Notification Supported HW/SW Device Configurations Guide

A6V12131888_en_b_70

Smart Infrastructure

2023-09-30

Table of Contents

Information Security

NOTICE	
!	This document is classified as “Restricted”. Restricted information is intended for Siemens’ employees and third parties (for example, suppliers, customers) collaborating with Siemens only. This means that it is possible to share information in this document with third parties that are interested in our product on a “need-to-know” basis. However, distributing this document to the public or publishing it on the internet is prohibited.

Copyright Notice

Notice

For further information, contact your nearest Siemens Industry, Inc. representative.

To the Reader

Your feedback is important to us. If you have comments about this manual, please submit them to: SBT_technical.editor.us.sbt@siemens.com

Credits

Edition: 2023-09-30

Document ID: A6V12131888_en_b_70

About This Document

Purpose

This manual describes the main tasks a Field Engineer has to perform in order to configure Notification devices.

Scope

This document applies to the system version 7.0.

Target Audience

Project Engineers are responsible for planning and configuring a customer project. They provide the parameterization of products, devices, and systems and are responsible for general system troubleshooting. They have the training appropriate to their function and to the products, devices, and systems to be configured. They are familiar with the applied operating system(s) and the related network environment.

Liability Disclaimer

We have checked the contents of this manual for agreement with the hardware and software described. Since deviations cannot be precluded entirely, we cannot guarantee full agreement. However, the data in this manual are reviewed regularly and any necessary corrections included in subsequent editions. Suggestions for improvement are welcome.

Product Security Disclaimer

Siemens products and solutions provide IT-specific security functions to ensure the secure operation of building comfort, fire safety, security management and physical security systems. The security functions on these products and solutions are important components of a comprehensive security concept.

However, it is necessary to implement and maintain a comprehensive, state-of-the-art security concept that is customized to individual security needs. Such a security concept may result in additional site-specific preventive action to ensure that the building comfort, fire safety, security management or physical security systems for your site are operated in a secure manner. These measures may include, but are not limited to, separating networks, physically protecting system components, user awareness programs, in-depth security, and so on.

For additional information on building technology security and our offerings, contact your Siemens sales or project department. We strongly recommend signing up for our security advisories, which provide information on the latest security threats, patches and other mitigation measures.

http://www.siemens.com/innovation/en/technology-focus/siemens-cert/cert-security-advisories.htm

Document Conventions

The following table lists conventions to help you use this document in a quick and efficient manner.

Convention	Examples
Numbered Lists (1, 2, 3…) indicate a procedure with sequential steps.	**1.** Turn OFF power to the field panel. **2.** Turn ON power to the field panel. **3.** Open the panel.
One-step procedures are indicated by a bullet point.	● Expand the **Event List**.
Conditions that you must complete or must be met before beginning a procedure are designated with a ⊳. Intermediate results (what will happen following the execution of a procedure step), are designated with an indented ⇨. Results, after completing a procedure, are designated with a ⇨.	⊳ The report you want to print is open. **1.** Click **Print** 🖨. ⇨ The **Print** dialog box displays. **2.** Select the printer and click **Print**. ⇨ The print confirmation displays.
Bold font indicates something you should type or select, or when a dialog box or window is specified.	Type **F** for field panels. Click **OK** to save changes and close the dialog box. The **Create a New Project** dialog box displays.
Menu paths in procedures are indicated in **bold**.	Select **File > Text, Copy > Group**, which means from the **File** menu, select **Text**, **Copy** and then **Group**.
File paths containing placeholders display the placeholders in *italics* enclosed in square brackets.	[*installation drive*:]\[*installation folder*]\[*project*]\...
Error and system messages are displayed in `Courier New` font.	The message `Report Definition successfully renamed` displays in the status bar.
Italics are used to emphasize new or important terms.	The reaction processor continuously executes a user-defined set of instructions called the *control program*.
ℹ	This symbol signifies a Note. Notes provide additional information or helpful hints.
Cross references to other information in printed material are indicated with an arrow and the page number, enclosed in brackets: [→ 92]	For more information on creating flowcharts, see Flowcharts [→ 92].

Getting Help

For more information about our products, contact your local Siemens representative.

Safety Messages According to ANSI Z535.6

ANSI standard safety messages are used throughout Help to make you aware of important information. ANSI distinguishes between *property damage* messages and *personal injury* messages.

- The property damage message has this label: NOTICE.
- The personal injury messages have these labels: CAUTION!, WARNING!, DANGER!

Examples:

NOTICE	
!	**Property Damage Warning Message** Equipment damage or loss of data may occur if you do not follow a procedure or instruction as specified.

⚠ **CAUTION**	
⚠	**Caution Safety Message** Minor or moderate injury may occur if you do not follow a procedure or instruction as specified.

⚠ **WARNING**	
⚠	**Warning Safety Message** Personal injury or property damage may occur if you do not follow a procedure as specified.

⚠ **DANGER**	
⚡	**Danger Safety Message** Electric shock, death, or severe property damage may occur if you do not perform a procedure as specified.

Document Revision History

Document Identification

The document ID is structured as follows:
ID_Language(COUNTRY)_ModificationIndex_ProductVersionIndex
Example: A6Vnnnnnnnn_en_a_02

Document Revision History.

Modification Index	Edition Date	Brief Description
b	2020-10-31	Market Release Edition
a	2020-05-31	Market Release Edition

1 MNS Supported Physical Device Configurations

This section provides additional procedures for configuring the Notification Devices.

1.1 ESPA Paging System

ESPA 4.4.4 Interface

This section provides additional procedures for integrating the European Selective Paging Manufacturer's Association (ESPA) 4.4.4 compliant device.

Configuring and verifying ESPA Paging System

This section provides the steps for the configuration and verification of the device.

Configuration to communicate to the device requires two main steps. First, configure the internal settings of the device. To do this, install the Perle DeviceManager on a computer connected to the same network as the device to be configured.

The second step is to configure the driver on the computer that will be communicating with the device over the network. There are several methods used to communicate with the device. One method uses the TruePort driver.

NOTE:
TruePort is a COM port re-director driver utility that is installed on the server. TruePort creates a *virtual serial port* or *virtual COM port*. All COM port directed data sent by the application is re-directed by TruePort across the IP/Ethernet network to the remote device. Data and serial port signaling is transparently communicated between the application and remote device.

Certificate Creation From System Management Console

To establish a secure communication, certificates must be configured.

The following is the recommended workflow for working with the **Certificates** in System Management Console (SMC).

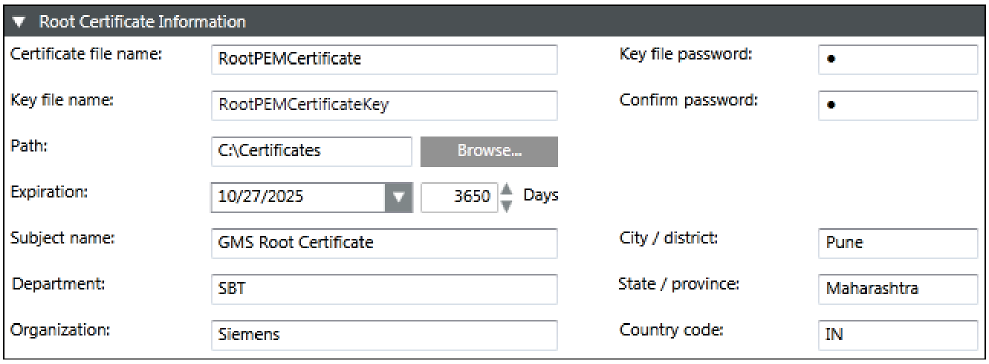
- Create Root Certificate Windows store based (.pem).

1. In the **Console** tree, select the **Certificate** node.

   ➪ The **Certificates** tab displays.

2. Click **Create Certificate** and then select **Create Root Certificate (.pem)** .

   ➪ The **Root Certificate Information** expander displays.



▼ Root Certificate Information

Certificate file name:	RootPEMCertificate	Key file password:	•
Key file name:	RootPEMCertificateKey	Confirm password:	•
Path:	C:\Certificates Browse...		
Expiration:	10/27/2025 ▼ 3650 Days		
Subject name:	GMS Root Certificate	City / district:	Pune
Department:	SBT	State / province:	Maharashtra
Organization:	Siemens	Country code:	IN

3. In the **Root Certificate Information** expander, provide the details as follows:
   a. Enter the **Certificate file name**.

b. Enter the **Key file name**.
c. Enter the **Key file password** and **confirm** it.
d. Browse for the location to store the root certificate and the root key file on the disk. By default, the path of the last created root certificate is selected.
e. Set the **Expiration** (validity period) duration in days. By default, the certificate expires after 3650 days.
f. Enter the following information about the Subject:
—**Subject name**
— *(Optional)* **Department**
— *(Optional)* **Organization**
— *(Optional)* **City / district**
— *(Optional)* **State / province**
— *(Optional)* **Country code.** (exactly two characters)

4. Click **Save** 💾.

⇨ If confirmed, the data entered during the root certificate creation is validated, and on successful root certificate creation,
- the new root certificate (.pem file) and the root key file are created at the specified location on the disk.

Tips for Working with (.pem) Root Certificates

- The **Certificate file name** and the **Key file name**
  - Must not contain blanks or special characters (/,\,?,<, >,*,|,").
  - The **Certificate file name** and the **Key file name** cannot be the same.
- When the user creates a root certificate for the first time, all the fields appear blank. For all subsequent root certificate creation (.pfx or .pem based), some fields, such as **Path**, **Organization**, and so on, are pre-populated with the information from the last-created root certificate.

Device Configuration

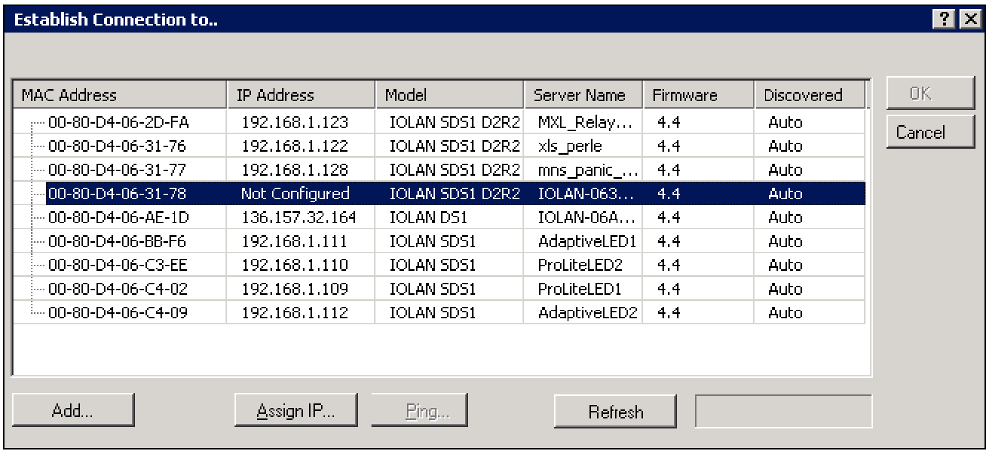
▷ Ensure that the Perle DeviceManager is installed on a computer located in the same network as the Perle device to be configured.

▷ Ensure that the following certificates are created using the System Management Console (SMC) or obtained from the site's IT department in Privacy Enhanced Mail (PEM) format:
a) Root Certificate (.pem)
b) Root Certificate Key
Refer to the Certificate Creation From System Management Console section for more information on creating certificates using SMC.

▷ Combine the Root Certificate Key file and Root Certificate into one file (using type command in command prompt, for example, **type RootCertificateKey.pem RootCertificate.pem > RootCombineCert.pem**.

▷ If preconfigured .dme file is available then refer Import DME File.

1. Start Perle DeviceManager.



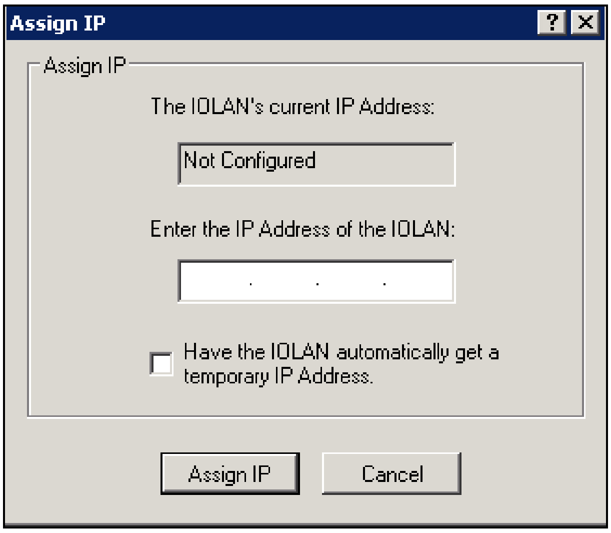
Establish Connection to..

MAC Address	IP Address	Model	Server Name	Firmware	Discovered
00-80-D4-06-2D-FA	192.168.1.123	IOLAN SDS1 D2R2	MXL_Relay...	4.4	Auto
00-80-D4-06-31-76	192.168.1.122	IOLAN SDS1 D2R2	xls_perle	4.4	Auto
00-80-D4-06-31-77	192.168.1.128	IOLAN SDS1 D2R2	mns_panic_...	4.4	Auto
00-80-D4-06-31-78	Not Configured	IOLAN SDS1 D2R2	IOLAN-063...	4.4	Auto
00-80-D4-06-AE-1D	136.157.32.164	IOLAN DS1	IOLAN-06A...	4.4	Auto
00-80-D4-06-BB-F6	192.168.1.111	IOLAN SDS1	AdaptiveLED1	4.4	Auto
00-80-D4-06-C3-EE	192.168.1.110	IOLAN SDS1	ProLiteLED2	4.4	Auto
00-80-D4-06-C4-02	192.168.1.109	IOLAN SDS1	ProLiteLED1	4.4	Auto
00-80-D4-06-C4-09	192.168.1.112	IOLAN SDS1	AdaptiveLED2	4.4	Auto

⇨ All similar devices under that network should be visible.

2. Select the device to configure and click **Assign IP**.
NOTE 1: If the device in the window is not visible, verify the device has power and is connected to the network. Check the display on the device; the power button should be solid green and the link button should be solid amber/green.
NOTE 2: If issues persist, unplug the Ethernet cable and power. Wait 5 seconds and then plug in the Ethernet cable followed by the power supply. Wait at least 90 seconds while the device reboots.
NOTE 3: If there are still remaining issues, manually reset the device by holding down the small Reset button located on the device for ten seconds or until the Power button is solid amber and then release. Wait 90 seconds for the device to reboot and initialize. If the device still does not work, replace the unit or check the network.

3. Manually enter an IP address or select the **Have the IOLAN automatically get a temporary IP Address** check box below to have the DHCP assign one automatically. Then click **Assign IP**.



Assign IP

Assign IP

The IOLAN's current IP Address:

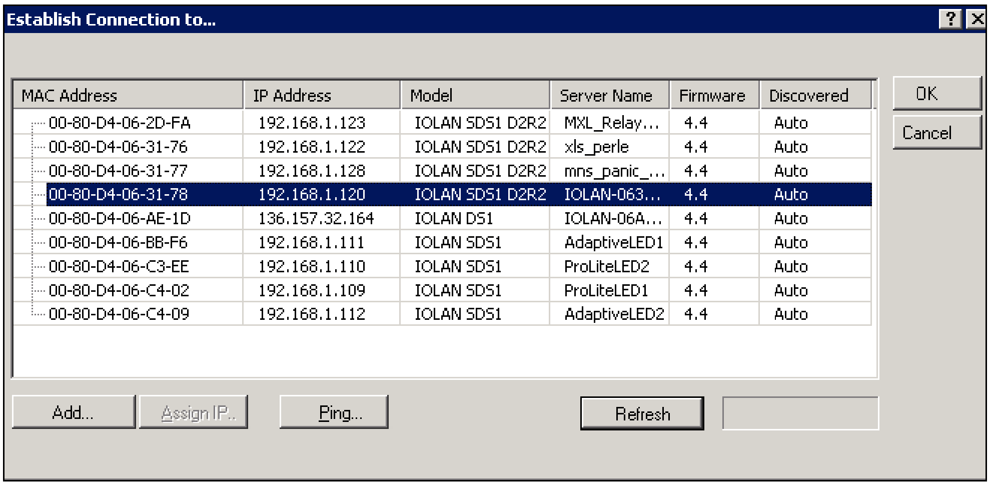
Not Configured

Enter the IP Address of the IOLAN:

. . .

☐ Have the IOLAN automatically get a temporary IP Address.

⇨ The **Establish Connection to** window appears with an IP address.

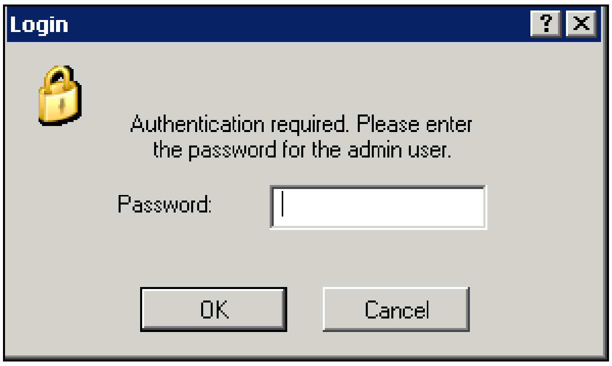


Establish Connection to...

MAC Address	IP Address	Model	Server Name	Firmware	Discovered
00-80-D4-06-2D-FA	192.168.1.123	IOLAN SDS1 D2R2	MXL_Relay...	4.4	Auto
00-80-D4-06-31-76	192.168.1.122	IOLAN SDS1 D2R2	xls_perle	4.4	Auto
00-80-D4-06-31-77	192.168.1.128	IOLAN SDS1 D2R2	mns_panic_...	4.4	Auto
00-80-D4-06-31-78	192.168.1.120	IOLAN SDS1 D2R2	IOLAN-063...	4.4	Auto
00-80-D4-06-AE-1D	136.157.32.164	IOLAN DS1	IOLAN-06A...	4.4	Auto
00-80-D4-06-BB-F6	192.168.1.111	IOLAN SDS1	AdaptiveLED1	4.4	Auto
00-80-D4-06-C3-EE	192.168.1.110	IOLAN SDS1	ProLiteLED2	4.4	Auto
00-80-D4-06-C4-02	192.168.1.109	IOLAN SDS1	ProLiteLED1	4.4	Auto
00-80-D4-06-C4-09	192.168.1.112	IOLAN SDS1	AdaptiveLED2	4.4	Auto

4. Select the device again, and click **OK** to log into the device for configuring.

5. At the **Login** window, type in the device password. The factory default password is: **superuser**.



Login

Authentication required. Please enter the password for the admin user.

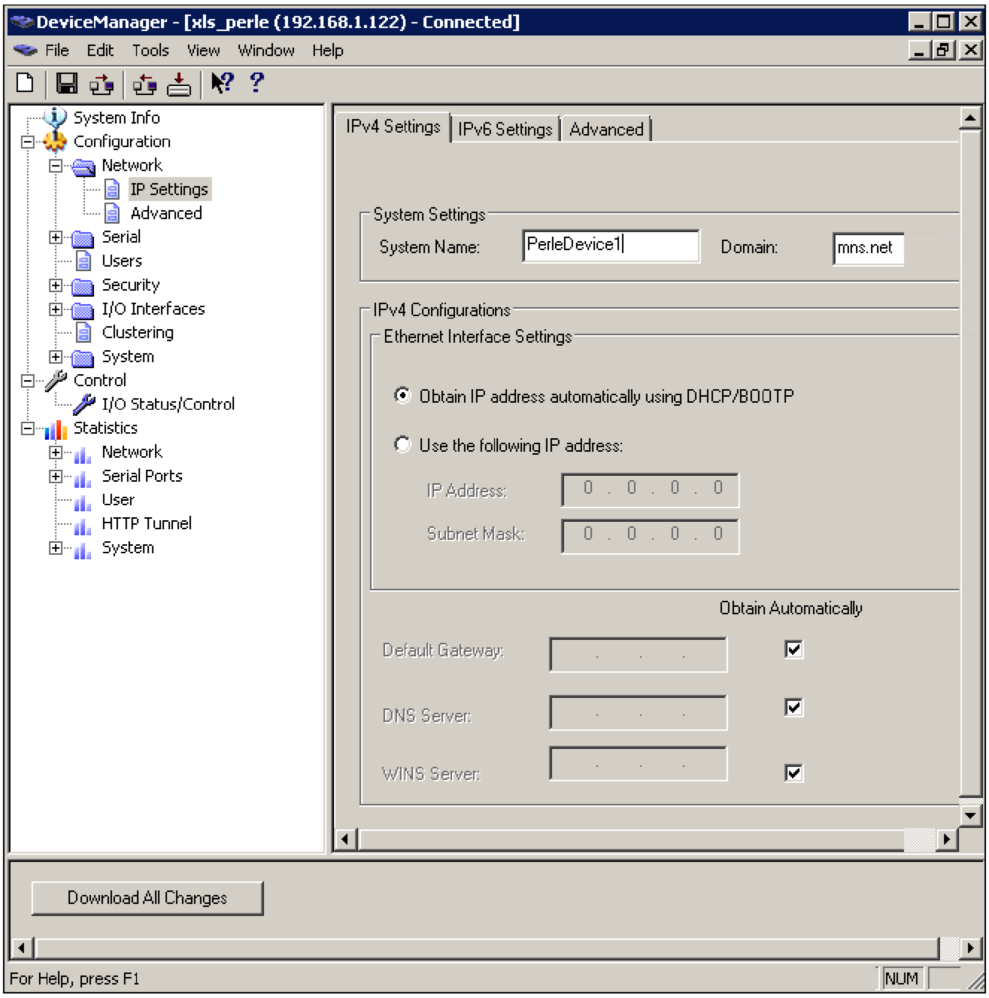
Password:

Fig. 1: Login Window

Network Set Up

To further configure the network settings of the device, log into the device using Perle DeviceManager. Do the following:

1. In the Perle **DeviceManager** tree view, click the **Network folder** and then **IP Settings**.
   NOTE: In this area, configure additional parameters for the network settings, such as configuring a **static IP address or DHCP**.



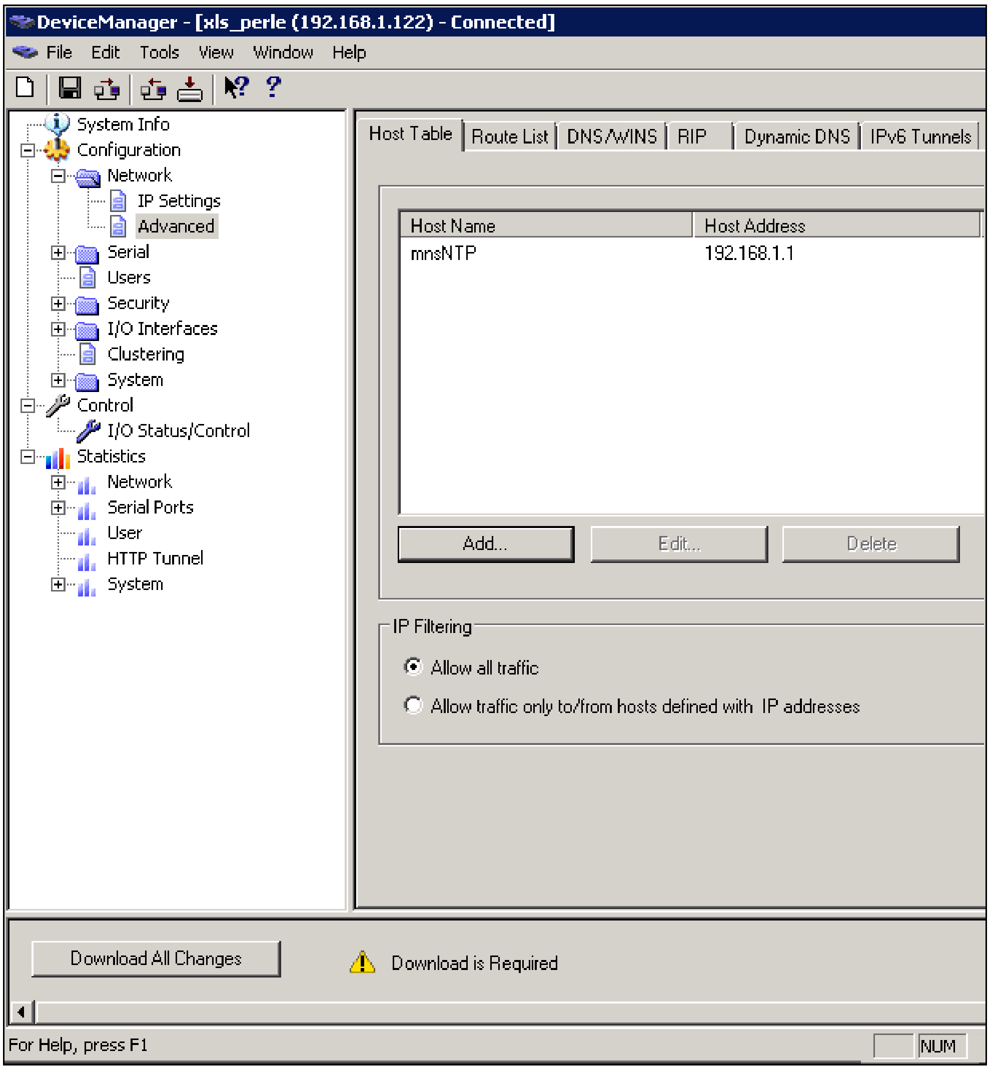
System Name: PerleDevice1
Domain: mns.net

● Obtain IP address automatically using DHCP/BOOTP
○ Use the following IP address:

IP Address: 0 . 0 . 0 . 0
Subnet Mask: 0 . 0 . 0 . 0

Default Gateway: ☑
DNS Server: ☑
WINS Server: ☑

2. On the **IPv4 Settings** tab, in the **System Name** field, give the device a distinguishable name to help identify this device from other similar devices.
   NOTE 1: The System Name will also be used by the device to create a fully qualified domain name.
   NOTE 2: By default, the device is always **IOLAN** followed by the last three bytes of the device's MAC address.
3. In the **Domain** field, enter the domain name used for the client’s network (for example, **AmericaUniversity.net**).
   NOTE: The device is capable of receiving the domain automatically from DHCP. However, DHCP would have to be configured to set the domain as a parameter.
4. Select **Network > IP Settings > Advanced** folder.
5. Select the **Register Address in DNS** check box.
6. Select the **Advanced** folder in the tree view.



Host Name	Host Address
mnsNTP	192.168.1.1

IP Filtering

● Allow all traffic

○ Allow traffic only to/from hosts defined with IP addresses

7. In the **Host Table** tab, click **Add** to add the NTP host.

8. Enter a descriptive name for the NTP server (for example, **mnsNTP**).

9. Enter the IP address or the fully qualified domain name of an available NTP server.
   NOTE: An available NTP server is required to enable SSL on the device.

10. Click **OK**.

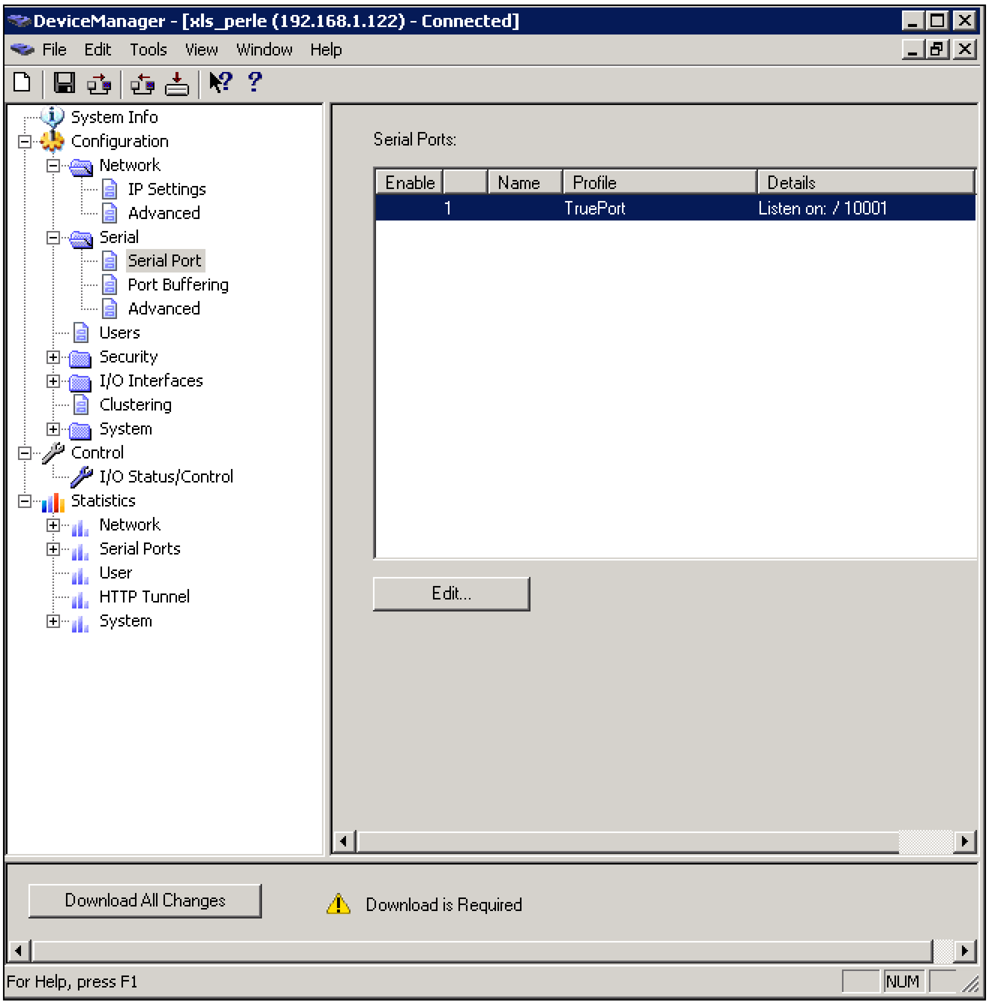
Serial Settings

▷ The user must have logged in to the device using DeviceManager.

1. In the Perle **DeviceManager** window, select **Serial > Serial Port**.

2. Configure the number of serial ports and the device profile. Only one serial port per device is required for serial communication.

3. Select the default serial port and click **Edit**.



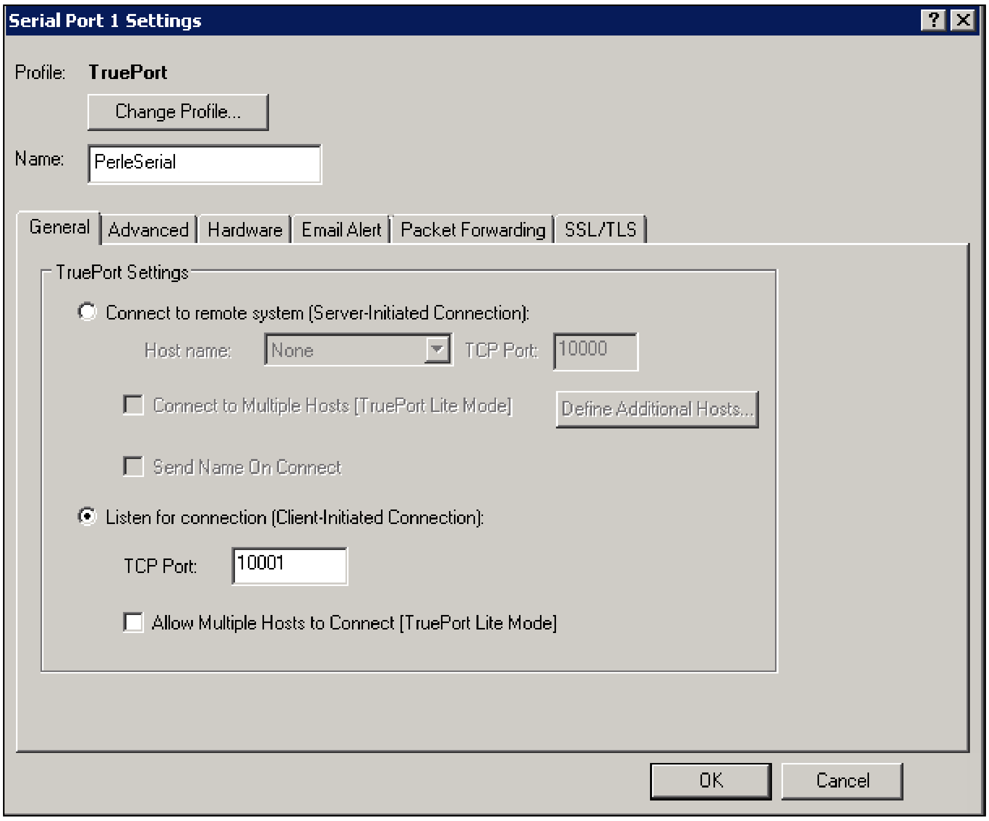
Serial Ports:

Enable		Name	Profile	Details
	1		TruePort	Listen on: / 10001

Download is Required

For Help, press F1

4. In the **Serial Ports Settings** window, click **Change Profile**. Select the **TruePort** profile and click **OK**.



Serial Port 1 Settings

Profile: **TruePort**

Change Profile...

Name: PerleSerial

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

TruePort Settings

○ Connect to remote system (Server-Initiated Connection):

Host name: None TCP Port: 10000

□ Connect to Multiple Hosts [TruePort Lite Mode] Define Additional Hosts...

□ Send Name On Connect

● Listen for connection (Client-Initiated Connection):

TCP Port: 10001

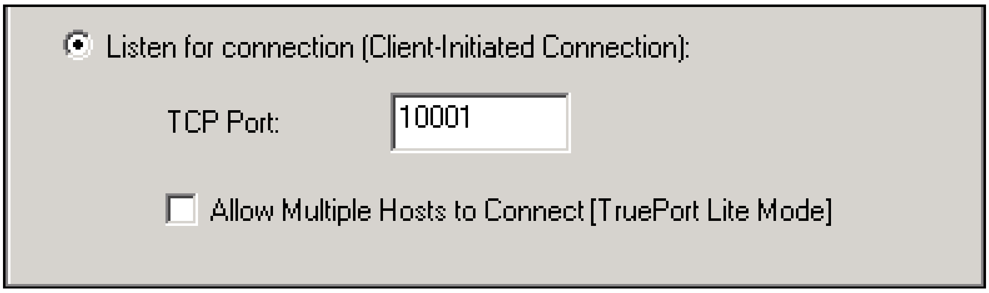
□ Allow Multiple Hosts to Connect [TruePort Lite Mode]

OK Cancel

➪ The **Serial Port Settings** window changes to reflect the new profile.

5. Select the **General** tab.
6. Select **Listen for connection (Client-Initiated Connection)**.

   ➪ In this mode, the device will wait for the server to establish a connection.
7. Enter the TCP port for communicating with the device. By default, the TCP port will always be **10001**.
   NOTE: Always check to make sure the port selected is not already in use by another application/service on the server. To check, open a Command Prompt, type **netstat**, and press **Enter**. A list of all current TCP connections and ports will be listed.
8. Select the **Connect to Multiple Hosts** check box.
9. Click **OK**.

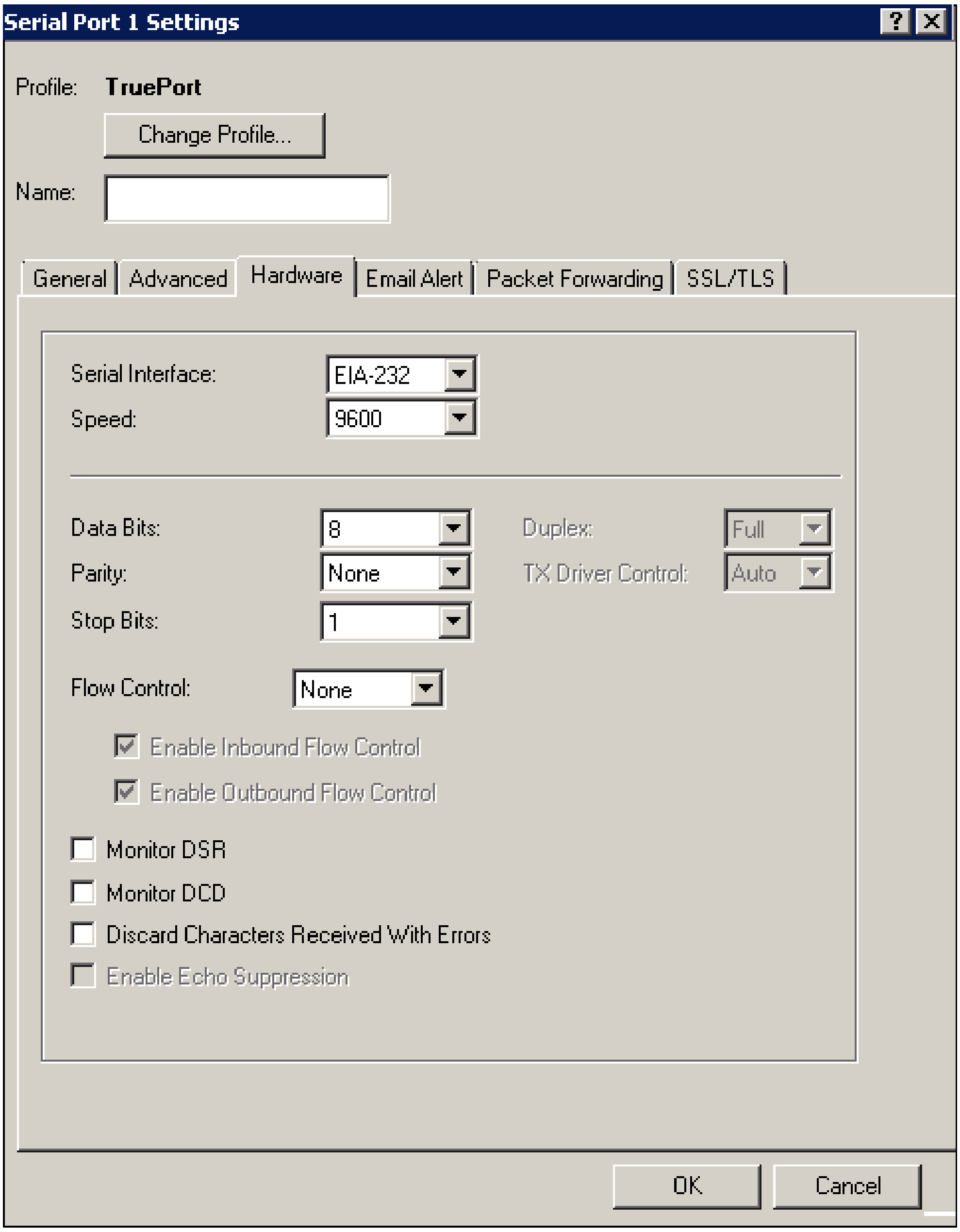


● Listen for connection (Client-Initiated Connection):

TCP Port: 10001

□ Allow Multiple Hosts to Connect [TruePort Lite Mode]

10. Select the **Hardware** tab.



Profile: **TruePort**

Name:

Serial Interface: EIA-232

Speed: 9600

Data Bits: 8

Parity: None

Stop Bits: 1

Duplex: Full

TX Driver Control: Auto

Flow Control: None

☑ Enable Inbound Flow Control

☑ Enable Outbound Flow Control

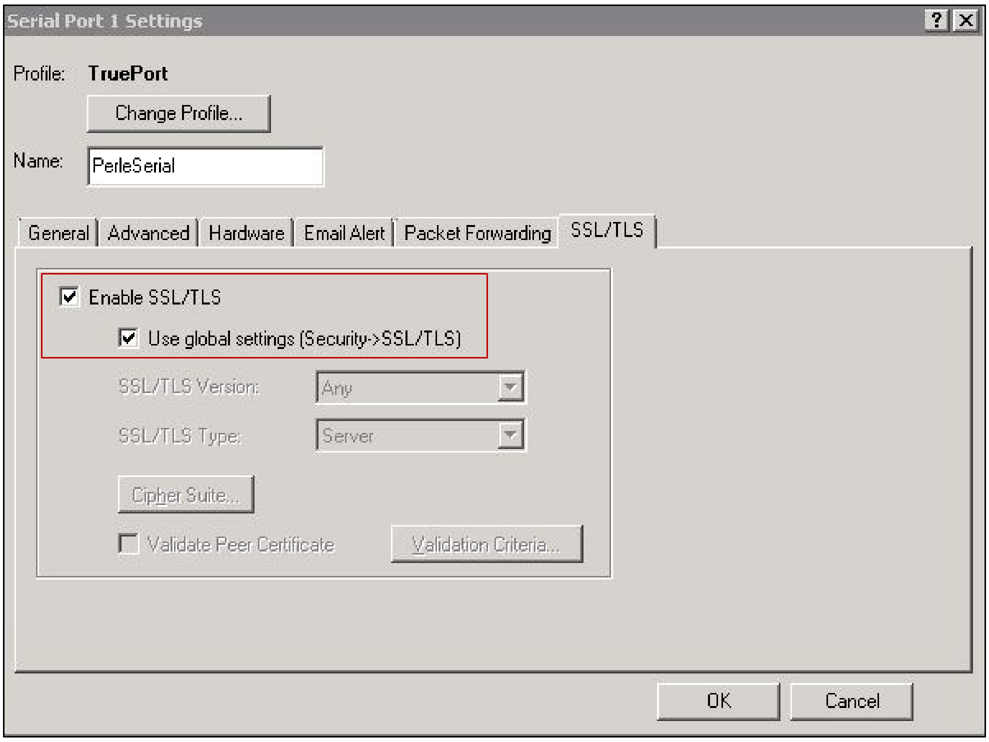
□ Monitor DSR

□ Monitor DCD

□ Discard Characters Received With Errors

□ Enable Echo Suppression

11. For **Serial Interface**, select either **EIA-232** (RS-232), **EIA-422** (RS-422) or **EIA-485** (RS-485).
12. Set **Speed** to the serial interface baud rate (for example, **9600**).
13. Set **Data Bits** to the number of bits of the serial protocol (for example, **8** bits).
14. Select the appropriate **Parity**.
15. Set the appropriate number of **Stop Bits**.
16. Select the type of **Flow Control** used.
17. Do not select the **Monitor DSR** check box.
18. Do not select the **Monitor DCD** check box.
19. Select the **SSL/TLS** tab.



Profile: TruePort

Name: PerleSerial

☑ Enable SSL/TLS

☑ Use global settings (Security->SSL/TLS)

SSL/TLS Version: Any

SSL/TLS Type: Server

□ Validate Peer Certificate

20. Select the following check boxes:

- **Enable SSL/TLS**.
- **Use global settings (Security>SSL/TLS)**.

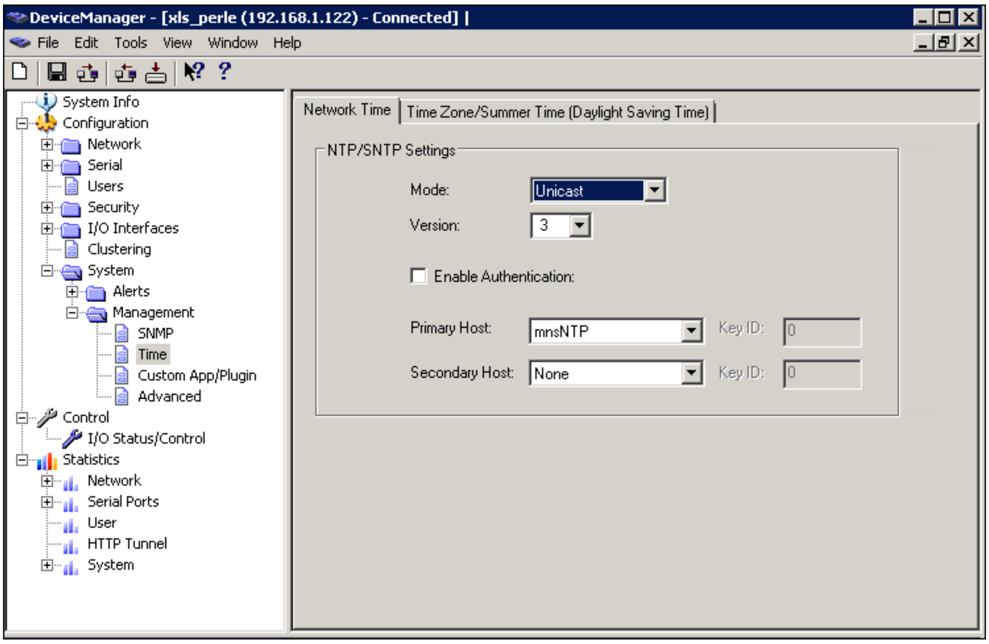
21. Click **OK**.

22. Select **Configuration > System > Management > Time**.

23. Select the **Network Time tab**.

24. Set the following parameters.

- **SNTP Mode**: Unicast
- **SNTP Version**: 3
- **Primary Host**: Select the NTP server name created earlier.
- **Secondary Host**: Select alternative NTP server name, otherwise set the name as Primary Host.
  NOTE: **Network Time** works best when the version matches that of the NTP server. Windows time servers generally default to Version 2. External NTP servers generally work with Version 3. If unsure, verify with the client's network administrator.



NTP/SNTP Settings

Mode: Unicast

Version: 3

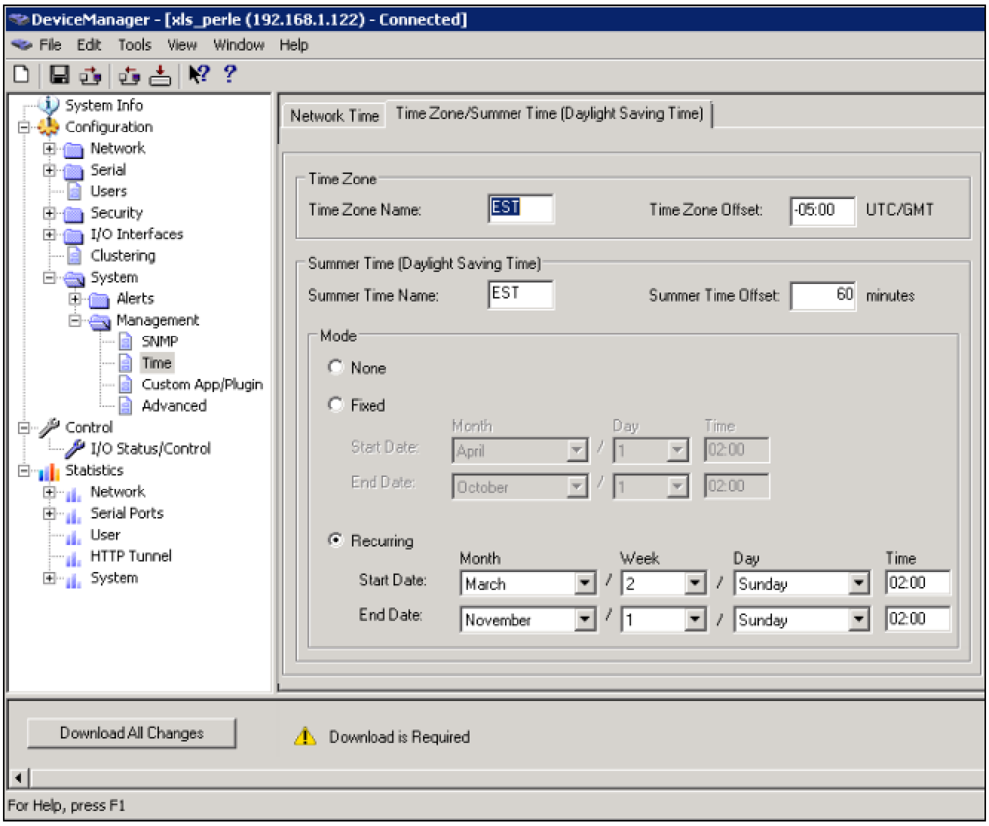
☐ Enable Authentication:

Primary Host: mnsNTP Key ID: 0

Secondary Host: None Key ID: 0

25. Select the **Time Zone/Summer Time (Daylight Saving Time)** tab.

26. Configure the parameters as per the details mentioned in Time Zone/Summer Time (Daylight Saving Time) parameters.



Time Zone

Time Zone Name: EST Time Zone Offset: -05:00 UTC/GMT

Summer Time (Daylight Saving Time)

Summer Time Name: EST Summer Time Offset: 60 minutes

Mode

○ None

○ Fixed

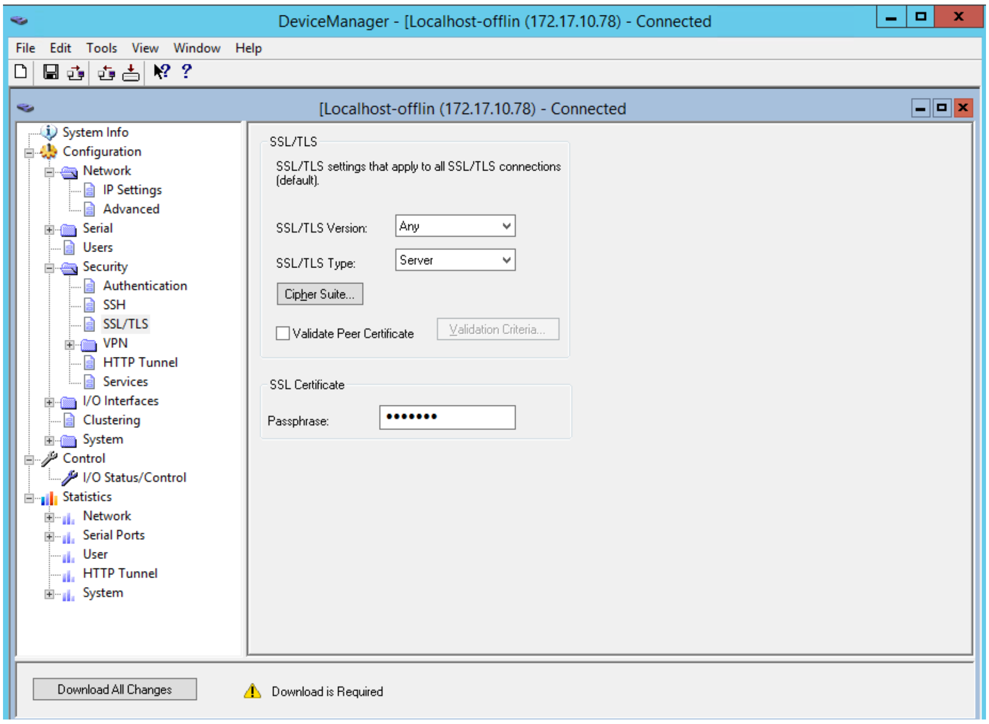
	Month	Day	Time
Start Date:	April	1	02:00
End Date:	October	1	02:00

● Recurring

	Month	Week	Day	Time
Start Date:	March	2	Sunday	02:00
End Date:	November	1	Sunday	02:00

Download is Required

27. Select **Configuration>Security>SSL/TLS**.



SSL/TLS settings that apply to all SSL/TLS connections (default).

SSL/TLS Version: Any

SSL/TLS Type: Server

☐ Validate Peer Certificate

Passphrase: •••••••

Download is Required

28. Set **SSL/TLS Version** field to **Any**.

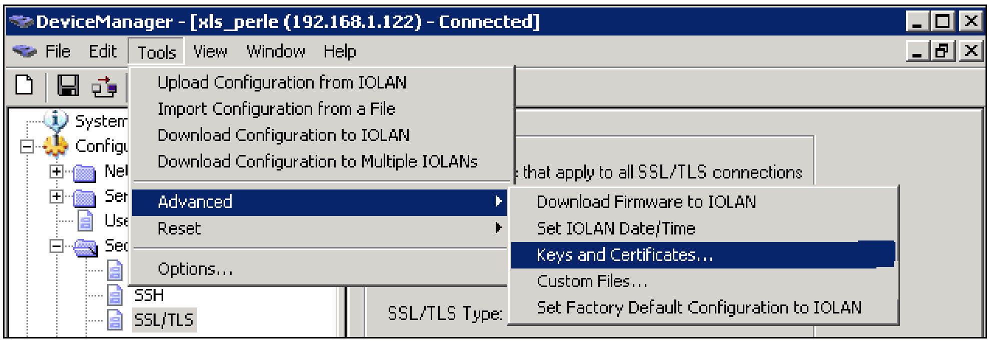
29. Set **SSL/TLS Type** field to **Server**.

30. Select the **SSL Certificate** expander.

31. Enter the password of the Root certificate(.pem) in the **Passphrase** field.

32. Select **Tools > Advanced > Keys and Certificates**.

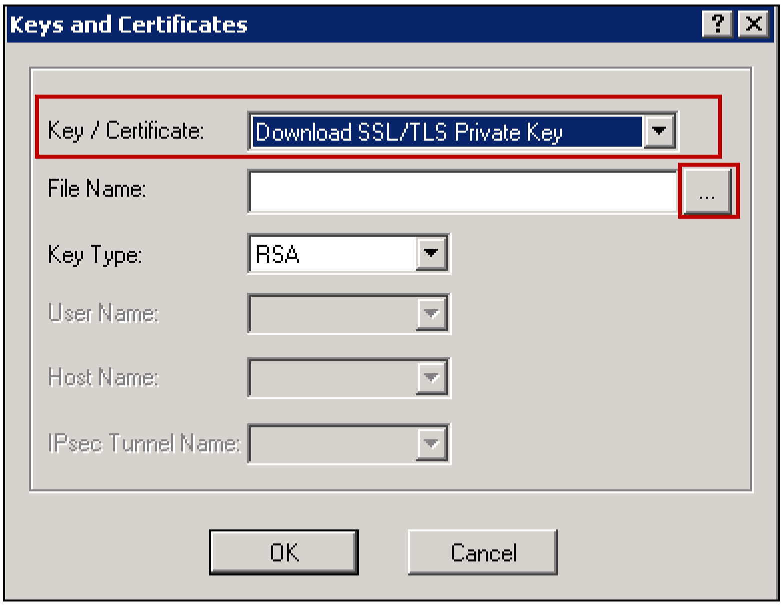
➩ The **Keys and Certificates** dialog box displays.


DeviceManager - [xls_perle (192.168.1.122) - Connected]
File Edit Tools View Window Help
Upload Configuration from IOLAN
Import Configuration from a File
Download Configuration to IOLAN
Download Configuration to Multiple IOLANs
Advanced
Reset
Options...
Download Firmware to IOLAN
Set IOLAN Date/Time
Keys and Certificates...
Custom Files...
Set Factory Default Configuration to IOLAN
System
Config
Net
Ser
Use
Sec
SSH
SSL/TLS
that apply to all SSL/TLS connections
SSL/TLS Type:

33. In the **Key/Certificate** drop-down list, select **Download SSL/TLS Private Key**.

34. Click the browse button and upload the private key for the root certificate(.pem).

35. Click **OK**.



36. Select **Tools > Advanced > Keys and Certificates**.

37. In the **Key/Certificate** drop-down list, select **Download SSL/TLS Certificate**.

38. Click the browse button and upload the combined root certificate (RootCombineCert.pem file). Refer to the Device Configuration section for more information on combining the root certificate.

39. Click **OK**.

40. Select **Tools>Advanced>Keys and Certificates**.

41. In the **Key/Certificate** drop-down list, select **Download SSL/TLS CA**.

42. Click the browse button and upload the Root certificate (RootCertificate.pem file).

43. Click **OK**.

44. Click **Download All Changes** to make the changes to the device.

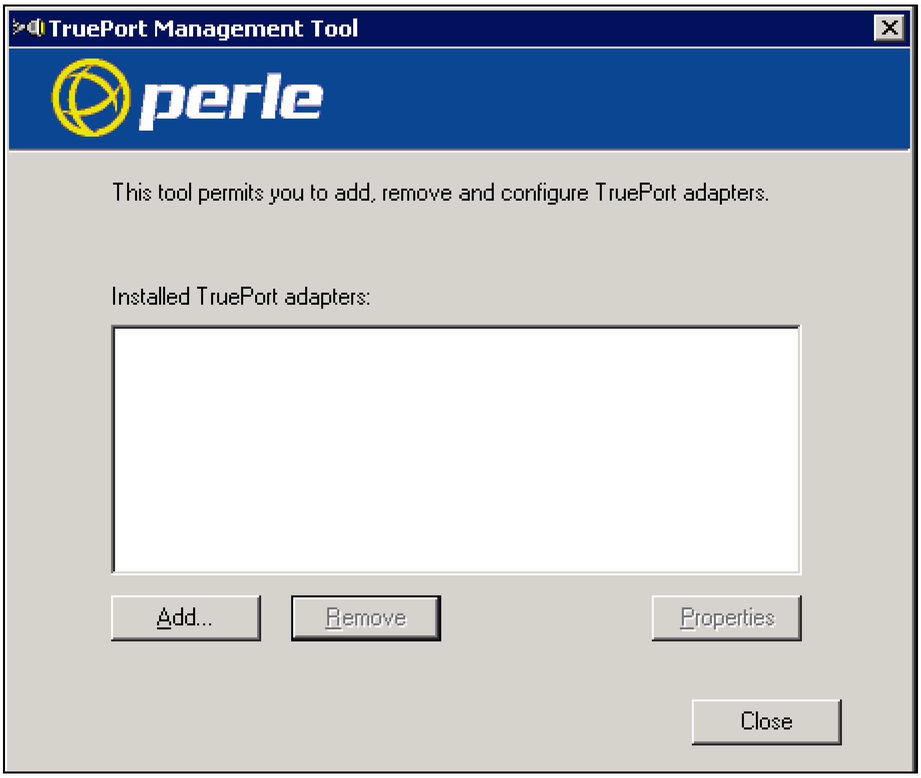
45. Click **Reboot IOLAN**.
NOTE: If a reboot is performed on the device, or power is reconnected, it will take 90 seconds for the device to reboot and initialize. When the device is ready, the Power button will be solid green and the Link button will be solid amber or green.

⇨ The device is now configured.

TruePort Driver Configuration

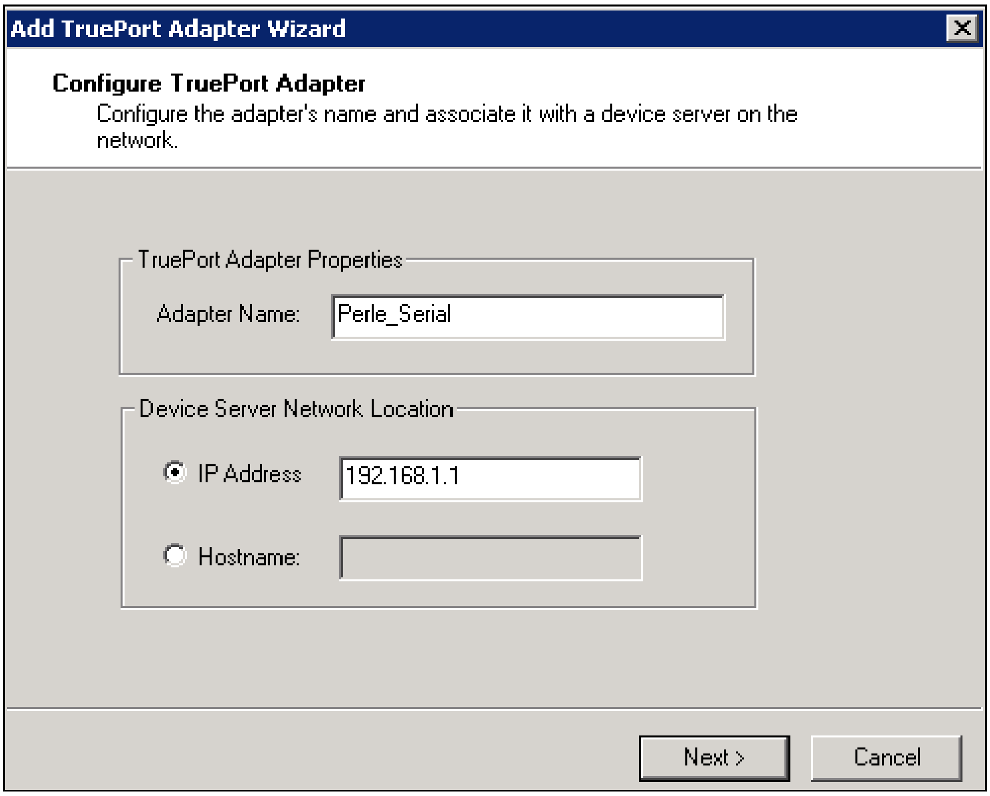
▷ The TruePort driver is the second part of the process to link the device to the server. TruePort is only used when the device is configured with the TruePort profile. The TruePort driver is designed to manage all similar devices communicating with the server. Since TruePort creates a virtual COM port, the recommended procedure is that each device has a unique COM port for each service.
NOTE: Serial communication and I/O access are each considered a separate service and therefore require separate COM ports.

1. Install TruePort on the server.
2. Start the **TruePort Management Tool**.
3. At the **TruePort Management Tool** window, click **Add**.


TruePort Management Tool
perle
This tool permits you to add, remove and configure TruePort adapters.
Installed TruePort adapters:
Add...
Remove
Properties
Close

4. Enter a name for the TruePort Adapter.
NOTE: This adapter will serve a particular device and therefore map to a specific COM port. Try to make the name descriptive so that the adapter can easily be tracked back to a particular device.

5. Enter the IP Address or the Hostname the device is using, and then click **Next**.


Add TruePort Adapter Wizard
Configure TruePort Adapter
Configure the adapter's name and associate it with a device server on the network.
TruePort Adapter Properties
Device Server Network Location
Next >
Cancel

Adapter Name: Perle_Serial

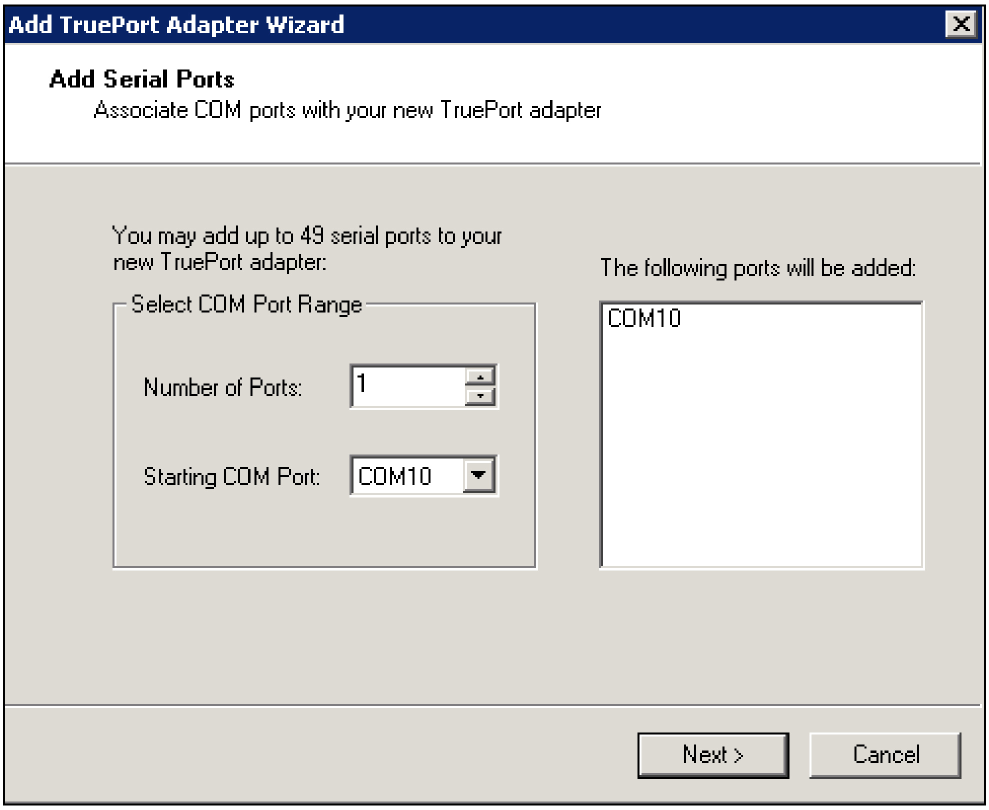
● IP Address 192.168.1.1

○ Hostname:

6. Leave the number of ports set to **1** (if also using I/O access, then it is also possible to set ports to **2**, or add another later). Select the COM port needed to assign to that particular device. By convention, start at COM100 and increment

for each device and service configured. This will help to avoid any conflicts with the existing COM ports or other devices. TruePort allows for the creation of up to 4096 COM ports.

7. Click **Next**.



Add TruePort Adapter Wizard

Add Serial Ports

Associate COM ports with your new TruePort adapter

You may add up to 49 serial ports to your new TruePort adapter:

Select COM Port Range

Number of Ports: 1

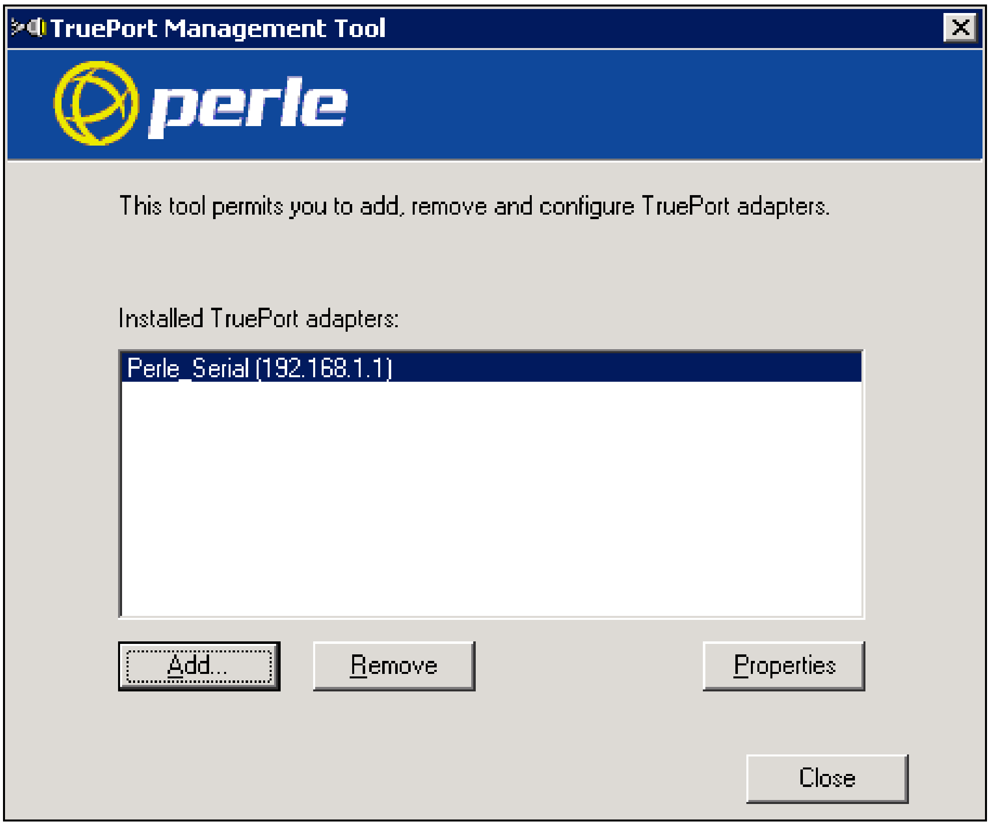
Starting COM Port: COM10

The following ports will be added:

COM10

➪ The TruePort Adapter will be visible in the **TruePort Management Tool**.

8. To edit the TruePort settings, select the adapter to edit and click **Properties**.



TruePort Management Tool

This tool permits you to add, remove and configure TruePort adapters.

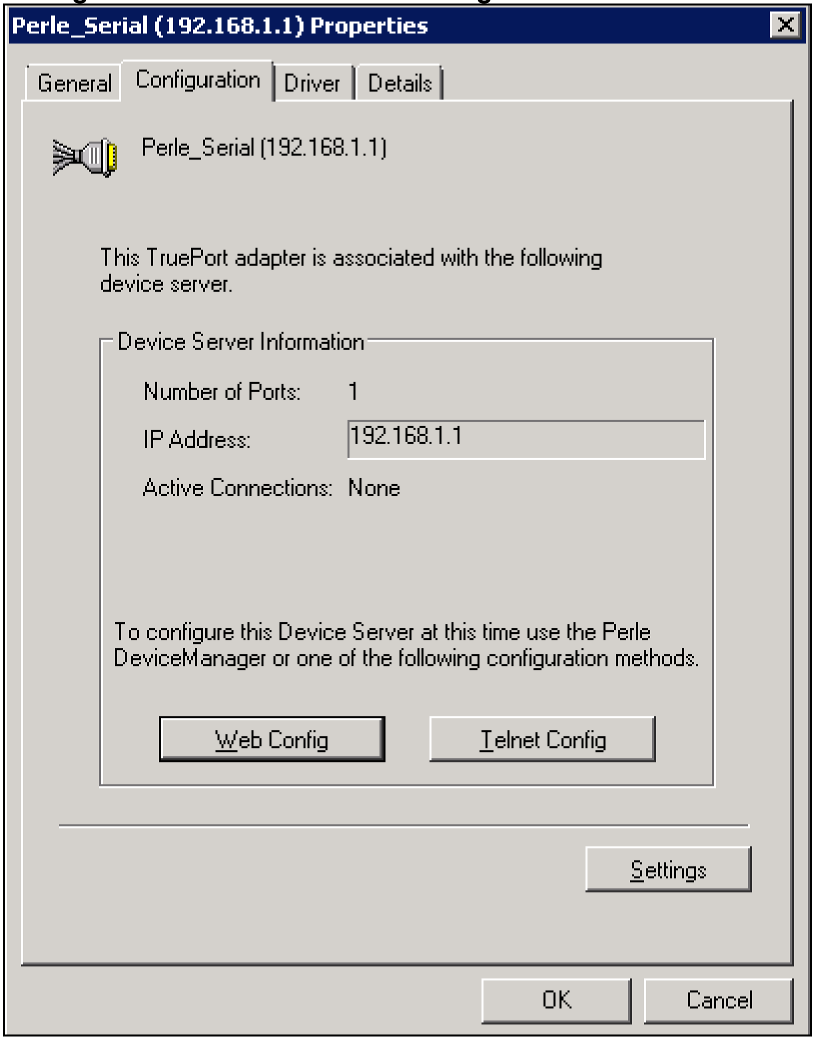
Installed TruePort adapters:

Perle_Serial (192.168.1.1)

Fig. 2: Installed TruePort Adapters

ESPA Paging System - Serial Settings

1. Select the Properties window of the device port to be configured, click the **Configuration** tab and then click **Settings**.



Perle_Serial (192.168.1.1) Properties

Perle_Serial (192.168.1.1)

This TruePort adapter is associated with the following device server.

Device Server Information

Number of Ports: 1

IP Address: 192.168.1.1

Active Connections: None

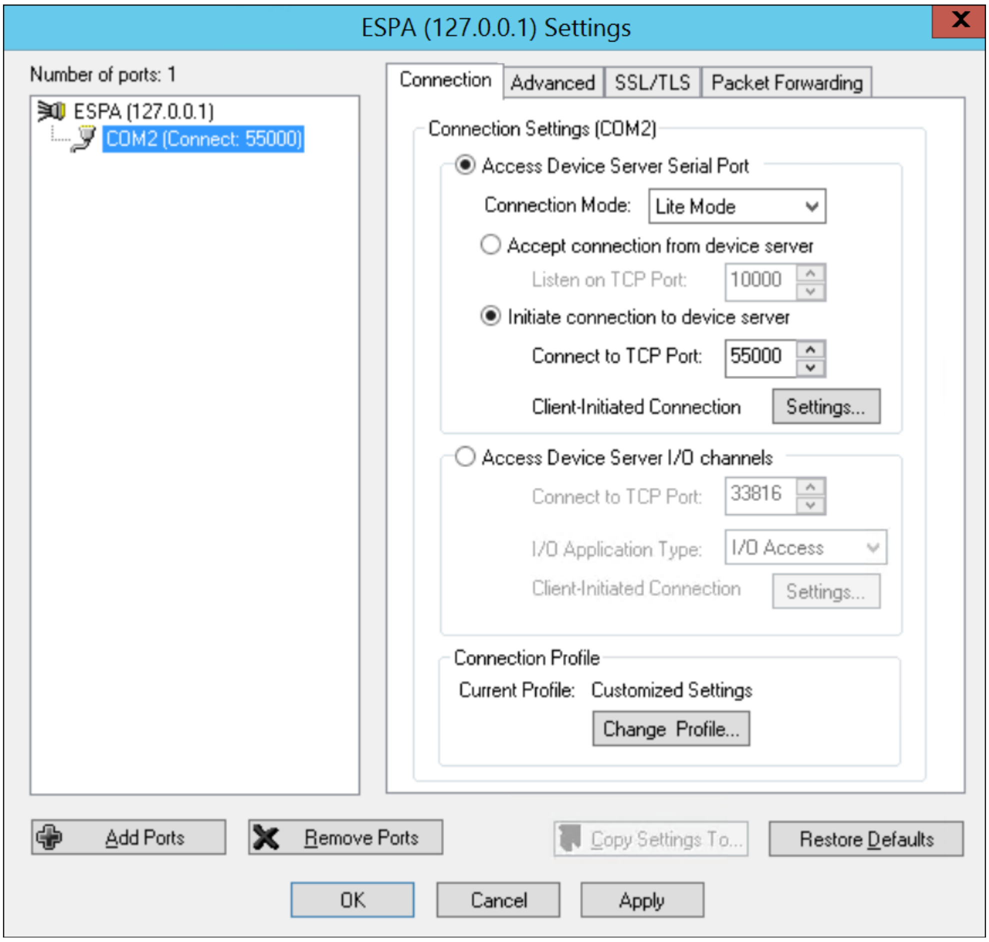
To configure this Device Server at this time use the Perle DeviceManager or one of the following configuration methods.

2. Click the target COM port listed in the tree view.

   ➪ The TruePort and COM port settings for this adapter displays.

3. Select the **Connection** tab.

4. Select **Initiate connection to device server**.



● Access Device Server Serial Port

Connection Mode: Lite Mode

○ Accept connection from device server

Listen on TCP Port: 10000

● Initiate connection to device server

Connect to TCP Port: 55000

Client-Initiated Connection [Settings...]

○ Access Device Server I/O channels

Connect to TCP Port: 33816

I/O Application Type: I/O Access

Client-Initiated Connection [Settings...]

Connection Profile

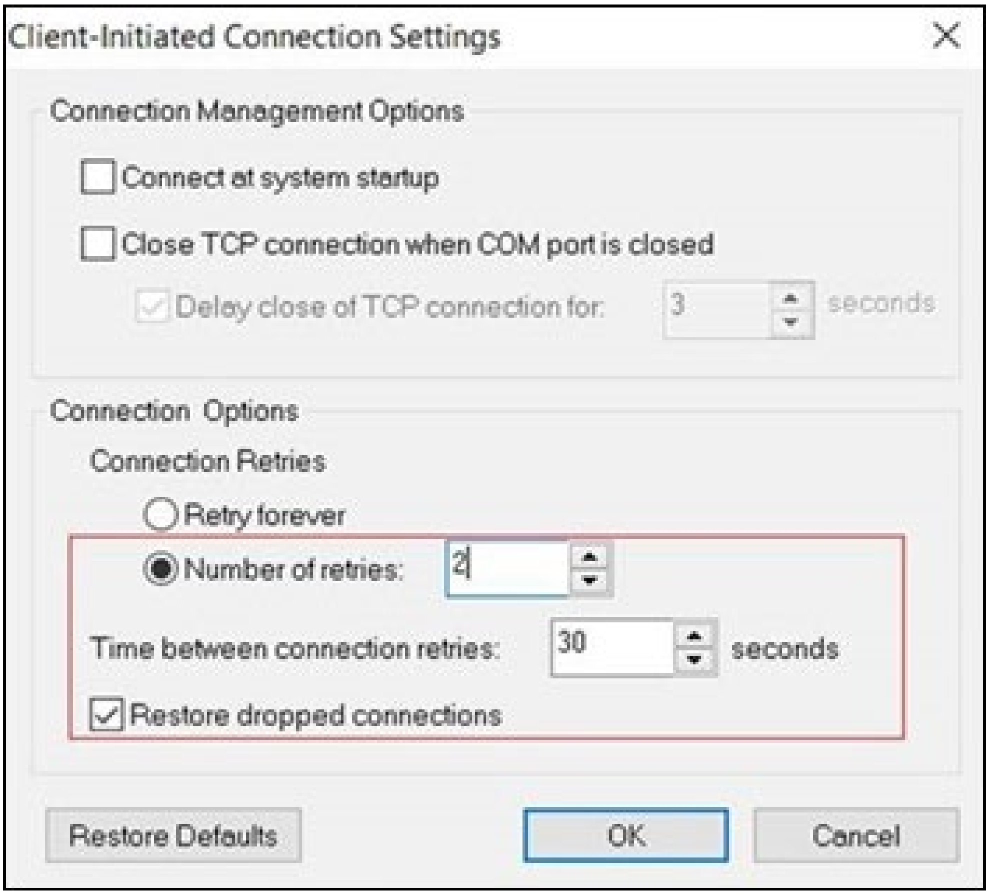
Current Profile: Customized Settings

[Change Profile...]

– Select **Connect to TCP Port**, enter the port number that was previously assigned to the device through the Perle DeviceManager.

5. Click the **Settings** button next to **Client-Initiated Connection**.

⇨ The following window displays:



Client-Initiated Connection Settings

Connection Management Options

□ Connect at system startup

□ Close TCP connection when COM port is closed

☑ Delay close of TCP connection for: 3 seconds

Connection Options

Connection Retries

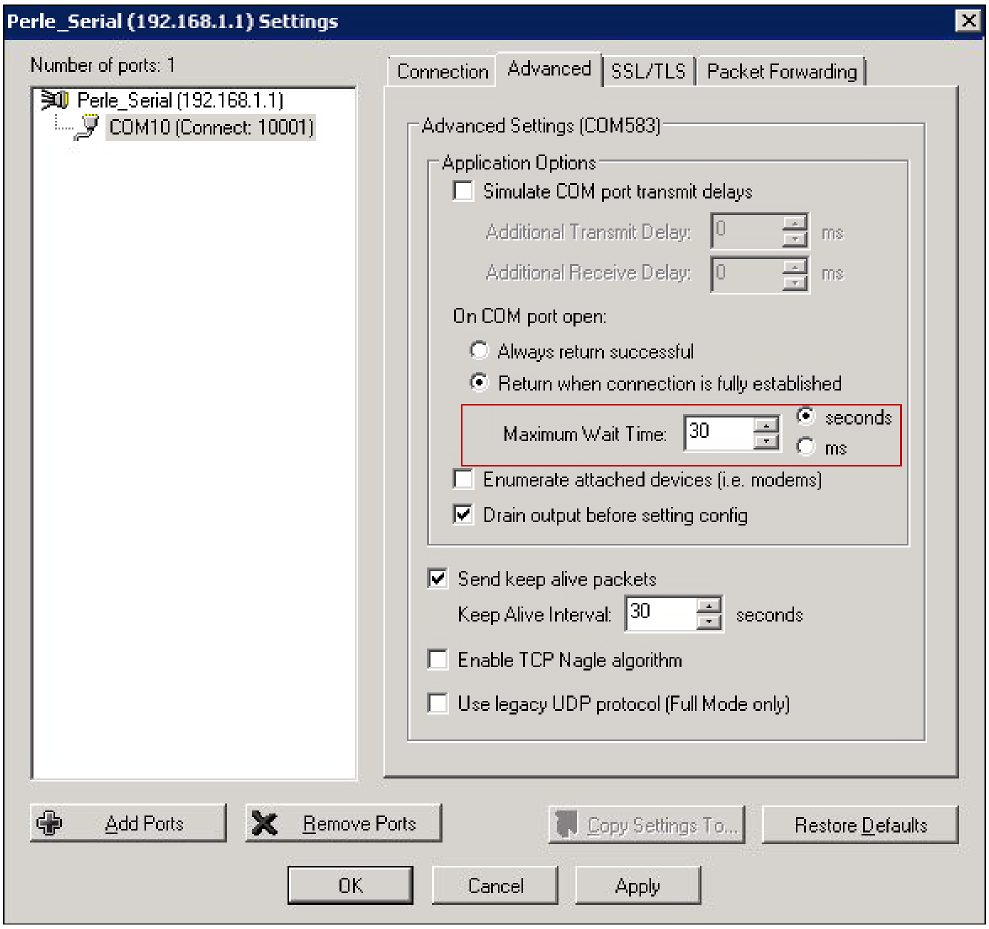
○ Retry forever

● Number of retries: 2

Time between connection retries: 30 seconds

☑ Restore dropped connections

6. Select the **Connect at system startup** check box.
7. For **Connection Retries**, select **Retry forever**.
8. Click **OK**.
9. Click the **Advanced** tab.



Perle_Serial (192.168.1.1) Settings

Number of ports: 1

Perle_Serial (192.168.1.1)
COM10 (Connect: 10001)

Advanced Settings (COM583)

Application Options

□ Simulate COM port transmit delays

Additional Transmit Delay: 0 ms

Additional Receive Delay: 0 ms

On COM port open:

○ Always return successful

● Return when connection is fully established

Maximum Wait Time: 30 ● seconds ○ ms

□ Enumerate attached devices (i.e. modems)

☑ Drain output before setting config

☑ Send keep alive packets

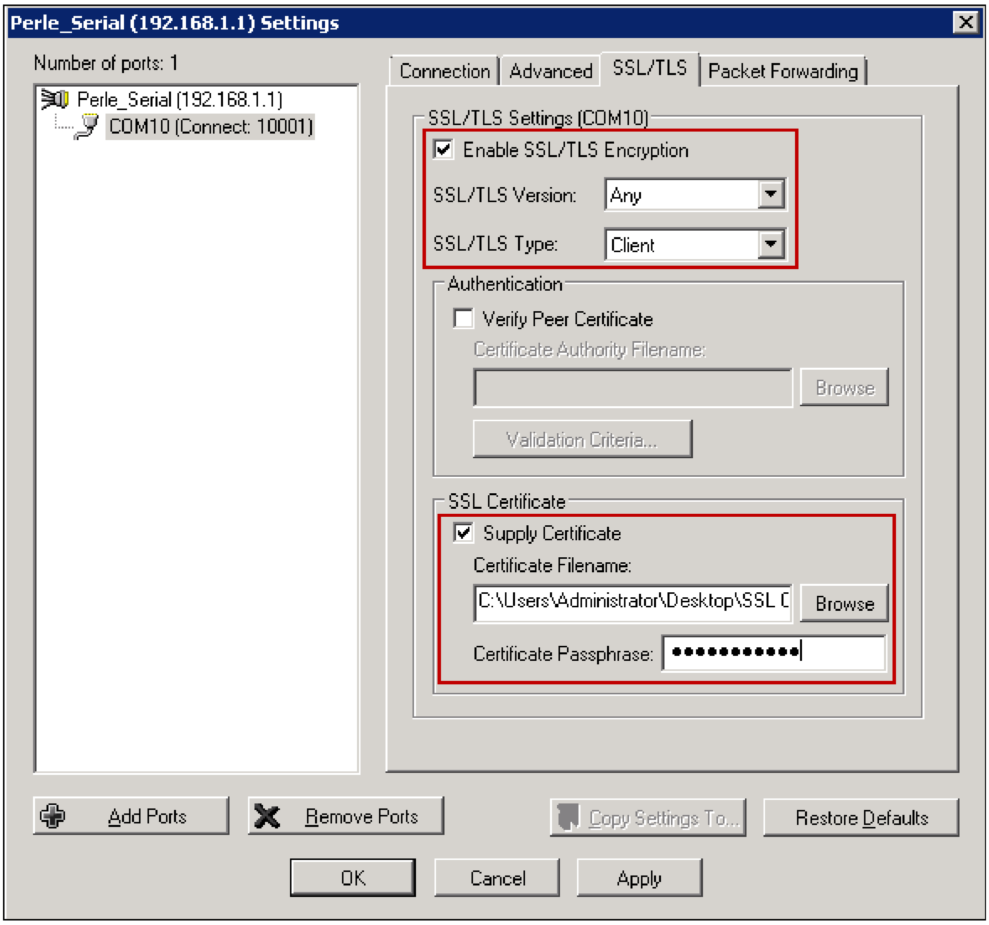
Keep Alive Interval: 30 seconds

□ Enable TCP Nagle algorithm

□ Use legacy UDP protocol (Full Mode only)

10. Set **Maximum Wait Time** to **30 seconds**.

11. Select the **SSL/TLS** tab.



Number of ports: 1

Perle_Serial (192.168.1.1)
COM10 (Connect: 10001)

SSL/TLS Settings (COM10)

☑ Enable SSL/TLS Encryption

SSL/TLS Version: Any

SSL/TLS Type: Client

Authentication

☐ Verify Peer Certificate

Certificate Authority Filename:

SSL Certificate

☑ Supply Certificate

Certificate Filename: C:\Users\Administrator\Desktop\SSL C

Certificate Passphrase: ●●●●●●●●●●●●

12. Select the **Enable SSL/TLS Encryption** check box.

13. Set the **SSL/TLS Version** field to **Any**.

14. Set the **SSL/TLS Type** field to **Client**.

15. Select the **Supply Certificate** check box.

16. Click the browse button and select the combined Root certificate. Refer to the Device Configuration section for more information on combining a Root certificate.

17. Enter the password in the **Certificate Passphrase** field.

18. Click **Apply** and then **OK**.

19. Restart the Perle TruePort service.

Device Verification

ESPA Paging System - Serial Port

The easiest method to test the serial port is to attach the Perle device to the ESPA Paging System Managed device and view any incoming messages directly from a serial terminal, such as PuTTY.

PuTTY can be downloaded from the following link:

http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe

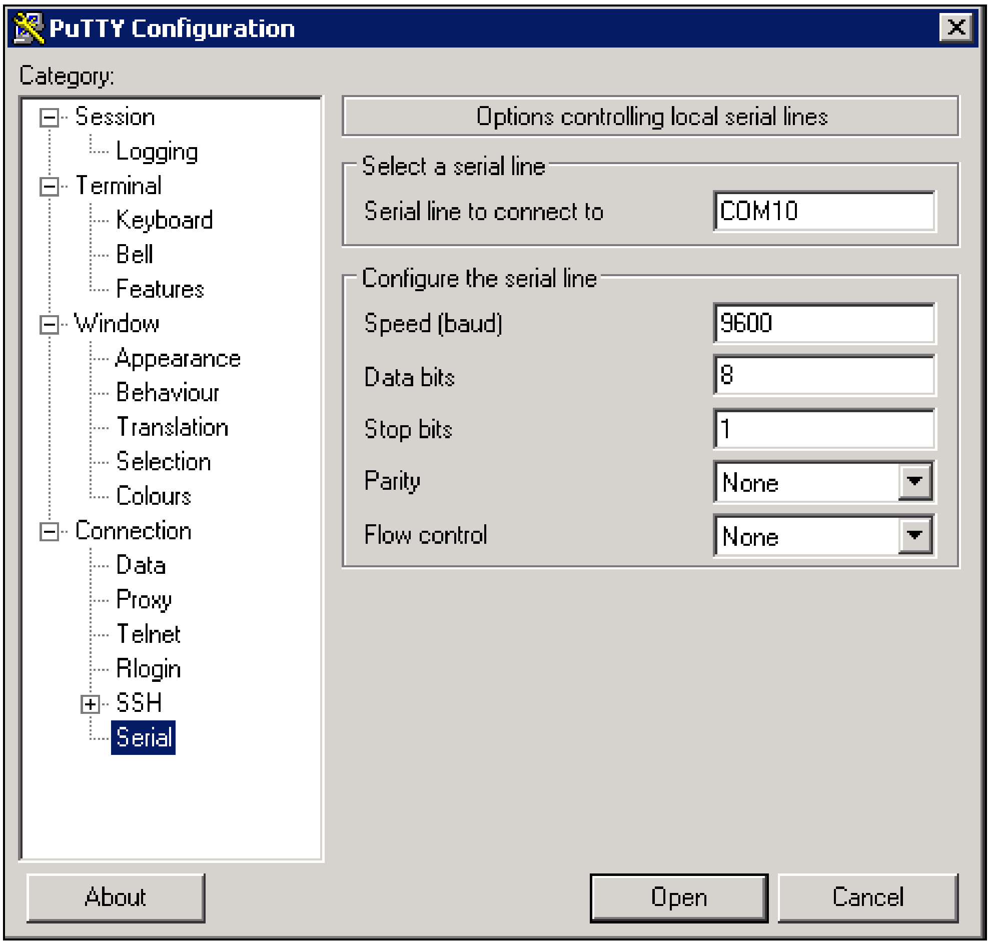
To test the serial port, open up PuTTY from the server on the serial COM port. If the COM port opens, then the TruePort driver is working properly.

The steps for testing ESPA Paging System communication are as follows:

1. Open PuTTY, and select **Connection** > **Serial**.

2. For **Serial line to connect to**, enter the TruePort COM port number.

3. Enter the parameters for **Speed (baud)**, **Data bits**, **Stop bits**, **Parity** and **Flow control** for the external device that will be transmitting ESPA Paging System data.



Options controlling local serial lines

Select a serial line

Serial line to connect to: COM10

Configure the serial line

Speed (baud): 9600

Data bits: 8

Stop bits: 1

Parity: None

Flow control: None

4. Select **Session > Serial**.
5. Click **Open** to establish a serial session.
6. While the serial session is open, force a response from the external device so that serial ESPA Paging System data is sent. This data should now be in the terminal session.
   NOTE: If no data is sent, verify that RX and TX pins are not switched. If data is incoherent, check that the serial settings (**baud rate**, **data bits**, **stop bits**, **parity**, and **flow control**) are all set properly. Settings need to match in PuTTY, Perle (through Perle device manager) and the external ESPA Paging System Managed device.

ESPA Paging System Troubleshooting

Problem: Once the device is created in the **Device Editor** section, the corresponding device gets in **Connected** state based on the **Check Status Rate** configured in the **Configuration Properties** of the driver. However, at times the device does not get connected after the **Check Status Rate** duration.

Solution: Perform the following steps in sequence until the device gets connected after a particular step. After each step, wait for the **Check Status Rate** duration and monitor the device connection status

1. Restart the TruePort service.
2. Reimport the certificates on device manager and reboot the Perle IOLAN device.
3. Reboot the Server.
4. Disconnect the power cable of the Perle IOLAN device, wait for a few seconds and then reconnect the power cable.
5. Power off and on the devices connected to the Perle IOLAN device.

Installing ESPA 4.4.4 Interface Device

This section provides information for mounting the hardware and gives details about the wiring and connection of the device.

Prerequisites

The prerequisites for the installation of ESPA 4.4.4 Interface Managed device are as follows:

- ESPA 4.4.4 Interface Managed device
- RS-232 communication cable
  NOTE: As per ESPA 4.4.4 protocol, enter the following values for the corresponding fields while configuring the ESPA 4.4.4 Managed device: Data Bits - 7, Parity - even parity, and Stop Bits – 2

Mechanical Installation

For instructions on the mechanical installation, refer to the manufacturer’s installation manual included with the ESPA 4.4.4 Interface Managed device.

Electrical Installation

For instructions on the electrical installation, see the installation manual included by the manufacturer with the ESPA 4.4.4 Interface Managed device.

Perle Device Installation

Prerequisites

Before proceeding, ensure that the following items are available:

- Perle IOLAN SDS1 (serial only model)
- 9-30VDC (400mA min) power supply, if not included with device
- Category 5 Ethernet cable
- Computer or server in the same subnet network as the device
- The device installation CD or a computer with network access
- DB9 RS-232 serial cable – for use in serial communication applications.
  NOTE 1: The driver (TruePort) used to communicate with the device must be installed on the same server/machine that runs the MNS application.
  NOTE 2: Have an RJ45 jack available that is connected to a properly configured IP network. The network must allow for IP addresses to be assigned statically or through DHCP.
  NOTE 3: To configure the device, a computer located in the same network is required.
  NOTE 4: Prior to commissioning the system, a compatibility check should be performed for all devices and services to be integrated (refer to the Notification *System Description* document for compatibility information).

Mounting

The Perle device has two brackets on the side of the mounting holes. The recommended procedure is to fasten the device to a flat surface by placing screws through the mounting holes.

Power

1. For the Perle device, use a power adaptor capable of 9-30VDC output and 400mA. If there is a barrel connector, cut the connector off and plug the leads into the terminal block marked **9-30VDC** on the device.
2. Before supplying power, check the polarity of the adaptor leads. The grounded lead should connect to the pin marked "–".
3. The hot lead should be connected to the pin marked "**+**".

⇨ On each power-up or reboot, the device takes at least 90 seconds before becoming operational. When the device is completely booted up, the **Power/Ready** display should be solid green.

Ethernet

1. Plug one end of the Ethernet cable to the RJ45 jack on the device.
2. Connect the other end of the Ethernet cable to your network jack.

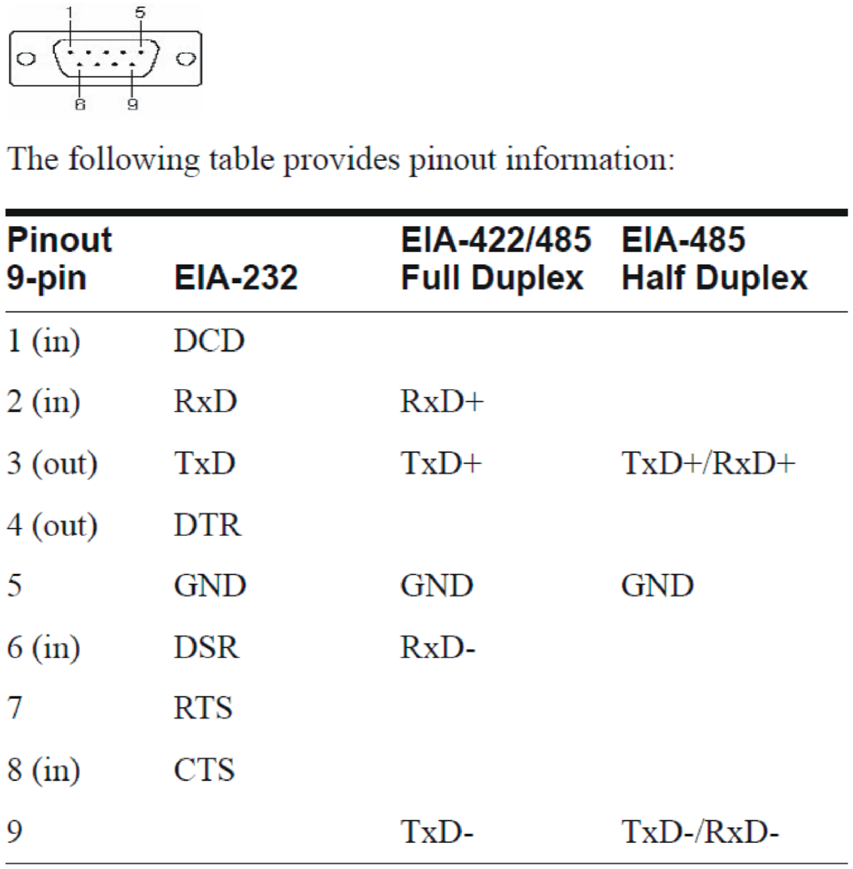
⇨ After a few seconds, the **Link/10/100** should be solid amber or green.
NOTE: Amber refers to a 100Mb connection. Green refers to a 10Mb connection.
NOTE:
The device does not have DHCP turned on as factory default. Configure the device to use DHCP or assign a static IP with a computer that is attached to the same subnet.

Serial Connector

Plug one end of the serial cable to the DB9 connector on the device. Connect the other end of the serial cable to the device that will communicate serially.

Some devices do not have different connectors for serial communication or custom pinout. As a result, use the DB9 pinout for the following Perle device as a reference on how to properly wire the serial cable.

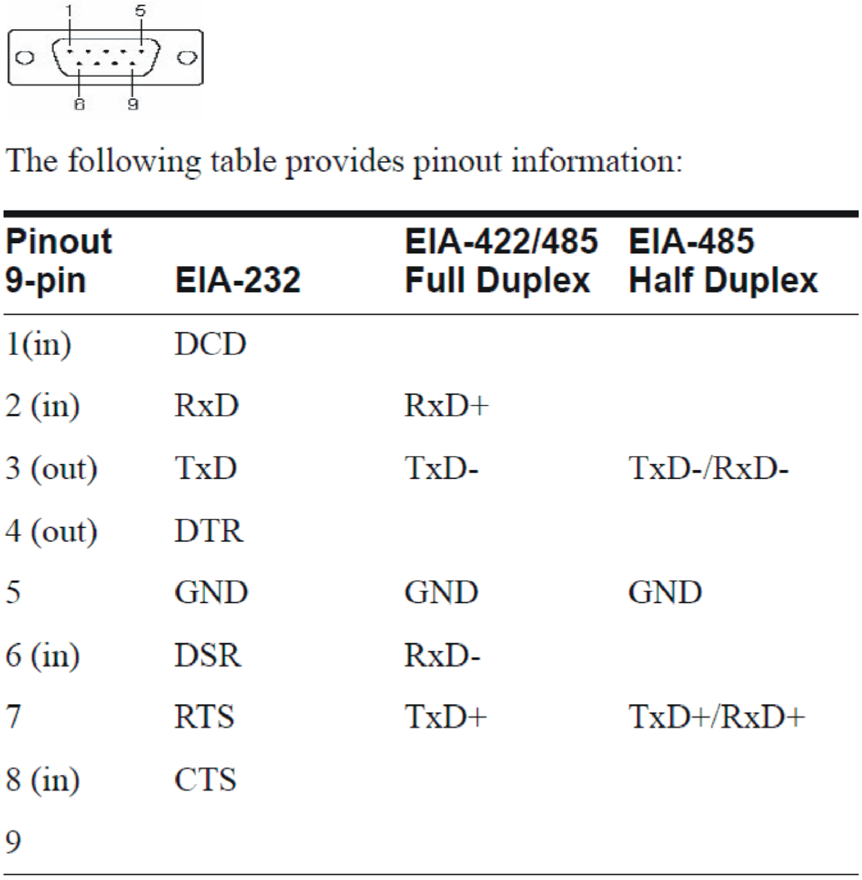
NOTE:
Keep the Console/Serial switches on the device in OFF position.



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-

Fig. 3: SDS1 Pinout



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	TxD+	TxD+/RxD+
8 (in)	CTS		
9			

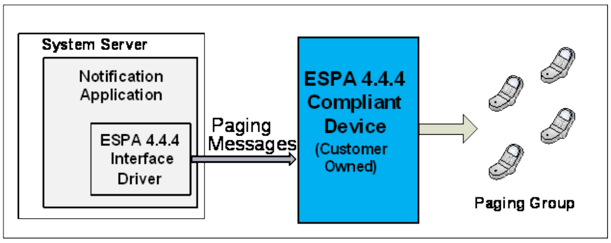
Fig. 4: TD2R2 Pinout

NOTE:
RS232 pinout on both models are the same. However, RS485 pinout differs on both.

ESPA Paging System Device

This section provides reference and background information for integrating the European Selective Paging Manufacturer's Association (ESPA) 4.4.4 compliant device. For procedures or workflows, see the step-by-step section.

Notification provides the capability to integrate with existing paging systems in the ESPA 4.4.4 protocol, this allows Notification to send messages to paging recipients. The following figure is a conceptual overview of a simplified set up.

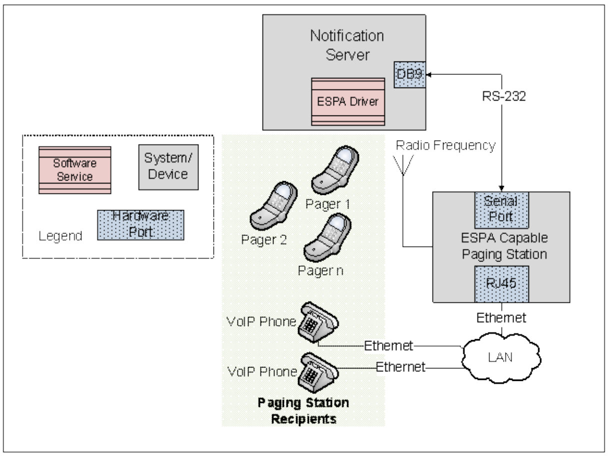

System Server
Notification Application
ESPA 4.4.4 Interface Driver
Paging Messages
ESPA 4.4.4 Compliant Device (Customer Owned)
Paging Group

Note 1: The paging messages launched by Notification cannot be canceled. Notification only supports Launch operations for paging messages.

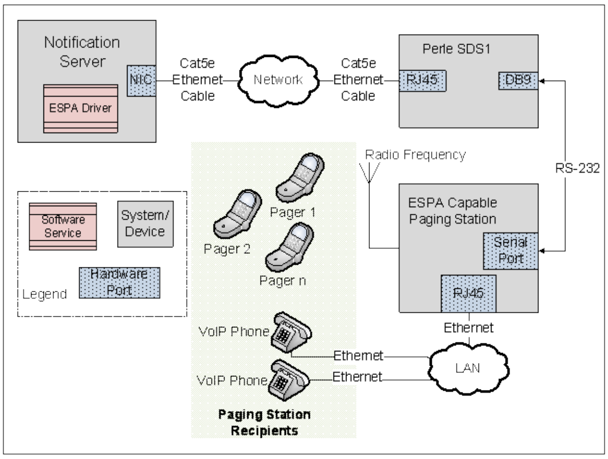
Note 2: The ESPA 4.4.4 protocol supports up to 128 characters. However, the ASCOM device currently tested with Notification supports 120 characters.

Note 3: The ESPA 4.4.4 protocol only supports the International Alphabet No. 5 (IA5) character set.

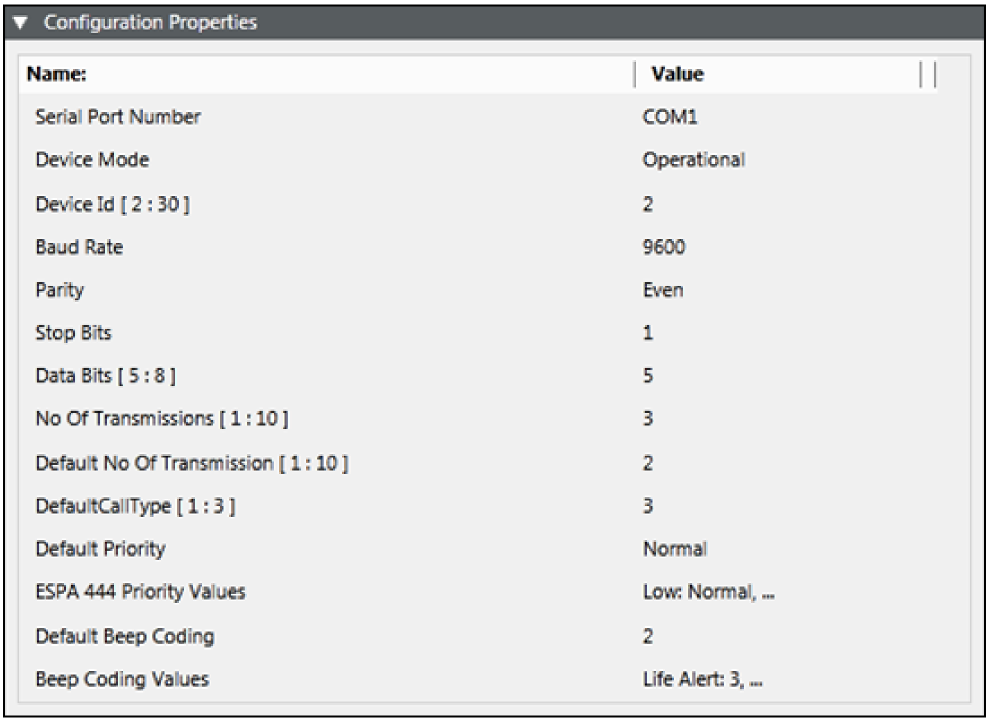
Below is an overview over a system using the RS-232 configuration:



ESPA Paging System ration:



ESPA Paging System –Configuration Properties



Configuration Properties

Name:	Value
Serial Port Number	COM1
Device Mode	Operational
Device Id [2 : 30]	2
Baud Rate	9600
Parity	Even
Stop Bits	1
Data Bits [5 : 8]	5
No Of Transmissions [1 : 10]	3
Default No Of Transmission [1 : 10]	2
DefaultCallType [1 : 3]	3
Default Priority	Normal
ESPA 444 Priority Values	Low: Normal, ...
Default Beep Coding	2
Beep Coding Values	Life Alert: 3, ...

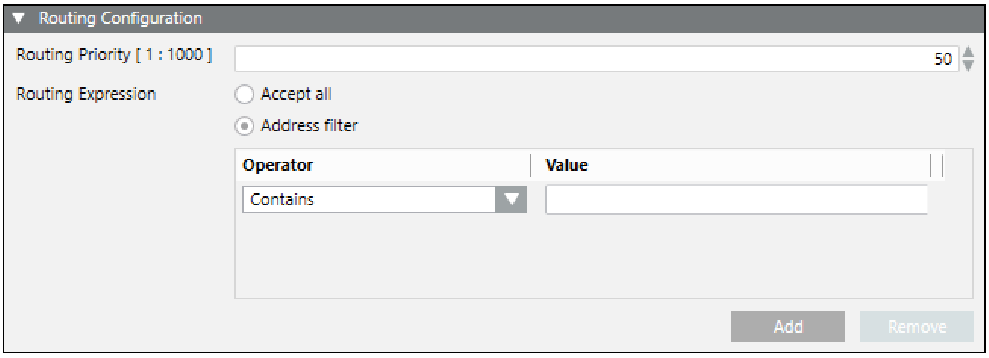
- **Serial Port Number**: Enter the COM port address of the device. The user should enter a valid COM port address string of the device. This string should always have the format as COM followed by an unassigned integer number, for example, COM1.
- **Device Mode**: Select one of the following modes from the drop-down list: **Disabled**: In this mode, the driver does not process the messaging command

and/or the device configuration change command, but will perform status checks for the device. The device remains in a Disconnected state.
Operational: In this mode, the driver processes the messaging command, the device configuration change command, and performs status checks for the device. The device will be in a Disconnected / Connected state based on the connection state.
Administrative: In this mode, the driver processes the device configuration change command and performs status checks for the device. The device will be in a Disconnected / Connected state based on the connection state.

- **Device ID**: Enter the ID assigned to the device.
- **Baud Rate**: Select the Baud Rate the device is using serially from the drop-down list.
- **Parity**: Select the Parity, the device is using from the drop-down list.
- **Stop Bits**: Select the number of Stop Bits, the device serial protocol is using from the drop-down list.
- **Data Bits**: Select the number of Data Bits, the device is using to communicate serially.
  NOTE: The value range is 5 to 8 bits.
- **No. of Transmissions**: Enter the number of attempts, a message should be sent by the ESPA managed device to the corresponding recipients. For example, if the No. of Transmissions is set to 3, the ESPA managed device sends the message 3 times to the recipients. If the delivery of the message to the recipients is successful in these 3 attempts, the ESPA managed device sends the acknowledgement to the Notification system. If the delivery is not successful, the ESPA managed device sends the negative acknowledgement to the Notification system.
- **Default No. of Transmissions**: Enter the default value of the number of transmissions of the ESPA managed device.
  NOTE: Refer to the configuration manual provided by the ESPA managed device manufacturer for the default values. Change the default value but the value defined in the ESPA managed device should be equal to the value defined in Default No. of Transmissions field of the Notification system.
- **Default Call Type**: Contains the default values of call types for the ESPA managed device. The details of each call type are mentioned below:
  1 - Reset (cancel) call
  2- Speech call
  3 - Standard call
  NOTE: Refer to the configuration manual provided by the ESPA managed device manufacturer for the default values.
- **Default Priority**: Contains the default value of priority for the ESPA managed device.
  NOTE: Refer to the configuration manual provided by the ESPA managed device manufacturer for the default values.
- ESPA 4.4.4 Priority Values: Map the message priority with the ESPA 4.4.4 priority values.
- **Default Beep Coding**: Contains the default value of beep coding records for the ESPA managed device.
  NOTE: Refer to the configuration manual provided by the ESPA managed device manufacturer for the default values.
- Beep Coding Values: Maps the message type with the beep coding values.

ESPA Paging System - Routing Configuration

The **Routing Configuration** expander displays the fields required for the configuration of routing priority and routing expressions for the device. It is possible to add more than one operator in the **Routing Expression** expander. The logical function followed here is OR. For example, if the user selects **Contains** as one operator and **Starts with** as another operator, Notification will search for either the value specified under **Starts with** or **Contains** operators.



▼ Routing Configuration

Routing Priority [1 : 1000]: 50

Routing Expression: ○ Accept all ● Address filter

Operator	Value
Contains	

- **Routing Priority**: Select the routing priority for the ESPA managed device. If more than one managed devices of the same type are configured, then based on this priority setting, the managed device is selected sequentially. For verifying whether this device can be used for sending message to a recipient or not, the routing expression of the managed device must match the address format of the recipient. Select any number from 1 to 1000.
NOTE: A Routing Priority of 1 will have the highest priority.
- **Routing Expression**: Enter an operator. This operator is evaluated against the recipient user device addresses. If a recipient address matches the operator set in the Routing Expression, the message for that recipient user device address gets routed through an intermediate device.
- **Accept all**: Select to allow all routing expressions.
- **Address filter**: Select to allow a specific operator listed under Operator drop-down list.
- ESPA 4.4.4 Interface - Operator: Select a filter criterion.
- **Value**: Enter the value for the selected filter criterion.
- **Add**: Allows the user to add an operator.
- **Remove**: Allows the user to remove an operator.

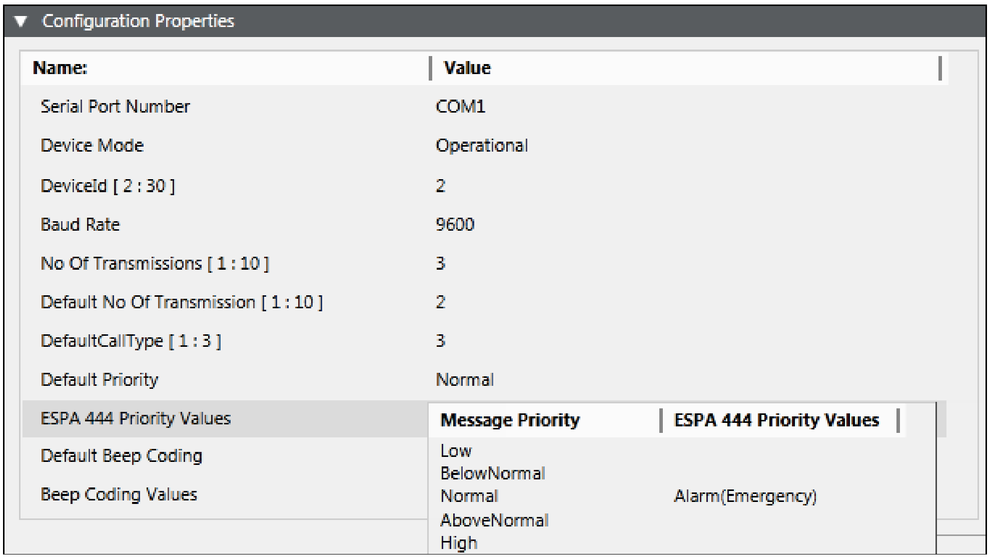
ESPA Paging System - Operator

Operator	Description
Contains	Checks whether the recipient user address string contains the assigned value or not. If it does, the corresponding message is routed through the device.
Does Not Contain	Checks whether the recipient user address string contains the assigned value or not. If it does not, the corresponding message is routed through the device.
Starts with	Checks whether the recipient user address string starts with the assigned value or not. If it does not, the corresponding message is routed through the device.
Does Not Start With	Checks whether the recipient user address string starts with the assigned value or not. If it does not, the corresponding message is routed through the device.
Ends With	Checks whether the recipient user address string ends with the assigned value or not. If it does, the corresponding message is routed through the device.
Does Not End With	Checks whether the recipient user address string ends with the assigned value or not. If it does not, the corresponding message is routed through the device.
Equals	Checks whether the recipient user address string is equal to the assigned value or not. If it does, the corresponding message is routed through the device. This operator performs character by character match between the recipient user device address and the assigned value. If the recipient user device address is 91-123 and the assigned value is 91123, the corresponding message is not routed through the device.

Not equals	Checks whether the recipient user address string is equal to the assigned value or not. If it does not, the corresponding message is routed through the device. This operator performs character by character match between the recipient user device address and the assigned value. If the recipient user device address is 91-123 and the assigned value is 91123, the corresponding message is routed through the device.
Less Than	This operator is evaluated only with numeric values (whole numbers or non-negative integers) of the recipient user device address and the assigned value. Enter numeric values from 0 to 9,223,372,036,854,775,807 (maximum 64 bits long). If the recipient user device address string contains a character other than digits or + or - sign, the corresponding message is not routed through the device. This operator performs mathematical Less Than or Equal To (<=) operation.
Less Than Or Equal To	This operator is evaluated only with numeric values (whole numbers or non-negative integers) of the recipient user device address and the assigned value. Enter numeric values from 0 to 9,223,372,036,854,775,807 (maximum 64 bits long). If recipient user device address string contains a character other than digits or + or - sign, the corresponding message is not routed through the device. This operator performs mathematical Less Than or Equal To (<=) operation.
Greater Than	This operator is evaluated only with numeric values (whole numbers or non-negative integers) of the recipient user device address and the assigned value. Enter numeric values from 0 to 9,223,372,036,854,775,807 (maximum 64 bits long). If the recipient user device address string contains a character other than digits or + or - sign, the corresponding message is not routed through the device. This operator performs mathematical Less Than or Equal To (<=) operation.
Greater Than Or Equal To	This operator is evaluated only with numeric values (whole numbers or non-negative integers) of the recipient user device address and the assigned value. Enter numeric values from 0 to 9,223,372,036,854,775,807 (maximum 64 bits long). If the recipient user device address string contains a character other than digits or + or - sign, the corresponding message is not routed through the device. This operator performs mathematical Less Than or Equal To (<=) operation.
Regular expression	This operator is used to evaluate the recipient device address with Regular expression given in the assigned value string.

ESPA Paging System - Device Capability Mapping to Message Priorities

The ESPA Paging System Managed device allows the mapping of the ESPA 4.4.4 priority values to the message priorities of outgoing messages. For every message priority select ESPA 4.4.4 priority values. For example, a notification priority High can be associated with ESPA 4.4.4 priority value Alarm (Emergency). Refer to the following image for more information.



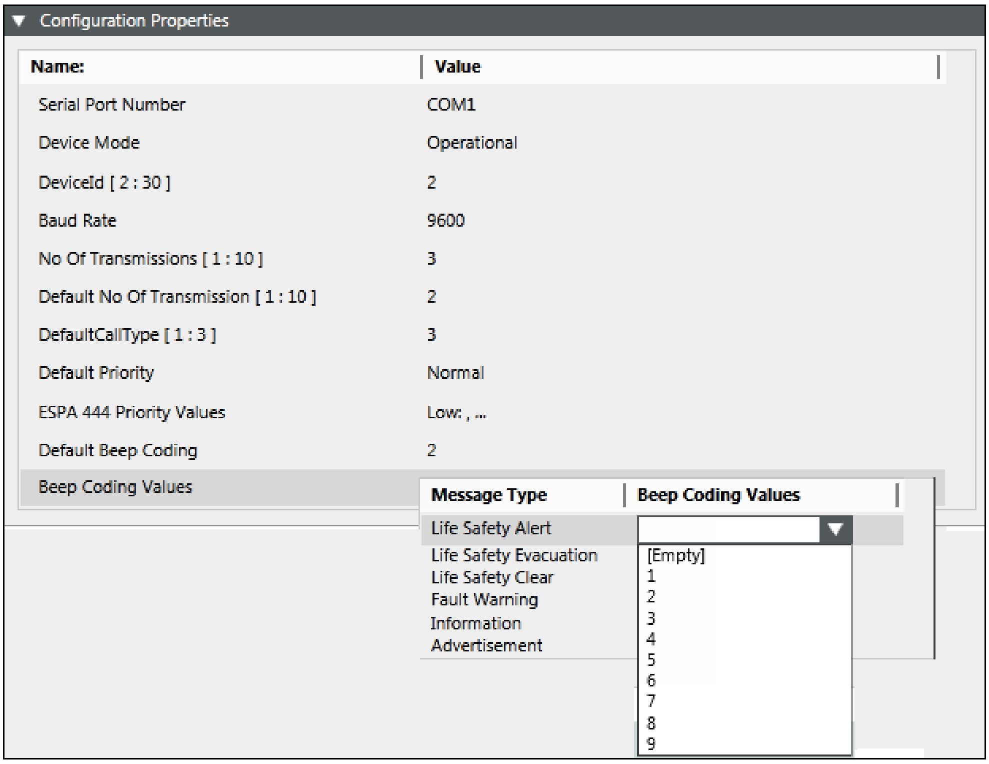
Configuration Properties

Name:	Value
Serial Port Number	COM1
Device Mode	Operational
DeviceId [2 : 30]	2
Baud Rate	9600
No Of Transmissions [1 : 10]	3
Default No Of Transmission [1 : 10]	2
DefaultCallType [1 : 3]	3
Default Priority	Normal
ESPA 444 Priority Values	
Default Beep Coding	
Beep Coding Values	

Message Priority	ESPA 444 Priority Values
Low	
BelowNormal	
Normal	Alarm(Emergency)
AboveNormal	
High	

ESPA Paging System - Device Capability Mapping to Message Types

The ESPA 4.4.4 Managed device allows mapping of each message type to a corresponding beep coding value. Select a beep coding value for each message type. The beep coding values are available in the drop-down list. Refer to the following image for details.



Name:	Value
Serial Port Number	COM1
Device Mode	Operational
DeviceId [2 : 30]	2
Baud Rate	9600
No Of Transmissions [1 : 10]	3
Default No Of Transmission [1 : 10]	2
DefaultCallType [1 : 3]	3
Default Priority	Normal
ESPA 444 Priority Values	Low: , ...
Default Beep Coding	2
Beep Coding Values	

Message Type	Beep Coding Values
Life Safety Alert	
Life Safety Evacuation	
Life Safety Clear	
Fault Warning	
Information	
Advertisement	

Examples of Regular Expressions

Regular Expressions	Description
^\d+	String starts with one or more digits only.
^[+](91)	String should start with +91.
^.+?\d$	String ending with digits only.
^[0-9]{10}(52|56|57)$	String is 12 digits long (numbers only) and ends with 52, 56, or 57.
^9881231231$	Matching exact mobile number.

1.2 GSM Modem Device

GSM Gateway

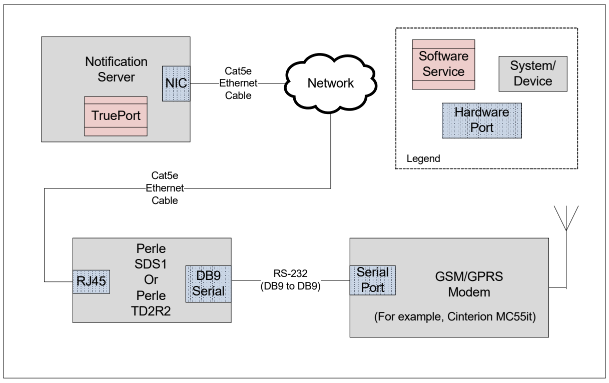
This section provides reference and background information for integrating the Global System for Mobile Communications (GSM) Gateway with the system. For procedures or workflows, see the step-by-step section.

Notification allows configuration of the GSM Terminal device to deliver SMS messages to intended recipients and to receive reply SMS messages from the recipient users. The system sends messages to the SMS receiver devices using a GSM Gateway with Attention (AT) command.

The GSM Terminal device can be configured using Perle configuration or using Serial Cable configuration using the Recommended Standard 232 interface (RS 232).

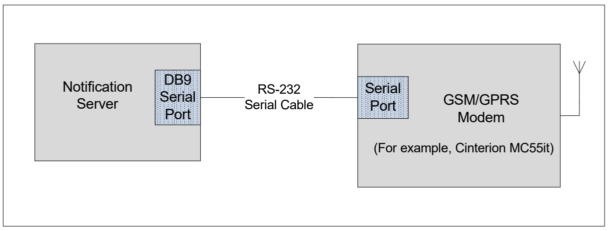
Use the two examples with images below for further information:

Below is an overview over the system using the Perle configuration:



NOTE 1:
The GSM Terminal device accepts a SIM card that has SMS services enabled. Without enabling these services on a SIM card, you cannot send SMS through the device.
NOTE 2:
In order to use message reply and the escalation functionality, the mobile number configured in the recipient user device must have the following number format: +[country code][number]. For example, +17327572923.
NOTE 3:
Notification through GSM modem supports Universal Coded Character Set 2-byte (UCS-2) character encoding. For example; it is possible to send Cyrillic and Chinese SMS.

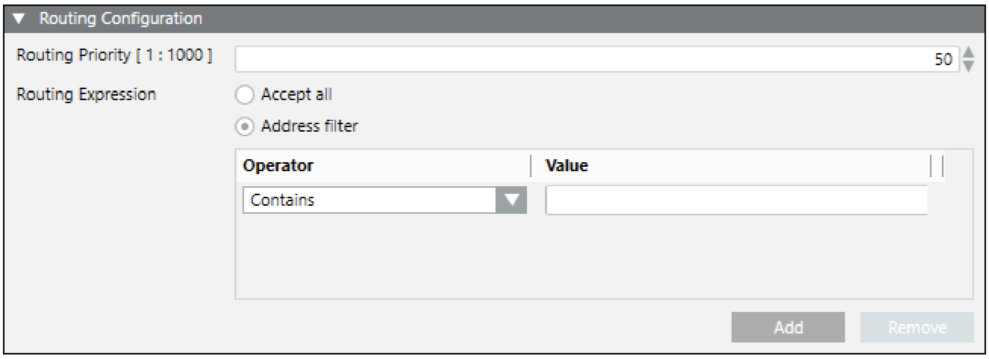
Below is an overview over the system using Serial Cable configuration:



NOTE:
The Configuring GSM Gateway section details the configuration settings required while using Perle. If using the Serial Cable configuration, skip the *Perle Device Installation* and *Engineering* sections.

Routing Configuration Expander

This expander displays the fields required for the configuration of the routing priority and routing expressions for the device. More than one operator can be added under the **Routing Expression** expander. The logical function followed here is OR. For example, if you select **Contains** as one operator and **Starts with** as another operator, Notification will search for either the value specified under **Starts with** or **Contains**.



Routing Priority [1 : 1000] 50
Routing Expression ○ Accept all
● Address filter

Operator	Value
Contains	

- **Routing Priority**: Select the routing priority for the GSM Terminal device. The routing priority determines, in which order the routing expressions of the devices configured under the same field network are evaluated. Select a number between 1 and 1000 as the Routing Priority.
NOTE 1: A Routing Priority of 1 will have the highest priority.

NOTE 2: It is acceptable that two GSM Terminal devices have the same routing priority as long as it is guaranteed that their routing expressions cannot match against the same recipient user device address. The routing expressions have to be mutually exclusive otherwise, the system's routing behavior is non-deterministic.

- **Routing Expression**: Enter one or more Operator/Value expressions. These expressions are evaluated against each Recipient User Device address that a message is sent to. If an address matches at least one of the Operator/Value expressions of a GMS Terminal device, the message to that Recipient User Device will be routed through the intermediate GMS Terminal device.
- **Accept all**: Specify if this managed device can be used for messaging to a recipient that is in any address format.
- **Address filter**: Select to accept only those routing expressions which meet the conditions set under Operator and Value.
- Operator: Select the condition for the routing expression from the drop-down list.
- **Value**: Enter a suitable value for the selected Operator condition.
- **Add**: Add Operator and Value.
- **Remove**: Remove Operator and Value.

Operator Conditions for the Routing Expressions

Operator	**Description**
Contains	Checks whether the recipient user address string contains the assigned value. If yes, the corresponding message is routed through the device.
Does Not Contain	Checks whether recipient user address string contains the assigned value. If not, the corresponding message is routed through the device.
Starts with	Checks whether recipient user address string starts with the assigned value. If yes, the corresponding message is routed through the device.
Does Not Start With	Checks whether recipient user address string starts with the assigned value. If not, the corresponding message is routed through the device.
Ends With	Checks whether recipient user address string ends with the assigned value. If yes, the corresponding message is routed through the device.
Does Not End With	Checks whether recipient user address string ends with the assigned value. If not, the corresponding message is routed through the device.
Equals	Checks whether recipient user address string is equal to the assigned value. If yes, the corresponding message is routed through the device. This operator performs a character by character match between the recipient user device address and the assigned value. If the recipient user device address is 91-123 and the assigned value is 91123, the corresponding message is not routed through the device.
Not equals	Checks whether recipient user address string is equal to the assigned value. If not, the corresponding message is routed through the device. This operator performs a character by character match between the recipient user device address and the assigned value. If the recipient user device address is 91-123 and the assigned value is 91123, the corresponding message is not routed through the device.
Less Than	This operator is evaluated only with numeric values (whole numbers or non-negative integers) of the recipient user device address and the assigned value. You can enter numeric values from 0 to 9,223,372,036,854,775,807 (maximum 64 bits long). If the recipient user device address string contains a character other than digits or a + or - sign, the corresponding message is not routed through the device. This operator performs the mathematical Less Than or Equal To (<=) operation.

Less Than Or Equal To	This operator is evaluated only with numeric values (whole numbers or non-negative integers) of the recipient user device address and the assigned value. You can enter numeric values from 0 to 9,223,372,036,854,775,807 (maximum 64 bits long). If the recipient user device address string contains a character other than digits or + or - sign, the corresponding message is not routed through the device. This operator performs the mathematical Less Than or Equal To (<=) operation.
Greater Than	This operator is evaluated only with numeric values (whole numbers or non-negative integers) of the recipient user device address and the assigned value. You can enter numeric values from 0 to 9,223,372,036,854,775,807 (maximum 64 bits long). If the recipient user device address string contains a character other than digits or a + or - sign, the corresponding message is not routed through the device. This operator performs the mathematical Less Than or Equal To (<=) operation.
Greater Than Or Equal To	This operator is evaluated only with numeric values (whole numbers or non-negative integers) of the recipient user device address and the assigned value. You can enter numeric values from 0 to 9,223,372,036,854,775,807 (maximum 64 bits long). If the recipient user device address string contains a character other than digits or + or - sign, the corresponding message is not routed through the device. This operator performs the mathematical Less Than or Equal To (<=) operation.
Regular expression	This operator is used to evaluate recipient device address with regular expression given in the assigned value string.

Examples of Regular Expressions

Regular Expressions	Description
^\d+	String starts with one or more digits only.
^[+](91)	String should start with +91.
^.+?\d$	String ending with digits only.
^[0-9]{10}(52|56|57)$	String is 12 digits long (numbers only) and ends with 52, 56, or 57.
^9881231231$	Matching exact mobile number.

GSM Modem

This section provides additional procedures for integrating the Global System for Mobile Communications (GSM) Gateway with the system.

Installing GSM Modem Device

This section provides information for mounting the hardware and gives details about the wiring / connection of the device.

Perle Device Installation

Prerequisites

Before proceeding, ensure that the following items are available:

- Perle IOLAN SDS1 TD2R2
- 9-30VDC (400mA min) Power Supply, if not included with Perle IOLAN SDS1 TD2R2
- Category 5 Ethernet cable
- Computer or Server to communicate with the device

The device Installation CD or a computer with network access.

NOTE 1:

The driver (TruePort) that is used to communicate with the device must be installed on the same server/machine that runs Notification.

NOTE 2:

Make sure to have an RJ45 jack available that is connected to a properly

configured IP network. The network must allow for IP addresses to be assigned statically or through Dynamic Host Configuration Protocol (DHCP).
NOTE 3:
To configure the device, a computer located in the same network is necessary.
NOTE 4:
The maximum cable length for a serial cable is 50 feet.

Mounting

The Perle SDS1 has two brackets on the side of the mounting holes. It is recommended to install the device on a flat surface by placing screws through the mounting holes.

Power

1. For the Perle SDS1, use a power adapter capable of 9-30VDC output and 400mA. If your Perle unit has terminal blocks for power, cut off the barrel connector of the power supply and plug the leads into the terminal block marked *9-30VDC* on the device.
2. Before supplying power, check the polarity of the adapter leads. The grounded lead should connect to the pin marked –.
3. The hot lead should be connected to the pin marked **+**.

⇨ On each power-up or reboot, the device takes at least 90 seconds before becoming operational. When the device is completely booted up, the **Power/Ready** LED will be solid green.

Ethernet

1. Plug one end of the Ethernet cable into the RJ45 jack on the device.
2. Connect the other end of the Ethernet cable to your network jack.

⇨ After a few seconds, the **Link/10/100** should be a solid orange or green color. **NOTE:** Orange color refers to a 100Mb connection. Green color refers to a 10Mb connection.

NOTE:
The device does not have DHCP turned on as a factory default setting. The device will need to be configured to use DHCP or assign a static IP with a computer that is attached to the same subnet.

Serial Connector

Plug one end of the serial cable into the DB9 connector on the device. Connect the other end of the serial cable to the GSM Terminal device with which serial communication is required.

NOTE: Keep the Console/Serial switches on the device in OFF position.

Terminal Device Installation

Prerequisites

The prerequisites for installing the GSM Terminal device are as follows:

- GSM Terminal device
- Standard serial cable
  NOTE :
  A USB-to-Serial converter is required if there are no serial ports available on the server.

Configuring and verifying GSM Modem

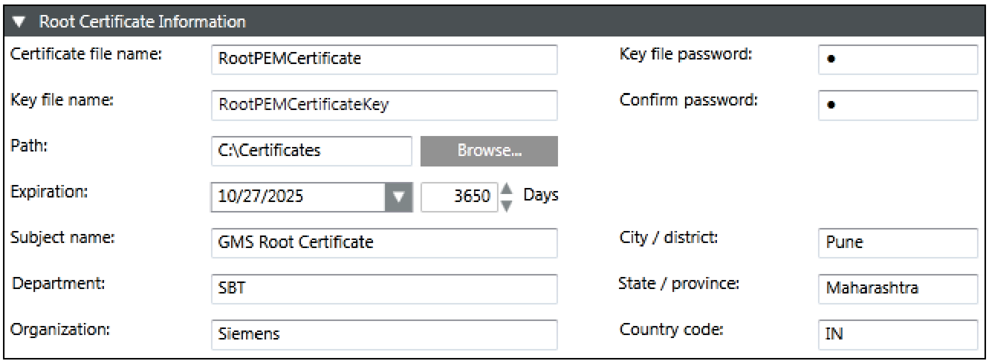
This section provides the steps linked with the configuration and verification of the device.

Certificate Creation From System Management Console

To establish a secure communication, certificates need to be configured.

Creating a Root Certificate (.pem)

1. In the **Console** tree, select the **Certificate** node.
   ⇨ The **Certificates** tab displays.
2. Click **Create Certificate** and then select **Create Root Certificate (.pem)** .
   ⇨ The **Root Certificate Information** expander displays.



▼ Root Certificate Information

Certificate file name:	RootPEMCertificate	Key file password:	•
Key file name:	RootPEMCertificateKey	Confirm password:	•
Path:	C:\Certificates Browse...		
Expiration:	10/27/2025 ▼ 3650 Days		
Subject name:	GMS Root Certificate	City / district:	Pune
Department:	SBT	State / province:	Maharashtra
Organization:	Siemens	Country code:	IN

3. In the **Root Certificate Information** expander, provide the details as follows:
   a. Enter the **Certificate file name**.
   b. Enter the **Key file name**.
   c. Enter the **Key file password** and **confirm** it.
   d. Browse for the location to store the root certificate and the root key file on the disk. By default, the path of the last created root certificate is selected.
   e. Set the **Expiration** (validity period) duration in days. By default, the certificate expires after 3650 days.
   f. Enter the following information about the Subject:
   —**Subject name**
   — *(Optional)* **Department**
   — *(Optional)* **Organization**
   — *(Optional)* **City / district**
   — *(Optional)* **State / province**
   — *(Optional)* **Country code** (maximum two characters)
4. Click **Save** .

⇨ If confirmed, the data entered during the root certificate creation is validated, and on successful root certificate creation,
- the new root certificate (.pem file) and the root key file are created at the specified location on the disk.

Working with (.pem) Root Certificates

- The **Certificate file name** and the **Key file name**
  - Must not contain blanks or special characters (/,\,?,<, >,*,|,").
  - The **Certificate file name** and the **Key file name** cannot be the same.
- When the user creates a root certificate for the first time, all the fields appear blank. For all subsequent root certificate creation (.pfx or .pem based), some fields, such as **Path**, **Organization**, and so on, are pre-populated with the information from the last-created root certificate.

Software Configuration

The software configuration needed to communicate to the device requires the following two main steps:

1. First, configure the internal settings of the device. To do this, install DeviceManager on a computer connected to the same network as the device to be configured.
2. The second step is to configure the driver on the computer that will be communicating with the device over the network. There are several methods used to communicate with the device, one of which is a TruePort driver.
   NOTE:
   TruePort is a COM port re-director driver utility that is installed on the server. This utility creates a *virtual serial port* or *virtual COM port*. All COM port directed data sent by the application is re-directed by TruePort across the IP/Ethernet network to the remote device. Data and serial port signaling is transparently communicated between the application and remote device.

Device Configuration

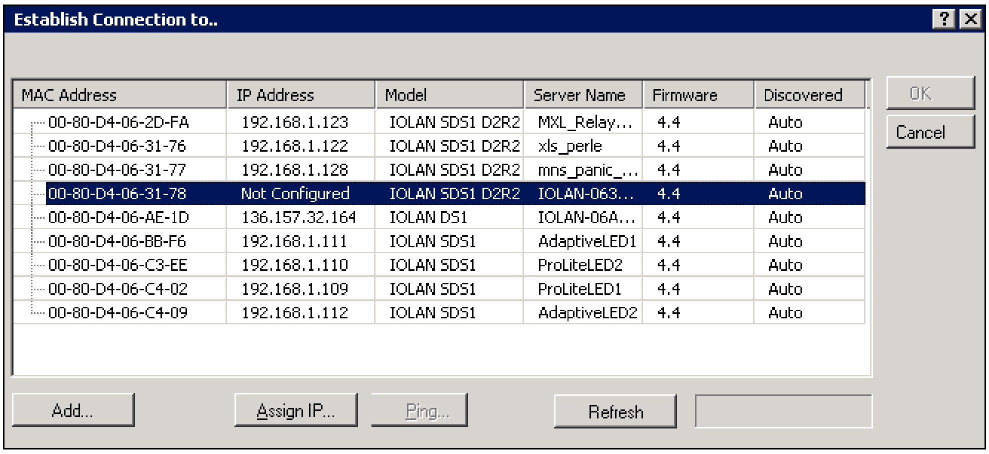
▷ Ensure that the DeviceManager is installed on a computer located under the same network as the device to configure.

▷ Ensure that the following certificates are created using the System Management Console (SMC) or obtained from the site's IT department in Privacy Enhanced Mail (PEM) format:
a) Root Certificate (.pem)
b) Root Certificate Key
Refer to the Certificate Creation From System Management Console section for more information on creating certificates using SMC.

▷ Combine the Root Certificate Key file and Root Certificate into one file (using cat command in command prompt, for example, **cat RootCertificateKey.pem RootCertificate.pem > RootCombineCert.pem**.

▷ If preconfigured .dme file is available then refer GSM Gateway - Import DME File.

1. Start the DeviceManager.

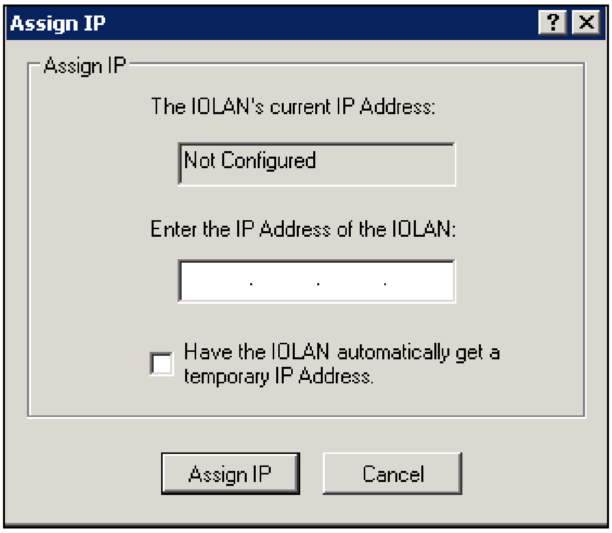

Establish Connection to..

MAC Address	IP Address	Model	Server Name	Firmware	Discovered
00-80-D4-06-2D-FA	192.168.1.123	IOLAN SDS1 D2R2	MXL_Relay...	4.4	Auto
00-80-D4-06-31-76	192.168.1.122	IOLAN SDS1 D2R2	xls_perle	4.4	Auto
00-80-D4-06-31-77	192.168.1.128	IOLAN SDS1 D2R2	mns_panic_...	4.4	Auto
00-80-D4-06-31-78	Not Configured	IOLAN SDS1 D2R2	IOLAN-063...	4.4	Auto
00-80-D4-06-AE-1D	136.157.32.164	IOLAN DS1	IOLAN-06A...	4.4	Auto
00-80-D4-06-BB-F6	192.168.1.111	IOLAN SDS1	AdaptiveLED1	4.4	Auto
00-80-D4-06-C3-EE	192.168.1.110	IOLAN SDS1	ProLiteLED2	4.4	Auto
00-80-D4-06-C4-02	192.168.1.109	IOLAN SDS1	ProLiteLED1	4.4	Auto
00-80-D4-06-C4-09	192.168.1.112	IOLAN SDS1	AdaptiveLED2	4.4	Auto

➪ All similar devices under that network should be visible.

2. Select the device to configure and click **Assign IP**.
   NOTE 1: If the device in the window is not visible, verify that the device has power and is connected to the network. Check the LEDs on the device; the power LED should be solid green and the link LED should be solid amber/green.
   NOTE 2: If issues persist, unplug the Ethernet cable and power. Wait 5 seconds and then plug in the Ethernet cable followed by the power supply. Wait at least 90 seconds while the device reboots.
   NOTE 3: If there are still remaining issues, manually reset the device by holding down the small Reset button located on the device for 10 seconds or until the Power LED is solid amber and then release. Wait 90 seconds for the device to reboot and initialize. If still unsuccessful, replace the unit or check the network.

3. Manually enter an IP address or select the **Have the IOLAN automatically get a temporary IP Address** check box below to have the DHCP assign one automatically. Then click **Assign IP**.


Assign IP

Assign IP

The IOLAN's current IP Address:

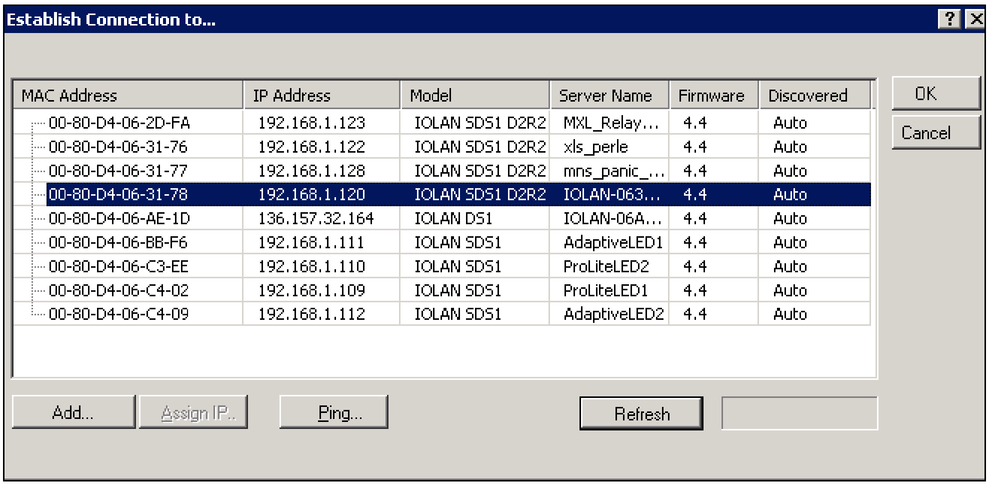
Not Configured

Enter the IP Address of the IOLAN:

. . .

□ Have the IOLAN automatically get a temporary IP Address.

➪ The **Establish Connection to** window appears with an IP address.

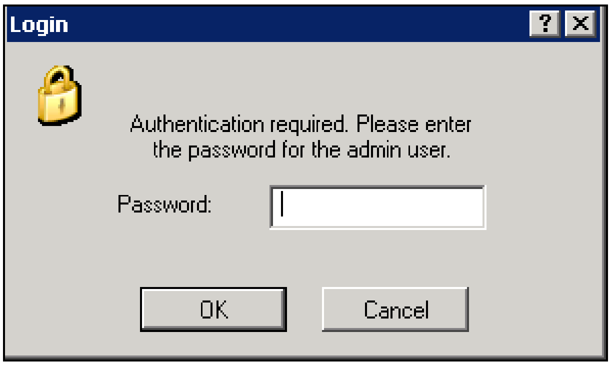


Establish Connection to...

MAC Address	IP Address	Model	Server Name	Firmware	Discovered
00-80-D4-06-2D-FA	192.168.1.123	IOLAN SDS1 D2R2	MXL_Relay...	4.4	Auto
00-80-D4-06-31-76	192.168.1.122	IOLAN SDS1 D2R2	xls_perle	4.4	Auto
00-80-D4-06-31-77	192.168.1.128	IOLAN SDS1 D2R2	mns_panic_...	4.4	Auto
00-80-D4-06-31-78	192.168.1.120	IOLAN SDS1 D2R2	IOLAN-063...	4.4	Auto
00-80-D4-06-AE-1D	136.157.32.164	IOLAN DS1	IOLAN-06A...	4.4	Auto
00-80-D4-06-BB-F6	192.168.1.111	IOLAN SDS1	AdaptiveLED1	4.4	Auto
00-80-D4-06-C3-EE	192.168.1.110	IOLAN SDS1	ProLiteLED2	4.4	Auto
00-80-D4-06-C4-02	192.168.1.109	IOLAN SDS1	ProLiteLED1	4.4	Auto
00-80-D4-06-C4-09	192.168.1.112	IOLAN SDS1	AdaptiveLED2	4.4	Auto

4. Select the device again, and click **OK** to log into the device for configuring.

5. Enter the device password. The factory default password is: **superuser**.



Login

Authentication required. Please enter the password for the admin user.

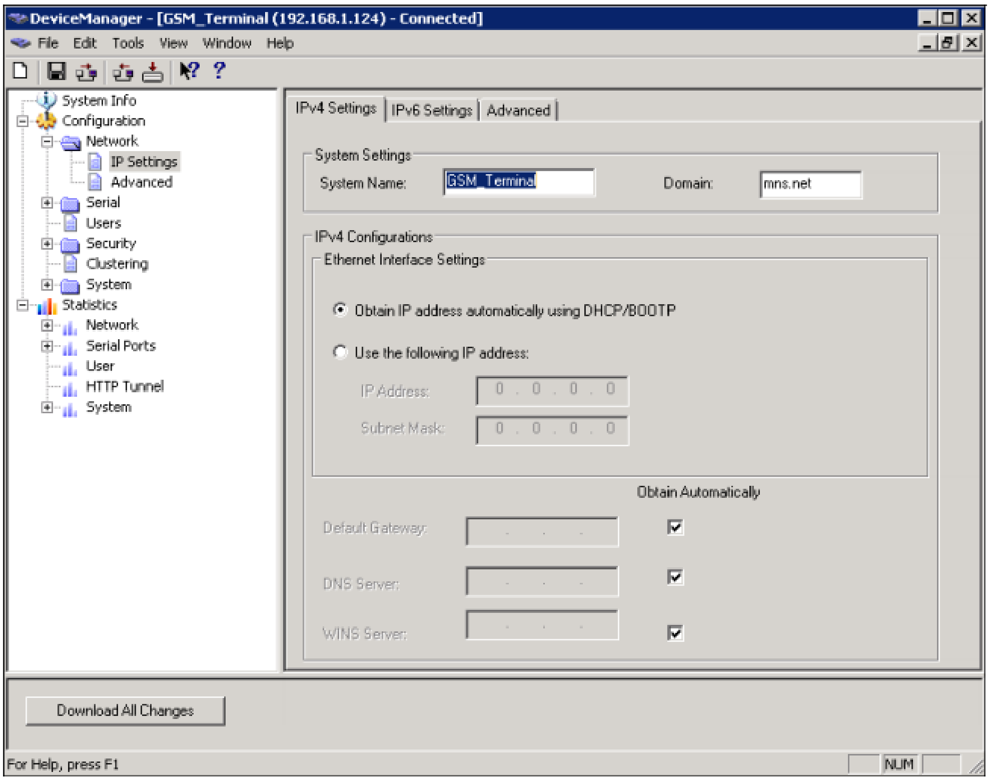
Password:

Fig. 5: Login window

Network Setup

To further configure the network settings of the device, log into the device using DeviceManager. Do the following:

1. In the **Device Manager** window, select **Network > IP Settings**.
   NOTE: In this area, configure additional parameters for the network settings, such as configuring a **static IP address or DHCP**.



DeviceManager - [GSM_Terminal (192.168.1.124) - Connected]

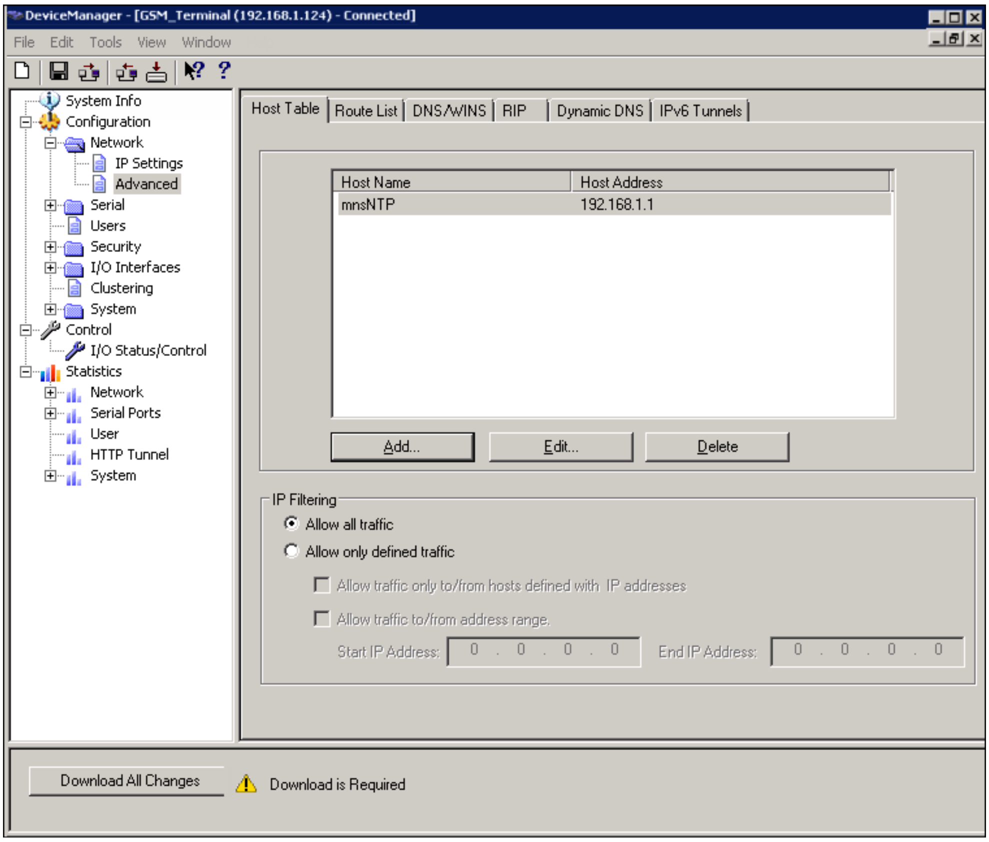
System Settings
System Name: GSM_Termina
Domain: mns.net

IPv4 Configurations
Ethernet Interface Settings
● Obtain IP address automatically using DHCP/BOOTP
○ Use the following IP address:
IP Address: 0 . 0 . 0 . 0
Subnet Mask: 0 . 0 . 0 . 0

Obtain Automatically
Default Gateway: ☑
DNS Server: ☑
WINS Server: ☑

For Help, press F1

2. Select the **System Name** field, give the device a name that helps in distinguishing the corresponding device from other similar devices.
   NOTE 1: The System Name will also be used by the device to create a fully qualified domain name.
   NOTE 2: By default, the device is always **IOLAN** followed by the last three bytes of the device MAC address.
3. Select the **Domain** field, enter the domain name used on the client’s network. In this example, the fully qualified domain name is **GSM_Terminal.mns.net**.
   NOTE: If DHCP is configured, the device automatically receives domain information.
4. Select the **Network > IP Settings > Advanced** tab, select the check box **Register Address in DNS**.
5. Click the **Advanced** tab on the left-hand side of the screen.



DeviceManager - [GSM_Terminal (192.168.1.124) - Connected]

Host Name	Host Address
mnsNTP	192.168.1.1

IP Filtering

● Allow all traffic

○ Allow only defined traffic

□ Allow traffic only to/from hosts defined with IP addresses

□ Allow traffic to/from address range.

Start IP Address: 0 . 0 . 0 . 0 End IP Address: 0 . 0 . 0 . 0

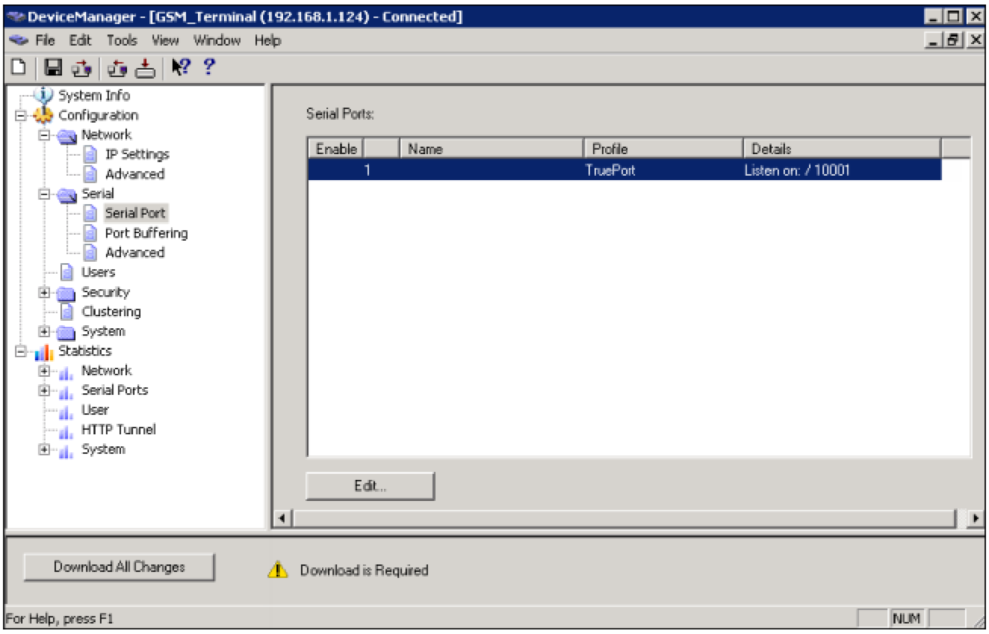
⚠ Download is Required

6. Select the **Host Table** tab, click **Add** to add an NTP host.
7. Enter a descriptive name for the NTP server. For example, **mnsNTP**.
8. Enter the IP address or the fully qualified domain name of an available NTP server.
   NOTE: An available NTP server is required to enable SSL on the device.
9. Click **OK**.

Serial Settings

1. In the **Device Manager** window, select **Serial**.
2. Select **Serial Ports**.

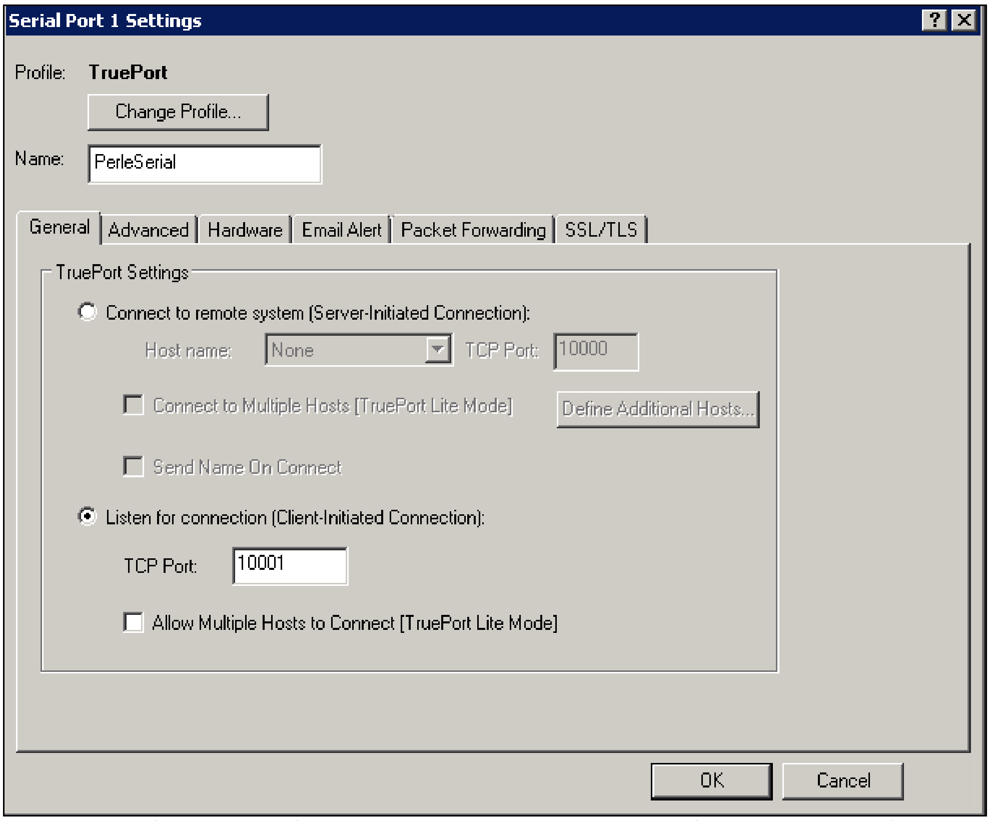
   ⇨ Begin configuring the number of serial ports and the profile the device will use. Only one serial port per device is required for serial communication.
3. Select the default serial port and click **Edit**.



Serial Ports:

Enable	Name	Profile	Details
1		TruePort	Listen on: / 10001

4. In the **Serial Port settings** window, click **Change Profile**.
5. Select the **TruePort** profile and click **OK**.



Profile: TruePort

Name: PerleSerial

TruePort Settings

○ Connect to remote system (Server-Initiated Connection):

Host name: None TCP Port: 10000

□ Connect to Multiple Hosts [TruePort Lite Mode]

□ Send Name On Connect

● Listen for connection (Client-Initiated Connection):

TCP Port: 10001

□ Allow Multiple Hosts to Connect [TruePort Lite Mode]

⇨ The **Serial Port Settings** window will change to reflect the new profile.

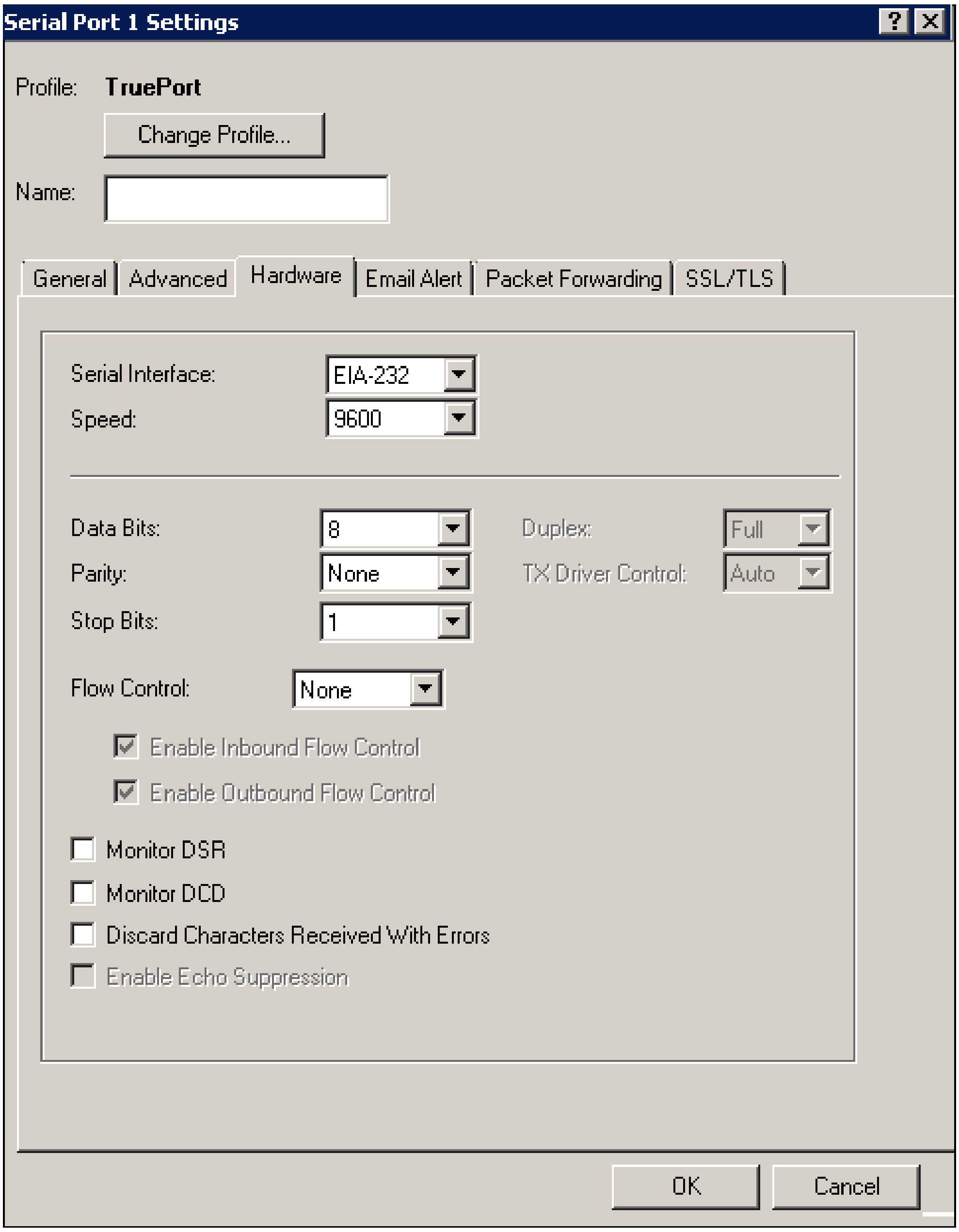
6. Select the **General** tab.
7. Select **Listen for connection (Client-Initiated Connection)**.

   ⇨ In this mode, the device will wait for the server to establish a connection.
8. Enter the TCP port needed to communicate to the device. By default, the TCP port is **10001**.

   NOTE: Always check to make sure the port selected is not already in use by another application/service on the server. To check, open a command prompt, type **netstat**, and press **Enter**. A list of all current TCP connections and ports will be listed.

9. Ensure that the **Allow Multiple Hosts to Connect [TruePort Lite Mode]** check box is unselected so that other servers cannot connect simultaneously to the same device. Click **OK**.

10. Select the **Hardware** tab.



Serial Port 1 Settings

Profile: TruePort

Name:

Serial Interface: EIA-232

Speed: 9600

Data Bits: 8

Parity: None

Stop Bits: 1

Duplex: Full

TX Driver Control: Auto

Flow Control: None

☑ Enable Inbound Flow Control

☑ Enable Outbound Flow Control

□ Monitor DSR

□ Monitor DCD

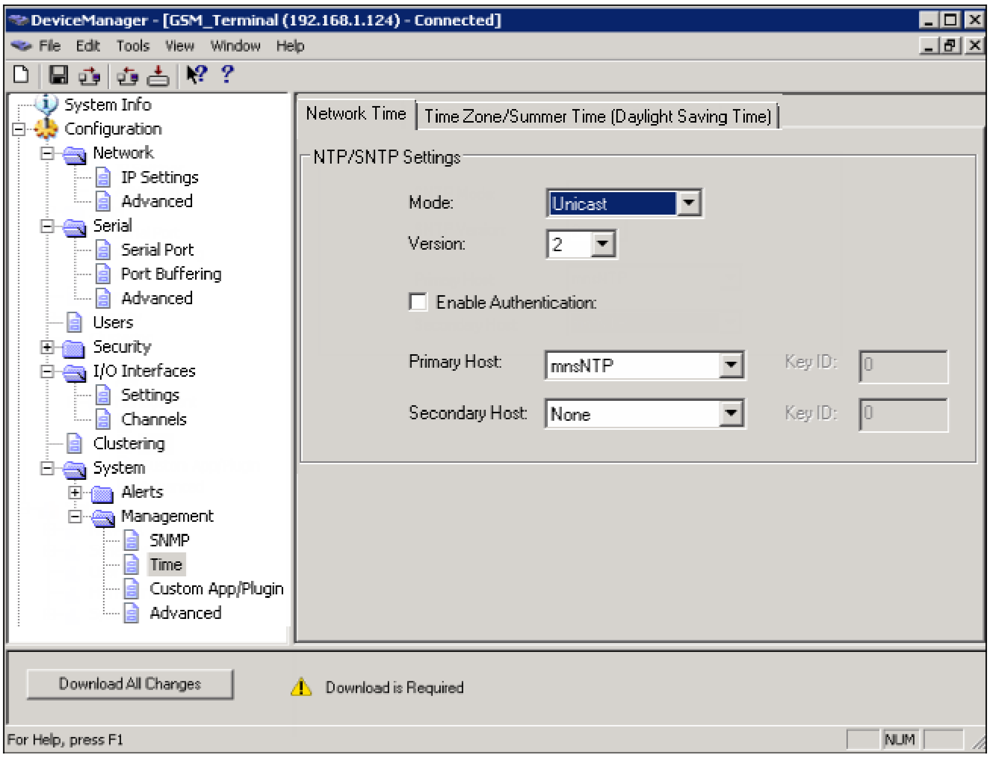
□ Discard Characters Received With Errors

□ Enable Echo Suppression

11. Select the **Hardware** tab, set the following parameters:

   – Select **EIA-232** (RS-232) from the **Serial Interface** drop-down list.
   – Select **9600** from the **Speed** drop-down list.
   – Select **8** from the **Data Bits** drop-down list.
   – Select **None** from the **Parity** drop-down list.
   – Select **1** from the **Stop Bits** drop-down list.
   – Set Flow Control to **None**.
   – Keep the **Monitor DSR**, **Monitor DCD**, and **Discard Characters Received With Errors** check boxes unselected.

12. Click the **SSL/TLS** tab and do the following:
    - Select the following check boxes:
      Enable SSL/TLS
      Use Global settings (Security > SSL/TLS).
    - Click **OK**.
13. Select **Configuration > System > Management > Time**.



Mode: Unicast

Version: 2

□ Enable Authentication:

Primary Host: mnsNTP Key ID: 0

Secondary Host: None Key ID: 0

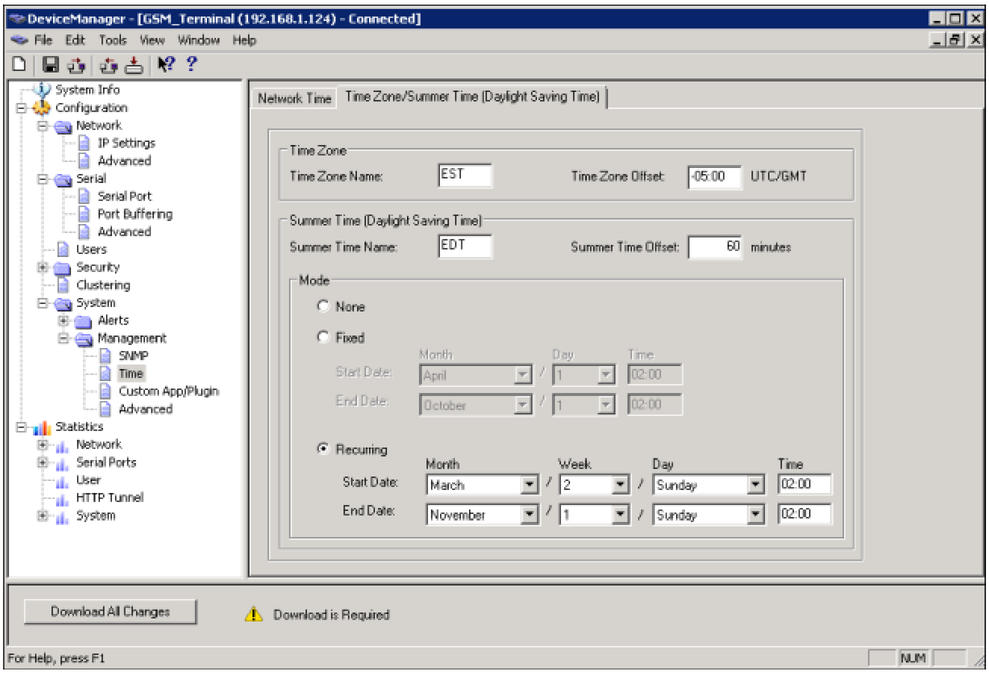
Download is Required

For Help, press F1

NUM

14. Select the **Network Time** tab, set the following parameters.
    - **Mode:** Unicast
    - **Version:** 2
    - Leave the **Enable Authentication** check box unselected.
    - **Primary Host:** Select the NTP server name created earlier.
    - **Secondary Host:** Select alternative NTP server name, otherwise set name as primary host.

      NOTE: Network time works best when the version matches that of the NTP server. Windows time servers generally default to Version 2. External NTP servers generally work with Version 3. Verify with the client’s network administrator.
15. Select the **Time Zone/Summer Time (Daylight Saving Time)** tab.
16. Configure the parameters as per the details mentioned in the Time Zone/Summer Time (Daylight Saving Time) parameters.



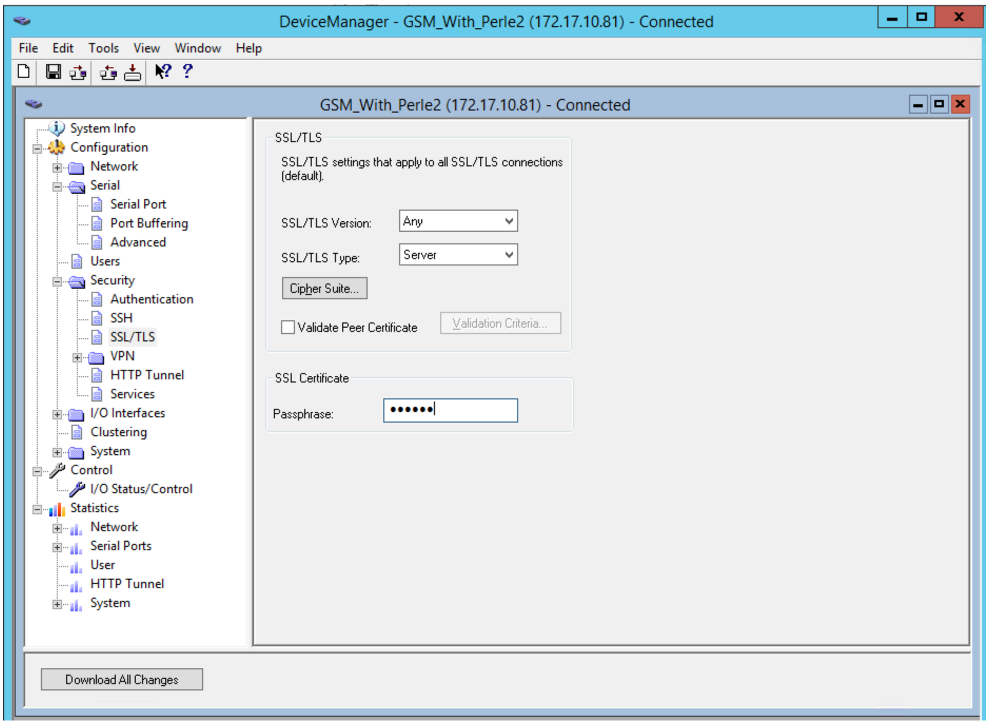
Time Zone
Time Zone Name: EST
Time Zone Offset: -05:00 UTC/GMT

Summer Time (Daylight Saving Time)
Summer Time Name: EDT
Summer Time Offset: 60 minutes

Mode
○ None
○ Fixed
Start Date: April / 1 / 02:00
End Date: October / 1 / 02:00
● Recurring

	Month	Week	Day	Time
Start Date:	March	2	Sunday	02:00
End Date:	November	1	Sunday	02:00

17. Select **Configuration > Security > SSL/TLS**.



SSL/TLS

SSL/TLS settings that apply to all SSL/TLS connections (default).

SSL/TLS Version: Any

SSL/TLS Type: Server

□ Validate Peer Certificate

SSL Certificate

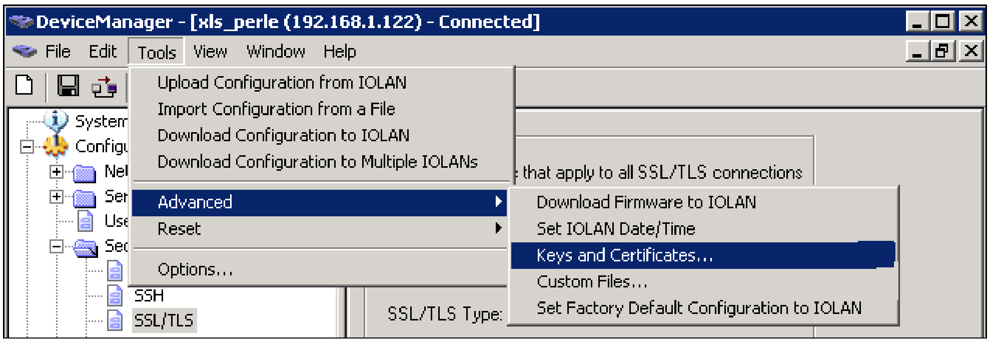
Passphrase: ••••••

18. Set the **SSL/TLS Version** field to **Any**.

19. Set the **SSL/TLS Type** field to **Server**.

20. Select **SSL Certificate** section, enter the password of the Root certificate(.pem) in the **Passphrase** field.

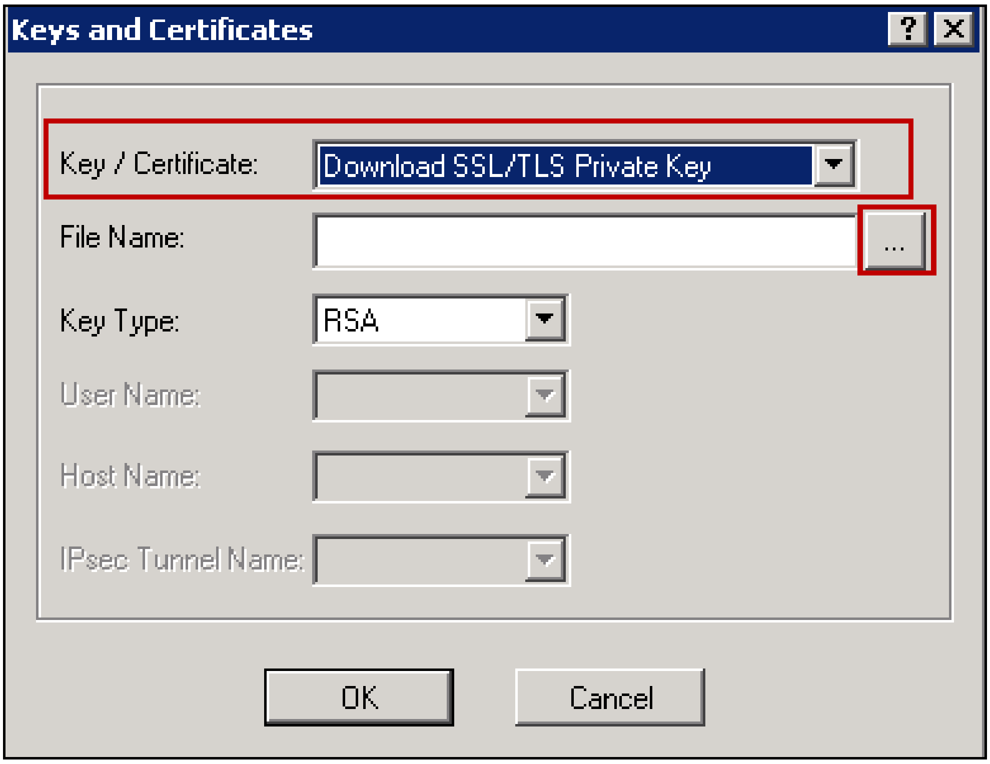
21. Select **Tools > Advanced > Keys and Certificates**. The **Keys and Certificates** dialog box displays.


DeviceManager - [xls_perle (192.168.1.122) - Connected]
File
Edit
Tools
View
Window
Help
System
Configu
Net
Ser
Use
Sec
SSH
SSL/TLS
Upload Configuration from IOLAN
Import Configuration from a File
Download Configuration to IOLAN
Download Configuration to Multiple IOLANs
Advanced
Reset
Options...
that apply to all SSL/TLS connections
SSL/TLS Type:
Download Firmware to IOLAN
Set IOLAN Date/Time
Keys and Certificates...
Custom Files...
Set Factory Default Configuration to IOLAN

22. In the **Key/Certificate** drop-down list, select **Download SSL/TLS Private Key**.

23. Click the browse button and upload the private key for the root certificate (pem).

24. Click **OK**.


Keys and Certificates

Key / Certificate: Download SSL/TLS Private Key

File Name:

Key Type: RSA

User Name:

Host Name:

IPsec Tunnel Name:

25. Select **Tools > Advanced > Keys and Certificates**.

26. In the **Key/Certificate** drop-down list, select **Download SSL/TLS Certificate**.

27. Click the browse button and upload the combined root certificate (RootCombineCert.pem file). Refer to the Device Configuration section for more information on combining the root certificate.

28. Click **OK**.

29. Select **Tools > Advanced > Keys and Certificates**.

30. In the **Key/Certificate** drop-down list, select **Download SSL/TLS CA**.

31. Click the browse button and upload the root certificate (RootCertificate.pem file).

32. Click **OK**.

33. Click **Download All Changes** to make the changes to the device. Click **Reboot IOLAN** to complete.
NOTE: Any time device reboot of the device is needed, or power is

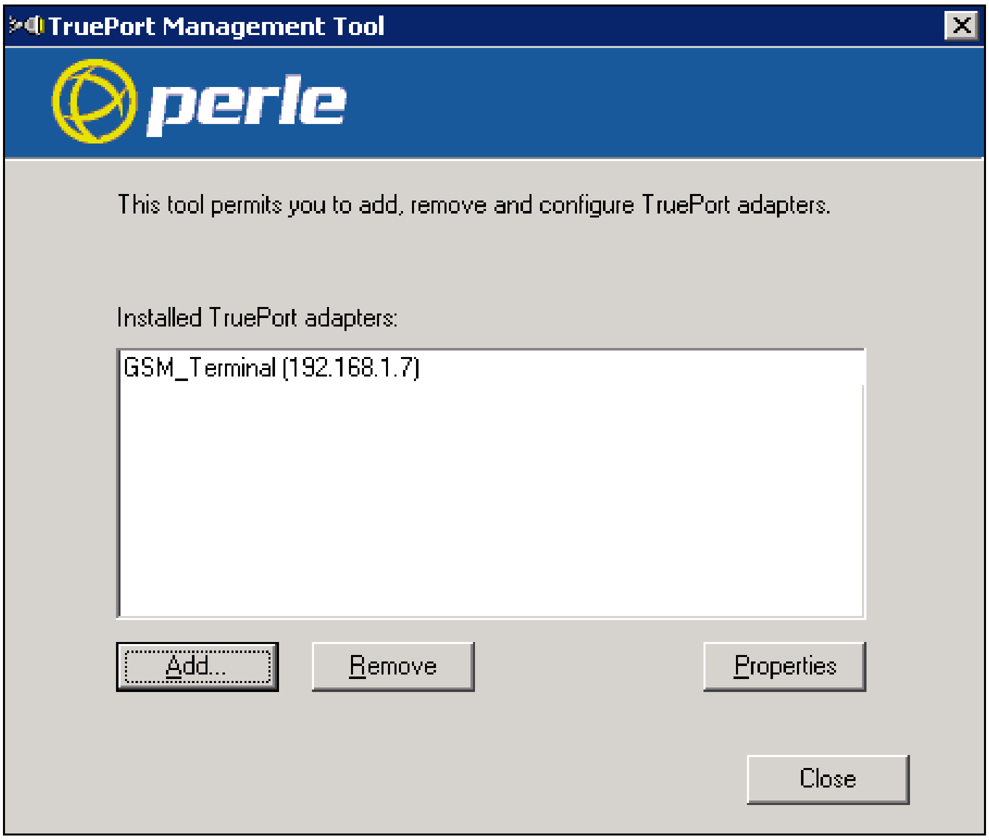
reconnected, it will take 90 seconds for the device to reboot and initialize. When ready, the Power LED will be a solid green color and the Link LED will be a solid orange or green.

➪ The device is now configured.

TruePort Driver Configuration

The TruePort driver is the second part of the process to link the device to the server. TruePort is only used when the device is configured to use the TruePort profile. The TruePort driver is designed to manage all similar devices communicating with the server. Since TruePort creates a virtual COM port, it is recommended that each device has a unique COM port for each service. **NOTE:** Serial communication and I/O access are each considered a separate service and therefore require separate COM ports.

1. Install TruePort on the server.
2. Start the **TruePort Management Tool**.
3. In the **TruePort Management Tool** window, click **Add**.

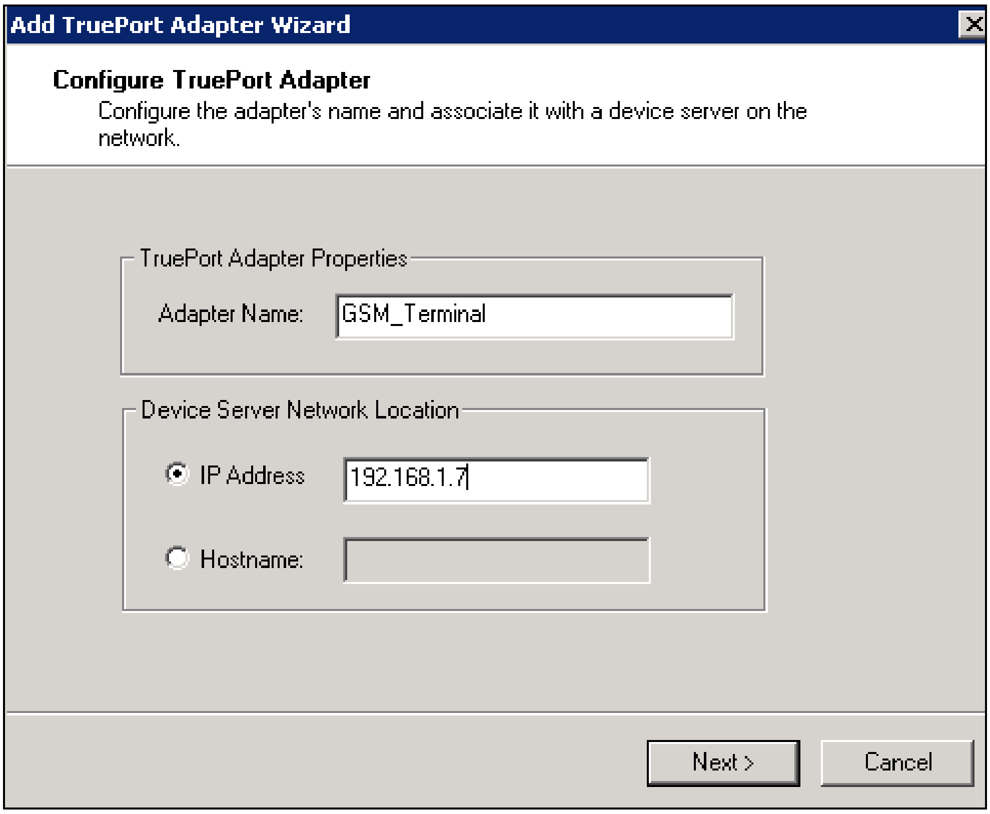


This tool permits you to add, remove and configure TruePort adapters.

Installed TruePort adapters:

GSM_Terminal (192.168.1.7)

4. Enter a name for the TruePort Adapter.
NOTE: This Adapter will serve a particular device and therefore map to a specific COM port. Try to make the name descriptive so that the Adapter can easily be tracked back to a particular device.
5. Enter the IP address or the hostname the device is using, and then click **Next**.

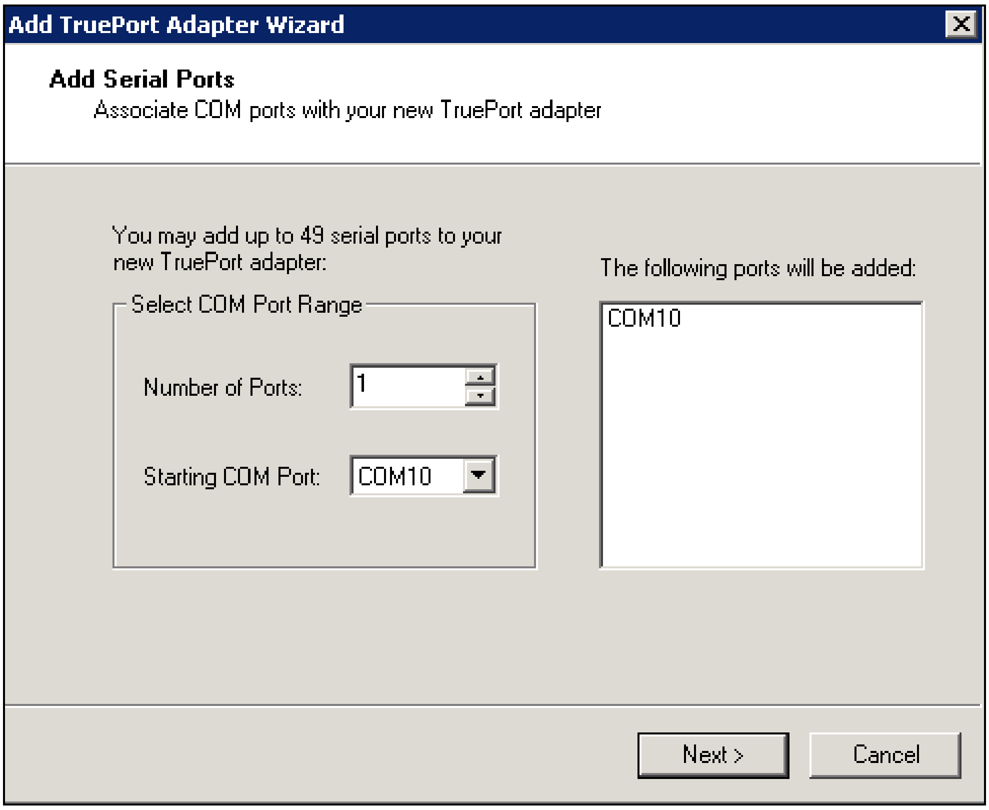


Configure TruePort Adapter
Configure the adapter's name and associate it with a device server on the network.

TruePort Adapter Properties
Adapter Name: GSM_Terminal

Device Server Network Location
● IP Address 192.168.1.7
○ Hostname:

6. Leave the number of ports set to **1** (if using I/O access, set ports to **2**, or add another later). Select the COM port to assign to that particular device. By convention, start at COM100 and increment for each device and service configured. This will help to avoid any conflicts with existing COM ports or other devices. TruePort allows creation up to 4,096 COM ports.
7. Click **Next**.



Add TruePort Adapter Wizard

Add Serial Ports

Associate COM ports with your new TruePort adapter

You may add up to 49 serial ports to your new TruePort adapter:

Select COM Port Range

Number of Ports: 1

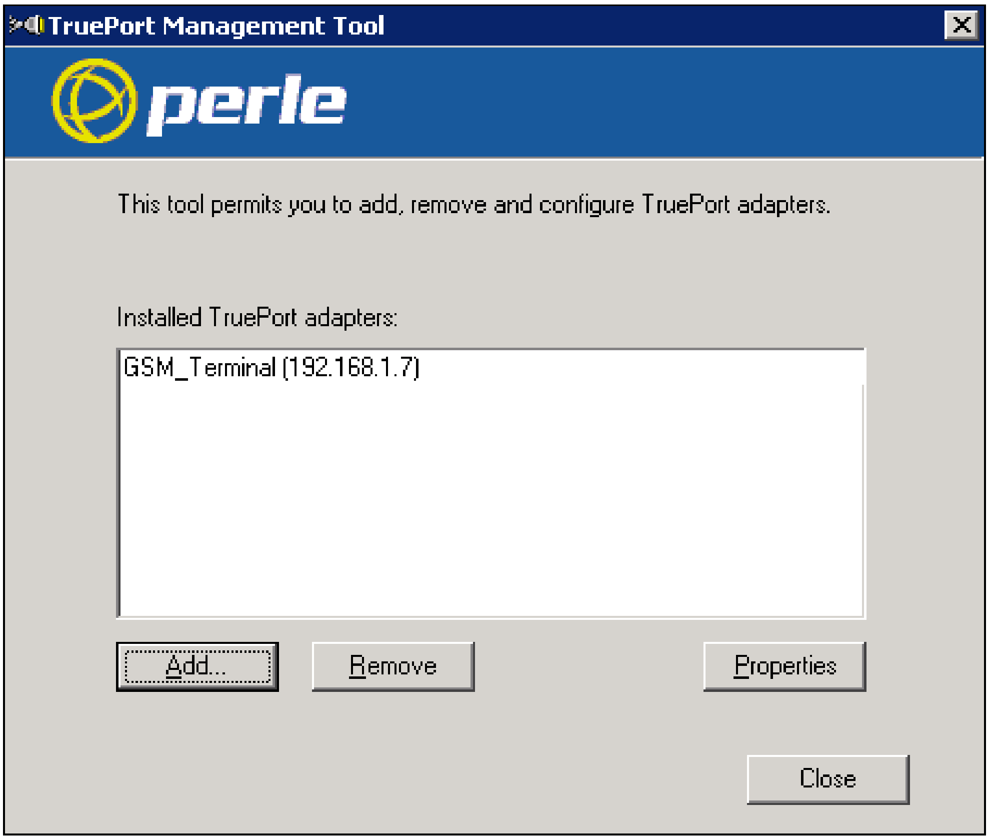
Starting COM Port: COM10

The following ports will be added:

COM10

➪ The TruePort Adapter in the TruePort Management Tool is visible.

8. To edit the TruePort settings, select the adapter to edit and click **Properties**.



TruePort Management Tool

This tool permits you to add, remove and configure TruePort adapters.

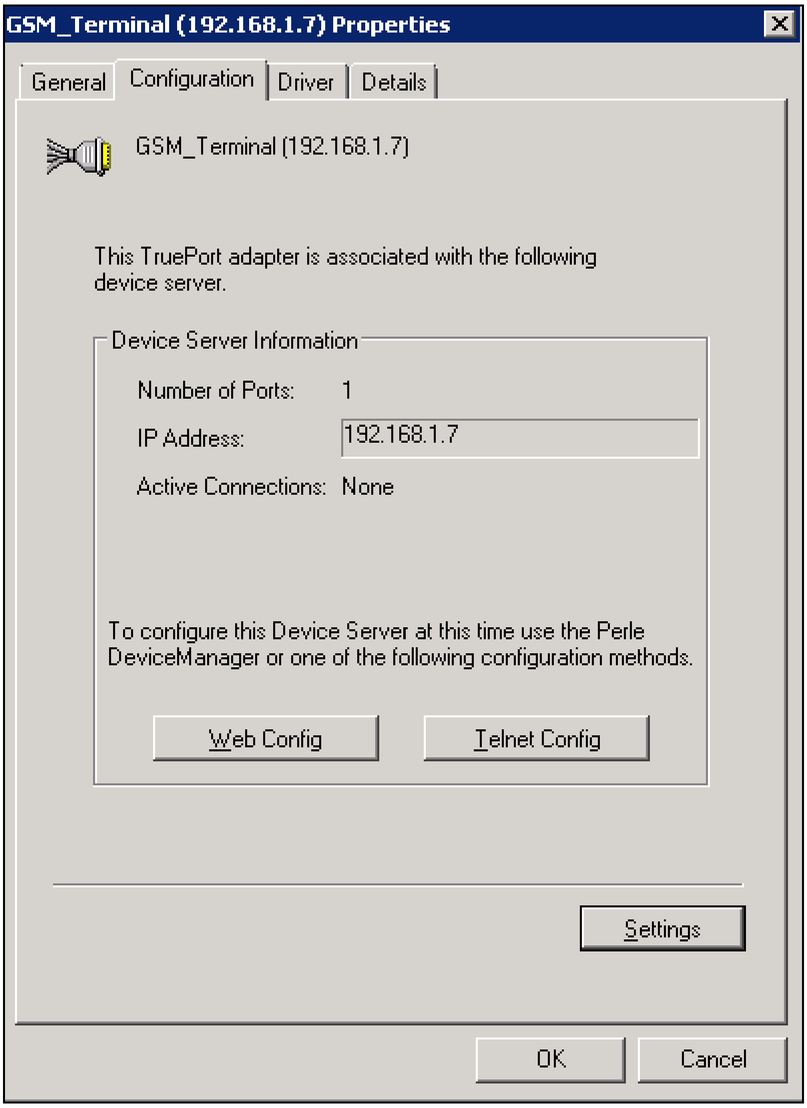
Installed TruePort adapters:

GSM_Terminal (192.168.1.7)

Fig. 6:

Serial Settings

1. Select the **Properties** window of the device port to be configured, click the **Configuration** tab and then click **Settings**.



GSM_Terminal (192.168.1.7) Properties

GSM_Terminal (192.168.1.7)

This TruePort adapter is associated with the following device server.

Device Server Information

Number of Ports: 1

IP Address: 192.168.1.7

Active Connections: None

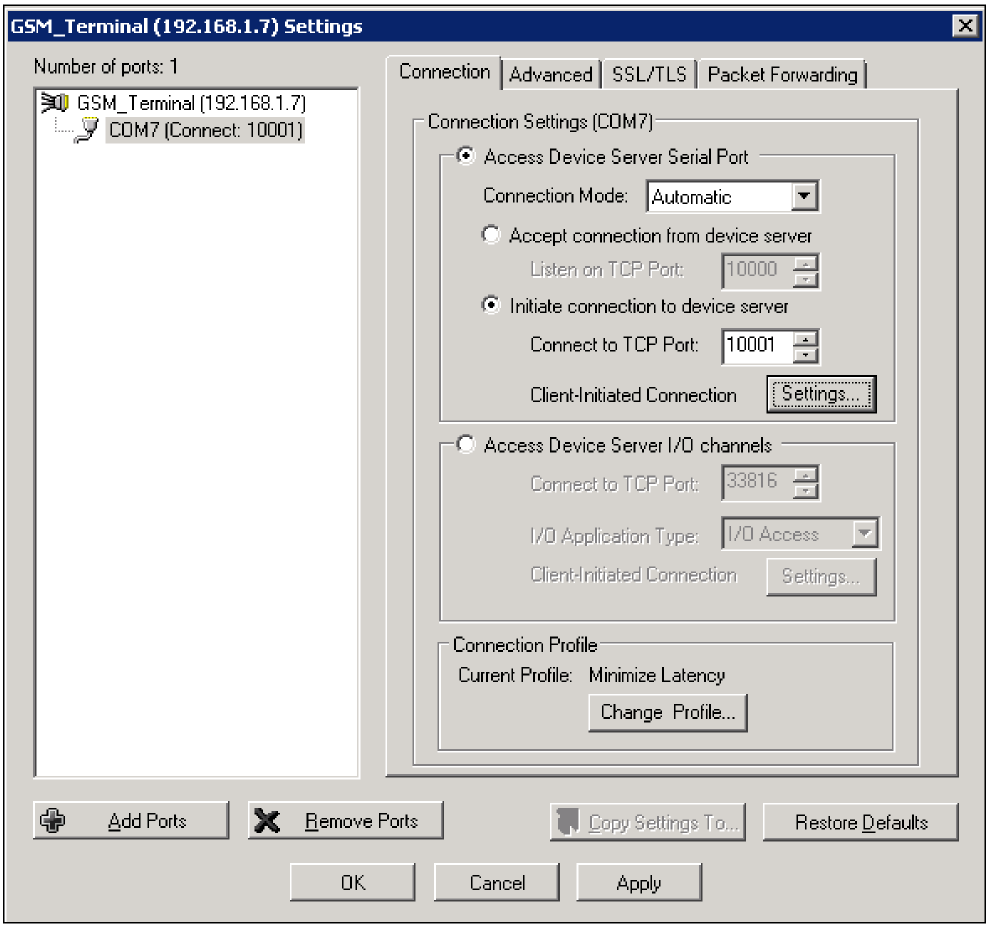
To configure this Device Server at this time use the Perle DeviceManager or one of the following configuration methods.

2. Click the COM port.

   ➪ This will display the TruePort and COM port settings for this adapter.

3. Select the **Connection** tab.

4. Select **Initiate connection to device server**.



GSM_Terminal (192.168.1.7) Settings

Number of ports: 1

GSM_Terminal (192.168.1.7)
COM7 (Connect: 10001)

Connection Settings (COM7)

● Access Device Server Serial Port

Connection Mode: Automatic

○ Accept connection from device server

Listen on TCP Port: 10000

● Initiate connection to device server

Connect to TCP Port: 10001

Client-Initiated Connection

○ Access Device Server I/O channels

Connect to TCP Port: 33816

I/O Application Type: I/O Access

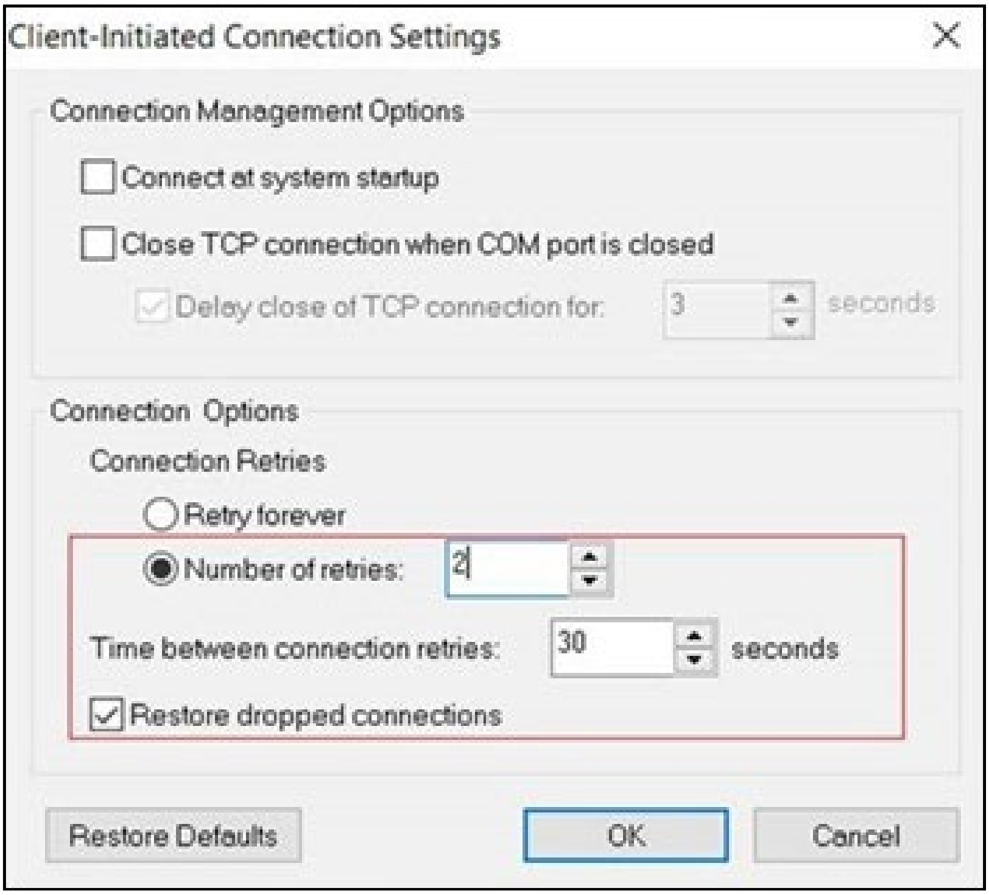
Client-Initiated Connection

Connection Profile

Current Profile: Minimize Latency

- Select **Connect to TCP Port**, enter the port number that was previously assigned to the device using the device manager.

5. Click the **Settings** button next to **Client-Initiated Connection**.



Client-Initiated Connection Settings

Connection Management Options

□ Connect at system startup

□ Close TCP connection when COM port is closed

☑ Delay close of TCP connection for: 3 seconds

Connection Options

Connection Retries

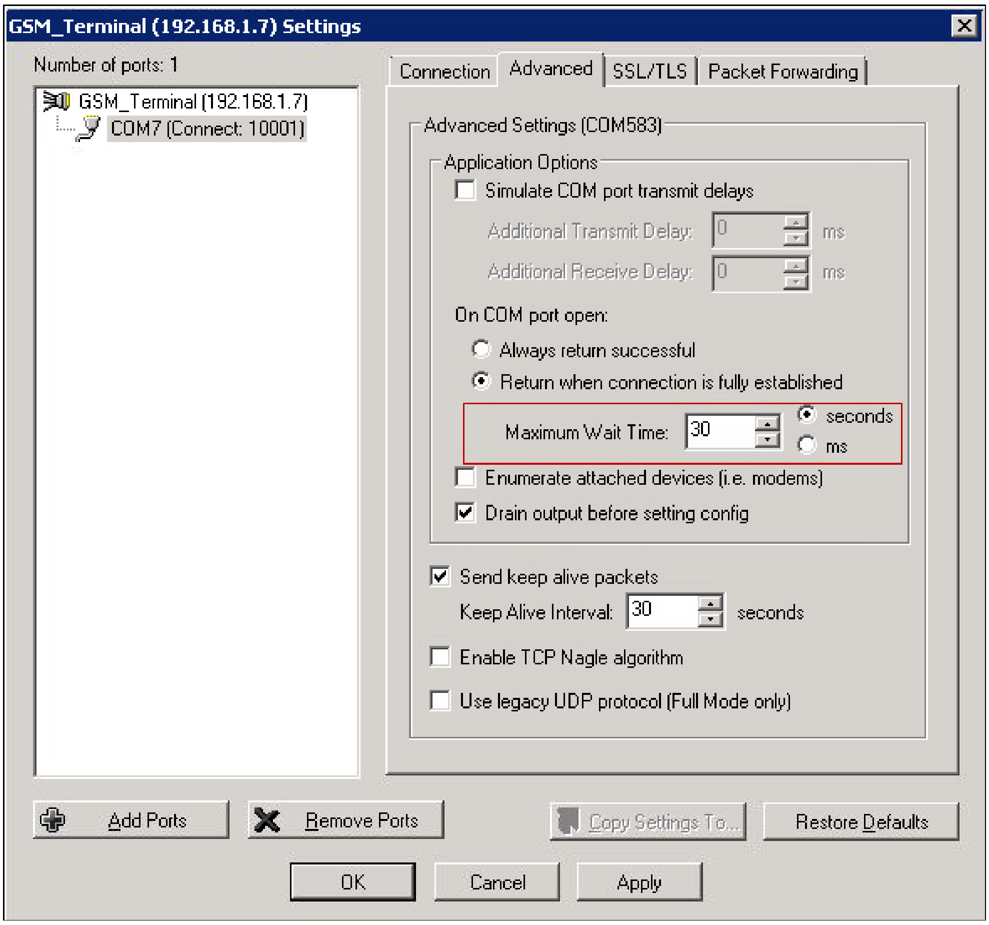
○ Retry forever

● Number of retries: 2

Time between connection retries: 30 seconds

☑ Restore dropped connections

6. In the **Client-Initiated Connection Settings** window, select the **Connect at system startup** check box.
7. For **Connection Retries**, select **Retry forever**.
8. Select the **Advanced** tab.



GSM_Terminal (192.168.1.7) Settings

Number of ports: 1

GSM_Terminal (192.168.1.7)
COM7 (Connect: 10001)

Advanced Settings (COM583)

Application Options

☐ Simulate COM port transmit delays

Additional Transmit Delay: 0 ms

Additional Receive Delay: 0 ms

On COM port open:

○ Always return successful

● Return when connection is fully established

Maximum Wait Time: 30 ● seconds ○ ms

☐ Enumerate attached devices (i.e. modems)

☑ Drain output before setting config

☑ Send keep alive packets

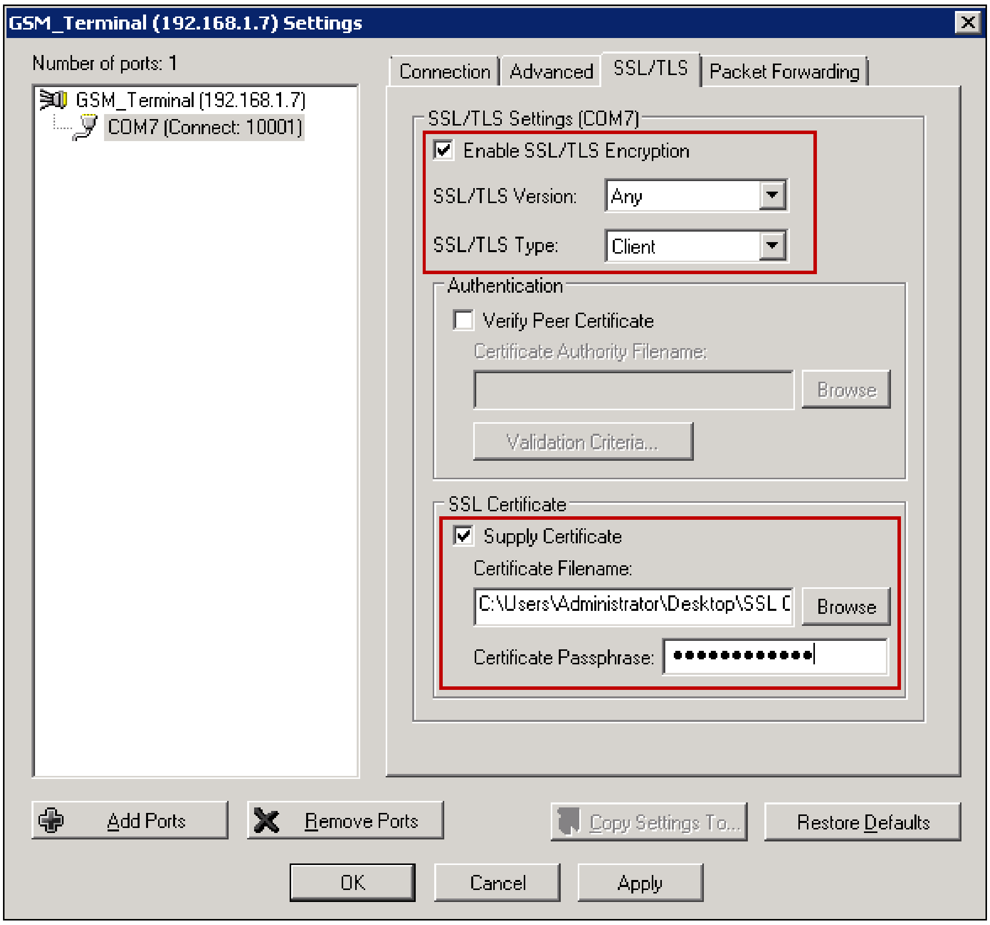
Keep Alive Interval: 30 seconds

☐ Enable TCP Nagle algorithm

☐ Use legacy UDP protocol (Full Mode only)

9. Set **Maximum Wait Time** to **30 seconds**.

10. Select the **SSL/TLS** tab.



GSM_Terminal (192.168.1.7) Settings

Number of ports: 1

GSM_Terminal (192.168.1.7)
COM7 (Connect: 10001)

SSL/TLS Settings (COM7)

☑ Enable SSL/TLS Encryption

SSL/TLS Version: Any

SSL/TLS Type: Client

Authentication

□ Verify Peer Certificate

Certificate Authority Filename:

SSL Certificate

☑ Supply Certificate

Certificate Filename: C:\Users\Administrator\Desktop\SSL C

Certificate Passphrase: ●●●●●●●●●●●●

11. Select the **Enable SSL/TLS Encryption** check box.

12. Set the **SSL/TLS Version** field to **Any**.

13. Set the **SSL/TLS Type** field to **Client**.

14. Select the **Supply Certificate** check box.

15. Click the browse button and select the combined root certificate. Refer to the Device Configuration section for more information on combining a root certificate.

16. Enter the password in the **Certificate Passphrase** field.

17. Click **Apply** and then **OK**.

18. Restart the Perle TruePort service.

Device Verification

Serial Port

Test the settings of the TruePort application and Perle SDS1 device by connecting the device to the GSM Terminal and sending a message directly using a serial terminal, such as PuTTY.

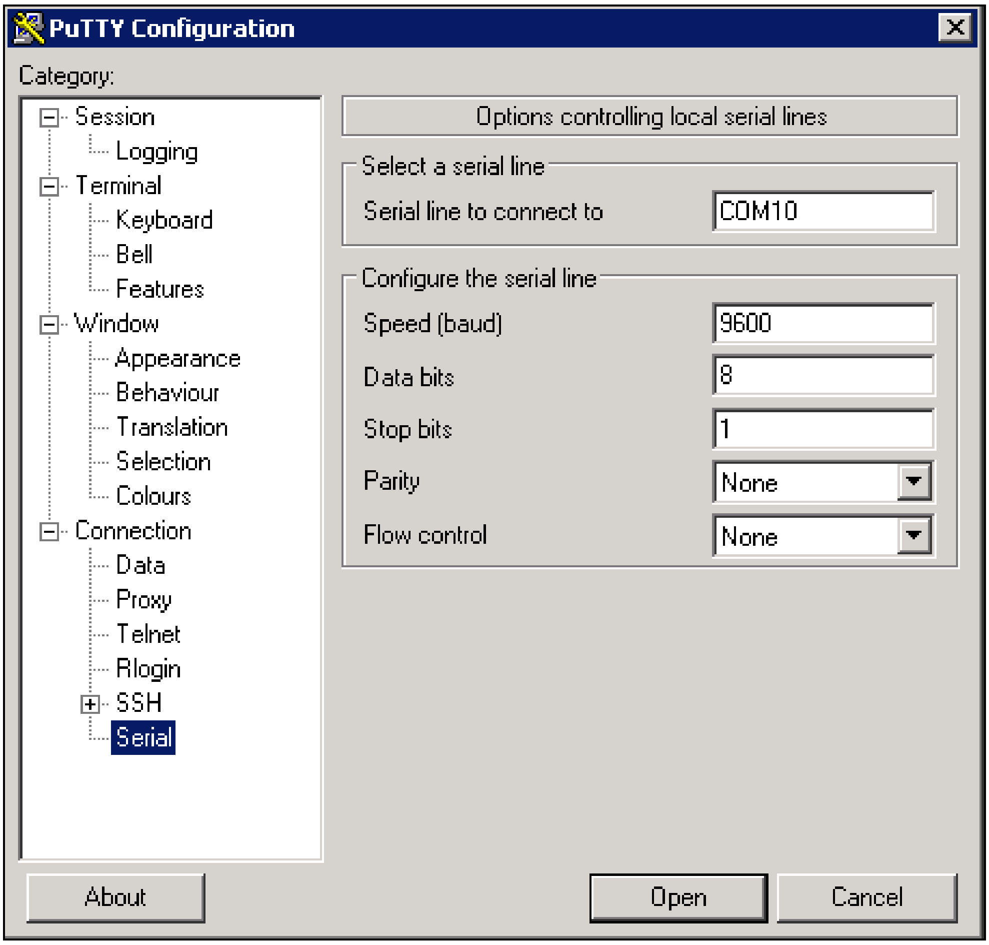
PuTTY can be downloaded from the following link:

http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe

To test the serial port, open up a HyperTerminal or PuTTY session from the server on the serial COM port. If the COM port opens, then the TruePort driver is working properly.

The steps for testing GSM Terminal communication are as follows:

1. Open PuTTY and select **Connection > Serial**.
2. For a Serial line to connect to, enter the TruePort COM port number created in TruePort Driver Configuration.
3. Enter the parameters for baud rate, data bits, stop bits, parity, and flow control for the external device that will be transmitting Serial data.
   - **Speed (baud):** 9600
   - **Data Bits:** 8
   - **Stop Bits:** 1
   - **Parity:** None
   - **Flow Control:** None



PuTTY Configuration

Options controlling local serial lines

Select a serial line

Serial line to connect to: COM10

Configure the serial line

Speed (baud): 9600

Data bits: 8

Stop bits: 1

Parity: None

Flow control: None

4. Select **Session > Serial**.
5. Click **Open** to establish a serial session.
6. Enter the command **AT** and send the command through the terminal application.

⇨ If the result of the command is **OK,** the device is connected properly. If the result is **ERROR**, the device is not connected properly.

GSM Modem Troubleshooting

Problem: Once the device is created in the **Device Editor** section, the corresponding device gets in **Connected** state based on the **Check Status Rate** configured in the **Configuration Properties** of the driver. However, at times the device does not get connected after the **Check Status Rate** duration.

Solution: Perform the following steps in sequence until the device gets connected after a particular step. After each step, wait for the **Check Status Rate** duration and monitor the device connection status.

1. Restart the TruePort service.
2. Reimport the certificates on device manager and reboot the Perle IOLAN device.
3. Reboot the Server.
4. Disconnect the power cable of the Perle IOLAN device, wait for a few seconds and then reconnect the power cable.
5. Power off and on the devices connected to the Perle IOLAN device.

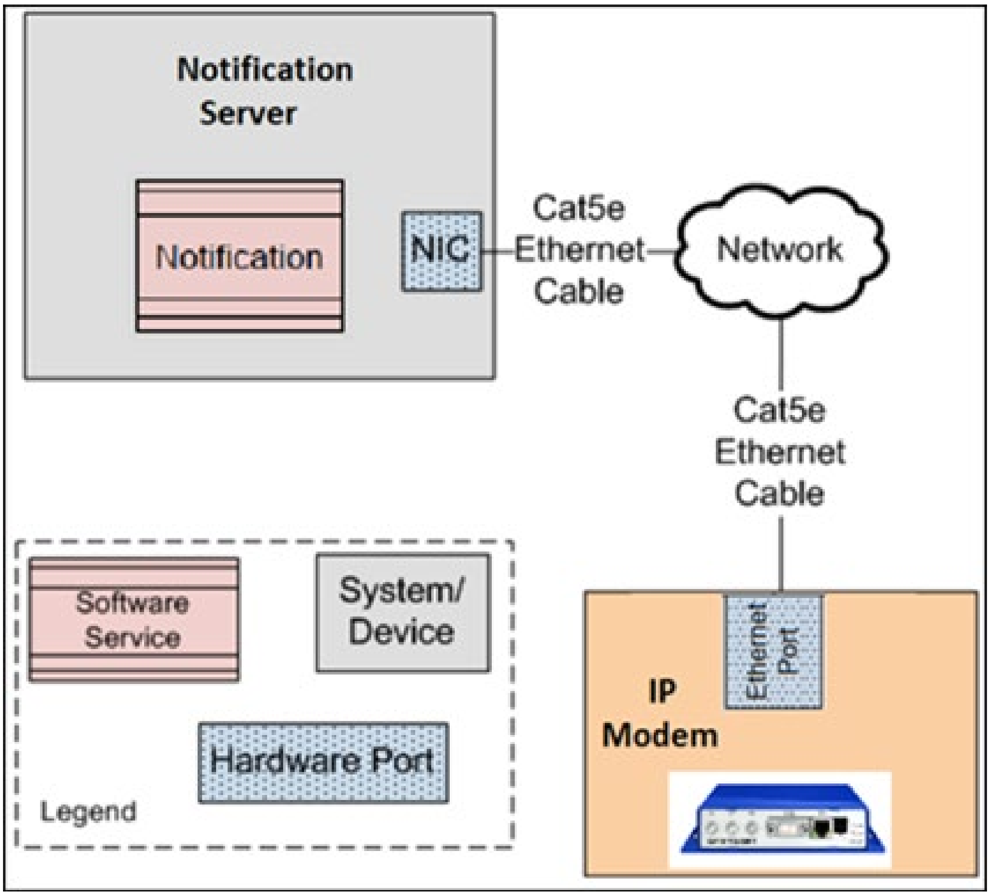
1.3 IP Modem Device

IP Modem

This section provides reference and background information for integrating the Global System for Mobile Communications (GSM) Gateway with the system. For procedures or workflows, see the step-by-step section.

Notification allows configuration of the IP Modem to deliver SMS messages to the intended recipients and receive replies from the recipient users. The system sends messages to the SMS receiver devices using the IP Modem with Attention (AT) command. The IP Modem can be configured using TCP/IP Protocol.

Below is an overview of the system using the TCP/IP over LAN configuration:

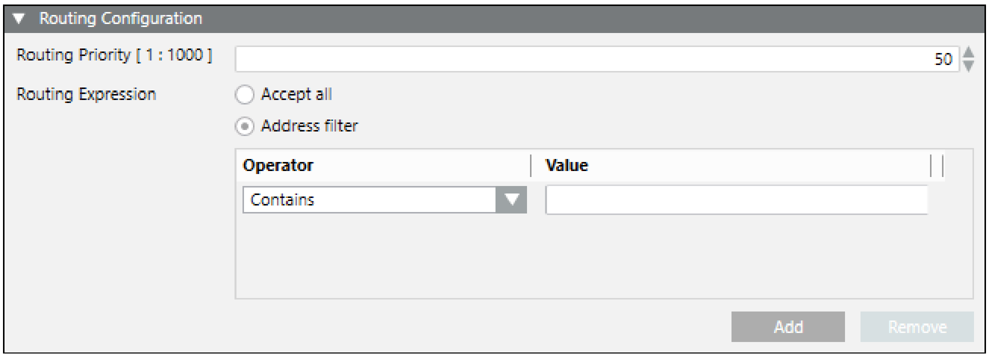


NOTE 1:
The GSM Terminal device accepts a SIM card that has the SMS services enabled. Without enabling these services on a SIM card, you cannot send SMS through the device.
NOTE 2:

In order to use message reply and the escalation functionality, the mobile number configured in the recipient user device must have the following number format: +[country code][number]. For example, +17327572923.
NOTE 3:
More tested modems are listed in the *Desigo CC System Description* guide.

Routing Configuration Expander

This expander displays the fields required for the configuration of the routing priority and routing expressions for the device. More than one operator can be added under the **Routing Expression** expander. The logical function followed here is OR. For example, if you select **Contains** as one operator and **Starts with** as another operator, Notification will search for either the value specified under **Starts with** or **Contains**.



▼ Routing Configuration

Routing Priority [1 : 1000]: 50

Routing Expression: ○ Accept all ● Address filter

Operator	Value
Contains	

- **Routing Priority**: Select the routing priority for the GSM Terminal device. The routing priority determines, in which order the routing expressions of the devices configured under the same field network are evaluated. Select a number between 1 and 1000 as the Routing Priority.
  NOTE 1: A Routing Priority of 1 will have the highest priority.
  NOTE 2: It is acceptable that two GSM Terminal devices have the same routing priority as long as it is guaranteed that their routing expressions cannot match against the same recipient user device address. The routing expressions have to be mutually exclusive otherwise, the system's routing behavior is non-deterministic.
- **Routing Expression**: Enter one or more Operator/Value expressions. These expressions are evaluated against each Recipient User Device address that a message is sent to. If an address matches at least one of the Operator/Value expressions of a GMS Terminal device, the message to that Recipient User Device will be routed through the intermediate GMS Terminal device.
- **Accept all**: Specify if this managed device can be used for messaging to a recipient that is in any address format.
- **Address filter**: Select to accept only those routing expressions which meet the conditions set under Operator and Value.
- **Operator**: Select the condition for the routing expression from the drop-down list.
- **Value**: Enter a suitable value for the selected Operator condition.
- **Add**: Add Operator and Value.
- **Remove**: Remove Operator and Value.

Operator Conditions for the Routing Expressions

Operator	Description
Contains	Checks whether the recipient user address string contains the assigned value. If yes, the corresponding message is routed through the device.
Does Not Contain	Checks whether recipient user address string contains the assigned value. If not, the corresponding message is routed through the device.

Starts with	Checks whether recipient user address string starts with the assigned value. If yes, the corresponding message is routed through the device.
Does Not Start With	Checks whether recipient user address string starts with the assigned value. If not, the corresponding message is routed through the device.
Ends With	Checks whether recipient user address string ends with the assigned value. If yes, the corresponding message is routed through the device.
Does Not End With	Checks whether recipient user address string ends with the assigned value. If not, the corresponding message is routed through the device.
Equals	Checks whether recipient user address string is equal to the assigned value. If yes, the corresponding message is routed through the device. This operator performs a character by character match between the recipient user device address and the assigned value. If the recipient user device address is 91-123 and the assigned value is 91123, the corresponding message is not routed through the device.
Not equals	Checks whether recipient user address string is equal to the assigned value. If not, the corresponding message is routed through the device. This operator performs a character by character match between the recipient user device address and the assigned value. If the recipient user device address is 91-123 and the assigned value is 91123, the corresponding message is not routed through the device.
Less Than	This operator is evaluated only with numeric values (whole numbers or non-negative integers) of the recipient user device address and the assigned value. You can enter numeric values from 0 to 9,223,372,036,854,775,807 (maximum 64 bits long). If the recipient user device address string contains a character other than digits or a + or - sign, the corresponding message is not routed through the device. This operator performs the mathematical Less Than or Equal To (<=) operation.
Less Than Or Equal To	This operator is evaluated only with numeric values (whole numbers or non-negative integers) of the recipient user device address and the assigned value. You can enter numeric values from 0 to 9,223,372,036,854,775,807 (maximum 64 bits long). If the recipient user device address string contains a character other than digits or + or - sign, the corresponding message is not routed through the device. This operator performs the mathematical Less Than or Equal To (<=) operation.
Greater Than	This operator is evaluated only with numeric values (whole numbers or non-negative integers) of the recipient user device address and the assigned value. You can enter numeric values from 0 to 9,223,372,036,854,775,807 (maximum 64 bits long). If the recipient user device address string contains a character other than digits or a + or - sign, the corresponding message is not routed through the device. This operator performs the mathematical Less Than or Equal To (<=) operation.
Greater Than Or Equal To	This operator is evaluated only with numeric values (whole numbers or non-negative integers) of the recipient user device address and the assigned value. You can enter numeric values from 0 to 9,223,372,036,854,775,807 (maximum 64 bits long). If the recipient user device address string contains a character other than digits or + or - sign, the corresponding message is not routed through the device. This operator performs the mathematical Less Than or Equal To (<=) operation.
Regular expression	This operator is used to evaluate recipient device address with regular expression given in the assigned value string.

Examples of Regular Expressions

Regular Expressions	Description
^\d+	String starts with one or more digits only.
^[+](91)	String should start with +91.
^.+?\d$	String ending with digits only.
^[0-9]{10}(52|56|57)$	String is 12 digits long (numbers only) and ends with 52, 56, or 57.
^9881231231$	Matching exact mobile number.

IP Modem

This section provides additional procedures for integrating the IP Modem Gateway with the system.

Installing IP Modem Device

This section provides information to the user for mounting the hardware and wiring or connection details for the device.

Prerequisites

The prerequisites required for the device installation include the following:

1. IP Modem
2. Antenna
3. SIM Card
4. Cat5e Ethernet Cable
5. External DC Power Supply
6. Power Cable

Note 1: Before applying power to the router, connect the components that you required for your applications. You cannot operate the router without connected antenna, inserted SIM card, nor connected power supply.

Note 2: The router can be damaged if you have not connected the main antenna during the router operation.

- LTE antennas:
  - Terminal antenna Taoglas TG.30.8113, order code: BB-TG30
  - Magnetic mount antenna Taoglas GA.110.101111, order code: BB-GA110
- Power Supply 12V / 12W, order code: BB-RPS-v3-MO4-M
  - Multi country (EU, UK, AUS, US)
  - Level Efficiency VI

Antenna

Use a SMA connector to connect the antennas to the router. The main antenna is connected to the router by screwing on the ANT connector (see the figure below). A second diversity antenna can be connected to the DIV connector to improve performance.

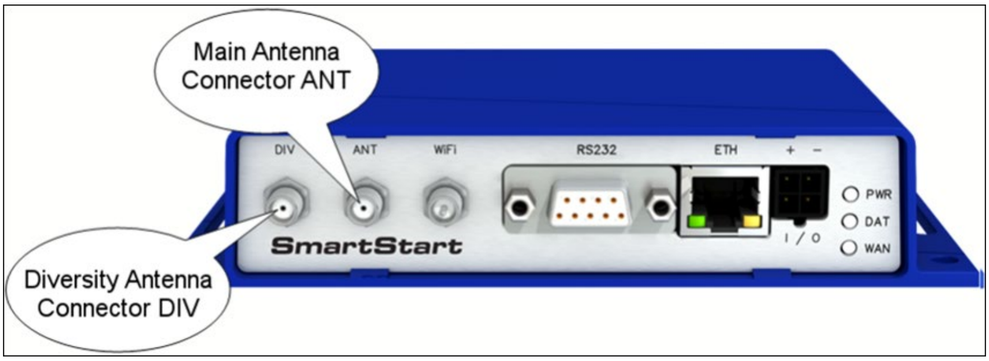
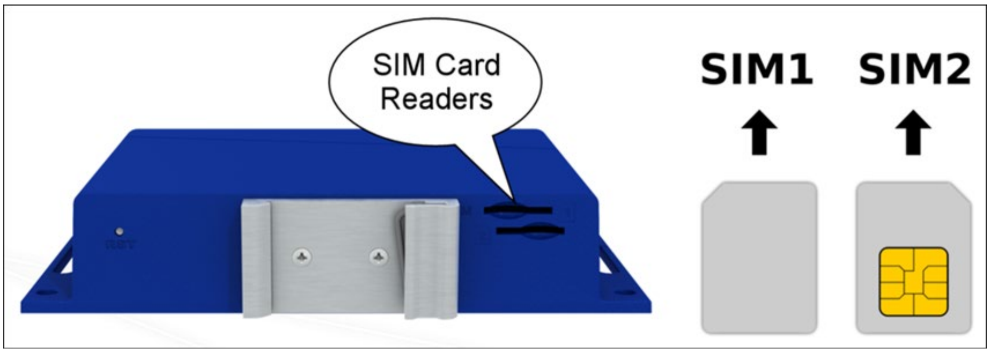


Fig. 7:

SIM Card

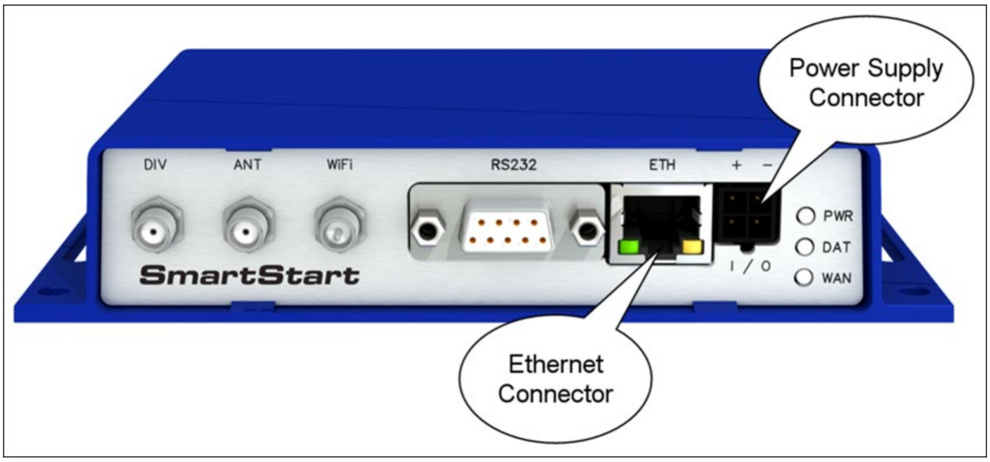
The SIM card readers, for 3 V and 1.8 V SIM cards, are located on the rear panel of the router. If you intend to use this device to communicate over a cellular network, place an activated data-provisioned SIM card into the SIM card reader. Push your SIM card into the SIM1 or SIM2 slot until it clicks in place.

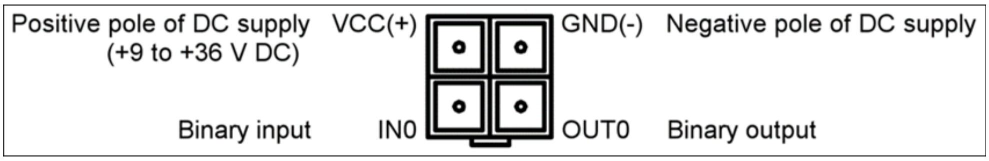
Note: Disconnect the router from the power supply, before handling the SIM card.



Power

The router requires an external DC power supply. The DC voltage required is between +9 to +36 V DC. The router has built-in protection against reverse polarity without signaling. Connect the power supply cable to the PWR connector on the front panel of the router (see figure below).





Ethernet

Provision is available for connecting an Ethernet to the ETH connector on the front panel.

Note: Connect your laptop or PC to this port to get a local web-server for device configuration and diagnostics.

Configuring and verifying IP Modem

This section provides the steps linked with the configuration and verification of the device.

Prerequisites

The following are the prerequisites required for the device configuration:

1. Computer is connected to the same subnet as the IP Modem.
2. Web browser required for accessing the IP Modem's internal web server.

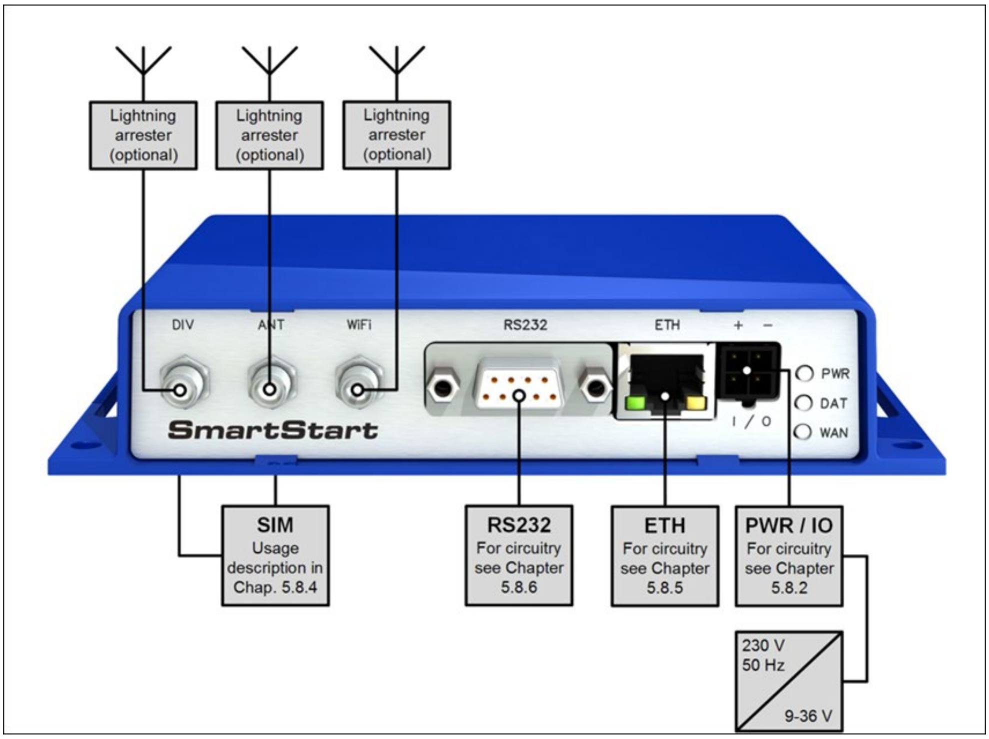
IP Modem Configuration

Configuration by Web Browser

Note: If router is already configured ignore steps 1 to 4

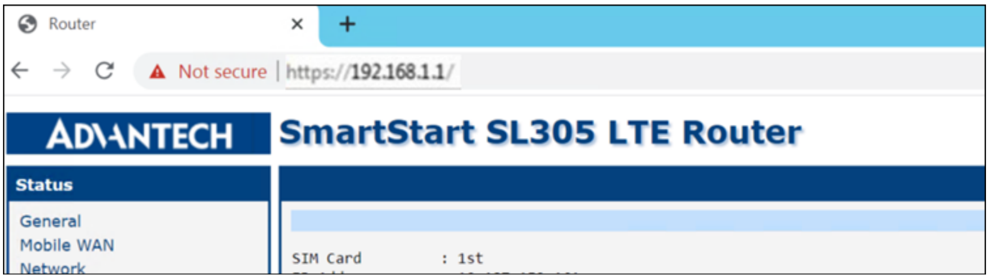
▷ Before putting the router into operation, it is necessary to connect all the components that are required to run your applications. Do not forget to insert a SIM card.
Note: The router cannot operate without a connected antenna, SIM card and power supply. The router may get damaged if the antenna is not connected.

1. Connect your laptop or PC to this port to get a local web server for device configuration and diagnostics.


Lightning arrester (optional)
Lightning arrester (optional)
Lightning arrester (optional)
DIV
ANT
WiFi
RS232
ETH
+ −
PWR
DAT
WAN
I / O
SmartStart
SIM Usage description in Chap. 5.8.4
RS232 For circuitry see Chapter 5.8.6
ETH For circuitry see Chapter 5.8.5
PWR / IO For circuitry see Chapter 5.8.2
230 V 50 Hz
9-36 V

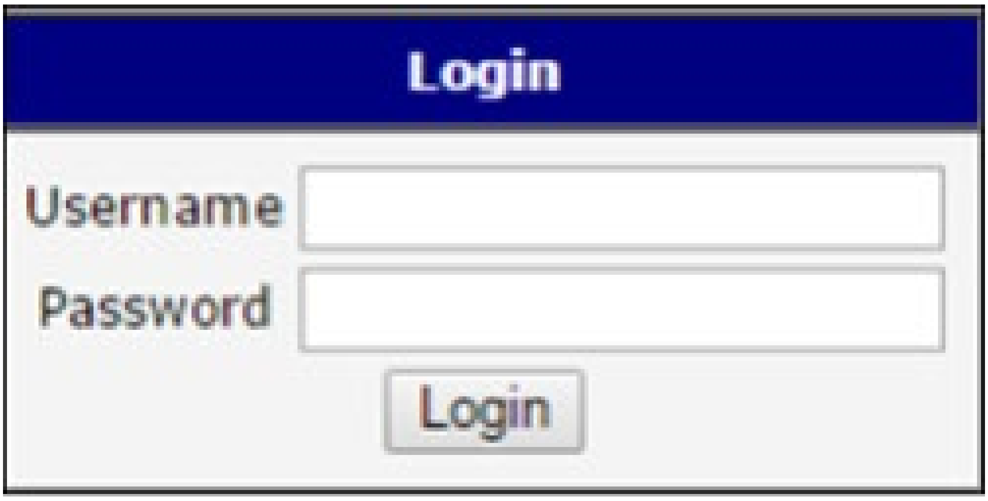
➩ The router will start when a power supply is connected to the router. By default, the router will automatically start to log on to the default APN. These router behaviors can be changed via the web interface.
Note: If no SIM card is inserted in the router, it is not possible for the router to operate. Any inserted SIM card must have active data transmission.

2. Enter the IP address of the router into the web browser. The default IP address of the router is 192.168.1.1. It is necessary to use HTTPS protocol for secure communication over a network.

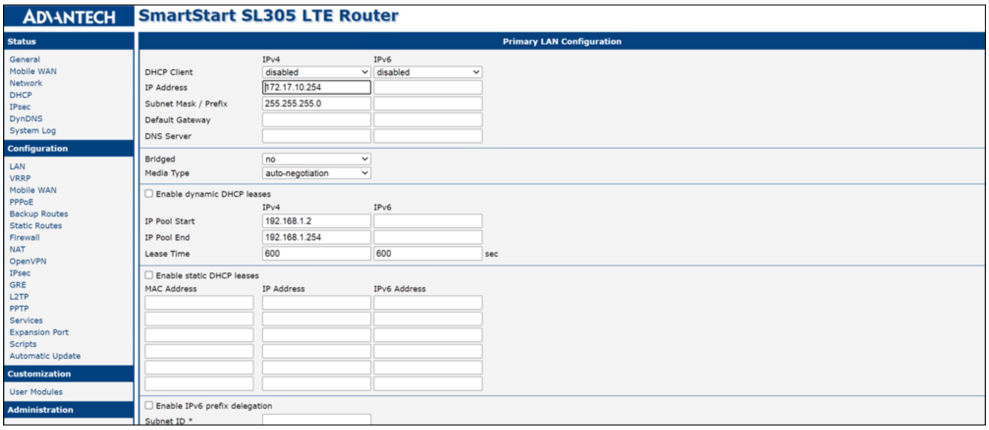

Router
Not secure | https://192.168.1.1/
ADVANTECH
SmartStart SL305 LTE Router
Status
General
Mobile WAN
Network

SIM Card : 1st

3. Enter the default username “root” and default password available on the back of the device for configuration.



– Set the Primary LAN Configuration, if you are configuring the IP modem for the first time. If you have already configured the IP modem, then in this step you can update the Primary LAN Configuration.
Note: An IP address is required for the IP Modem before the device configuration process. After an initial IP address is obtained, the IP Modem can be reconfigured with a static IP address.



Primary LAN Configuration

	IPv4	IPv6	
DHCP Client	disabled	disabled	
IP Address	172.17.10.254		
Subnet Mask / Prefix	255.255.255.0		
Default Gateway			
DNS Server			
Bridged	no		
Media Type	auto-negotiation		

□ Enable dynamic DHCP leases

	IPv4	IPv6	
IP Pool Start	192.168.1.2		
IP Pool End	192.168.1.254		
Lease Time	600	600	sec

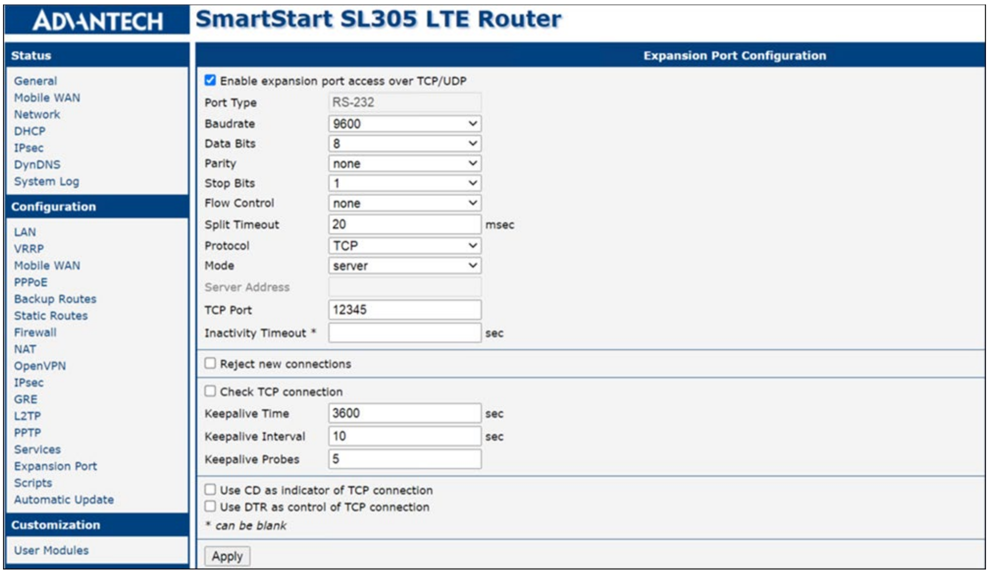
□ Enable static DHCP leases

MAC Address	IP Address	IPv6 Address

□ Enable IPv6 prefix delegation

Subnet ID *

4. Set **TCP port** under **Expansion Port Configuration.**



Expansion Port Configuration

☑ Enable expansion port access over TCP/UDP

Port Type	RS-232	
Baudrate	9600	
Data Bits	8	
Parity	none	
Stop Bits	1	
Flow Control	none	
Split Timeout	20	msec
Protocol	TCP	
Mode	server	
Server Address		
TCP Port	12345	
Inactivity Timeout *		sec

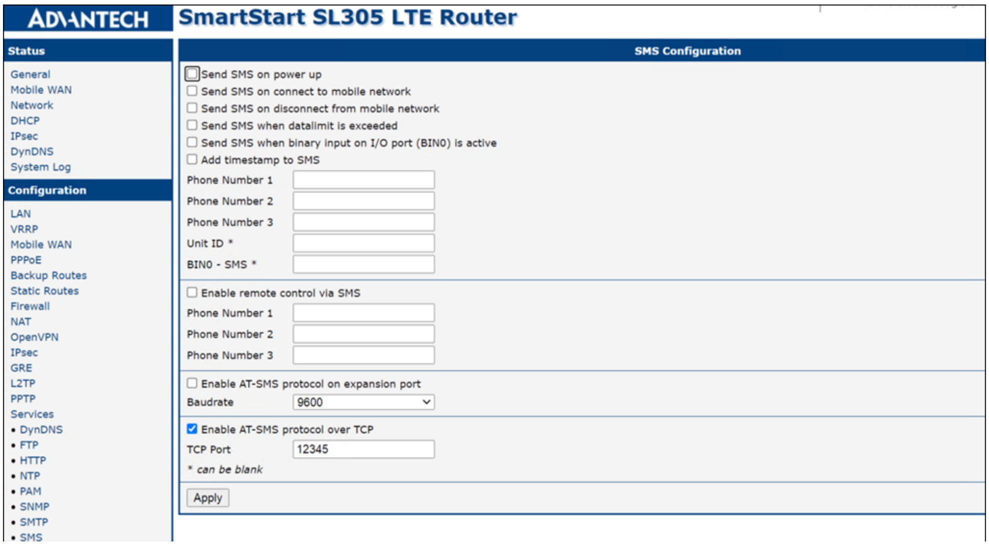
□ Reject new connections

□ Check TCP connection

Keepalive Time	3600	sec
Keepalive Interval	10	sec
Keepalive Probes	5	

□ Use CD as indicator of TCP connection
□ Use DTR as control of TCP connection
* *can be blank*

5. Enable **At-SMS protocol over TCP** under **SMS Configuration.**



SMS Configuration

□ Send SMS on power up
□ Send SMS on connect to mobile network
□ Send SMS on disconnect from mobile network
□ Send SMS when datalimit is exceeded
□ Send SMS when binary input on I/O port (BIN0) is active
□ Add timestamp to SMS

Phone Number 1
Phone Number 2
Phone Number 3
Unit ID *
BIN0 - SMS *

□ Enable remote control via SMS

Phone Number 1
Phone Number 2
Phone Number 3

□ Enable AT-SMS protocol on expansion port

Baudrate 9600

☑ Enable AT-SMS protocol over TCP

TCP Port 12345

* *can be blank*

6. Reboot the modem.
   - If you are configuring the IP modem for the first time, then you need to disconnect the laptop or PC from IP modem ETH port and connect the device in network subnet.
     Ignore this step if you are not configuring for the first time.

For detailed information

https://icr.advantech.cz/support/router-models/download/551/smartstart-sl305-user-s-manual-20200724.pdf

http://advdownload.advantech.com/productfile/Downloadfile1/1-1I8983B/Start_Guide_SmartStart_SmartFlex_SmartMotion_EN_20170125.pdf

1.4 Redundancy Supplemental

Redundancy Supplemental

This section provides reference and background information for integrating the Redundancy Supplemental feature. For procedures and workflows, see step-by-step section.

Notification provides a redundancy feature using an off-the-shelf redundancy solution from Stratus Technologies called everRun 7.2. Notification requires the everRun 7.2 enterprise version 7.2.0.0, or greater. Please see the everRun documents for details on how redundancy is realized. A successful Notification redundant setup includes the following step.

- Creating a Windows Server 2008 R2 Standard Virtual Machine (VM) in the server pool.

Server Failover

Failover is a backup operational mode in which the functions of a system component such as a processor, server, network, or database are assumed by secondary system components when the primary component is unavailable in case of failure or scheduled down time.

Server Failover by Notification

Notification uses Stratus everRun 7.2 to provide failover. For instructions on installing everRun 7.2 software, see Installing Stratus everRun 7.4.1.

Notification is installed on a Virtual Machine protected via everRun 7.2 software. In case of a hardware failure on one of the servers, everRun 7.2 automatically transitions the protected Virtual Machine to the other server in the pool. Due to this transition, clients and devices connected to the Notification system continue to remain connected without loss of functionality thus achieving the required failover. For verification of server failover, see Verifying Failover.

Redundancy Supplemental

This section provides additional procedures for integrating the Redundancy Supplemental feature.

For workflows, see the step-by-step section.

Installing Stratus everRun 7.4.1

First, contact Stratus to receive the installation ISOs, MSIs, and documents. Stratus usually sends an email with a user name and password that can be used in a particular Stratus site, where all the artifacts (ISOs, MSIs, and documents) for the version of everRun can be downloaded. The following sections detail the installation of everRun 7.4.1 The documents and other required artifacts for this version are also listed in the section Reference Docs.

Reference Docs

Each customer is provided a user account on the Stratus portal http://www.stratus.com/services-support/downloads/?product=everrun&release=7-4-1-0 with access to download the latest software, hotfixes, and help documents.

Prerequisites

- **Installation Files**

The installation software is available for download on the Stratus portal. Notification has completed testing on **everRun 7.4.1**.

- **Licenses**

EverRun license: This is received through email which contains the license key.

- **Hardware Configuration**

▷ **Virtualization** needs to be enabled in the BIOS of the machines on which CentOS will be installed. This feature is turned OFF in the default BIOS settings. To turn it ON, go into the BIOS setup of the machine at startup. For the Dell servers, use the following steps:

1. Press **F2** during boot to enter system setup.
2. Use the **UP**/**DOWN** arrow keys to highlight Processor settings and press **ENTER**.
3. Use the **UP**/**DOWN** arrow keys to select **Virtualization Technology**. Use the **LEFT**/**RIGHT** arrow keys to enable.
   NOTE: CentOS installation is not possible without enabling this setting or if there is no hardware support for virtualization.

Preparation

The everRun installation for Notification consists of two servers as part of the redundant pool. A web browser is used to log on to the Stratus everRun Availability Console.

Ensure that everRun version below 7.4.1 is not installed.

NOTE: The IP addresses need to be static. Hence, the IP address to be used needs to be decided before beginning the installation of CentOS.

Refer to the everRun's *User's Guide* located at http://everrundoc.stratus.com/7.4.1.0/en-us/Default.htm#Help/P02_Support/N_SupportDocs.htm%3FTocPath%3DSupporting Documents for more details on the configuration and connection of the different Network Interface Cards (NIC):

- ETH0/NIC0: Not used
- ETH1/NIC1 links of the servers will be used for **Management** links. This needs to be connected to 1 Gbps links on the switch.
- ETH2/NIC2 and ETH3/NIC3 will be used for the **A** links.
- ETH4/NIC4 and ETH5/NIC5 will be used for **Business** links.

Network Setup

Physical Connection for the Different Ports

Each server has six Ethernet ports. Connect them as indicated below.

NOTE:
The numbers assigned to the NICs below may change depending on how the network cards itself have been connected in the system

NICNum	Network num	Bandwidth	Connected to?	Comments
NIC 0	Network 0	1 Gbps	Not connected	
NIC 1	Network 1	1 Gbps	MNS switch	Connection to the MNS switch. Note that this has to be a 1 Gbps connection or else the initial sync of the VM takes longer and EverRun UI may continuously display an error.
NIC 2, 3	Network 2, 3	10 Gbps	A links. Cross connected between the servers.	Special 10GB link cables need to be used in this instance. If that is not available, use Cat-5E or Cat-6 cables.
NIC 4	Network 4	100 Mbps/1 Gbps	Connected to company network. This is optional and is used for accessing to VM via the corporate network for testing and other activities.	If required, this adaptor also needs to be added to the VM and configured to use the company network gateway. This may be useful for debugging when developers on the dev network need to access the VM. Contact the IT department for configuring IP address.
NIC 5	Network 5	100 Mbps/1 Gbps	Management links connected to the MNS switch.	This adapter needs to be added to the VM. Since it is connected to the MNS switch, this would be the Business link. The IP address can be statically assigned to 192.168.1.3. In case of failover, this IP address would still be available.

Installing Software on the First Physical Machine Using the User Interface

This section describes how to perform an initial installation of the everRun software on node0, which is the first physical machine (PM).
NOTE: To perform an installation by mounting the ISO image, you must first configure your system's remote-management feature (for example, iDRAC on a Dell system). See the manufacturer's documentation for instructions.

1. Power on the first PM, if it is not already powered on, and either insert the installation software DVD or mount the ISO image.

2. As the system powers on, enter the BIOS and configure the required and optional BIOS settings as described in the *Configuring the BIOS* section of the everRUN’s *User’s Guide* located at: http://everrundoc.stratus.com/7.4.1.0/en-us/Default.htm#Help/P02_Support/N_SupportDocs.htm%3FTocPath%3DSupporting Documents

3. When the installation software loads, the **Welcome** window displays with the installation options as described in the *Installation Options* section of the everRUN's *User's Guide* located at: http://everrundoc.stratus.com/7.4.1.0/en-us/Default.htm#Help/P02_Support/N_SupportDocs.htm%3FTocPath%3DSupporting Documents
From this window, choose the following option to perform the initial installation:
   - Installing via the user interface - This method is best for users who are not familiar with the installation process and who prefer to follow a GUI-based procedure with prompts.
4. Use the arrow keys to select **Install everRun** > **Create a new system**, and press **Enter**.
NOTE: No action is required until the window described in the next step displays.
5. The **Select** interface for private physical machine connection window sets the physical interface to use for the private network. To use the first embedded port, use the arrow keys to select em1 (if it is not already selected), and then press **F12** to save your selection and select the next window.
NOTE 1: If you are not sure of which port to use, use the arrow keys to select one of the ports, and click **Identify**. The LED on the selected port will then flash for 30 seconds, allowing you to identify it. Since the LED may also flash due to activity on that network, Stratus recommends that you leave the cable disconnected during the identification process. Reconnect the cable immediately after identification is complete.
NOTE 2: If the system contains no embedded ports, select the first option interface instead.
6. The Select interface for managing the system (ibiz0) window sets the physical interface to use for the management network. To use the second embedded port, use the arrow keys to select em2 (if it is not already selected), and then press **F12** to save your selection and select the next window.
NOTE: If the system contains only one embedded port, select the first option interface. If the system contains no embedded ports, select the second option interface.
7. The Select the method to configure ibiz0 window sets the management network for node0 as either a dynamic or static IP configuration. Typically, you set this as a static IP configuration, so use the arrow keys to select Manual configuration (Static Address) and press **F12** to save your selection and select the next window. However, to set this as a dynamic IP configuration, select Automatic configuration via DHCP and press **F12** to save your selection and select the next window.
8. If you selected Manual configuration (Static Address) in the previous step, the Configure em2 window displays. Enter the following information and press **F12**.
   - IPv4 address
   - Netmask
   - Default gateway address
   - Domain name server address
NOTE 1: Contact your network administrator for this information.
NOTE 2: If you enter invalid information, the window redisplays until you enter valid information.
9. At this point, the installation continues without additional prompts. No action from you is required until the first PM reboots. After it reboots, do the following:
   - Remove the DVD, or unmount the ISO image.
   - If you configured the IP address dynamically, record its IP address as described in *Recording the Management IP Address* section of the

everRUN’s *User’s Guide* located at:
http://everrundoc.stratus.com/7.4.1.0/en-us/Default.htm#Help/P02_Support/N_SupportDocs.htm%3FTocPath%3DSupporting Documents

Installing Software on the Second Physical Machine Using the User Interface

This topic describes how to perform an initial installation of the everRun software on node1, which is the second physical machine (PM).
NOTE: To perform an installation by mounting the ISO image, you must first configure your system's remote-management feature (for example, iDRAC on a Dell system). See the manufacturer's documentation for instructions.

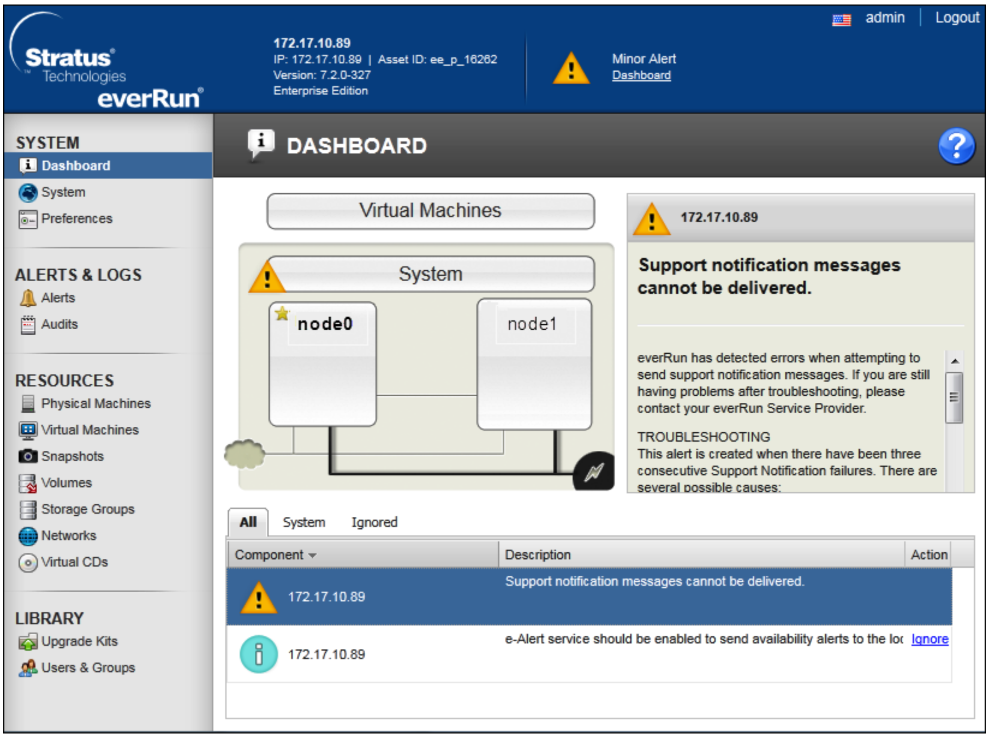
1. Power on the second PM, if it is not already powered on, and either insert the installation software DVD or mount the ISO image.
2. As the system powers on, enter the BIOS and configure the required and optional BIOS settings as described in the *Configuring the BIOS* section of the everRUN’s *User’s Guide* located at:
   http://everrundoc.stratus.com/7.4.1.0/en-us/Default.htm#Help/P02_Support/N_SupportDocs.htm%3FTocPath%3DSupporting Documents
   - ➩ When the installation software loads, the **Welcome** window displays and displays the options shown in the *Installation Options* section of the everRUN’s *User’s Guide* located at:
     http://everrundoc.stratus.com/7.4.1.0/en-us/Default.htm#Help/P02_Support/N_SupportDocs.htm%3FTocPath%3DSupporting Documents
     From this window, you can perform the initial installation using either the user interface or the command line.
3. Use the arrow keys to select **Replace PM** > **Join system: Initialize data**, and press **Enter**.
   NOTE: No action is required until the window described in the next step displays.
4. The **Select interface for private Physical Machine connection** window sets the physical interface to use for the private network. To use the first embedded port, use the arrow keys to select **em1** (if it is not already selected), and then press **F12** to save your selection and select the next window.
   NOTE 1: If you are not sure of which port to use, use the arrow keys to select one of the ports, and click **Identify**. The LED on the selected port will then flash for 30 seconds, allowing you to identify it. Since the LED may also flash due to activity on that network, Stratus recommends that you leave the cable disconnected during the identification process. Reconnect the cable immediately after identification is complete.
   NOTE 2: If the system contains no embedded ports, select the first option interface instead.
5. The **Select interface for managing the system (ibiz0)** window sets the physical interface to use for the management network. To use the second embedded port, use the arrow keys to select **em2** (if it is not already selected), and then press **F12** to save your selection and select the next window.
   NOTE: If the system contains only one embedded port, select the first option interface. If the system contains no embedded ports, select the second option interface.
6. The **Select the method to configure ibiz0** window sets the management network for node1 as either a dynamic or static IP configuration. Typically, you set this as a static IP configuration, so use the arrow keys to select **Manual**

configuration (Static Address) and press **F12** to save your selection and select the next window. However, to set this as a dynamic IP configuration, select **Automatic configuration via DHCP** and press **F12** to save your selection and select the next window.

7. If you selected **Manual configuration(Static Address)** in the previous step, the **Configure em2** window displays. Enter the following information and press **F12**:
   - IPv4 address
   - Netmask
   - Default gateway address
   - Domain name server address
     NOTE 1: Contact your network administrator for this information.
     NOTE 2: If you enter invalid information, the window redisplays until you enter valid information.

8. At this point, the installation continues without additional prompts. No action from you is required until the second PM reboots. After it reboots, do the following:
   - Remove the DVD, or unmount the ISO image.
   - If you configured the IP address dynamically, record its IP address as described in the *Recording the Management IP Address* section of the everRUN's *User's Guide* located at: [http://everrundoc.stratus.com/7.4.1.0/en-us/Default.htm#Help/P02_Support/N_SupportDocs.htm%3FTocPath%3DSupporting Documents](http://everrundoc.stratus.com/7.4.1.0/en-us/Default.htm#Help/P02_Support/N_SupportDocs.htm%3FTocPath%3DSupporting%20Documents)

9. Log on to the everRun Availability Console and verify that node1 displays on the **DASHBOARD**.



172.17.10.89
IP: 172.17.10.89 | Asset ID: ee_p_16262
Version: 7.2.0-327
Enterprise Edition

Minor Alert
Dashboard

172.17.10.89

Support notification messages cannot be delivered.

everRun has detected errors when attempting to send support notification messages. If you are still having problems after troubleshooting, please contact your everRun Service Provider.

TROUBLESHOOTING
This alert is created when there have been three consecutive Support Notification failures. There are several possible causes:

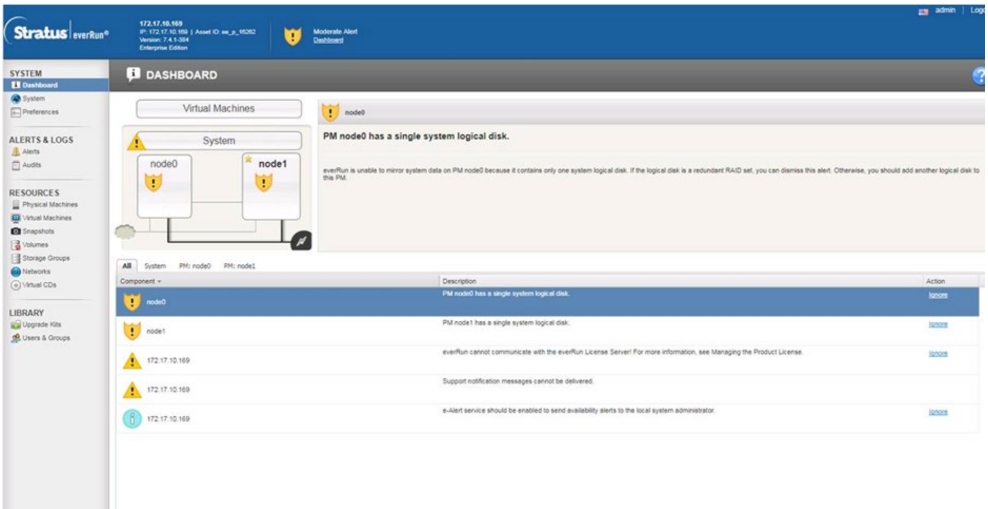
Component	Description	Action
172.17.10.89	Support notification messages cannot be delivered.	
172.17.10.89	e-Alert service should be enabled to send availability alerts to the loc	Ignore

Troubleshooting the Physical Machine

For information on troubleshooting the physical machines, refer to the *Troubleshooting Physical Machines* section of the everRUN's *User's Guide* located at:

http://everrundoc.stratus.com/7.4.1.0/en-us/Default.htm#Help/P02_Support/N_SupportDocs.htm%3FTocPath%3DSupporting Documents

If there are any issues in the installation of everRun 7.2 software, the Alert icon ❗ displays on the **DASHBOARD** of the everRun Availability Console.



node0

PM node0 has a single system logical disk.

everRun is unable to mirror system data on PM node0 because it contains only one system logical disk. If the logical disk is a redundant RAID set, you can dismiss this alert. Otherwise, you should add another logical disk to this PM.

Component	Description	Action
node0	PM node0 has a single system logical disk.	Ignore
node1	PM node1 has a single system logical disk.	Ignore
172.17.10.169	everRun cannot communicate with the everRun License Server! For more information, see Managing the Product License.	Ignore
172.17.10.169	Support notification messages cannot be delivered.	
172.17.10.169	e-Alert service should be enabled to send availability alerts to the local system administrator.	Ignore

Troubleshooting the Java Errors Encountered on the EverRun Availability Console

For information on troubleshooting the Java errors encountered on the everRun Availability Console, refer to:

http://docs.oracle.com/javase/7/docs/technotes/guides/jweb/jcp/jcp.html

Supporting Documents

For release information, reference and troubleshooting information, refer to the *Supporting Documents* section of the everRUN's *User's Guide* located at http://everrundoc.stratus.com/7.4.1.0/en-us/Default.htm#Help/P02_Support/N_SupportDocs.htm%3FTocPath%3DSupporting Documents.

Verifying Failover

This section describes the process for verifying failover before and after Notification installation.

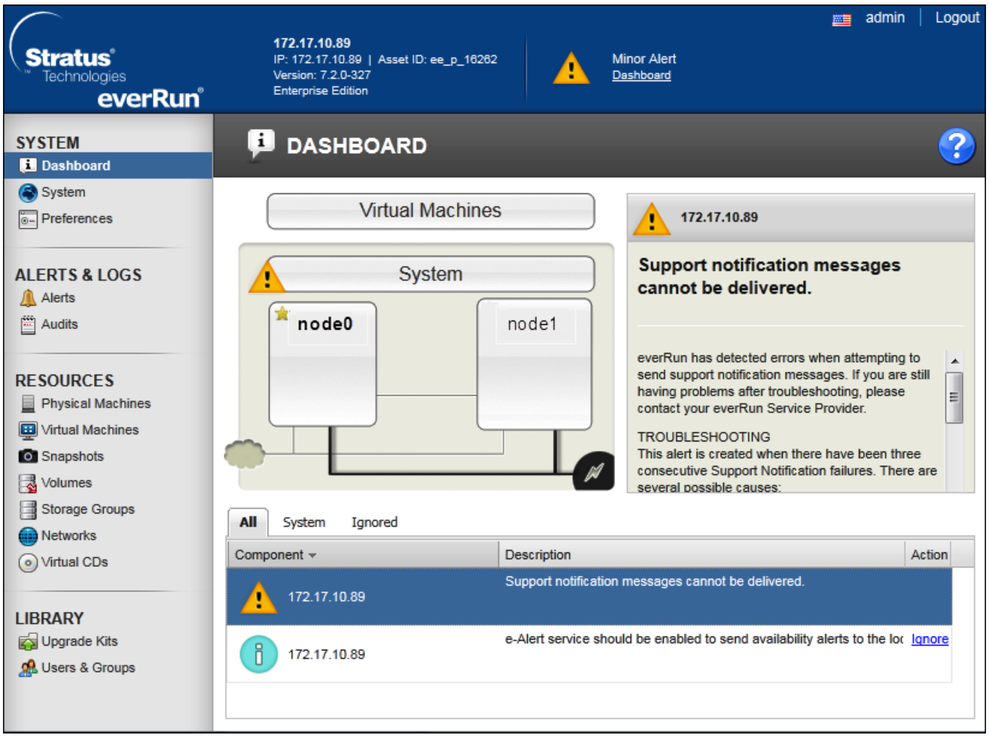
For background information on Server Failover, see Server Failover.

Select an appropriate link under **Further information** section for the task you want to perform.

Verification Before Installing Notification

▷ Virtual Machines are created and protected with everRun 7.2.

1. Connect to the protected Virtual Machine via remote desktop.
2. Open a browser in the client machine and start streaming a video.
3. While the video is being played, forcibly bring down one of the servers, for example, **node0** by pulling the plug.
   NOTE: Bring down the server on which the currently active compute instance of the protected Virtual Machine is running so that a transition occurs.



172.17.10.89
IP: 172.17.10.89 | Asset ID: ee_p_16262
Version: 7.2.0-327
Enterprise Edition

Minor Alert
Dashboard

172.17.10.89

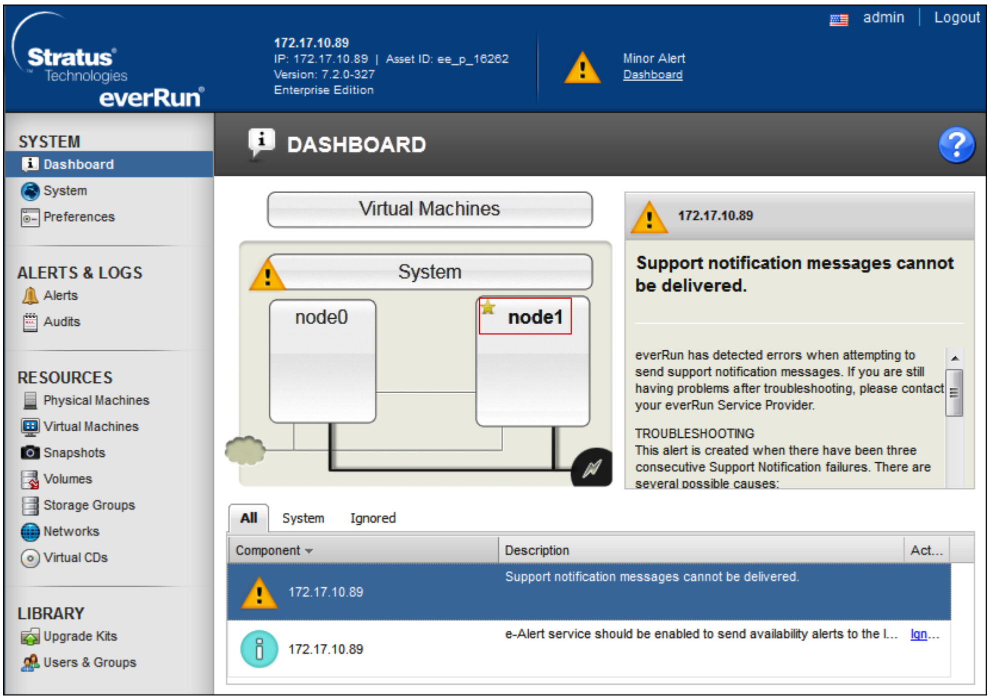
Support notification messages cannot be delivered.

everRun has detected errors when attempting to send support notification messages. If you are still having problems after troubleshooting, please contact your everRun Service Provider.

TROUBLESHOOTING
This alert is created when there have been three consecutive Support Notification failures. There are several possible causes:

Component	Description	Action
172.17.10.89	Support notification messages cannot be delivered.	
172.17.10.89	e-Alert service should be enabled to send availability alerts to the loc	Ignore

⇨ The remote desktop connection to the protected Virtual Machine is not lost and the video continues to stream. The star icon ★ is shifted to **node1** making **node1** as the primary physical machine.



172.17.10.89
IP: 172.17.10.89 | Asset ID: ee_p_16262
Version: 7.2.0-327
Enterprise Edition

Minor Alert
Dashboard

172.17.10.89

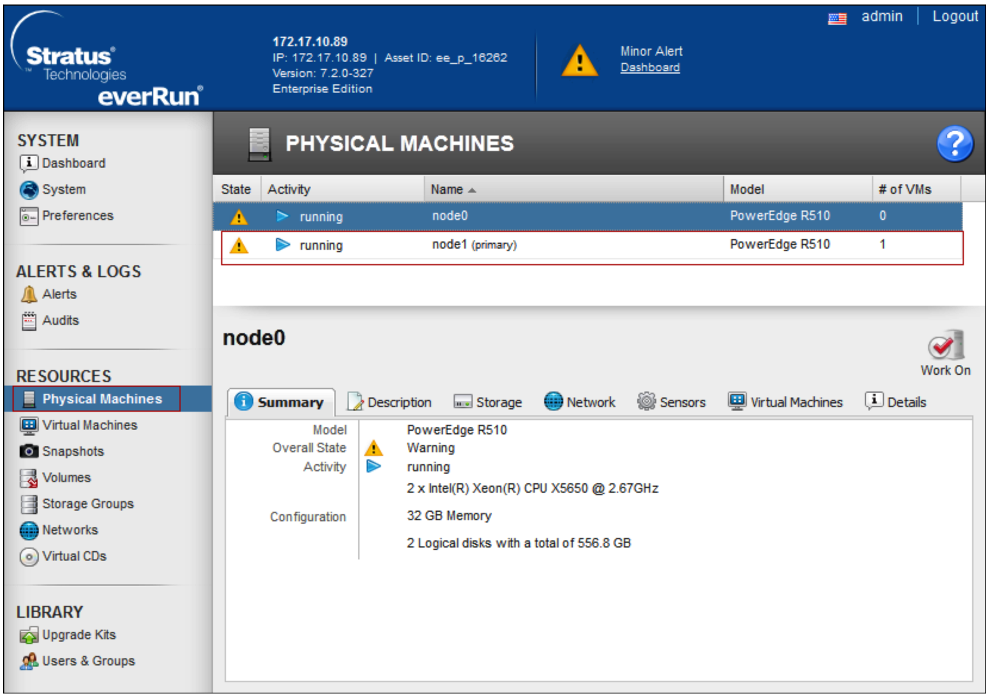
Support notification messages cannot be delivered.

everRun has detected errors when attempting to send support notification messages. If you are still having problems after troubleshooting, please contact your everRun Service Provider.

TROUBLESHOOTING
This alert is created when there have been three consecutive Support Notification failures. There are several possible causes:

Component	Description	Act...
172.17.10.89	Support notification messages cannot be delivered.	
172.17.10.89	e-Alert service should be enabled to send availability alerts to the l...	Ign...

4. Select **Physical Machines** to verify that **node1** is the primary physical machine.



172.17.10.89
IP: 172.17.10.89 | Asset ID: ee_p_16262
Version: 7.2.0-327
Enterprise Edition

State	Activity	Name ▲	Model	# of VMs
⚠	▶ running	node0	PowerEdge R510	0
⚠	▶ running	node1 (primary)	PowerEdge R510	1

node0

Model	PowerEdge R510
Overall State	⚠ Warning
Activity	▶ running
Configuration	2 x Intel(R) Xeon(R) CPU X5650 @ 2.67GHz 32 GB Memory 2 Logical disks with a total of 556.8 GB

Fig. 8: Verification for the Primary Physical Machine

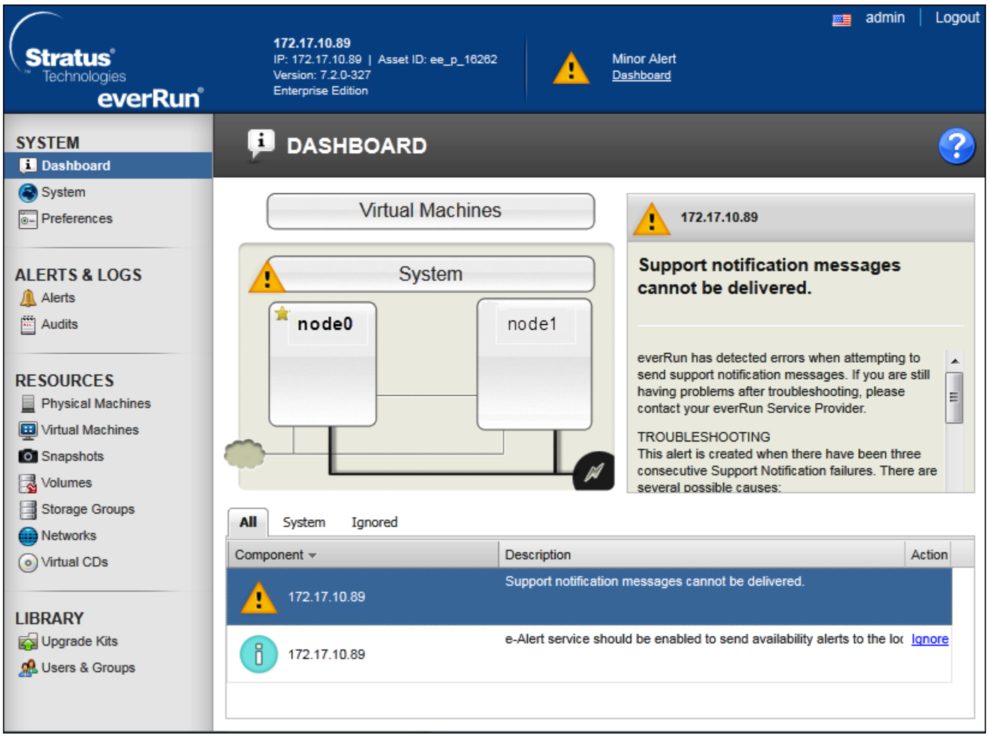
Verification After Installing Notification

▷ Virtual Machines are created and protected with everRun 7.2.

▷ Notification is installed on the client machines.

1. Connect a client machine to the protected Virtual Machine via remote desktop.
2. Forcibly bring down one of the servers for example, **node0** by pulling the plug.

   NOTE: Bring down the server on which the currently active compute instance of the protected Virtual Machine is running so that a transition occurs.



172.17.10.89
IP: 172.17.10.89 | Asset ID: ee_p_16262
Version: 7.2.0-327
Enterprise Edition

172.17.10.89

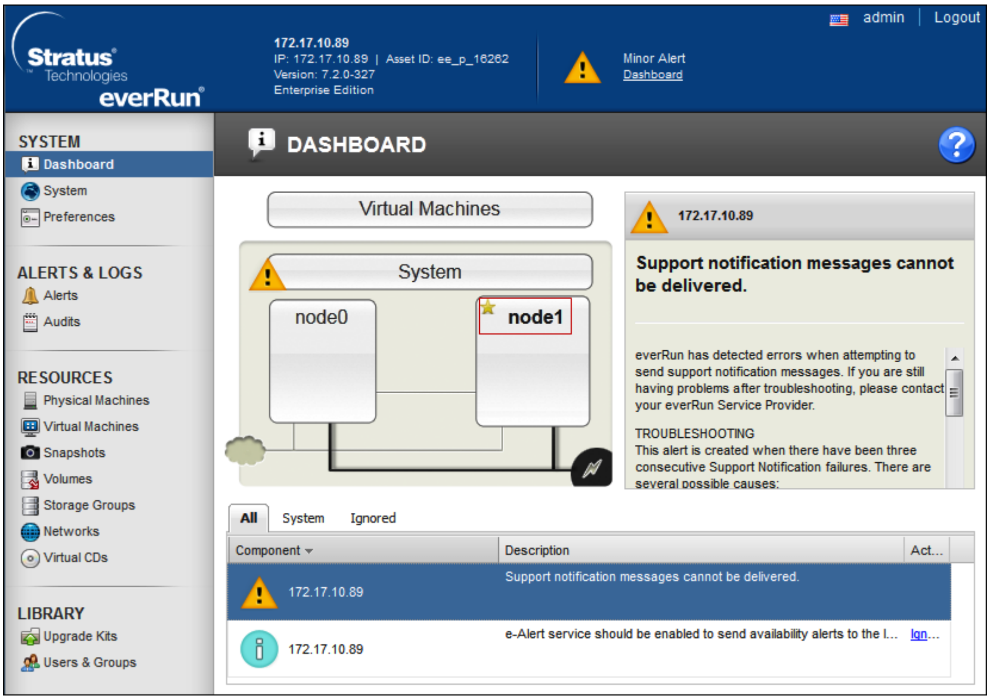
Support notification messages cannot be delivered.

everRun has detected errors when attempting to send support notification messages. If you are still having problems after troubleshooting, please contact your everRun Service Provider.

TROUBLESHOOTING
This alert is created when there have been three consecutive Support Notification failures. There are several possible causes:

Component	Description	Action
172.17.10.89	Support notification messages cannot be delivered.	
172.17.10.89	e-Alert service should be enabled to send availability alerts to the loc	Ignore

⇨ Client does not lose the remote desktop connection to the protected Virtual Machine and all the Notification features are still accessible. The star icon ★ is shifted to **node1** making **node1** as the primary physical machine.



172.17.10.89
IP: 172.17.10.89 | Asset ID: ee_p_16262
Version: 7.2.0-327
Enterprise Edition

172.17.10.89

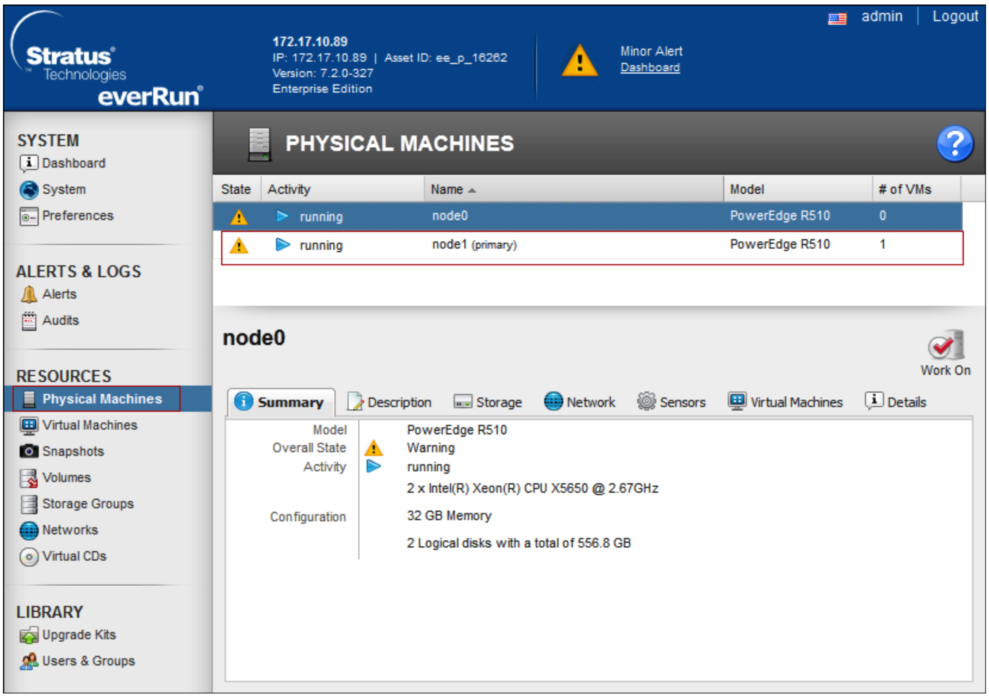
Support notification messages cannot be delivered.

everRun has detected errors when attempting to send support notification messages. If you are still having problems after troubleshooting, please contact your everRun Service Provider.

TROUBLESHOOTING
This alert is created when there have been three consecutive Support Notification failures. There are several possible causes:

Component	Description	Act...
172.17.10.89	Support notification messages cannot be delivered.	
172.17.10.89	e-Alert service should be enabled to send availability alerts to the l...	Ign...

3. Select **Physical Machines** to verify that **node1** is the primary physical machine.



172.17.10.89
IP: 172.17.10.89 | Asset ID: ee_p_16262
Version: 7.2.0-327
Enterprise Edition

State	Activity	Name	Model	# of VMs
⚠	▶ running	node0	PowerEdge R510	0
⚠	▶ running	node1 (primary)	PowerEdge R510	1

node0

Model	PowerEdge R510
Overall State	⚠ Warning
Activity	▶ running
	2 x Intel(R) Xeon(R) CPU X5650 @ 2.67GHz
Configuration	32 GB Memory
	2 Logical disks with a total of 556.8 GB

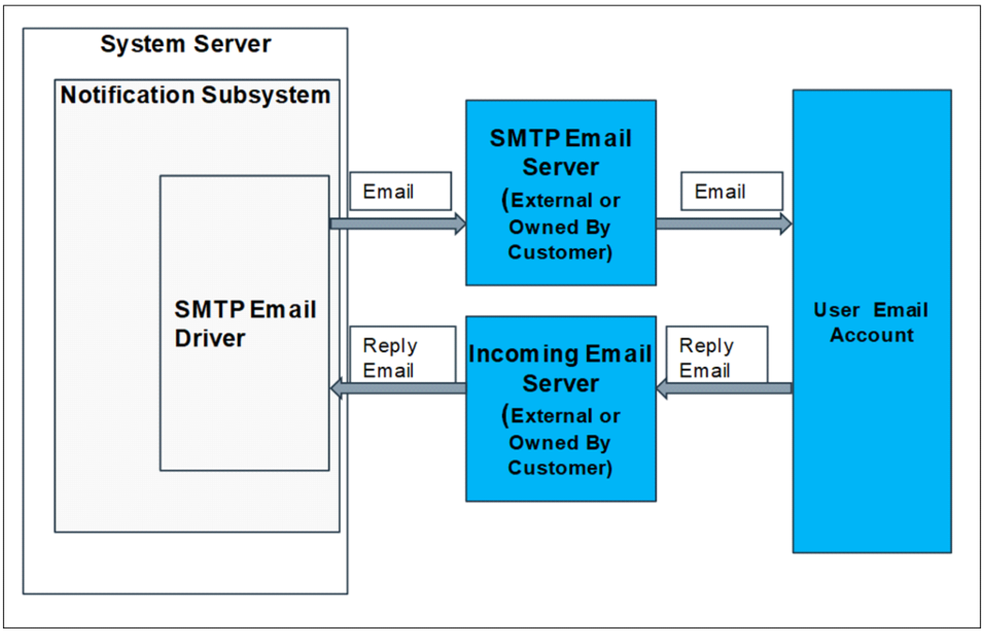
Fig. 9: Verification for the Primary Physical Machine

1.5 SMTP Email Server

SMTP Email Server

This section contains general reference information about SMTP Email Server. For procedures and workflows, see the step-by-step section.

Though technically SMTP Email Server is not a device, Notification generally uses the term device for entities participating in notification delivery, including intermediary services such as an SMTP Email Server.

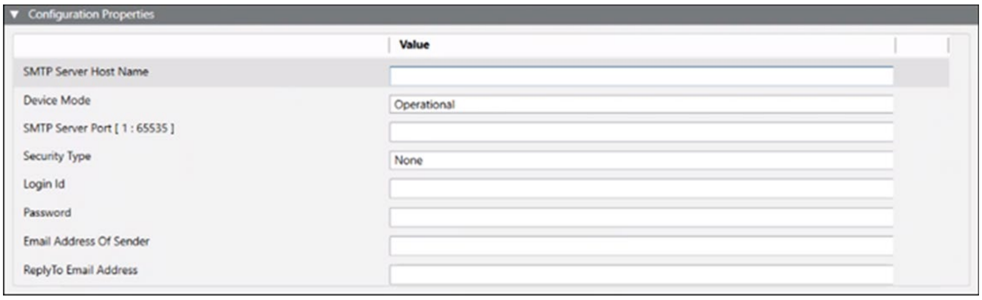

System Server
Notification Subsystem
SMTP Email Driver
Email
Reply Email
SMTP Email Server (External or Owned By Customer)
Incoming Email Server (External or Owned By Customer)
Email
Reply Email
User Email Account

Notification provides the capability to send messages to intended recipients as well as receive reply messages from them. To achieve this, Notification uses an SMTP Server to send emails through the SMTP protocol to email recipients. The email recipients send reply emails which are received by Notification through the

Incoming Email Server. Notification supports retrieving reply emails from an Incoming Email Server by one of two protocols:

- Internet Message Access Protocol (IMAP)
- Post Office Protocol 3 (POP3)

Configuration Properties for SMTP Email Server



▼ Configuration Properties

	Value
SMTP Server Host Name	
Device Mode	Operational
SMTP Server Port [1 : 65535]	
Security Type	None
Login Id	
Password	
Email Address Of Sender	
ReplyTo Email Address	

- **SMTP Server Host Name**: Enter the IP address or the server name of the SMTP Server.
- **Device Mode**: Select one of the following modes from the drop-down list:
  Disabled: In this mode, the driver does not process the messaging command, the device configuration change command, and perform status checks for the device. The device remains in disconnected state.
  Operational: In this mode, the driver processes the messaging command, the device configuration change command, and performs status checks for the device. The device will be in Disconnected/Connected state based on the connection state.
  Administrative: In this mode, the driver processes the device configuration change command and performs status checks for the device. The device will be in Disconnected/Connected state based on the connection state.
- **SMTP Server Port**: Enter the port number to use for the SMTP Server. Typically, this is 25 for most SMTP Servers. Check with the local IT admin or the SMTP Server host admin for the exact port number.
- **Security Type:** Select the options from the drop-down list.
  - **None:** No secure connection is provided.
  - **SSL:** Secure Sockets Layer (SSL) provides secure connection.
  - **TLS:** Transport Layer Security (TLS) provides secure connection.

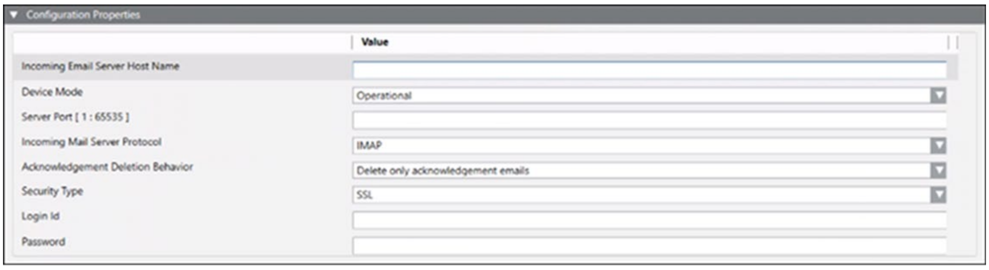
Refer to SMTP Email - External SMTP Providers Settings for more information.

- **Login Id**: Enter the SMTP Server's user name. Not used if the selected **Security Type** is **None**.
- **Password**: Enter the SMTP Server's password for the corresponding user account. Not used if the selected **Security Type** is **None**.
  NOTE: The Password is stored in encrypted format for security reasons. An App password needs to be entered for gmail accounts with two step verification.
- **Email Address of Sender**: Enter the email address that will be shown as **Sender ID** in the email notifications that are delivered. This email account is used by Notification to interact with the Recipient users.
  NOTE: Enter a valid email address in this field. If an invalid email address is entered in this field, no email delivery will occur at all.
- **Reply to Email Address**: Enter the email address that will be used to receive emails when recipients choose to reply to email notifications.
  NOTE: Enter a valid email address in this field. If an invalid email address is entered in this field, no email delivery will occur at all.

NOTE 1:
Some networks may have restrictions connecting to external SMTP servers like those offered by Google. Check with the local IT admin for means of accessing such external services should the need arise

NOTE 2:
When using an external SMTP server like Google, the first message sent out may result in failure since Google requires the account holder to authenticate the usage of the SMTP service. Log into the Gmail account and perform the verification steps so that the SMTP server is usable by Notification.

Configuration Properties for Incoming Email Server



▼ Configuration Properties

	Value
Incoming Email Server Host Name	
Device Mode	Operational
Server Port [1 : 65535]	
Incoming Mail Server Protocol	IMAP
Acknowledgement Deletion Behavior	Delete only acknowledgement emails
Security Type	SSL
Login Id	
Password	

- **Incoming Server Host Name**: Enter the host name or the IP address of the Incoming Email Server.
- **Device Mode**: Select one of the following modes from the drop-down list:
  Disabled: In this mode, the driver does not process the messaging command, the device configuration change command, and perform status checks for the device. The device remains in disconnected state.
  Operational: In this mode, the driver processes the messaging command, the device configuration change command, and performs status checks for the device. The device will be in Disconnected/Connected state based on the connection state.
  Administrative: In this mode, the driver processes the device configuration change command and performs status checks for the device. The device will be in Disconnected/Connected state based on the connection state.
- **Server Port**: Enter the port number to use for the Incoming Email Server. Typically, this is 995 for POP servers and 993 for IMAP servers. Check with the local IT admin or the Incoming Email Server host admin for the exact port number.
- **Incoming Email Server Protocol**: Select the Server Protocol for the incoming email, for example, POP3 or IMAP.
- **Acknowledgement Deletion Behavior**: Select the deletion behavior for the acknowledgements from the drop-down list:
  Delete only acknowledgement emails - The driver deletes only messages that are recognized as MNS acknowledgement messages from the email account after processing them. Use this option if the configured email account is also used for other purposes. Choosing this option might require periodic, manual purging of non-MNS messages in the email account.
  NOTE: The ‘Out of Office’ replies are not considered as a valid acknowledgement and hence will be deleted on selecting this option.
  Delete all incoming emails - The driver deletes all messages whether they are recognized as MNS acknowledgement messages (deletion after processing) or non-MNS messages. Choosing this option allows the system to run unattended because non-MNS messages will not collect in the email account.
- **Security Type:** Select the options from the drop-down list.
  - **None:** No secure connection is provided.
  - **SSL:** Secure Sockets Layer (SSL) provides secure connection.
  - **TLS:** Transport Layer Security (TLS) provides secure connection.

Refer to SMTP Email - External SMTP Providers Settings for more information.
NOTE: This option needs to be selected accordingly when the Incoming email

server on the customer site mandates this for connections to the Incoming Email Server.

- **Login Id**: Enter the Incoming Email Server's login ID. This email account is used by Notification to interact with Recipient users.
- **Password**: Enter the Incoming Email Server's password for the corresponding user account.
  NOTE: The Password is stored in encrypted format for security reasons.

External SMTP Providers Settings

Providers	SMTP Server Host Name	SMTP Server Port	Security Type	Username	Password
Gmail	smtp.gmail.com	587	TLS	A valid Gmail address	App Password of the corresponding Gmail account. Available only for accounts with two step verification
		465	SSL		
Yahoo	smtp.mail.yahoo.com	587	TLS	A valid Yahoo email address	App Password of the corresponding Yahoo email account
		465	SSL		
Hotmail	smtp.live.com	25	None	A valid Hotmail email address	Password of the corresponding Hotmail email account
GMX	mail.gmx.com	25	None	A valid GMX email address	Password of the corresponding GMX email account
		465	SSL		
		587	TLS		
Vodafone	smtp.vodafone.de	25 or 587	None	A valid Vodafone email address	Password of the corresponding Vodafone email account
T-Online	securesmtp.t-online.de	587	TLS	A valid T-Online email address	Password of the corresponding T-Online email account
	smtpmail.t-online.de	465	SSL	A valid T-Online email address	Password of the corresponding T-Online email account
		25	None		

External Incoming Email Server Settings

Providers	Server Type	Server Address	Server Port	Security Type	Login Id	Password
Gmail	IMAP	imap.gmail.com	993	SSL	A valid Gmail login ID	App Password of the corresponding Gmail account
	POP3	pop.gmail.com	995	SSL	A valid Gmail login ID	App Password of the corresponding Gmail account
Yahoo	IMAP	imap.mail.yahoo.com	993	SSL	A valid Yahoo login ID	App Password of the corresponding Yahoo email account

	POP3	pop.mail.yahoo.com	995	SSL	A valid Yahoo login ID	App Password of the corresponding Yahoo email account
Hotmail	IMAP	imap-mail.outlook.com	993	SSL	A valid Hotmail login ID	Password of the corresponding Hotmail email account
	POP3	pop-mail.outlook.com or pop3.live.com	995	SSL	A valid Hotmail login ID	Password of the corresponding Hotmail email account
GMX	IMAP	imap.gmx.com	993	SSL	A valid GMX login ID	Password of the corresponding GMX email account
	POP3	pop.gmx.com	995	SSL	A valid GMX login ID	Password of the corresponding GMX email account
Vodafone	IMAP	imap.vodafone.de	993	SSL	A valid Vodafone login ID	Password of the corresponding Vodafone email account
	POP3	pop.vodafone.de	995	SSL	A valid Vodafone login ID	Password of the corresponding Vodafone email account
T-Online	IMAP	imapmail.t-online.de	993	SSL	A valid T-Online login ID	Password of the corresponding T-Online email account
	POP3	popmail.t-online.de	995	SSL	A valid T-Online login ID	Password of the corresponding T-Online email account
	IMAP	secureimap.t-online.de	993	SSL	A valid T-Online login ID	Password of the corresponding T-Online email account
	POP3	securepop.t-online.de	995	SSL	A valid T-Online login ID	Password of the corresponding T-Online email account

- In order to use Hotmail POP Server, set the **Check Status Rate** approximately equal to 900000 milliseconds (15 minutes) and the **Input Messages Polling Interval** to 450 seconds approximately
- In case of Gmail POP Server, during shutdown situations of **MNS Service Host**, the email replies received by the **SMTP Email Driver** will not be logged in the Database by Notification System.
- For enabling POP or IMAP Servers, refer to the instructions provided on the specific email provider's site like Gmail, Yahoo, and so on.
- POP or IMAP External Incoming Email is not UL approved

SMTP Email Server

This section provides additional procedures of SMTP Email Server.

For workflows, see the Creating and Configuring SMTP Email Server section.

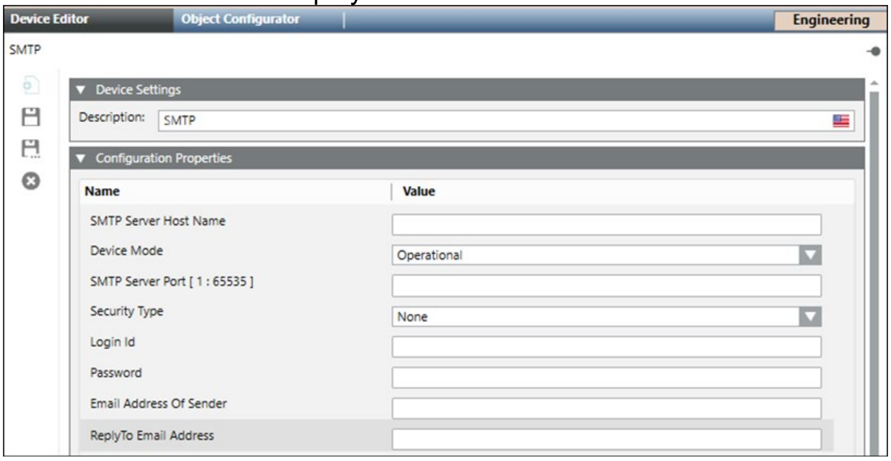
Configuring Message Identity

▷ An **SMTP Email Server** is added.
NOTE: For more information on adding devices, please refer to the *Devices* section.

▷ System Manager is in **Engineering** mode.

1. In System Browser, select **Management View**.
2. Select **Project** > **Field Networks** > **SMTP Email Server Field Network**.
3. Select the **SMTP Email Server**.

   ⇨ The **Device Editor** tab displays.



Description: SMTP

Name	Value
SMTP Server Host Name	
Device Mode	Operational
SMTP Server Port [1 : 65535]	
Security Type	None
Login Id	
Password	
Email Address Of Sender	
ReplyTo Email Address	

4. Enter a valid email address in **Email Address Of Sender** and **ReplyTo Email Address** under the **Configuration Properties** expander.
5. Click **Save** .

⇨ The Message Identity settings are saved.

Issued by
Siemens Switzerland Ltd
Smart Infrastructure
Global Headquarters
Theilerstrasse 1a
CH-6300 Zug
+41 58 724 2424
www.siemens.com/buildingtechnologies