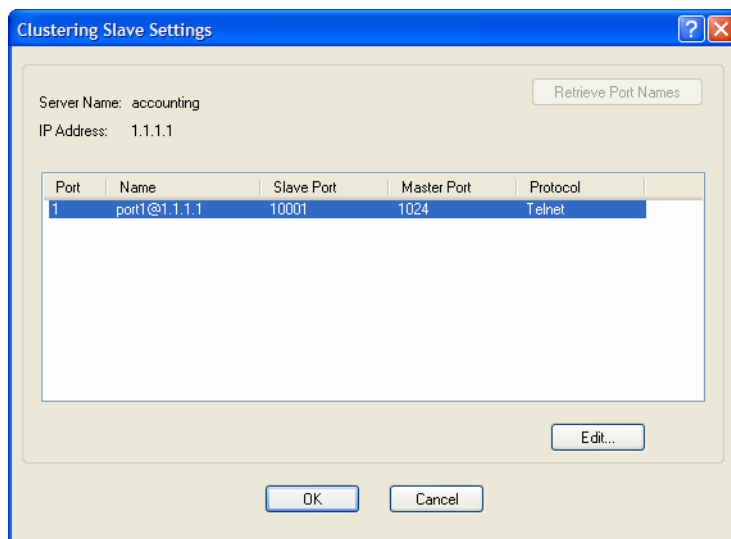
Configure the following parameters:

- | | |
|---------------------------------|---|
| Server Name | Specify a name for the slave Terminal Server in the clustering group. This name does not have to correspond to the proper host name, as it is just used within the Terminal Server.
Field Format: Maximum 15 alphanumeric characters, including spaces |
| IP Address | Specify the IP address of the slave Terminal Server in the clustering group.
Field Format: IPv4 |
| Number of Ports | Specify the number of ports in the Slave Terminal Server that you are adding to the clustering group.
Data Options: 1,2,4,8,16,24,32,48
Default: 1 |
| Starting Slave TCP Port | Specify the first TCP Port number (as specified in the slave Terminal Server'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 Terminal Server DS Port number to. This number should not be a port number that is already in use by the master Terminal Server.
Default: 1024, and then increments by one for each new slave entry |
| Protocol | Specify the protocol that will be used to access the slave Terminal Server port.
Data Options: SSH, Telnet
Field Format: Telnet |

Advanced Clustering Slave Options

Overview

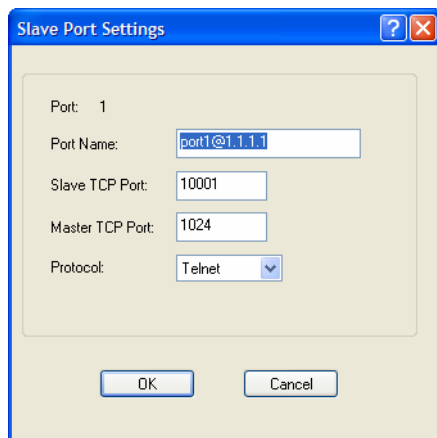
The **Advanced** button provides a means of configuring each individual serial port's name, connection protocol, and port association in the clustered Terminal Server slave. The **Clustering Slave Settings** window displays each clustered serial port slave entry, you need to click the **Edit** button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



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

Editing Clustering Slave Settings

Change the individual serial port settings Slave Port Settings window.



Configure the following parameters:

Port Name

Specify a name for the port.

Default: A combination of the port number, the @ symbol, and the IP address; for example, **port1@172.22.23.101**.

Slave TCP Port	<p>Specify the TCP Port number configured on the Slave Terminal Server that is associated to the port number you are configuring.</p> <p>Range: 1-99999</p>
Master TCP Port	<p>Specify the TCP port number you want to map to the Slave Terminal Server TCP Port. Users will use this TCP port number to access the Slave Terminal Server's port.</p> <p>Default: 1024, and then increments by one for each new slave entry</p>
Protocol	<p>Specify the protocol that will be used to access the port.</p> <p>Data Options: SSH, Telnet</p> <p>Default: Telnet</p>

12 Configuring the System

Introduction

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

Alerts

Email Alerts

Overview

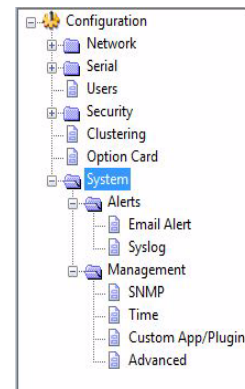
Email notification can be set at the Server and/or Line levels. You can set email notification at these levels because it is possible that the person who administers the Terminal Server might not be the same person who administers the serial device(s) attached to the Terminal Server port. Therefore,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

Functionality

Email notification requires an SMTP host that is accessible by the Terminal Server to process the email messages sent by the Terminal Server. 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
- Terminal Server System Failure, Error Level
- Authentication Failure, Notice Level
- Successful Login, Downloads (all), Configuration Save Commands, Info Level



Field Descriptions

Configure the following 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
The list above is in decreasing order of priority (Emergency being the highest and Debug being the lowest).
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 will be the contents of the "from" field in the generated email.
- 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 Terminal Server host table or the SMTP host IP address.
- HTTP Tunnel** Specific the HTTP tunnel to be used for this connection.
- Encryption** Select the type of encryption to be used.
Options: None (all information is sent in the clear), TLS, SSL
Default: None
- 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 the username is 64 characters.
- Password** Enter the password associated with the user configured in "Username".
Maximum size of the password is 64 characters.

Verify Peer Validation	<p>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 Terminal Server. 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.</p> <p>Default: Enabled if SSL or TLS encryption is selected. Disabled if no encryption is selected.</p>
TCP Port	<p>This is the TCP port used to communicate with the email server.</p> <p>Default: 25 for non-SSL, 465 if SSL/TLS is used</p>
NTLM Domain	<p>Select this field only 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.</p> <p>Options: 1-32 characters</p>

Syslog

Overview

The Terminal Server 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.

Field Descriptions

Configure the following parameters:

Primary Host	<p>The first preconfigured host that the Terminal Server will attempt to send system log messages to; messages will be displayed on the host's monitor.</p> <p>Default: None</p>
Secondary Host	<p>If the Terminal Server cannot communicate with the primary host, then the Terminal Server will attempt to send system log messages to this preconfigured host; messages will be displayed on the host's monitor.</p> <p>Default: None</p>
HTTP Tunnel	<p>Select the HTTP tunnel to use for this connection.</p>

Level

Choose the event level that triggers a syslog entry.

Data Options: Emergency, Alert, Critical, Error, Warning, Notice, Info, Debug

Default: Emergency

Management

SNMP

Overview

If you are using SNMP to manage/configure the Terminal Server, 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 Terminal Server; this can be done in the DeviceManager, WebManager, CLI, or Menu. You must then load the blackbox-sds.MIB (found on the CD-ROM packaged with the Terminal Server) file into your SNMP manager before you connect to the Terminal Server.

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

Field Descriptions

Configure the following parameters:

The screenshot shows the SNMP configuration window with the following sections:

- Contact Information:** Fields for Contact and Location.
- Communities (Version 1 and Version 2):** A table with columns for Community, Internet Address, and Permissions. The first row shows 'public' for Community, '0.0.0.0' for Internet Address, and 'Readwrite' for Permissions. There are three empty rows below.
- Users (Version 3):** Two columns for Read-Write and Read-Only users. Each column has fields for User, Security Level (set to 'None'), Auth Algorithm (set to 'MD5'), Auth Password, Confirm Password, Privacy Algorithm (set to 'DES'), Privacy Password, and Confirm Password.

Contact	The name and contract 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 Terminal Server. If the address is 0 . 0 . 0 . 0, any SNMP manager with the Community name can access the Terminal Server. 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 Terminal Server. Field Format: IPv4 or IPv6 address

Permissions	Permits the Terminal Server 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	Specified 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-Only User	Specified user can only view SNMP variables.
V3 Read-Write Confirm Password	Retype the privacy password.
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 Privacy Password** Retype the privacy password.

SNMP TRAPS

- Trap checkbox** Check this box to enable the entry of the trap information.
- Internet Address** Defines the hosts (by IP address) that will receive trap messages generated by the Terminal Server. Up to four trap hosts can be defined.
Field Format: IPv4 or IPv6 address
- Version** Select the version of the trap you want the Terminal Server to send. Valid options are v1, v2c or v3.
Default: v1
- Type** Select between Trap and Inform. Inform requires the host receiving the trap to acknowledge the receipt of the trap.
- Community** The name of the group that devices and management stations running SNMP belong to. Community only applies to SNMP version v1 and v2c.
- HTTP Tunnel** Select the HTTP tunnel to use for this connection.

Timeout	This is only used for Inform traps. Select the number of seconds to wait for acknowledge of the trap. Default: 1 second
Retries	This is only used for Inform traps. Select the number of times the trap will be sent if no acknowledge is received. Default: 3
V3 Trap User	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.
V3 Trap Security	Select the security level for the V3 traps. This must match the configuration set up in the SNMP manager. Data Options: None —No security is used. Auth —Trap authentication is used. Auth/Priv —Trap authentication and privacy (encryption) settings are used. Default: None
V3 Trap Auth Algorithm	Specify the authentication algorithm that will be used for the read-only user. Data Options: MD5, SHA Default: MD5
V3 Trap Auth Password	Type in the password associated with traps sent from this host.
V3 Trap Auth Confirm Password	Re-enter the password associated with traps sent from this host.
V3 Trap Privacy Algorithm	Specify the privacy algorithm (encryption) which will be used with traps. Data Options: DES, AES Default: DES
V3 Trap Privacy Password	Type in the password associated with the encryption method being used for traps.
Use Default Engine ID	When this field is selected, the firmware will use the default Engine ID. The default Engine ID uses the MAC address of the Ethernet interface to ensure that the Engine ID is unique to this agent.
Create Engine ID 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 Terminal Server on your network.

Time

Overview

You can set standard and summer time (daylight savings time) in the Terminal Server. You can specify the summer time settings as absolute, on a fixed date and time, or relative, on something like the third day of the third week at this time in June.

Functionality

The Terminal Server has a real-time internal clock, allowing the date and time to be set and viewed. It will maintain the time over a short power outage and after reboots of the Terminal Server. If you do not set the time, it will start the clock at the factory set time.

When you set the Terminal Server'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 Terminal Server through the DeviceManager and your PC's time zone is set to Pacific Standard Time (GMT -8:00) and the Terminal Server's time zone is set to Eastern Standard Time (GMT -5:00), the Terminal Server's time is actually three hours ahead of your PC's time. Therefore, if you set the Terminal Server's time to 2:30 pm in the DeviceManager, the Terminal Server'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.

Network Time Tab Field Descriptions

You can configure your NTP/SNTP client in the Terminal Server to automatically synchronize the Terminal Server's time.

The screenshot shows the 'Network Time' tab with the 'Time Zone/Summer Time (Daylight Saving Time)' sub-tab selected. Below this, the 'NTP/SNTP Settings' section contains the following fields:

- Mode:** A dropdown menu currently set to 'None'.
- Version:** A dropdown menu currently set to '4'.
- Enable Authentication:** An unchecked checkbox.
- Primary Host:** A dropdown menu currently set to 'None'.
- Key ID:** A text input field containing '0'.
- Secondary Host:** A dropdown menu currently set to 'None'.
- Key ID:** A text input field containing '0'.

Configure the following parameters:

NTP/SNTP Mode The NTP/SNTP mode.

Data Options:

- **None**—NTP/SNTP is turned off.
- **Unicast**—Sends a request packet periodically to the Primary host. If communication with the Primary host fails, the request will be sent to the Secondary host.
- **Broadcast/Multicast**—Listen for any broadcasts from an NTP/SNTP server and then synchronizes its internal clock to the message.
- **Manycast/Anycast**—Sends a request packet as a broadcast on the LAN to get a response from any NTP/ SNTP server. The first response that is received is used to synchronize its internal clock and then operates in **Unicast** mode with that NTP/SNTP server.

Default: None

NTP/SNTP Version Version of NTP/SNTP.

Range: 1-4

Default: 4

Enable Authentication Sets the NTP/SNTP server authentication On or Off.

Default: Off

Key ID Specify the key ID associated with this host. This key must exist in the ntp/sntp (symmetric key) file that was downloaded to the Terminal Server.

Valid Key ID's: 1-65534

(**Note:** the structure for the ntp/sntp (symmetric key) file can be found in your Terminal Server's User Guide - Appendix J)

Primary Host	The name of the primary NTP/SNTP server from the Terminal Server host table. Valid with Unicast and Multicast modes, although in Multicast mode, the Terminal Server will only accept broadcasts from the specified host NTP/SNTP server.
Secondary Host	The name of the secondary NTP/SNTP server from the Terminal Server host table. Valid with Unicast and Multicast modes, although in Multicast mode, the Terminal Server will only accept broadcasts from the specified host NTP/SNTP server.
HTTP Tunnel	Specify the HTTP tunnel to be used for this connection.

Time Zone/Summer Time Tab Field Descriptions

You can configure an automatic summer time (daylight savings time) time change.

Configure the following parameters:

Time Zone Name	The name of the time zone to be displayed during standard time. Field Format: Maximum 4 characters and minimum 3 characters (do not use angled brackets < >)
Time Zone Offset	The offset from UTC for your local time zone. Field Format: Hours <i>hh</i> (valid -12 to +14) and minutes <i>mm</i> (valid 0 to 59 minutes)
Summer Time Name	The name of the configured summer time zone; this will be displayed during the summer time setting. If this parameter is not set, then the summertime feature will not work. Field Format: Maximum 4 characters and minimum 3 characters (do not use angled brackets < >)
Summer Time Offset	The offset from standard time in minutes. Valid values are 0 to 180. Range: 0-180 Default: 60

Summer Time Mode

You can configure the summer time to take effect:

- **None**—No summer time change.
- **Fixed**—The summer time change goes into effect at the specified time every year. For example, April 15 at 1:00 pm.
- **Recurring**—The summer time changes goes into effect every year at same relative time. For example, on the third week in April on a Tuesday at 1:00 pm.

Default: None

Fixed Start Date

Sets the exact date and time in which the Terminal Server's clock will change to summer time (daylight saving time) hours.

Fixed End Date

Sets the exact date and time in which the Terminal Server's clock will end summer time hours and change to standard time.

Recurring Start Date

Sets the relative date and time in which the Terminal Server's clock will change to summer time (daylight saving time) hours. Sunday is considered the first day of the week.

Recurring End Date

Sets the relative date and time in which the Terminal Server's clock will end summer time hours and change to standard time. Sunday is considered the first day of the week.

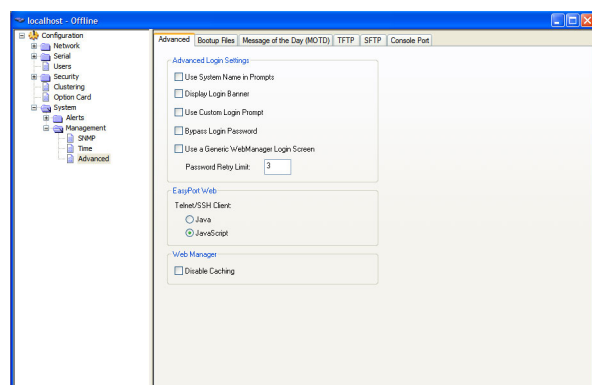
Advanced

Overview

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

Login Tab Field Descriptions

Configure the following parameters:

**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 Terminal Server login prompt, CLI prompt, WebManager login screen, and the heading of the Menu.

Default: Disabled

Display Login Banner	<p>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.</p> <p>Default: Disabled</p>
Use Custom Login Prompt	<p>When set, and a custom language file is in use, the login prompt will use the string defined in the language file as the login prompt instead of the default prompt, login:.</p> <p>Default: Disabled</p>
Use a Generic WebManager Login Screen	<p>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.</p> <p>Default: Disabled</p>
Bypass Login Password	<p>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.</p> <p>Default: Disabled</p>
Password Retry Limit	<p>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.</p> <p>Default: 3</p>
EasyPort Web	<p>Select Java if communication is via port 23(Telnet) or port 22(SSH) and the Terminal Server is not restricted by a firewall.</p> <p>Select Javascript if you need to communicate through a firewall on port 8080 using EasyPort Web.</p> <p>To end and close a Telnet session, type CTRL] then type quit</p> <p>To end and close a SSH session, on a new line type ~ . (period).</p>
Disable Caching	<p>When this option is selected, the Web Manager will no longer cache web pages.</p>

Bootup Files Tab Field Descriptions

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

Configure the following 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 Terminal Server'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 Terminal Server that will be loaded when the Terminal Server is rebooted. |
| Use SFTP | Check this box if you wish to use SFTP (Secure File Transfer Protocol) instead of TFTP (Trivial File Transfer Protocol). The Terminal Server 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 Terminal Server'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 Terminal Server that will be loaded when the Terminal Server is rebooted. |

Message of the Day (MOTD) Tab Field Descriptions

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

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

- The message of the day file is retrieved from a SFTP/TFTP server every time a user logs into the Terminal Server. You must have a SFTP/TFTP server running on any host that you are uploading or downloading files to/from when using SFTP/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 Terminal Server and retrieved locally every time a user logs into the Terminal Server. You can download a MOTD file to the Terminal Server 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 Terminal Server, you must specify the MOTD file name

in the **Filename** field to access it as the message of the day (no **SFTP/TFTP Host** parameter is required when the file is internal).

Advanced | **Bootup Files** | Message of the Day (MOTD) | TFTP | SFTP | Console Port

TFTP Host:

Filename:

☐ Use SFTP

☐ Display MOTD in WebManager/EasyPort Web

Configure the following parameters:

- | | |
|--|--|
| TFTP Host | The host that the Terminal Server 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 Terminal Server. The Terminal Server 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 | Select the HTTP tunnel to use 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 Terminal Server 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 Tab Field Descriptions

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.

Advanced | Bootup Files | Message of the Day (MOTD) | **TFTP** | SFTP | Console Port

Retry:

Timeout: seconds

Host:

HTTP Tunnel:

Configure the following parameters:

Retry	The number of times the Terminal Server will retry to transmit a TFTP packet to/from a host when no response is received. A value of 0 (zero) means that the Terminal Server will not attempt a retry. Range: 0-5 Default: 5
Timeout	The time, in seconds, that the Terminal Server will wait for a successful transmit or receipt of TFTP packets before retrying a TFTP transfer. Range: 3-10 Default: 3 seconds
Host	The name of the Host to use for this connection
HTTP Tunnel	Select the HTTP tunnel to use for this connection.

SFTP Tab Field Descriptions

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

Configure the following parameters:

Enable Compression	Enables compression of all data. Compression of data is desirable on slow connections, however on faster networks, compression will degrade data transmission rates.
Auto Logon	When checked, the Terminal Server will automatically log into the SFTP server using the Name field. If Keyboard Interactive is checked the Terminal Server will also send the Password field.
Name	Enter the user name that will be used to automatically log into the SFTP server
Password	Enter the password that will be used to automatically log into the SFTP server
Host	Select the host entry from the Terminal Server's host table which corresponds to the SFTP server.
HTTP Tunnel	Select the HTTP tunnel to use for this connection.
SSH 1 enable	Enable the negotiation of the SSH1 protocol.
SSH 1 Cipher	Select the encryption cipher to be used if the SSH1 protocol is used. Valid options are "3DES" or "Blowfish".

SSH 2 enable	Enable the negotiation of the SSH2 protocol.
SSH 2 Cipher	Select the encryption cipher(s) to be used if the SSH2 protocol is used. You can provide up to five values in order of preference. Valid options are “3DES”, “Blowfish”, “AES-CBC”, “CAST”, “AES-CTR”, “AES-GCM”, ChaCha20Poly1305 and “Arcfour”.
SSH 3 enable	Enable the negotiation of the SSH2 protocol.
SSH 3 Cipher	Select the encryption cipher(s) to be used if the SSH2 protocol is used. You can provide up to five values in order of preference. Valid options are “3DES”, “Blowfish”, “AES-CBC”, “CAST”, “AES-CTR”, “AES-GCM”, ChaCha20Poly1305 and “Arcfour”.
SSH 4 enable	Enable the negotiation of the SSH2 protocol.
SSH 4 Cipher	Select the encryption cipher(s) to be used if the SSH2 protocol is used. You can provide up to five values in order of preference. Valid options are “3DES”, “Blowfish”, “AES-CBC”, “CAST”, “AES-CTR”, “AES-GCM”, ChaCha20Poly1305 and “Arcfour”.
SSH 5 enable	Enable the negotiation of the SSH2 protocol.
SSH 5 Cipher	Enable the negotiation of the SSH2 protocol.
Authentication RSA	Allow RSA to be used as the method of authenticating the Terminal Server.
Authentication DSA	Allow DSA to be used as the method of authenticating the Terminal Server.
Keyboard Interactive	Allow Keyboard Interactive to be used as the method of authenticating the Terminal Server.

Console Port Tab Field Descriptions

This tab is found on rack mount models and is used to configure the Admin/Console port.

The screenshot shows a web interface with several tabs: Login, Bootup Files, Message of the Day (MOTD), TFTP, and Console Port. The Console Port tab is active. It contains two dropdown menus: 'Baud Rate' and 'Flow Control'.

Configure the following parameters:

Baud Rate	Specifies the baud rate of the line connected to the dedicated console port. Data Options: 9600, 19200, 38400, 57600, 115200 Default: 9600
Flow Control	For Terminal Server models that have a dedicated console port, defines how the data flow is handled. Data Options: <ul style="list-style-type: none"> • Soft—Data flow control is handled by the software. • Hard—Data flow control is handled by the hardware. • None—There is no data flow control. Default: None

13 System Administration

Introduction

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.

Managing Configuration Files

Saving Configuration Files

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

- In DeviceManager, select **File, Save As** from the menu bar. 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 Terminal Server 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.
- In WebManager, select under the **Administration** option, select **Backup/Restore**. Click the **Backup** button.

Downloading Configuration Files

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

- In DeviceManager:
 1. Connect to the Terminal Server to retrieve the current configuration file.
 2. Open the configuration file you want to download to the Terminal Server 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 Terminal Server** or click the **Download All Changes** button.
 4. Reboot the Terminal Server.
- In WebManager:
 1. Under the **Administration** option, select **Backup/Restore**.
 2. Browse to the configuration file that you want to download to the Terminal Server.
 3. Click the **Restore** button.
 4. Reboot the Terminal Server.

Downloading Configuration Files to Multiple Terminal Servers

You can download a configuration file to multiple Terminal Servers 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** Terminal Servers.
2. Specify the Terminal Servers that you want to download the configuration to:

Enter the following information for each Terminal Server that you want to configure with the same configuration file:

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

3. Click **Add** to add the Terminal Server to the download list. You can also click on a Terminal Server and edit any information and then click **Update** to make the edits permanent.
4. Click 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 Terminal Server'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** Terminal Server. The working configuration file will automatically be loaded into the DeviceManager.

Specifying a Custom Factory Default Configuration

When you receive the Terminal Server, it comes with a factory default configuration that it can be reset to at any time. Administrators might find it useful to customize the factory default configuration file, so that if the Terminal Server 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 Terminal Server**—You can download a custom factory default file to the Terminal Server using any of the configuration methods. In DeviceManager, you must connect to the Terminal Server and then select **Tools, Advanced, Custom Files, Custom Factory Default Configuration** and then specify the file. In WebManager, you must connect to the Terminal Server and then select **Administration, Reset, Factory Defaults, Set Current Configuration as Factory Default**.
- **Download the current configuration to the Terminal Server**—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 Terminal Server). In DeviceManager, select **Tools, Advanced, Set Factory Default to Terminal Server**. In WebManager, select **Administration, Reset, Factory Defaults, Get and Set Factory Default Configuration File**.

Resetting to the Original Factory Default Configuration

When you press the Reset button on the Terminal Server, the following take place:

- **Less than 3 seconds**—Reboots the Terminal Server.
- **Between 3 and 10 seconds**—Reboots the Terminal Server and resets the configuration to the factory default (either the original default configuration or the custom default configuration).
- **Over 10 seconds**—Reboots the Terminal Server and resets the configuration to the original factory default configuration.

Downloading Terminal Server Firmware

To upgrade the Terminal Server firmware (software):

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

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

Setting the Terminal Server's Date and Time

When you set the Terminal Server'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 Terminal Server through the DeviceManager and your PC's time zone is set to Pacific Standard Time (GMT -8:00) and the Terminal Server's time zone is set to Eastern Standard Time (GMT -5:00), the Terminal Server's time is actually three hours ahead of your PC's time. Therefore, if you set the Terminal Server's time to 2:30 pm in the DeviceManager, the Terminal Server'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 Terminal Server's internal clock time to the time specified, with no interpretation.

To set the Terminal Server's system clock in DeviceManager, select **Tools, Advanced, Set Unit Time/Date** and in WebManager select **Administration, Date/Time**.

Configure the following parameters:

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

Rebooting the Terminal Server

When you download any file (configuration, keys, certificates, firmware, etc.) to the Terminal Server, you must reboot the Terminal Server 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 Terminal Server's serial port/s statistics back to zero.

Resetting the Terminal Server to Factory Defaults

You can reset the Terminal Server to its factory default configuration by selecting **Tools, Reset, Reset to Factory Default** in DeviceManager and **Administration, Reset, Factory Defaults** in WebManager. The Terminal Server will automatically reboot itself with the 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 Terminal Server for this to take effect, it works instantly.

Language Support

Two language files, in addition to English, are supplied on the supplemental CD, 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 Terminal Server and select the **Language** option of **Custom Language** or **Customlang** (custom language), making the Menu and CLI field labels display in the desired language.

You can view Menu or 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 Terminal Server and is not overwritten by your new language. Each user logged into the Terminal Server 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 are provided on the supplemental CD.

To load one of the supplied languages into the Terminal Server, so the Menu or CLI fields appear in another language, do the following:

1. Open the supplemental CD and identify the language file, either **bb_ds_French.txt** or **bb_ds_German.txt**, or supply one of your own translated files.
2. Copy the language file to a host machine on the network; place it in the main file system or on the main hard drive.
3. Either use the SFTP/TFTP defaults in the Terminal Server or, configure as necessary, SFTP/TFTP in the Terminal Server.
4. In the CLI of the Terminal Server, enter the host IP address and file name; for example,

```
netload customlang 172.16.4.1 /temp/bb_ds_French.txt
snetload customlang 172.16.4.1 /temp/bb_ds_French.txt
```

The Terminal Server will download the language file via either TFTP or SFTP.

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.

5. 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.

6. The user will see the change of language when he/she logs out (**Main Menu**, **Sessions Menu**, **Logout**) and logs back into the Terminal Server. 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 Terminal Server 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 Terminal Server 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 Menu or 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).

Software Upgrades and Language Files

If you receive a software upgrade for the Terminal Server, the language files supplied on the supplemental diskette/CD might also have been updated. We will endeavour to provide a list of those changes in another text file on the same supplemental CD.

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

If you are already using one of the supplied languages, French or German, you probably want to update the language file in the Terminal Server. Until you update the Terminal Server 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:

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

Downloading Terminal Definitions

All terminal types can be used on the Terminal Server. Some terminal types which are not already defined in the Terminal Server, however, are unable to use Full Screen mode (menus) and may not be able to page through sessions properly. When installed, the Terminal Server 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 Terminal Server. The terminal definitions can be downloaded from a TCP/IP host.

To download terminal definitions, follow these steps:

1. Configure SFTP/TFTP in the Terminal Server as necessary.
2. Select **Tools, Advanced, Custom Files** from the menu bar in DeviceManager and **Administration, Custom Files** in WebManager.
3. 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 Terminal Server.
4. 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 Terminal Server 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 Terminal Server to its factory default settings (this will reset it to the original factory default or custom factory default settings, depending on what has been configured) through any of the following methods:

- You can push in the recessed button at the back of the Terminal Server hardware for three to ten seconds (pushing it in and then quickly releasing will just reboot the Terminal Server)
- DeviceManager, select **Tools, Reset, Reset to Factory Defaults**
- CLI, at the command line type, **reset factory**
- WebManager, select **Administration, Reset, Factory Default**, and then click 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 Terminal Server to the factory defaults
- have another user that has **admin** level rights, if one is already configured, reset the Admin password

14 Applications

Introduction

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

Configuring Modbus

This sections provides a brief overview of the steps required to configure the Terminal Server for your Modbus environment. You can read the [Modbus Gateway Settings](#) and [Modbus Serial Port Settings](#) sections for more specific information about the Modbus settings.

Overview

This section describes the high-level steps required to configure the Terminal Server as a Modbus Master or Slave Gateway.

Configuring a Master Gateway

To configure a Master Gateway (Modbus Master connected to the serial side of the Terminal Server), 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, click 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, click the **Advanced Slave Settings** button to configure global Slave Gateway settings.
5. For specialized configuration options, select the **Advanced** tab and configure as required.

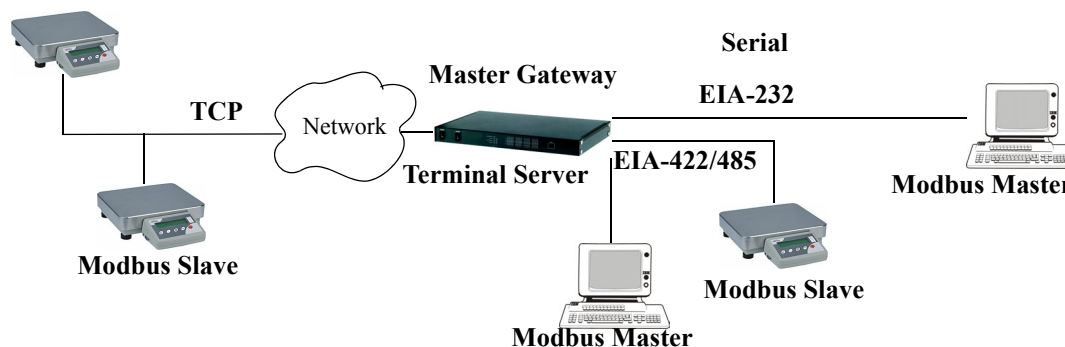
Modbus Gateway Settings

The scenarios in this section are used to illustrate how the Terminal Server's Modbus Gateway settings are incorporated into a Modbus device environment. Depending on how your Modbus Master or Slave devices are distributed, the Terminal Server can act as both a Slave and Master Gateway(s) on a multiport Terminal Server or as either a Slave or Master Gateway on a single port Terminal Server.

Modbus Master Gateway

The Terminal Server acts as a Master Gateway when the Modbus Master is connected to a serial port on the Terminal Server. Each Modbus Master can communicate to UID's 1-247.

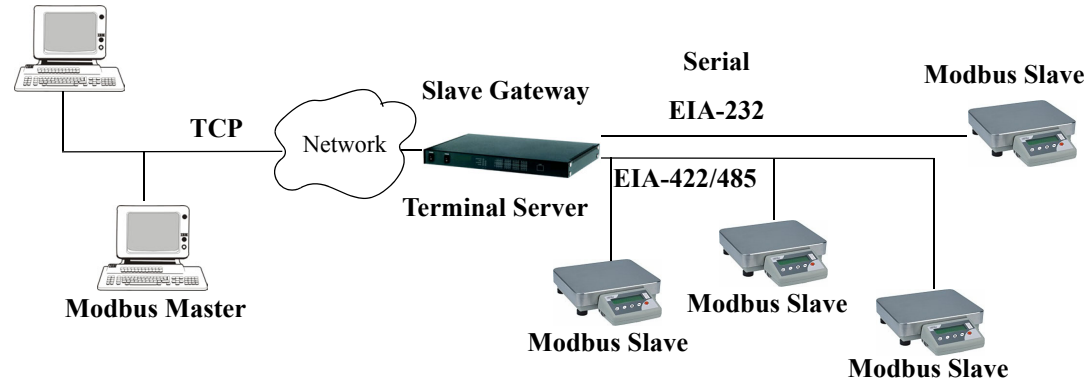
Modbus Slave



Modbus Slave Gateway

The Terminal Server 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 Terminal Server. Note: The Terminal Server provides a single gateway to the network-attached Modbus Masters. This means that all Modbus Slaves attached to the Terminal Server'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

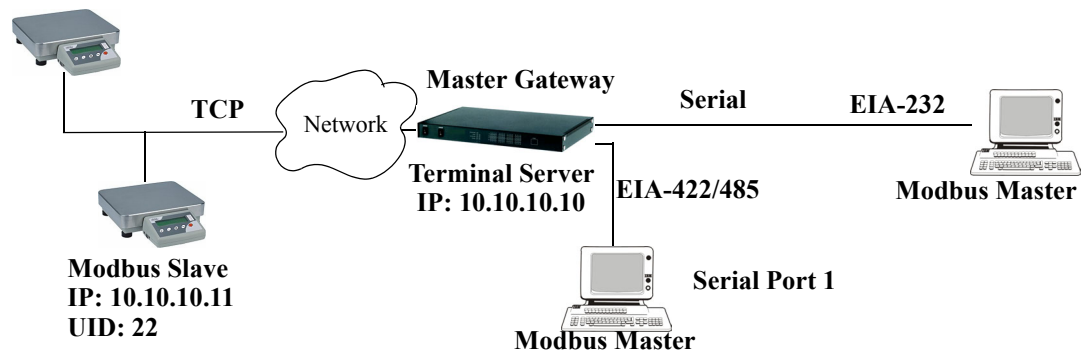


Modbus Serial Port Settings

Modbus Master Settings

When the Modbus Masters is attached to the Terminal Server'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 Terminal Server 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. Click the **Destination Slave IP Mappings** button and click the **Add** button in the **Destination Slave IP Mappings** window.
4. Configure the **Destination Slave IP Mappings** window as follows:

The screenshot shows the 'Destination Modbus Slave IP Settings' dialog box. It contains the following fields and options:

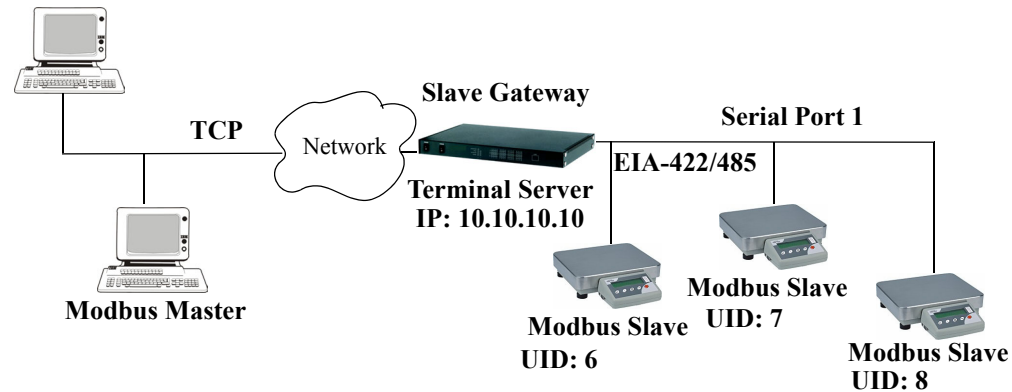
- UID:** Start: 22, End: 23
- Destination:**
 - Type: ☒ Host, ☐ Gateway
 - IP Address: Start: 10.10.10.11, End: 10.10.10.12
- Protocol:** ☒ TCP, ☐ UDP
- UDP/TCP Port:** 502
- Buttons: OK, Cancel

The Terminal Server 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 Terminal Server 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 Terminal Server, configure the serial port to the **Modbus Gateway** profile acting as a Modbus Slave. There is only one Slave Gateway in the Terminal Server, 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:

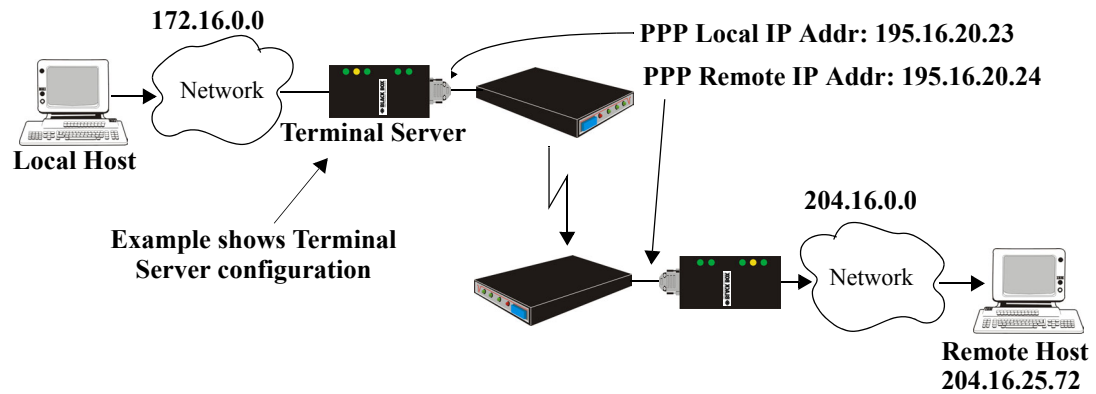
1. Select the **Modbus Gateway** profile for serial port 1.
2. On the **General** tab, enable the **Modbus Slave** parameter.
3. Still on the **General** tab, specify the **UID Range** as 6-8 as shown below:

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 green dot). The 'UID Range' is set to '6-8'. The 'Protocol' is set to 'Modbus/RTU' (indicated by a green dot). The 'Append CR/LF' checkbox is unchecked.

4. Click the **Advanced Slave Settings** button to verify that the default settings are acceptable.

Configuring PPP Dial On Demand

The Terminal Server can be configured to access remote networks via modems connected to the serial interface of the Terminal Server. By configuring the Terminal Server 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.

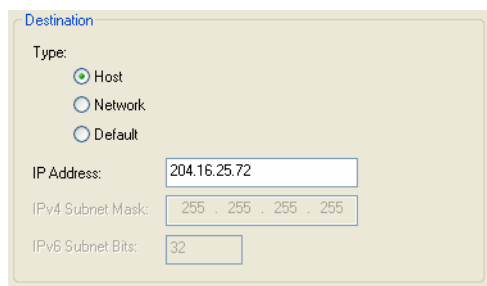
PPP Settings

IPv4 Local IP Address:	195 . 16 . 20 . 23
IPv4 Remote IP Address:	195 . 16 . 20 . 24
IPv4 Subnet Mask:	255 . 255 . 255 . 0

6. Next you need to create a gateway and destination route entry. Select **Network**, **Advanced**, and the **Route List** tab.

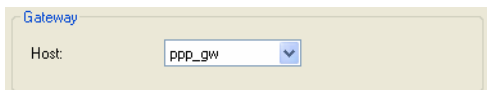
For the destination, if you want the connection to be able to reach any host in the remote network, set the **Type** to **Network** and specify the network IP address and subnet/prefix bits; if you want the connection to go directly to a specific remote host, set the **Type** to **Host** and specify the host's IP address.

We want a specific host to be the destination, so we configured the **Type** as **Host**:



The image shows a 'Destination' configuration window. It has a 'Type' section with three radio buttons: 'Host' (selected), 'Network', and 'Default'. Below this, there are three input fields: 'IP Address' with the value '204.16.25.72', 'IPv4 Subnet Mask' with the value '255 . 255 . 255 . 255', and 'IPv6 Subnet Bits' with the value '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 image shows a 'Gateway' configuration window. It has a 'Host' label followed by a dropdown menu that currently displays 'ppp_gw'.

Setting Up Printers

The Terminal Server 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 Terminal Server 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.

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 the following syntax:

```
rmp <filename> <ip_address> <Terminal_Server_Name>:p<#>
```

where **<#>** is the Terminal Server serial port number (10000 + serial port number).

Remote Printing Using Host-Based Print Handling Software

Printers connected to the Terminal Server can be accessed by TCP/IP hosts using print handling software.

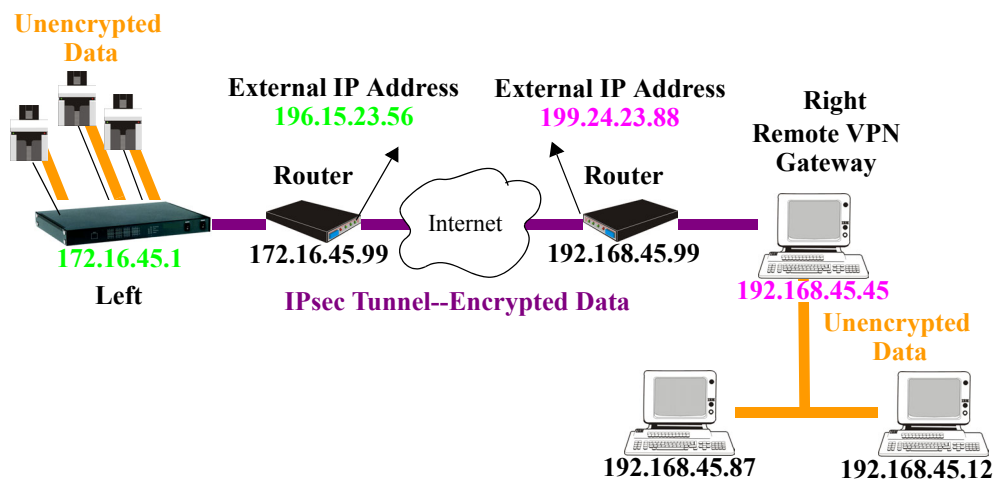
1. Set the serial port to **TCP Sockets**. Enable the **Listen for connection option**. On the **Hardware** tab, configure the **Speed**, **Flow Control**, **Stop Bits**, **Parity**, and **Bits** parameters so that they match the printer's port settings.
2. Save your settings and restart the serial port.
3. The print handling software needs to know the **Name** of the Terminal Server and the **TCP Port** number assigned to the printer serial port.

Configuring a Virtual Private Network

You can configure the Terminal Server to act as a Virtual Private Network (VPN) gateway using the IPsec protocol. Any of the following scenarios can be configured using one Terminal Server and a host/server running IPsec software or two Terminal Servers, each acting as the VPN gateway. All the examples have **NAT Traversal (NAT_T)** enabled, since both VPN gateways are running through routers.

Terminal Server-to-Host/Network

The following example shows how to configure an IPsec tunnel between serial devices connected to the Terminal Server 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.



1. Configure the IPsec tunnel in the Terminal Server:

Ipspec Tunnel

Name:

Authentication Method:

Secret:

Local Device (Terminal Server): ☒ Left ☐ Right

Local

IP Address:

External IP Address:

Next Hop:

Host/Network Address:

IPv4 Subnet Mask:

IPv6 Subnet Bits:

Remote

IP Address:

External IP Address:

Next Hop:

Host/Network Address:

IPv4 Subnet Mask:

IPv6 Subnet Bits:

Boot Action:

2. Use a utility (for example, Openswan's `newhostkey/showhostkey` utilities) to generate the RSA signature public key. Copy the public key portion to a file using the following format:

```
<description>=<keydata>
```

or just

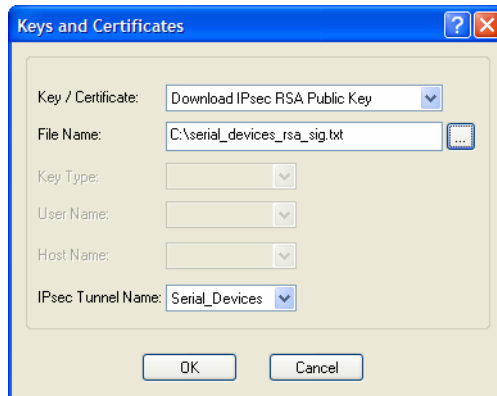
```
<keydata>
```

For example:

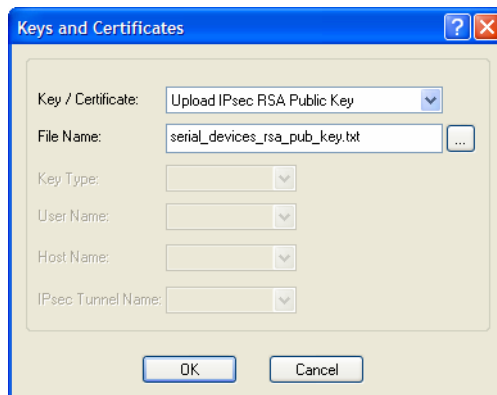
```
# RSA 1024 bits   scs48_vpn   Tue Jan  3 15:29:33 2006
lefttrnsigkey=0sAQOEmzSTdNv1ZUJW9UmPtUY84gM5AGEAOq9gUwFqnOUSeSfnuX1xPe+Mc+uf
XYvg1vxYZ0XhdIh1FwFeeIQLyRvD447mjriMFjJfheMUtHqOZhvWSE18ZfGEXNOo7yagZqLzjxu9
XJIA2SAGV+/LL3epPqW2fV5ORxVrf7uWn7I5FQ==
```

Note that the pound sign (#) indicates a comment line and all characters in that line are ignored. The key value itself should not have any carriage returns.

3. In the DeviceManager, select **Tools, Advanced, Keys and Certificates**. In the WebManager, select **Tools, Administration, Keys/Certificates**. Download the RSA signature file to the DeviceManager, specifying the IPsec tunnel it's for:



4. In the same **Keys and Certificates** window, upload the Terminal Server's RSA signature public key:

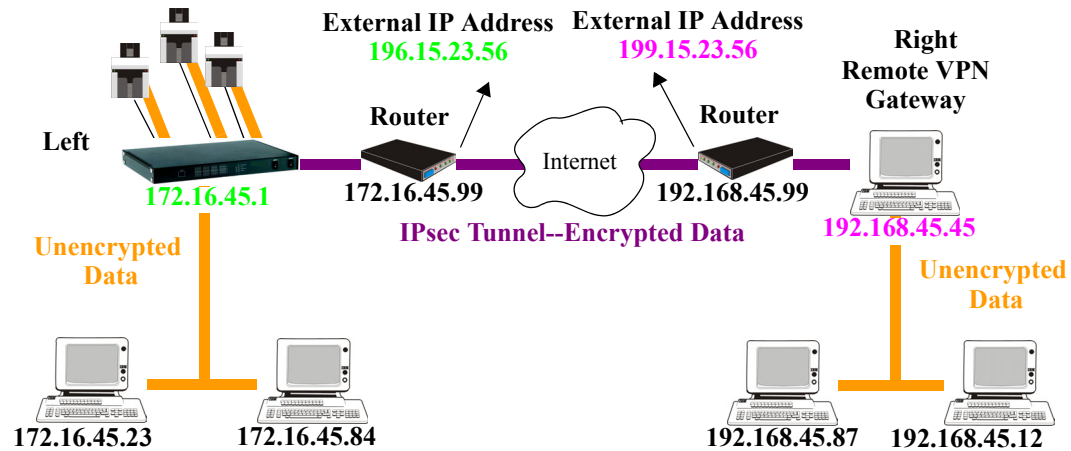


Install the Terminal Server's public key in the remote VPN gateway for the Serial_Devices IPsec tunnel.

5. 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 Terminal Server can be accessed by the VPN tunnel, since they are included in the network configuration as part of the **172.16.45.0** subnetwork.



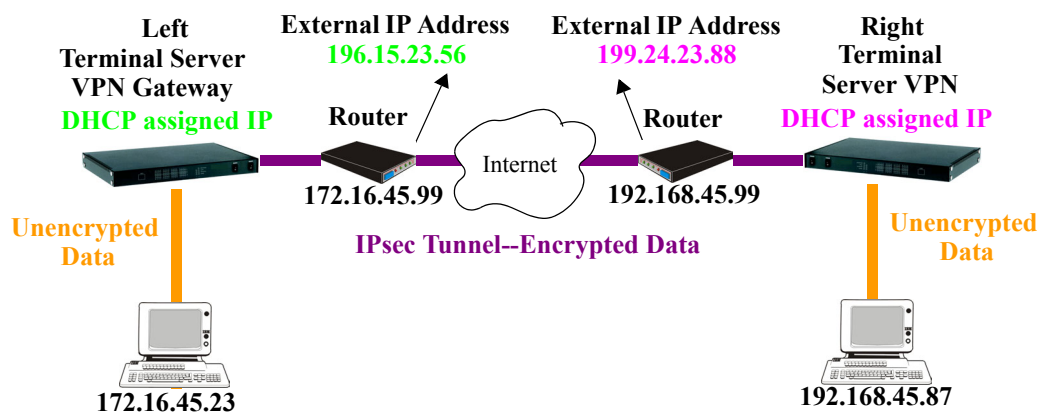
1. Configure the IPsec tunnel in the Terminal Server:

2. Click 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 Terminal Server, you need to add (append) the signer of the X.509 certificate to the CA list file and then download the file to the Terminal Server by selecting **Tools, Advanced, Keys and Certificates**. In the **Keys and Certificates** window, select **Download SSL/TLS CA** and the file name and click **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 Terminal Servers 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 Terminal Server VPN gateways have a DHCP assigned IP address.



1. The following window configures the Left Terminal Server VPN Gateway:

`%defaultroute` is entered for the **Local IP Address** because the IP address is DHCP assigned and is therefore subject to change.

- The following window configures the Right Terminal Server 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 contains eight dots. The 'Local Device (Terminal Server)' is set to 'Right'. The 'Local' section has the following values: IP Address: %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 the following values: IP Address: %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. 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.

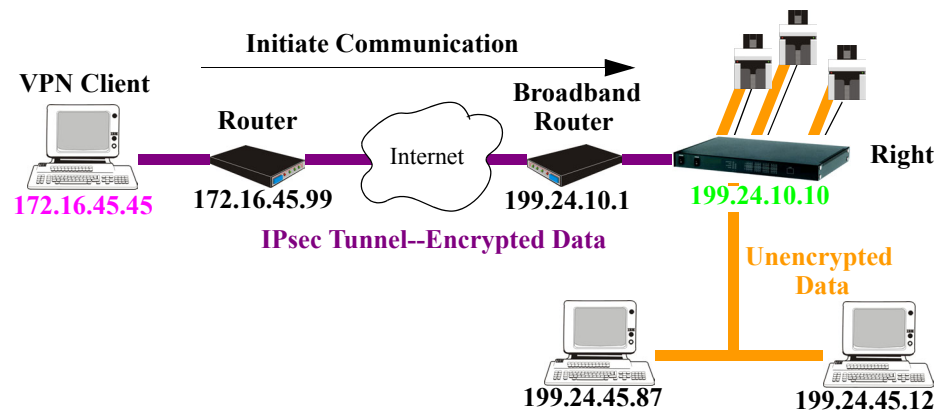
`%any` is entered for the **Remote IP Address** to indicate that it will accept a VPN connection from any host/network; this is necessary because the Left Terminal Server VPN gateway is DHCP assigned and cannot be known.

Also note that **Boot Action** on the Left Terminal Server VPN gateway is set to **Start**, meaning that it will try to initiate the VPN connection, while the **Boot Action** on the Right Terminal Server 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 Terminal Server will accept VPN connections from multiple VPN clients on private networks that want to access the public **199.24.0.0** subnet 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 Terminal Server:

The **Remote IP Address** field is **%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

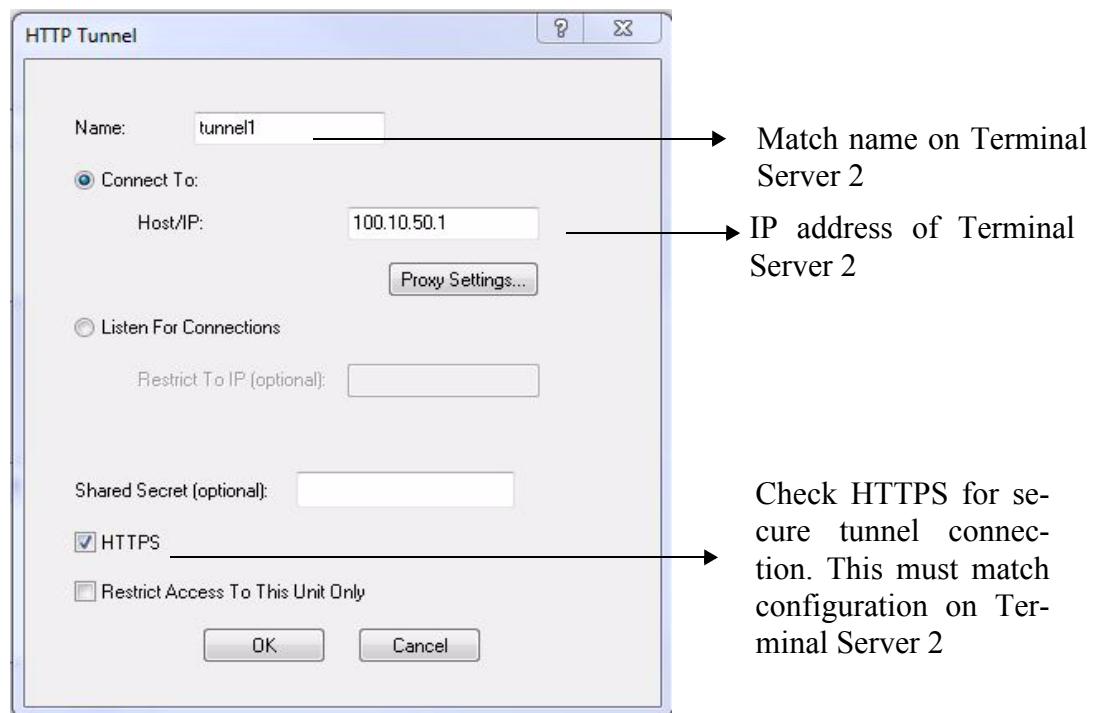
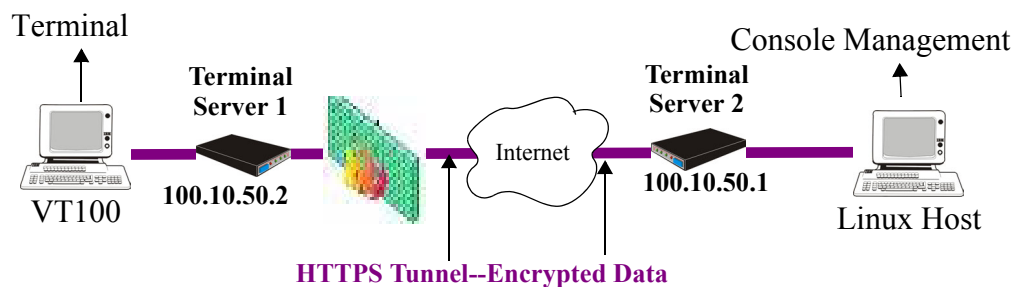
Note: When HTTP tunneling is used TCP and UDP ports 50000 and above are reserved and should not be configured by the user.

Serial-to Serial

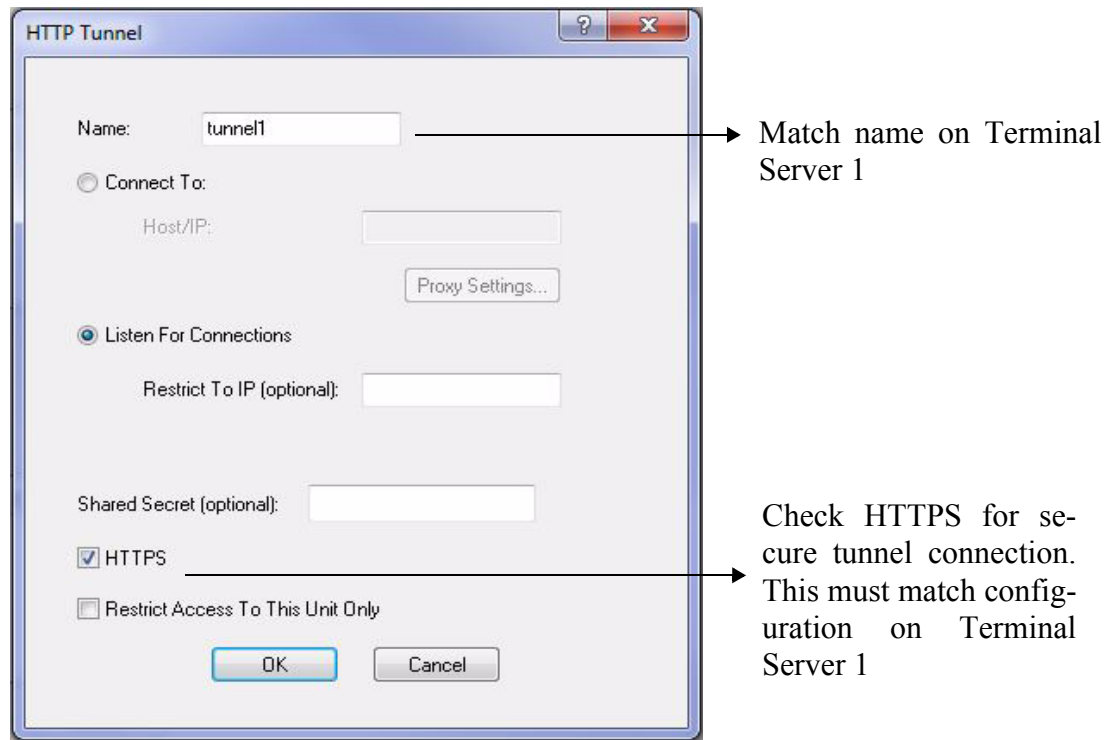
The following example will demonstrate how to set up a serial device (VT100 Terminal) to serial device (Linux host, console port) connection via an HTTPS tunnel. HTTPS will be used because data security is required. Terminal Server 1 is behind the firewall, so it will need to initiate the HTTP tunnel connection.

For more HTTP tunneling configuration parameters see [Configuring HTTP Tunnels](#)

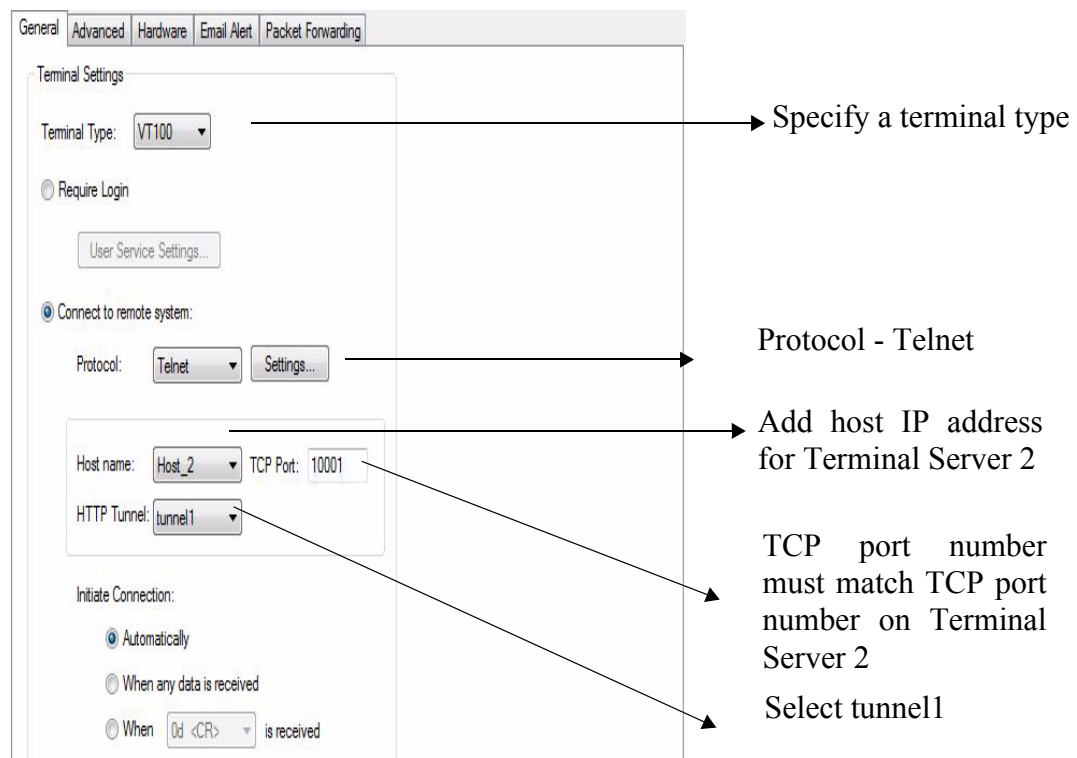
Configure a “connect to” HTTP tunnel on Terminal Server 1



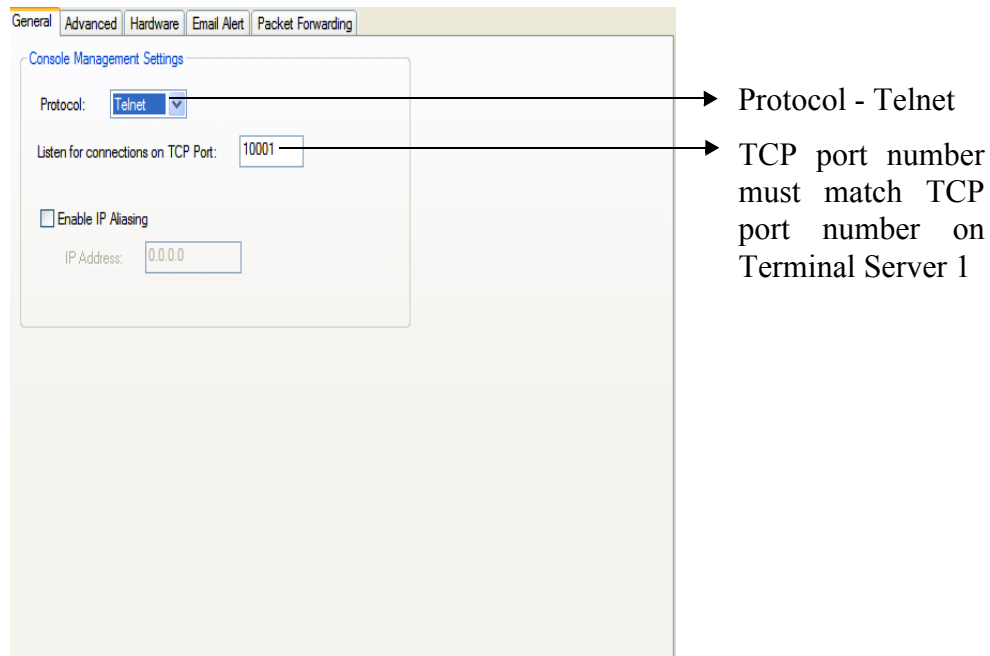
Configure a “Listen for connection” HTTP tunnel on Terminal Server 2



On Terminal Server 1, under *Serial port configuration*, select serial ports /Terminal profile.



On Terminal Server 2, *under serial port configuration*, select serial port and configure for Console Management profile..

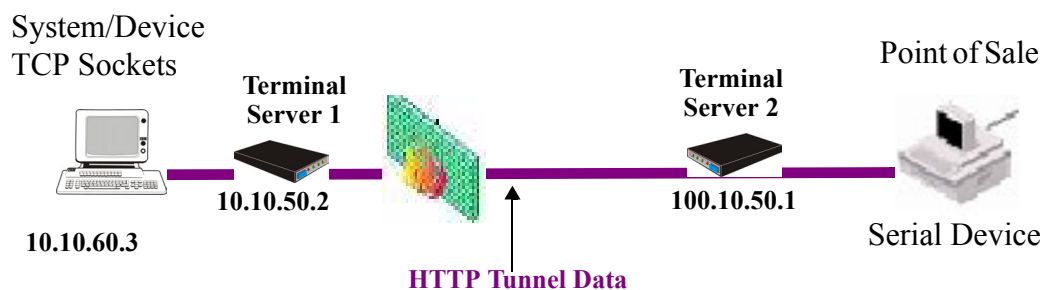


The setup for HTTP Tunnel serial-to-serial is now complete.

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 Terminal Server 1 is behind the firewall, it will need to initiate the tunnel connection to Terminal Server 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](#)



Configure a “connect to” HTTP tunnel on Terminal Server 1

The screenshot shows the 'HTTP Tunnel' configuration window. The 'Name' field is set to 'tunnel1'. The 'Connect To' radio button is selected, and the 'Host/IP' field contains '100.10.50.1'. The 'Listen For Connections' radio button is unselected. The 'Shared Secret (optional)' field is empty. The 'HTTPS' checkbox is unchecked, and the 'Restrict Access To This Unit Only' checkbox is also unchecked. The 'OK' and 'Cancel' buttons are at the bottom. Two arrows point from text labels to the 'Name' and 'Host/IP' fields.

Name: tunnel1

Match name on Terminal Server 1

Connect To:

Host/IP: 100.10.50.1

IP address of Terminal Server 2

Proxy Settings...

Listen For Connections

Restrict To IP (optional):

Shared Secret (optional):

HTTPS

Restrict Access To This Unit Only

OK Cancel

Configure a “Listen for connection” HTTP tunnel on Terminal Server 2

The screenshot shows the 'HTTP Tunnel' configuration window. The 'Name' field is set to 'tunnel1'. The 'Listen For Connections' radio button is selected. The 'Host/IP' field is empty. The 'Shared Secret (optional)' field is empty. The 'HTTPS' checkbox is unchecked, and the 'Restrict Access To This Unit Only' checkbox is also unchecked. The 'OK' and 'Cancel' buttons are at the bottom. One arrow points from a text label to the 'Name' field.

Name: tunnel1

Match name on Terminal Server 1

Connect To:

Host/IP:

Proxy Settings...

Listen For Connections

Restrict To IP (optional):

Shared Secret (optional):

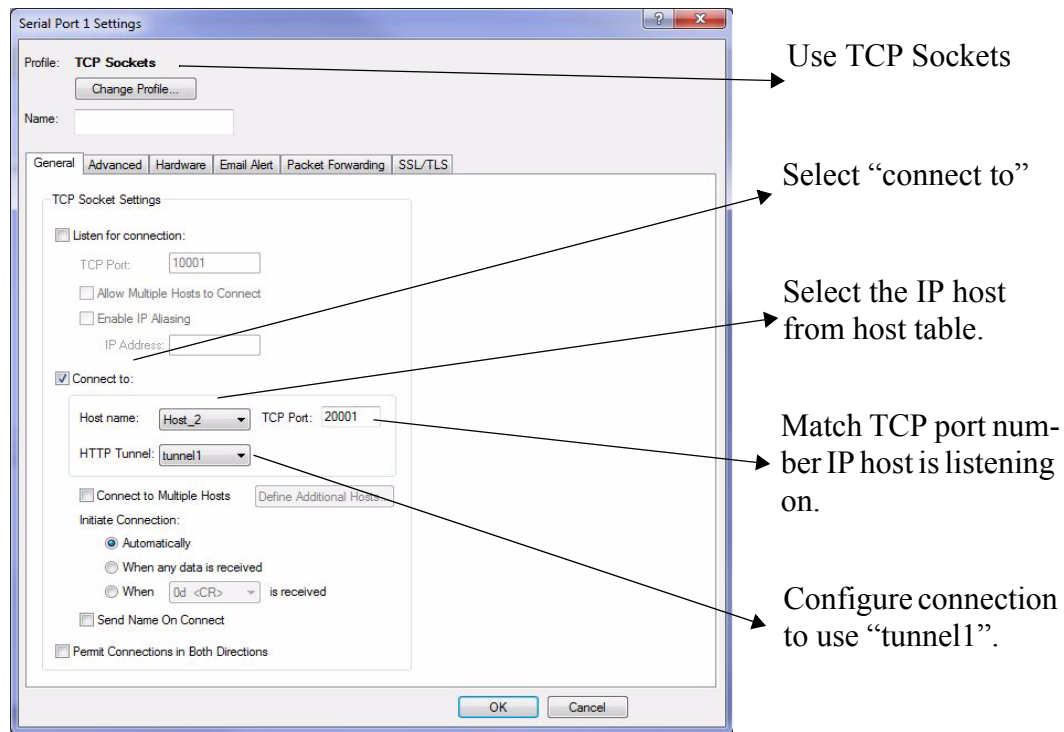
HTTPS

Restrict Access To This Unit Only

OK Cancel

Add The IP host to the host table on Terminal Server 2.

Configure the serial port on Terminal Server 2, as follows;



When Terminal Server 1 boots, it will establish an HTTP tunnel to Terminal Server 2.

Terminal Server 2 will initiate a connection between the serial device and the IP host. The connection will use the destination TCP port 20001.

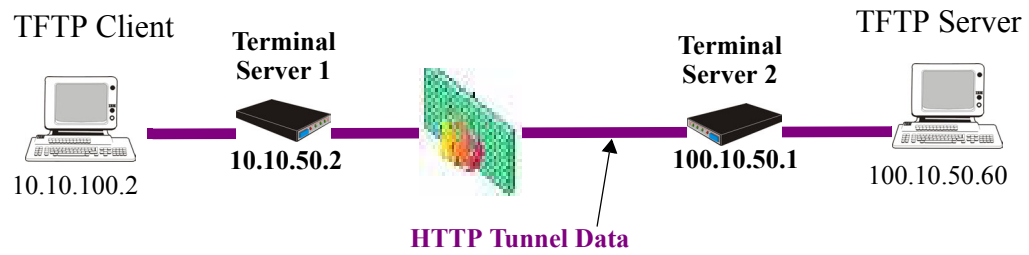
The setup for HTTP Tunnel Host-to-Serial is now complete.

Host-to Host

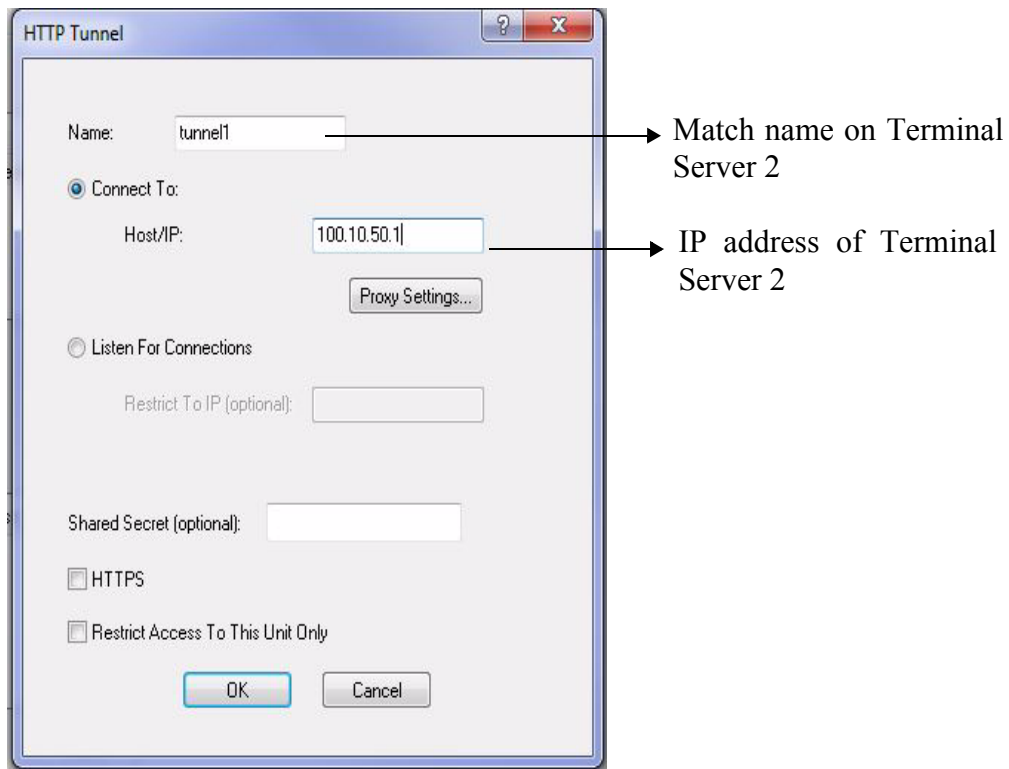
The following example will demonstrate how to setup an IP Host (10.10.100.2) to an IP Host (100.10.50.60) connection via an HTTP tunnel. In this example, the hosts are doing a TFTP transfer which uses the UDP protocol.

Terminal Server 1 is behind the firewall, so it will need to initiate the tunnel connection to Terminal Server 2.

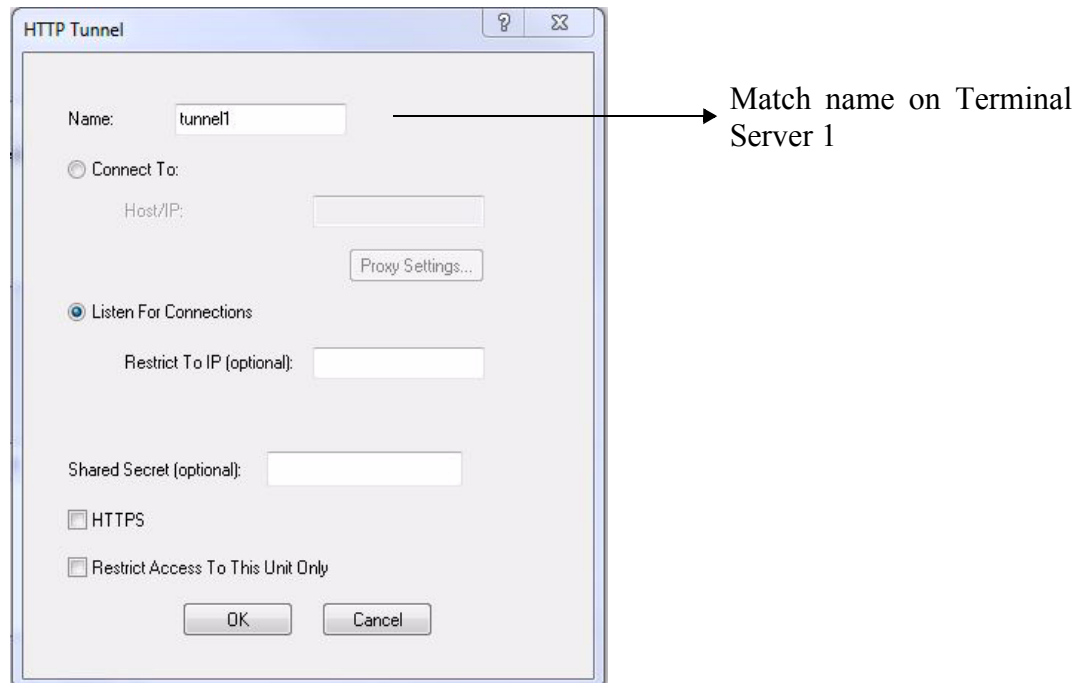
For more HTTP tunneling configuration parameters see [Configuring HTTP Tunnels](#)



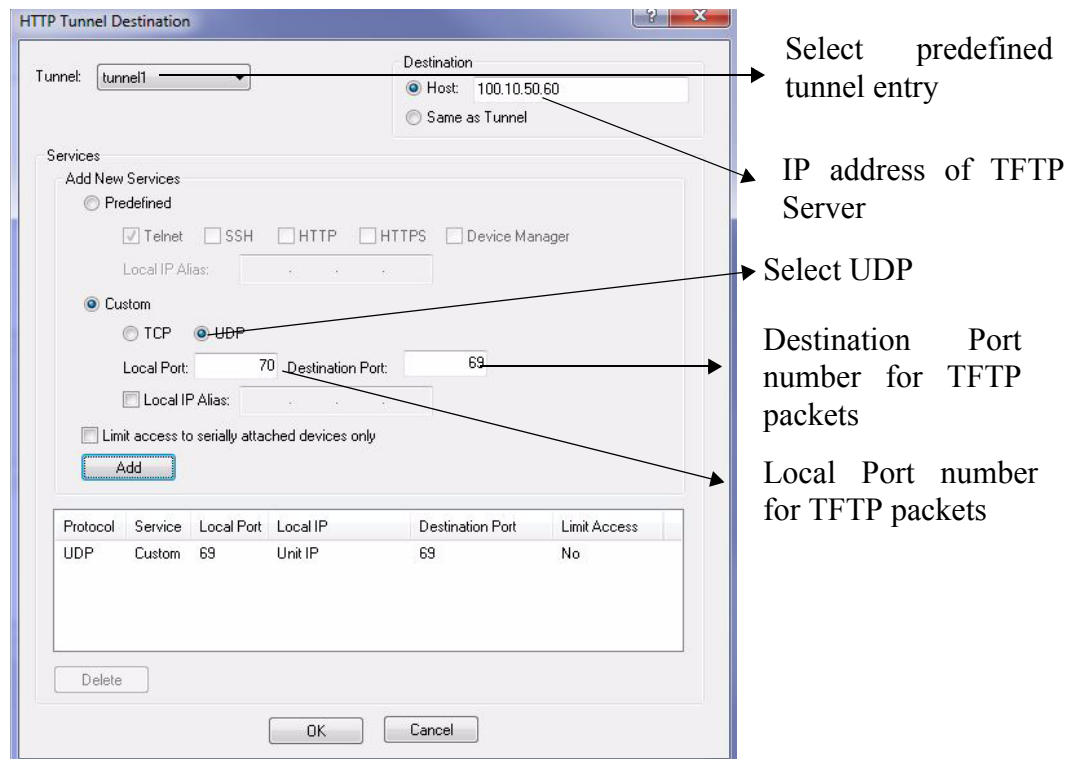
Configure a “connect to” HTTP tunnel on Terminal Server 1



Configure a “Listen for connection” HTTP tunnel.



On Terminal Server 1, under *HTTP Tunnel*, add a Tunnel destination.



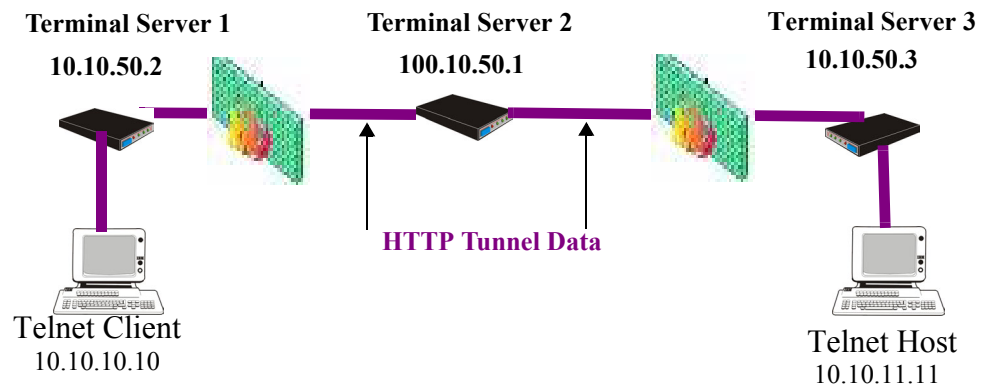
The setup for HTTP Tunnel Host-to-Host is now complete.

Tunnel Relay

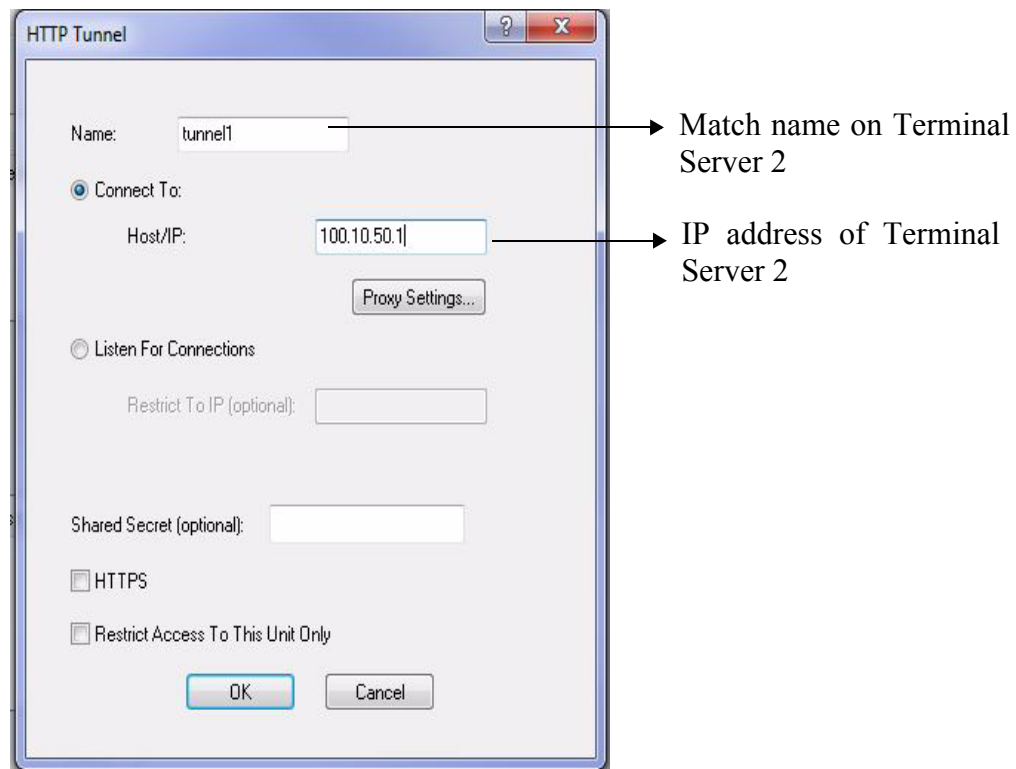
The following example will demonstrate how to setup an IP host (10.10.10.10) to an IP Host (10.10.11.11) connection using HTTP tunnels when both hosts are sitting behind a firewall. To do this, a third Terminal Server which is not behind a firewall is required.

Because Terminal Server 1 and Terminal Server 3 are both behind a firewall, each will need to initiate a connection to Terminal Server 2 who is in the open.

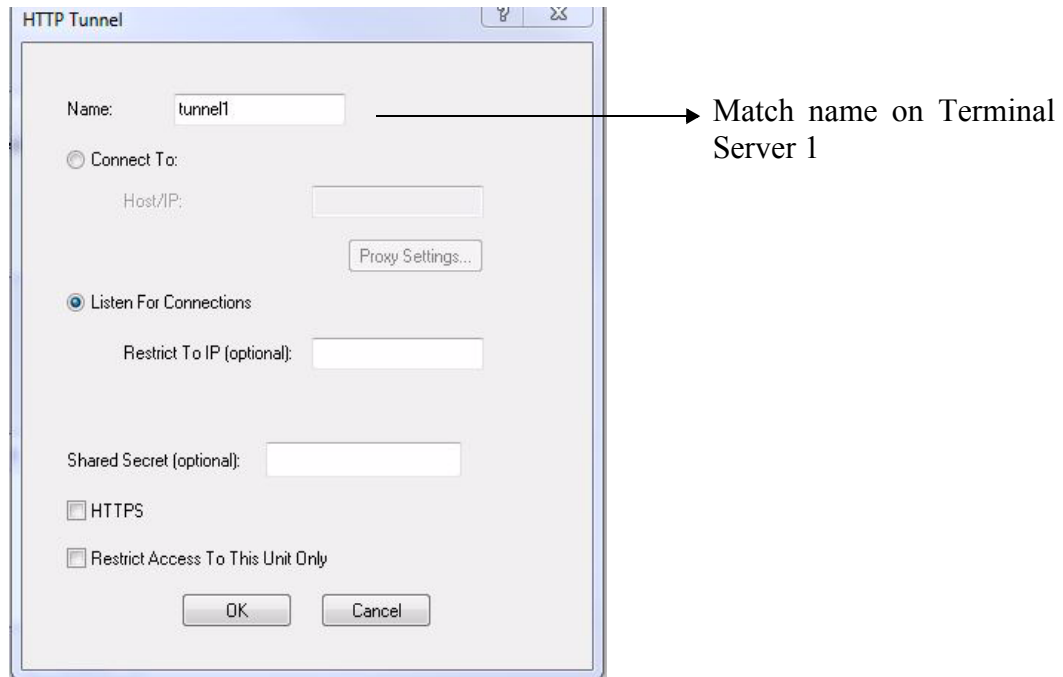
For more HTTP tunneling configuration parameters see [Configuring HTTP Tunnels](#)



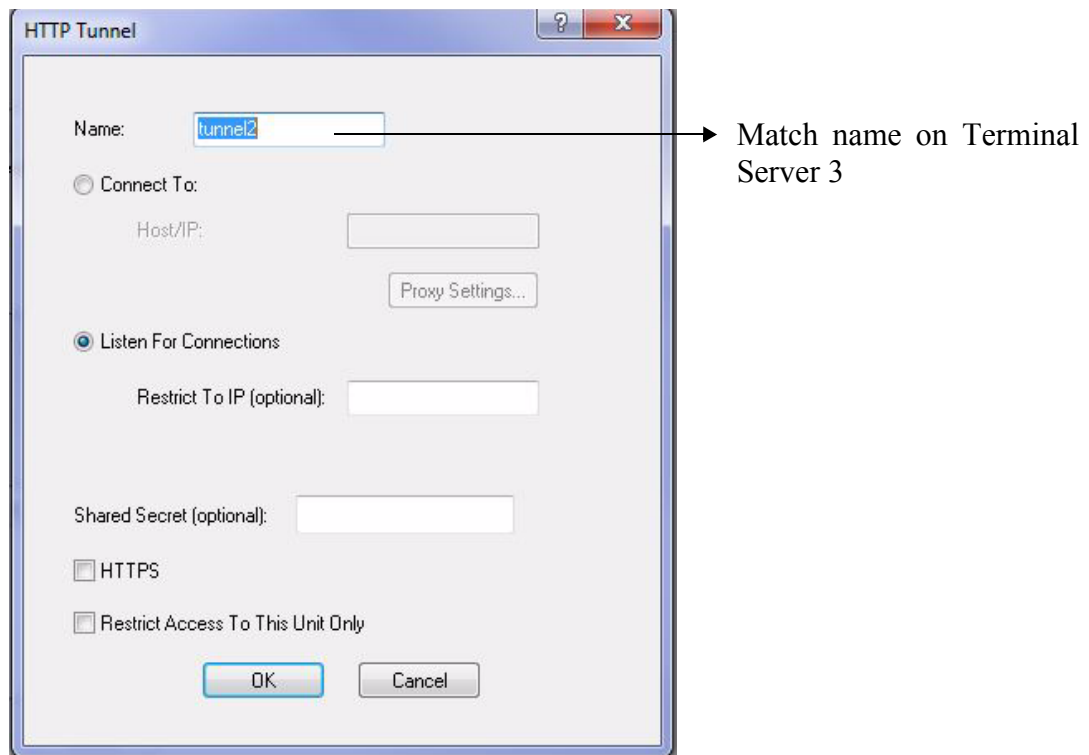
Configure a “connect to” HTTP tunnel on Terminal Server 1



Configure a “Listen for connection” HTTP tunnel on Terminal Server 2



Configure a second “Listen for connection to Terminal Server



Configure a “connect to” HTTP tunnel on Terminal Server 3

Match name on Terminal Server 2

IP address of Terminal Server 2

On Terminal Server 1, *under HTTP Tunnel*, add a Tunnel destination

Select tunnel1

Select Same as Tunnel

Select TCP

Destination port number to be used by Terminal Server 1 for communications. Default starts at 40001.

This is the port number the telnet client will use.

Protocol	Service	Local Port	Local IP	Destination Port	Limit Access
TCP	Custom	40002	Unit IP	40001	No

On Terminal Server 2, under *HTTP Tunnel*, add a Tunnel destination.

The screenshot shows the 'HTTP Tunnel Destination' dialog box. The 'Tunnel' dropdown is set to 'tunnel2'. The 'Destination' section has 'Host' selected with the IP address '10.10.11.11'. Under 'Services', 'Predefined' is selected, and 'Telnet' is checked. The 'Local Port' is set to '40001' and the 'Destination Port' is set to '23'. The 'Protocol' is set to 'TCP'. A table at the bottom shows the configuration: Protocol: TCP, Service: Custom, Local Port: 40001, Local IP: Unit IP, Destination Port: 23, Limit Access: No. Annotations point to the 'tunnel2' dropdown, the 'Host' IP address, the 'TCP' radio button, the 'Destination Port' field, and the 'Local Port' field.

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 Terminal Server 2 for commu-

Protocol	Service	Local Port	Local IP	Destination Port	Limit Access
TCP	Custom	40001	Unit IP	23	No

Note: This value must match destination port number on Terminal Server 1

The setup for HTTP Tunnel Relay is now complete.

15 SSL/TLS Ciphers

Valid SSL/TLS Ciphers

This chart displays all of the valid SSL/TLS cipher combinations.

Full Name	Key-Exchange	Authentication	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	Authentication	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
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

A RADIUS and TACACS+

Introduction

This chapter describes the parameters that can be passed to the Terminal Server when a user logs into the Terminal Server (serial port set to profile **Terminal**) from external authentication RADIUS and TACACS+ servers.

RADIUS

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 Terminal Server parameters if the user has also been set up as a local user in the Terminal Server, 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 Terminal Server from a RADIUS server in response to an successful authentication request.

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 Terminal Server'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 Terminal Server itself then a port number of 0 is sent.

Type	Name		Description
6	Service-Type	Response	<p>Indicates the service to use to connect the user to the Terminal Server. A value of 6 indicates administrative access to the Terminal Server. Supported values are:</p> <ul style="list-style-type: none"> • 1—Login • 3—Callback-Login <p>Equivalent to the Terminal Server User Service set by Type 15, Login-Service.</p> <ul style="list-style-type: none"> • 2—Framed • 4—Callback-Framed <p>Equivalent to the Terminal Server 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 Terminal Server User Service DSprompt.</p> <ul style="list-style-type: none"> • 6—Administrative User • 11—Callback Administrative User <p>Equivalent to Terminal Server User Service DSprompt and the User gets Admin privileges.</p>
7	Framed-Protocol	Response	<p>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:</p> <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	<p>Indicates a compression protocol to be used for the PPP or SLIP link. Supported value is:</p> <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	<p>Indicates the Terminal Server User Service to use to connect the user a host. Supported values are:</p> <ul style="list-style-type: none"> • 0—Telnet • 1—Rlogin • 2—TCP Clear • 5—SSH • 6—SSL Raw

Type	Name		Description
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 Terminal Server will add routes to the user's PPP interface in the same order they were received
25	Class	Response	Received attributes are send in the Accounting Reply messages.
26	Vendor-Specific	Response	<p>The Black Box defined attributes for line access rights and user level. See BLACK BOX® 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: Blackbox-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: Blackbox-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: Blackbox-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 Terminal Server 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.

Type	Name		Description
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.
87	NAS-Port-Id	Response	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 Terminal Server management session. For DeviceManager sessions: "DEVMGR" For HTTP sessions: "HTTP"
95	NAS-IPv6-Address	Response	The IPv6 address of the Terminal Server.
96	Framed-Interface-Id	Response	The remote IPv6 interface identifier for the remote end of the PPP link.
98	Login-IPv6-Host	Response	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 Terminal Server 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 Terminal Server 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 Terminal Server LAN interface.
5	NAS-Port	Port Line number of Terminal Server.
6	Service-Type	<p>Indicates the service to use to connect the user to the Terminal Server. A value of 6 indicates administrative access to the Terminal Server. Supported values are:</p> <ul style="list-style-type: none"> • 1—Login • 3—Callback-Login <p>Equivalent to the Terminal Server User Service set by Type 15, Login-Service.</p> <ul style="list-style-type: none"> • 2—Framed • 4—Callback-Framed <p>Equivalent to the Terminal Server 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 Terminal Server User Service DSPrompt.</p> <ul style="list-style-type: none"> • 6—Administrative User • 11—Callback Administrative User <p>Equivalent to Terminal Server 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.

Type	Name	Description
48	Acct-Output-Packets	Number of packets which were transmitted to the user during this session.
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.
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 DeviceManager sessions: “DEVMGR” For HTTP sessions: “HTTP”
95	NAS-IPv6-Address	The IPv6 address of the Terminal Server
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 Terminal Server 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 Terminal Server are discarded. Below is a list of the RADIUS parameters and their Terminal Server parameters:

RADIUS Parameter	Terminal Server Parameter
Service-Type	This has no Terminal Server 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 Terminal Server.
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.

BLACK BOX® RADIUS Dictionary Example

The Terminal Server has defined Vendor Specific RADIUS attributes in order for the RADIUS server to be configured to support the Terminal Server 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 Black Box defined attributes for the RADIUS server for a 4-port Terminal Server (although the dictionary can contain 48 ports, even if they are not all defined):

```
# Blackbox dictionary.
#
#       Black Box Corporation
#       http://www.blackbox.com/
#
#       Enable by putting the line "$INCLUDE dictionary.blackbox" 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   Blackbox           1966
```

```
#   Blackbox Extensions
```

ATTRIBUTE	Blackbox-Clustered-Port-Access	99	integer	Blackbox
ATTRIBUTE	Blackbox-User-Level	100	integer	Blackbox
ATTRIBUTE	Blackbox-Line-Access-Port-1	101	integer	Blackbox
ATTRIBUTE	Blackbox-Line-Access-Port-2	102	integer	Blackbox
ATTRIBUTE	Blackbox-Line-Access-Port-3	103	integer	Blackbox
ATTRIBUTE	Blackbox-Line-Access-Port-4	104	integer	Blackbox
ATTRIBUTE	Blackbox-Line-Access-Port-5	105	integer	Blackbox
ATTRIBUTE	Blackbox-Line-Access-Port-6	106	integer	Blackbox
ATTRIBUTE	Blackbox-Line-Access-Port-7	107	integer	Blackbox
ATTRIBUTE	Blackbox-Line-Access-Port-8	108	integer	Blackbox
ATTRIBUTE	Blackbox-Line-Access-Port-9	109	integer	Blackbox
ATTRIBUTE	Blackbox-Line-Access-Port-10	110	integer	Blackbox
ATTRIBUTE	Blackbox-Line-Access-Port-11	111	integer	Blackbox
ATTRIBUTE	Blackbox-Line-Access-Port-12	112	integer	Blackbox
ATTRIBUTE	Blackbox-Line-Access-Port-13	113	integer	Blackbox
ATTRIBUTE	Blackbox-Line-Access-Port-14	114	integer	Blackbox
ATTRIBUTE	Blackbox-Line-Access-Port-15	115	integer	Blackbox
ATTRIBUTE	Blackbox-Line-Access-Port-16	116	integer	Blackbox
ATTRIBUTE	Blackbox-Line-Access-Port-17	117	integer	Blackbox
ATTRIBUTE	Blackbox-Line-Access-Port-18	118	integer	Blackbox
ATTRIBUTE	Blackbox-Line-Access-Port-19	119	integer	Blackbox
ATTRIBUTE	Blackbox-Line-Access-Port-20	120	integer	Blackbox
ATTRIBUTE	Blackbox-Line-Access-Port-21	121	integer	Blackbox
ATTRIBUTE	Blackbox-Line-Access-Port-22	122	integer	Blackbox
ATTRIBUTE	Blackbox-Line-Access-Port-23	123	integer	Blackbox
ATTRIBUTE	Blackbox-Line-Access-Port-24	124	integer	Blackbox
ATTRIBUTE	Blackbox-Line-Access-Port-25	125	integer	Blackbox
ATTRIBUTE	Blackbox-Line-Access-Port-26	126	integer	Blackbox
ATTRIBUTE	Blackbox-Line-Access-Port-27	127	integer	Blackbox
ATTRIBUTE	Blackbox-Line-Access-Port-28	128	integer	Blackbox
ATTRIBUTE	Blackbox-Line-Access-Port-29	129	integer	Blackbox

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

Blackbox Clustered Port Access Values

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

Blackbox User Level Values

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

Blackbox Line Access Right Values

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

VALUE	Blackbox-Line-Access-Port-4	Disabled	0
VALUE	Blackbox-Line-Access-Port-4	Read-Write	1
VALUE	Blackbox-Line-Access-Port-4	Read-Input	2
VALUE	Blackbox-Line-Access-Port-4	Read-Input-Write	3
VALUE	Blackbox-Line-Access-Port-4	Read-Output	4
VALUE	Blackbox-Line-Access-Port-4	Read-Output-Write	5
VALUE	Blackbox-Line-Access-Port-4	Read-Output-Input	6
VALUE	Blackbox-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 Terminal Server parameters if the user has also been set up as a local user in the Terminal Server, 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 Terminal Server after authentication for users accessing the Terminal Server from the serial side and users accessing the Terminal Server from the Ethernet side connections.

Accessing the Terminal Server Through a Serial Port Users

This section describes the attributes which will be accepted by the Terminal Server 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 Terminal Server privilege level.
Blackbox_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 Terminal Server. If no value is specified, DSPrompt is the default User Service.
service = telnet { addr = port = }	IPv4 or IPv6 address TCP port number	Settings when Blackbox_User_Service is set to 0.
service = rlogin { addr = }	IPv4 or IPv6 address	Settings when Blackbox_User_Service is set to 1.

Name	Value(s)	Description
service = tcp_clear { addr = port = }	IPv4 or IPv6 address TCP port number	Settings when Blackbox_User_Service is set to 2.
service = slip { routing = addr = }	true (Send and Listen) false (None) IPv4 or IPv6 address	Settings when Blackbox_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 Blackbox_User_Service is set to 4.
service = ssh { addr = port = }	IPv4 or IPv6 address TCP port number	Settings when Blackbox_User_Service is set to 5.
service = ssl_raw { addr = port = }	IPv4 or IPv6 address TCP port number	Settings when Blackbox_User_Service is set to 6.

Accessing the Terminal Server Through a Serial Port - Example

The following example shows the parameters that can be set for users who are accessing the Terminal Server 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 seconds

idletime=x            # x = Idle timeout in seconds

Blackbox_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 Blackbox_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 Terminal Server from the Network

This section describes the attributes which will be accepted by the Terminal Server 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 Terminal Server privilege level.
Blackbox_Line_Access_#	# = port number 0 (Disabled) 1 (ReadWrite) 2 (ReadInput) 3 (ReadInputWrite) 4 (ReadOutput) 5 (ReadOutputWrite) 6 (ReadOutputInput) 7 (ReadOutputWrite)	For the specified line, provides the User's Line Access rights.
timeout	0-4294967	Session timeout in seconds.
idletime	0-4294967	Idle timeout in seconds
Blackbox_Clustered_Port_Access	0 (Disabled) 1 (Enabled)	Control access to clustered ports.

Accessing the Terminal Server from the Network- Example

The following example shows the parameters that can be set for users who are accessing the Terminal Server 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)

Blackbox_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 seconds

idletime=x              # x = Idle timeout in seconds

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

Note: Users who are accessing the Terminal Server 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)

Blackbox_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)

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

B Setting Jumpers

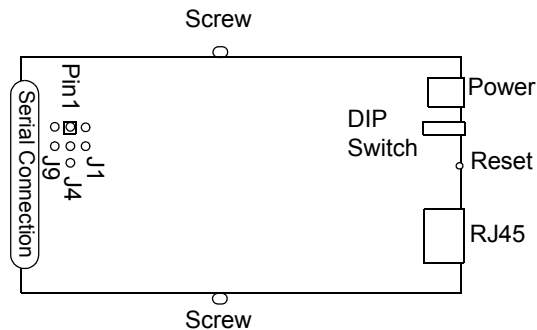
Introduction

The Terminal Server contains jumpers that you might need to set before you configure it and put it into production. You can set the power out pin, pin 9, to a fixed 5V DC output or to the external adapter output; this can range from 9-30V DC (if an external adapter is shipped with the Terminal Server, it has a 12V DC output); maximum output power is 1 (one) watt per a serial port. By default, the power out pin is set to no power. You can set the Terminal Server line termination to **on** or **off** (this is **off** by default) if you are using EIA-422/485.

Terminal Server 1-Port DB25 Male/Female

To change the settings, do the following:

1. Unplug the Terminal Server from the electrical outlet and disconnect everything from the box.
2. Open the case by unscrewing the two side screws, one on each side, and lifting off the top of the case. You should see the following:

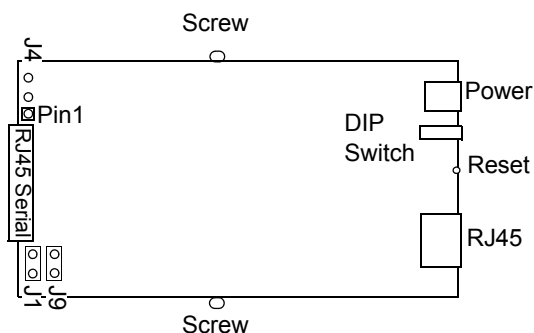


3. To change the power pin out, locate J4. For the fixed 5V DC output, jumper pins 1 and 2. For the output to equal the external adapter input, jumper pins 2 and 3.
4. To turn line termination **on**, locate and jumper both J1 and J9.
5. Close the Terminal Server case by replacing the case lid and the two screws. You can now power it on with the new settings.

Terminal Server 1-Port RJ45

To change the settings, do the following:

1. Unplug the Terminal Server from the electrical outlet and disconnect everything from the box.
2. Open the case by unscrewing the two side screws, one on each side, and lifting off the top of the case. You should see the following:

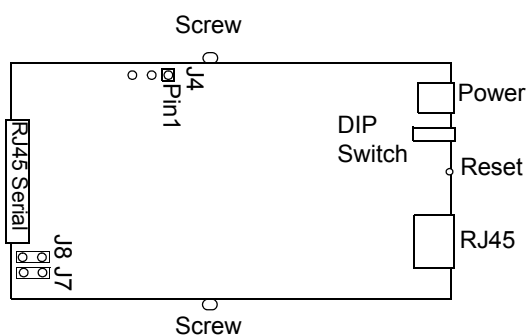


3. To change the power pin out, locate J4. For the fixed 5V DC output, jumper pins 1 and 2. For the output to equal the external adapter input, jumper pins 2 and 3.
4. To turn line termination **on**, locate and jumper both J1 and J9.
5. Close the Terminal Server case by replacing the case lid and the two screws. You can now power it on with the new settings.

PoE Device Server 1-Port

To change the settings, do the following:

1. Unplug the Terminal Server from the electrical outlet and disconnect everything from the box.
2. Open the case by unscrewing the two side screws, one on each side, and lifting off the top of the case. You should see the following:

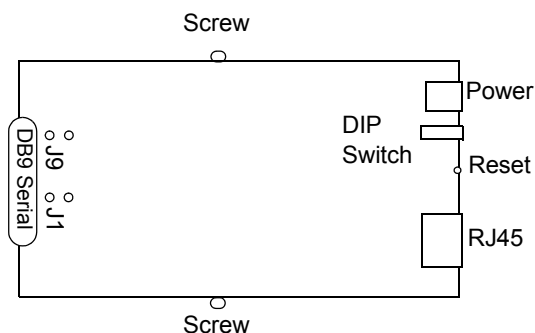


3. To change the power pin out, locate J4. For the fixed 5V DC output, jumper pins 1 and 2. For the output to equal the external adapter input, jumper pins 2 and 3.
4. To turn line termination **on**, locate and jumper both J7 and J8.
5. Close the Terminal Server case by replacing the case lid and the two screws. You can now power it on with the new settings.

Terminal Server 1-Port DB9

To change the settings, do the following:

1. Unplug the Terminal Server from the electrical outlet and disconnect everything from the box.
2. Open the case by unscrewing the two side screws, one on each side, and lifting off the top of the case. You should see the following:

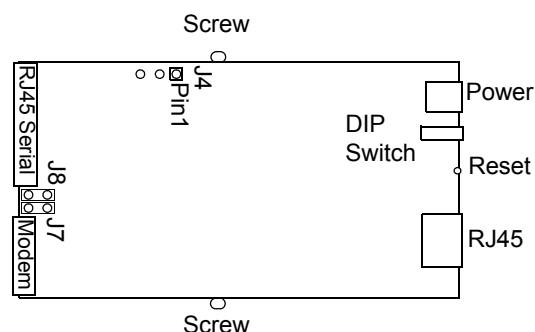


3. To turn line termination **on**, locate and jumper both J1 and J9.
4. Close the Terminal Server case by replacing the case lid and the two screws. You can now power it on with the new settings.

Modem Device Server 1-Port

To change the settings, do the following:

1. Unplug the Terminal Server from the electrical outlet and disconnect everything from the box.
2. Open the case by unscrewing the two side screws, one on each side, and lifting off the top of the case. You should see the following:

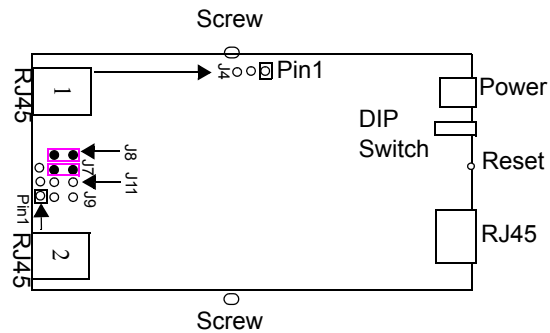


3. To change the power pin out, locate J4. For the fixed 5V DC output, jumper pins 1 and 2. For the output to equal the external adapter input, jumper pins 2 and 3.
4. To turn line termination **on**, locate and jumper both J7 and J8.
5. Close the Terminal Server case by replacing the case lid and the two screws. You can now power it on with the new settings.

2-Port Terminal Server

To change the settings, do the following:

1. Unplug the Terminal Server from the electrical outlet and disconnect everything from the box.
2. Open the case by unscrewing the two side screws, one on each side, and lifting off the top of the case. You should see the following:

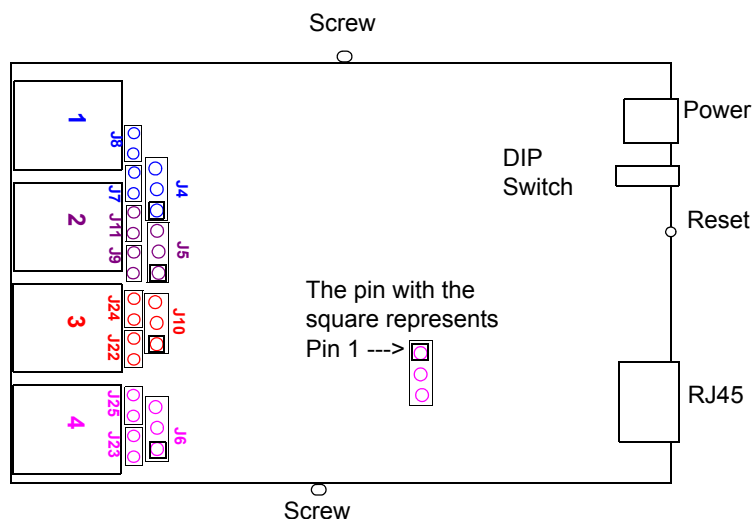


3. To change the power pin out, locate the set of three pins associated with the line you want to set (Line 1 is J4; Line 2 is the set the three pins just to the left of port 2). For the fixed 5V DC output, jumper pins 1 and 2. For the output to equal the external adapter input, jumper pins 2 and 3.
4. To turn line termination **on** for Line 1, locate and jumper both J7 and J8 (as shown in the diagram). To turn line termination **on** for Line 2, locate and jumper both J11 and J9.
5. Close the Terminal Server case by replacing the case lid and the two screws. You can now power it on with the new settings.

4-Port Desktop Secure Terminal Server

To change the settings, do the following:

1. Unplug the Terminal Server from the electrical outlet and disconnect everything from the box.
2. Open the case by unscrewing the two side screws, one on each side, and lifting off the top of the case. You should see the following:



3. The following table describes how to jumper the pins for line termination, fixed 5V output, and for output equal to the external adapter input:

Port/Line #	Line Termination	5V Output	Input Volt Output
1	Jumper J7 and J8	J4, jumper pins 1 & 2	J4, jumper pins 2 & 3
2	Jumper J9 and J11	J5, jumper pins 1 & 2	J5, jumper pins 2 & 3
3	Jumper J22 and J24	J10, jumper pins 1 & 2	J10, jumper pins 2 & 3
4	Jumper J23 and J25	J6, jumper pins 1 & 2	J6, jumper pins 2 & 3

4. Close the Terminal Server case by replacing the case lid and the two screws. You can now power it on with the new settings.

C Accessories

Introduction

This chapter provides information about peripheral Terminal Server options that can be ordered separately from the product. Contact your sales representative to find out how to order the products listed in this appendix.

Installing a BLACK BOX® PCI Card

This sections describes how to install the BLACK BOX® PCI modem card in your Secure Console Server rack mount model.



Secure Console Server
PCI Modem Card

The location and brackets are slightly different for the 32-port rack mount models, but the basic installation concept is the same. The PCI modem bracket is found on the serial side of the 8-port/16-port/32-port models.

Note: Do not touch any of the components within the Secure Console Server while performing the PCI modem card installation.

1. Unscrew the six screws on the top of the Secure Console Server.



2. Unscrew the four screws along the bottom of the serial side of the Secure Console Server. On the SCS 8-port/16-port/32-port models, this includes the screw that is at the bottom of the PCI face plate.



3. Slide the top of the Secure Console Server off of the chassis.
4. Carefully holding the bracket just behind the face plate, unscrew the two screws at the top of the 8-port/16-port/32-port removable face plate.



The 8-port/16-port/32-port models are displayed below with the face plate and bracket taken apart.



5. Unscrew the screw in the bracket. The 8-port/16-port/32-port bracket is shown below.



6. Slide the PCI modem card into the bracket.



7. The black bracket should then fit on the inside of the PCI modem card bracket. Align the adapter card bracket and then insert the screw and tighten it to keep it firmly in place.



Note: You must attach the bracket to the PCI modem card before you slide it into the PCI slot.

8. You can now replace the top of the Secure Console Server chassis by aligning it and sliding it into the base. You can throw away the face plate, as you will not be needing it.



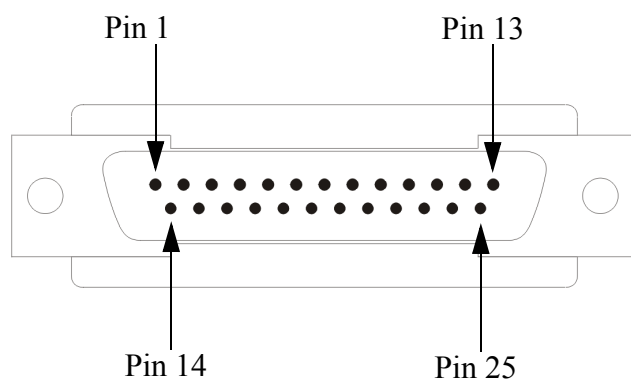
9. Replace all the screws on the top and the serial side of the Secure Console Server.

D Pinouts and Cabling Diagrams

Serial Pinouts

DB25 Male

This section defines the pinouts for the DB25 male connection used on the 1-port Terminal Server. The power out pin, Pin 9, is available in the Secure Device Server model only.



The following table provides pinout information:

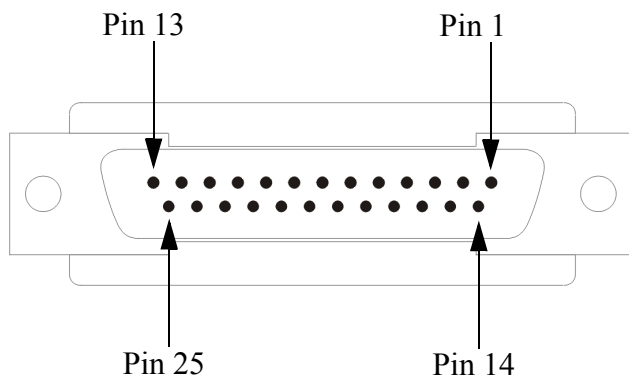
Pinout	EIA-232	EIA-422	EIA-485 Full Duplex	EIA-485 Half Duplex
1	Shield	Shield	Shield	Shield
2 (out)	TxD			
3 (in)	RxD			
4 (out)	RTS			
5 (in)	CTS			
6 (in)	DSR			
7	GND	GND	GND	GND
8 (in)	DCD			
9	Power out	Power out	Power out	Power out
12	Power in	Power in	Power in	Power in
13		CTS-		
14		TxD+	TxD+	DATA+
15		TxD-	TxD-	DATA-

Pinout	EIA-232	EIA-422	EIA-485 Full Duplex	EIA-485 Half Duplex
18		RTS+		
19		RTS-		
20 (out)	DTR			
21		RxD+	RxD+	
22		RxD-	RxD-	
25		CTS+		

The power in pin, pin 12, can be 9-30V DC.

DB25 Female

This section defines the pinouts for the DB25 female connection used on the 1-port Terminal Server. The power out pin, Pin 9, is available in the Secure Device Server model only.



The following table provides pinout information:

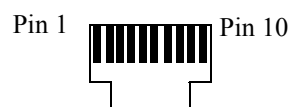
Pinout	EIA-232	EIA-422	EIA-485 Full Duplex	EIA-485 Half Duplex
1	Shield	Shield	Shield	Shield
2 (in)	RxD			
3 (out)	TxD			
4 (in)	CTS			
5 (out)	RTS			
6 (out)	DTR			
7	GND	GND	GND	GND
8 (in)	DCD			
9	Power out	Power out	Power out	Power out
12	Power in	Power in	Power in	Power in
13		RTS-		
14		RxD+	RxD+	

Pinout	EIA-232	EIA-422	EIA-485 Full Duplex	EIA-485 Half Duplex
15		RxD-	RxD-	
18		CTS+		
19		CTS-		
20 (in)	DSR			
21		TxD+	TxD+	DATA+
22		TxD-	TxD-	DATA-
25		RTS+		

The power in pin, pin 12, can be 9-30V DC.

RJ45

This section defines the pinouts for the RJ45 connection. 1-port, 2-port, and 4-port desktop models have a 10-pin RJ45 connector and all rack mount models have an 8-pin RJ45 connector.



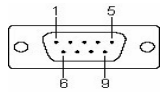
The following table provides pinout information:

Pinout 10-pin	Pinout 8-pin	EIA-232	EIA-422	EIA-485 Full Duplex	EIA-485 Half Duplex
1		Power In	Power In	Power In	Power In
2 (in)	1	DCD			
3 (out)	2	RTS	TxD+	TxD+	DATA+
4 (in)	3	DSR			
5 (out)	4	TxD	TxD-	TxD-	DATA-
6 (in)	5	RxD	RxD+	RxD+	
7	6	GND	GND	GND	GND
8 (in)	7	CTS	RxD-	RxD-	
9 (out)	8	DTR			
10		Power out	Power out	Power out	Power out

The power in pin, Pin 1, can be 9-30V DC. The 2-port Terminal Server has power in on Port 2 only. The 4-port Terminal Server has power in on Port 4 only.

DB9 Male

This section defines the pinouts for the DB9 male connection used on the 1-port Terminal Server.

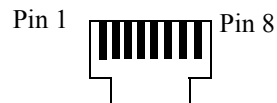


The following table provides pinout information:

Pinout 9-pin	EIA-232	EIA-422/485 Full Duplex	EIA-485 Half Duplex
1 (in)	DCD		
2 (in)	RxD	RxD+	
3 (out)	TxD	TxD+	TxD+/RxD+
4 (out)	DTR		
5	GND	GND	GND
6 (in)	DSR	RxD-	
7	RTS		
8 (in)	CTS		
9		TxD-	TxD-/RxD-

Power Over Ethernet Pinouts

This section defines the pinouts for the RJ45 Ethernet connection used on the PoE Terminal Server models.



The following table provides pinout information:

Pinout	Standard	802.3AF Unit-4 Wire	802.3AF Unit-8 Wire
1	Tx+	Tx+/+Voltage	Tx+
2	Tx-	Tx-/ +Voltage	Tx-
3	Rx+	Rx+/- Voltage	Rx+
4	N/C		+Voltage
5	N/C		+Voltage
6	Rx-	Rx-/ -Voltage	Rx-
7	N/C		-Voltage
8	N/C		-Voltage

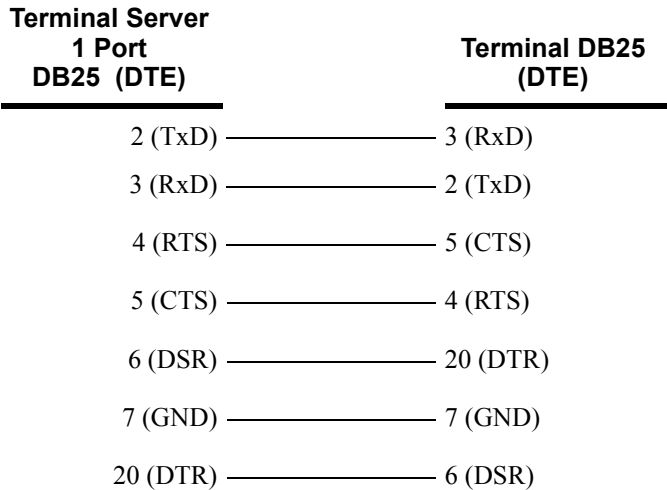
EIA-232 Cabling Diagrams

This section shows how to create EIA-232 cables that are compatible with the Terminal Server.

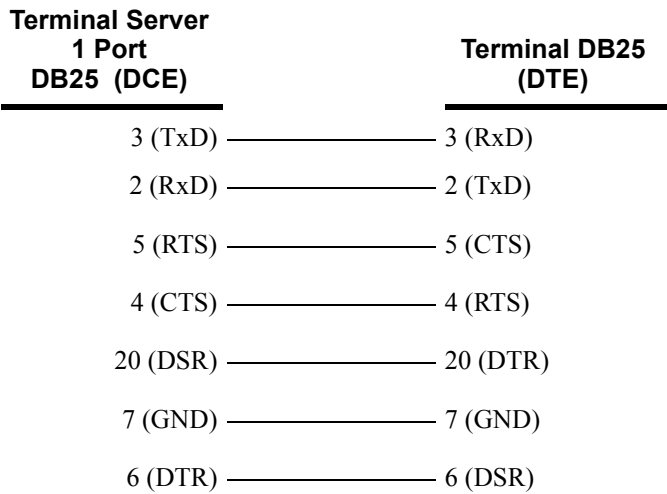
Terminal DB25 Connector

The following diagrams show how the null modem cable should be configured when connecting to a terminal DB25.

DB25 Male



DB25 Female



RJ45

BLACK BOX® RJ45		Terminal DB25 (DTE)	
10-pin	8-pin		
4 (DSR)	3	—————	20 (DTR)
3 (RTS)	2	—————	5 (CTS)
5 (TxD)	4	—————	3 (RxD)
6 (RxD)	5	—————	2 (TxD)
7 (GND)	6	—————	7 (GND)
8 (CTS)	7	—————	4 (RTS)
9 (DTR)	8	—————	6 (DSR)

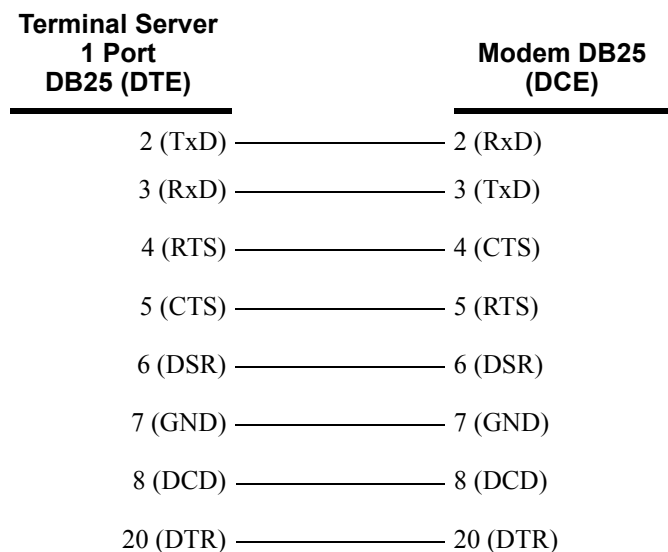
DB9 Male

Terminal Server 1 Port DB9 Male	Terminal DB25 (DTE)
3 (TxD)	————— 3 (RxD)
2 (RxD)	————— 2 (TxD)
7 (RTS)	————— 5 (CTS)
8 (CTS)	————— 4 (RTS)
6 (DSR)	————— 20 (DTR)
5 (GND)	————— 7 (GND)
4 (DTR)	————— 6 (DSR)

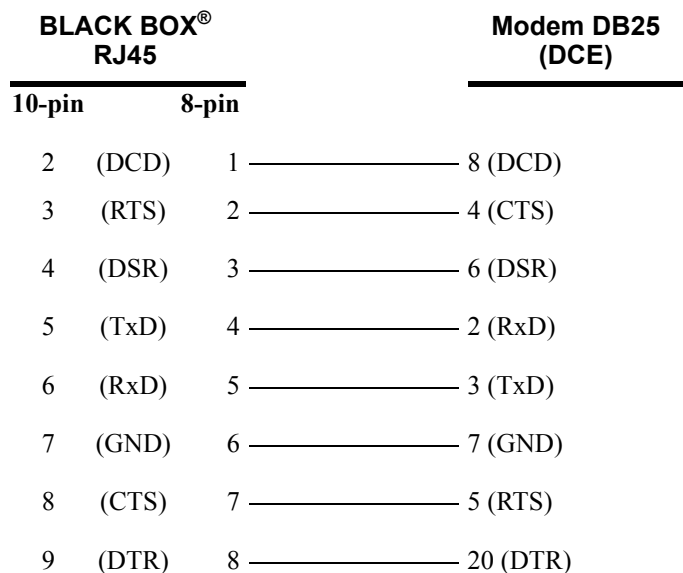
Modem DB25 Connector

The following diagrams show how a standard straight through cable should be configured when connecting to a DB25 modem.

DB25 Male



RJ45



DB9 Male**Terminal Server
1 Port
DB9 Male****Modem DB25
(DCE)**

1 (DCD)	8 (DCD)
2 (RxD)	3 (TxD)
3 (TxD)	2 (RxD)
4 (DTR)	20 (DTR)
5 (GND)	7 (GND)
6 (DSR)	6 (DSR)
7 (RTS)	4 (CTS)
8 (CTS)	5 (RTS)

E

Virtual Modem AT Commands

Virtual Modem Initialization Commands

Note: Virtual Modem initialization commands are only supported on Terminal Server firmware and configurators version 3.2 or higher.

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. n=1, no result codes will be sent. (default)
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 Terminal Server when VModem is in "command" mode.	n=0, disable echo. n=1, enable echo. (default)
+++ATH	Hang up. This command instructs the Terminal Server 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 Terminal Server will not accept incoming sessions until an ATA is issued by the serial device. In "auto answer" mode, the Terminal Server will automatically accept an incoming connection request.	Register=0, sets "manual answer" mode Register=1-255, "auto answer" mode (default)

Command	Description	Options
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 Terminal Server to initiate the connection.	
AT&Sn	Sets the behavior of Terminal Server'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 Terminal Server'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 modes 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 hex 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).	

F Utilities

Introduction

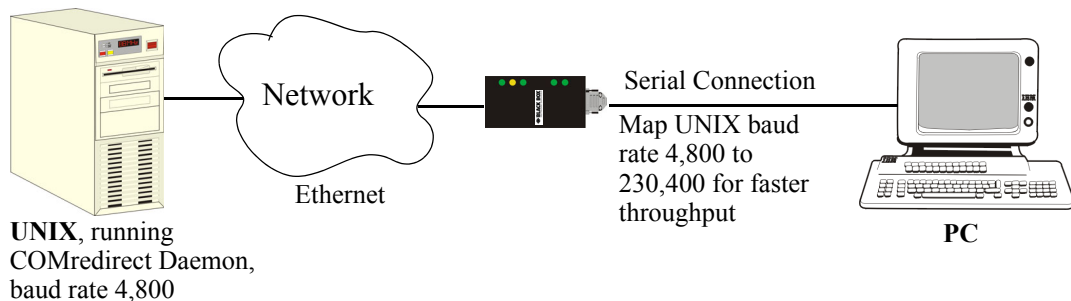
This chapter provides information on the COMredirect and Decoder utilities.

COMredirect

COMredirect is a com port redirector utility for the Terminal Server. It can be run in two modes:

- **COMredirect 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.
- **COMredirect 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 Terminal Server.

You use COMredirect when you want to connect extra terminals to a server using the Terminal Server rather than a multi-port serial card. COMredirect is especially useful when you want to improve data security, as you can enable an SSL/TLS connection between the COMredirect host port and the Terminal Server. When run on UNIX, COMredirect 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, COMredirect is supported on Linux, Windows®, SCO®, Solaris®, Unixware® and HP®. For more information, see the *COMredirect User Guide* for your platform on the CD-ROM.

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 operating systems:

- 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

G

Troubleshooting

Introduction

This chapter provides information that can help resolve problems with the Terminal Server.

Hardware Troubleshooting

The Power/Ready LED stays red after a boot.

If the Terminal Server Power/Ready LED is red and stays red for over 10 seconds, you have a hardware problem that might require factory service. First, try the following:

- In Console mode for desktop models or viewing the Console port in rack mount models, see if you need to reload the firmware, which can be found on the CD-ROM that came with the Terminal Server.
- If the bootloader option does not appear when you reboot the Terminal Server (to load new firmware), you need to make arrangements to return the Terminal Server.

If you purchased the Terminal Server less than 30 days before this problem appears, contact your distributor; otherwise, see the Black Box web site (www.blackbox.com) for factory service information. Note: no factory service can be done on a Terminal Server that has not been registered.

The Power/Ready LED on a rack mount model flashes red:

- **Good Boot:** When the Terminal Server cycles through a good boot, the Power/Ready LED cycles for several seconds and then stays a solid green.
- **Noncritical Error Boot:** When the Terminal Server cycles through a boot and a noncritical error occurs, such as a bad port, the Power/Ready LED will flash red briefly before displaying a solid green. You should reboot the Terminal Server while monitoring the Console port to view the error information.
- **Critical Error Boot:** When the Terminal Server cycles through a boot and a critical error occurs, such as corrupted firmware, the Power/Ready LED continues to flash red. View the Terminal Server reboot through the Console port for information on how to correct the problem.
- **Fatal Error Boot:** When the Terminal Server cycles through a boot and a fatal error occurs, the Power/Ready LED stays a solid red).

Communication Issues

General communication checks and practices are as follows:

- Are your cables connected and correctly configured? If you are using EIA-232, see [EIA-232 Cabling Diagrams](#) to verify that your cables are correctly configured.
- Ping your host? If you can ping but packet loss is reported, ping another host/device on the same network. This will tell you whether the problem is specific to the host/device or general to the network.
- After entering or changing IP information for your Terminal Server, *reboot* the Terminal Server (does not apply when using BOOTP or DHCP). Once the Terminal Server has rebooted, other network devices should be able to communicate with it (ping, telnet, etc.). Also, protocols such as ARP and proxy-ARP will work properly.
- Use the **show routes** command (command line only) or view the **Routes** statistics. Is there a route to the host?
- If the WebManager or DeviceManager cannot communicate with the Terminal Server, verify that the **Server Services HTTP** and/or **HTTPS** are enabled for WebManager and **DeviceManagerD** is enabled for DeviceManager. If you are using only HTTPS, the connection URL must start with **https://**.

DeviceManager Problems

Error Message: **16 bit Windows Subsystem - C:\WINDOWS\SYSTEM32\AUTOEXEC.NT. The system file is not suitable for running MS-DOS and Microsoft Windows applications. Choose 'Close' to terminate the application.**

The error message can be misleading, because it is displayed even if the **AUTOEXEC.NT** file is actually missing.

To verify whether you have the file, type `%windir%/system32/` in the address bar of an Explorer window. If there is no **AUTOEXEC.NT** file proceed as follows:

1. Browse to `%windir%/repair/` (usually `C:\WINDOWS\repair`).
2. Right-click and Copy the **AUTOEXEC.NT** file.
3. Browse to `%windir%/system32/` (usually `C:\WINDOWS\System32`).
4. Right-click inside the window and Paste the file.

The error condition described here may also be the result of corruption of the **AUTOEXEC.NT** file, in which case the above procedure may be helpful to restore a valid file.

If the above procedure does not fix the DeviceManager installation problem, see <http://support.microsoft.com/?kbid=324767> for the official Microsoft explanation.

Host Problems

Cannot access a host by name:

- If using DNS or if DNS is required, ensure a nameserver is configured on your Terminal Server and is accessible (ping it).
- If not using DNS, verify that the host is configured in the **Host Table**. Check access to the host by pinging it using the host's IP address.

Cannot access a host on a local network, verify:

- The network address is correct.
- The subnet mask is set correctly and reflects the network configuration.
- The broadcast address is set correctly and reflects the network configuration.

Cannot access a host on a remote network:

- Use the **show route** command to verify that there is a route to the remote host. If no gateway is specified, verify that a default gateway is specified. Ping the default gateway to check if it is working.
- Consider the situation beyond the gateway; for example, are intermediate gateways and the remote host available? Also, check the messages returned by the **ping** command; for example, that a particular host or gateway is unreachable.

Gateways added into the gateway table are ignored by the Terminal Server:

- Have you used BOOTP and entered a single static gateway in the bootptab file entry? If yes, the other gateways will be ignored.

Access to host lost after a few minutes.

- If the route to this host goes through routers, make sure those routers are all sending RIP packets across the networks.

RADIUS Authentication Problems

User is waiting up to 60 seconds before login is accepted or denied and Authentication is set to RADIUS. User has entered User Name and Password, and has pressed Enter.

- Check RADIUS configuration of primary and secondary authentication/accounting hosts specified, if you have retry and timeout values greater than the default, the Terminal Server will be spending time trying each of these hosts and keeping the user waiting.
- Adjust RADIUS configuration: specify just one host, reduce **Timeout** and **Retry** values to the default or less than default.

You cannot progress beyond the login and password prompts when authentication is set to RADIUS:

- On the RADIUS host, check the secret (password), you should see it displayed in clear text in the RADIUS clients file. If you are unsure whether it is the same secret which you entered in the Terminal Server, go to the Terminal Server and re-enter a new secret.
- On the RADIUS host, verify that there is only one entry for a particular user; do not have multiple entries of the same user name (even if the passwords are different).

Login Problems

You cannot obtain a login on *any* of the serial ports

- Connect via the Admin port and check the settings of the front-mounted ports; they have probably been set to a profile that does support serial connections, such as the Console Management profile (in CLI or Menu, 'direct' or 'silent' telnet/rlogin). Try setting the serial port(s) to the Terminal profile (DSlogin in CLI or Menu).

You have lost or don't know your password (as Admin user).

- You must reset the Terminal Server to its factory default settings using the **Reset** switch on the rear panel. There is no procedure to access the Terminal Server without a password.

Problems with Terminals

The following section concerns problems with the appearance of data on your terminal screen.

The Terminal Server logs me out after a few minutes:

- Check the **Idle Timer** value set for the user. The default setting for the **Idle Timer** for all users is 0 seconds (does not timeout).

Corrupt data.

- Check your line settings (baud rate, stop bits, etc.)

Missing data.

- Verify that the same type of flow control is set in both your terminal and on the Terminal Server's port.

Error message not permitted on a dumb terminal after typing the CLI command screen.

- Set your **Line** to **Termttype** VT100, ANSI or WYSE60 (or other form of terminal emulation, if you have downloaded one). The default line type in the Terminal Server is **Dumb**, which does not support the graphics characters necessary to view the text-based menus.

Screen corruption when using the text-based menu system.

- Verify that the terminal setup in the Terminal Server matches your terminal.
- Verify that entries in the term file match your terminal setup.
- If using a PC/computer, verify that the type of terminal emulation selected in your application matches those supported by the Terminal Server.

When using the function keys on your keyboard, nothing happens or your sessions keep swapping.

- Change your **Hotkey Prefix** character. The function keys on the keyboards of some terminals (like WYSE60) send character sequences which begin with **^a**; unfortunately, **^a** is also the default **Hotkey Prefix**, which you use to switch between sessions. A valid alternative would be **^b** (hex=02). If you are the system administrator, you can change any user's **Hotkey Prefix** character.

When using a downloaded terminal definition, you are having problems using arrow keys.

- Use Ctrl-K, Ctrl-J, Ctrl-H and Ctrl-L for up, down, left and right respectively.

When switching from a session back to the text menus, both screen images are superimposed.

- Press **^r** to redraw the screen.

INIT: Error in terminal file <filename>

- This error indicates that you have exceeded the 80 character limit for one or more of the terminal capabilities defined in the reported file.

INIT: Error on line n in terminal file <filename>

- You have omitted the = sign from the reported line.

Unknown IP Address

You have a Terminal Server already configured and you do know your password, but have lost, misconfigured, or don't know the IP address of the Terminal Server, and you cannot obtain a login.

- If the Terminal Server resides within the local network segment, you can use DeviceManager to find the Terminal Server.
- You can connect directly to the serial port of the Terminal Server, as explained in [Using a Direct Serial Connection to Specify an IP Address](#).

DHCP/BOOTP Problems

Messages: `host name too long or filename too long.`

- The Terminal Server can only accept host names of 14 characters or file names of 64 characters, so verify that you are not attempting to pass a string that is longer than those maximums.

DHCP or BOOTP have been set up to configure my Terminal Server, but does not seem to have done anything.

- Check that the server DHCP/BOOTP service is set to on, if not set it to on and reboot.
- Check that your BOOTP server is configured for your Terminal Server or that your DHCP server has an active lease pool (scope) with at least 1 free IP address.

You observe TFTP errors when the Terminal Server boots, for example:

TFTP: File not found : filename

TFTP: Timed out

This has a number of causes, including:

- The file names you specified to DHCP/BOOTP do not exist or are in the wrong place.
- The server for any of the downloadable files in your bootfile has no TFTP server running.
- Verify that lease data in your DHCP server manager is correct.
- Reset or restart the DHCP server.

Callback Problems

User Callback is On, and a number is configured for the line, but the Terminal Server is not calling the user back:

- Verify that the phone number is entered under the user (not the line).
- Verify that the callback **Phone Number** is valid.
- Verify that the modem at the user's end is set to 'auto-answer'.

Language Problems

In a customized language, the text strings appear in the wrong place in the Menu, CLI, or WebManager.

- Check the original ASCII text file you used to translate to your customised language. The sequence of the line much match exactly (be aware that comments don't affect line sequence, but can affect the actual line that the strings appear on). So, if you strip out all comments, if the original file says line 1000 should be string **none**, then line 1000 (stripped of comments) should be the translated version of **none**.

Modem Problems

The Terminal Server is not initializing the modem.

- Check your **Line Service** is set to **SLIP** or **PPP**. If your line service is set to any other type, the Terminal Server will not initialize a modem. You will need to configure the modem manually.

PPP Problems

The link fails on start-up when there are remote IP addresses set for both a user (Framed IP value) and a line (Remote IP address).

- Check the IP address set for the user; this is used in preference to the IP address set for a line. If there is a problem with the user's IP address, negotiation will fail; the Terminal Server will *not* use the line's IP address as an alternative.

The link fails on start-up and security (either PAP or CHAP) is enabled on the line.

- Check the remote client/device has the same setting; that is, PAP if the Terminal Server is using PAP. The Terminal Server does not perform negotiation with the remote end over PAP or CHAP.

At the remote end, the client software locks up when security (CHAP) is enabled on the line.

- Disable CHAP re-challenge parameter (challenge_interval) in the Terminal Server. Some PPP client software does not work when receiving CHAP re-challenges.

PPP is not running successfully over your 485 half-duplex environment.

- PPP is incompatible with half-duplex; it must be run over a full-duplex environment.

Printing Problems

The print job fails to print on the device attached to the serial port.

- On the line where the printer is attached, set **Line Service** to **Printer**. Print jobs will not print when the line service is set incorrectly.

When using RCP, the network host receives a rejection message from the Terminal Server. The result is that the print job does not take place.

- Print using LPD
or
- Modify the printer interface scripts on the network host to overcome this weakness of RCP. The modification will force the network host to continue trying to send the print job when the Terminal Server's printer port is busy.

Long Reboot Cycle

Rebooting the Terminal Server takes a long time.

If you are not using DHCP/BOOTP, disable this within the Server Services; otherwise, the Terminal Server waits to timeout for a request to DHCP/BOOTP.

SSL/TLS

If you are experiencing problems obtaining a successful SSL/TLS connection, you can set your **Syslog Level** to **Notice** and view the syslog for the following messages:

Line not SSL enabled. Abort connection when a user who is configured for **Service SSL_RAW** tries to login on the serial port.

The user has been configured for an **SSL_RAW** connection, but the line has not been configured to enable SSL. To resolve this, either enable the line for SSL or change the user's **Service** to **TCP_CLEAR** if SSL is not wanted.

Could not obtain peer's certificate.

- User has selected a cipher key exchange of ADH (anonymous Diffie-Hellman) and enabled Peer verification. ADH does not use certificates so they will not be sent in an SSL/TLS handshake. Disable Peer Verification or change to a cipher suite that uses certificates.
- User has selected Peer Verification on the configured SSL/TLS server and has not configured a certificate for the client. Either disable peer verification on the SSL/TLS server or configure a certificate for the SSL/TLS client.

SSL_accept failed on the SSL/TLS server device.

- The device has failed to accept an SSL/TLS connection on top of a TCP connection that has just been established. This could indicate that the peer from which COMredirect is trying to accept a connection from is not configured for SSL/TLS. Verify that the peer has been configured for an SSL/TLS client connection.

Certificate did not match configuration

- The message is displayed when **Validate Peer Certificate** has been enabled, but the configured **Validation Criteria** does not match the corresponding data in the certificate received from the peer. The data configured must match exactly to the data in the certificate. The data is also case sensitive.

unknown protocol message when trying to make an SSL/TLS connection

- This will be displayed when both sides of the TCP connection are configured as SSL/TLS clients. Change one of the end points to act as an SSL/TLS server.
- One of the endpoints is not configured for SSL/TLS. Make sure both endpoints are configured for SSL/TLS, verify that one is a client and the other is a server.

tlsv1 alert handshake failure or **sslv3 alert handshake failure**

- The remote site has an SSL/TLS error and is sending this message with an alert message. Look at the error messages on the remote end and fix the problem indicated.

IPv6 Issues

You are not seeing the IPv6 address value when you attempt to connect to the Terminal Server.

Many Windows® based systems have IPv6 support already enabled, however, if you need to install IPv6 then follow the procedure below.

To install IPv6 support do the following:

1. In Control Panel, double-click the **Network Connections** icon.
2. Double-click the **Local Area Connection** entry.
3. In the Local Area Connection Status window, click the **Properties** button on the **General** tab.
4. In the Local Area Connections window, click the **Install** button on the **General** tab.
5. In the Select Network Component Type window, select **Protocol** and click the **Add** button.
6. In the Select Network Protocol window, select **Microsoft TCP/IP version 6** and click the **OK** button.

H Data Logging

Introduction

This appendix provides additional information about the Data Logging feature.

COMredirect 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 COMredirect 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

Modbus Remapping

Introduction

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 Terminal Server translate the UID to a different UID for the slave device. The Master UID has to be unique on the Terminal Server. The Slave UID must be unique on each serial port. The translate rules are controlled by a file downloaded to the Terminal Server.

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 Terminal Server 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 Terminal Server 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 Translation 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 Terminal Server using:
 - Device Manager: use "tools-advanced-custom files" dialog "download other file"
 - Web Manager: use "administration-custom files" page "other file"
 - CLI: use the command "netload customapp-file" command

J

Symmetric Key File

Symmetric Key File

This section defines the layout of the NTP/SNTP Symmetric Key file that must be downloaded to the Terminal Server in order to use the 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.

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)+'9KRDSRuorQPiw	ascii string
5	SHA1	0e9e44502940294fa788aafaac34ccb126347d34	hex digit string
6	SHA1	f4e9e4454e9e4450294facb126309ff4ccb1200	hex digit string
7	SHA1	e9e44502949e4450294ccb12634e9e447d3489	hex digit string
8	SHA1	40294fa7894facb126502944fac4e9e788aafaa	hex digit string

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

Glossary

This chapter provides definitions for Terminal Server terms.

BOOTP (BOOTstrap Protocol)	An Internet protocol that enables a diskless workstation to discover its own IP address, the IP address of a BOOTP server on the network, and a file to be loaded into memory to boot the machine. This enables the workstation to boot without requiring a hard or floppy disk drive.
Callback	A security feature where the Terminal Server calls back the User at a predetermined number defined in the User's account.
CHAP (Challenge Handshake Authentication Protocol)	Standard authentication protocol for PPP connections. It provides a higher level of security than PAP and should be used whenever possible. <i>see PAP</i>
Community (SNMP)	An SNMP community is the group that devices and management stations running SNMP belong to. It helps define where information is sent.
DHCP (Dynamic Host Configuration Protocol)	A TCP/IP protocol that provides static and dynamic address allocation and management.
Direct Connection	Connections that bypass the Terminal Server enabling the user to log straight into a specific host. A direct connection is recommended where a user logging in to the Terminal Server is not required.
Ethernet	A high-speed (10Mbps,100Mbps) cable technology that connects devices to a LAN, using one or more sets of communication protocols.
Fixed Callback	A method where there is a specific number defined to callback a user.
Local Authentication	Uses the user ID and password stored within the Terminal Server User database.
LPD	Line Printer Daemon. A printer protocol that uses TCP/IP to establish connections between printers and workstations on a network. The technology was developed originally for BSD UNIX and has since become the de facto cross-platform printing protocol.
Modem Initialization String	A series of commands sent to the modem by a communications program at start up. These commands tell a modem how to set itself up in order to communicate easily with another modem.
MOTD	Message of the day. This is defined by a file whose contents display when users log into the Terminal Server.
Multicast	The broadcasting of messages to a specified group of workstations on a LAN, WAN, or internet.
NAK (Negative Acknowledgment)	A communication control character sent by the receiving destination indicating that the last message was not received correctly.

PAP (Password Authentication Protocol)	Standard authentication protocol for PPP connections. <i>see CHAP</i>
RADIUS (Remote Authentication Dial In Users Services)	An open standard network security server that communicates with the PAP protocol.
Reverse Connection	Connections that originate from a host that go directly to a serial device through the Terminal Server.
RIP (Routing Information Protocol)	A protocol that allows gateways and hosts to exchange information about various routes to different networks.
Roaming Callback	A method where the client supplies the number for callback when they dial in.
RPC	Remote Procedure Call. A type of protocol that allows a program on one computer to execute a program on a server computer.
Silent Connection	Silent connections are the same as direct connections except that they are permanently established. The host login prompt is displayed on the screen. Logging out redisplay this prompt. Silent connections, unlike direct connections, however, make permanent use of pseudo tty resources and therefore consume host resources even when not in use.
SNMP (Simple Network Management Protocol)	A protocol for managing network devices.
Subnet/Prefix Bits	Identifies the device's IP address, which portion constitutes the network address and which portion constitutes the host address.

A

admin

- default password 52
- lost password 258

ARP-Ping, setting an IP address 55

authentication, general 191

B

binary configuration file 66

BOOTP

- parameters 48
- setting an IP address 54

C

cabling, EIA-232 312

certificates

- LDAP CA list 227
- SSH, OpenSSH 227
- SSL 227

COMredirect utility 119, 318

configuration files

- formats 66

connecting to the Terminal Server

- console mode 33
- serial mode 33
- setting IP address 36

console mode 33

custom factory default configuration 252

D

DB25

pinouts

female 309

male 308

power in pin

female 310

male 309

DB9 male pinouts 311

DC power requirements 29

Decoder utility 319

default admin password 52

definitions 331

DeviceManager

- overview 38
- setting an IP address 52

DHCP

- parameters 48
- setting an IP address 54

direct connect

- setting an IP address 53

E

EasyPort Web 61

email notification events 106, 234

F

factory default configuration

- custom 252
- original 252

factory defaults, resetting to 258

H

Host 277

- host-based printing 265
- Host-to Host 277
- HTTP Tunnels 273

I

- installing
 - modem card 305
 - rack mount 34
- IPsec 211
- IPv6, setting an IP address 55

J

- jumpers
 - line termination 300
 - power out 300
 - setting 300

K

- keys
 - HTTPS 227
 - SSH 227

L

- L2TP/IPsec 216
- language
 - translating 255
 - upgrading firmware 255
- LDAP
 - parameters 197
- line termination, setting jumper 300
- LPD printing 265

M

- Menu
 - conventions 46
- MIB 48
- Modbus
 - configuration overview 259
 - gateway settings 260
 - line settings 261
- mode
 - console 33
 - serial 33
- modem card 305
- modem parameters 187

N

- NFS
 - Decoder utility 319
 - port buffering 183
- NIS parameters 201
- nnel 280

O

- online help, using 22
- OpenSSH 227

P

- parameters
 - BOOTP/DHCP 48
 - LDAP 197
 - modems 187
 - NIS 201
 - port buffering 184
 - RADIUS 193

- SecurID 200
- SSH server 202
- TACACS+ 199
- password
 - admin default 52
 - lost 258
- PCI slot 305
- pin, power in
 - DB25 female 310
 - DB25 male 309
 - serial RJ45 310
- pinouts
 - DB25 female 309
 - DB25 male 308
 - DB9 male 311
 - RJ45 ethernet 311
 - RJ45 serial 310, 330
- port buffering 183
 - Decoder utility
 - Decoder utility 184
 - local 183
 - parameters 184
 - remote 184
- power in pin
 - DB25 female 310
 - DB25 male 309
 - serial RJ45 310
- power out, setting jumper 300
- printers 265
- printing
 - host-based 265
 - LPD 265
 - RCP 265

R

- rack mount
 - description 33
 - installing 34
- RADIUS
 - parameters 193
 - supported RADIUS parameters 291
- RCP printing 265
- resetting to factory defaults 258
- RIP
 - overview 80
- RJ45
 - ethernet pinouts 311
 - serial pinouts 310, 330
- RJ45 serial power in pin 310

S

- SecurID parameters 200
- Serial 273
- serial mode 33
- Serial-to Host 275, 277
- Serial-to Serial 273
- services
 - line
 - printer 265
 - UDP 132
 - vmodem 158
- sessions 97
- setting an IP address
 - ARP-Ping 55

- BOOTP/DHCP 54
- DeviceManager 52
- direct connect 53
- IPv6 55
- SNMP
 - support MIBs 49
 - using 48
- SSH server parameters 202
- SSL certificate 227

T

- TACACS+ parameters 199
- terminal definitions
 - creating 256
 - downloading 256
- text configuration file 66

U

- UDP
 - configuring 132
- user sessions 97
- utility
 - COMredirect 119, 318
 - Decoder 319

V

- virtual modem 158
- vmodem
 - overview 158
- VNP
 - IPsec 211
- VPN 210
 - exceptions 217
 - L2TP/IPsec 216

W

- WebManager
 - overview 41



© Copyright 2016. Black Box Corporation. All rights reserved.

1000 Park Drive • Lawrence, PA 15055-1018 • 724-746-5500 • Fax 724-746-0746