SIEMENS

Notification Supported HW/SW Device Configurations Guide

A6V12131888_en_b_51
02.08.2022

Smart Infrastructure

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

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: 02.08.2022

Document ID: A6V12131888_en_b_51

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 5.0.

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*.
	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 Devices.

1.1 Adaptive LED Device

Adaptive LED Device

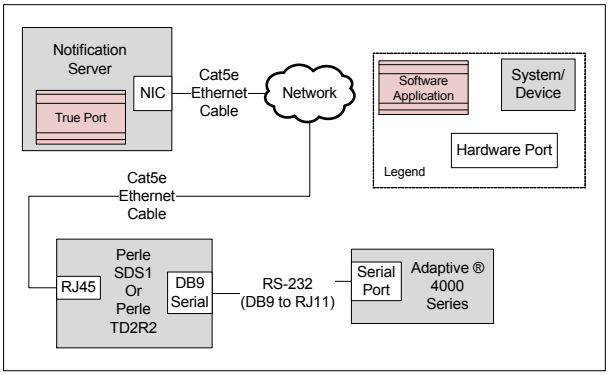
This section provides reference and background information for integrating the Adaptive LED Device. For procedures and workflows, see the step-by-step section.

The Adaptive® 4000 series LED displays provide on-premise text-based messaging as part of the solution. The Adaptive® 4000 series LED displays are serial based devices. Therefore, the deployment requires an IP-to-serial device to bridge the gap between the IP-based and the serial-based Adaptive® 4000 series LED displays.

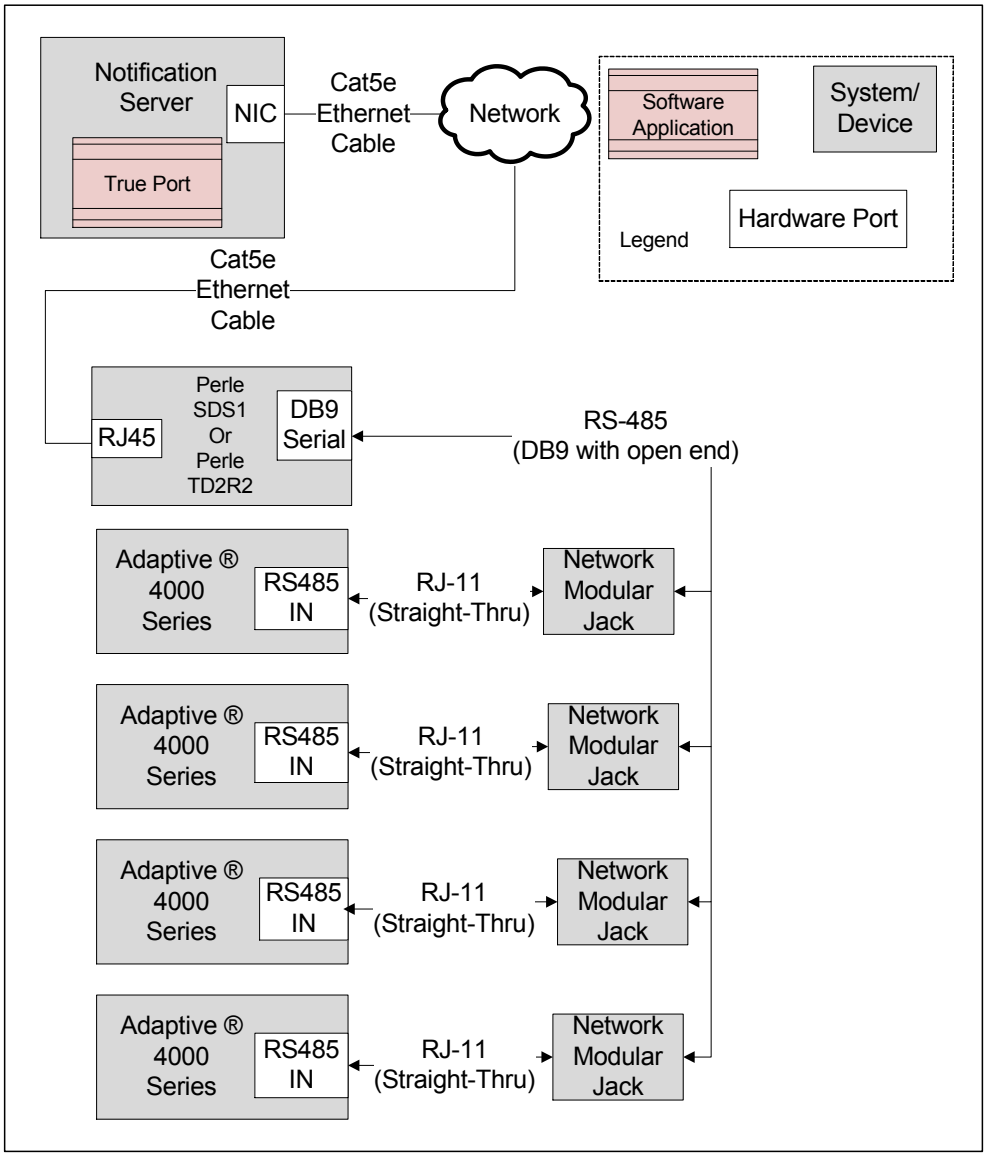
In addition, the Adaptive® 4000 series LED displays can be configured for RS-232 or RS-485 serial communication. RS-485 allows multiple Adaptive® 4000 series LED displays to be networked together and connected to a single IP-to-serial device.

Currently, special characters other than ASCII characters are not supported by the Adaptive® 4000 series LED displays.

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



Below is an overview over the system using the RS-485 configuration:



Notification can integrate with the Adaptive® 4000 series LED displays. The following models of Adaptive® 4000 series LED displays are supported by Notification.

- 4080C
- 4120C
- 4160C
- 4200C
- 4240C

Adaptive LED Device

The Adaptive 4000 series LED display must be installed properly before you begin the device and system configuration. Read the following topics to proceed with mounting the hardware, the device wiring and connection details.

Adaptive 4000 series LED display integration starts after the installation of the LED display. To integrate the Adaptive device, you must configure the serial address for the sign. Additional configuration is required on the Perle device for RS-485 and RS-232 interfaces.

Installing Perle Device

Prerequisites

Before proceeding, ensure that the following items are available:

- IOLAN SDS1 or IOLAN STS4-D
- 9-30VDC (400mA min) Power Supply, if not included with the Perle device
- Category 5 Ethernet cable
- Computer or Server to communicate with the Perle device
- The Perle device Installation CD or a computer with network access
- DB9 RS-232 serial cable – for use in serial communication applications.
  NOTE 1: The TruePort Driver that is used to communicate with the Perle device must be installed on the same server/machine that runs .
  NOTE 2: Make sure that the RJ45 jack 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 Perle device, the computer must be located under the same network.
  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 IOLAN SDS1 has two brackets on each side of the mounting holes. The installer is recommended to fasten the device to a flat surface by placing screws through the mounting holes.

Power

1. For the Perle IOLAN SDS1, use a power adaptor capable of 9-30 Vdc output and 400mA. If the 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 Perle device.
2. Before supplying power, check the polarity of the adaptor leads. The grounded lead should connect to pin marked –.
3. The hot lead should be connected to the pin marked **+**.

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

Ethernet

1. Plug one end of the Ethernet cable to the RJ45 jack on the Perle 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 Perle device does not have DHCP turned on as factory default. Configure the Perle 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 Perle device. Connect the other end of the serial cable to the Adaptive 4000 series.
NOTE: Keep the Console/Serial switch(s) present on the device in OFF position.

Installing Adaptive LED Display

Prerequisites

Before proceeding, make sure to have the following items available:

- Adaptive 4000 series LED display
- RS-232 Communication cable (25-foot, manufacturer P/N 1088-8625)
- RJ12 female to sub-D female, manufacturer P/N 1088-9108
- AC power cable (bundled with LED Display)
- Cat5e Ethernet cable

Optional:

- Modular network jack – to network multiple signs together
- J12 cabling – to network multiple signs together

Mechanical Installation

- For instructions on the mechanical installation, see the *Alpha Series Sign Installation* section that was included by the manufacturer with the Adaptive 4000 series.

Electrical Installation

The electrical installation for Adaptive 4000 series LED display can be done using two interfaces:

- RS-232
- RS-485

Before starting the installation, see the following image for the Adaptive RJ12 Pin-Out structure:

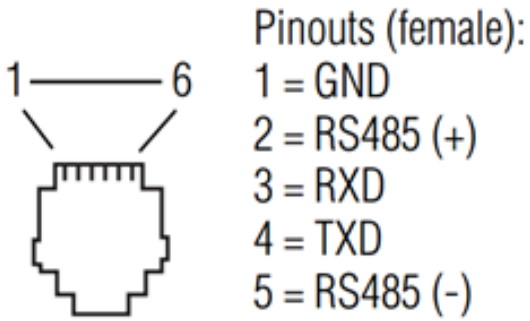


Fig. 1: Adaptive RJ12 Pin-Out Structure

RS-232 Interface

RS-232 interface requires the following wires:

- GND for ground
- TxD and RxD (data lines)

RS-232 wiring provides the easiest form of connectivity with the Adaptive 4000 series. By default, Adaptive comes with an RJ12 to DB9 serial cable wired in a RS-232 configuration.

NOTE:
RS-232 wiring does not offer multi-drop. Therefore, you cannot connect multiple Adaptive LED displays together. Connect only one Adaptive LED display to each Perle device.
At 9600 baud rate, the maximum length of the serial cable from the Adaptive LED display to the Perle device should be 250 feet.

For detailed instructions on installing RS-232 interface, see RS-232 Interface.

RS-485 Interface

RS-485 interface requires the following wires:

- RS-485+ and RS-485- for data.

NOTE: GND is not required for RS-485, but connection to the shield wire or your serial cable is recommended.

RS-485 offers two advantages over RS-232 wiring:

- Multiple Adaptive signs can be connected together and can communicate to a single Perle device as RS-485 offers multi-drop.
- RS-485 offers a longer cable length between the Perle device and the farthest sign.
  NOTE: The farthest sign is determined by the longest communications path back to the Perle device. This distance can include drop nodes or physical length cable.

The following figure demonstrates how multiple Adaptive signs are strung together and connected to a single Perle device.

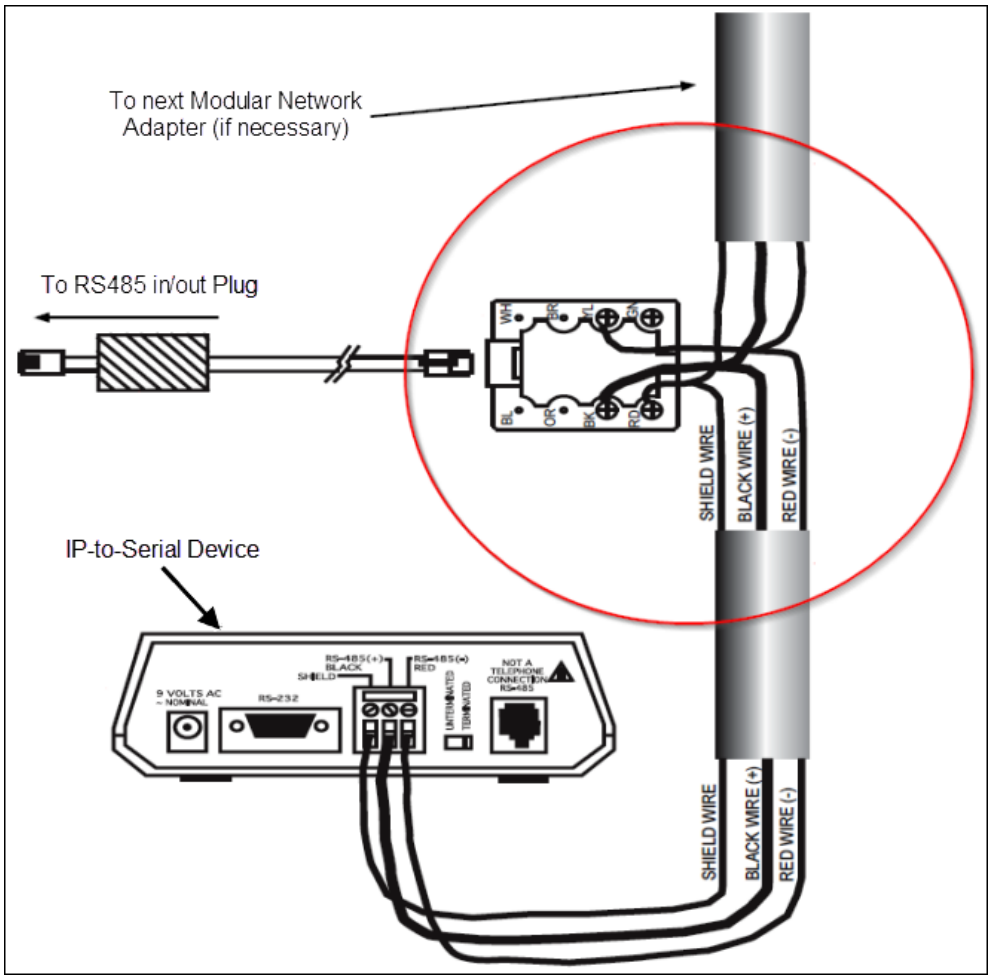


Fig. 2: Multiple Signs

For detailed instructions on installing RS-485 interface, see RS-485 Interface.

RS-232 Interface

1. Mount the LED display to a flat surface using the mounting brackets included within a LED display.
2. Plug the **RJ12** connector of the serial cable to the port marked **RS232** on the LED display.
3. Connect the **DB9** side of the serial cable to the **DB9** connector on the **Perle SDS1**.

4. Connect the power adapter to the port marked **DC IN** on the LED display.
5. Plug the adapter into an AC outlet.

⇨ If the LED display is factory default, demo text and graphics appear on the LED display.

RS-485 Interface

1. Connect the **DB9** female end of the serial cable to the **DB9** male end of the Perle SDS1 device.
2. With the other end of the serial cable cut or open, determine which wires correspond to pins **3, 5, 7** and **9** and shield on the **DB9** connector.
   NOTE: Use an ohmmeter to verify that the wires match the correct pins.
3. Using the appropriate pinout, connect **RS485+**, **RS485-**, **GND**, and **Shield** wires to the modular jack as shown in the image below:

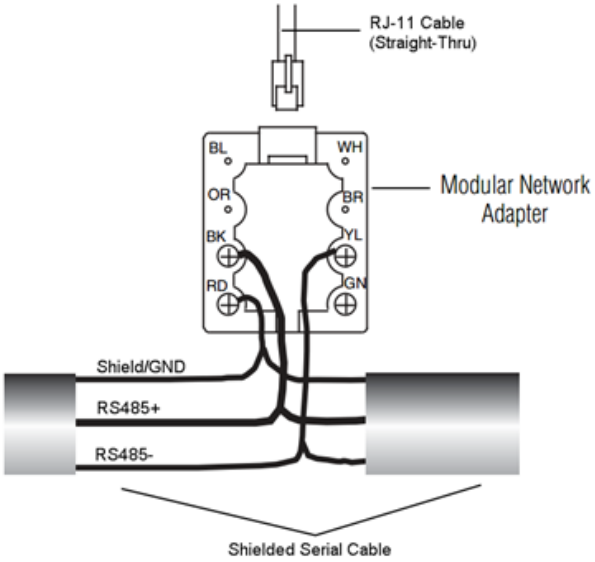
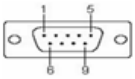


Fig. 3: RS-485 Shield Wires

4. Plug one end of the **RJ12** straight-through cable into the module jack.
5. Connect the other end to the port on the Adaptive sign marked **RS-485 IN** or **RS-232 IN**.
   NOTE: To connect to another sign, follow the demonstration of how multiple Adaptive LED displays are strung together and connected to a single Perle device in the Electrical Installation section.
6. Alternatively, you can plug one end of a straight-through **RJ12** cable into the port marked **RS-485 OUT** or **RS-485 IN** on an already connected sign into the port marked **RS-485 IN** or **RS-232 IN** on the sign to be connected.

For more details about wiring the Perle device, see the Perle Device Installation section.

Depending on the Perle device model, there are two RS-485 pinouts. The following image is the pinout for **I/O** versions of the Perle device:

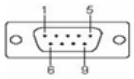


The following table provides pinout information:

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-	RS485+
4 (out)	DTR			
5	GND	GND	GND	GND/ Shield
6 (in)	DSR	RxD-		
7	RTS	TxD+	TxD+/RxD+	RS485+
8 (in)	CTS			
9				

Fig. 4: I/O Pinout

The following image is the pinout for the **Serial Only** versions of the Perle device:



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+	RS485+
4 (out)	DTR			
5	GND	GND	GND	GND/ Shield
6 (in)	DSR	RxD-		
7	RTS			
8 (in)	CTS			
9		TxD-	TxD-/RxD-	RS485-

Fig. 5: Serial Only Pinout

Verifying the Installation of Adaptive LED Display

After correct installation and wiring, the Adaptive 4000 series LED display, on boot up, displays information such as baud rate, sign address, and a welcome message.

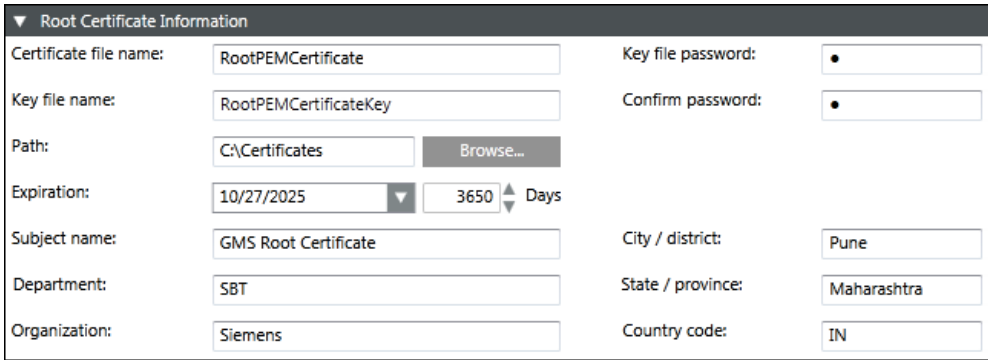
If there is no display, verify power is present.

Certificate Creation from System Management Console

To establish a secure communication, certificates must be configured.

The recommended workflow for working with the **Certificates** in System Management Console (SMC) is to create a Root Certificate Windows store based (.pem).

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



3. In the **Root Certificate Information** expander, enter the following information:
   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. After the root certificate has been successfully created,
- the new root certificate (.pem file) and the root key file are created at the specified location.

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.
- To create a host certificate (.pem file), the user must have a root certificate (.pem file) and root key (.pem) file along with its password. Multiple host certificates can be created using one root certificate (.pem file).
- The user can browse and use this (.pem) root certificate for securing Client/ Server communication, when the project properties are modified.

Software Configuration

Communicating with the Perle device requires the following two main configuration steps.

1. Configure the internal settings of the Perle device. To do this, install DeviceManager on a computer connected to the same network as the Perle device to be configured.
2. Configure the driver on the computer that will be communicating with the Perle device over the network. There are several methods used to communicate with the Perle device. One of which is TruePort Driver.

To enable SSL security between the Perle Device and the server, the user will either create a SSL certificate using System Management Console (SMC) or obtain SSL certificates from the site's IT department. The following three certificates are required:

1. Certificate Authority (CA) certificate - used on the Perle device
2. Server certificate - used on both the Perle device and Trueport
3. Server certificate key - used on the Perle device

All certificates should be in X.509 format with a Privacy Enhanced Email (PEM) extension. Both the server certificate and key should be a single file.

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.

Device Configuration

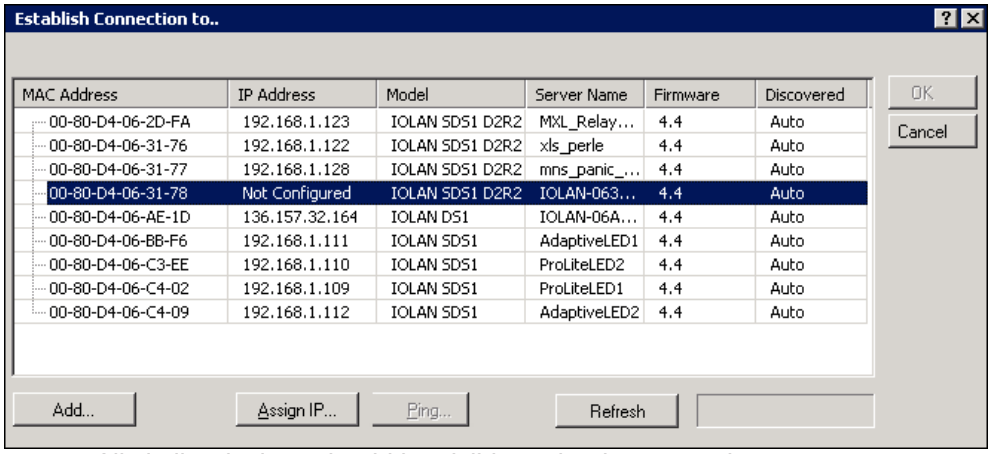
▷ Ensure that the DeviceManager is installed on a computer located under the same network as the Perle device to configure.

▷ Ensure that the following certificates are created using 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
See 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 the cat command in the command prompt. For example, **cat RootCertificateKey.pem RootCertificate.pem > RootCombineCert.pem**.

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

1. Start **DeviceManager**.

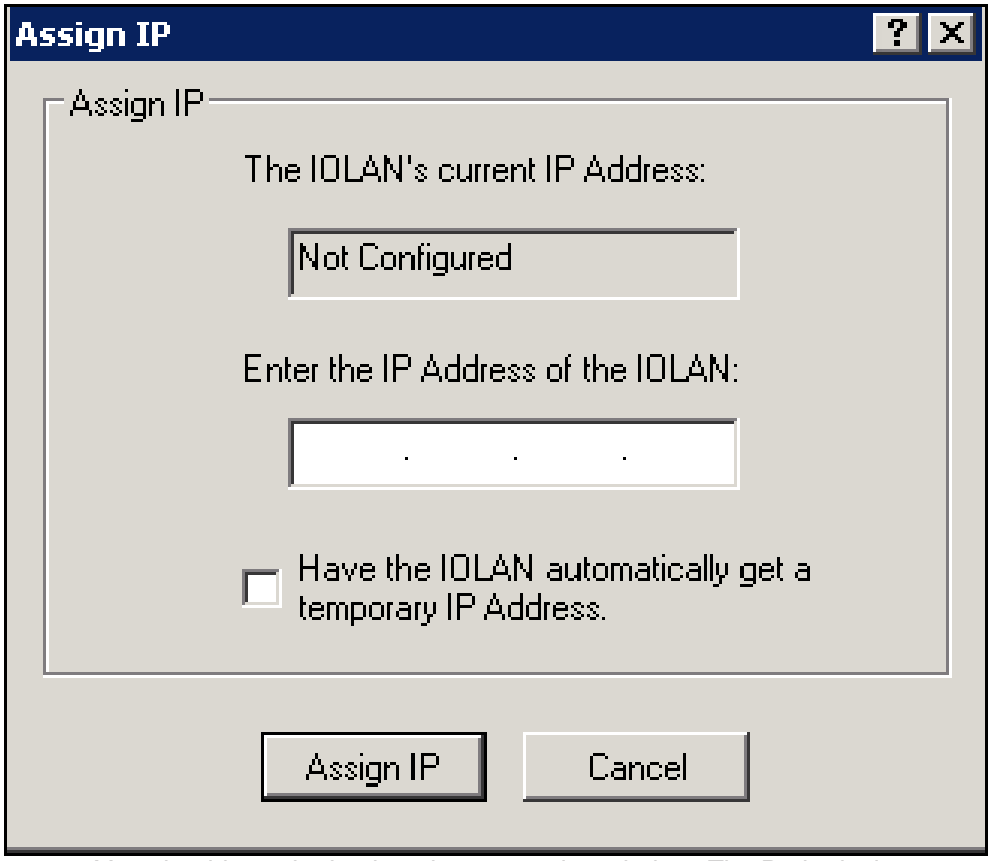


➪ All similar devices should be visible under that network.

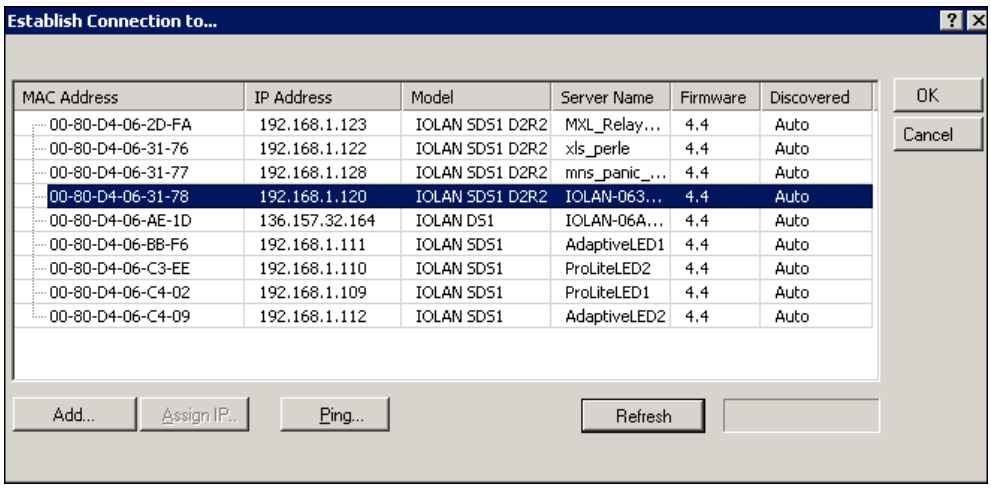
2. Select the Perle device you want to configure and click **Assign IP**.

   ⇨ The **Assign IP** dialog box displays.
   NOTE 1: If you cannot see the device in the window, verify that the device has power and is correctly 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 or green.
   NOTE 2: If issues persist, unplug the Ethernet cable and power. Wait for five 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 issues, you can manually reset the device by holding down the small Reset button located on the device for ten seconds or until the Power LED is solid amber and then release. Wait 90 seconds for 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 to have the DHCP assign one automatically. Then click **Assign IP**.



   ⇨ You should now be back to the connection window. The Perle device should be assigned an IP address.



4. Select the Perle device again, and click **OK** to log into the device for configuring.
5. In the **Login** window, enter the device password. The factory default password is **superuser**.

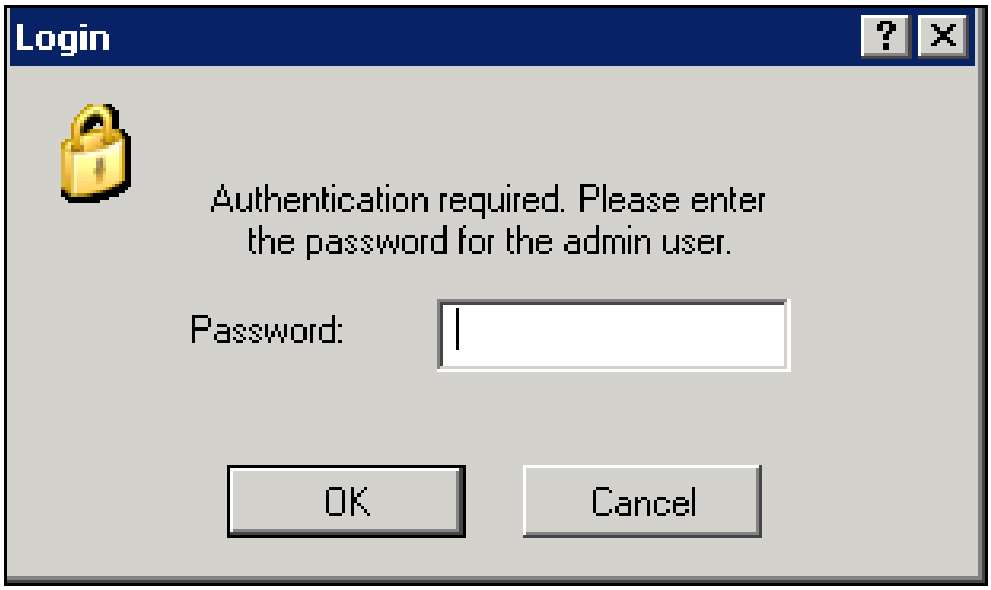
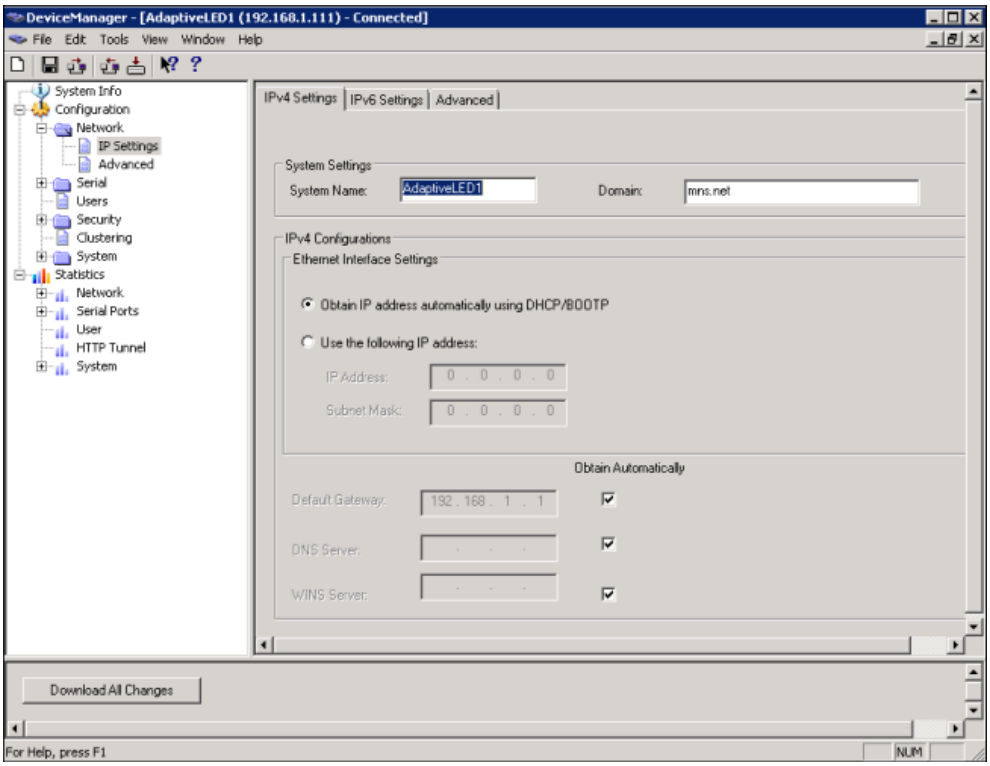


Fig. 6: Login Window

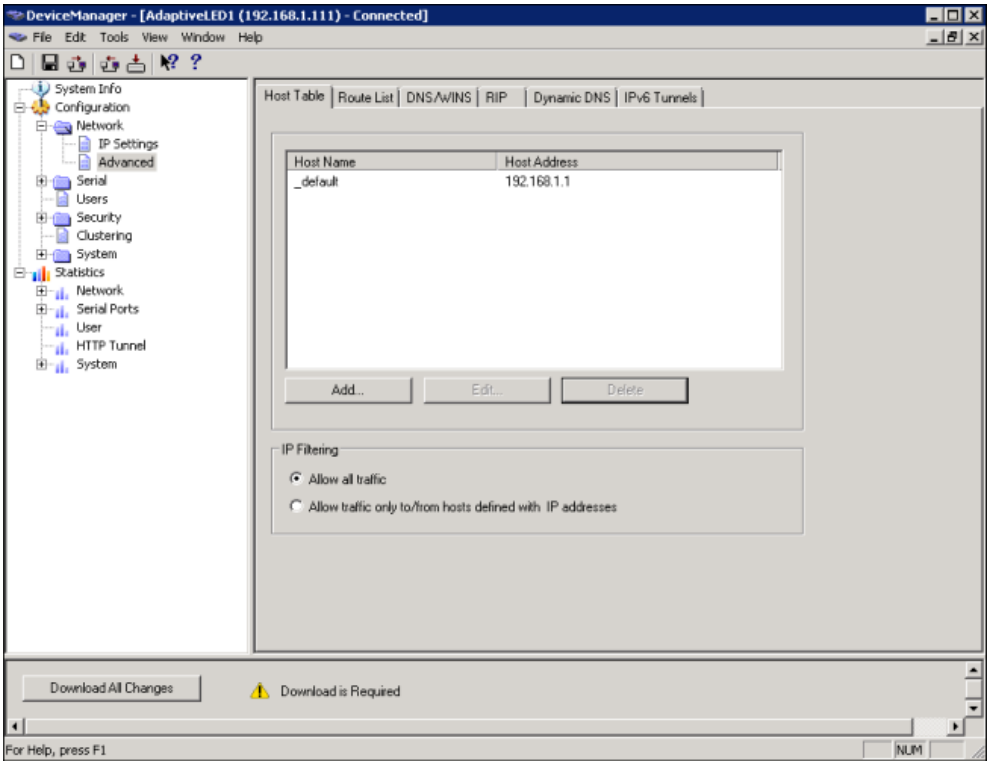
Network Setup

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

1. In the **DeviceManager** window, click **Network folder** and then **IP Settings**.
   NOTE: In this area, the user can configure additional parameters for the network settings, such as **static IP address or DHCP**.



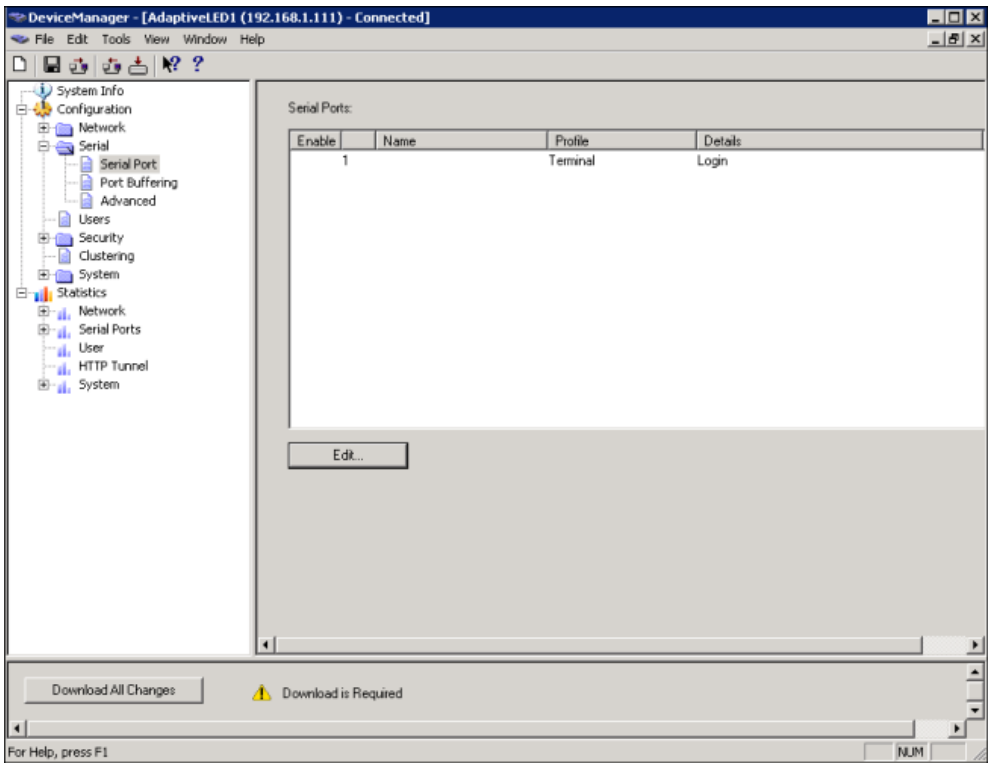
2. Under the **System Name** field, enter a distinguishable name to help identify the device from other similar devices.
   NOTE 1: The System Name is also used by the device to create a fully qualified domain name.
   NOTE 2: By default, the device is always **IOLAN** followed by the last three bytes of the device MAC address.
3. Under the **Domain** field, enter the domain name used on the client's network (for example, **AmericaUniversity.net**).
   NOTE: The device can receive the domain automatically from DHCP. However, DHCP must be configured to set domain as a parameter.
4. Select **Network > IP Settings > Advanced** tab.
5. Select the **Register Address in DNS** check box.
6. Click the **Advanced** tab on the left-hand side.



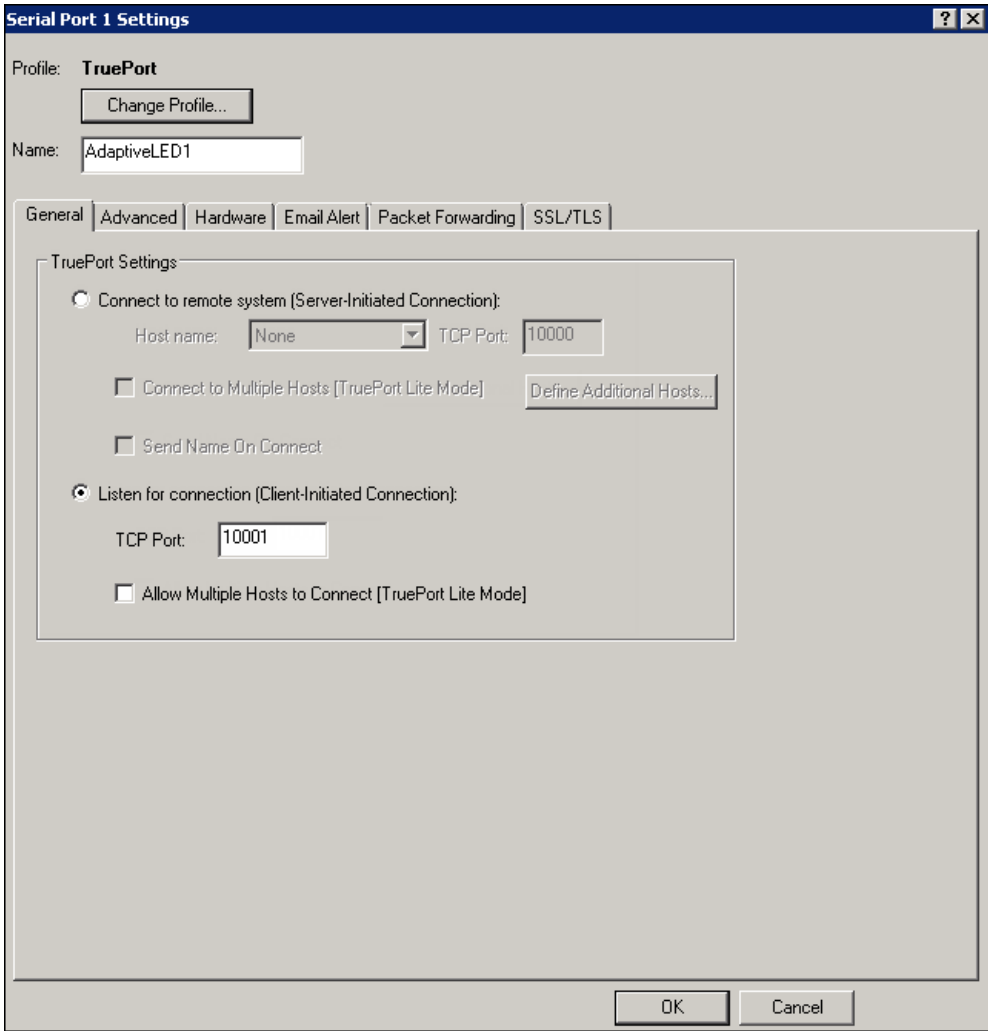
7. Select the **Host Table** tab.
8. Click **Add** to add an NTP host.
9. Enter a descriptive name for the NTP server (for example, **mnsNTP**).
10. Enter the IP address or the fully qualified domain name of an available NTP server.
    NOTE: An available NTP server is required to enable SSL on the device.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

Serial Settings

1. In the **Device Manager** window, click the **Serial** folder on the right and then **Serial Port**.
   NOTE: Configure the number of serial ports and the profile the device will use. Only one serial port per device is required for serial communication.
2. Select the default serial port and click **Edit**.

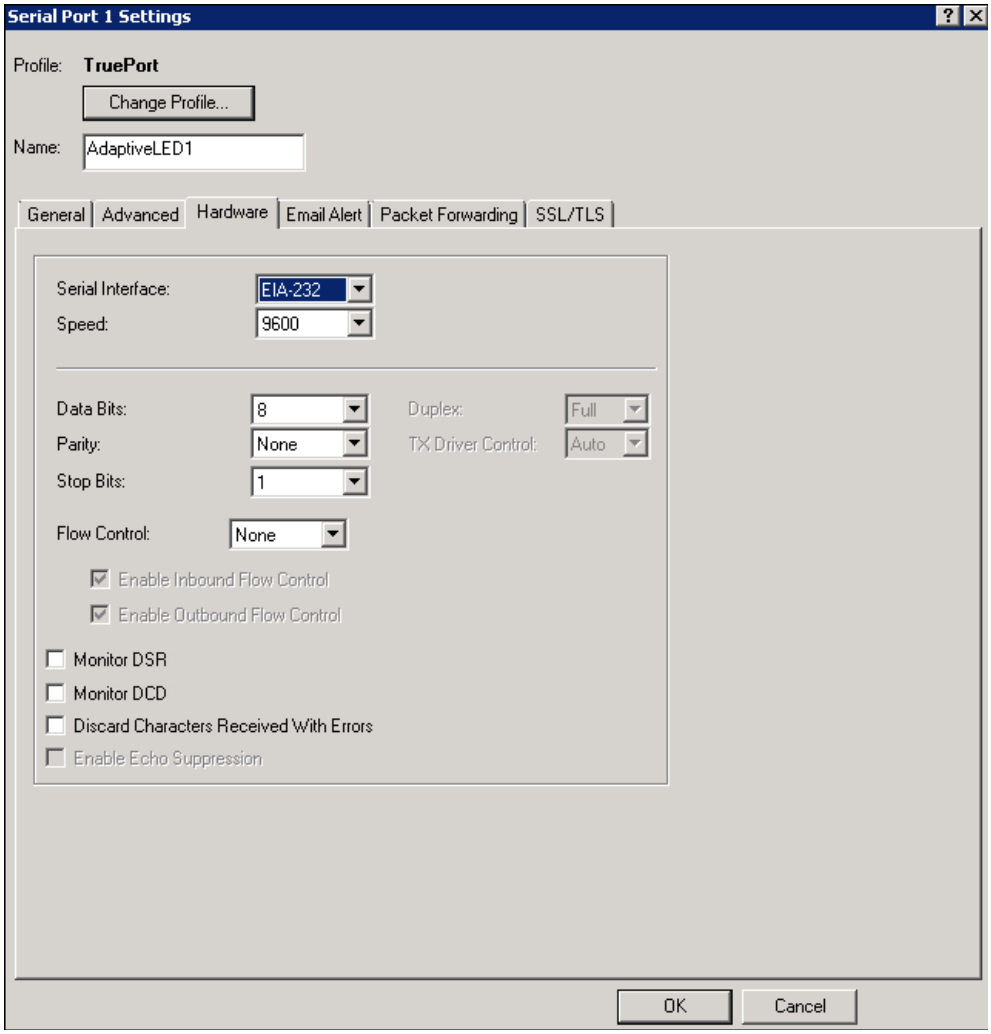


3. In the **Serial Port 1 Settings** window, click **Change Profile**. Select the **TruePort** profile and click **OK**.



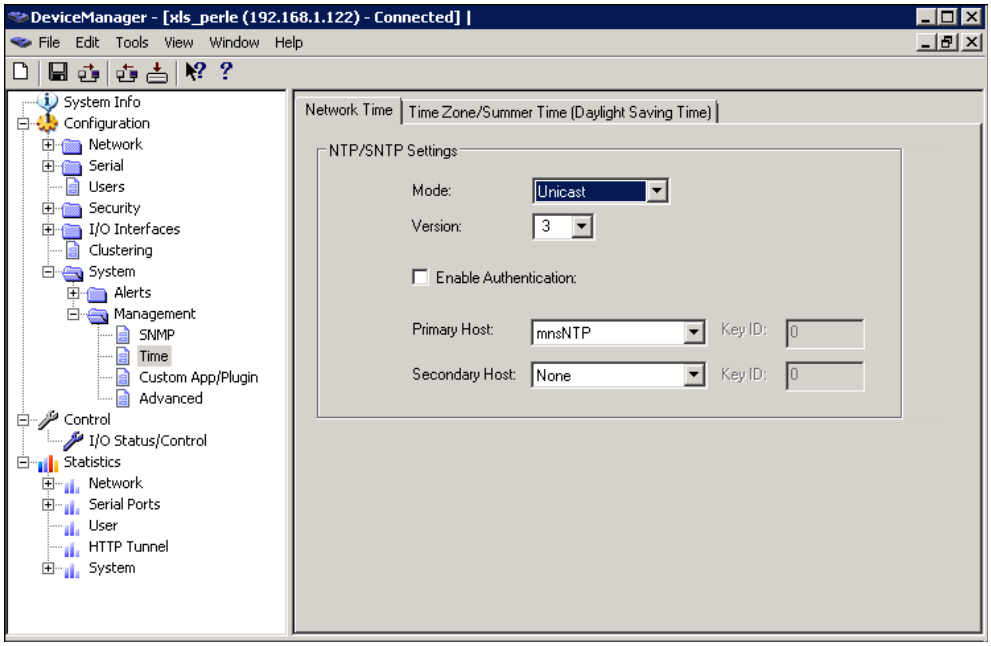
⇨ The **Serial Port 1 Settings** window will change to reflect the new profile.

4. Select the **General** tab.
5. Select **Listen for connection (Client-Initiated Connection)**.
   ⇨ In this mode, the device will wait for the server to establish a connection.
6. Enter the TCP port that should communicate with the device. By default, the TCP port is always **10001**.
   NOTE: Always check to make sure selected port 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 display.
7. Ensure that the **Allow Multiple Hosts to Connect [TruePort Lite Mode]** check box is cleared. Click **OK**.
8. Select the **Hardware** tab.

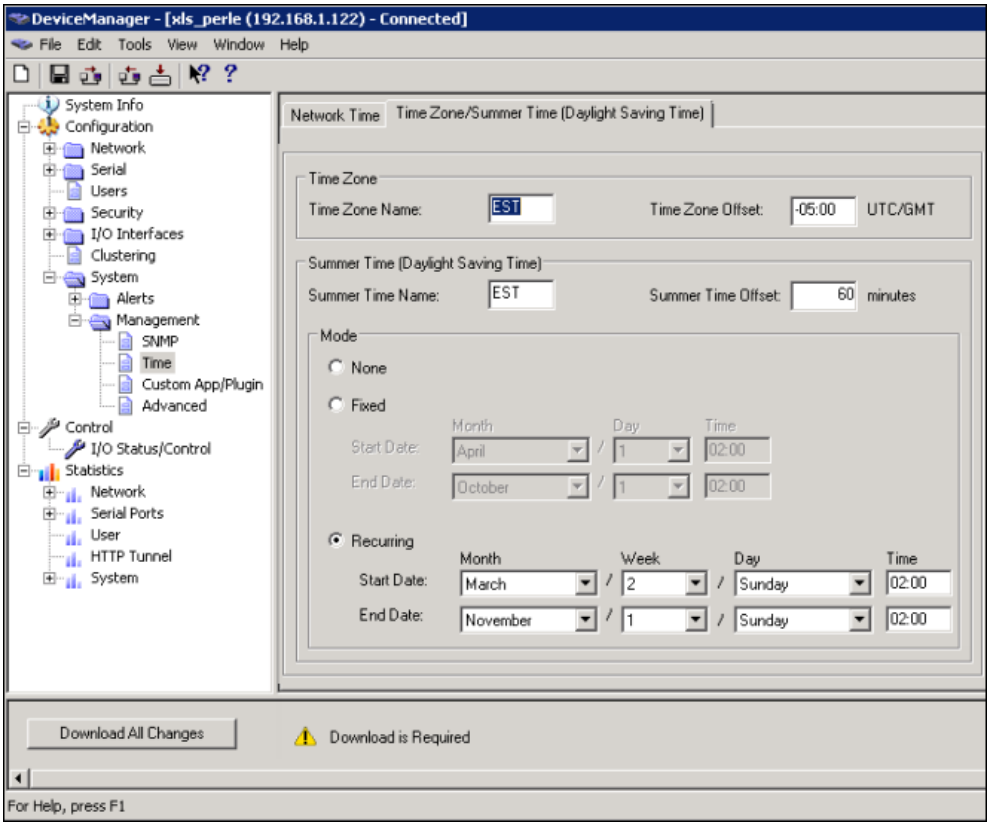


9. Select either **EIA-232** (RS-232) or **EIA-485** (RS-485) in Serial Interface.
10. Set **Speed** to **9600**.
11. Set **Data Bits** to **8**.
12. Set **Parity** to **None**.
13. Set **Stop Bits** to **1**.
14. Set **Flow Control** to **None**.
15. Do not select the **Monitor DSR** check box.
16. Do not select the **Monitor DCD** check box.

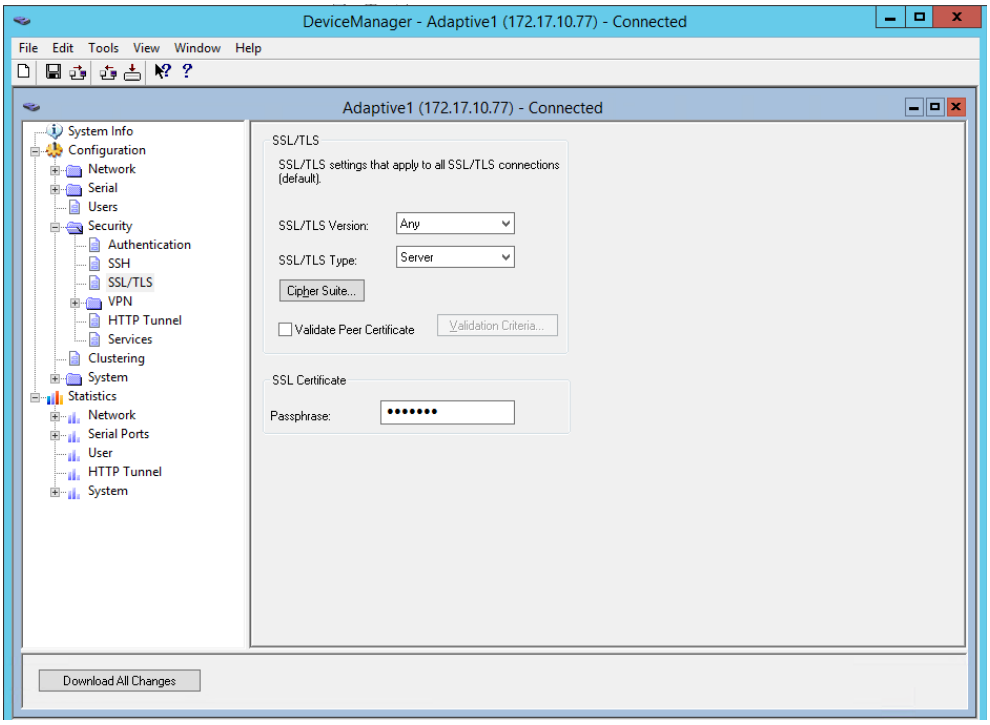
17. Do not select the **Discard Characters Received With Errors** check box.
18. Select the **SSL/TLS** tab.
19. Select the following check boxes:
    - **Enable SSL/TLS**.
    - **Use Global settings (Security > SSL/TLS)**.
20. Click **OK**.
21. Select **Configuration > System > Management >Time**.
22. Select the **Network Time tab**.
23. Do the following parameter settings:
    - **Mode:** Unicast
    - **Version:** 3
    - Leave the **Enable Authentication** check box cleared.
    - **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. If you are unsure, verify with the client's network administrator.



24. Select the **Time Zone/Summer Time (Daylight Saving Time)** tab.
25. Configure the parameters as per the details mentioned in Time Zone/Summer Time (Daylight Saving Time) parameters.



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



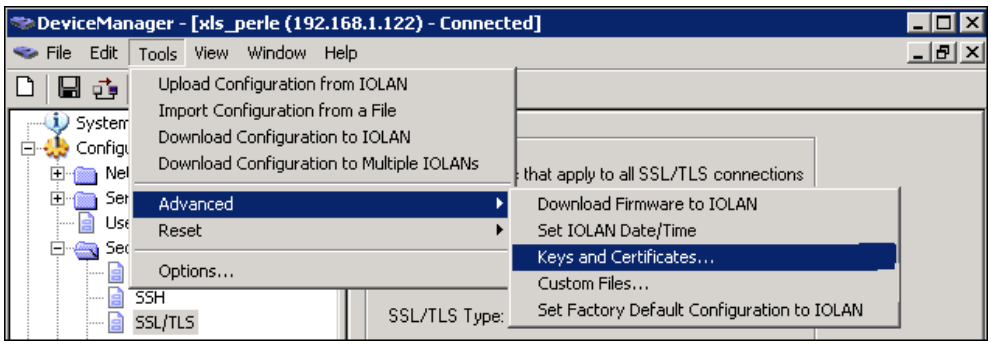
27. Set **SSL/TLS Version** field to **Any**.

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

29. In the **SSL Certificate** dialog box, enter the password of the root certificate (.pem) in the **Passphrase** field.

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

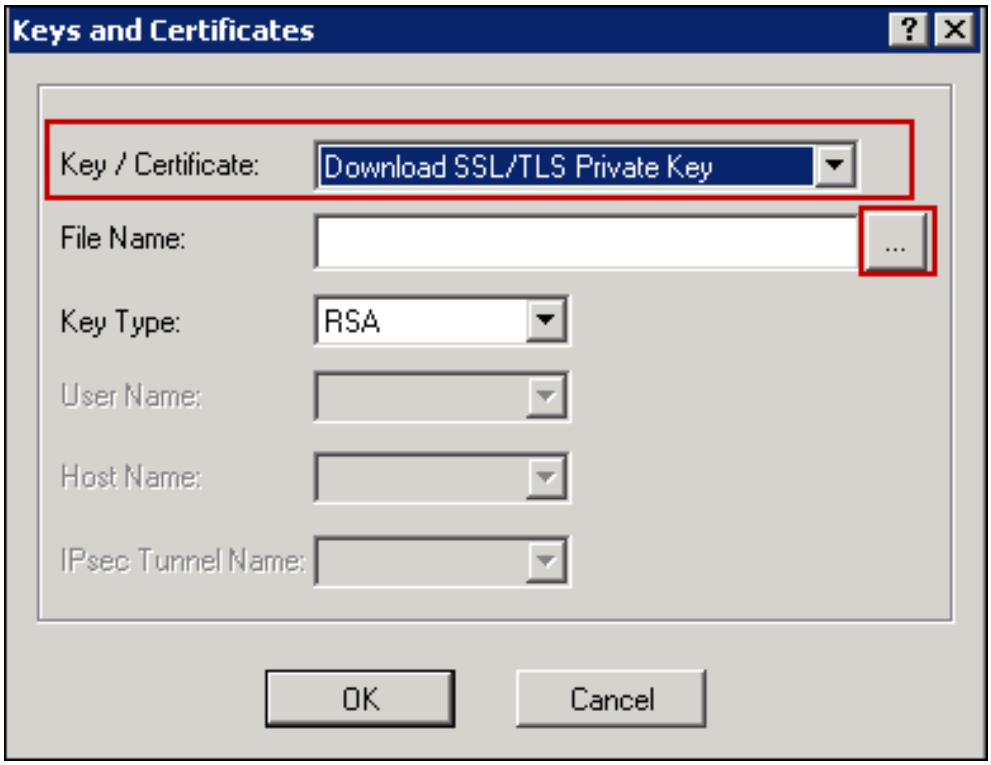
⇨ The **Keys and Certificates** dialog box displays.



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

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

33. Click **OK**.



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

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

36. Click the **Browse** button and upload the combined root certificate (RootCombineCert.pem file). Refer to the Certificate Creation From System Management Console section for more information on combining the root certificate.

37. Click **OK**.

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

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

40. Click the **Browse** button and upload the root certificate (RootCertificate.pem file).

41. Click **OK**.

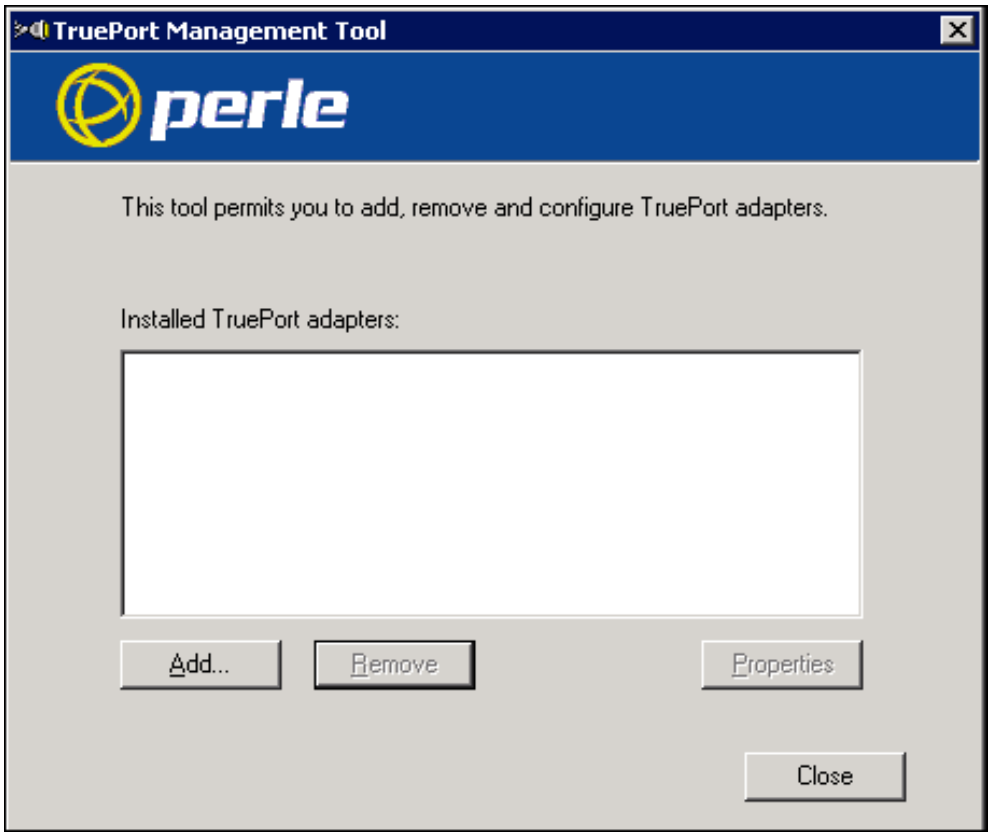
42. Click **Download All Changes** to make the changes to the device.
43. Click **Reboot IOLAN**.
    NOTE: Any time you reboot the device, or power is reconnected, you must wait 90 seconds for the device to reboot and initialize. When the device is ready, the Power LED will be solid green and the Link LED will be solid amber or green.

⇨ The device is now configured.

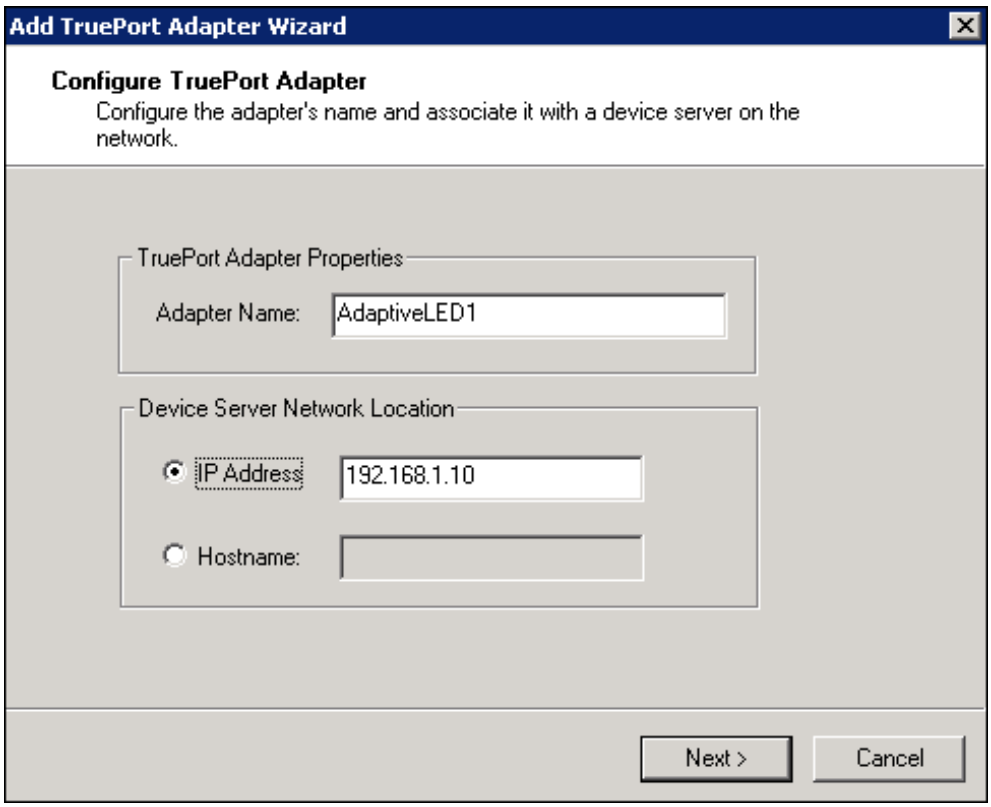
TruePort Driver Configuration

▷ The TruePort driver is the second part of the process to link the device to the system server. TruePort is only used when the Perle 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, the recommendation is that each device has its own and 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.

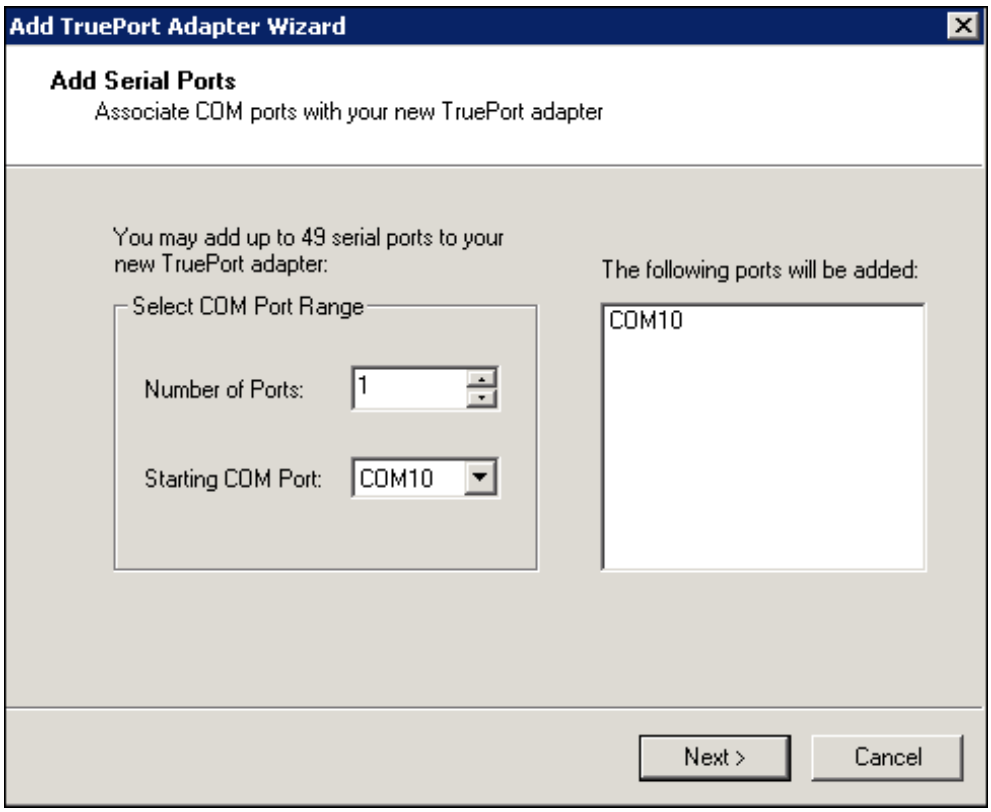
1. Install TruePort on the server. TruePort can be downloaded from Perle's website or installed from the CD included with the device.
2. Start the **TruePort Management Tool**.
3. In the TruePort Management Tool window, Click **Add**.



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 which can easily be tracked back to a particular device.
5. Enter the IP address or the hostname the device is using.

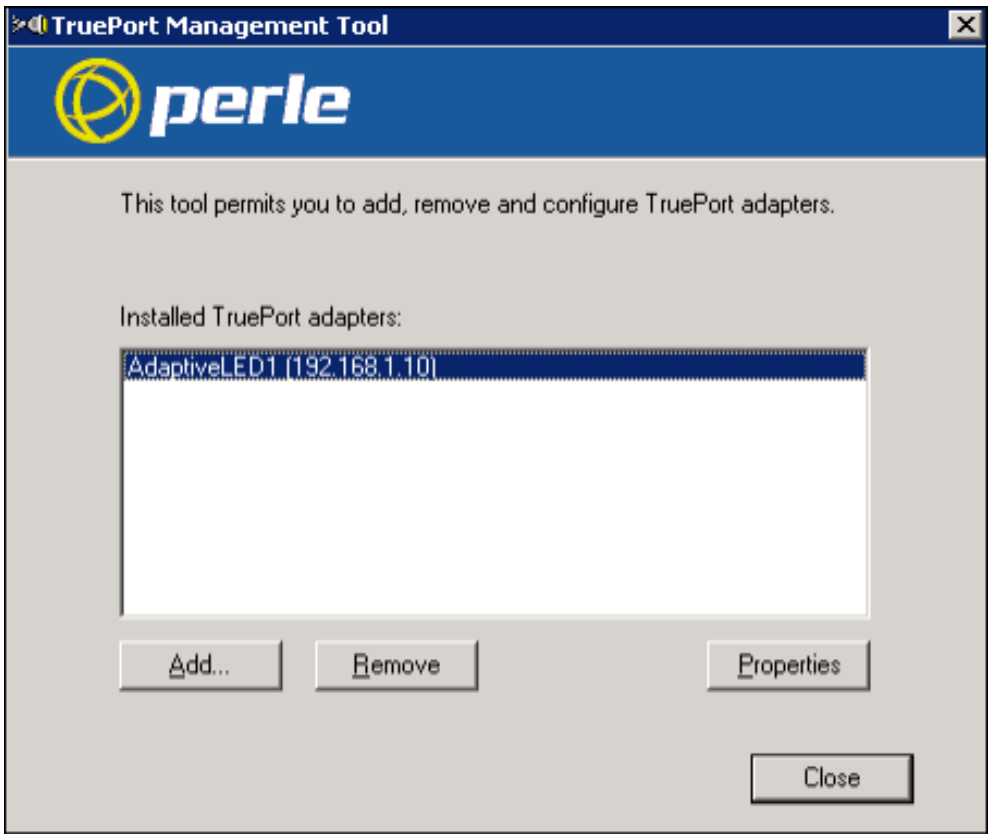


6. Click **Next**.
7. Leave the number of ports set to **1** (for I/O access, set ports to **2**, or add another later). Select the COM port for that particular device. By convention, start at COM100 and increment for each device and service configured. This will help to avoid any conflicts with existing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



⇨ TruePort Adapter in the TruePort Management Tool is visible now.

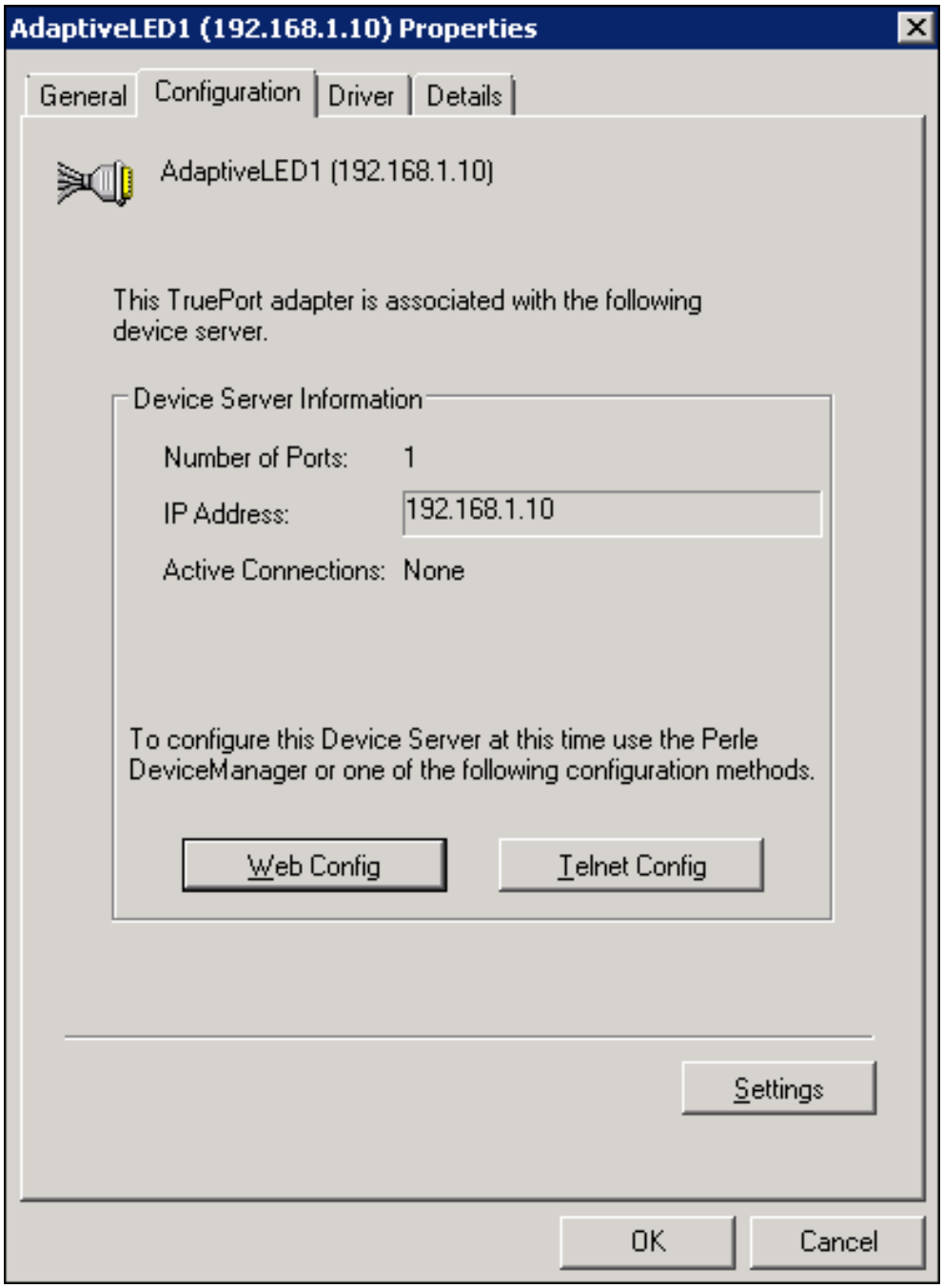
9. To edit the TruePort settings, select the adapter to edit and click **Properties**.



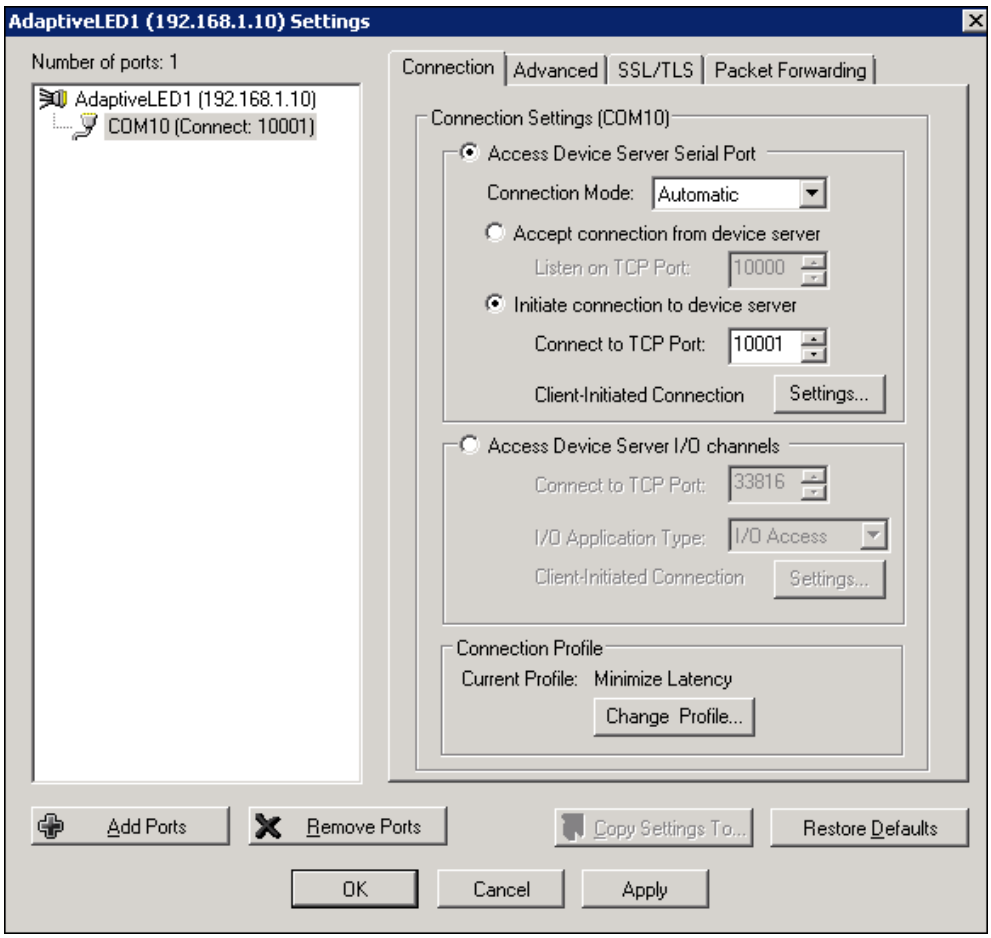
Serial Settings

1. Select the **Properties** window of the device port to be configured.
2. Select the **Configuration** tab.

3. Click **Settings**.



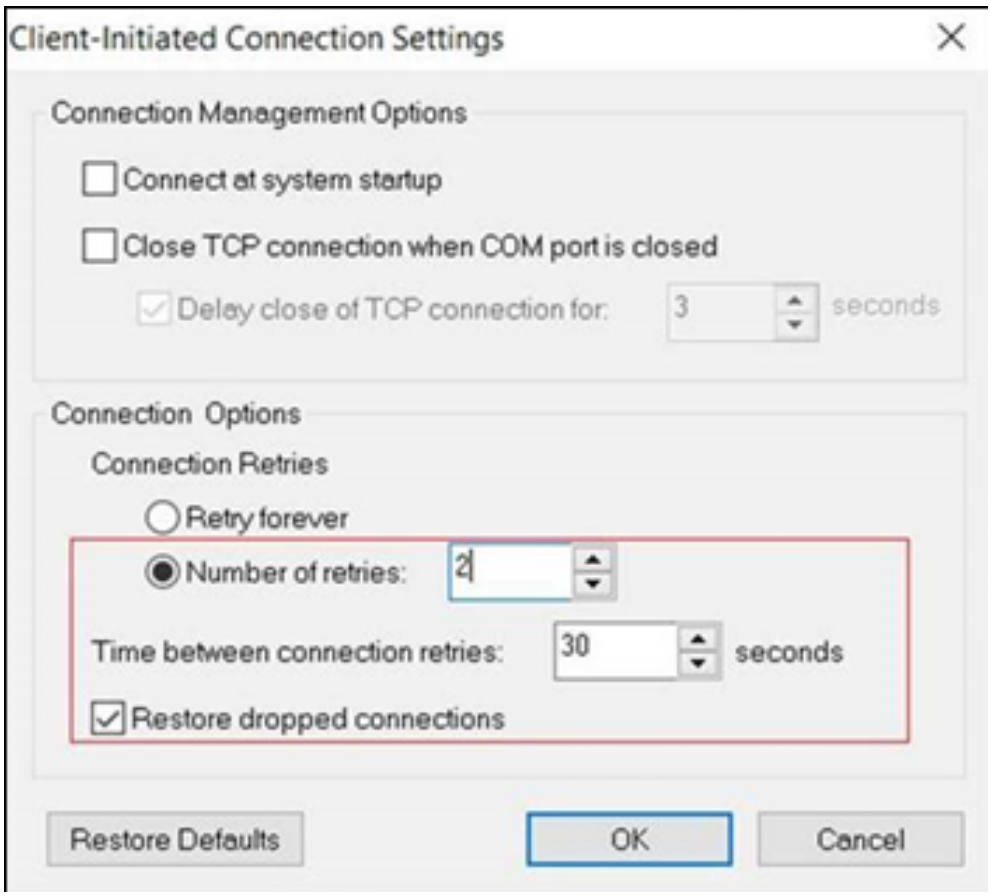
4. Click the COM port on the left-hand side.
   ⇨ The TruePort and COM port settings for this adapter display.
5. Select the **Connection** tab.
6. Click **Initiate connection to device server**.



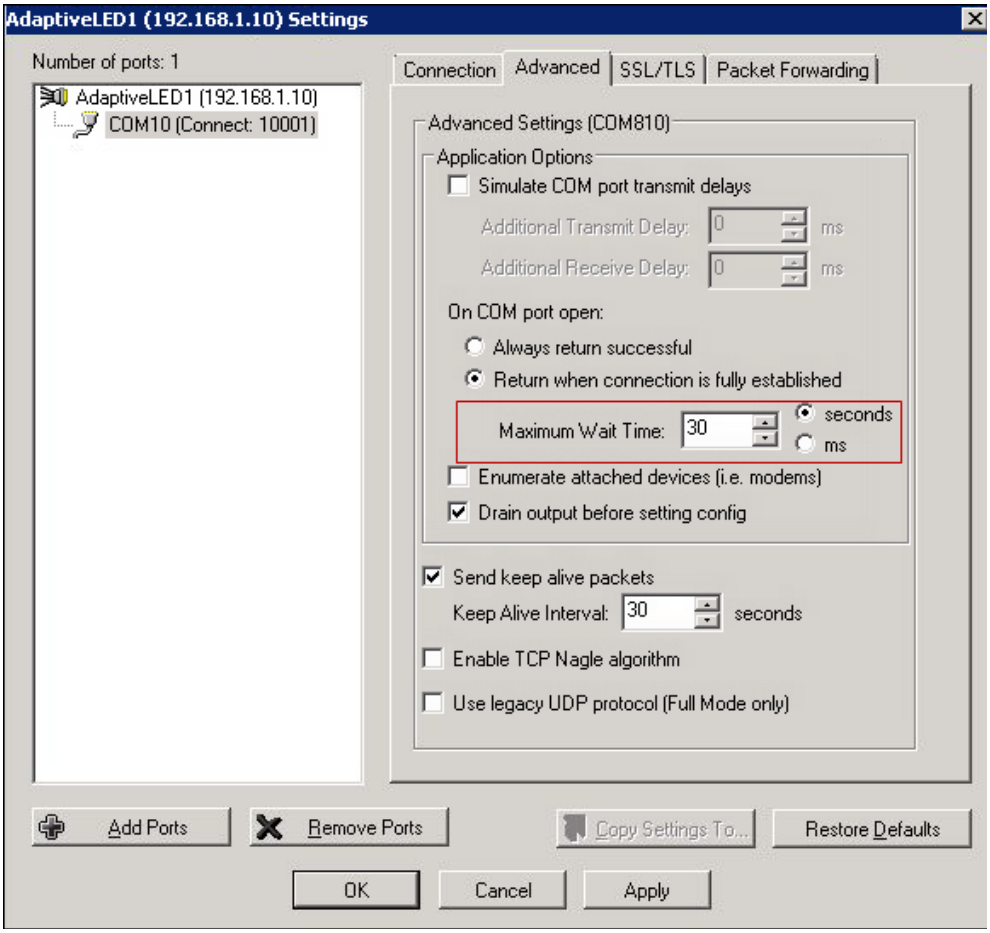
– Under **Connect to TCP Port**, enter the port number that was previously assigned to the device using the device manager.

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

   ⇨ The **Client-Initiated Connection** window displays.

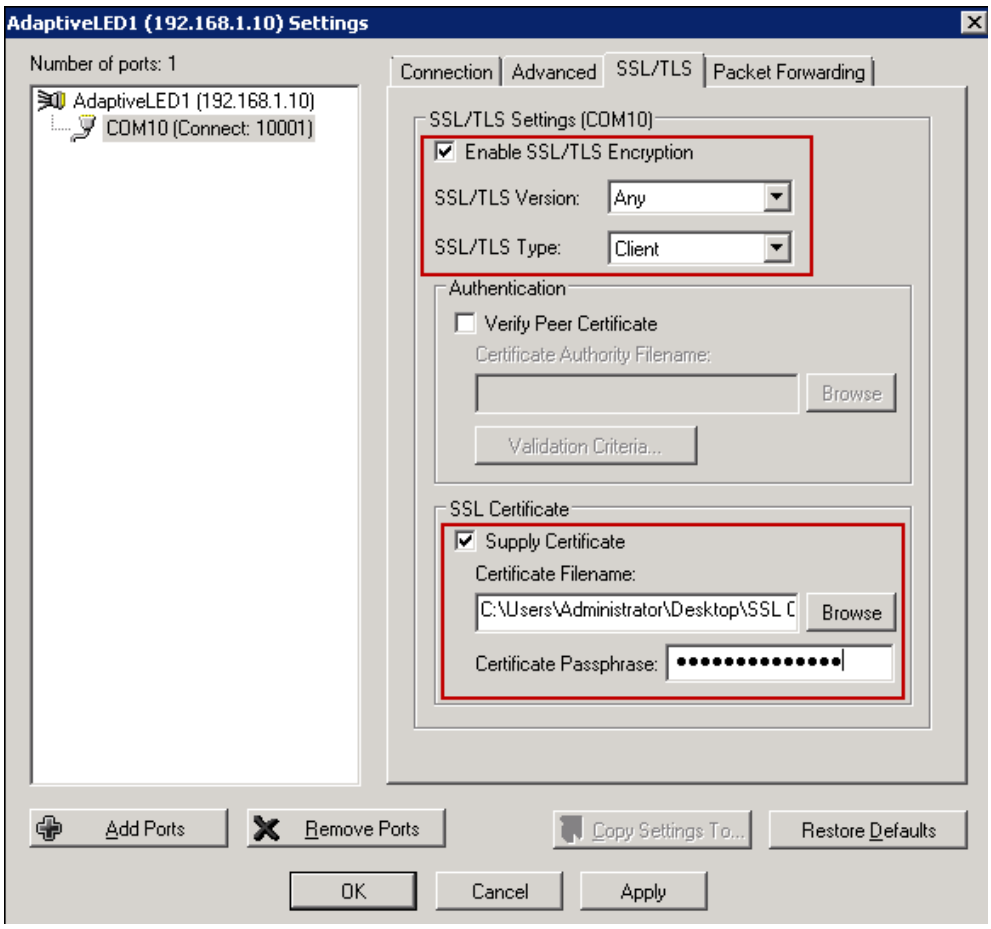


8. Select the **Connect at system startup** check box.
9. For **Connection Retries**, select **Retry forever**.
10. Click **OK**.
11. Select the **Advanced** tab.



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

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



14. Select the **Enable SSL/TLS Encryption** check box.
15. Set the **SSL/TLS Version** field to **Any**.
16. Set the **SSL/TLS Type** field to **Client**.
17. Select the **Supply Certificate** check box.
18. Click the browse button and select the combine Root certificate. Refer to the --- MISSING LINK --- section for more information on combining a Root certificate.
19. Enter the password in the **Certificate Passphrase** field.
20. Click **Apply** and then **OK**.
21. Restart the **Perle TruePort Service** from the SMC.

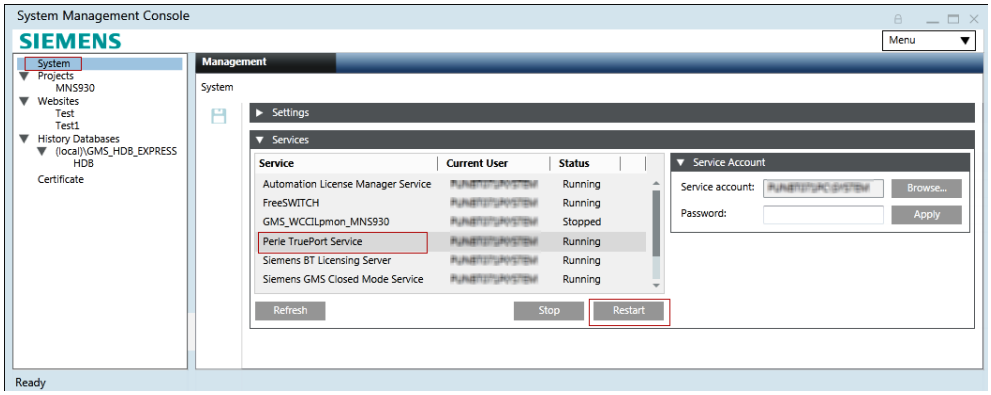


Fig. 7: Restarting the Perle TruePort Service

Device Verification

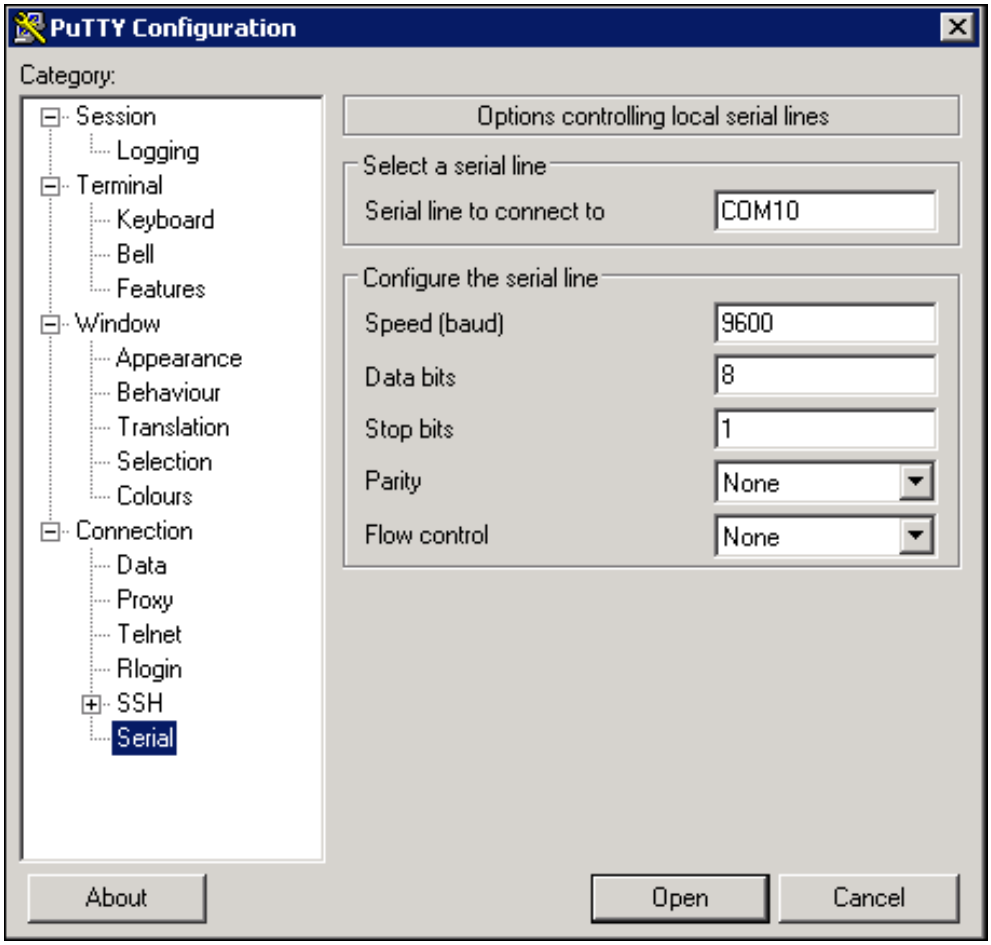
To test whether the Perle SDS1 is configured correctly, open a PuTTY session from the server using the serial COM port that was previously created from the Adaptive ® 4000 series. If you can open the COM port, then the TruePort driver is working properly.

PuTTY can be downloaded from the following link:

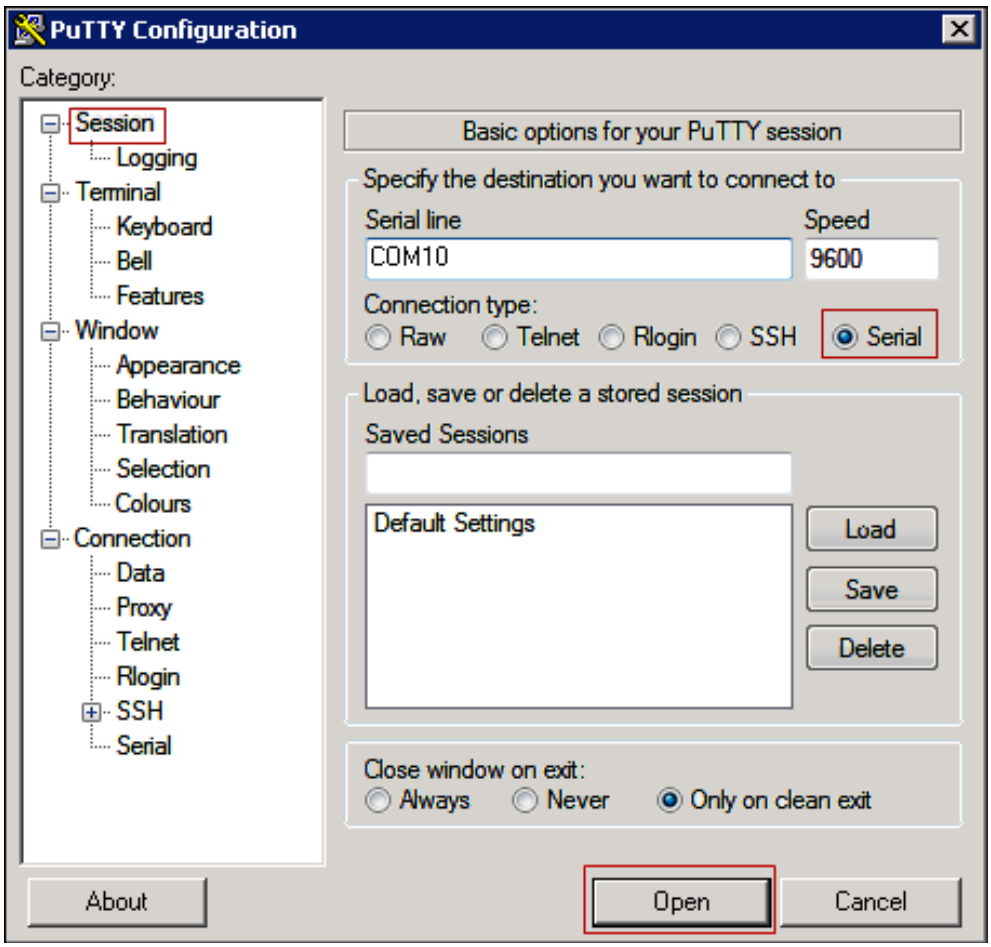
http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe

The steps for testing Adaptive communication are as follows:

1. Open PuTTY and select **Connection > Serial**.
2. For 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 Adaptive 4000 series.
   - **Baud Rate:** 9600
   - **Data Bits:** 8
   - **Stop Bits:** 1
   - **Parity:** None
   - **Flow Control:** None



4. Click **Session** and select **Serial**.
5. Click **Open** to establish a serial session.
   NOTE: If PuTTY denies a connection, check your TruePort settings.



Configuring Adaptive LED Display

Prerequisites

Before proceeding, make sure to have the following items available:

- Adaptive 4000 series LED display
- RJ11 to DB9 Serial cable (bundled with LED sign)

Device Configuration

Perform the following steps to configure the serial address of the Adaptive sign:

1. Press **PROGRAM** on the remote control shipped with the sign.
2. Press **BACK** until **SET SERIAL ADDRESS** or **SET SERIAL** is displayed.
3. Press **ADV**.
4. Enter a number (For example, 10).
   NOTE 1: A serial address is actually a number from 0 to 255 in hexadecimal (00 to FF). However, in typical use entering a number from 00 to 99 is fine.
   NOTE 2: The default serial address of a sign is set to 00.
5. Press **RUN** twice to set the new serial address and return the sign to normal operation.

⇨ The serial address is set.
NOTE:
After the serial address of the Adaptive 4000 series LED display is set, further configuration is required on the Perle device.

Adaptive LED Device Troubleshooting

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. If the device does not get connected after the **Check Status Rate** duration, then perform 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.

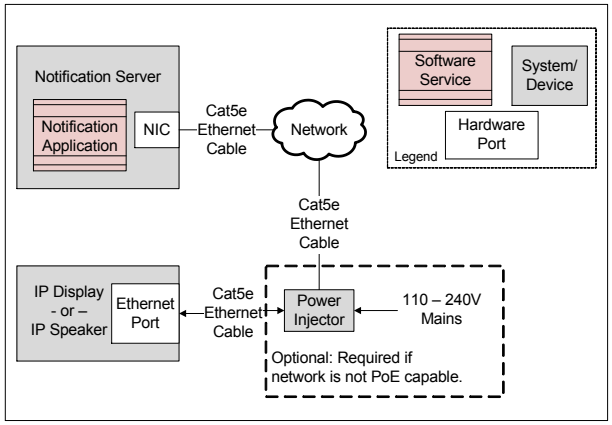
1.2 Advanced Network Devices (AND)

Advanced Network Devices (AND)

This section provides reference and background information for integrating the AND Device. For procedures or workflows, see the *step-by-step* section for Creating and Configuring AND IP Display Device and Creating and Configuring AND IP Speakers.

Device Overview

The IP Displays and IP Speakers communicate with the server through Internet Protocol (IP). The IP Displays and IP Speakers are connected to a network switch through Cat5e Ethernet cable. The IP Displays and IP Speakers are Power over Ethernet (PoE) devices that receive power from the Ethernet port on the device. The Cat5e Ethernet cable must be connected to a Power over Ethernet (PoE) capable network or a separate power injector is required to power the device.



can integrate with devices from two Advanced Network Devices (AND) product families: IP Display products and IP Speaker products.

The system can integrate with the following AND products that conform to the UL-60950 standard.

IP Displays

- IPSWD (without flashers)
- IPSWD-RWB
- IPCSS-RWB
- IPCSL-RWB

- IPCDS-RWB
- IPSIGNL-RWB

IP Speakers

- IPSWS-SM
- IPSWS-FM
- IPSCM-RM
- IPSWS-SM-O

The integration between , the AND IP Displays, and the AND IP Speakers enable to send text and/or audio messages. These messages will go to the AND IP Displays and the AND IP Speakers. The textual messages are delivered to the AND IP Displays. The AND IP Speaker products do not have textual message capabilities.

In this version of , the integration between , the AND IP Displays and the AND IP Speakers does not support the following AND device features:

- Microphone for bidirectional communication or listening in
- General Purpose I/O (GPIO) for sensing conditions or controlling remote activation
- Flasher Activation. (**AND IP Displays** now support Flasher activation)

NOTE: The IP ClockWise software by Advanced Network Devices is not required for integrating with devices from the Advanced Network Devices product families.

General Overview of Advanced Network Devices

can integrate with devices from two Advanced Network Devices (AND) product families: IP Display products and IP Speaker products.

The system can integrate with the following AND products that conform to the UL-60950 standard.

IP Displays

- IPSWD (without flashers)
- IPSWD-RWB
- IPCSS-RWB
- IPCSL-RWB
- IPCDS-RWB
- IPSIGNL-RWB

IP Speakers

- IPSWS-SM
- IPSWS-FM
- IPSCM-RM
- IPSWS-SM-O

The integration between , the AND IP Displays, and the AND IP Speakers enable to send text and/or audio messages. These messages will go to the AND IP Displays and the AND IP Speakers. The textual messages are delivered to the AND IP Displays. The AND IP Speaker products do not have textual message capabilities.

In this version of , the integration between , the AND IP Displays and the AND IP Speakers does not support the following AND device features:

- Microphone for bidirectional communication or listening in
- General Purpose I/O (GPIO) for sensing conditions or controlling remote activation
- Flasher Activation. (**AND IP Displays** now support Flasher activation)

NOTE:
The IP ClockWise software by Advanced Network Devices is not required for integrating with devices from the Advanced Network Devices product families.

Installation and Configuration

Installing AND 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:

- Advanced Network Device (AND) IP Display or IP Speaker
- Cat5e Ethernet Cable

The optional prerequisite includes:

- Ethernet Power Injector

AND Mechanical Installation

1. Remove the back frame by removing the four Torx screws on the side of the device.
2. Mount the back frame to a flat surface by placing screws through the eight mounting holes located on the frame.

⇨ The mechanical installation of the device is now complete.

AND Electrical Installation

1. Connect the Ethernet cable to the Ethernet port on the back of the device.
2. Connect the other end to the power injector or a PoE capable switch/hub/router.
   NOTE: The AND IP Displays and IP Speakers are Power over Ethernet (PoE) only devices. They receive all of their power over the Ethernet cable.
3. Verify that the network is PoE ready.
   NOTE: If the network is not PoE ready, a power injector must be purchased and installed.

⇨ The device boot process is started.

AND Installation Verification

On successful connection, the LED sign will display the following in sequence:

- Advanced Network Devices
- Firmware
- MAC
- IP Address
  NOTE 1:
  If nothing is displayed when Ethernet cable is connected, verify that PoE is available.
  NOTE 2:
  If the Dynamic Host Configuration Protocol (DHCP) with a rotating bar is displayed, then the device is unable to obtain an IP address. Check with the local site administrator for the DHCP availability. A DHCP server is required during the first reboot in order for the AND sign to obtain an initial IP address. After an initial IP address is obtained, the sign can be reconfigured with a static IP address.

Configuring and verifying AND Device

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:

- Computer connected to the same subnet as the IP Display or IP Speaker
- Web browser for accessing the IP Display‘s or IP Speaker‘s internal web server

AND Device Configuration

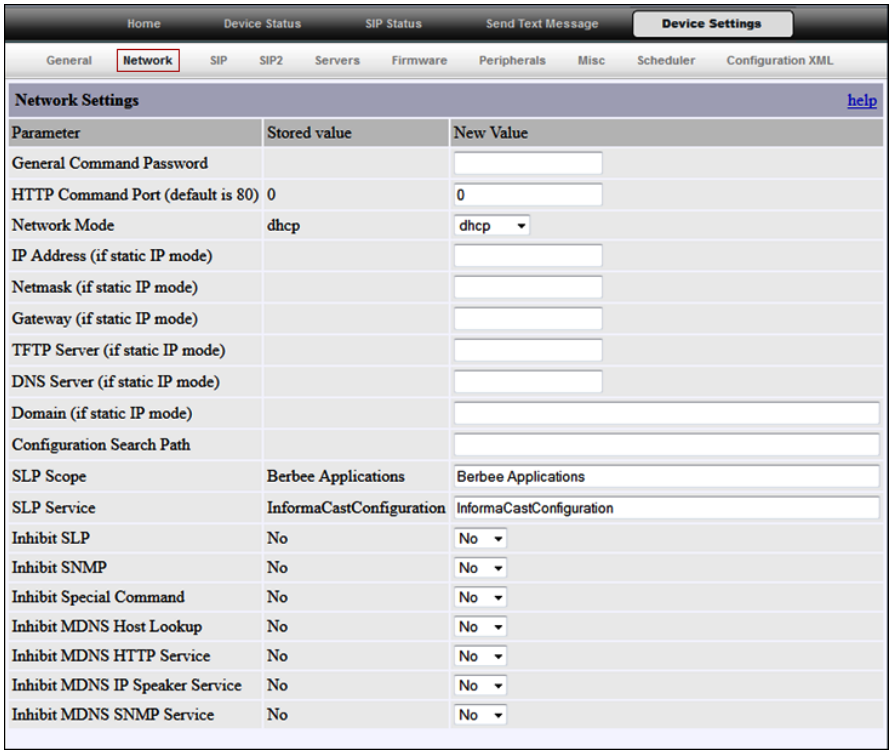
After the completion of the boot up process, the device will request an IP address through DHCP. Upon receiving the IP address, the device will display it before returning to the normal operation.

NOTE:
An IP address is required for the Advanced Network Devices before the device installation process. If the device is unable to receive an IP address, the device will continue to reboot and search again. A DHCP server is required during the first reboot in order for the AND sign to obtain an initial IP address. After an initial IP address is obtained, the sign can be reconfigured with a static IP address.

After receiving the IP address, log on to the device using a web browser on a computer attached to the same subnet as the sign.
URL: http://sign_ip_address

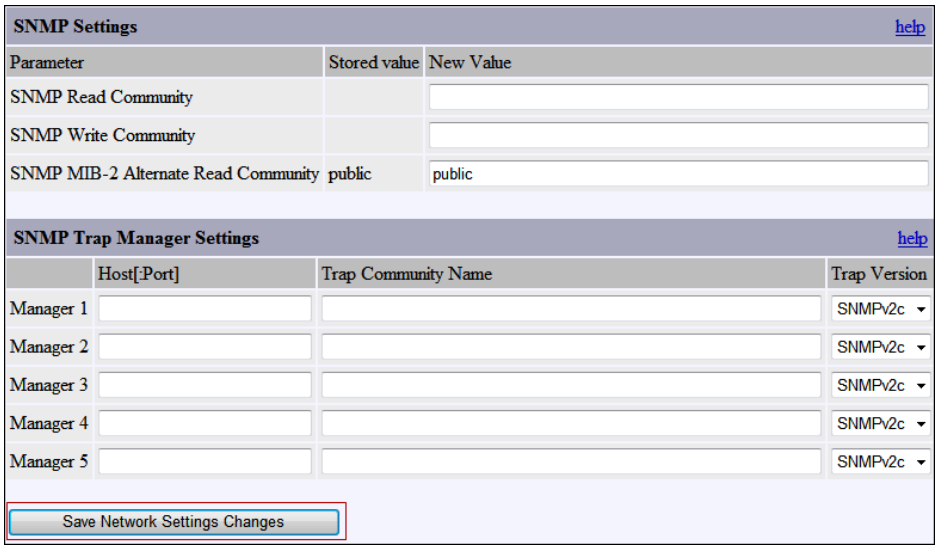
AND Display Configuration

1. Click **Device Settings**.
2. Select **Network**.
   ⇨ The **Network Settings** section displays.

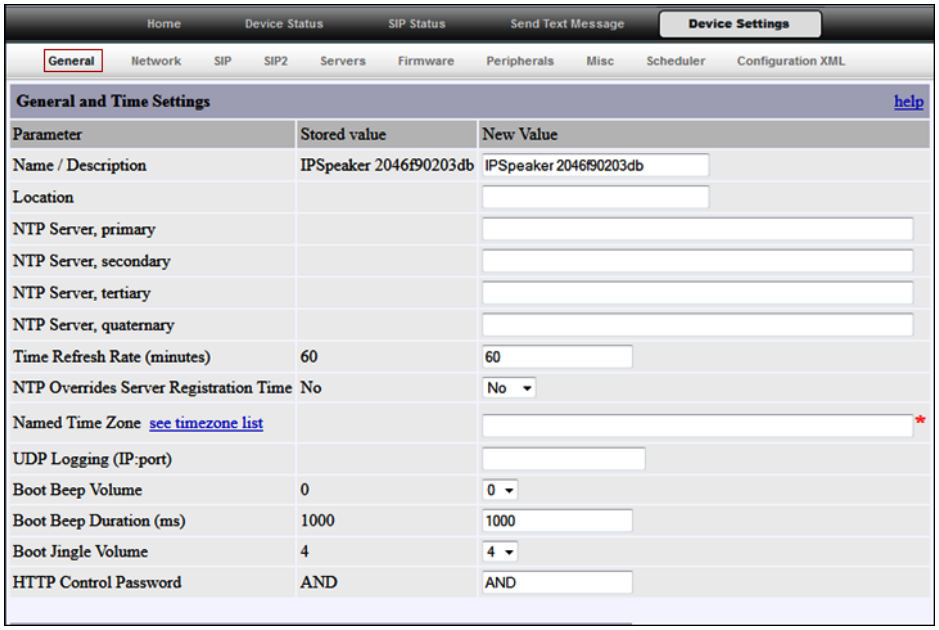


3. Enter the network settings in the **Network Settings** field.
   NOTE: To assign a static IP address, select the **static IP value** under **Network Mode** and enter the **IP address**, **Netmask**, and **Gateway underneath**.

4. Select **Save Network Settings Changes**.



5. Click **General** and do the following:

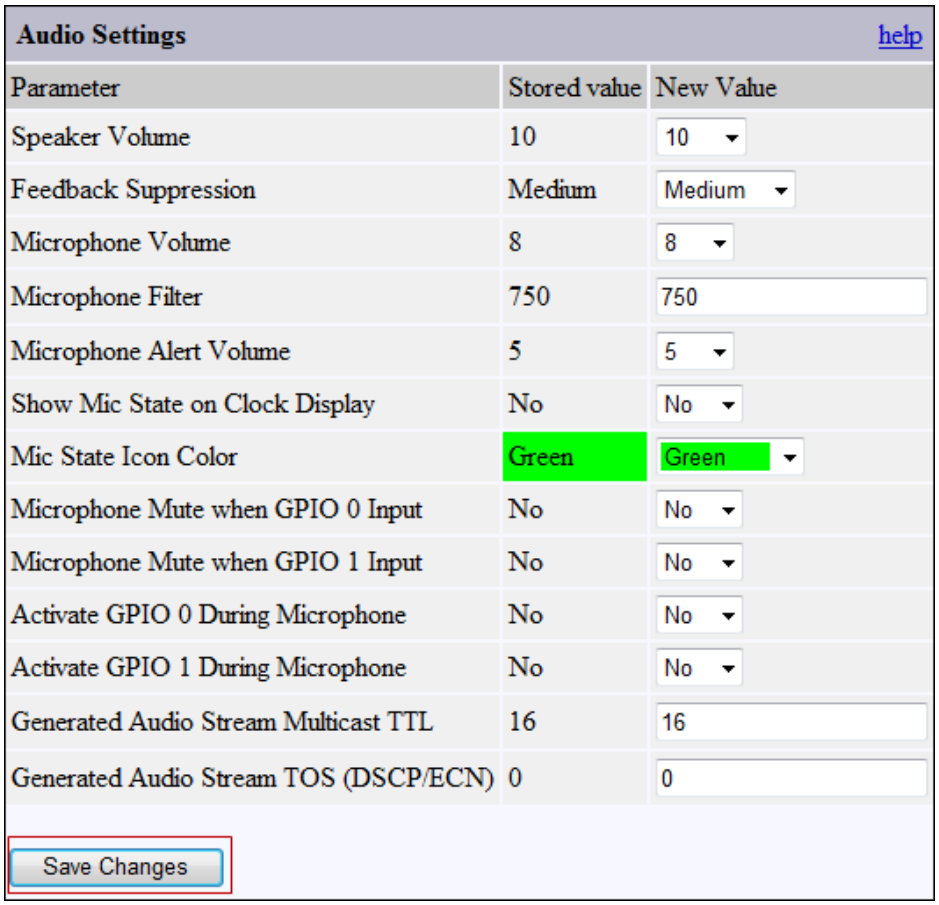


6. Enter a name for the sign in the **Name** field.
7. Enter the IP address of the main NTP server in the **NTP Server, primary** field.
   NOTE 1: This is required while using the sign as a clock during normal operation. It is also important in order to have accurate time stamps for the internal device logging.
   NOTE 2: It is recommended to use the NTP server.
8. Enter the IP address of the Backup NTP server in the **NTP Server, secondary** field.
   NOTE: In the case of primary NTP server failure, the device will access the secondary NTP server. This is optional but recommended.
9. Enter the appropriate string for your Time Zone in the **Named Time Zone** field.
10. Leave the **HTTP Control Password** (default) password as it is or set a new password in case the user wants to change the default password.

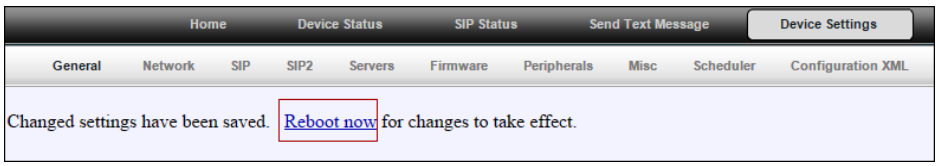
11. In the **Display Settings** section, set value to **100** in the **Display Brightness** field.

Display Settings		help
Parameter	Stored value	New Value
Time Format	12 hour	12 hour
Show Leading Zero	No	No
Show Seconds	Off	Off
Keep Clock Seconds Smaller	No	No
Blink Colon	Yes	Yes
Clock Font Note: The date field is shown only when the clock is using a multi-line font.	BatangChe Bold	BatangChe Bold
Clock Color	Cranberry	Cranberry
Seconds Color	Tan	Tan
AM Color	Olive	Olive
PM Color	Sienna	Sienna
Date Color Note: Use multi-line clock font to enable	Olive	Olive
Date Format Note: Use multi-line clock font to enable	%a, %b %e	%a, %b %e
Date Shown as Tiny Note: Use multi-line clock font to enable	Yes	Yes
Clock Above Small Text	No	No
Minute Progress Critical Start Second	0	0
Minute Progress Color	Hunter	Hunter
Minute Progress Critical Color	Cranberry	Cranberry
Text Font	Arial Bold	Arial Bold
Text Color	Cranberry	Cranberry
Timer Font	Retro 7 Narrow	Retro 7 Narrow
Countdown Timer Color	Green	Green
Countdown Timer Critical Color	Vermillion	Vermillion
Count Up Timer Color	Green	Green
Count Up Timer Critical Color	Vermillion	Vermillion
Display Brightness (0-100)	100	100

12. Set the **Speaker Volume** to the required level.



13. All other values are optional and can be left as default.
14. Click **Save Changes**.
15. A message displays for rebooting the device.

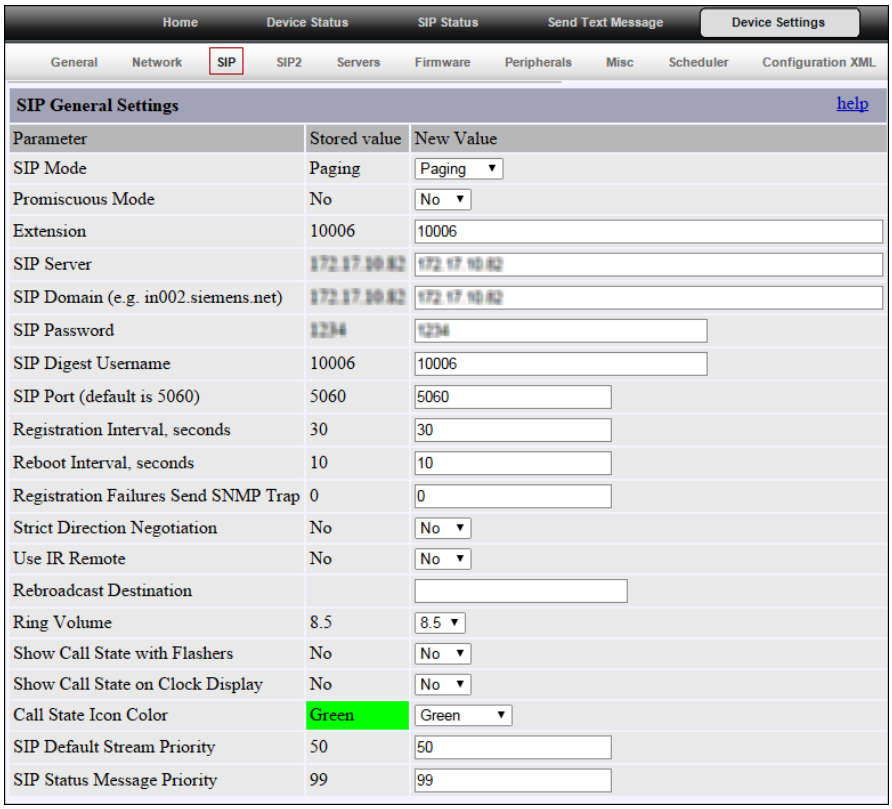


16. Click **Reboot now**.

AND Speaker Configuration

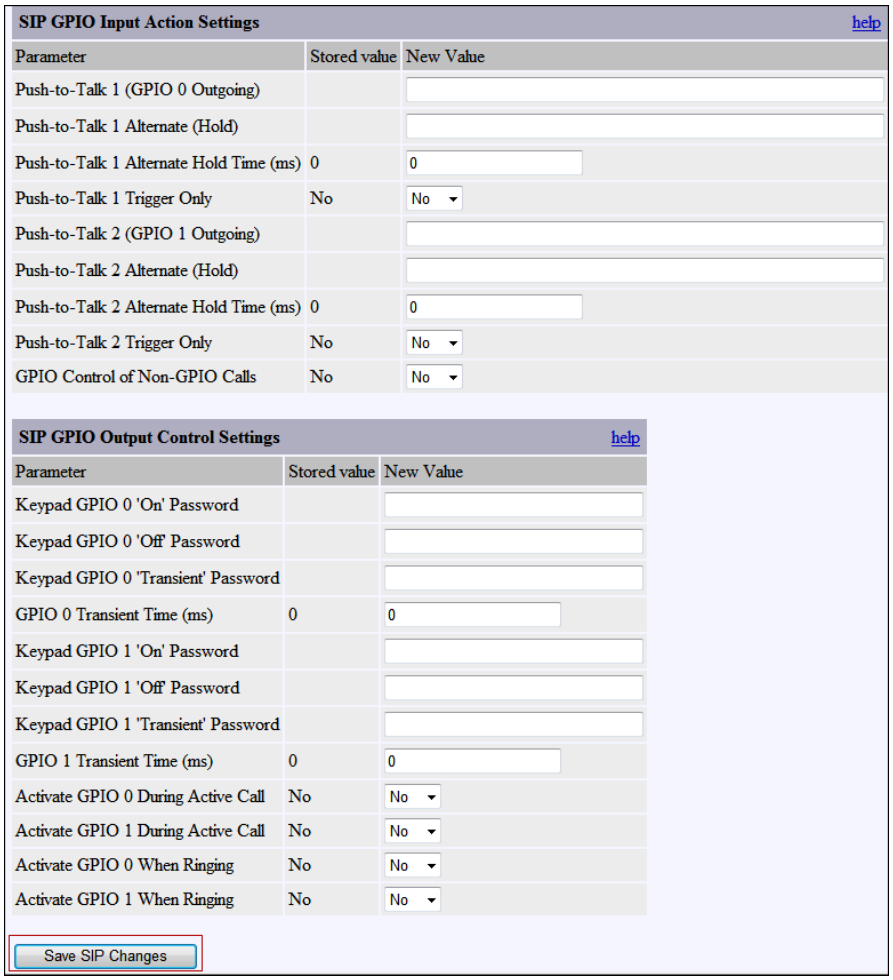
1. For configuring an AND IP Speaker, do the following:
   – Click **Device Settings**.

– Select **SIP**.
⇨ The **SIP General Settings** section displays.



– In the **SIP Mode** field, select **Paging**.
– Enter the FreeSwitch extension number configured for the corresponding AND IP Speaker in the **Extension** field.
– In the **SIP Server** field, enter the IP Address of the SIP Server.
– In the **SIP Domain** field, enter the IP Address of the SIP Server.
– In the **SIP Password** field, enter the password of the FreeSwitch extension.
– Set the **Ring Volume** to the required level.

– All other values are optional and can be left as default.



SIP GPIO Input Action Settings help

Parameter	Stored value	New Value
Push-to-Talk 1 (GPIO 0 Outgoing)		
Push-to-Talk 1 Alternate (Hold)		
Push-to-Talk 1 Alternate Hold Time (ms)	0	0
Push-to-Talk 1 Trigger Only	No	No
Push-to-Talk 2 (GPIO 1 Outgoing)		
Push-to-Talk 2 Alternate (Hold)		
Push-to-Talk 2 Alternate Hold Time (ms)	0	0
Push-to-Talk 2 Trigger Only	No	No
GPIO Control of Non-GPIO Calls	No	No

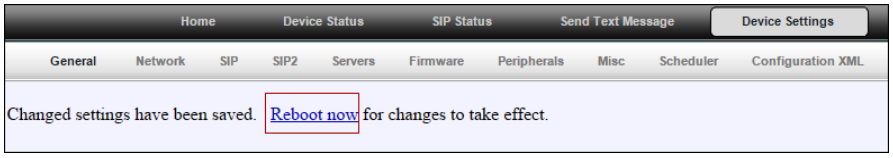
SIP GPIO Output Control Settings help

Parameter	Stored value	New Value
Keypad GPIO 0 'On' Password		
Keypad GPIO 0 'Off' Password		
Keypad GPIO 0 'Transient' Password		
GPIO 0 Transient Time (ms)	0	0
Keypad GPIO 1 'On' Password		
Keypad GPIO 1 'Off' Password		
Keypad GPIO 1 'Transient' Password		
GPIO 1 Transient Time (ms)	0	0
Activate GPIO 0 During Active Call	No	No
Activate GPIO 1 During Active Call	No	No
Activate GPIO 0 When Ringing	No	No
Activate GPIO 1 When Ringing	No	No

Save SIP Changes

2. Click **Save SIP Changes**.

   ⇨ A message displays for rebooting the device.



3. Click **Reboot now** to reboot the device.

Device Verification for AND Device

To test the configuration of the device, follow the steps below:

◈ Open a web browser and enter the following URL:
http://SIGN_IP_ADDRESS/signmsg?text=This+is+a+test+message&loops=3&maxseconds=0&pauseseconds=0&speed=5&color=red&font=arial_bold&human=1&button=Send+New+Text+Message
NOTE: Computer must be connected to the same subnet as the IP LED sign.

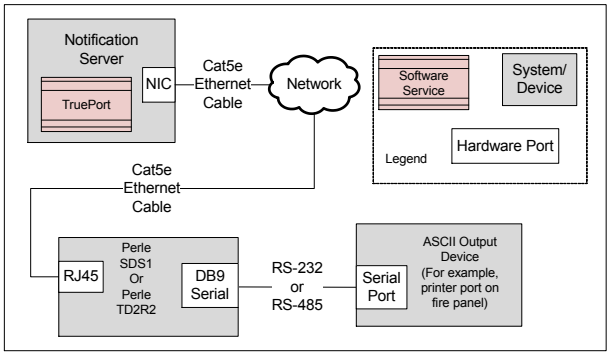
⇨ On successful device configuration, the sign will display `This is a test message` three times as per the configured color.

1.3 ASCII Input Device

ASCII Input Device

This section provides reference and background information for integrating the ASCII Input device. For procedures or workflows, see the step-by-step section.

provides the capability to read ASCII data that is sent serially over a RS-232, RS-485, or RS-422 interface. Additionally, this ASCII data can be analyzed for keywords or patterns through the use of Regular Expressions. A keyword or pattern found in an ASCII message can be then used to raise a management station event, or trigger a incident. Reading ASCII data requires the use of either the Perle SDS1 or TD2R2.

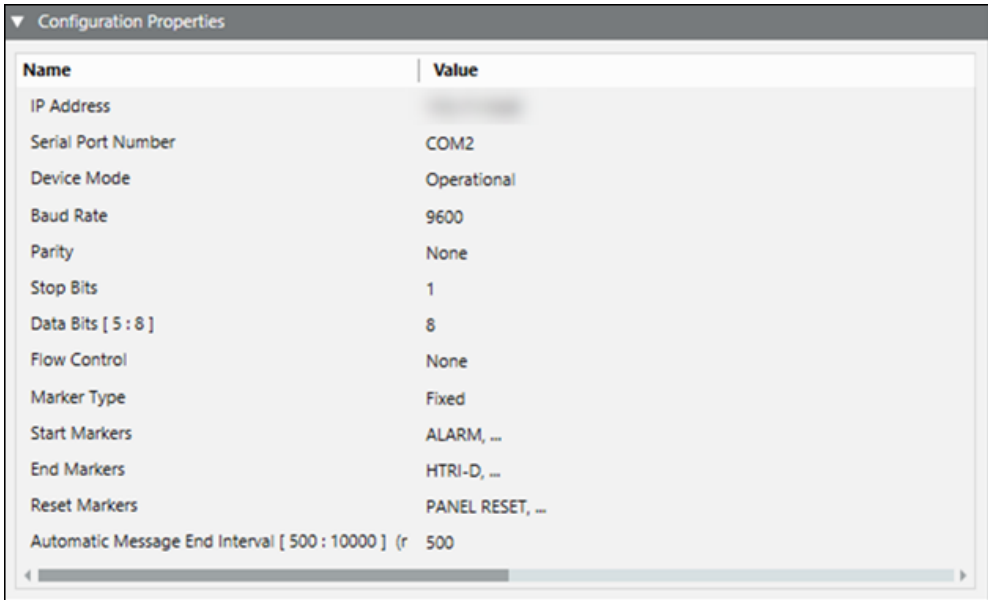


The Perle models SDS1 and TD2R2 provide remote serial access through Internet Protocol over Ethernet. This service provided by the device appears as a separate COM port on the Server. The COM port is automatically created by TruePort, a COM port redirector installed on the Server that works in conjunction with the application to establish a secure communications link. Below is a high level view of the device used in a typical ASCII input reading application on a deployment.

ASCII data streaming from a port on an external device can be read by the Perle device and sent over IP for analysis, filtering and triggering on the Server. The Perle device provides an RS232, RS485, and RS422 interface, which is software selectable.

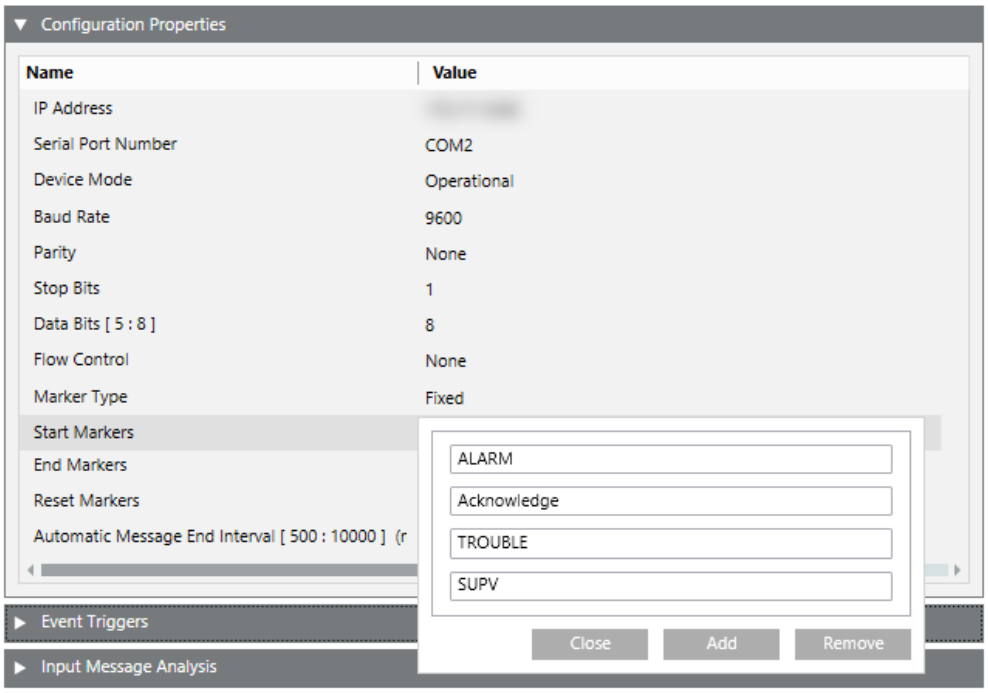
NOTE 1: The Perle IOLAN TD2R2 model provides I/O and relays in addition to a serial interface.
NOTE 2: The ASCII driver only supports input data comprised of the standard ASCII character set, which effectively means it supports only English letters and no international letters. International letters in received data will be replaced with question marks.

ASCII Input Device Workspace

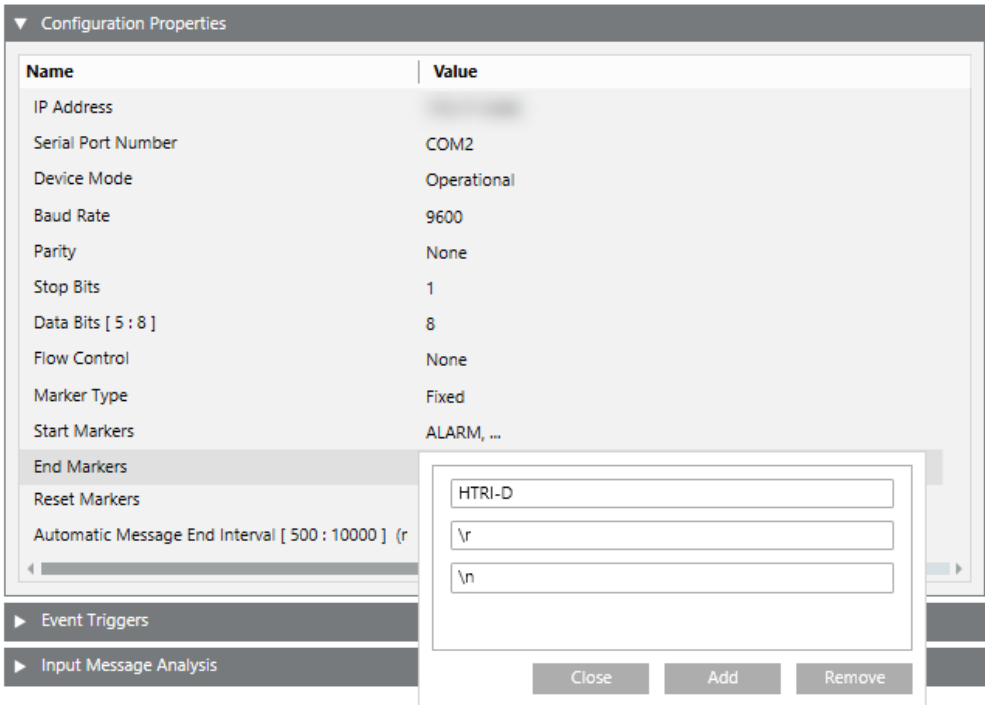


- **IP Address**: Set the IP address of the Perle device which is connected with Fire Panel and which provides the ASCII data from Fire Panel to MNS. In case if Fire Panel is directly connected to MNS server using serial cable, then set value as -1.
- **Serial Port Number**: Displays the COM port address of the device. Enter a valid COM port address string of the device. This string should always have the format as COM followed by unsigned integer number. For example, COM20. For more details, refer to the *Serial Settings* .section.
  NOTE: To check the COM ports that were used by the device, open the TruePort Management Tool.
- **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.
- **Baud Rate**: Select the Baud Rate used serially by the ASCII device from the drop-down list.
- **Parity**: Select the Parity used by the ASCII device from the drop-down list.
- **Stop Bits**: Select the number of Stop Bits the ASCII device serial protocol is using from the drop-down list.
- **Data Bits**: Displays the Data Bits of the device.
  NOTE: The value range is 5 to 8 bits.
- **Flow Control**: Select the type of Flow Control mechanism used by the ASCII device.
- Marker Type: Select one of the following type from drop-down list:
  Fixed: The driver splits the incoming serial data into individual messages by matching fixed patterns.
  Regex: The driver splits the incoming serial data into individual messages by matching regular expressions. This option gives more flexibility when matching with fixed patterns is not possible.
- **Start Markers**: This is an optional field. If configured, the driver uses the start marker to identify the start of messages in the input serial data. The driver will automatically extract a message when the Automatic Message End Interval expires after the occurrence of the most recent start marker. Refer to the table in 4.2.2 for resulting behavior in conjunction with an end marker. Multiple start markers can be configured as shown in the below image titled Configuration Properties with Start Markers for ASCII Input Perle Device.
- **End Markers**: This is an optional field. If configured, the driver uses the end marker to identify the end of messages in the input serial data. Refer to the table for resulting behavior in conjunction with a start marker. Multiple end markers can be configured as shown in the below image titled Configuration Properties with End Markers for ASCII Input Perle Device.
- **Reset Markers**: This is an optional field. If configured, the driver uses the reset marker to identify panel reset message in the messages extracted using start marker and end marker. Reset marker cannot be configured in regex form however it has to be configured in a fixed string form, ex. "PANEL RESET". User can configure multiple reset markers. On receiving panel reset message for a panel, driver clears all active events for this panel.
- **Automatic Message End Interval**: This is a mandatory field if only start markers OR no markers are configured, otherwise it is optional. This value represents the time interval at which data received from the device is used for extraction of messages by using available marker configuration. Refer to the table for the resulting behavior when used in conjunction with start and end markers.

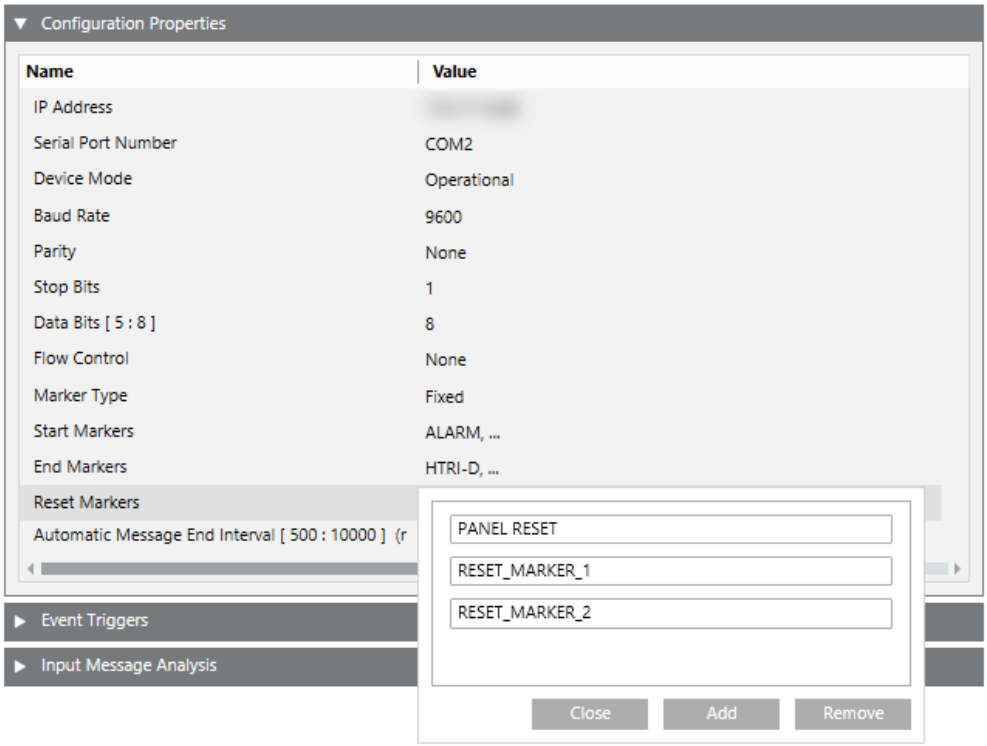
Start Markers



End Markers



Reset Markers



Behavior for different combinations of start and end marketer configuration settings

SM	EM	AMEI	Decision
0	0	1	If no markers are configured, then the driver will process all input data received up to the point of the automatic message end interval as a message. Please note that using this configuration is not recommended as the content of the extracted messages will depend entirely on the timing of the input data.
0	1	NA	The driver will always process the input data between two end markers as a message. The automatic message end interval setting will be ignored.
1	0	1	The driver will process the input data between two start markers as a message. When the driver has not identified a start marker in the input data for the specified automatic message end interval, it will consider the currently started message as complete and process it.
1	1	NA	The driver will process the input data between a start marker and an end marker as a message. The automatic message end interval setting will be ignored.

NOTE:
SM = Start Marker, EM = End Marker, AMEI = AutomaticMessageEndInterval
0 = Not Configured, 1 = Configured, N/A = Not applicable/Ignored

Marker Configuration Example

The following tables show samples of incoming serial data, configured marker type (fixed and regex) and extracted commands.

Start Marker

Marker Type	Message Sample	Marker	Extracted Commands
Fixed	Audibles Unsilenced 07:17:18 May 28,2016 Audibles Silenced 07:17:28 May 28,2016 Audibles Unsilenced 07:17:32 May 28,2016 Audibles Silenced 07:17:36 May 28,2016	Audibles	1.Audibles Unsilenced 07:17:18 May 28,2016 2. Audibles Silenced 07:17:28 May 28,2016 3. Audibles Unsilenced 07:17:32 May 28,2016 4.Audibles Silenced 07:17:36 May 28,2016

Regular Expression (Regex)	12:42:46 pm THU 21-JAN-16 4544 DUCT DET RETURN S. MECH BLDG 3:1-10 DUCT DETECTOR NORMAL 12:44:49 pm THU 21-JAN-16 4544 DUCT DET RETURN S. MECH BLDG 3:1-11 DUCT DETECTOR NORMAL	[0-9]{2}:[0-9]{2}:[0-9]{2} [ap]m [A-Z]{3} [0-9]{2}-[A-Z]{3}-[0-9]{2}	1. 12:42:46 pm THU 21-JAN-16 4544 DUCT DET RETURN S. MECH BLDG 3:1-10 DUCT DETEC-TOR NORMAL 2. 12:44:49 pm THU 21-JAN-16 4544 DUCT DET RETURN S. MECH BLDG 3:1-11 DUCT DETECTOR NORMAL

End Marker

Marker Type	Message Sample	Marker	Extracted Commands
Fixed	TROUBLE IN :5-2 07:17:50 May 28,2016 MNS Trouble 5-2:2, Trouble causing input, HTRI-D \r TROUBLE OUT :5-2 07:17:54 May 28,2016 MNS Trouble 5-2:2, Trouble causing input, HTRI-D \r TROUBLE IN :5-2 07:18:08 May 28,2016 MNS Trouble 5-2:2, Trouble causing input, HTRI-D \r	\r	1. TROUBLE IN:5-2 07:17:50 May 28,2016 MNS Trouble 5-2:2, Trouble causing input, HTRI-D 2. TROUBLE OUT :5-2 07:17:54 May 28,2016 MNS Trouble 5-2:2, Trouble causing input, HTRI-D 3. TROUBLE IN:5-2 07:18:08 May 28,2016 MNS Trouble 5-2:2, Trouble causing input, HTRI-D
Regular Expression (Regex)	Audibles Unsilenced 07:17:01 May 28,2016 Audibles Silenced 07:17:02 May 28,2016 Audibles Unsilenced 07:17:03 May 28,2016 Audibles Silenced 07:17:04 May 28,2016	[0-9]{2}:[0-9]{2}:[0-9]{2} [a-zA-Z]{3} [0-9]{2},[0-9]{4}	1. Audibles Unsilenced 07:17:01 May 28,2016 2. Audibles Silenced 07:17:02 May 28,2016 3. Audibles Unsilenced 07:17:03 May 28,2016 4. Audibles Silenced 07:17:04 May 28,2016

ASCII Input Device Troubleshooting

Problem: Once the ASCII Input Device is created in the **Device Editor** tab, 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.

ASCII Input Device

Installing ASCII Input Device

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

Prerequisites

Before proceeding, ensure that the following items are available:

- Perle IOLAN SDS1 (serial only model) or Perle IOLAN SDS1 TD2R2.
- 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) that is used to communicate with the device must be installed on the same server/machine that runs the application.
  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 DHCP.
  NOTE 3:
  To configure the device, a computer located in the same network is necessary.

Disclaimer:
Prior to the commissioning of 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 the 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 it 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 being operational. When the device has completely rebooted, the **Power/Ready** LED 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 the network jack.

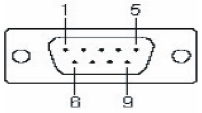
⇨ After a few seconds, the **Link/10/100** should be a solid amber or green.
NOTE: Amber refers to a 100Mb connection. Green refers to a 10Mb connection.
NOTE:
The device does not have DHCP turned on as factory default. The device will need to be configured to use DHCP or a static IP with a computer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

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 for serial communication (for example, an LED display or the ASCII output port of a fire panel).

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.

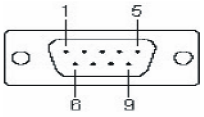
NOTE: Keep the Console/Serial switch(s) present on the device in OFF position.



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. 8: 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. 9: TD2R2 Pinout

NOTE:
RS-232 pinout on both models are the same. However, RS-485 pinout differs on both.

Configuring and verifying ASCII Input Device

This section provides the steps linked with 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.

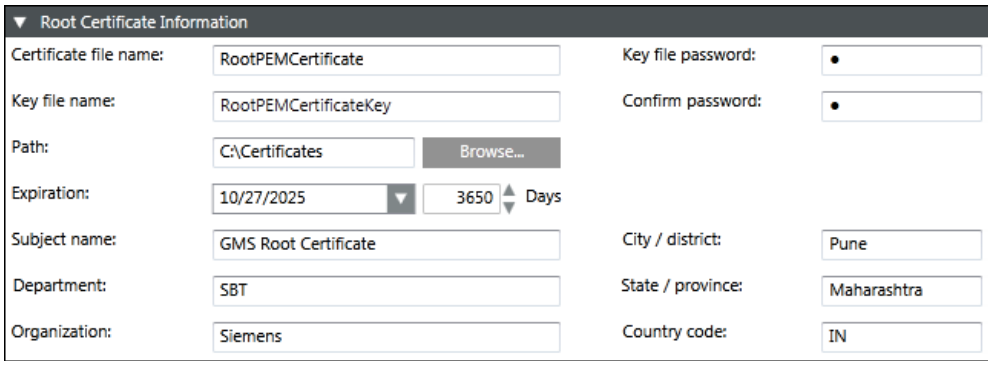
The second step is to configure the driver on the computer that will be communicating with the device over the network. There are several methods used to communicate with the device. One of which is with the TruePort driver.

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 the remote device.

Creating Certificate From System Management Console

To establish a secure communication, certificates must be configured.

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.



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.

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 device to be configured.

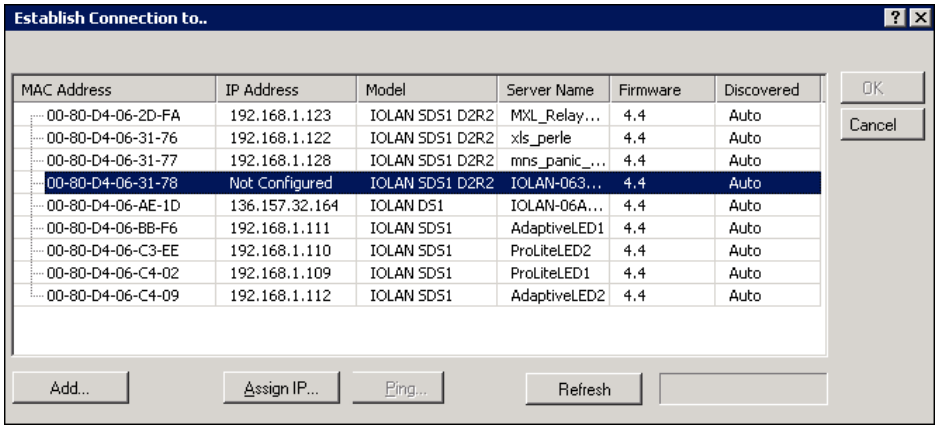
▷ Ensure that the following certificates are created using the System Management Console (SMC) or obtained from the site's IT department in Privacy Enhanced Mail (PEM) format:
a) Root Certificate (.pem)

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 cat command in command prompt, for example, **cat RootCertificateKey.pem RootCertificate.pem > RootCombineCert.pem**.

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

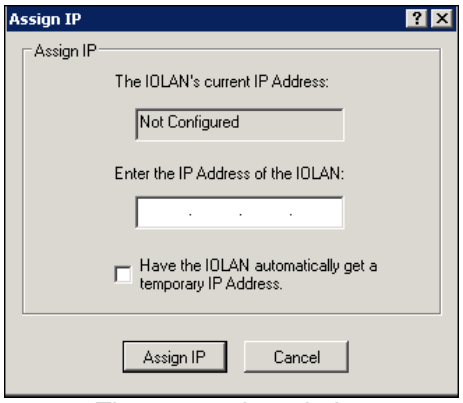
1. Start the **DeviceManager**.



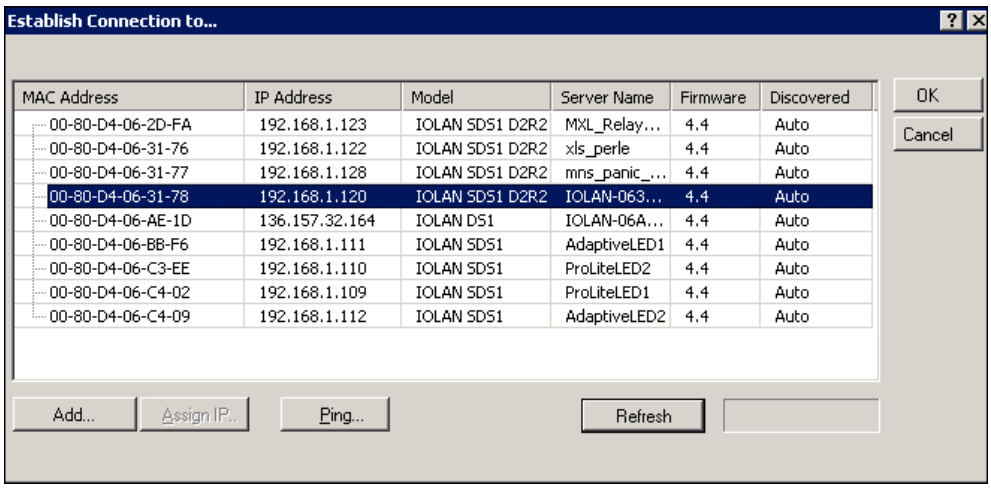
⇨ All similar devices under that network should be visible.

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 LEDs on the device; the power LED should be solid green and the link LED should be solid amber or 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**.



⇨ The connection window appears with an IP address.



4. Select the device again, and click **OK** to log into the device for configuring.
5. In the **Login** window, enter the device password. The factory default password is: **superuser**.

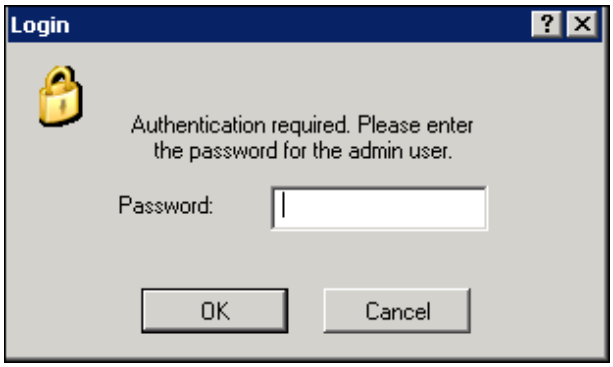
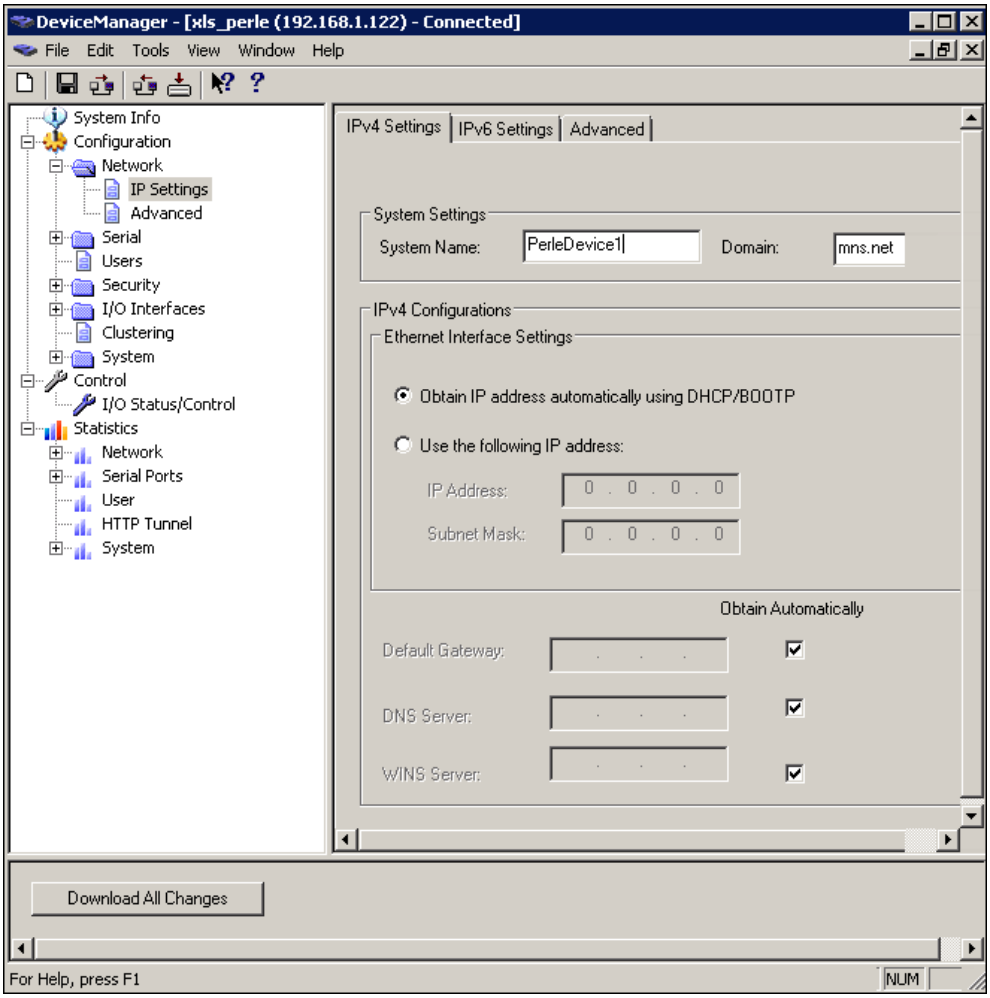


Fig. 10: Login Window

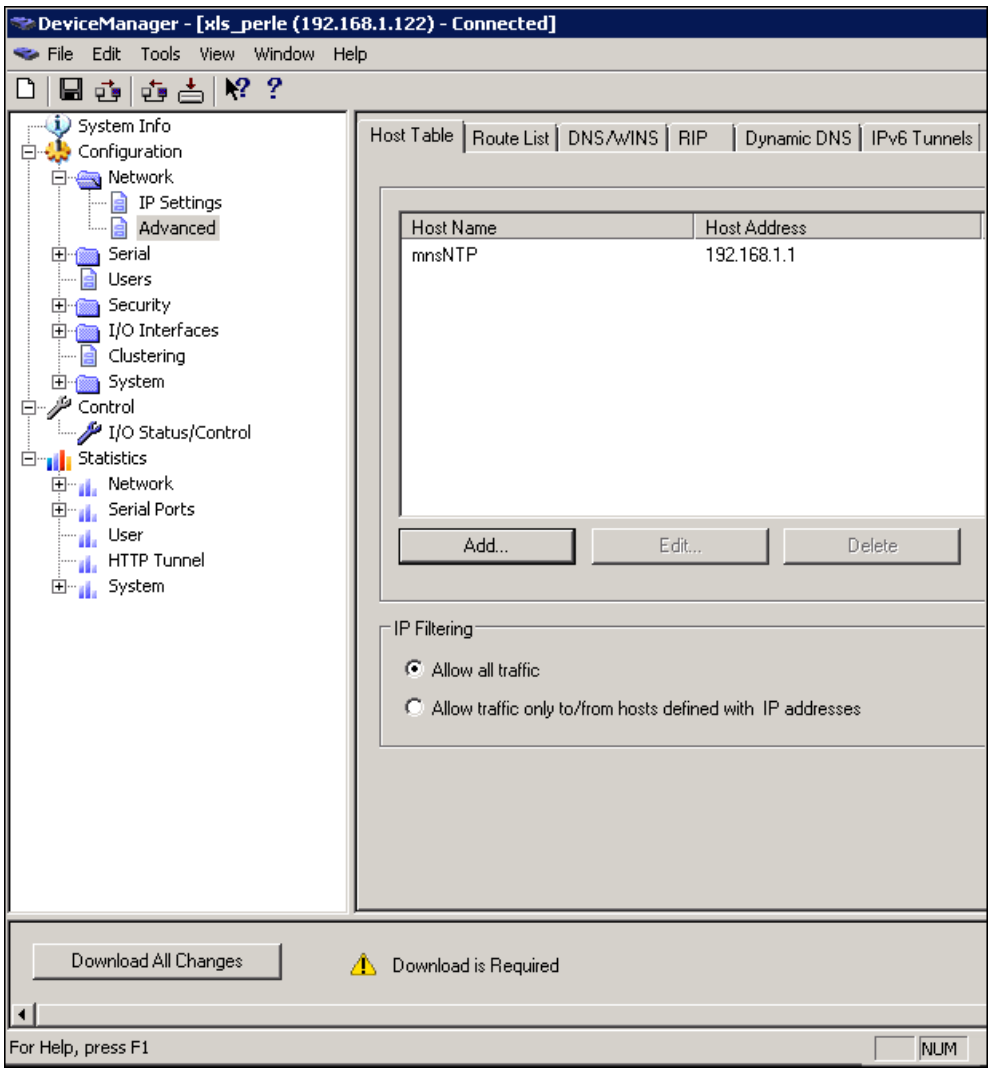
Network Set Up

To further configure the network settings of the device, log into the device using Perle DeviceManager. Proceed with 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**.



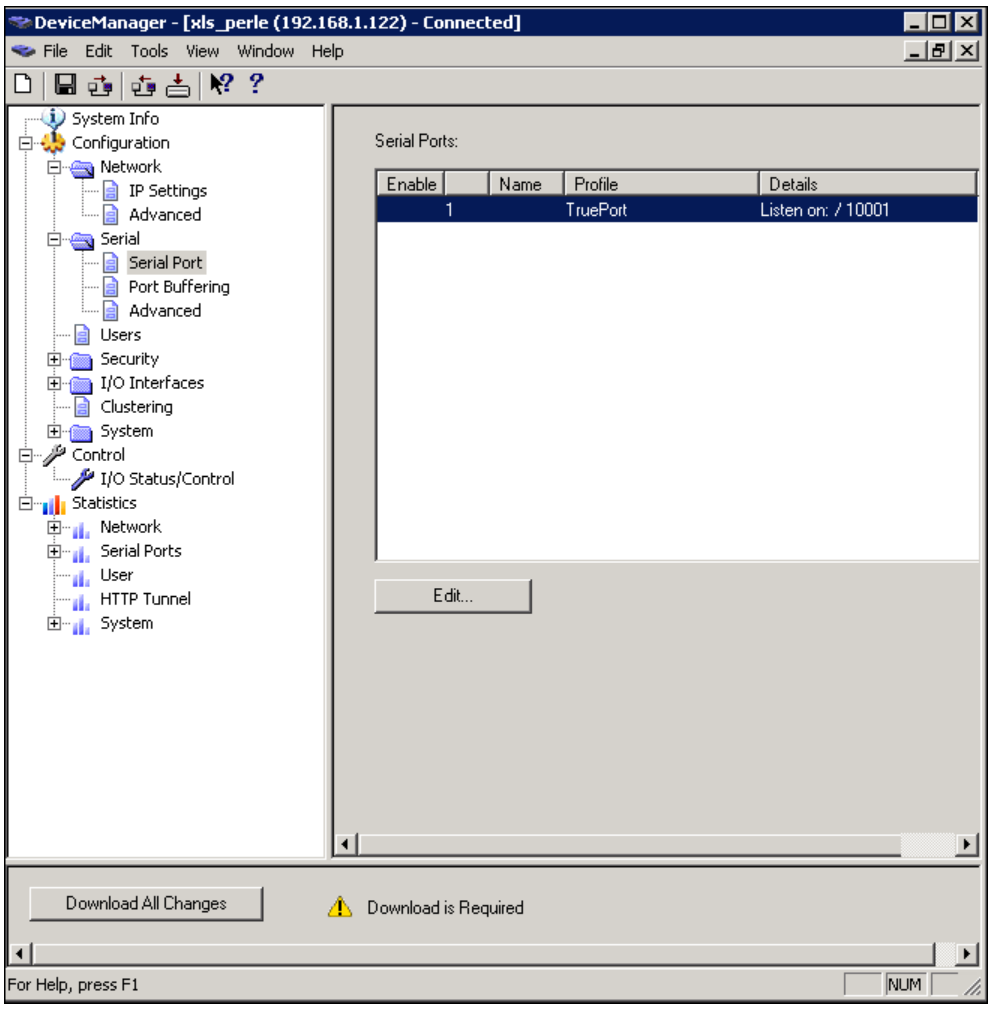
2. On the **Ipv4 Settings** tab, in the **System Name** field, give the device a distinguishable name to help identify this device from other similar devices.
   NOTE 1: The System Name will also be used by the device to create a fully qualified domain name.
   NOTE 2: By default, the device is always **IOLAN** followed by the last three bytes of the device 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**.
5. Select the **Register Address in DNS** check box.
6. Click the **Advanced** folder in the tree view.



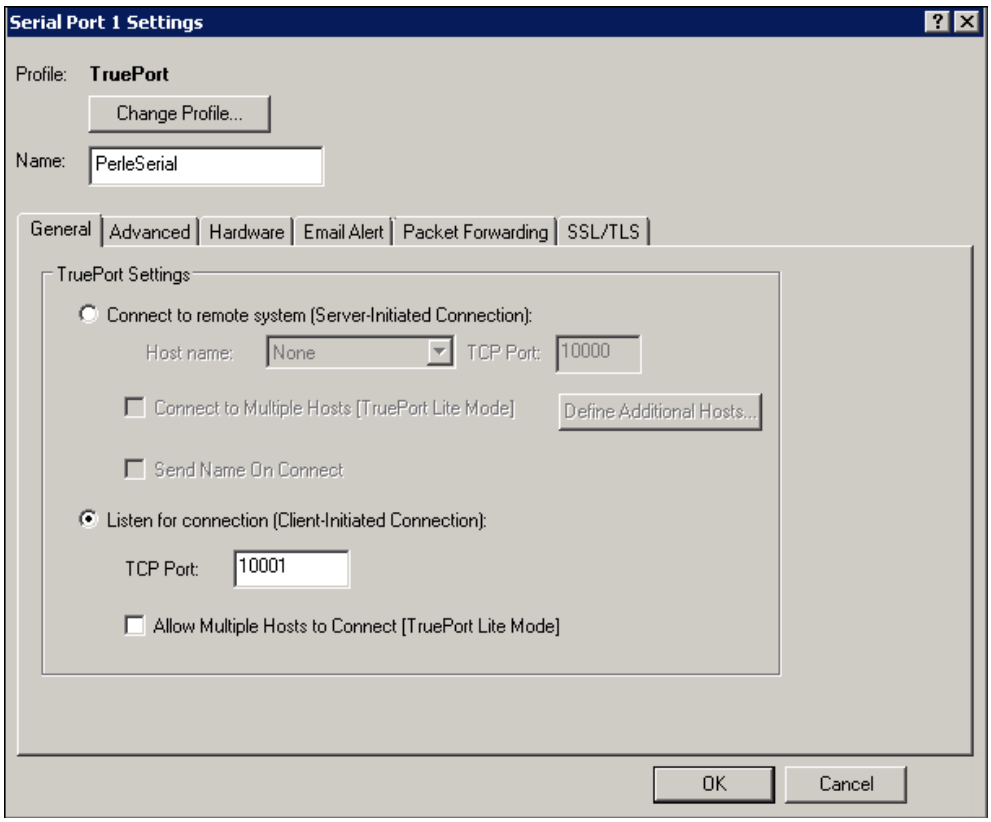
7. Select the **Host Table** tab.
8. Click **Add** to add an NTP host.
9. On the window, enter a descriptive name for the NTP server (for example, **mnsNTP**).
10. Enter the IP address or the fully qualified domain name of an available NTP server.
    NOTE: An available NTP server is required to enable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

Serial Settings

1. In the **DeviceManager** window, select **Serial > Serial-Port**.
   ⇨ Begin configuring the number of serial ports and the device profile. Only one serial port per device is required for serial communication.
2. Select the default serial port and click **Edit**.



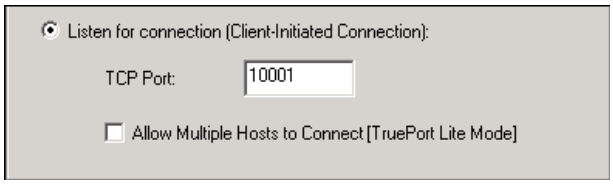
3. In the **Serial Ports Settings** window:
   a. Click **Change Profile**.
   b. Select the **TruePort** profile
   c. Click **OK**.



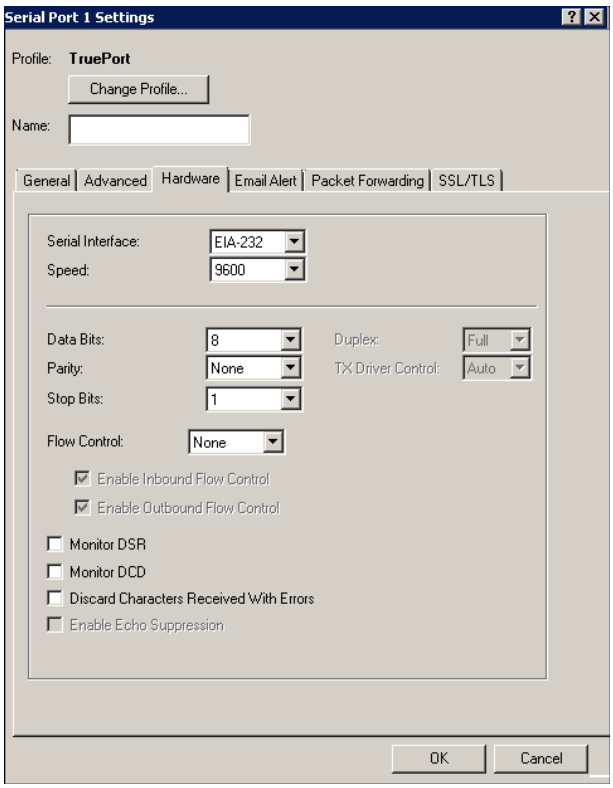
⇨ The **Serial Port Settings** window changes to reflect the new profile.

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

   ⇨ In this mode, the device will wait for the server to establish a connection.
6. Enter in 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.
7. Ensure that the **Allow Multiple Hosts to Connect [TruePort Lite Mode]** check box is cleared so that other servers cannot connect simultaneously to the same device. Click **OK**.

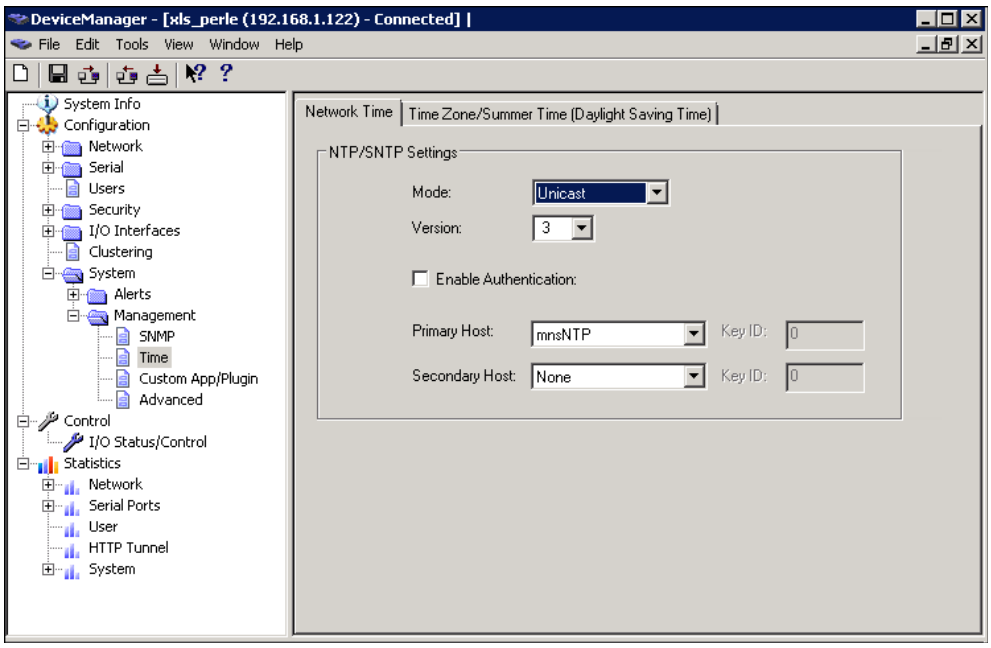


8. Select the **Hardware** tab.



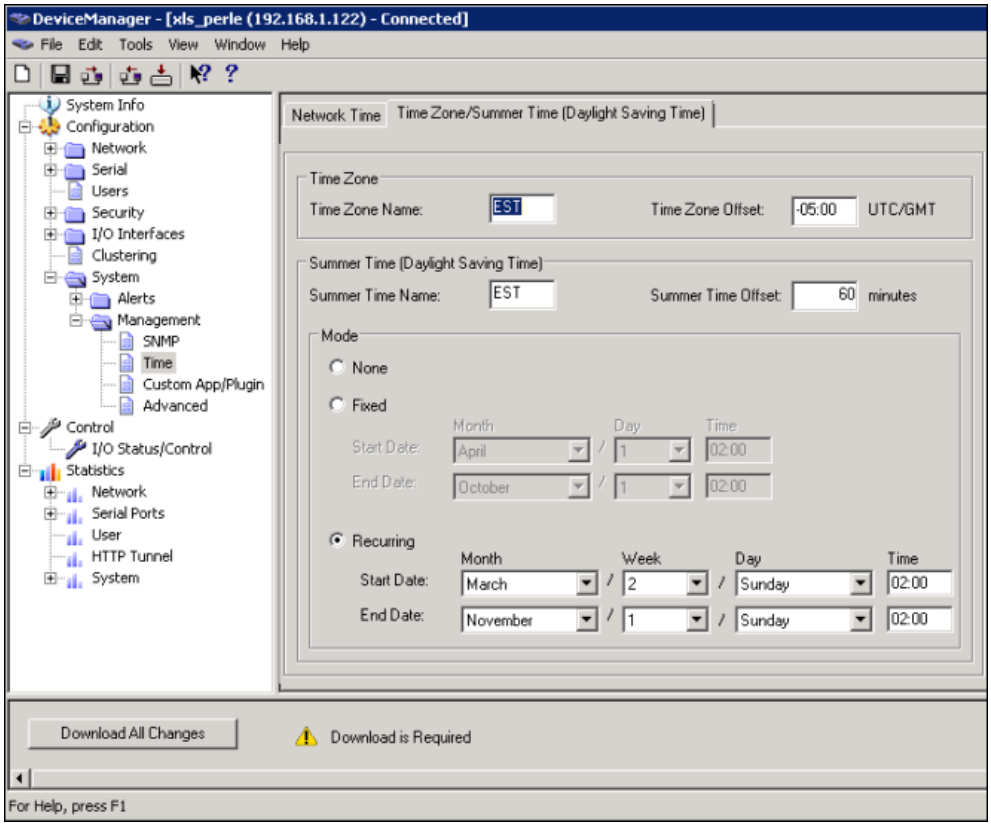
9. For **Serial Interface**, select either **EIA-232** (RS-232), **EIA-422** (RS-422) or **EIA-485** (RS-485).
10. Set the **Speed** to the serial interface baud rate (for example, **9600**).
11. Set **Data Bits** to the number of bits of the serial protocol (for example, **8** bits).
12. Select the appropriate **Parity**.
13. Set the appropriate number of **Stop Bits**.
14. Select the type of **Flow Control** used.
15. Do not select the **Monitor DSR** check box.
16. Do not select the **Monitor DCD** check box.
17. Do not select the **Discard Characters Received With Errors** check box.
18. Select the **SSL/TLS** tab.
19. Select the following check boxes:
    - **Enable SSL/TLS**.
    - **Use Global settings (Security>SSL/TLS)**.
20. Click **OK**.
21. Select **Configuration > System > Management > Time**.
22. Select the **Network Time tab**.
23. Do the following parameter settings:
    - **Mode**: Unicast
    - **Version**: 3
    - Leave the **Enable Authentication** check box cleared.
    - **Primary Host**: Select the NTP server name created earlier.
    - **Secondary Host**: Select an alternative NTP server name or 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.



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

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

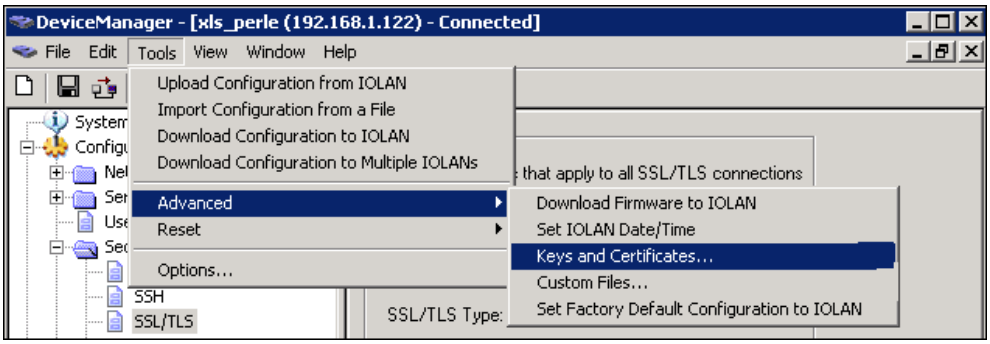


26. Select **Configuration>Security>SSL/TLS**.

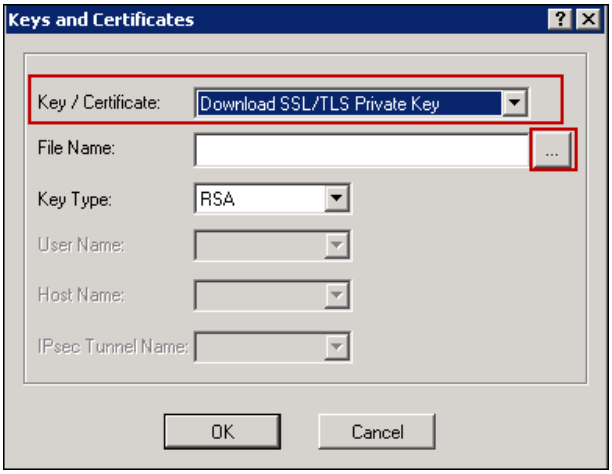
27. Set **SSL/TLS Version** field to **Any**.

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

29. Under **SSL Certificate** section, enter the password of the Root certificate (.pem) in the **Passphrase** field.
30. Select **Tools > Advanced > Keys and Certificates**.
    ⇨ The **Keys and Certificates** dialog box displays.



31. In the **Key/Certificate** drop-down list, select **Download SSL/TLS Certificate**.
32. Click the browse button and upload the private key for the Root certificate (.pem).
33. Click **OK**.
    NOTE: Certificates must be in PEM format.



34. Select **Tools > Advanced > Keys and Certificates**.
35. In the **Key/Certificate** drop-down list, select **Download SSL/TLS Certificate**.
36. 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.
37. Click **OK**.
38. Select **Tools>Advanced>Keys and Certificates**.
39. In the **Key/Certificate** drop-down list, select **Download SSL/TLS CA**.
40. Click the browse button and upload the root certificate (RootCertificate.pem file).
41. Click **OK**.

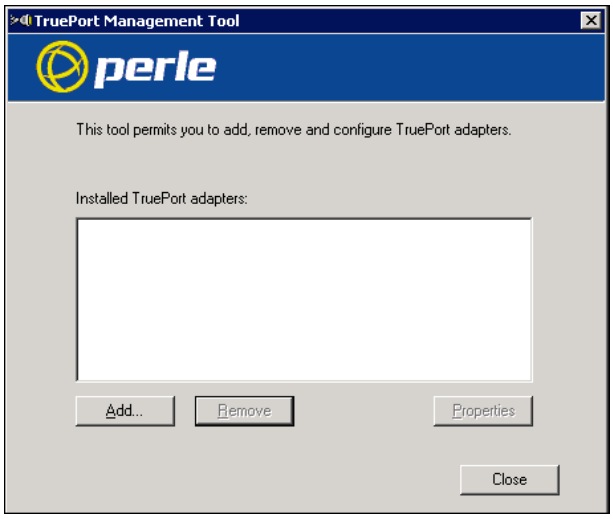
42. Click **Download All Changes** to make the changes to the device.
43. Click **Reboot IOLAN**.
    NOTE: Any time a reboot of the device is needed, or power is reconnected, it will take 90 seconds for the device to reboot and initialize. When the device is ready, the Power LED will be solid green color and the Link LED will be solid amber or green.

⇨ The device is now configured.

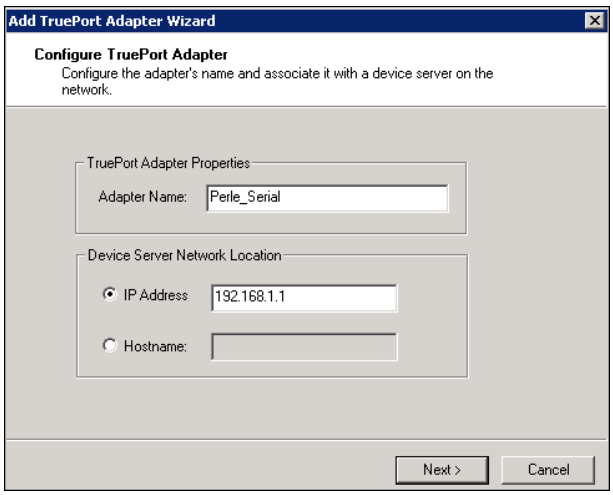
TruePort Driver Configuration

▷ 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 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. The recommended procedure is that each device has its own, unique COM port for each service.
NOTE: Serial communication and I/O access are each considered a separate service and require separate COM ports.

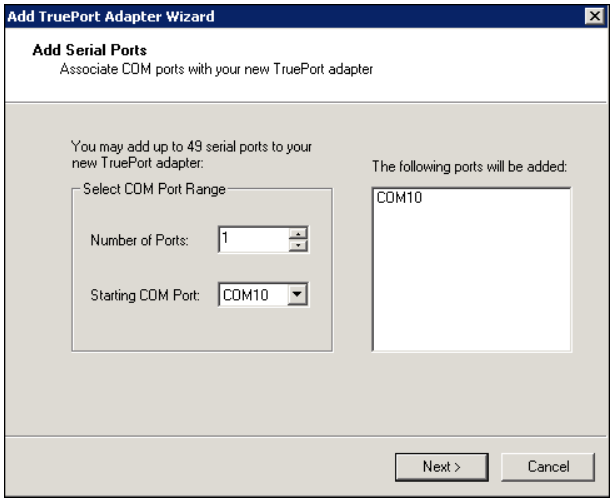
1. Install TruePort on the server.
2. Start the **TruePort Management Tool**.
3. In the **TruePort Management Tool** window, click **Add**.



4. Enter a name for the TruePort Adapter.
   NOTE: This adapter will serve a particular device and will 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**.

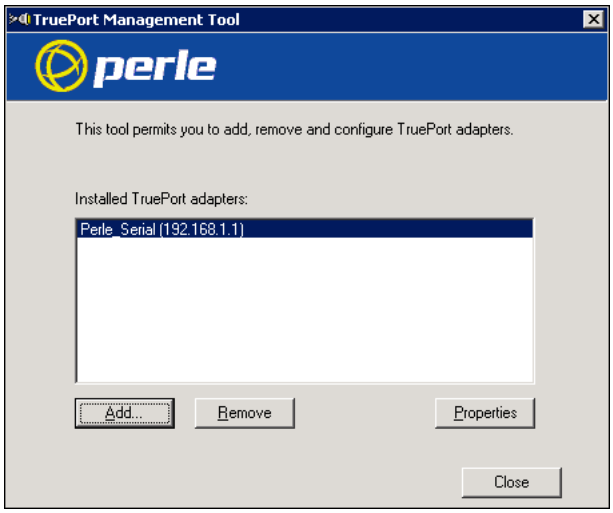


6. Leave the number of ports set to **1** (if using I/O access, set ports to **2**, or add another later). Select the COM port to assign to that particular device. By convention, start at COM100 and raise the increment for each device and service configured. This will help to avoid any conflicts with existing COM ports or other devices. TruePort allows creation of up to 4096 COM ports.
7. Click **Next**.



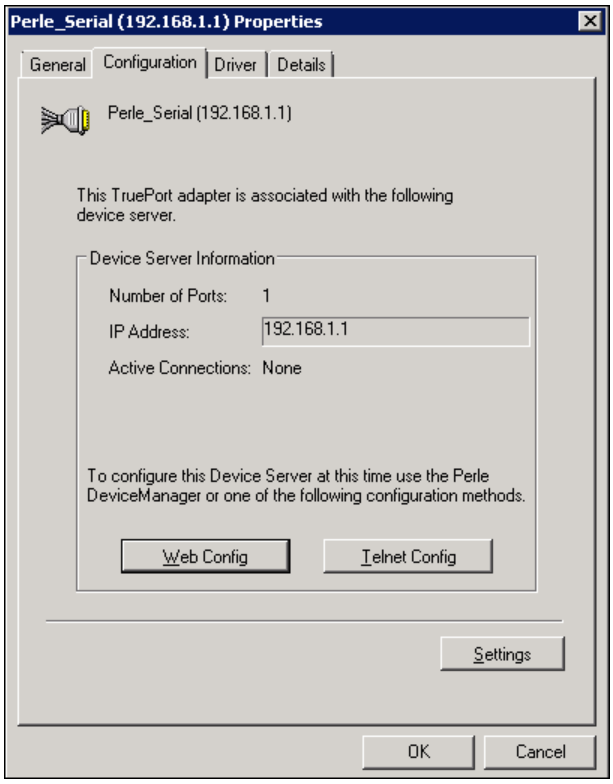
⇨ The TruePort Adapter in the **TruePort Management Tool** is visible.

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

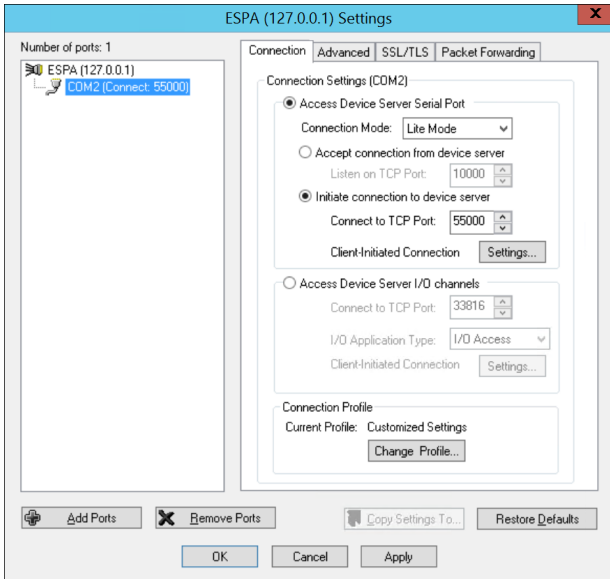


Serial Settings

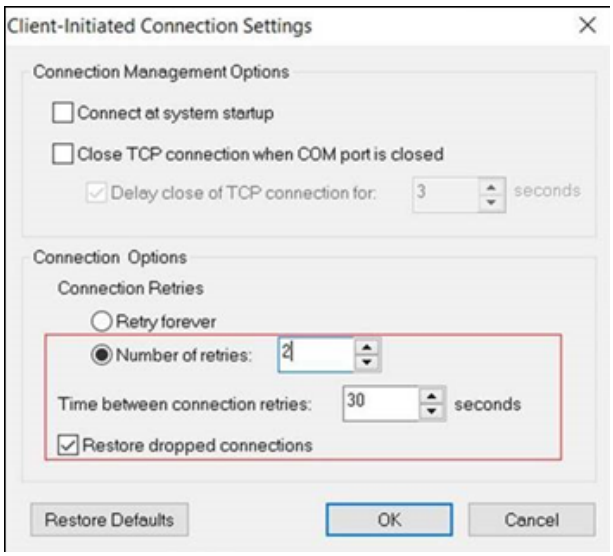
1. Select the properties window of the device port to be configured.
2. Select the **Configuration** tab.
3. Click **Settings**.



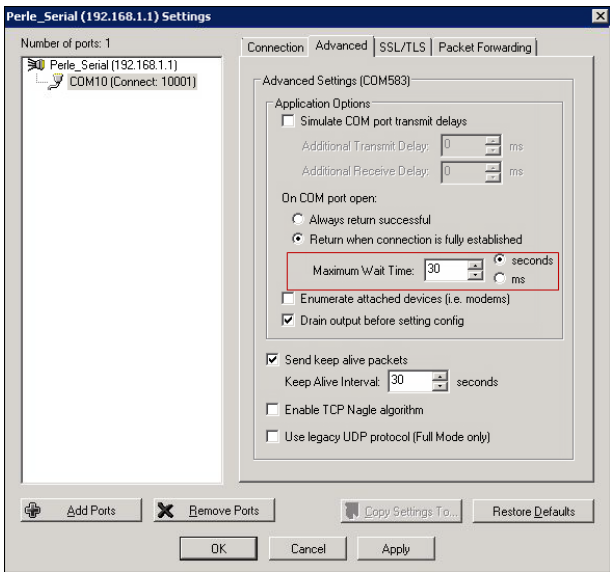
4. Click the target COM port listed in the tree view.
   ⇨ The TruePort and COM port settings for this adapter displays.
5. Select the **Connection** tab.
6. Select **Initiate connection to device server**.



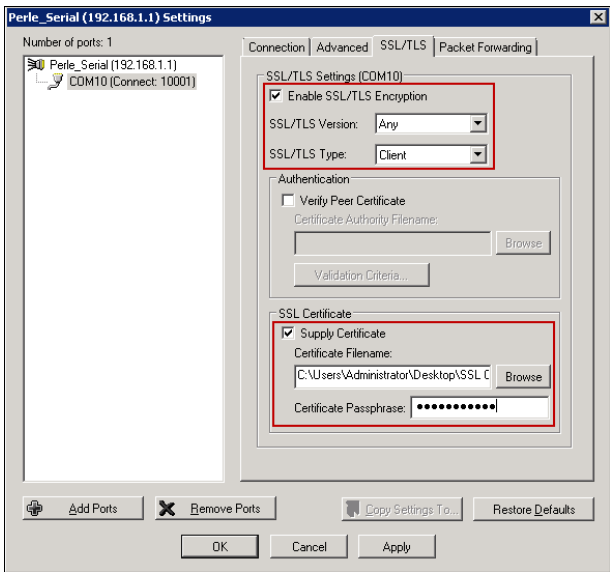
   – Under **Connect to TCP Port**, enter the port number that was previously assigned to the device through the Perle DeviceManager.
7. Click the **Settings** button next to **Client-Initiated Connection**.
   ⇨ The **Client-Initiated Connection** window displays:



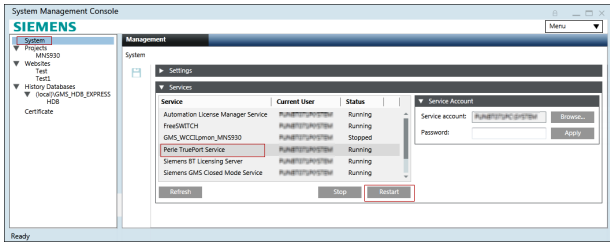
8. In the **Connection Options** section, do the settings only for the following parameters:
   - **Number of retries**: 2.
   - **Time between connection retries**: 30.
   - Select the **Restore dropped connections** check box.
9. In the **Connection Management Options** section, ensure that you do not select **Connect at system startup** and the **Close TCP connection when COM port is closed**.
10. Click **OK**.
11. Select the **Advanced** tab.



12. Set the **Maximum Wait Time** to **30 seconds**.
13. Select the **SSL/TLS** tab.



14. Select the **Enable SSL/TLS Encryption** check box.
15. Set the **SSL/TLS Version** field to **Any**.
16. Set the **SSL/TLS Type** field to **Client**.
17. Select the **Supply Browse** button **Certificate** check box.
18. Click and select the combined Root certificate. Refer to the Device Configuration section for more information on combining a Root certificate.
19. in the **Certificate Passphrase** field, enter the password.
20. Click **Apply**.
21. Click **OK**.
22. Restart the **Perle TruePort Service** from the SMC.



Device Verification

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

PuTTY can be downloaded from the following link:

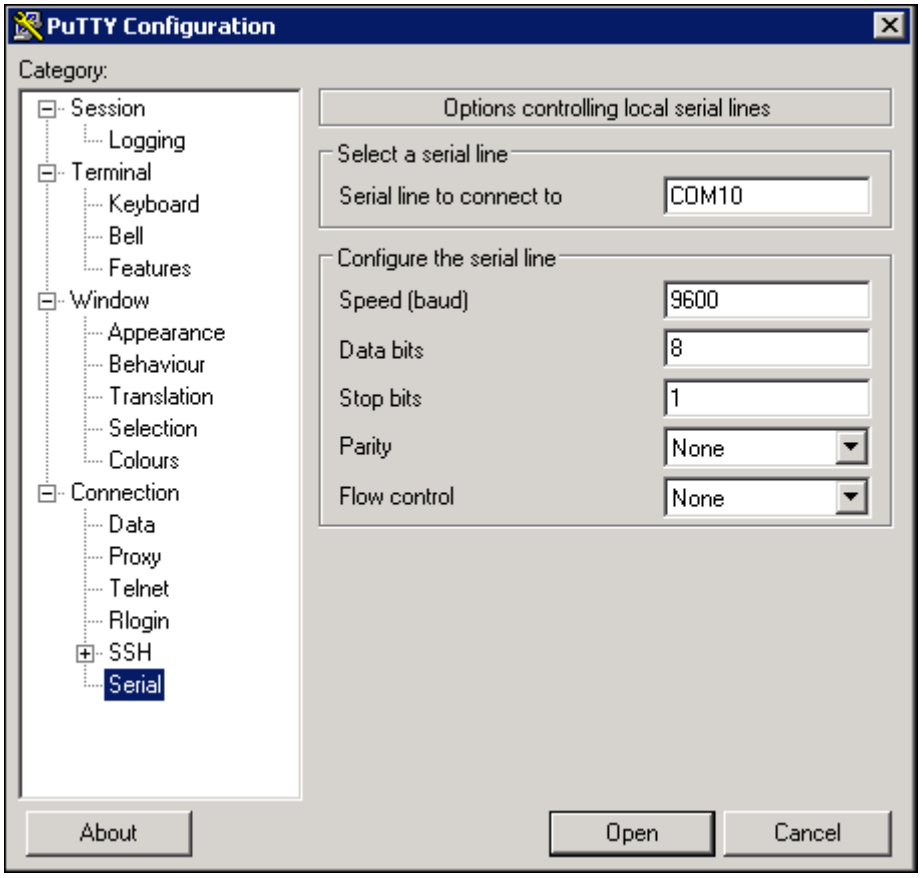
http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe

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 ASCII example below uses the following serial parameters:

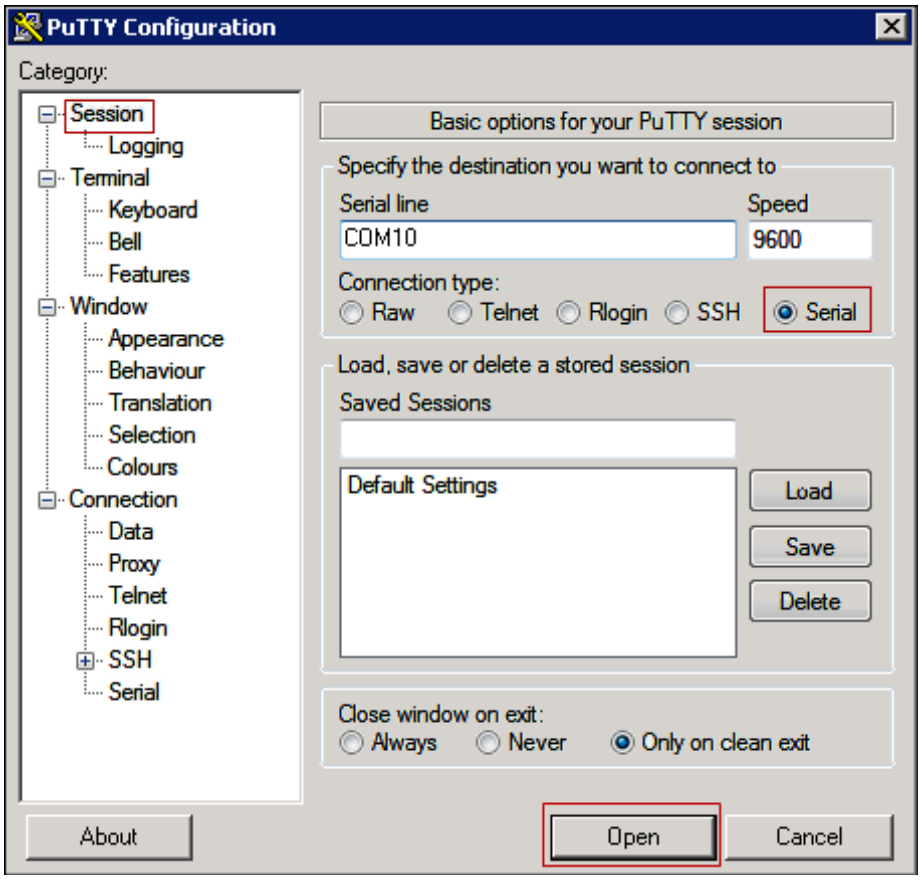
1. Open PuTTY, and select **Connection** > **Serial**.
2. For **Serial line to connect to**, enter the TruePort COM port number created in the TruePort Driver Configuration section.

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



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 ASCII data is sent. This data should be visible in the terminal session.
   NOTE: If no data is sent, verify that RX and TX pins are not switched. If the 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 ASCII device.

ASCII Input Device Troubleshooting

Problem: Once the ASCII Input Device is created in the **Device Editor** tab, 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.

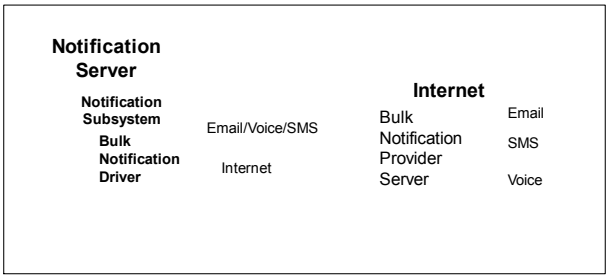
1. Restart the TruePort service.
2. Reimport the certificates on device manager and reboot the Perle IOLAN device.
3. Reboot the Server.
4. Disconnect the power cable of the Perle IOLAN device, wait for a few seconds and then reconnect the power cable.
5. Power off and on the devices connected to the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

1.4 Bulk Notification Server

Alert Solutions Bulk Notification Device

This section provides reference and background information for integrating the Alert Solutions' Bulk Notification Device. For procedures and workflows, see the step-by-step section.

Bulk Notification is the delivery of text and voice messages to a large number of recipients. fulfills this by interfacing with a third-party vendor called Alert Solutions.



Alert Solutions' services are accessible over the Internet which can access to send messages to the intended recipients. It is the customer's responsibility to obtain the credentials necessary to access Alert Solutions' services. These credentials are entered into during device configuration, which is detailed in the later sections of this document.

If all Internet traffic is to be routed through an authenticating proxy, then the Bulk Notification Driver needs to be deployed only on the main Server and not on the Front End Processor (FEP) since there can be authentication problems when those drivers attempt to access the Internet.

Prerequisite

For Bulk Notification to deliver bulk audio, a minimum of 5Mbps download and 1Mbps upload dedicated internet bandwidth is required.

Alert Solutions' Bulk Notification Workspace

- **User Name**: Enter the user name to access the bulk provider's services. This needs to be obtained from the bulk provider.
- **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.

- **Password**: Enter the password needed to access the bulk provider's services. The password needs to be obtained from the bulk provider.
  NOTE: The Password is stored in encrypted format for security reasons.
- **Audio - Server Link**: https://weblaunch.blifax.com/PostAPI/xml/VLNew.aspx.
- **Audio - Caller ID**: Enter the phone number that needs to be displayed as the Calling Phone number when recipients receive phone calls.
- **Audio - Maximum Redial**: Enter the number of times to redial when placing voice calls.
- **Email - Server Link**: https://weblaunch.blifax.com/PostAPI/xml/EBnew.aspx.
- **Email - Display Name**: Enter the name that needs to be displayed as the sender's name in the emails that are sent out.
- **Email - Sender Address**: Enter the email address that needs to be displayed as the sender's email address in the emails that are sent out.
- **Email - Reply To Address**: This is the email address that will be used when the recipient chooses to reply to the received email. Enter a valid ID if the user's replies need to be supported.
- **SMS - Server Link**: https://weblaunch.blifax.com/postapi/xml/MLnew.aspx.
- **SMS - Short Code**: Enter the short code number to be used for SMS and MMS messages. This needs to be obtained from the bulk notification provider.

Bulk Notification Server

Configuring Message Identity

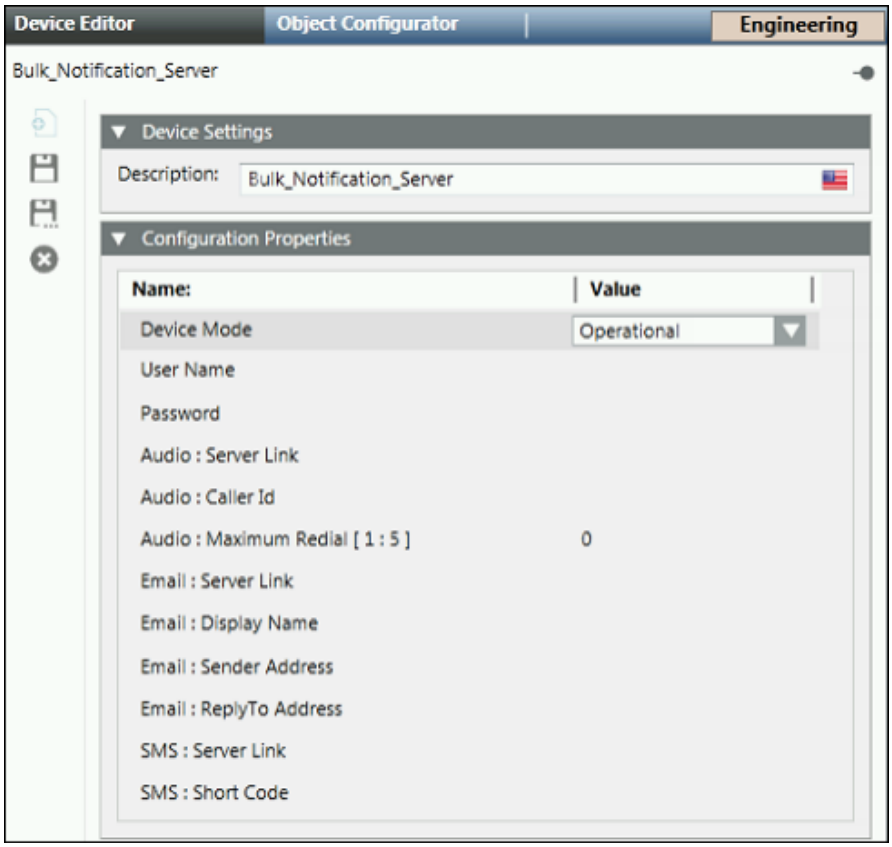
▷ A **Bulk Notification Server** is added.
NOTE: For more information on adding devices, refer to the Devices section.

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

1. In System Browser, select **Management View**.
2. Select **Project** > **Field Networks** > **Bulk Notification Server Field Network**.

3. Select the **Bulk Notification Server**.

   ⇨ The **Device Editor** tab displays.



4. Enter a valid telephone number in the **Caller Id** field.
5. Enter a valid email address in **Email : Reply To Address** and **Email : Sender Address** under the **Configuration Properties** expander.
6. Click **Save** .

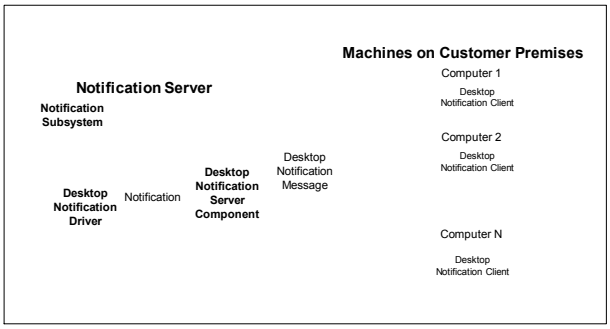
⇨ The Message Identity settings are saved.

1.5 Desktop Notification Device

Desktop Notification Device

This section provides reference and background information for integrating the Desktop Notification device. For procedures or workflows, see the step-by-step section.

The system has the capability to send desktop alerts to computers running Windows or Mac operating systems. provides this functionality by integrating with a third-party Desktop Notification system. This Desktop Notification system includes server and client components. The server component typically needs to be installed on the server, while the client components need to be installed on all computers that will receive Desktop Notifications from the system.



The Desktop Notification system also provides some functionalities that are provided by the system. However, the Desktop Notification system user interface cannot and should not be used to configure related features. The figure below gives an overview of a typical deployment of along with the Desktop Notification software.

Prerequisites

The Desktop Notification server component should be installed and the system should be functional before proceeding with the steps to configure the device into the Notification system. Refer to the Installing Alertus Software section for instructions on installation and configuration of the Desktop Notification software.

Desktop notification - Required Software

Desktop notification consists of the following components:

- **Alertus Server:** The server component that receives the messages that are displayed on a recipient's computer.
- **Alertus™ Desktop Client:** The client component that is installed on the Recipient's computer. This component connects with the Alertus Server and is responsible for displaying the messages when they are available on the server.
- For Alertus™ Desktop Client hardware requirements and key features specification, refer **http://www.alertus.com/desktop/**
- The **Alertus Server** is required to be installed on a Windows® Server 2008 R2 system. This is typically on the same system hosting the server.
  The **Alertus Server** can also be installed on a separate machine when the number of the Desktop Recipients is high (typically >1000).

Software Versions and Installer Files

The server and client components are delivered separately by Alertus. Verify that the following files are available before beginning the installation process. Using a different version may result in undefined results and the system may not work as expected.

Server Installer Files

The following files are required for installing the Alertus Server:

- **AlertusServer_5.3.8_Summer17_v3.3.170925.zip**: This archive contains the installer for Alertus server version v5.3.8 and WebApp version v3.3.170925. Extract the zip archive to a local folder before starting installation.
- **Customized_Server_Conf_Files.zip**: This archive contains alertus.keystore and Alertus.Middleware.impl.properties files. The keystore contains the license information for the server that will be issued by Alertus on purchasing the Alertus software. The AlertusMiddleware.impl.properties is a configuration file into which site specific configurations are entered. Do not extract the **Customized_Server_Conf_Files.zip** file as it will be extracted by setup and placed automatically to the respective location.
- **server.license**: A license file issued by the vendor for the desktop notification server.

Client Installer Files

The following files are required for installing the Alertus™ Desktop Client:

- **alertus-desktopalert_DotNet4.5_v4.0.5.1.msi** : This is the installer for the desktop client.
- **AlertusDesktopAlert.exe.config**: A configuration file that is deployed with the client installer. Details are explained in later sections of this document.

Desktop Notification

This section provides additional information for integrating the Desktop Notification device.

Installing Alertus Software

Manual Procedure

Use manual procedure if batch script for silent installation has not been provided by Alertus. If the silent installation scripts are available then select Server Installation - Using Silent Installer Script and follow instructions for using the silent installation scripts.

NOTE 1:

If Desktop Notification software is being installed on a machine that also runs the management station services, then the management station services need to be stopped before starting the installation process of Desktop Notification software. Otherwise, the Tomcat service which is installed as part of the Desktop Notification software fails to start.

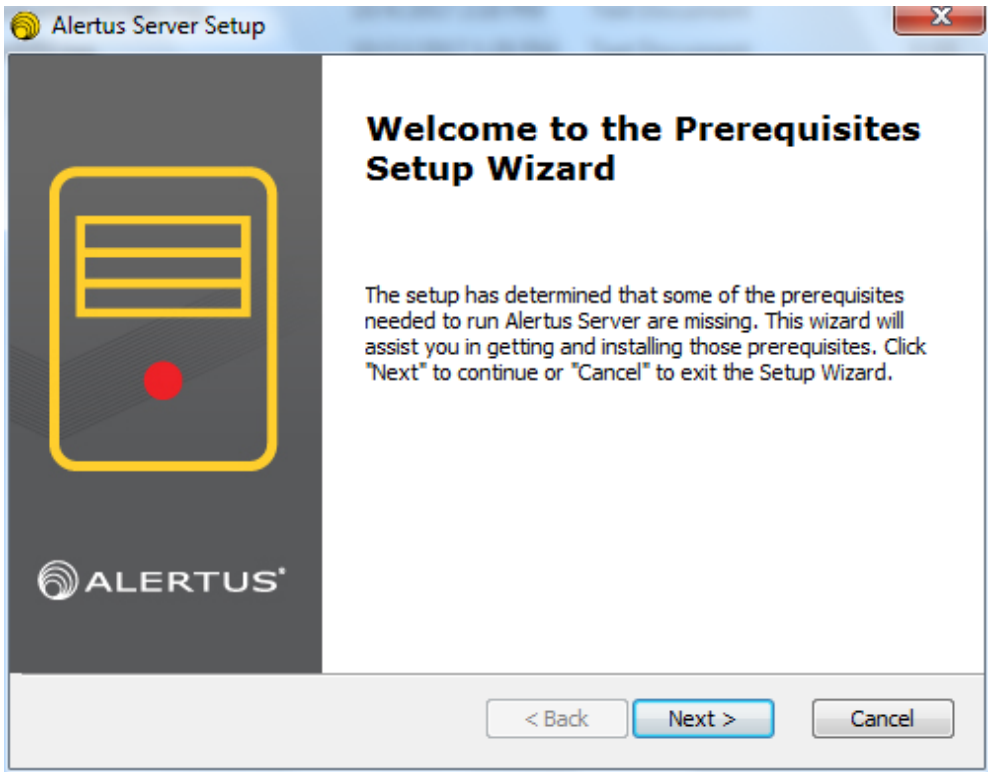
NOTE 2:

The log files created by the Apache Web Server and the Alertus software may consume significant space on the drive where the installation is performed. In order to avoid the system running into an insufficient disk space situation, the Alertus software should be installed on a drive other than the system (Windows) drive.

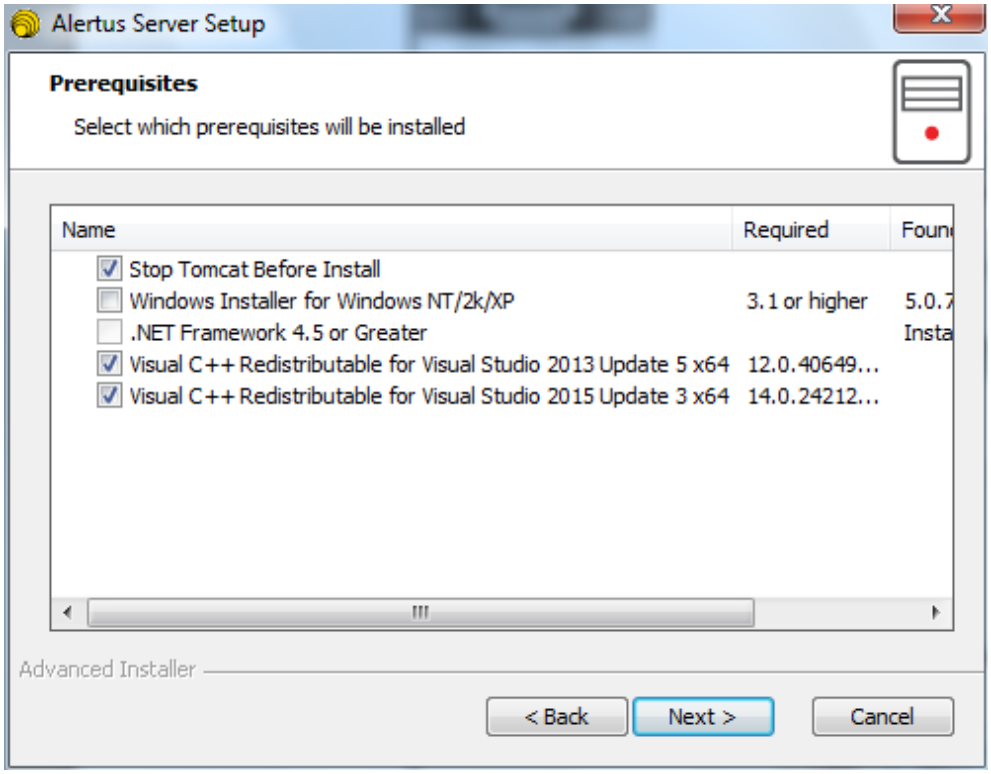
Alertus Server - Preparation

1. Extract the zip archive received from Alertus to a local folder on the machine where Alertus server components need to be installed.
   NOTE: For example, **[Installation Drive]:\Alertus-Install\AlertusServer_5.3.8_Summer17_v3.3.170925**.
2. Select the folder containing the Alertus Server installer.
3. Run the installer application **setup.exe** as **administrator**.
   NOTE: Running this installer as **administrator** is very important, or else there may be installation issues. This is typically done by right-clicking on the Install.exe file choosing **Run as administrator**.
   Enter the administrator password, if prompted.
   NOTE 1: Follow this step even when logged on as **administrator** on that machine.
   NOTE 2:The Alertus Server version displays as **5.3.8** once installed (and also during the installation).

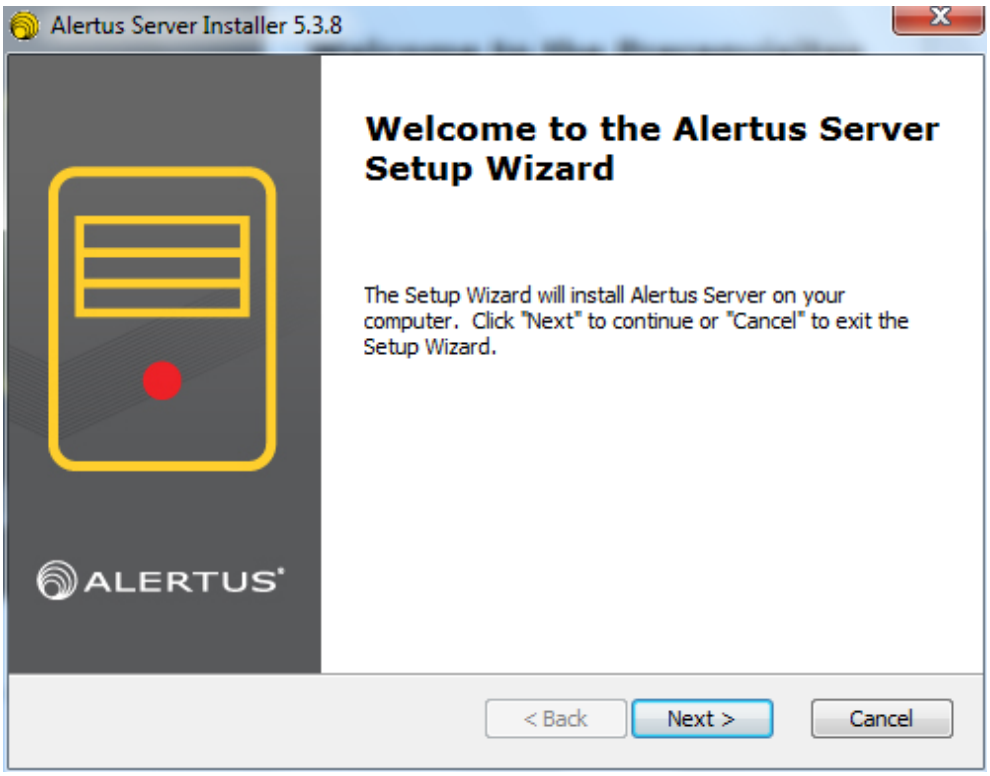
   ⇨ The Welcome to the Pre-requisites Setup Wizard message displays.



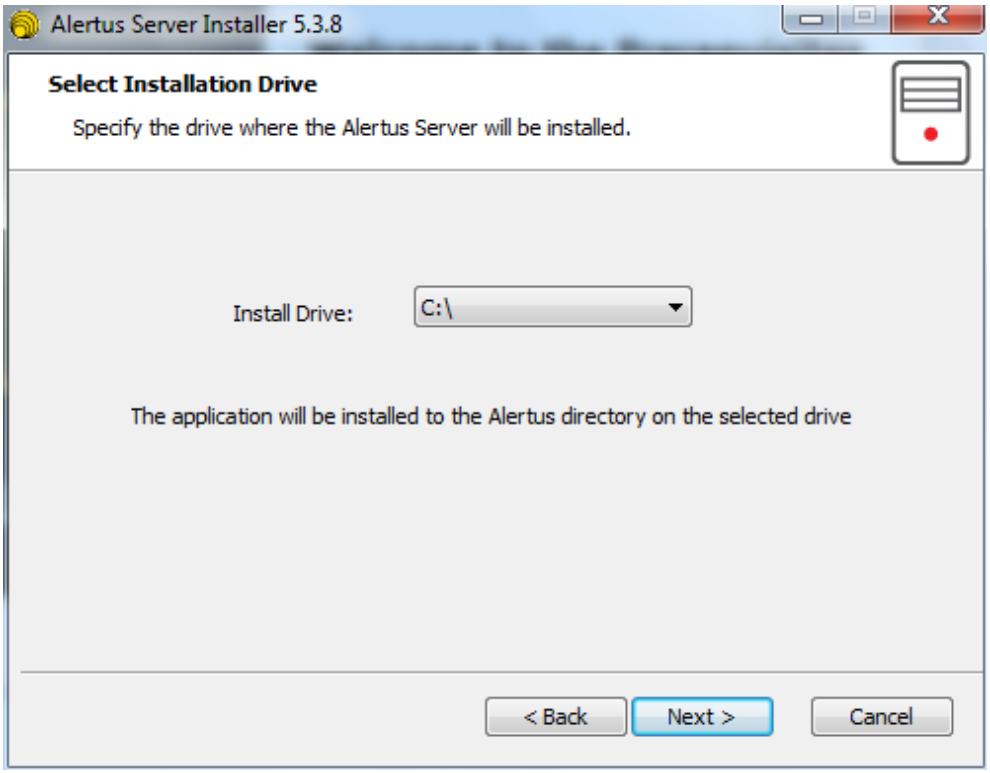
4. Click **Next**.
   ⇨ The installation drive selection dialog box displays.
5. Select the pre-requisites to be installed.



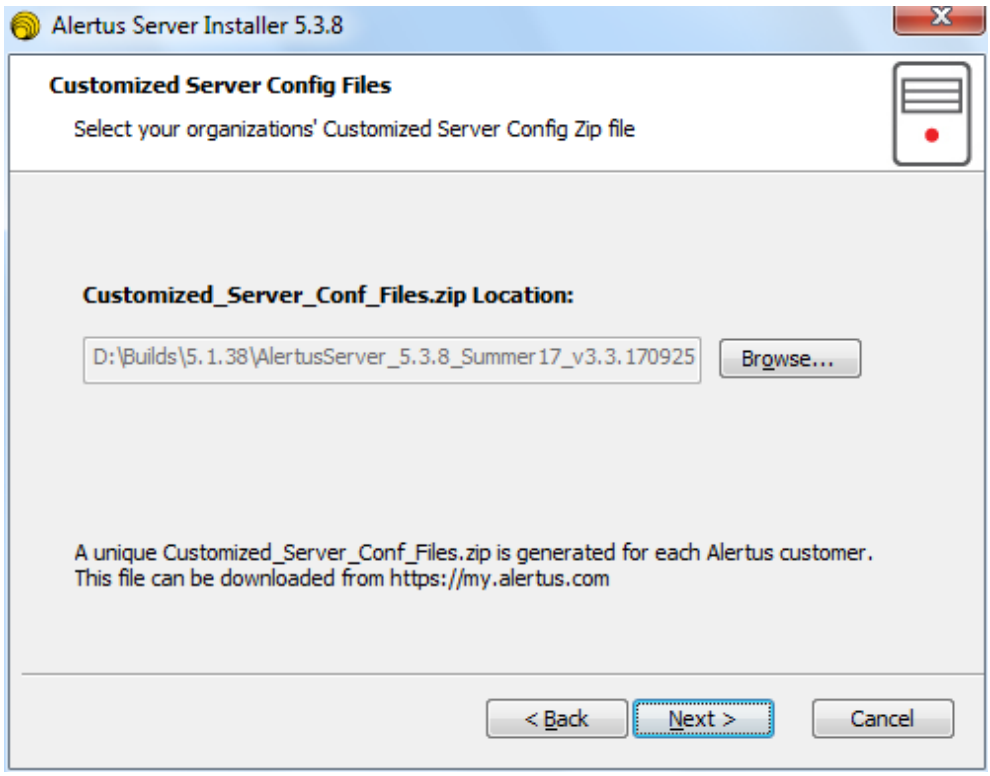
6. Click **Next**.
   ⇨ The Welcome to the Alertus Server Setup Wizard message displays.



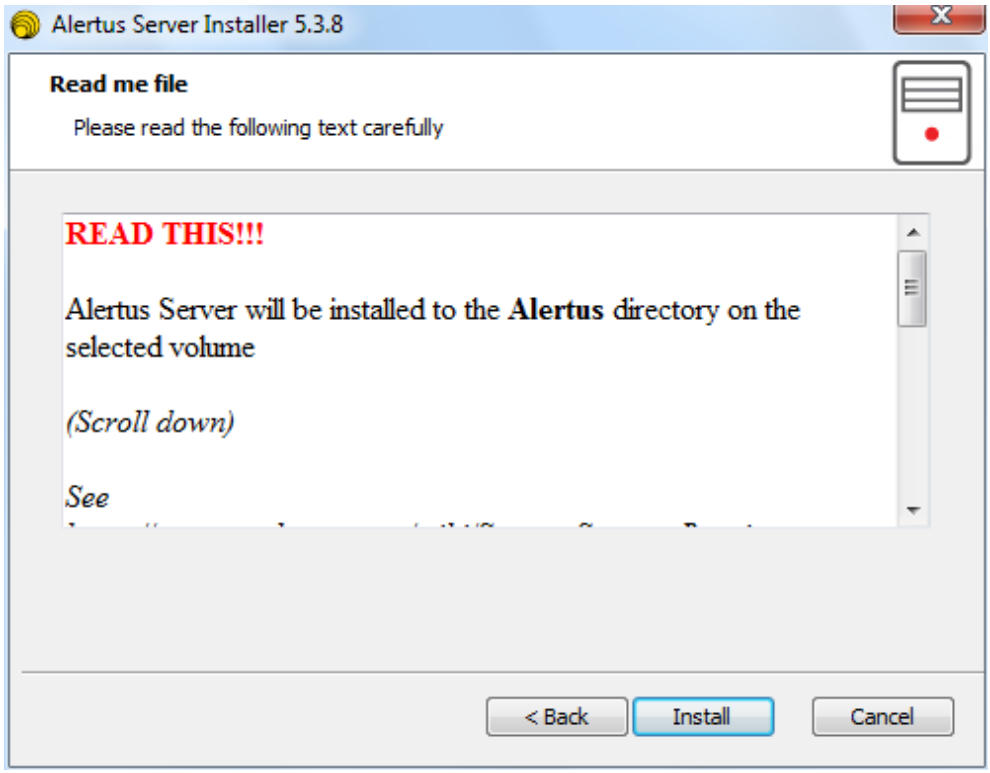
7. Select the directory for installation.



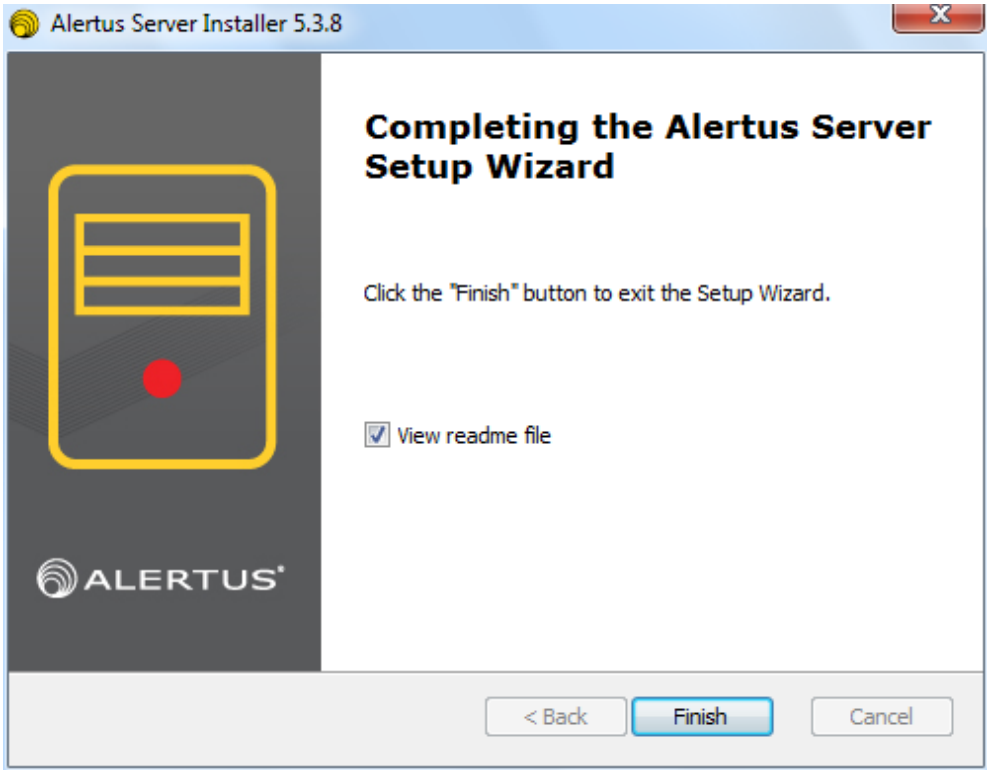
8. Click **Browse** and provide the location of the customized server config zip file.



9. Click **Next**.
10. Read the contents of **Read me file** and click **Install**.



11. After successful installation of the Alertus Server, click **Finish** to close the installation.



Alertus eEAS Server Configuration (Step 1)

1. Copy the file **server.license** to **[Installation Drive]:\Alertus\conf**.
   NOTE 1: The copy operation needs to be done manually via Windows. No separate user interface is available through the installer.
   NOTE 2: The **.keystore** file contains the license and will be given upon purchase of the Alertus software by Alertus.
   NOTE 3: The **AlertusMiddleware.impl.properties** file contains site specific configurations which needs to be modified as described in following step.
2. Using a text editor edit this file **AlertusMiddleware.impl.properties** and set the value for **organization.hostName**.
   NOTE: For **organization.hostName**, enter the IP address or the hostname of the server hosting the Alertus Server. In case of hostname, enter the server name with full domain name such as **servername.mns.net**.
3. Using a text editor edit the file **AlertusMiddleware.impl.properties** and add ::1 to **soap.alertusMiddlewareBasic.allowableIPs**.
   For example: soap.alertusMiddlewareBasic.allowableIPs = ::1;127.0.0.1

Web App Installation and Configuration (Step 2)

▷ Predetermine the ports to be used based on discussion with the customers. Contact the System Administration team on customer sites regarding port numbers assignment since there may be certain policies regarding this. After installing the Alertus server if there is a need to reconfigure the ports, follow the steps mentioned below.

1. Select **[Installation Drive]:\Alertus\webserver\conf**.
2. Using a text editor, like Notepad, open the **httpd.conf** file and navigate to the line starting with **Listen 80** (approximately line number 63), thereafter, change the numeric value to an available port number, for example, **10020.**
3. Save and close the file.

4. Open the **ssl.conf** file and navigate to the line starting with **Listen 443** (approximately line number 34), thereafter, change the numeric value to an available port number, for example, **10021.**
5. Save and close the file.
6. Select **[Installation Drive]:\Alertus\conf**.
7. Using a text editor, like Notepad, open the **impl_ssl.conf** file and navigate to the line starting with <**VirtualHost _default_:443**> (approximately line number 18), thereafter, change the numeric value to an available port number, for example, **10021**.
8. Restart the machine.
   NOTE 1:
   By default, Alertus uses port 80 for http and port 443 for ssl. Change the port numbers in the respectively named files to use the appropriate ports.
   NOTE 2:
   Some ports are reserved for specific uses. For example, port 25 is typically used for SMTP servers, port 80 for websites and so on. Be aware of this and use a port number that is generally not reserved for a different purpose. Doing so would block access to the Alertus user interface from the UI and the clients will not be able to connect to the server.
   NOTE 3:
   To avoid port conflicts between Alertus and other application running on the server, the following ports will be used by default on Alertus: port 10020 for HTTP, 10021 for HTTPS(SSL). Note that Alertus also uses ports 3306, 8029, and 8280.
   NOTE 4:
   It is recommended to use HTTPS port to connect to Notification.

Alertus Server Installation Verification (Step 3)

1. Start the Alertus website on local host from the menu **Start** > **All Programs** > **Alertus Technologies** > **Alertus Server** > **Launch Alertus activation software**.
   NOTE 1: The above menu option launches the default browser with the URL http://localhost/AlertusWeb. But if httpd.conf or ssl.conf was modified in previous steps the URL needs to be modified to get to the website. For example, http://localhost:10020/AlertusWeb. Note the use of port number 10020 in the URL. Modify the Windows shortcut menu for future use if needed.
   NOTE 2: The default browser is launched, which will connect to the website hosting the Alertus WebApp. If the connection is successful, a page asking the user to enter a user name and password appears.
   NOTE 3: In Step3 if the httpd.conf or the ssl.conf file was modified, it may be required to restart the machine before proceeding further.
2. Enter admin as the initial user name and password.
   NOTE 1: Log in with **admin** for the first time to change the credentials as required within the website.
   NOTE 2: Typically, the Alertus WebApp is not required for using the Alertus system with .
   NOTE 3: It is recommended to set a strong password for the Alertus application.
3. If there are errors reported in the browser and the Alertus WebApp remains inaccessible an do the following checks:
   a. Open the Windows Services Console by entering the command **services.msc** on the Windows command line.
   b. Check if all the services within the red box in the preceding screen capture are running. If not, try starting the service or services manually.

c. If manually restarting the service fails and reports an error, take a screen shot of the reported error and save the screen-shot for later use.
d. Restart the machine and check if the services are running.
e. Try accessing the WebApp.
NOTE: If all the highlighted services are not running, or if the website is still not accessible, it indicates an installation issue. Try installing the application again after uninstalling the Alertus software. Be sure to delete the folder **[Installation Drive]:\Alertus** after the uninstall process.

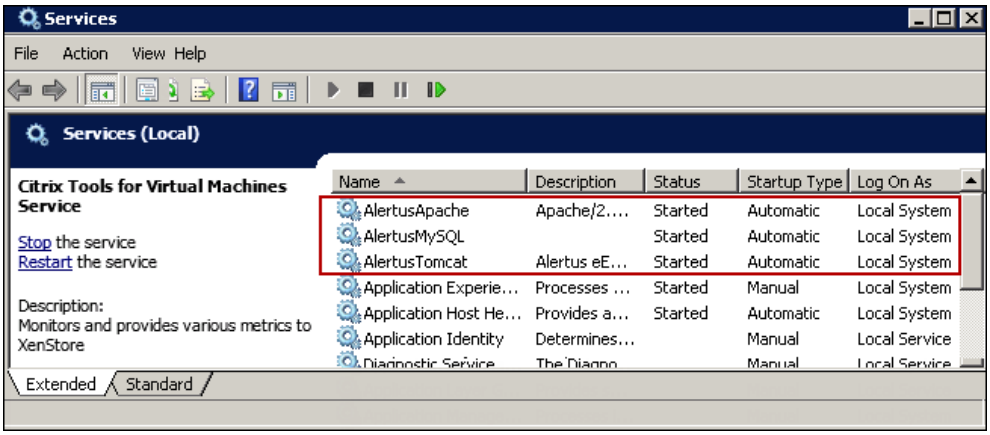


Fig. 11: Extended Services Window

NOTE 1:
Enabling HTTPS access may be required for deployment, so that communication to and from the website are encrypted. Contact Alertus for the necessary instructions. SSL certificates will be required to enable this feature. Siemens or Alertus will not supply these certificates.
NOTE 2:
Access to Alertus WebApp is not required for desktop notification features to work. Steps to access the WebApp are outlined here only to verify a successful Alertus server installation.

Installation of Alertus Server on a Dedicated Desktop Server Machine

If the **Alertus Server** is installed on a separate machine, perform the following additional steps to enable Desktop Driver to connect to the **Alertus Server**:

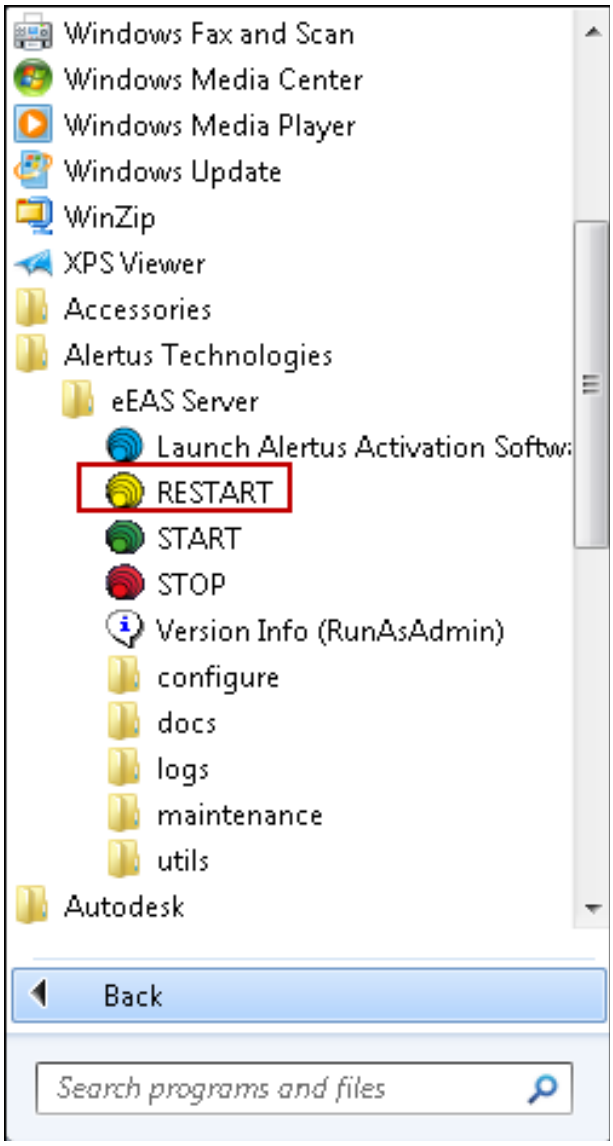
1. On the server, open **[Installation Drive]:\Alertus\conf\AlertusMiddleware.impl.properties**.
2. Locate the line starting with **soap.alertusMiddlewareBasic.allowableIPs**. This is approximately line 26.
3. After the **=** sign, enter the IP address of the machine on which the Desktop Driver is running.
   NOTE:
   To enable connection from any IP, delete all entries after the **=** sign. This improves the flexibility of the system but makes the system less secure since any system in the network is able to connect to the **Alertus Server**.

Disabling Alertus Server Logs

To disable Alertus Server logs do the following:

1. Open **[Installation Drive]:\Alertus\conf\impl_httpd.conf** in a text editor.
2. Uncomment the line, **SetEnvIf Request_URI /alertusmw/getActiveMessageForAlertDevice.jsp$ no_log** by removing the preceding **#**

3. Restart the Alertus Server by clicking **Windows Start menu** > **All Programs** > **Alertus Technologies** > **Restart**.



4. Check the latest **[Installation Drive]:\alertus\logs\apache-access.*.log** file to verify that requests are no longer being logged.

Installing Updates for Alertus Server

Follow the steps delivered with the update from Alertus.

NOTE: Only updates and versions of the Alertus softwares tested and approved by should be used.

Client Installation

Client machines receiving the notifications need to be able to access the server hosting the Alertus server.

Preparation for Windows

▷ Since the clients need to be installed on a number of machines that need to connect to the Alertus Server, perform the preparatory steps below before starting the installation of clients.

1. Deploy the DesktopAlert client installer, the associated configuration file and the optional custom logo file to a shared drive accessible from the machines where the clients will be installed.
   NOTE: This share drive does not necessarily have to be on the same machine on which the Alertus Server is installed.
2. If deploying a custom logo file, ensure that it is named **logo1.gif** and place it in the same folder as the installer and config file mentioned above. The optional custom logo must be a GIF image with a resolution of 400x100 pixels (width x height).
3. Using a text editor, such as Notepad, open the **AlertusDesktopAlert.exe.config** file (XML format).
4. Locate the tag **AlertusServerHostname**. This is approximately line 54.
5. In the following line, enter the IP address or hostname of the Alertus Server between the value tags.
6. Change the value for the tag **AlertusServerPort**, for example, **10020**. This is approximately on line 58. This will be the port number that was set in the httpd.conf file. If https access is enabled, enter the port number that was set in the ssl.conf file.

Preparation for Macs

▷ Alertus client installer for Mac is delivered via a .dmg file, for example, alertus-desktop-osx-2.9.22.706.dmg.

1. Create a share location that is accessible from all the MAC machines.
   NOTE: This share drive does not necessarily have to be on the same machine on which the Alertus Server is installed.
2. Extract the contents of the .dmg file into the share location. The .dmg file usually contains the following files:
   - **alertus-desktop-osx-x.x.xx.xxx.pkg** file which is the installer.
   - **AlertusDesktopAlert.exe.config** file which is the configuration file similar to that used with the Windows clients.
3. Modify the **AlertusDesktopAlert.exe.config** file as detailed in the Preparation for Windows section.
4. If deploying a custom logo file, ensure that the name of the logo is **logo1.gif** and place the corresponding logo in the same folder as the installer and config file mentioned above. The optional custom logo must be a GIF image with a resolution of 400x100 pixels (width x height).

Installation Steps

▷ Repeat the following steps on each machine where the client is to be installed.

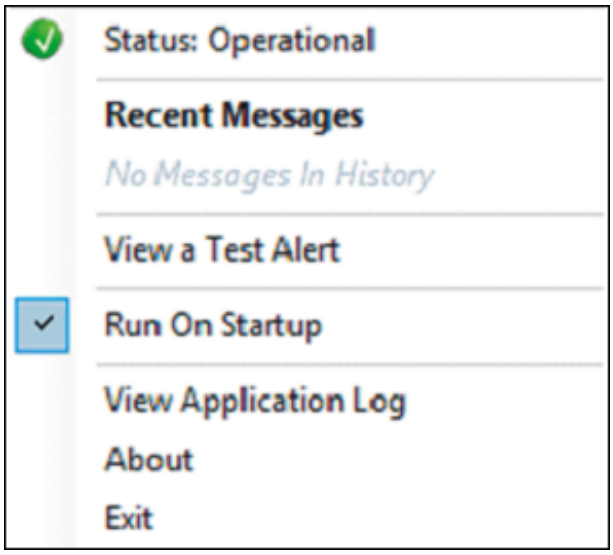
1. Select the network share location where Alertus client installer files are deployed.
2. Copy the files to a specific folder on the machine where the client is to be installed.

3. Double-click on the installer file to start installation.
   NOTE: The installer file is a .msi file for Windows and a .pkg file for Macs.
4. Follow the prompts in the user interface on the following screens to complete installation of the client.

Verifying Client Installation

▷ Once installation is complete, **Alertus Desktop Alert** is started and the icon is available in the taskbar notification area.

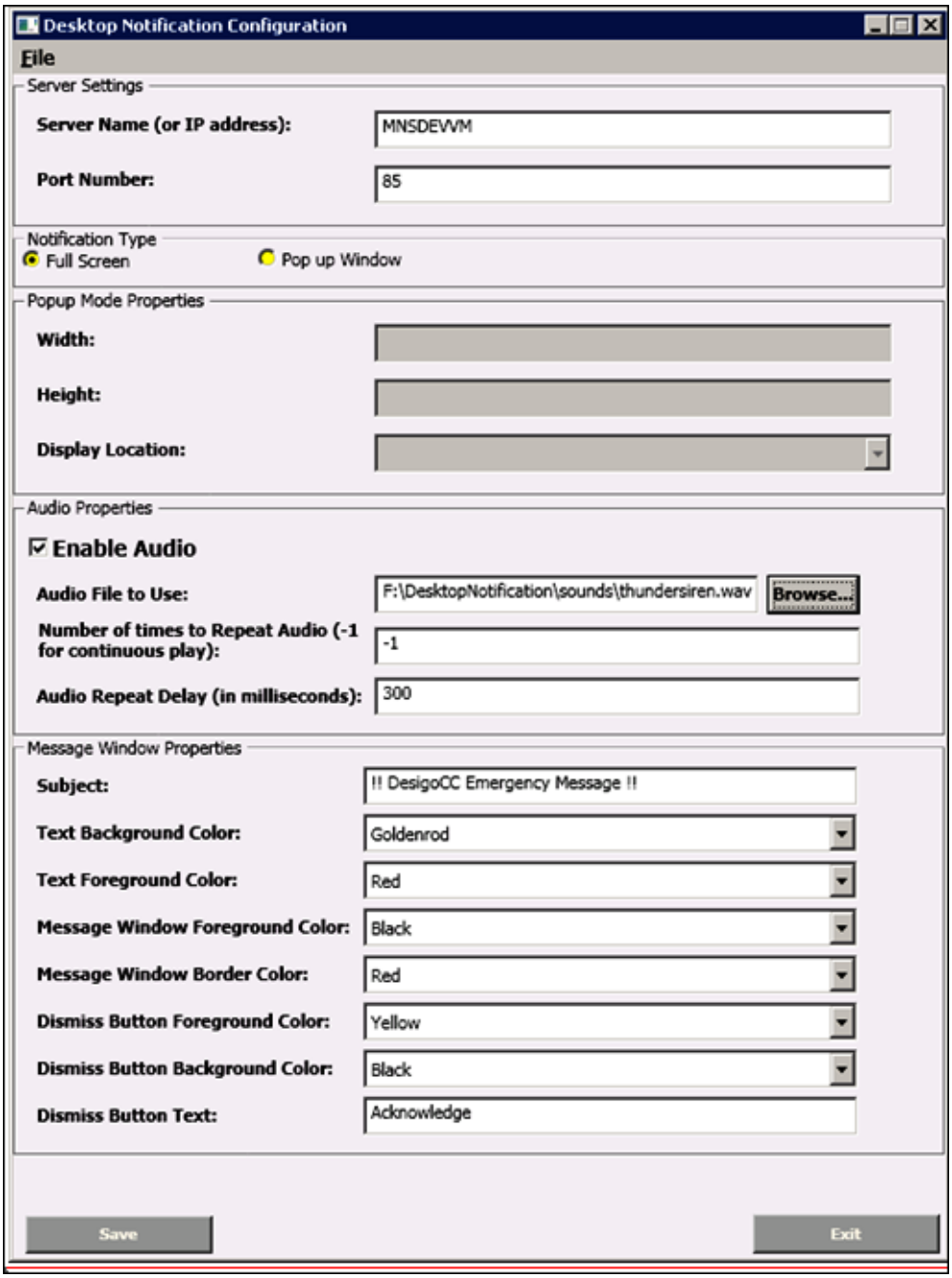
1. If the connection is successful, the icon will be displayed with a yellow color .
2. If the connection is unsuccessful, the icon will be displayed with a red color , indicating an error.
3. To enable logging, set the value of the tag **LoggingEnabled** to **true** in the **AlertusDesktopAlert.exe.config** file.
   NOTE 1: Enabling the logging can provide useful information as to why the connection failed.
   NOTE 2: Sometimes the connection to the server fails if the time on the server and the client machines are out of sync. This can be resolved by setting both machines to **sync time** from a common time server.
4. Right-clicking the icon displays the following menu.
   NOTE: The **Recent Messages** option displays messages that have not yet expired.



Creating Display Profiles

Before sending messages to the client machines, please define how the messages display on the desktop clients. The figure below gives an overview of the different configurable items of the client message.

*Fig. 12: The configuration of desktop notification messages is done through the Desktop Notification Configuration Tool on Notification server. Search **Desktop Notification Configuration Tool** from the Windows **Start** menu. Start the tool and set the different values as required.*



The table below depicts the different configurable properties of the desktop notification message.

Property	Description
Server Name (or IP Address)	Set the machine name or Alertus Server's IP address to use. The server should be accessible from the client machines using this server name or IP address.
Port Number	Select the port number to use. This would be the same port number that was set in the httpd.conf (or ssl.conf if ssl was enabled) during server configuration.
Notification Type	Select required notification type. Full screen or pop-up Window.
Width	If Popup type was selected for Notification type, set Width of the notification window. **NOTE:** Enter an integer value which is less than the width of the client systems.
Height	If Popup type was selected for Notification type, set Width of the notification window. **NOTE:** Enter an integer value which is less than the height of the client systems.
Display Location	If Popup type was selected for Notification type, select the location to display the message from the drop-down menu.
Enable Audio	Check Enable Audio, if an audio file needs to be played which the message is displayed on the client machines.
Audio File to Use	Browse and select the audio file to use. **NOTE:** Only wav files are supported. Files of smaller sizes ensure faster delivery of messages.
Number of Times to repeat Audio	Set the number of times to play the audio file. Set the value to -1 if audio needs to be played continuously.
Audio Repeat Delay	Set the delay time between successive playing of audio files. **NOTE:** A non-zero integer value must be set for time in milliseconds.
Subject	Enter the text that will appear as the subject of the message. In the above figure of the sample message this is set to !! **Emergency Message**!!.
Text background Color	Select required color from the respective drop-down menus.
Text Foreground Color	
Message Window Foreground Color	
Message Window Border Color	
Dismiss Button Foreground Color	
Dismiss Button Background Color	
Dismiss Button Text	Set the text to be displayed on the dismiss button. In the above figure of the sample message this is set to **Acknowledge**.

Once all configurations are done as detailed above, click **Save**.

- Save the profile under **[Installation Drive]:\Alertus\conf** on the server system.
  NOTE: If Alertus server is installed on dedicated server, the created profile is placed on following location:
  [Installation Drive]:\Alertus\conf on dedicated server
- Save the profile with file name **AlertusDesktopProfile1.properties**.
  NOTE 1:
  Multiple display profiles can be created with different names but the current system will use only the display profile with the name **AlertusDesktopProfile1.properties**.
  NOTE 2:

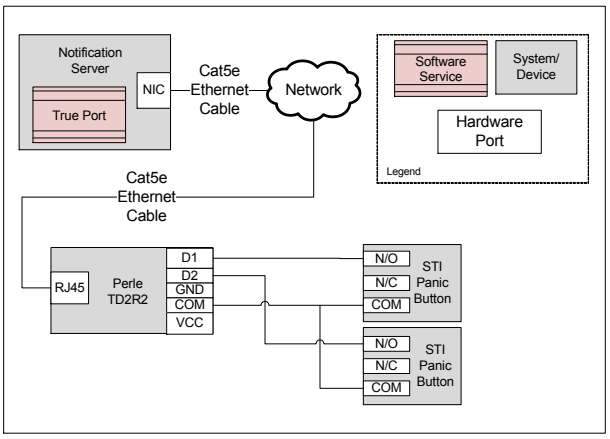
All clients connected to the Alertus server will display the message with the same profile settings.
NOTE 3:
If the user wants to use the alert sounds via the **AlertusDesktopProfile1.properties** file deployed on the server, the Audio portion of the Alert may be lost after a few messages have been sent. This will not affect the visual part of the Alert that will continue working as expected.

1.6 Digital Input Device

Digital Input Device

This section provides reference and background information for integrating the Digital Input device. For procedures or workflows, see the step-by-step section.

The STI SS-2*69E is an emergency stopper station that can be used to trigger events defined on the server. The stopper station is a push-to-activate, turn-to-reset form **C** contact. During activation, the switch closes sending a signal to the IP-to-Relay / IO device (Perle TD2R2). The server periodically monitors the Perle TD2R2 device and triggers an event if the Perle TD2R2 senses that the emergency button is closed.



Digital Input Device

This section provides additional procedured for integrating the Digital Input device.

Installing Digital Input Device

This section provides the user with information on mounting the hardware and connection details for each device.

Dry Contact Installation

The Dry Contact Installation section describes the prerequisites necessary to mount and wire the STI Emergency Stopper Station to the Perle IOLAN SDS1 TD2R2 device.

Prerequisites

The following is required prior to performing the following sections.

- STI SS-2*69E Emergency Stopper Station
- Perle SDS1 TD2R2 Ethernet I/O IP-to-Relay/IO device
- AWG copper wire

Mechanical Installation

- Follow the *Installation and Service Instructions* supplied by the manufacturer for proper mounting and wiring.

Electrical Installation

- For connectivity, uses the emergency button as a dry contact only. Connect an 18 AWG copper wire to the COM and N/O screw terminals; one on either side of the button housing.
  NOTE 1:
  Follow the manufacturer's *Installation and Service Instructions* for proper wire connections.
  NOTE 2:
  The COM and N/O wires must come from the same side. Either side of the button can be used for wiring.
- On the Perle TD2R2 device, connect the N/O wire to the D1 terminal and the COM wire to the COM terminal.
  NOTE:
  The wire length between the emergency button and the IP-to-IO device should not exceed six feet.

⚠ WARNING	
	**WARNING:** To measure inputs, requires that the input be a dry contact. Do not use high voltages on the emergency button terminals.

⚠ WARNING	
	**WARNING:** Running the wire over high voltage mains, high frequency lines, wireless appliances, or fluorescent lighting may cause interference or trigger false positives.

Installation Verification

Use an ohmmeter to measure the resistance between the N/O and COM wires. When the switch is open, the ohmmeter should show an open connection or a large resistance (several megohms). When the button is activated, the ohmmeter should measure no more than 1 Ohm resistance.

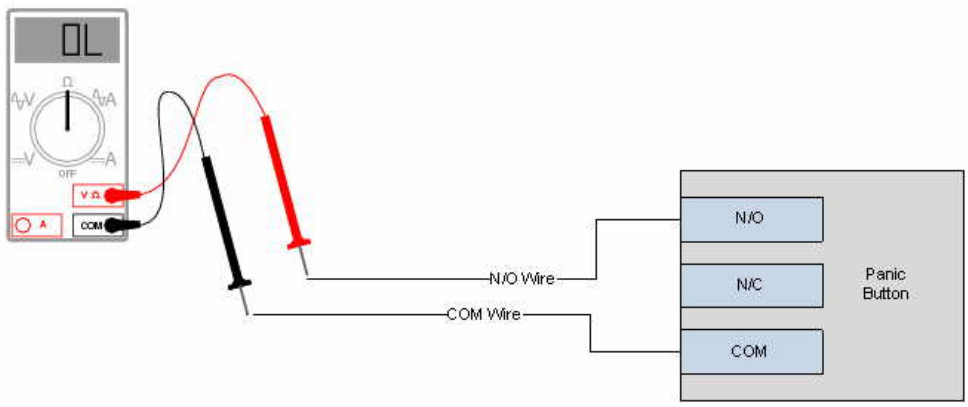


Fig. 13: Ohmmeter measuring resistance between the N/O and COM wires

Perle TD2R2 Installation

The Perle TD2R2 Installation section describes the prerequisites and steps to mount the device to a flat surface, supply power to the device, add an Ethernet network, and properly wire the device to allow a dry contact to be read.

Prerequisites

Before proceeding, ensure that the following items are available:

- Perle IOLAN SDS1 TD2R2
- 9-30VDC (400mA min) Power Supply, if not included with device
- Category 5 Ethernet cable
- Computer or Server to communicate with the device
- The device Installation CD or a computer with network access
- Hookup wire is necessary when using the I/O and relay pins
- STI emergency button, model SS-2*69E, is used in conjunction with the digital inputs

⚠ WARNING	
	**WARNING:** If configuring the Perle device for dry-contact detection, the same device cannot be used for relay control.

NOTE 1:
The driver (TruePort) that is used to communicate with the device must be installed on the same server/machine that runs .
NOTE 2:
Make sure to have an RJ45 jack available that is connected 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 connected to the same network is required.

Disclaimer:
Prior to commissioning of system, a compatibility check should be performed for all devices and services to be integrated (refer to the *Mass Notification System Description* document for compatibility information).

Mounting

The Perle SDS1 TD2R2 has two brackets on the side of the mounting holes. The installer is recommended to fasten the device to a flat surface by placing screws through mounting holes.

Power

This section describes the steps necessary to supply power to the device.

1. For the Perle TD2R2, use a power adaptor capable of 9-30VDC output and 400mA. If there is a barrel connector, cut off the connector 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** LED should be solid green.

⚠ WARNING	
⚠	**WARNING:** Connecting the power supply to the device with incorrect polarity can permanently damage the device and pose a fire risk.

Ethernet

The Ethernet section describes the steps necessary to provide ethernet network connectivity to the device.

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 the network jack.

⇨ After a few seconds, the **Link/10/100** should be solid amber or green.
NOTE1: Amber refers to a 100Mb connection. Green refers to a 10Mb connection.
NOTE2: The device does not have DHCP turned on as factory default. The user must configure the device to use DHCP or assign a static IP with a computer that is attached to the same subnetwork.

Digital Input

To measure an input, requires that the input be a dry contact. Do not use high voltages for input readings.

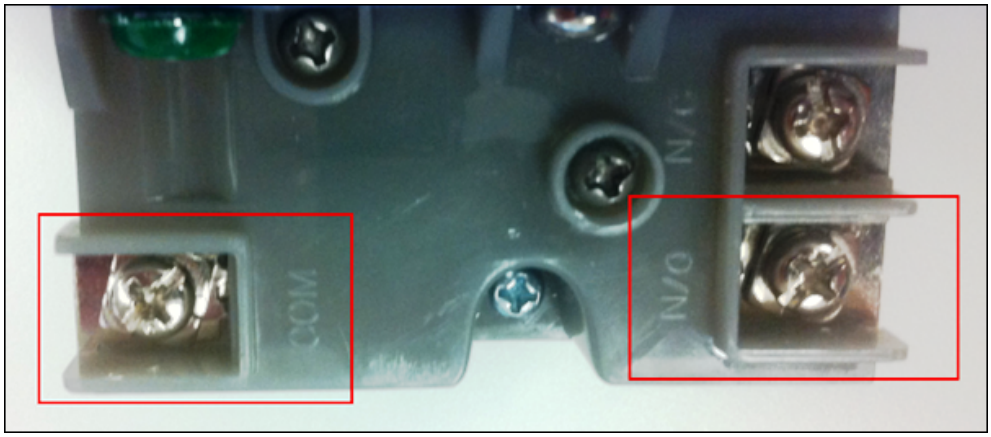
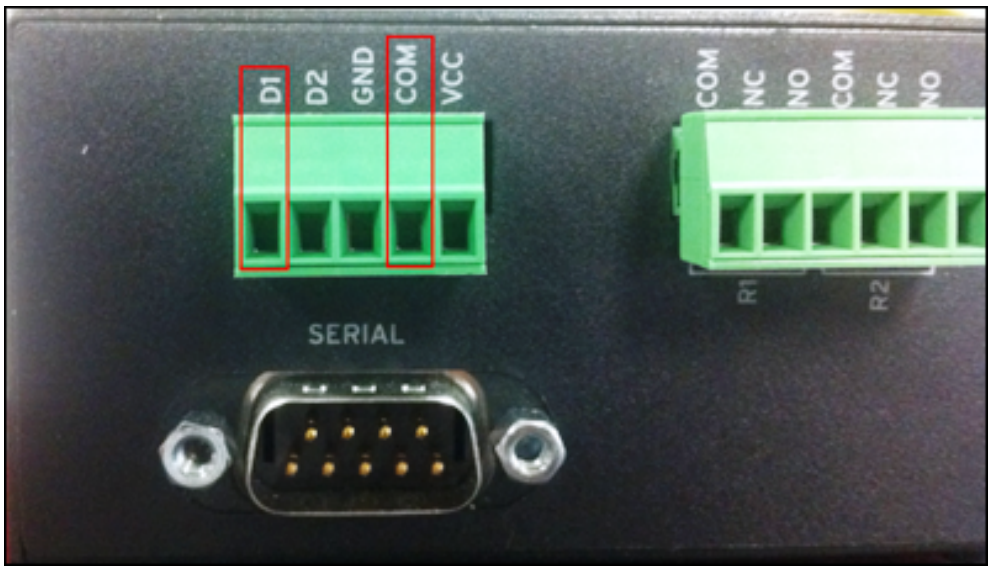


Fig. 14: Digital Input

1. On the STI emergency button, connect one piece of hookup wire to the Normally Open terminal (N/O) and another piece to the Common terminal (COM).

   ⇨ When the switch is closed, the N/O terminal will create a short with the COM terminal.



2. On the device, connect the N/O wire to the D1 terminal and the COM wire to the COM terminal.

⚠ WARNING	
⚠	**WARNING:** Emergency button wiring should be done in accordance with the electrical wiring standard for the installation region and the manufacturer's installation manual.

Configuring Digital Input Device

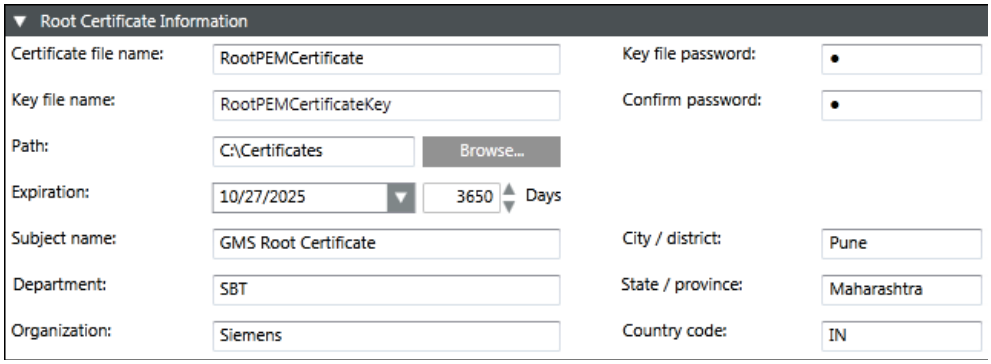
This section describes how to configure the Perle TD2R2 device.

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).

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.



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

Configuring the TD2R2 requires Perle's DeviceManager software. Install DeviceManager onto a computer that is connected to the same subnet network as the Perle device being configured.

Device Configuration for Perle TD2R2

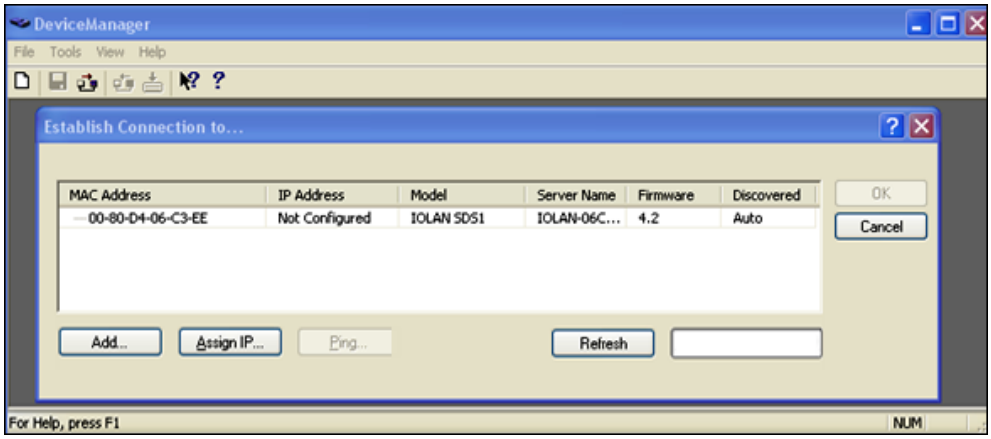
▷ Ensure that the Perle's DeviceManager software (included on the CD with the device) is installed on a computer located under the same network as the Perle device to configure.

▷ 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 Import DME File.

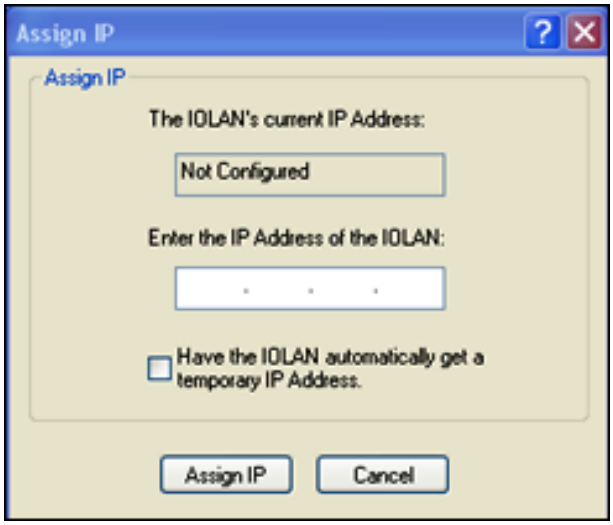
1. Start **DeviceManager**.



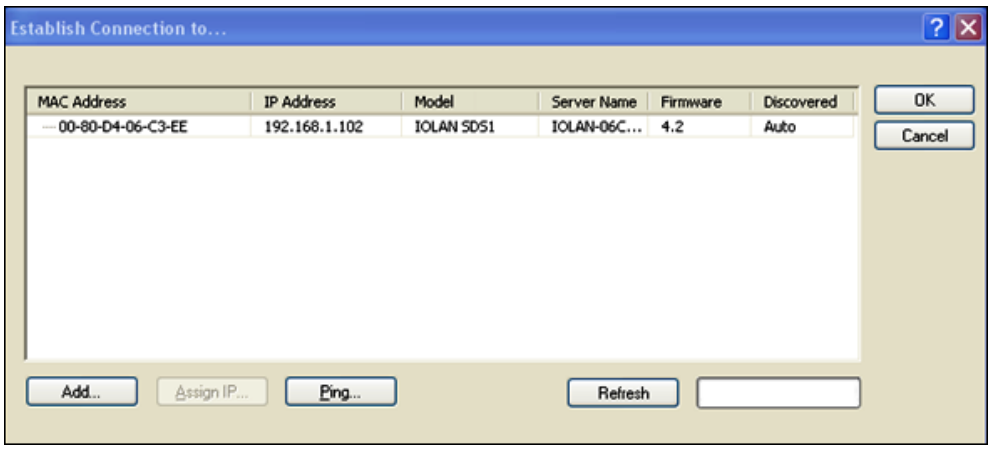
⇨ All similar devices aligned with that network will display.

2. Select the device to configure and click **Assign IP**.
   NOTE 1: If unable to see the device in the window, 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. A link LED color of amber means there is a 100Mbit network connection available. A link LED color of green means there is a 10 Mb network connection available.
   NOTE 2: If issues persist, unplug the Ethernet cable and power. Wait five 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 the reboot is 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**.



⇨ The **EstablishConnectionto** window displays with an IP address.



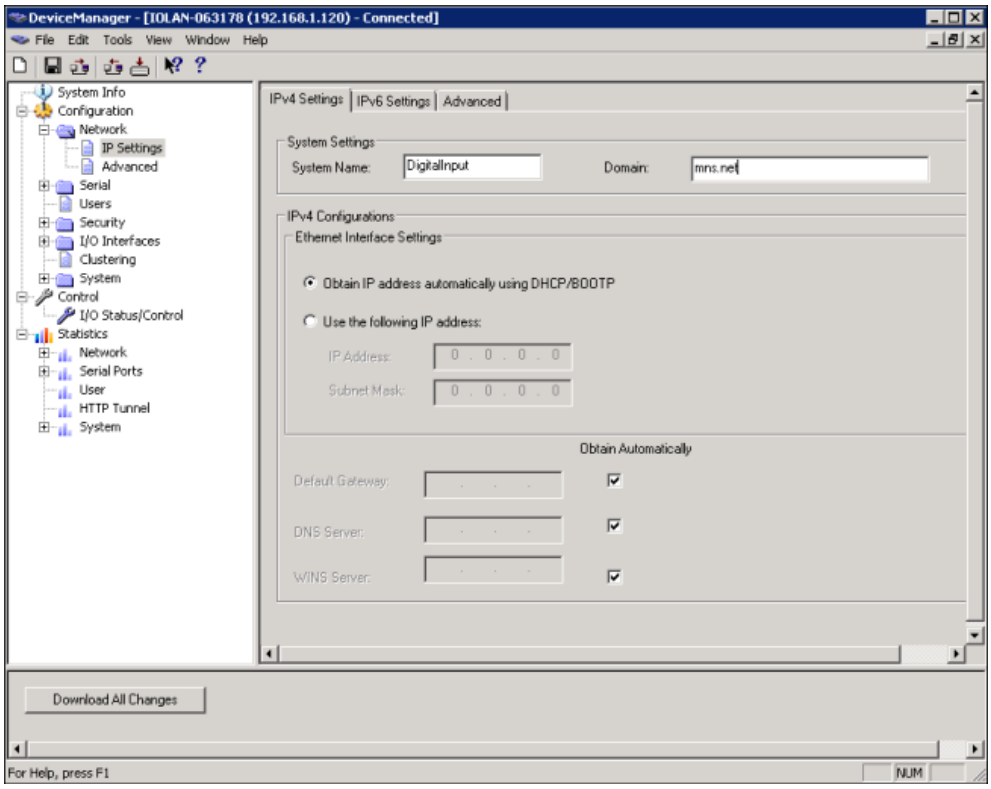
4. Select the device again, and click **OK** to log into the device for configuring.
5. At the login window, type in the device password. The factory default password is: **superuser**.

6. Click **OK**.

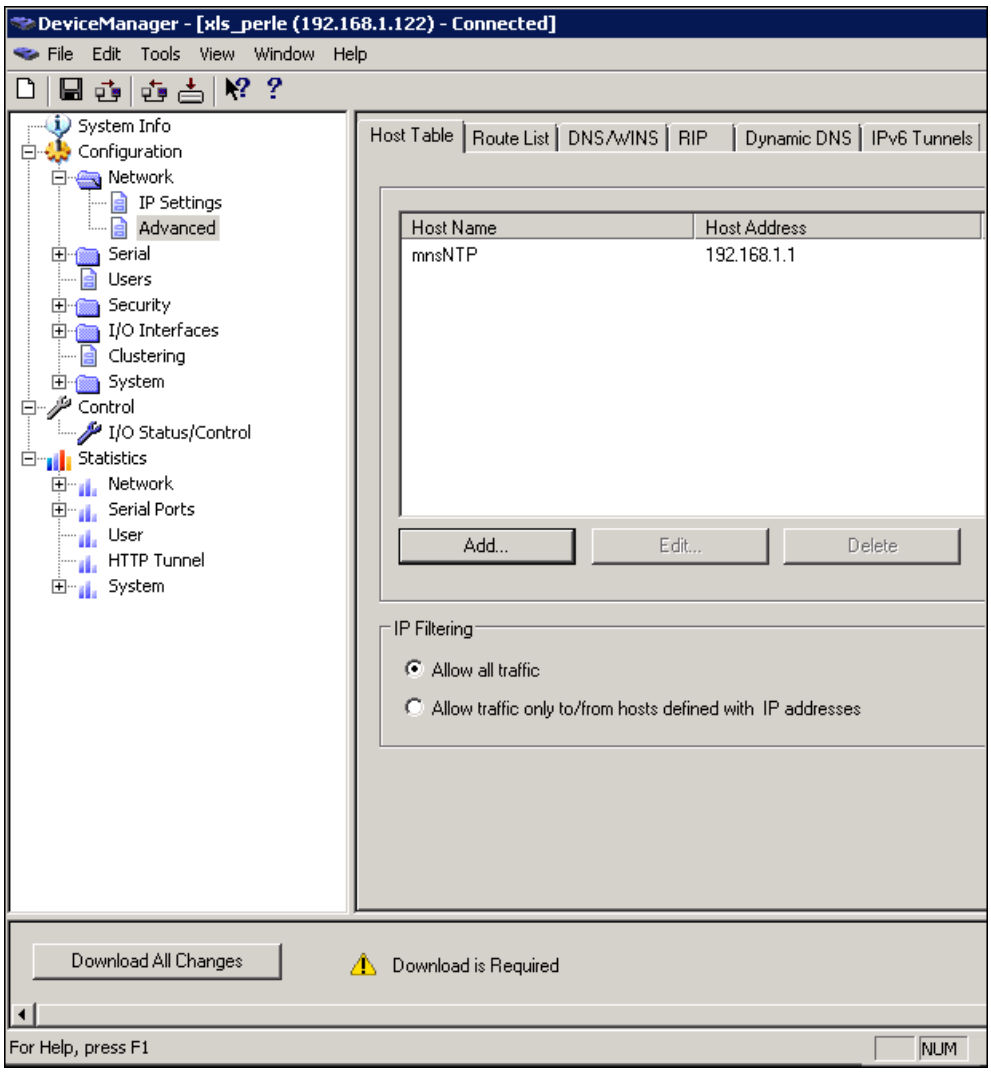
Network Setup

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

1. In the device manager window, click the **Network folder** and then **IP Settings**.
   NOTE: In this area, additional parameters can be configured for the network settings, such as configuring a **static IP address or DHCP**.



2. In the **System Name** field, enter a distinguishable name to help identify the device from similar devices.
   NOTE 1: The system name will also be used by the device to create the device's 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. Under the **Domain** field, use the domain name used on 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 domain as a parameter.
4. Select **Network > IP Settings > Advanced** tab, check the box **Register Address in DNS**.
5. Click the **Advanced** tab on the left-hand side.
6. Select the **Host Table** tab.
7. Click **Add** to add the NTP host.



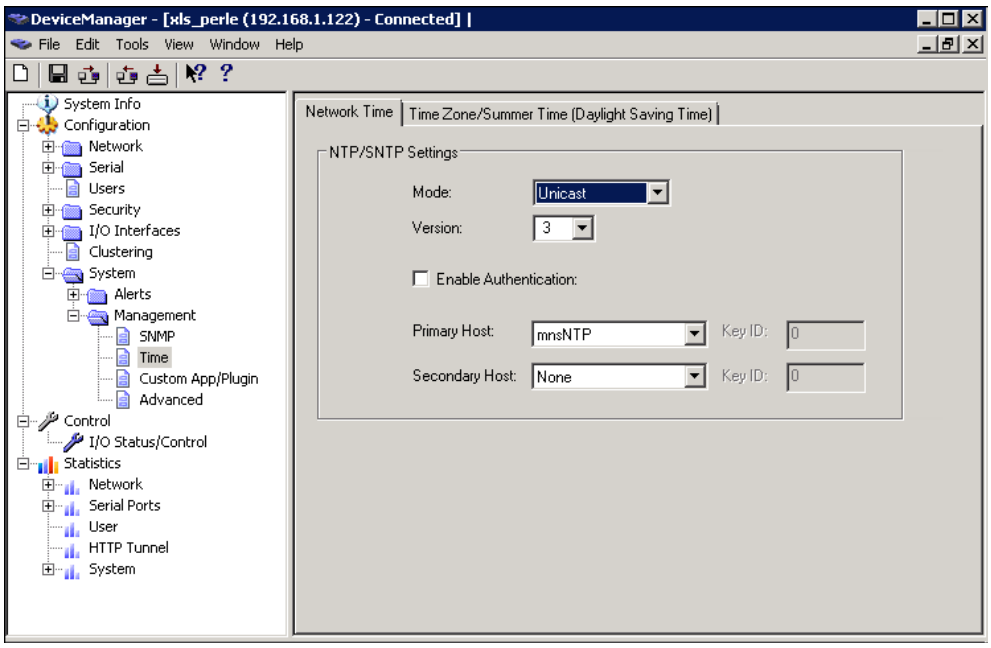
8. On the window, enter a descriptive name for the NTP server (For example, **mnsNTP**).
9. Enter the IP address or the fully qualified domain name of an available NTP server.
   NOTE: An available NTP server is required to enable SSL on the device.
10. Click **OK**.

Time and Security Settings

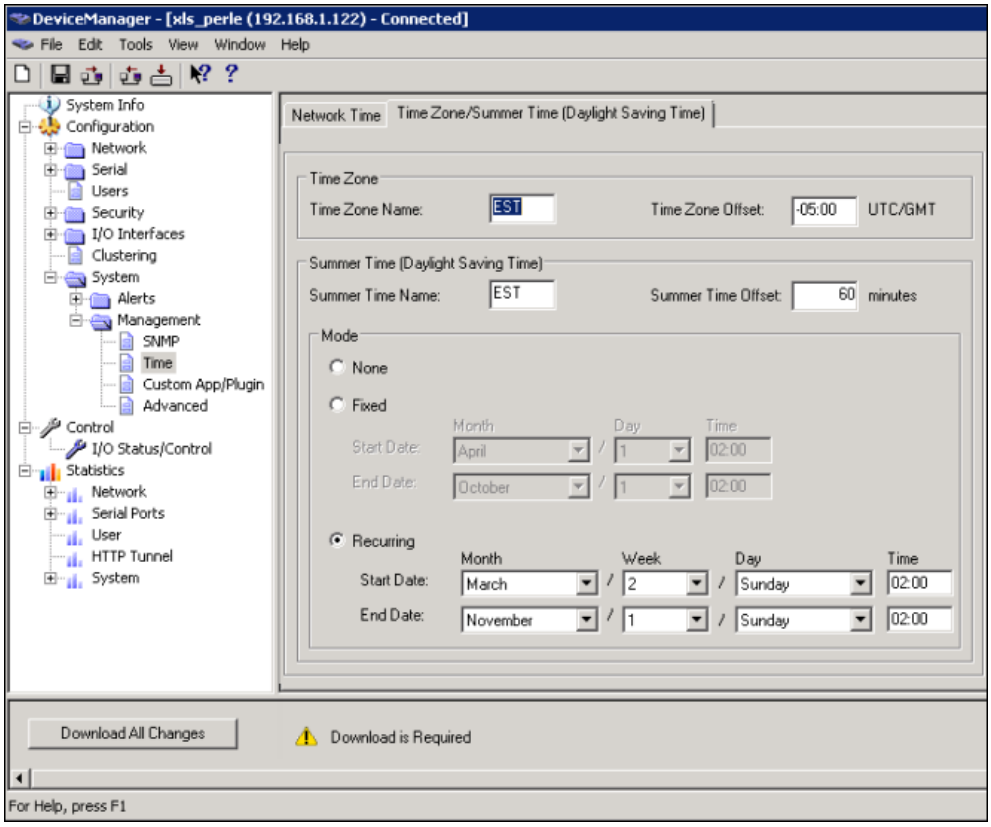
▷ The user must have logged in to the device using DeviceManager.

1. Select **Configuration > System > Management > Time**.
2. Select the **Network Time** tab
3. Do the following parameter settings:
   - **Mode**: Unicast
   - **Version**: 3
   - Leave the **Enable Authentication** check box cleared.
   - **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

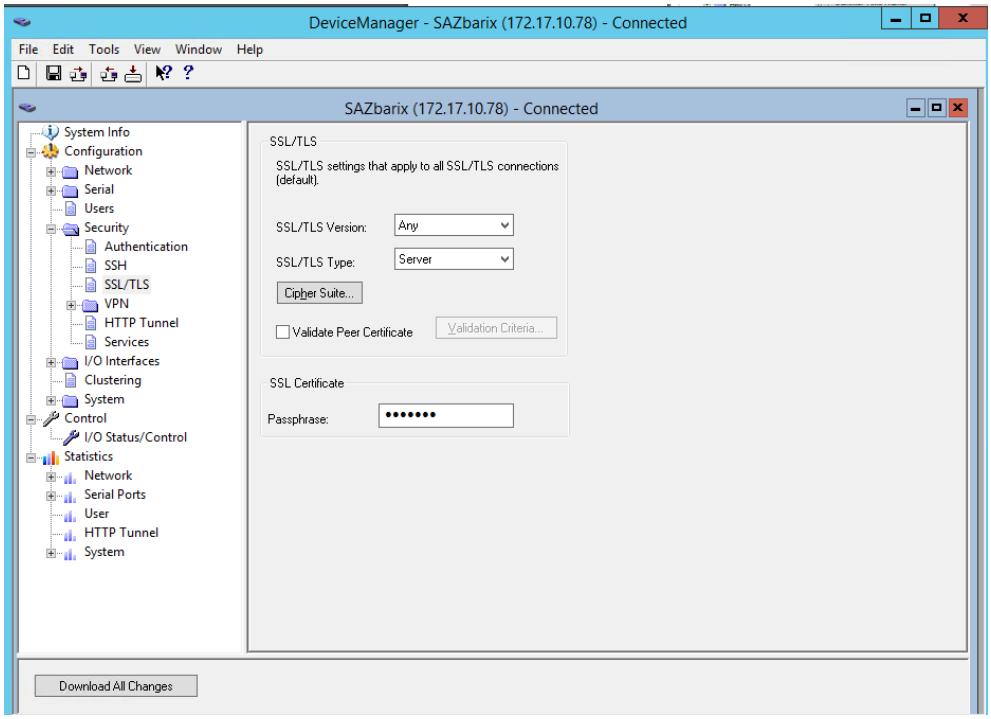
server. Windows time servers generally default to Version 2. External NTP servers generally work with Version 3. If unsure, verify with the client's network administrator.



4. Select the **Time Zone/Summer Time (Daylight Saving Time)** tab.
5. Configure the parameters using the details mentioned in Time Zone/Summer Time (Daylight Saving Time) parameters.

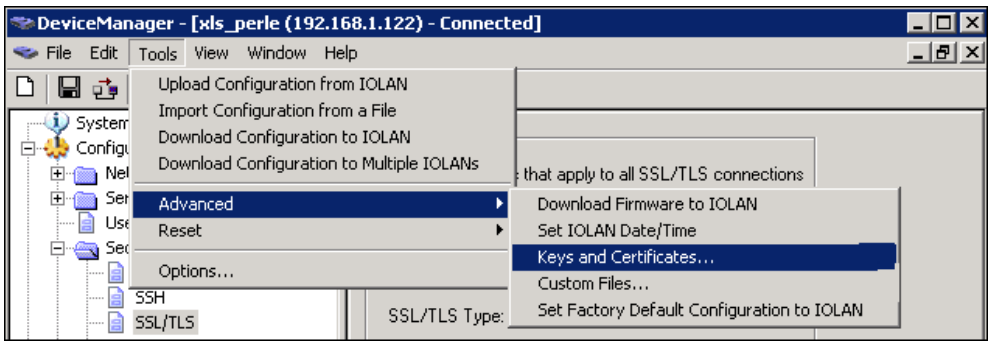


6. Select **Configuration>Security>SSL/TLS**.

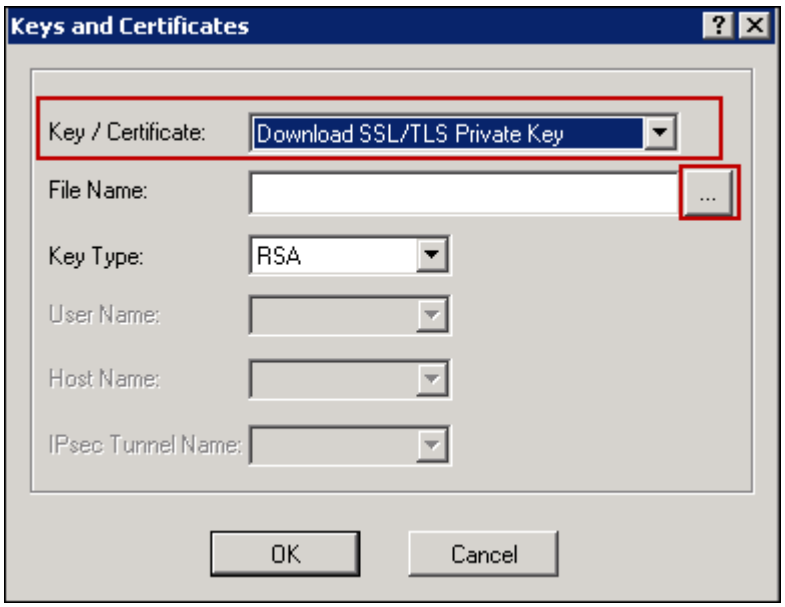


7. Set **SSL/TLS Version** field to **Any**.
8. Set **SSL/TLS Type** field to **Server**.
9. Under **SSL Certificate** section, enter the password of the SSL certificate in the **Passphrase** field.
10. Select**Tools > Advanced > Keys and Certificates**.

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



11. Under **Key/Certificate**, select **Download SSL/TLS Private Key**.
12. Click the browse button and upload the private key for the Root certificate (pem).
13. Click **OK**.



14. Select **Tools > Advanced > Keys and Certificates**.
15. In the **Key/Certificate** drop-down list, select **Download SSL/TLS Certificate**.
16. 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.
17. Click **OK**.
18. Select **Tools > Advanced > Keys and Certificates**.
19. In the **Key/Certificate** drop-down list, select **Download SSL/TLS CA**.
20. Click the browse button and upload the Root certificate (RootCertificate.pem file).
21. Click **OK**.

Time Zone/Summer Time (Daylight Saving Time) Parameters

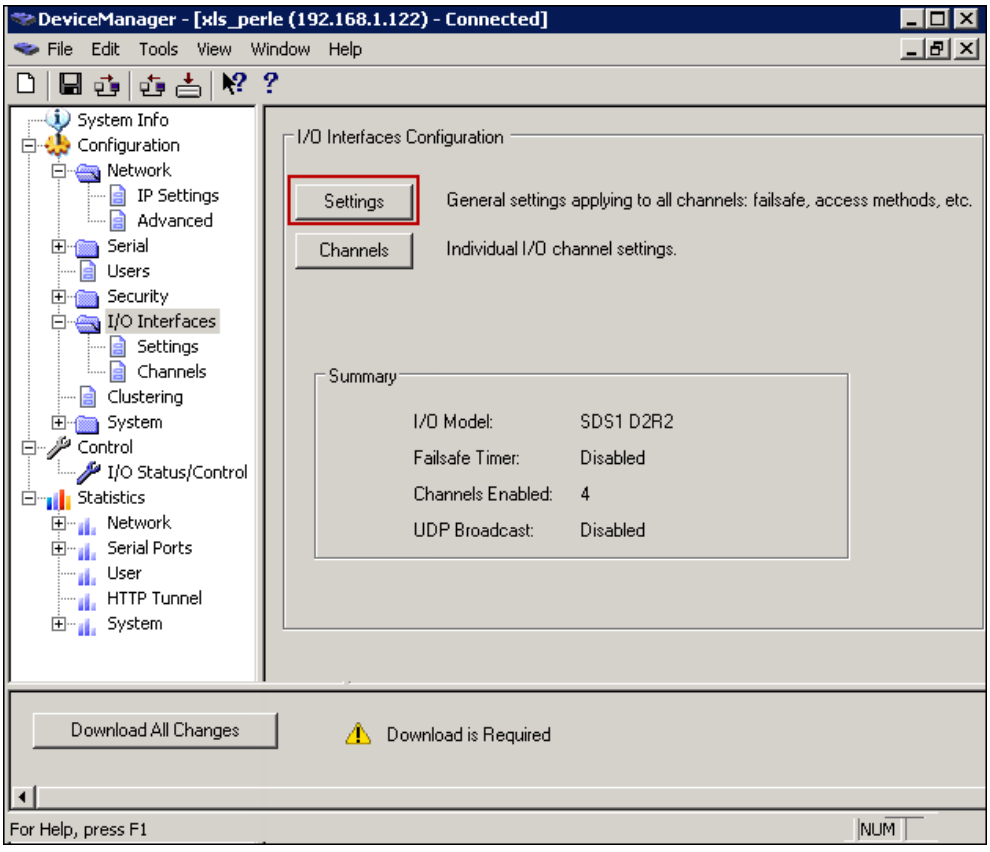
Field	Description
Time Zone Name	The name of the time zone to be displayed during standard time. **Field Format**: Maximum four characters and minimum three characters (do not use angle brackets <>)
Time Zone Offset	The offset from Coordinated Universal Time (UTC) for the local time zone. **Field Format:** Hours *hh* (valid -12 to +24) and minutes *mm* (valid 0 to 59 minutes)
Summer Time Name	The name of the configured summer time zone; this will be displayed during the summer time setting. If the parameter is not set, then the summertime feature will not work. **Field Format:** Maximum four characters and minimum three characters (do not use angle brackets <>)
Summer Time Offset	The offset from standard time in minutes. Valid values are 0 to 180. **Range:** 0-180 **Default:** 60

Summer Time Mode	Configure the summer time to take effect. **None**: No summer time change **Fixed**: The summer time change goes into effect at the specified time every year. For example, April 15 at 1:00 P.M. **Recurring**: The summer time change goes into effect every year at the same relative time. For example, on the third week in April on a Tuesday at 1:00 P.M. **Default**: None.
Fixed Start Date	Sets the exact date and time in which the IOLAN's clock will change to summer time (daylight saving time) hours.
Fixed End Date	Sets the exact date and time in which the IOLAN's clock will end summer time hours and change to standard time.
Recurring Start Date	Sets the relative date and time in which the IOLAN's clock will change to summer time (daylight saving time) hours. Sunday is considered the first day of the week.
Recurring End Date	Sets the relative date and time in which the IOLAN's clock will end summer time hours and change the standard time. Sunday is considered the first day of the week.

I/O Access Settings

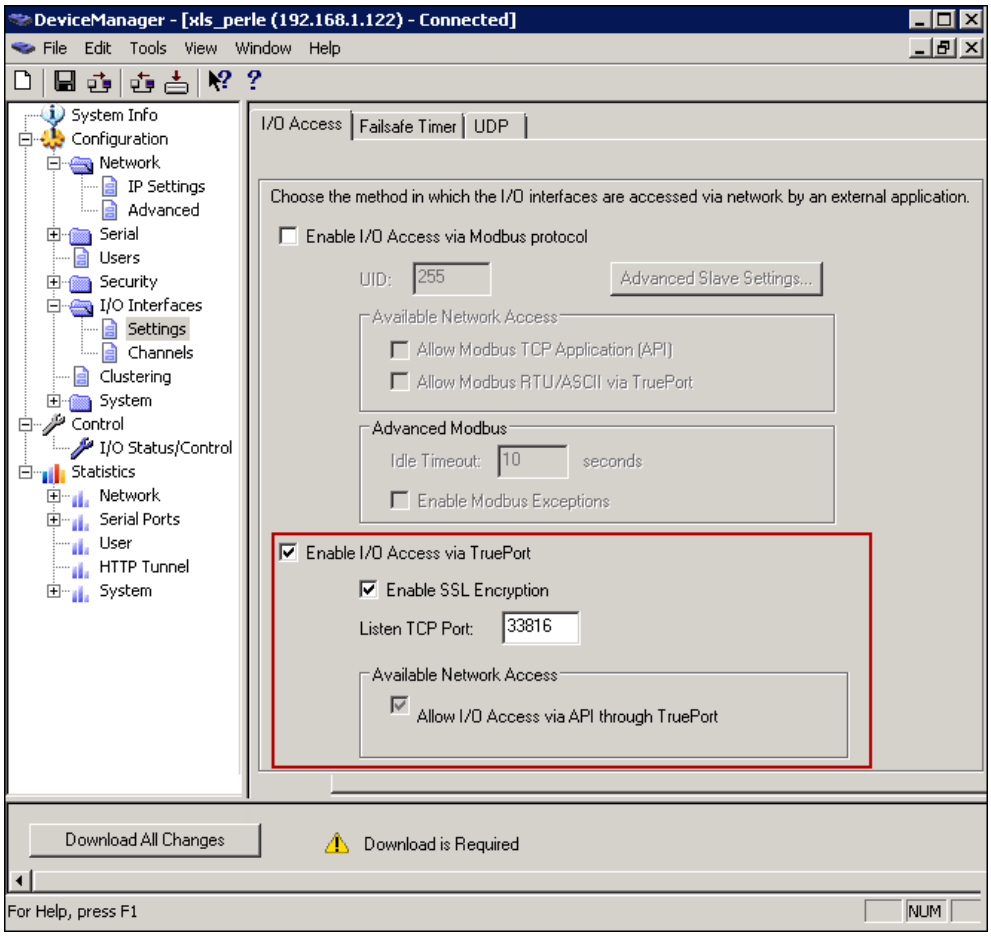
▷ The user must have logged in to the device using DeviceManager.

1. In the DeviceManager window, select **I/O Interfaces** on the left-hand side.
2. Click **Settings**.

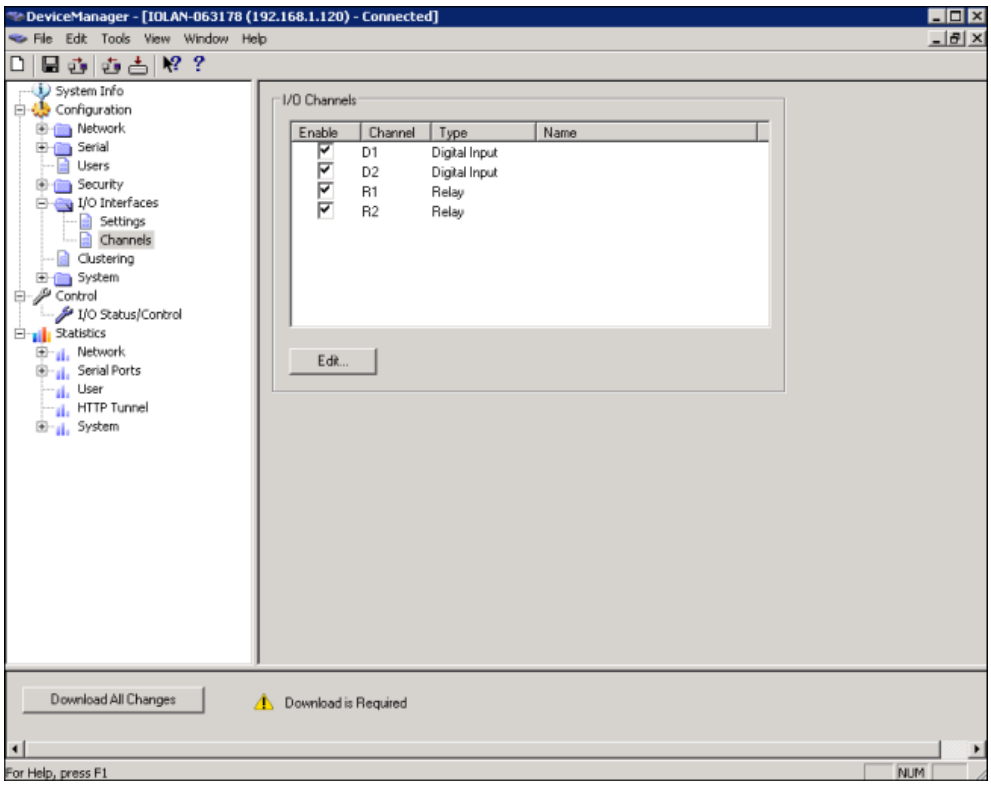


3. Select the **I/O Access** tab.

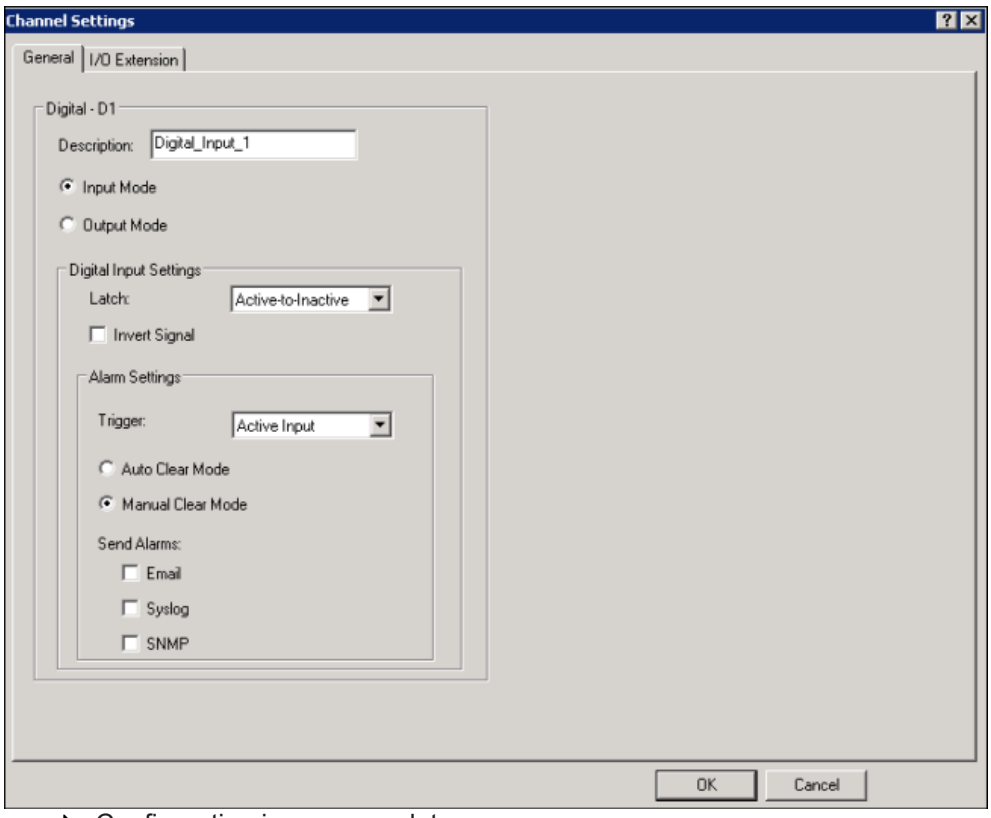
4. Select the **Enable I/O Access via TruePort** check box.
   NOTE 1: By default, the device listens to I/O commands on TCP port 33816. The I/O TCP port can be changed, as long as the change does not conflict with other services or TruePort ports.
   NOTE 2: Always check to make sure the port selected 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.



5. Select the **Enable SSL Encryption** check box.

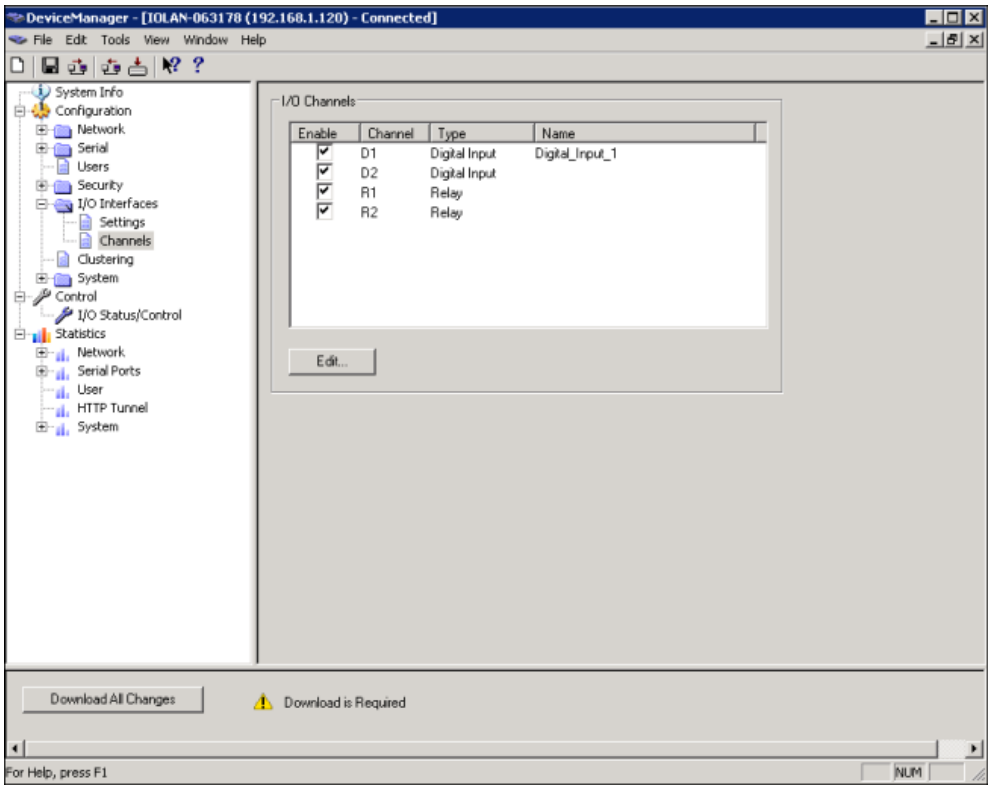


6. Select **I/O Interfaces > Channels**.
7. Select the digital input to use and click **Edit**. The configuration is the same for both inputs.
8. Give the input a **Description** name.
9. Verify that **Input Mode** is selected.
10. Under the **Latch** setting, select **Active-to-Inactive**.
11. Select **Trigger**.
    a. Select **Active Input**.
    b. Make sure **Manual Clear Mode** is selected.
12. Click **OK**.



⇨ Configuration is now complete.

13. Click **Download All Changes** to make the changes to the device or continue with other settings.

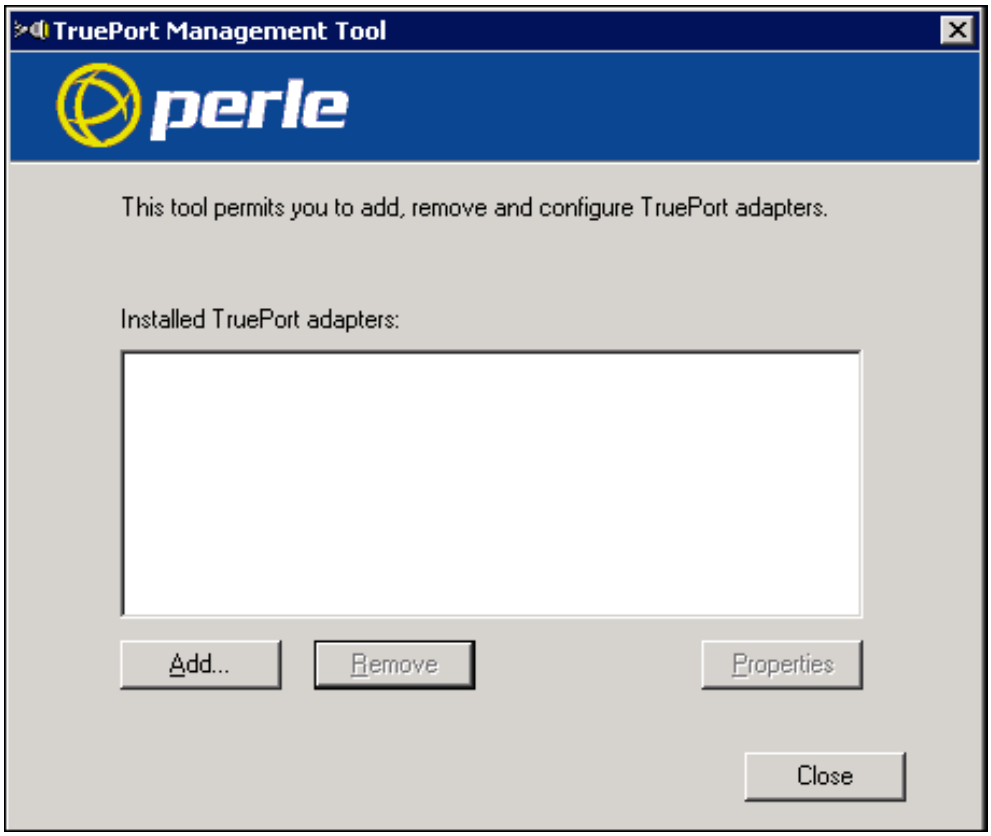


14. Click **Reboot IOLAN**.
NOTE: Any time you reboot the device, or power is reconnected, wait 90 seconds for the device to reboot and initialize. When the device is ready, the Power LED will be solid green and the Link LED will be solid amber or green.

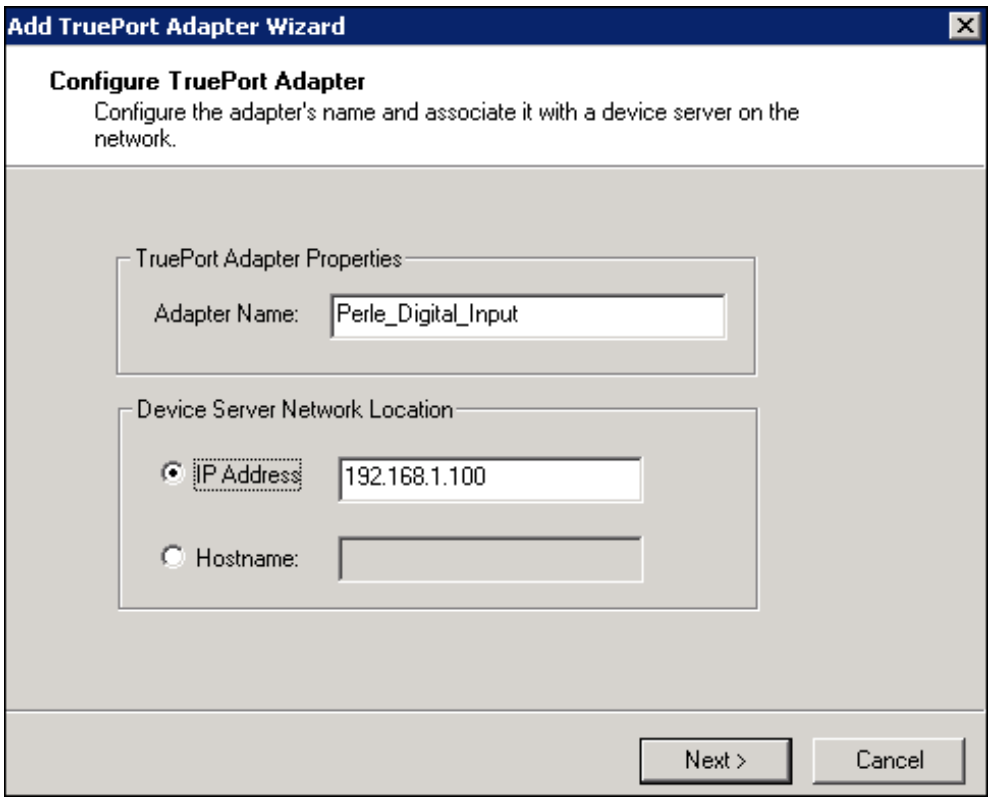
TruePort Driver Configuration

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, each device is recommended to have its own and 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.

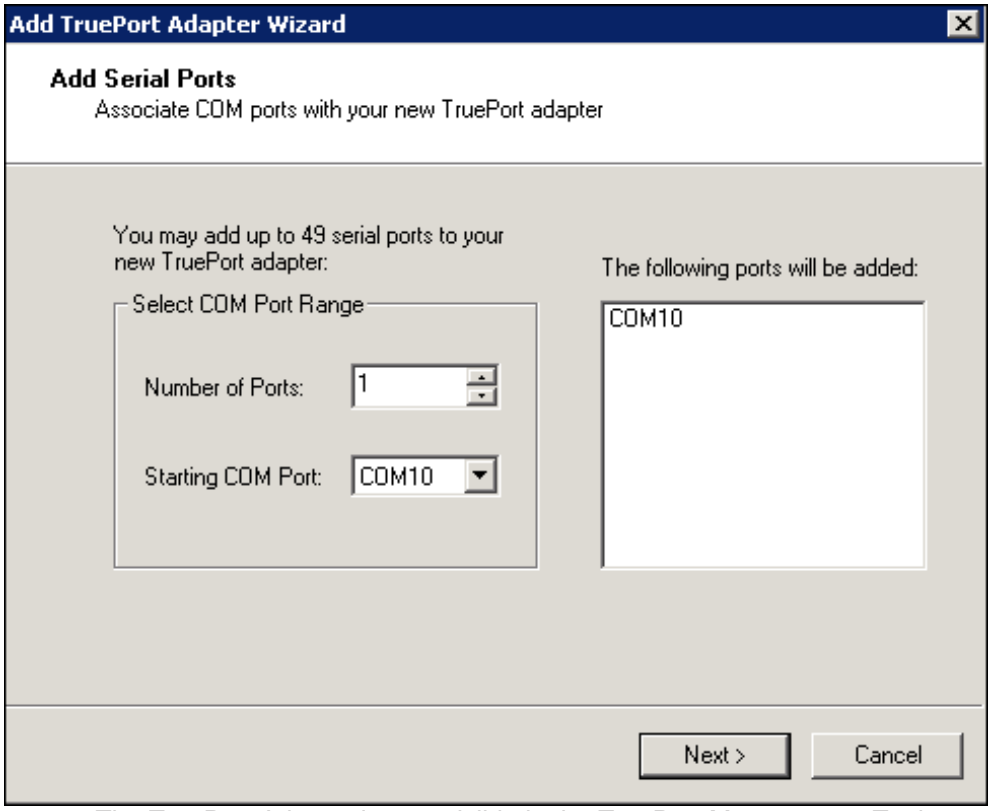
1. Install TruePort on the server.
2. Start the **TruePort Management Tool**.
3. At the management window, click **Add**.



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, then click **Next**.



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 the user to create up to 4,096 COM ports.
7. Click **Next**.



⇨ The TruePort Adapter is now visible in the TruePort Management Tool.

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

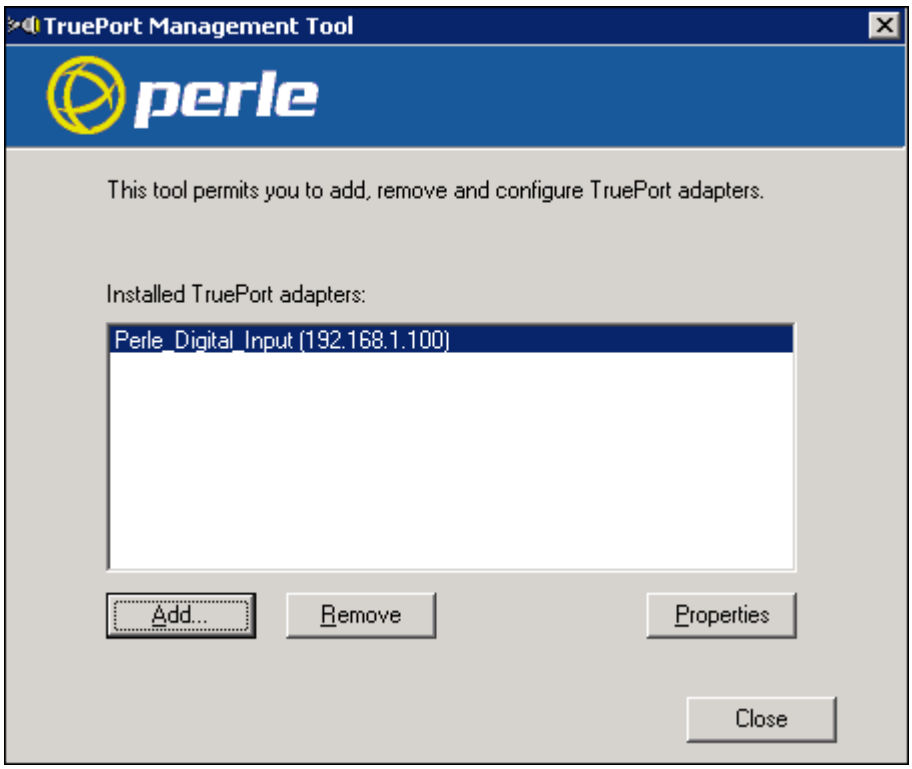
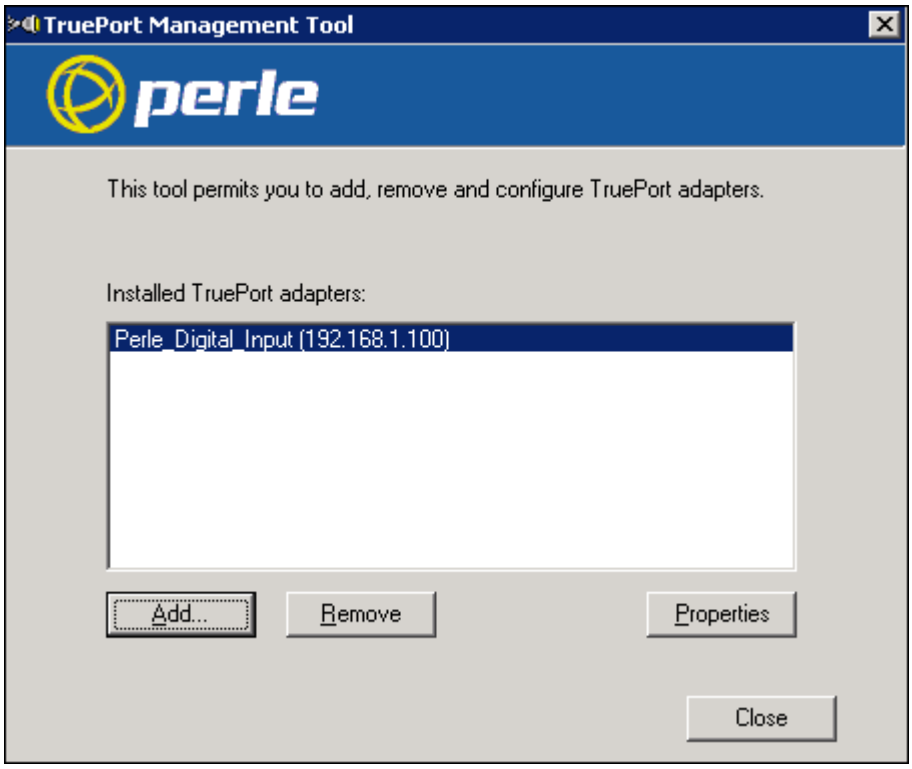


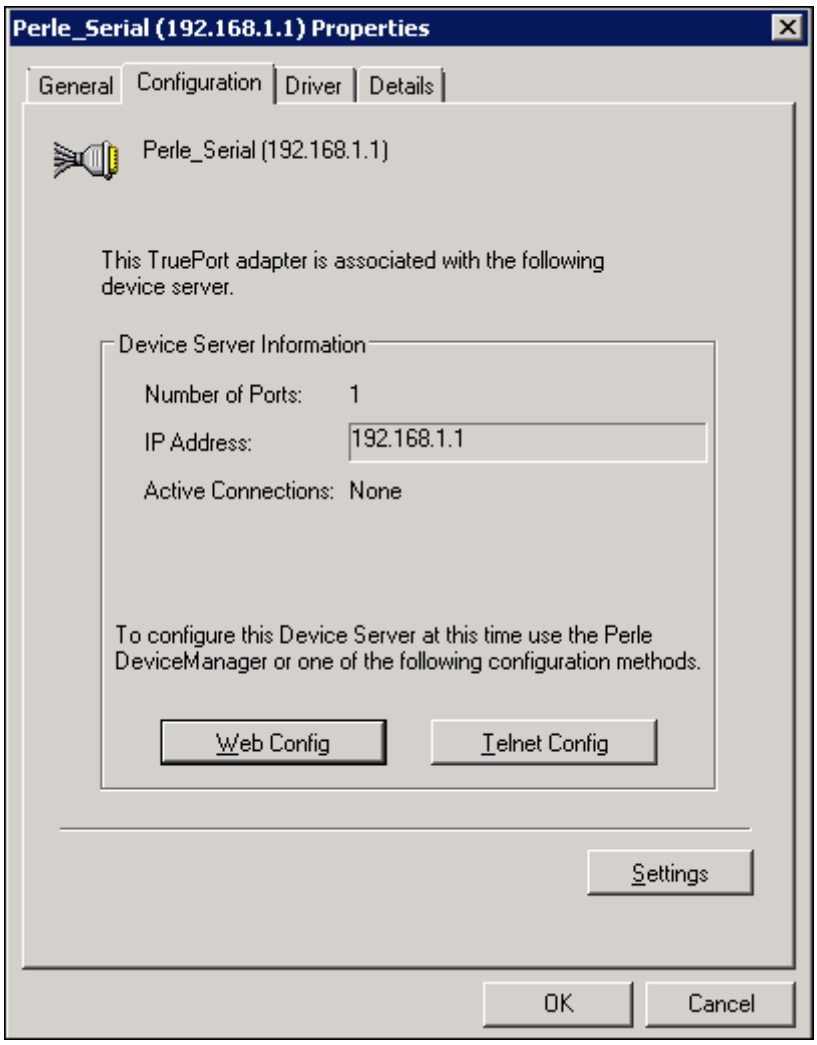
Fig. 15: Installed TruePort adapters

I/O Access Settings

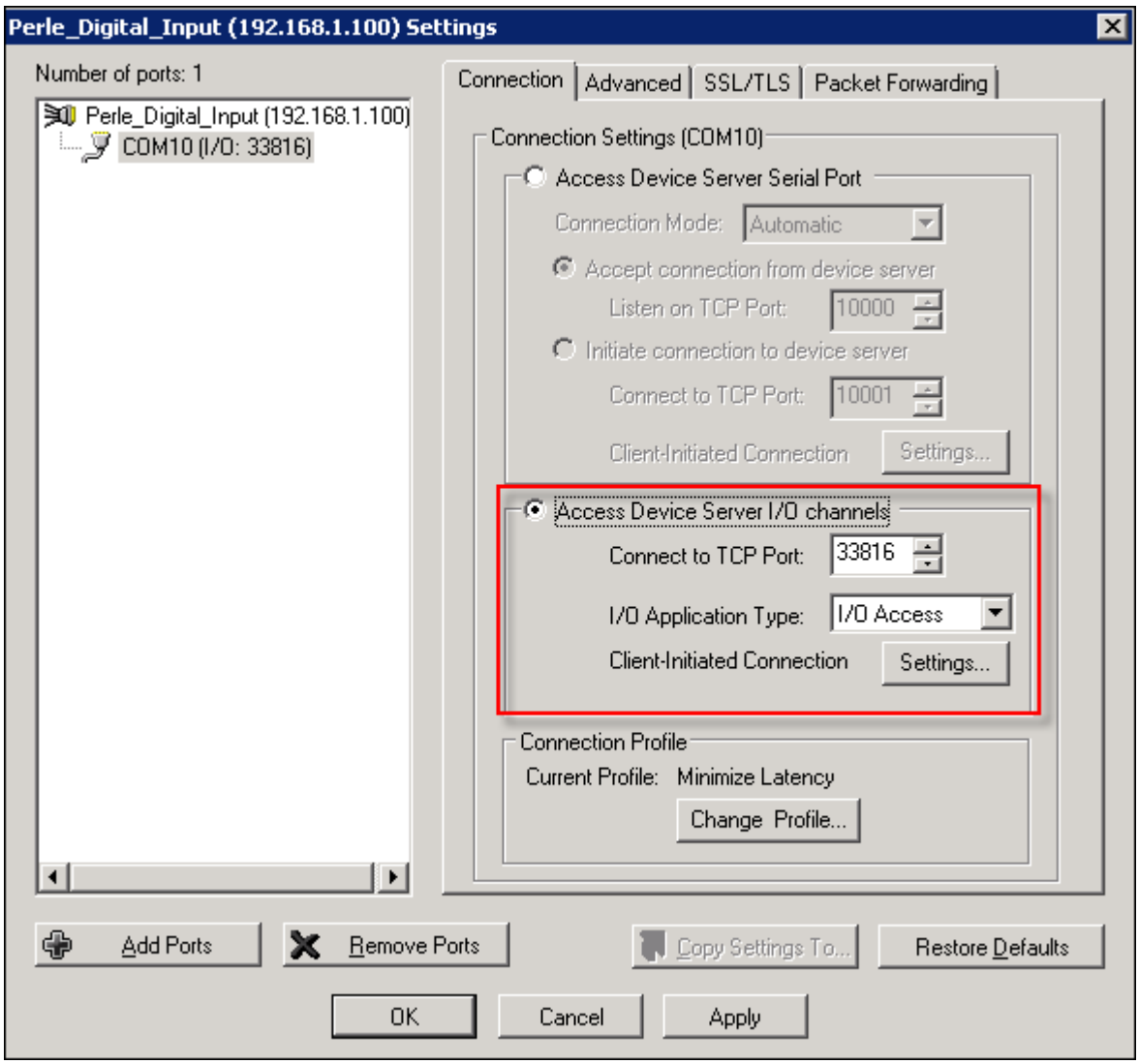
1. Start the **TruePort Management Tool**, select the Perle device to configure and click **Properties**.



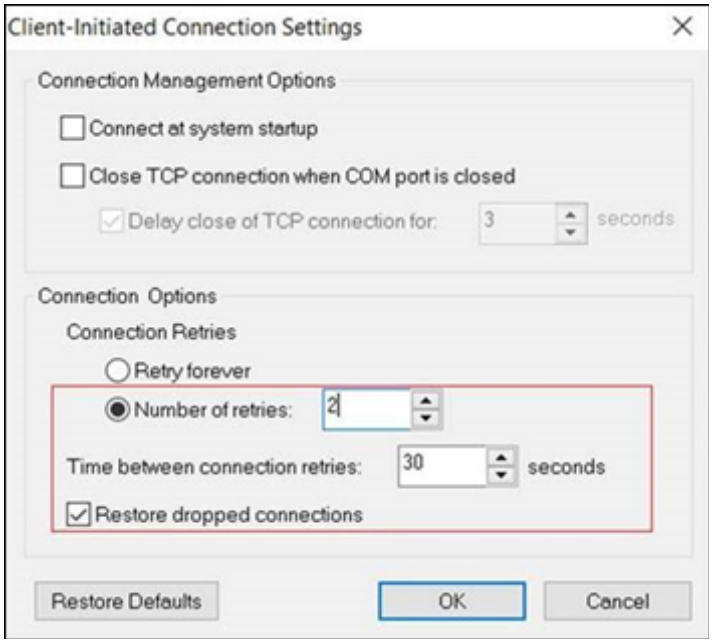
2. Select the **Configuration** tab.
3. Click **Settings**.



4. If two COM ports are created for this device, select one to use for I/O access. If the COM port is being used, the other COM port should be reserved for serial communication. If a second COM port is not added, click the **Add Ports** on the bottom of the window to add the second COM port.
5. Select the **Connection** tab.
6. Select **Access Device Server I/O channels**.
   - Select the **TCP port** that was configured on the device for I/O access.
   - In the **I/O Application Type** drop-down list, select **I/O Access**.



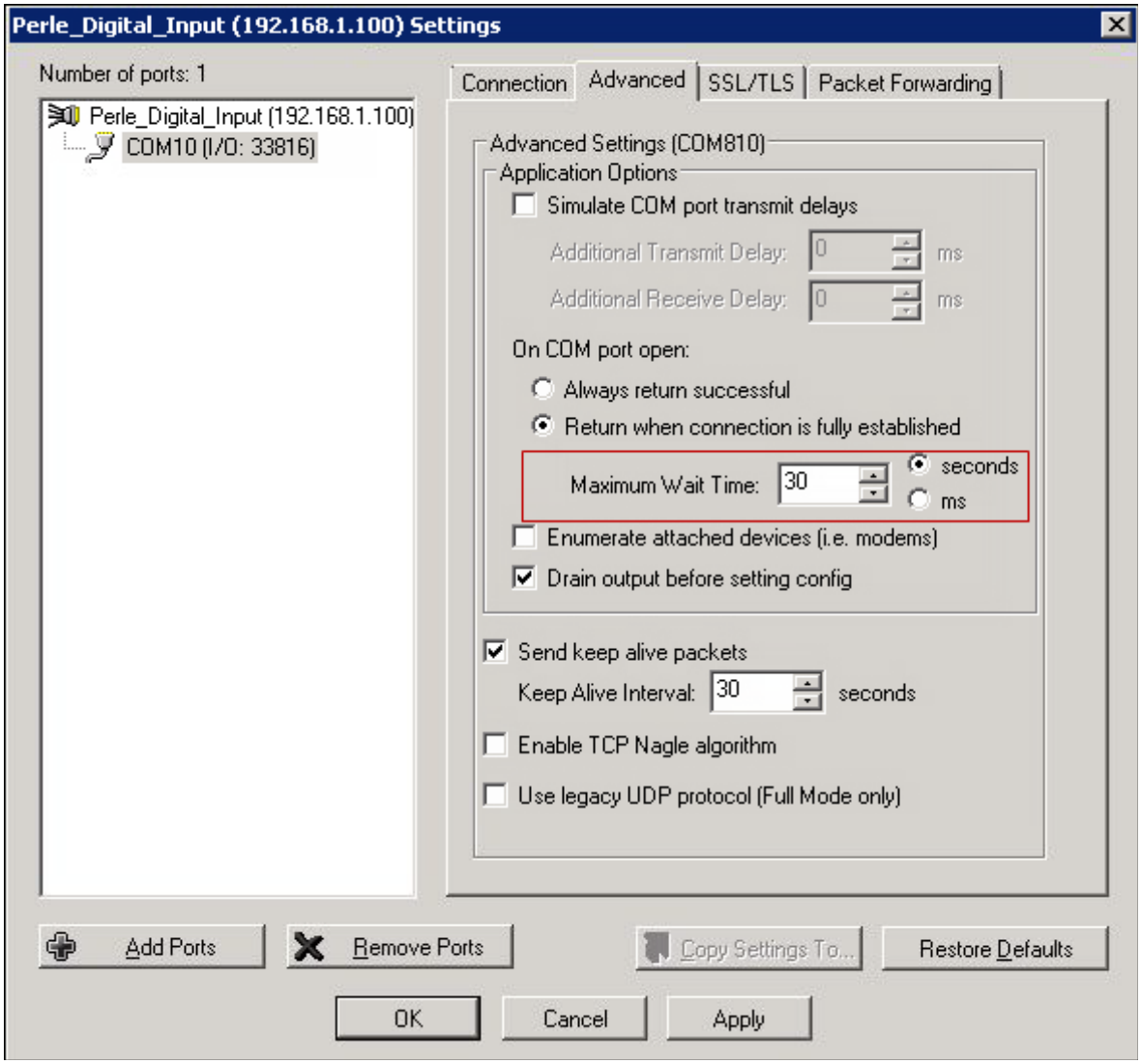
7. Click **Settings** next to **Client-Initiated Connection**.
   ⇨ The **Client-Initiated Connection** window displays.



8. Select the **Connect at system startup** check box.
9. For **Connection Retries**, select **Retry forever**.

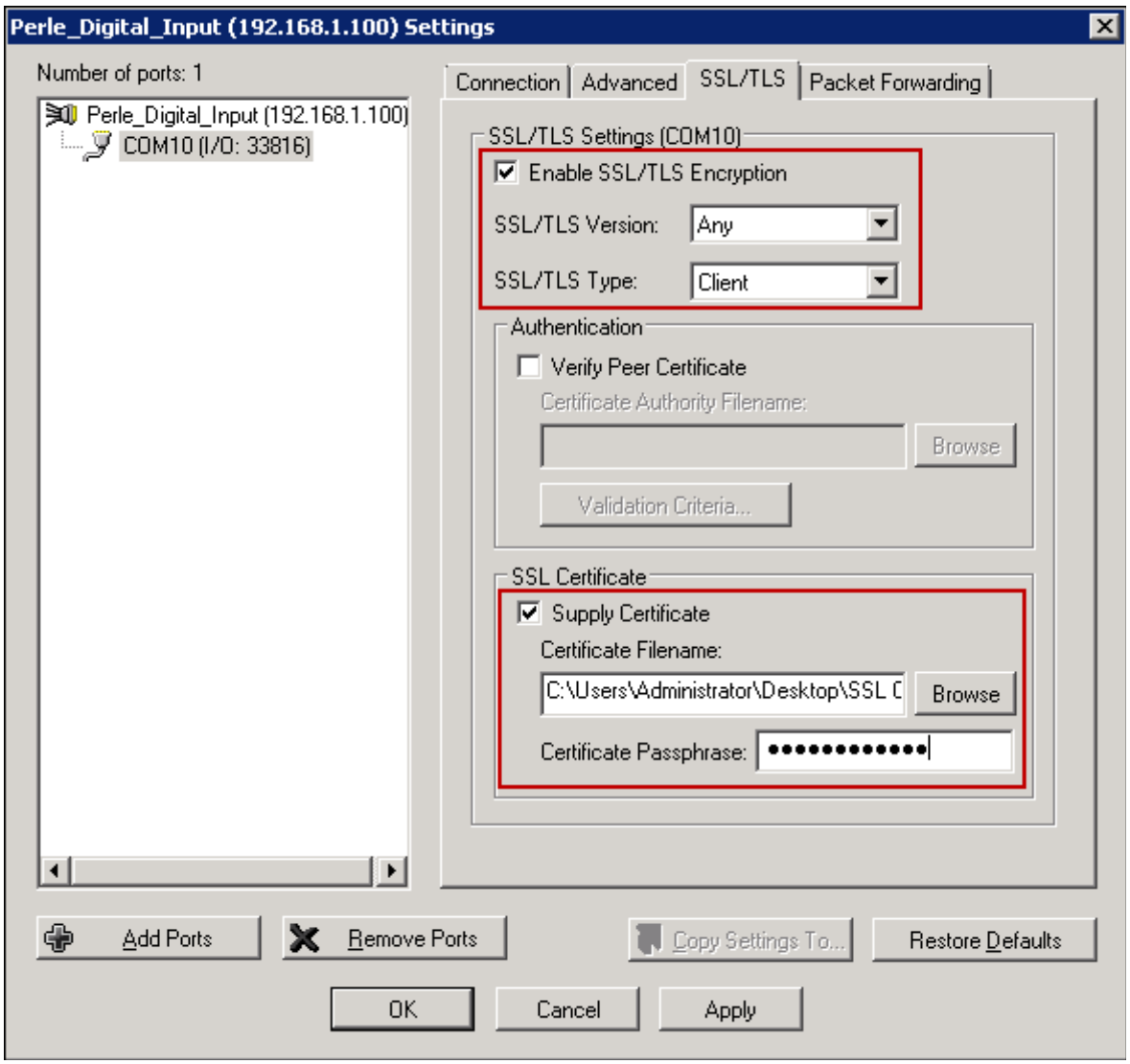
10. Click **OK**.

11. Select the **Advanced** tab.

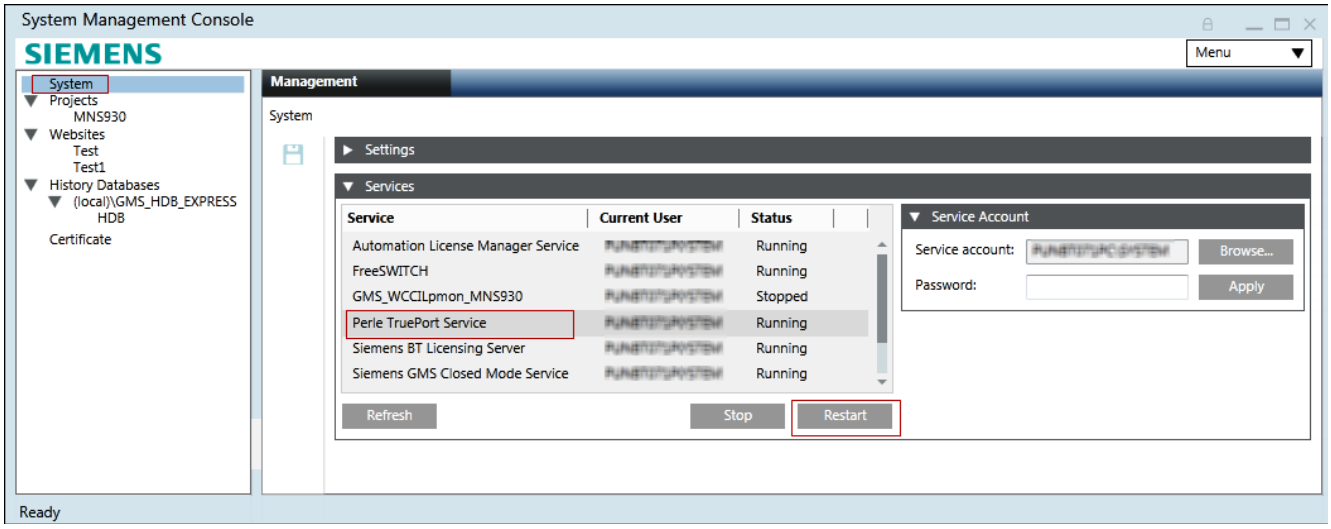


12. Set **Maximum Wait Time** to **30 seconds**.

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



14. Select the **Enable SSL/TLS Encryption** check box.
15. Set the **SSL/TLS Version** field to **Any**.
16. Set the **SSL/TLS Type** field to **Client**.
17. Select the **Supply Certificate** check box.
18. Click the browse button and select the combined root certificate. Refer to the --- MISSING LINK --- section for more information on combining a root certificate.
19. Enter the password in the **Certificate Passphrase** field.
20. Click **Apply** and then **OK**.
21. Restart the **Perle TruePort Service** from the SMC.



⇨ The TruePort driver is ready for I/O access.

Device Verification

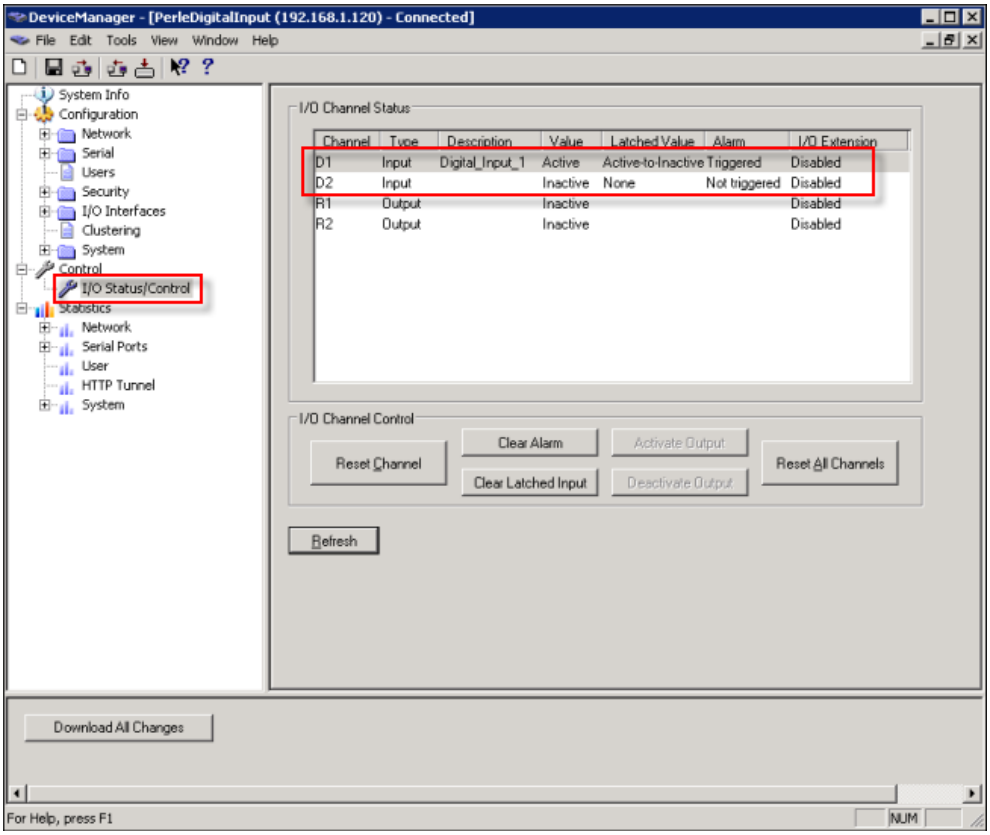
▷ The Perle device is configured for inputs.
NOTE: To test that the device is configured and the digital inputs display properly, use the **I/O Status/Control** section of the Perle DeviceManager.

▷ A dry contact switch, such as the STI Emergency stopper station is present, wired to the I/O terminals of the Perle device.

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

1. In the Perle DeviceManager, select **Control** > **I/O Status/Control**.

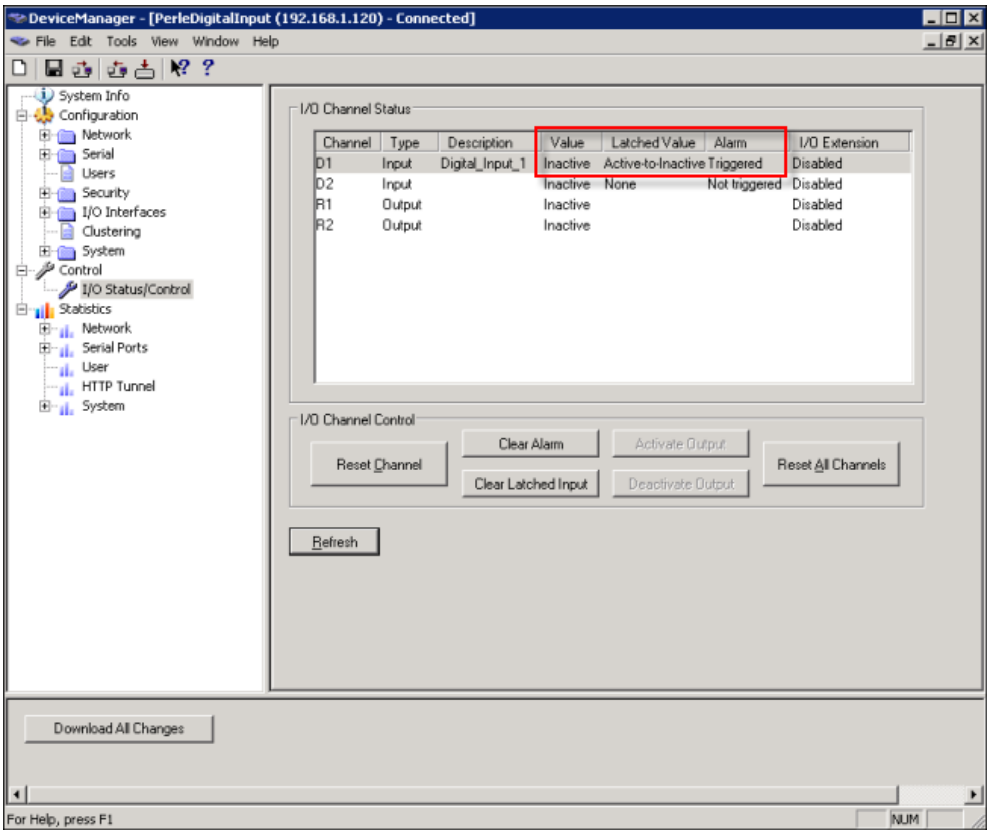
   ⇨ The current status of all inputs and relays is visible.



2. Close the contact switch.

3. Click **Refresh**.

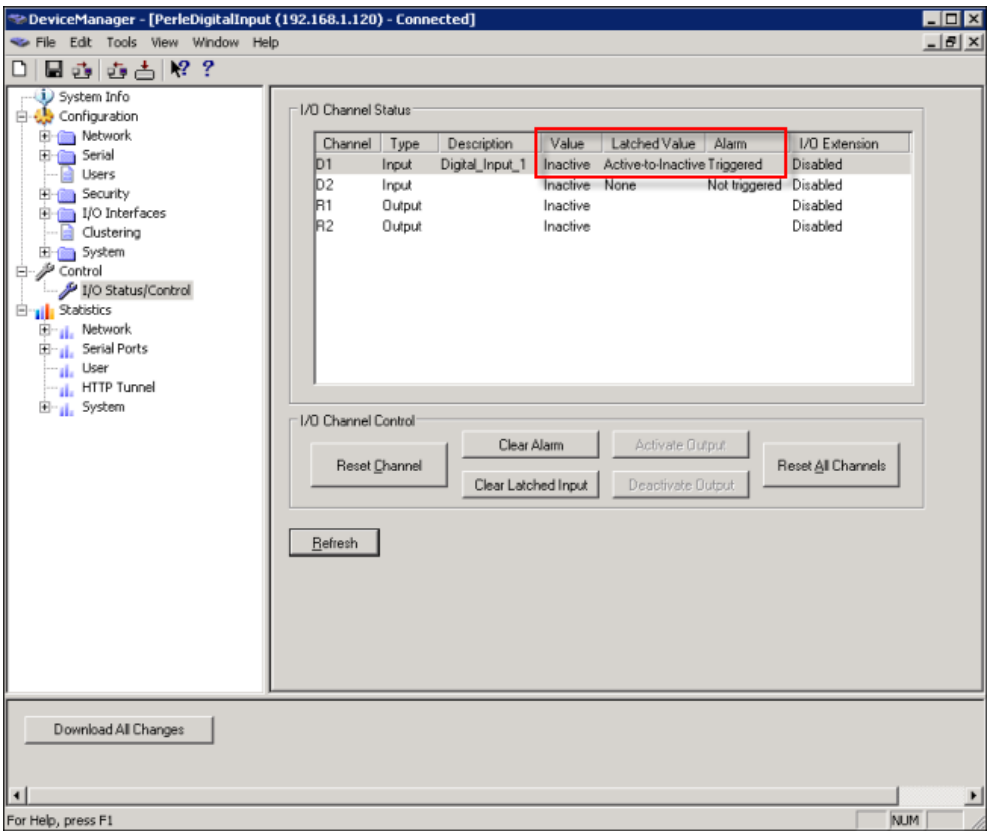
   ⇨ The fields change to the corresponding state:
   Value: Active
   Latched Value: Active-to-Inactive
   Alarm: Triggered



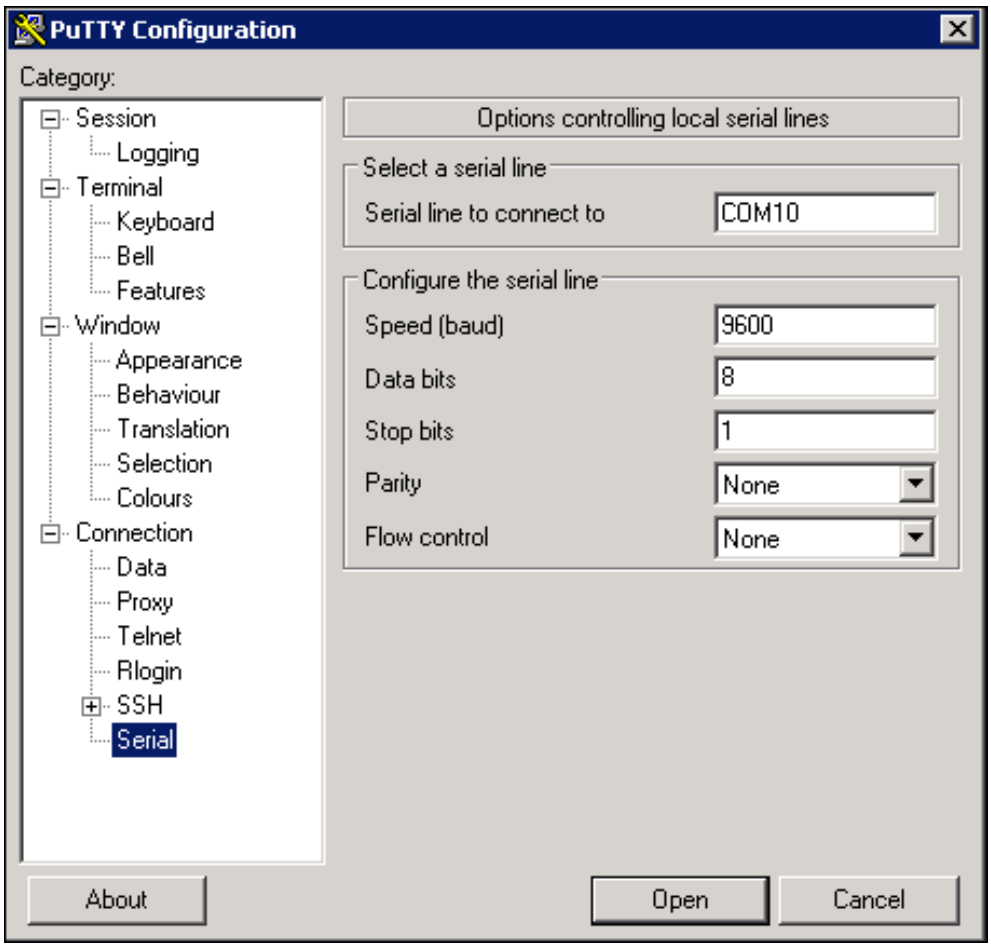
4. Release the contact switch.

5. Click **Refresh**.

   ⇨ The fields change to the corresponding state:
   Value: Inactive
   Latched Value: Active-to-Inactive
   Alarm: Triggered



6. If the behavior is correct, click **Reset All Channels** to clear all the internal device values. Otherwise, check the settings for the device inputs.
7. To verify that TruePort COM port is working correctly, use PuTTY from the server on the serial COM port. If the COM port can be opened, then the TruePort driver is working properly. PuTTY can be downloaded from the following link:
   http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe
8. Open PuTTY, and select **Connection** > **Serial**.
9. For **Serial line to connect to**, enter the TruePort COM port number created in TruePort Driver Configuration.
10. Enter the following default parameters:
    - **Baud Rate**: 9600
    - **Data Bits**: 8
    - **Stop Bits**: 1
    - **Parity**: None
    - **Flow Control**: None



11. Select **Session** > **Serial**.

12. Click **Open** to establish a serial session. If the user is denied access to open the COM port, check that the COM port in TruePort is configured correctly to connect to the Perle device.

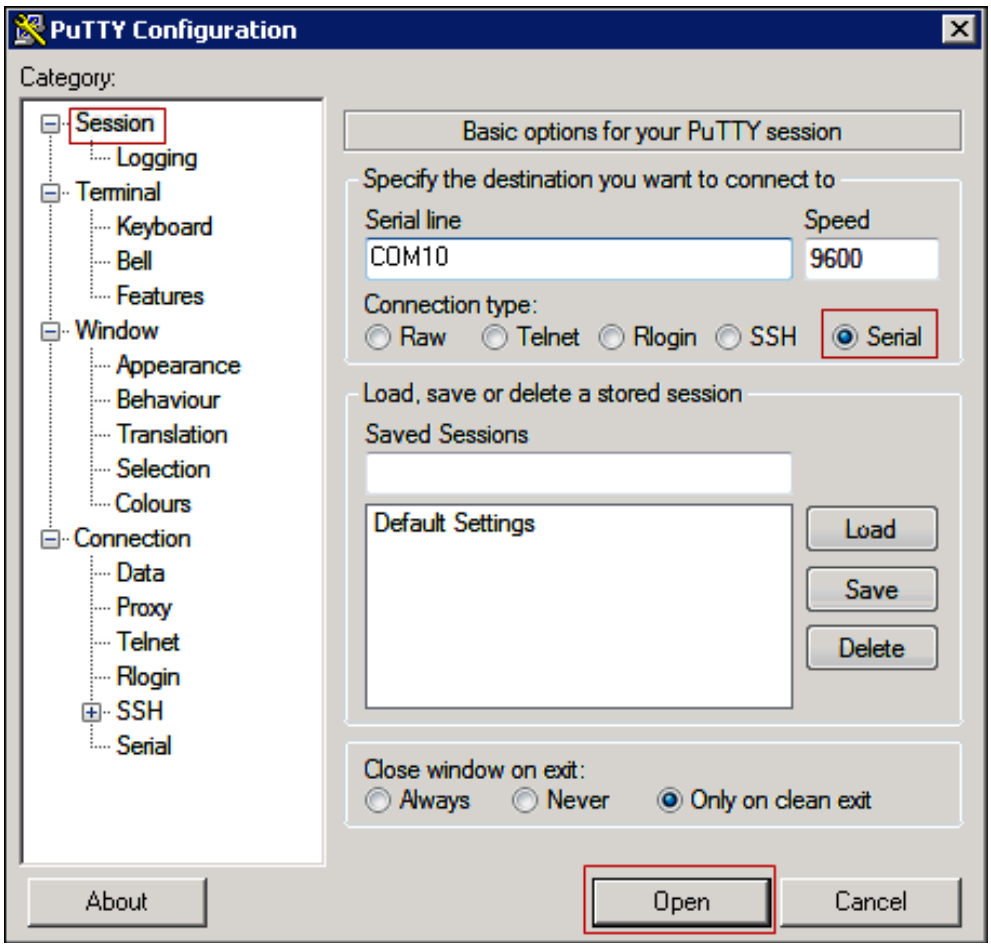


Fig. 16: Selecting Serial Option

Digital Input - Device Engineering

There is no further configuration required for the emergency stopper station. Additional configuration is required for the Perle TD2R2 to communicate with . There are two areas of configuration. The first is to configure the TD2R2 device to correctly read input and send the appropriate responses back to . The second area of configuration is the TruePort driver which uses to communicate with the TD2R2 device.

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.

(Example) Input Triggering

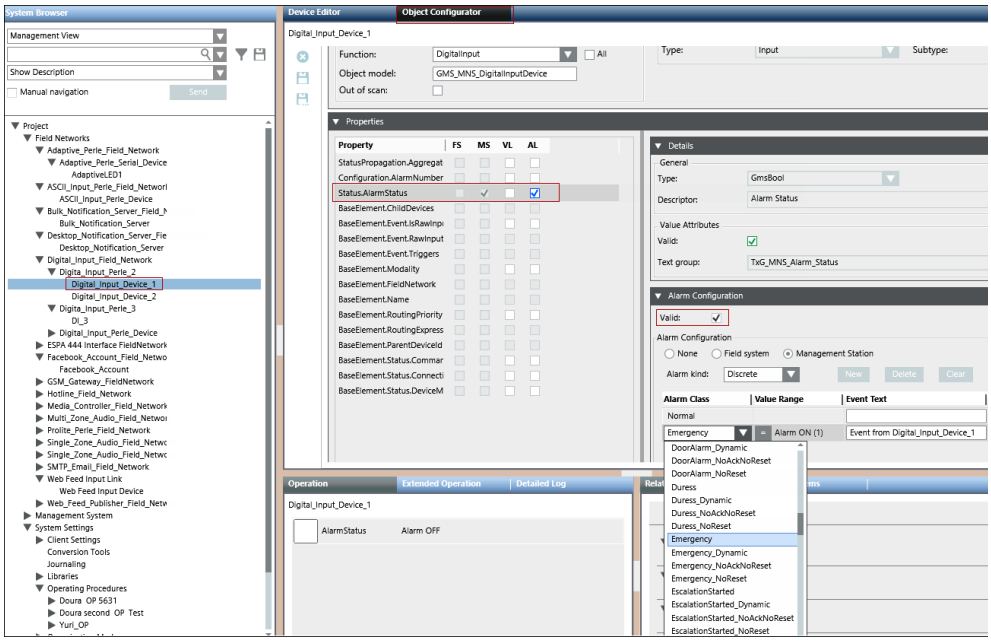
Scenario: Two Digital Input Devices are configured with Panic Buttons. Panic Button 1 is connected to Perle Device 1 and Relay 1. Panic Button 2 is connected to Perle Device 1 and Relay 2. If Panic Button 1 is pressed, Incident 1 should be initiated and if Panic Button 2 is pressed, Incident 2 should be initiated.

Procedure:

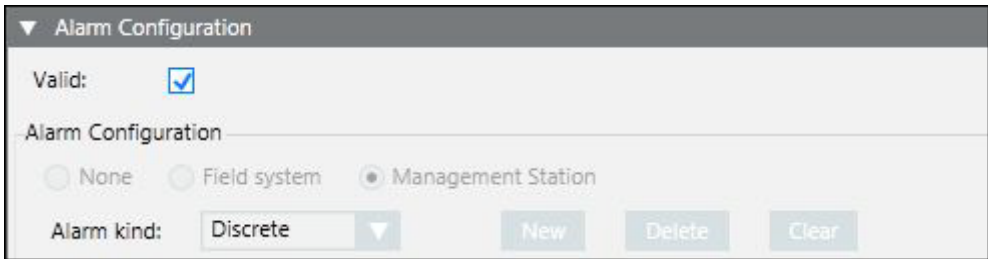
▷ System Manager is in **Engineering** mode.

1. In System Browser, select **Management View**.
2. Select **Project > Digital_Input_Field_Network**.

3. Configure two Digital Input Devices as **Digital_Input_Device_1** and **Digital_Input_Device_2**.
4. Select **Digital_Input_Device_1**.

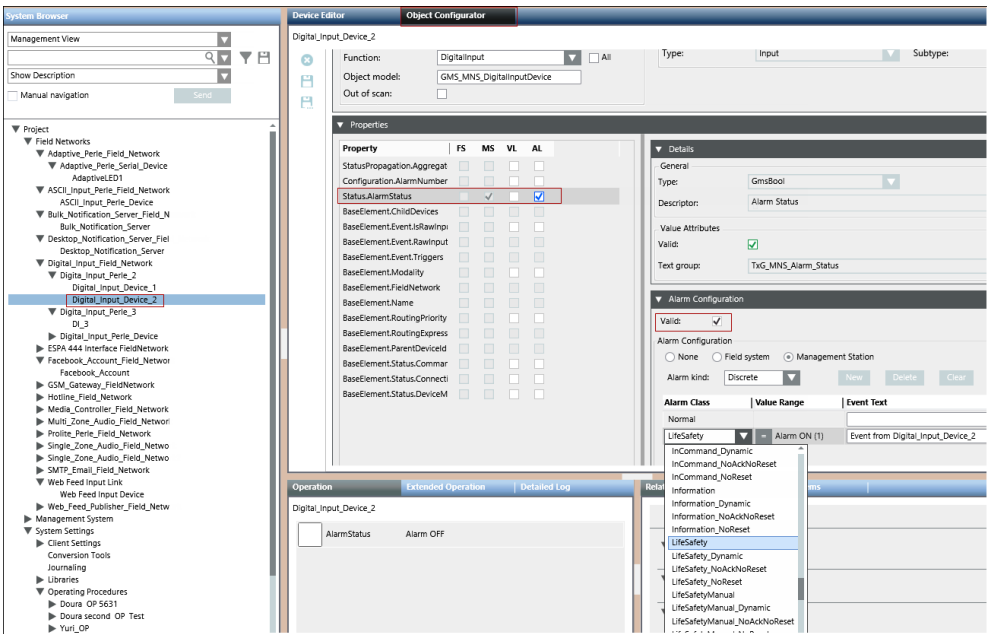


5. Select the **Object Configurator** tab.
6. In the **Properties** expander, select the **Status.AlarmStatus** property.
7. In the **Alarm Configuration** expander, select the **Valid** check box.

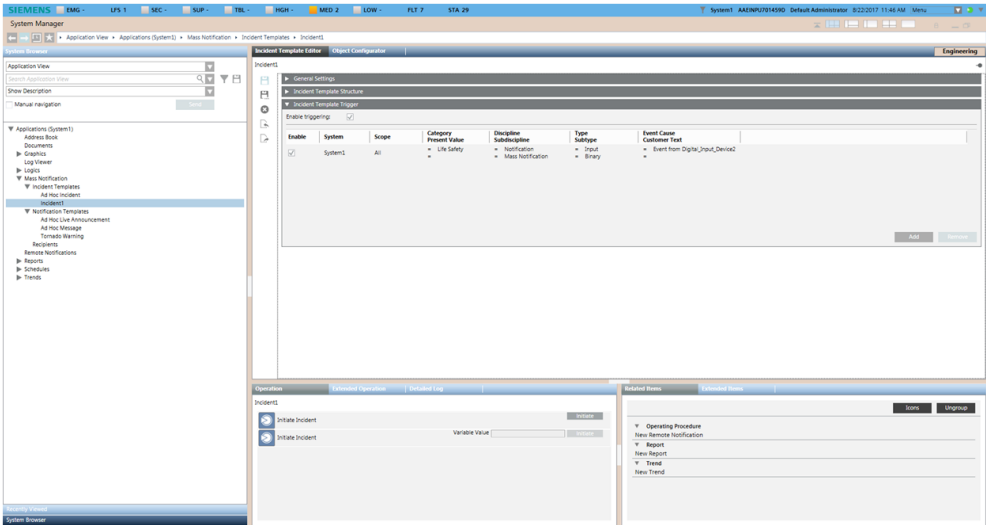


⇨ The color of the **Valid** check box changes from blue to black.

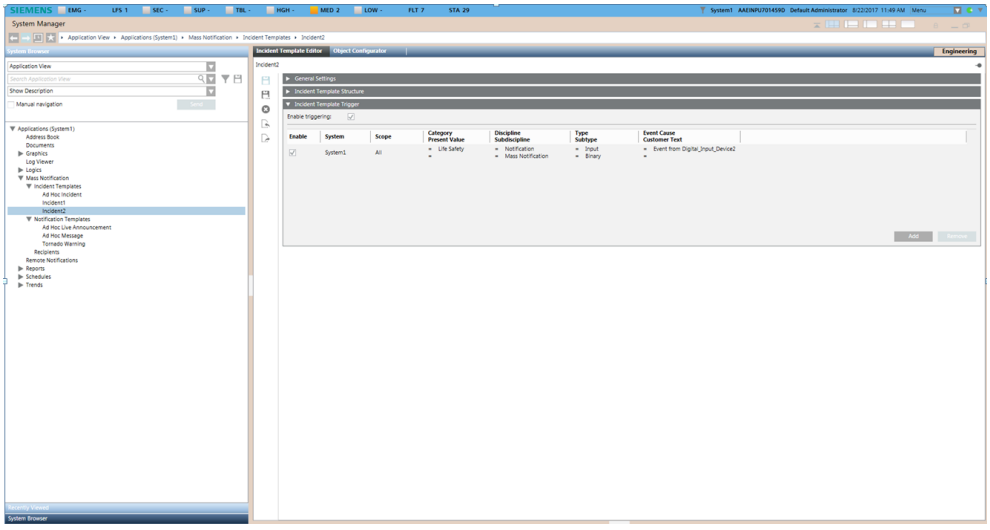
8. Select the alarm class from the **Alarm Class** drop-down list. For example, **Emergency**.
9. Enter the event text in the **Event Text** field. For example, **Event from Digital_Input_Device_1**.
10. Select **Digital_Input_Device_2**.



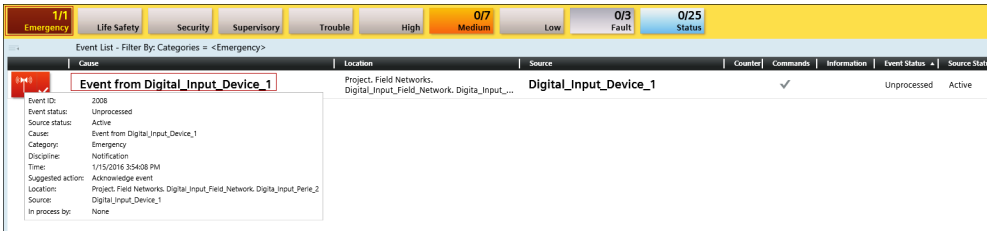
11. Select the **Object Configurator** tab.
12. In the **Properties** expander, select the **Status.AlarmStatus** property.
13. In the **Alarm Configuration** expander, select the **Valid** check box.
    ⇨ The color of the **Valid** check box changes from blue to black.
14. Select the alarm class from the **Alarm Class** drop-down list. For example, **LifeSafety**.
15. Enter the event text in the **Event Text** field. For example, **Event from Digital_Input_Device_2**.
16. Click **Save** .
17. Click **Engineering**.
18. Select **Applications** > **Mass Notification** > **Incident Templates**.
19. Click **Create** .
    ⇨ The **Create New Object** dialog box displays.
20. Select **Incident Template** from the **Child Type** drop-down list.
21. Enter a name in the **Name** field. For example, **Incident1**.
22. Click **OK**.
    ⇨ The **Incident Template Editor** tab displays.
23. In the **Incident Template Trigger** expander, click **Add**.
24. Configure the fields as shown in the following image:



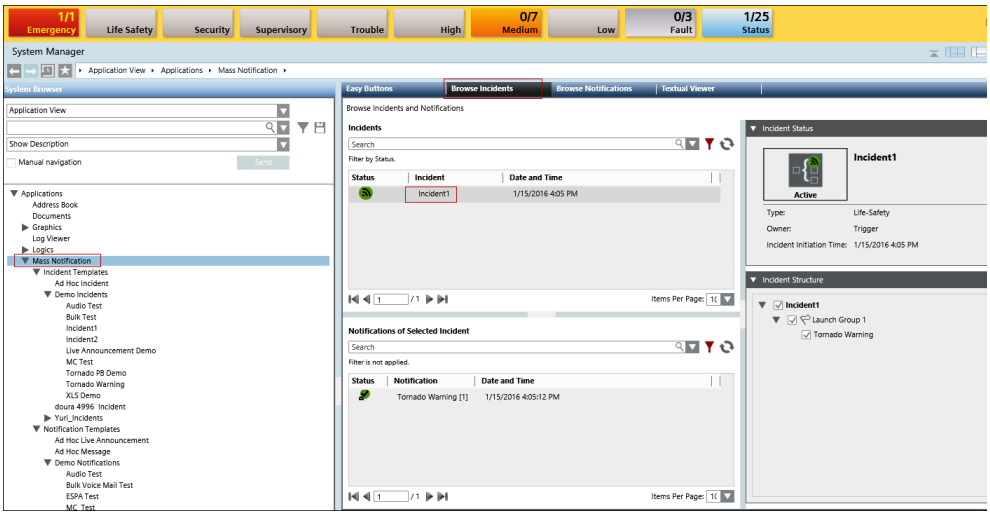
25. Click **Save** .
26. Select the **Incident Templates** node.
27. Click **Create** .
    ⇨ The **Create New Object** dialog box displays.
28. Select **Incident Template** from the **Child Type** drop-down list.
29. Enter a name in the **Name** field. For example, **Incident2**.
30. Click **OK**.
    ⇨ The **Incident Template Editor** tab displays.
31. In the **Incident Template Trigger** expander, click **Add**.
32. Configure the fields as shown in the following image:



33. Click **Save** .
34. Press Panic Button 1.
    ⇨ Event from **Digital_Input_Device_1** will be generated.

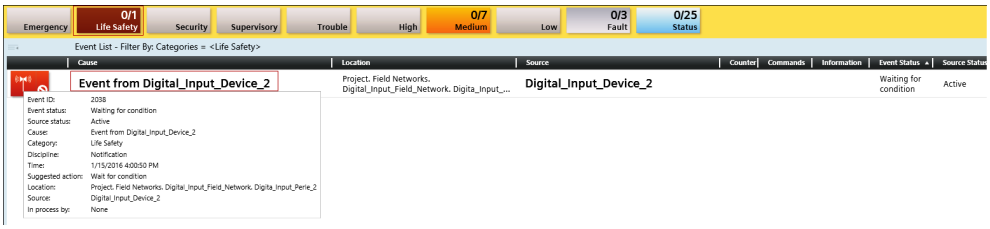


➪ The **Incident1** will be initiated which can be verified from the **Browse Incidents** tab:
a. In System Browser, select **Application View**.
b. Select **Applications** > **Mass Notification**.
c. Select the **Browse Incidents** tab.

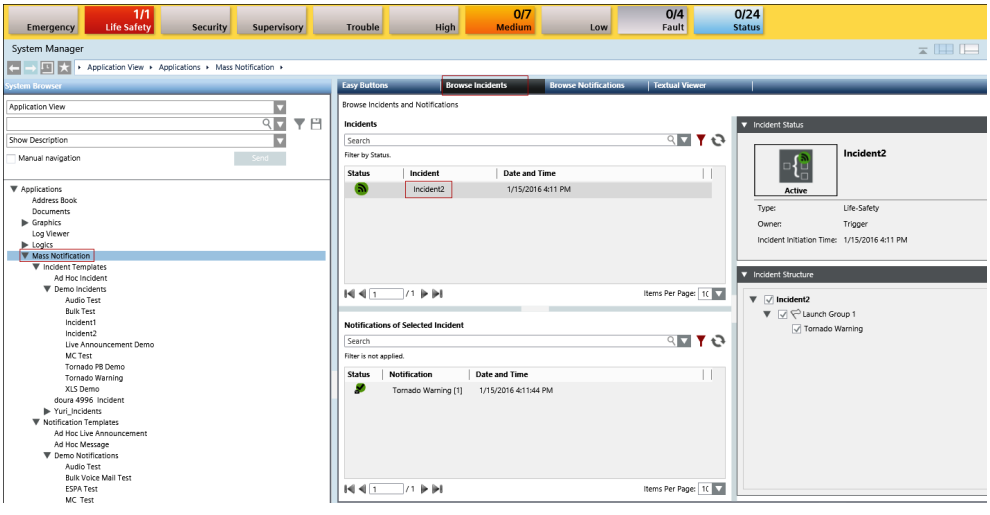


35. Press Panic Button 2.

➪ Event from **Digital_Input_Device_2** will be generated.



➪ The **Incident2** will be initiated which can be verified from the **Browse Incidents** tab:
a. In System Browser, select **Application View**.
b. Select **Applications** > **Mass Notification**.
c. Select the **Browse Incidents** tab.

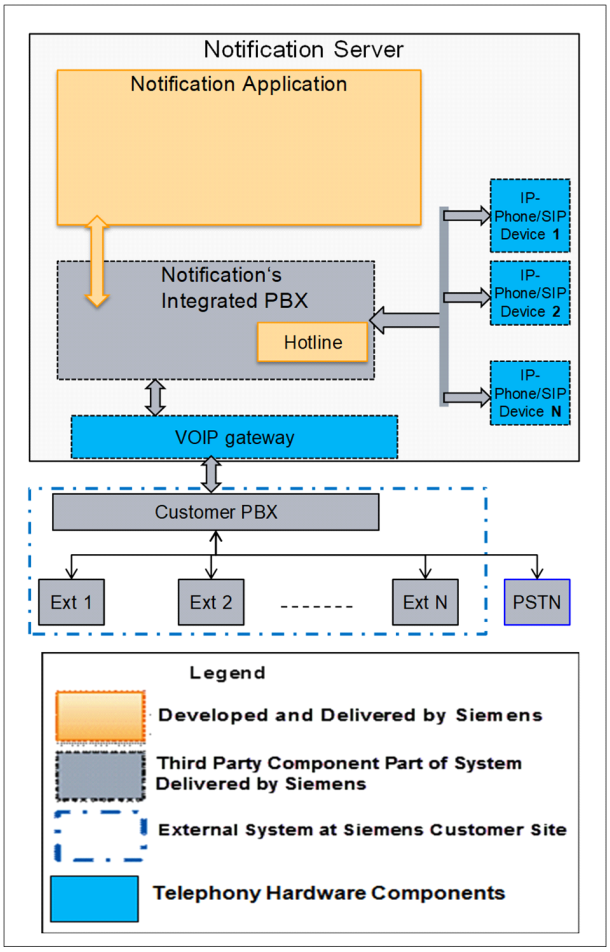


1.7 Emergency Hotline Extension Device

Emergency Hotline Extension Device

This section contains general reference and background information about integrating the Emergency Hotline Extension device. For procedures and workflows, see step-by-step section.

uses an VoIP Switch to deliver the different audio content to the intended recipients. With an Emergency hotline, a user can call the hotline to access active messages published by . The hotline device itself exists as an extension on ‘s VoIP Switch. The following figure gives an overview of how the system is setup and the different ways in which the hotline can be accessed.



Accessing the Emergency Hotline

connects to the customer’s PBX via a VoIP gateway. As a result, the hotline can be accessed:

- From an IP phone connected to the ‘s VoIP Switch on server.
- From any extension phone connected to the customer’s PBX provided the necessary steps for integrating the system with the customer’s PBX has been completed.
- From any outside phone (mobile or landline). In this case the customer needs to publish the number that needs to be used by their intended recipients to reach the hotline. This is possible only after integrating the system with the customer’s PBX.
  For example, if the customer is a school or university, then all students, faculty and other people are intended recipients and they must be aware of the number to dial to access active messages published by to the hotline.

1.8 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.

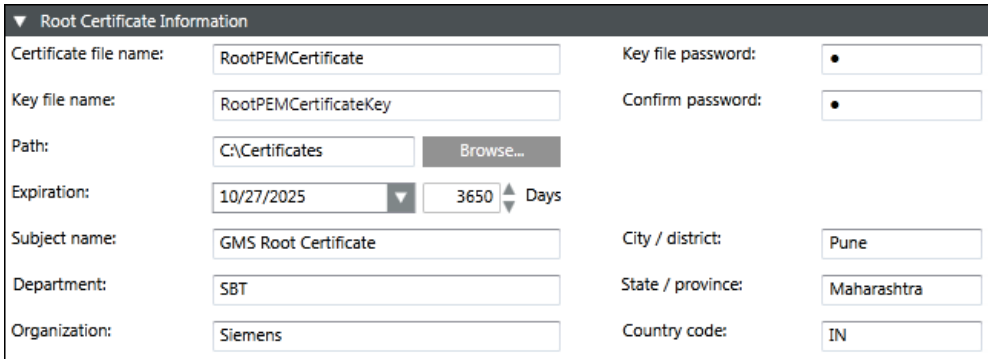
Certificate Creation From System Management Console

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.



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

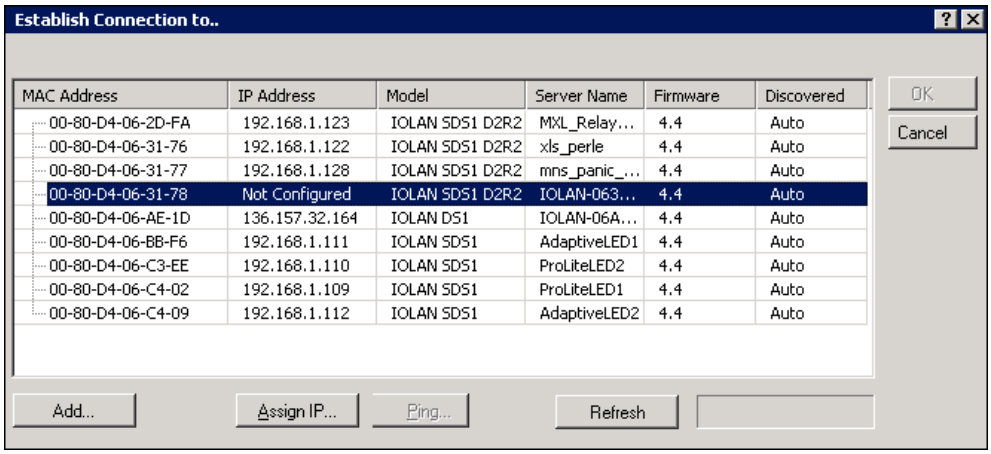
▷ Ensure that the Perle DeviceManager is installed on a computer located in the same network as the Perle device to be configured.

▷ 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.

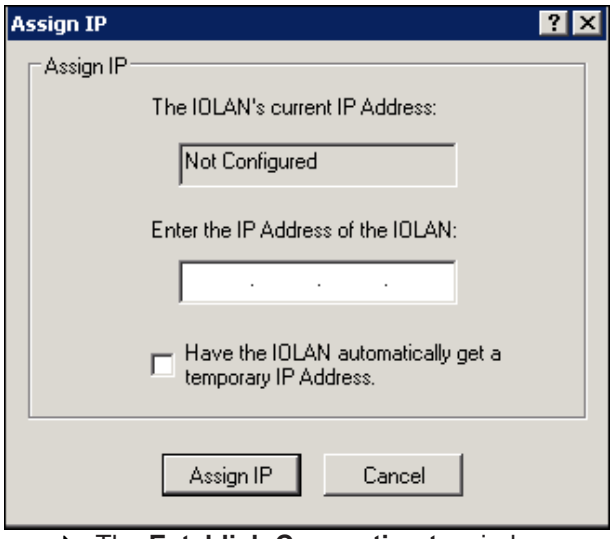


⇨ All similar devices under that network should be visible.

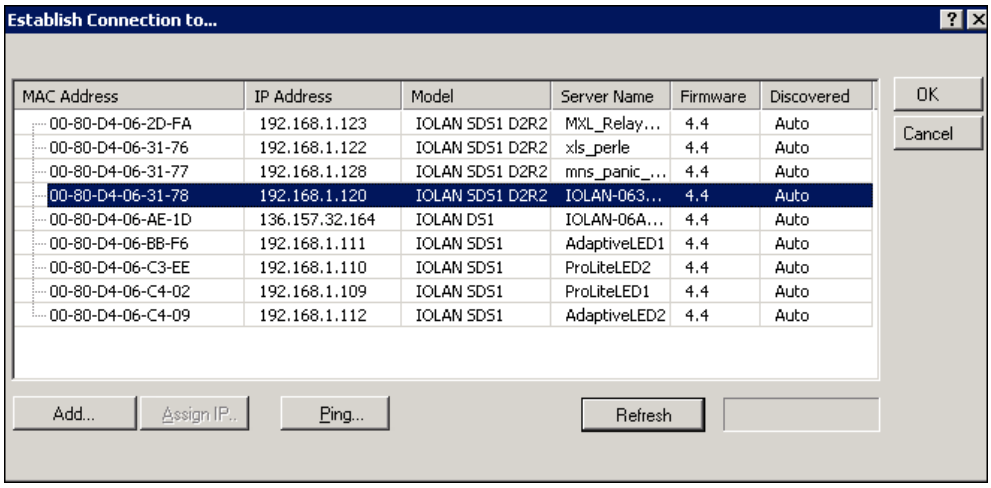
2. Select the device to configure and click **Assign IP**.
NOTE 1: If the device in the window is not visible, verify the device has power and is connected to the network. Check the display on the device; the power

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**.



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



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**.

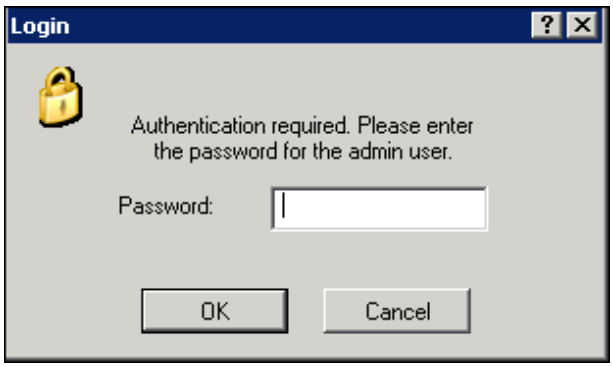
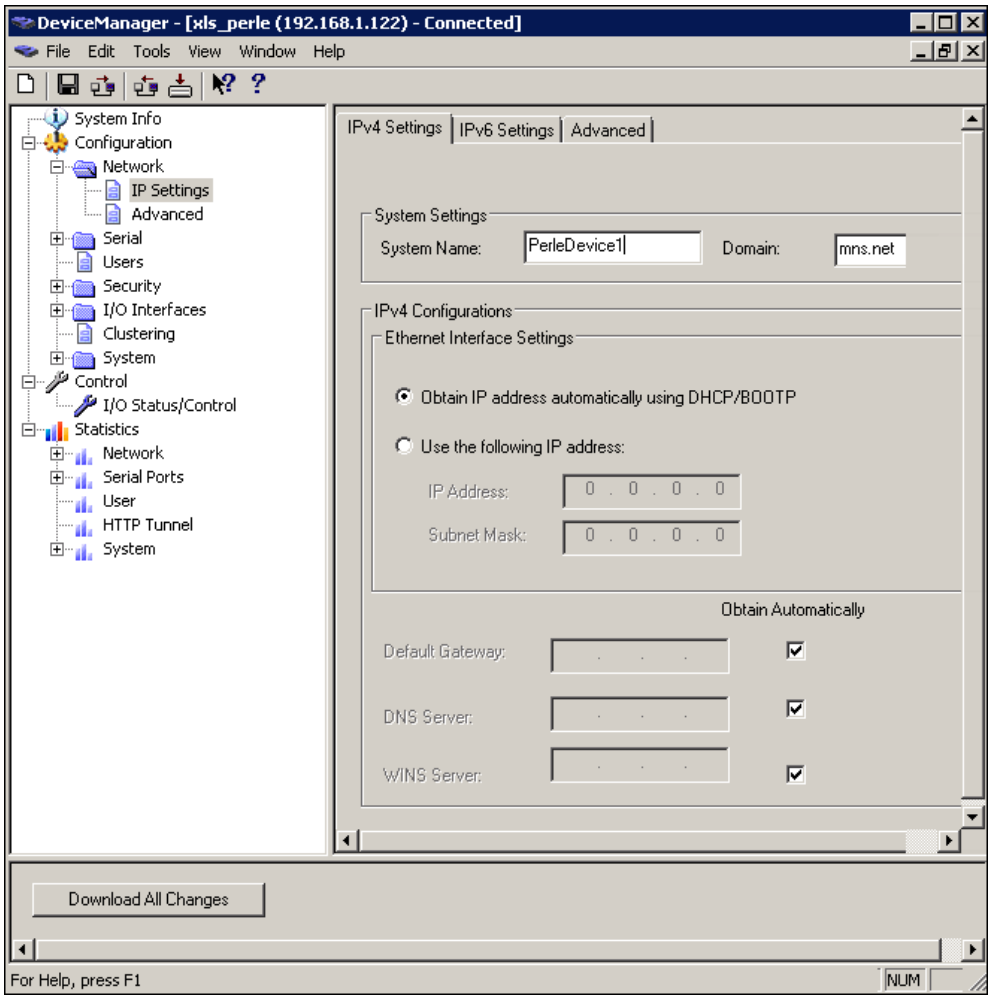


Fig. 17: Login Window

Network Set Up

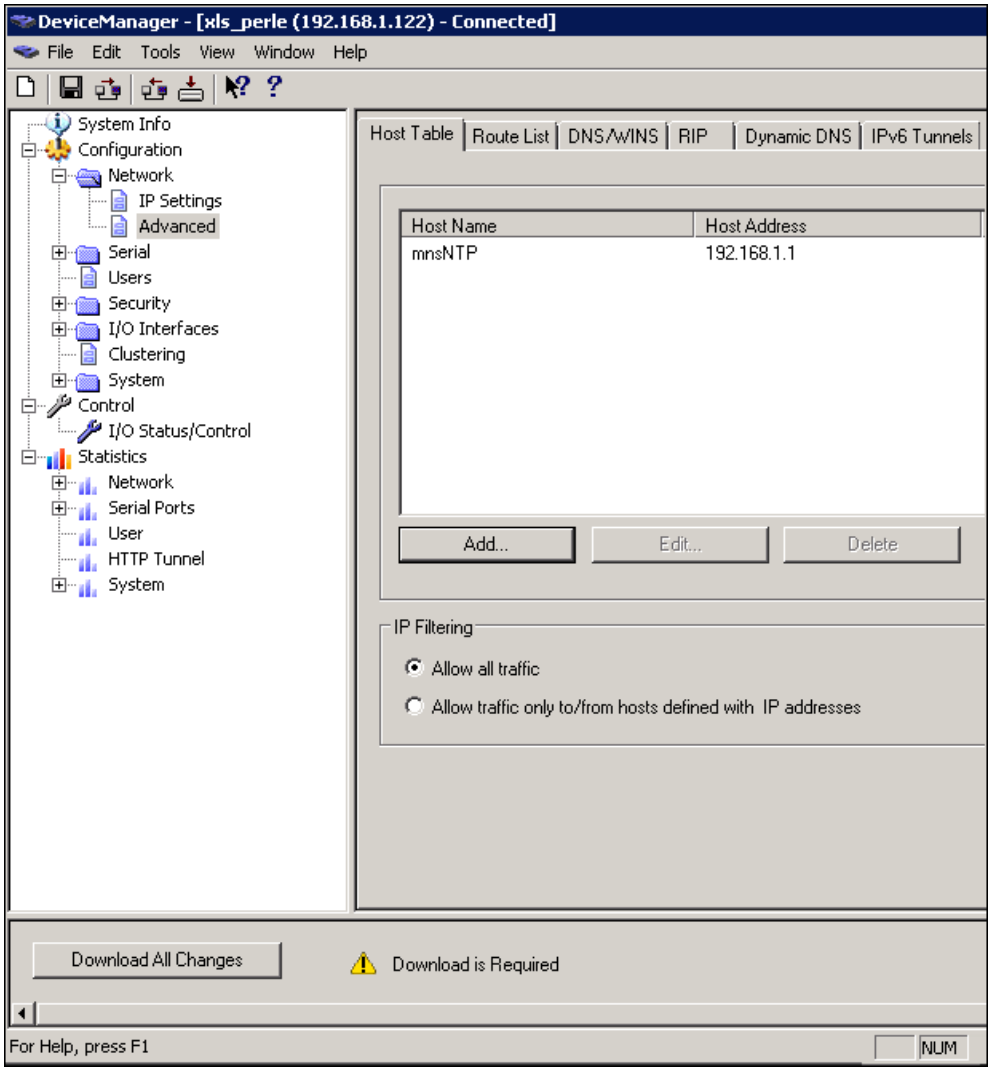
To further configure the network settings of the device, log into the device using Perle DeviceManager. Do the following:

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**.



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.



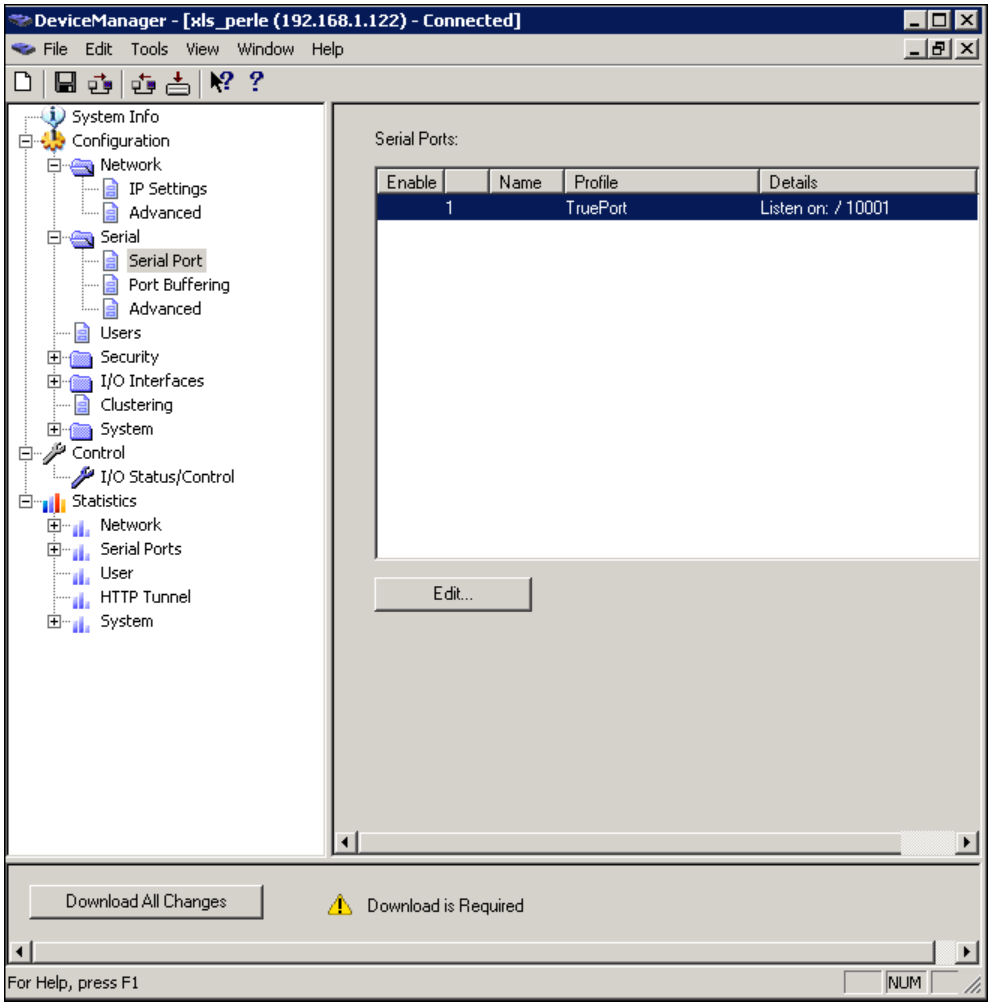
7. In the **Host Table** tab, click **Add** to add the NTP host.
8. Enter a descriptive name for the NTP server (for example, **mnsNTP**).
9. Enter the IP address or the fully qualified domain name of an available NTP server.
   NOTE: An available NTP server is required to enable SSL on the device.
10.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

Serial Settings

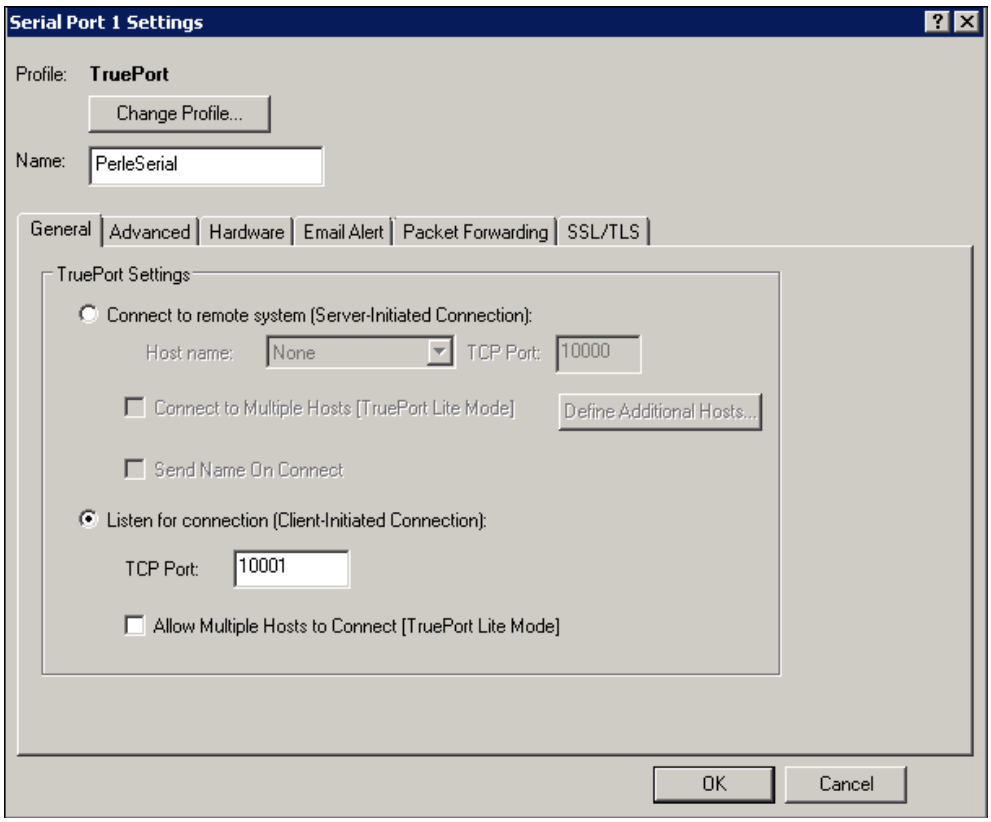
▷ The user must have logged in to the device using DeviceManager.

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**.



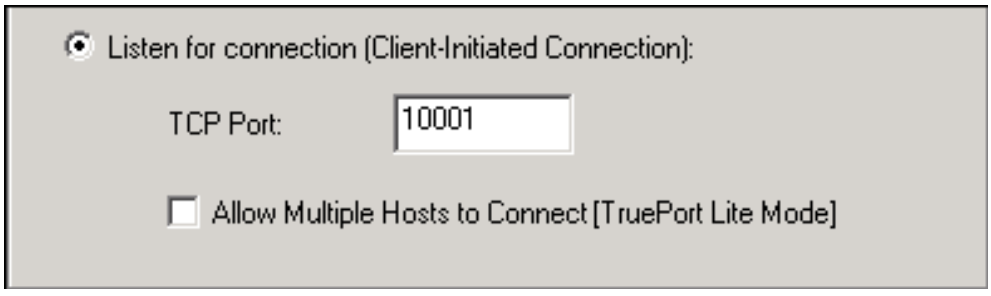
4. In the **Serial Ports Settings** window, click **Change Profile**. Select the **TruePort** profile and click **OK**.



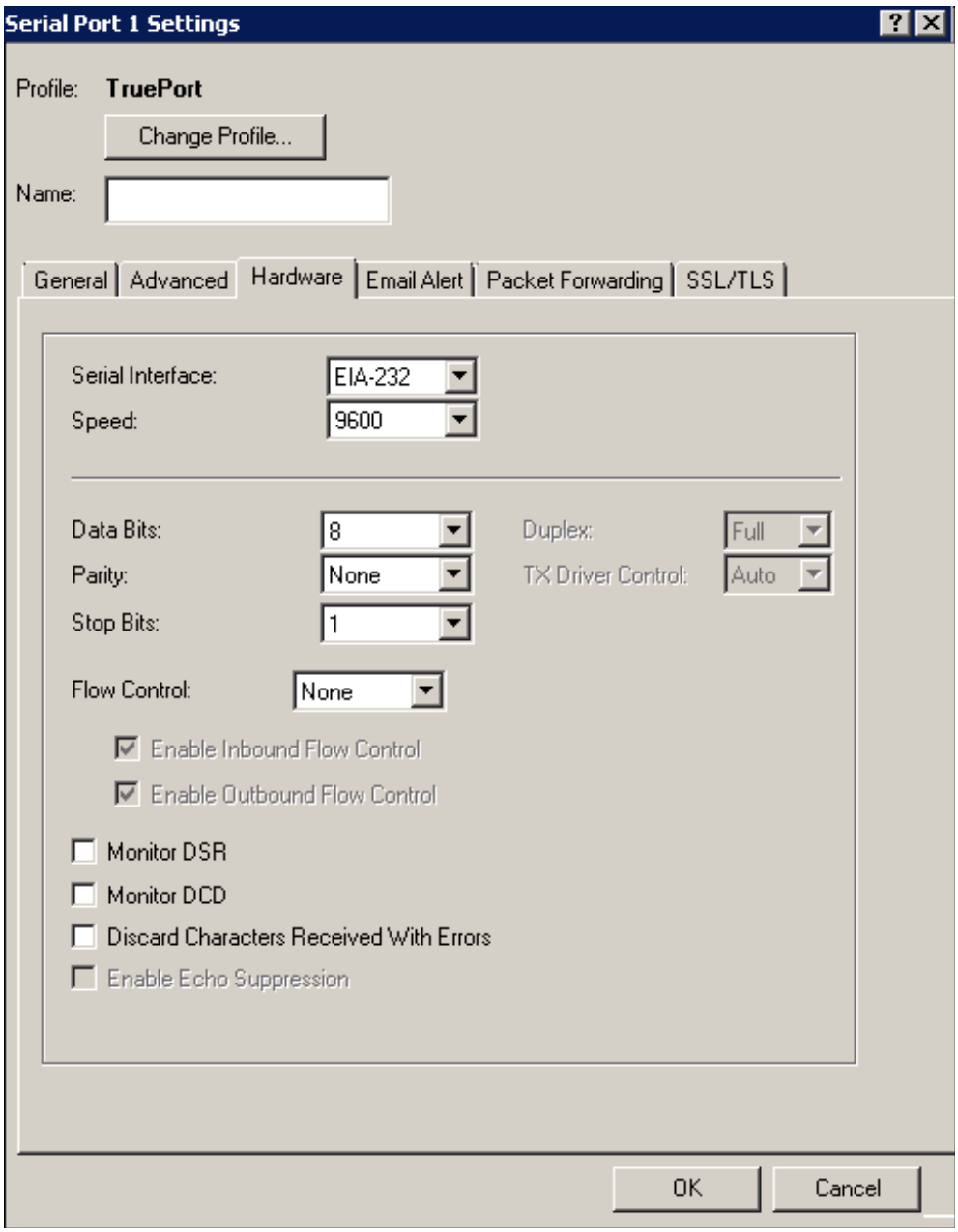
⇨ The **Serial Port Settings** window changes to reflect the new profile.

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

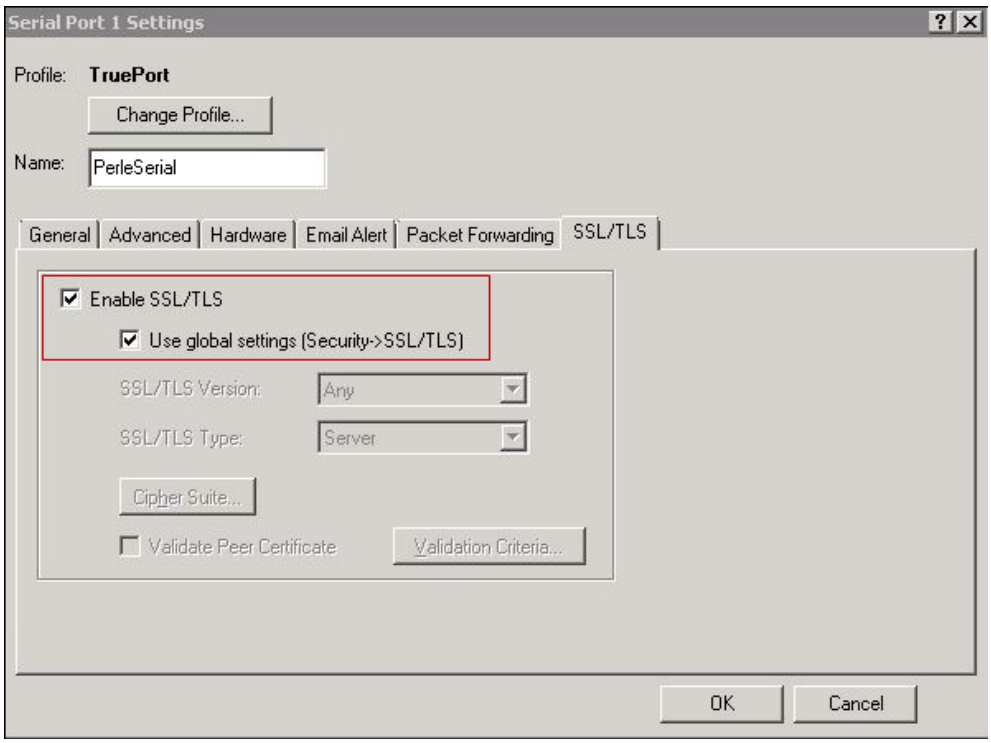
   ⇨ In this mode, the device will wait for the server to establish a connection.
7. Enter the TCP port for communicating with the device. By default, the TCP port will always be **10001**.
   NOTE: Always check to make sure the port selected is not already in use by another application/service on the server. 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**.



10. Select the **Hardware** tab.



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.



20. Select the following check boxes:

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

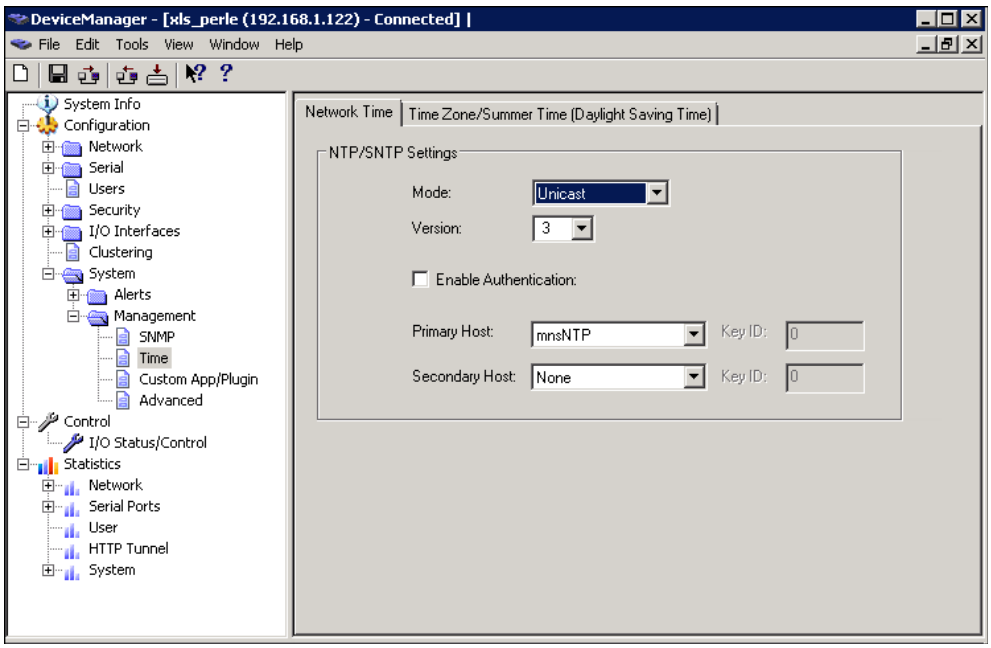
21. Click **OK**.

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

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

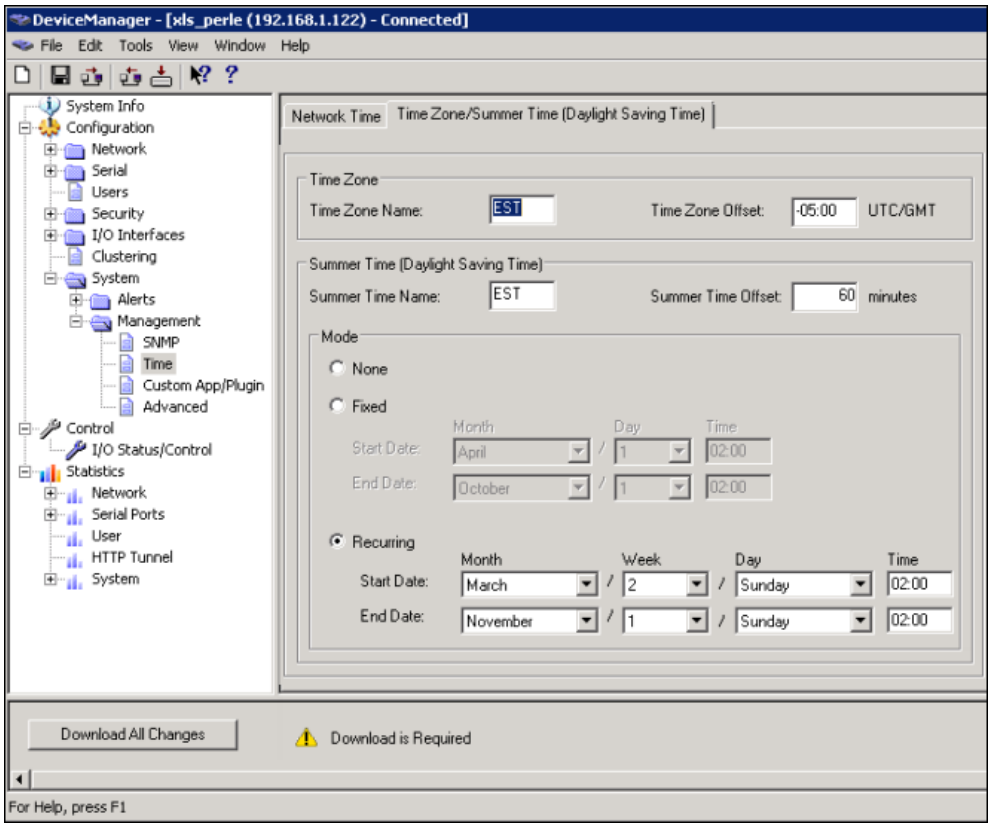
24. Set the following parameters.

- **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.

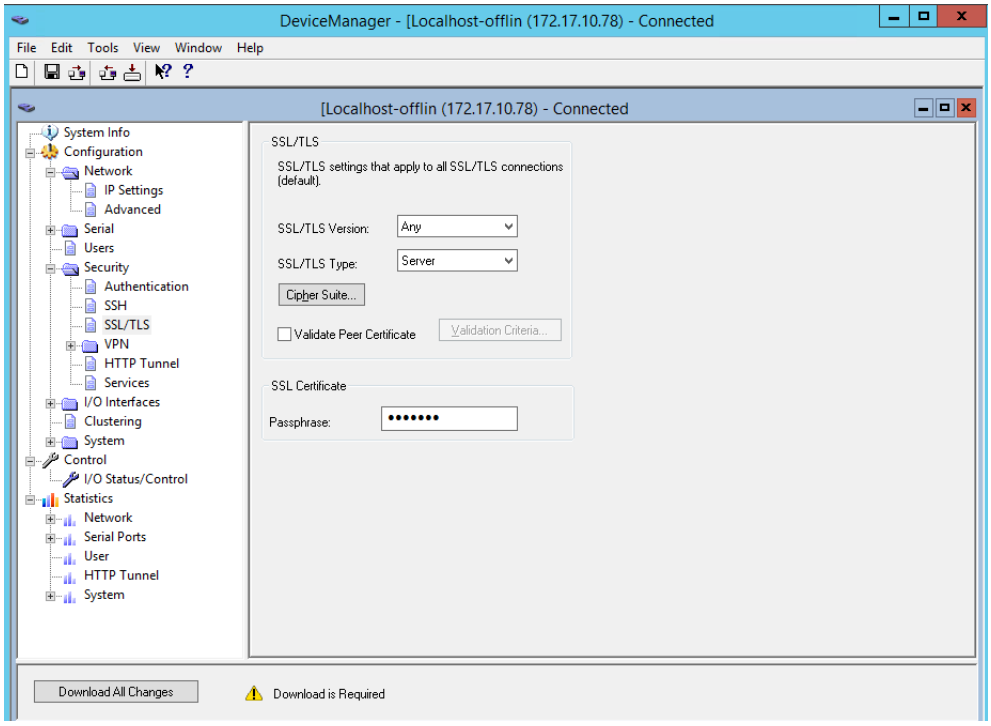


25. Select the **Time Zone/Summer Time (Daylight Saving Time)** tab.

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



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



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

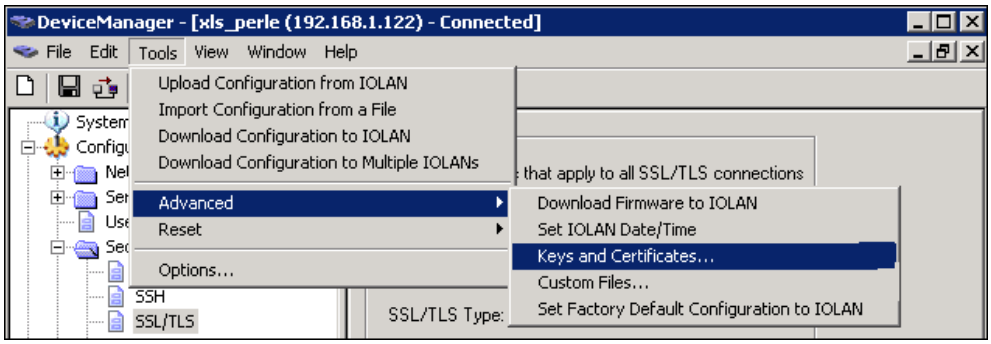
29. Set **SSL/TLS Type** field to **Server**.

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**.

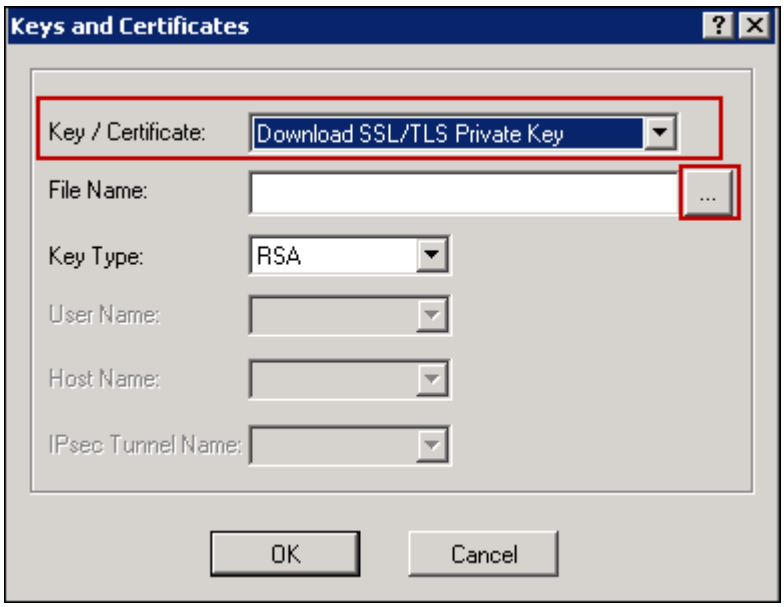
⇨ The **Keys and Certificates** dialog box displays.



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**.



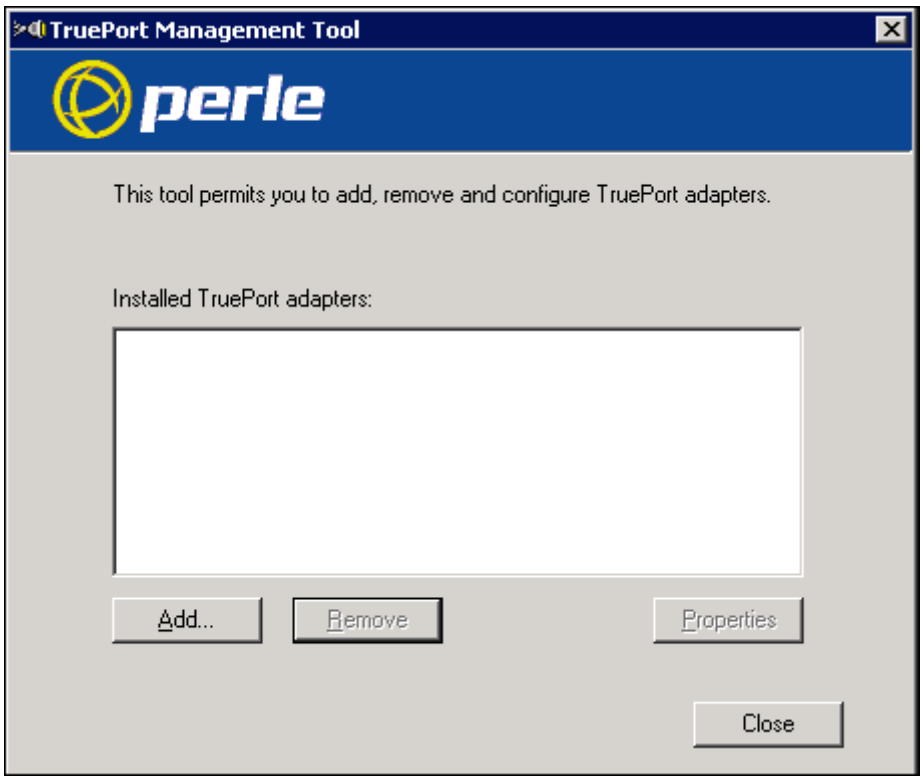
36. Select **Tools > Advanced > Keys and Certificates**.
37. In the **Key/Certificate** drop-down list, select **Download SSL/TLS Certificate**.
38. Click the browse button and upload the combined root certificate (RootCombineCert.pem file). Refer to the Device Configuration section for more information 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.

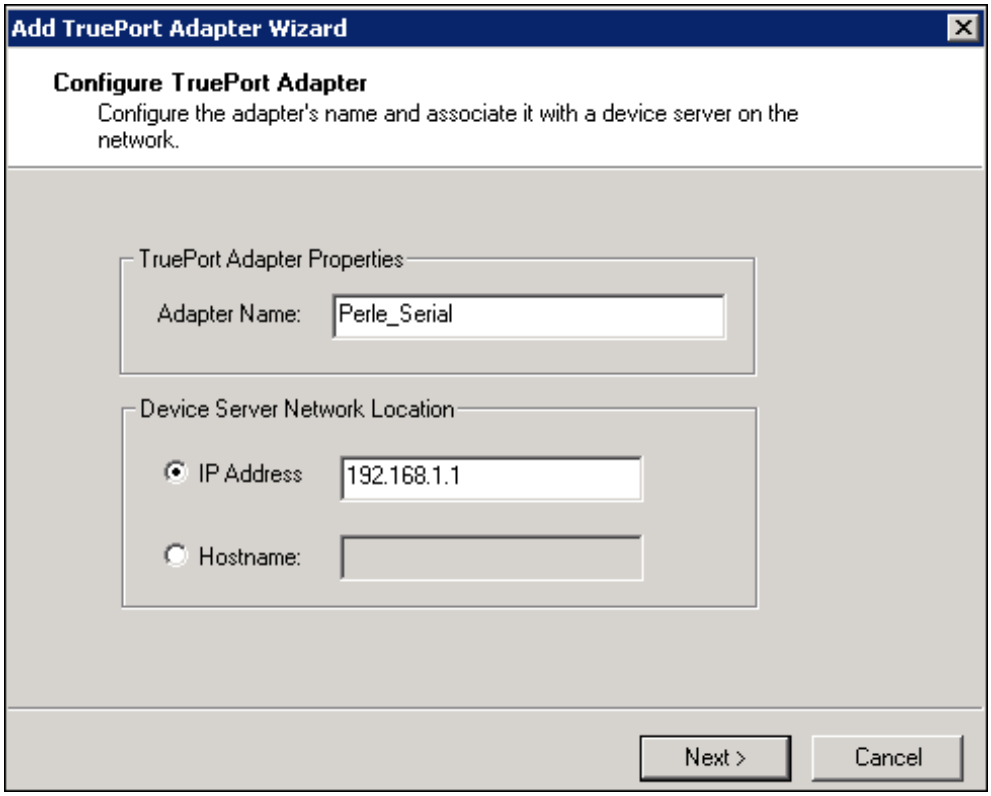
TruePort Driver Configuration

▷ 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**.



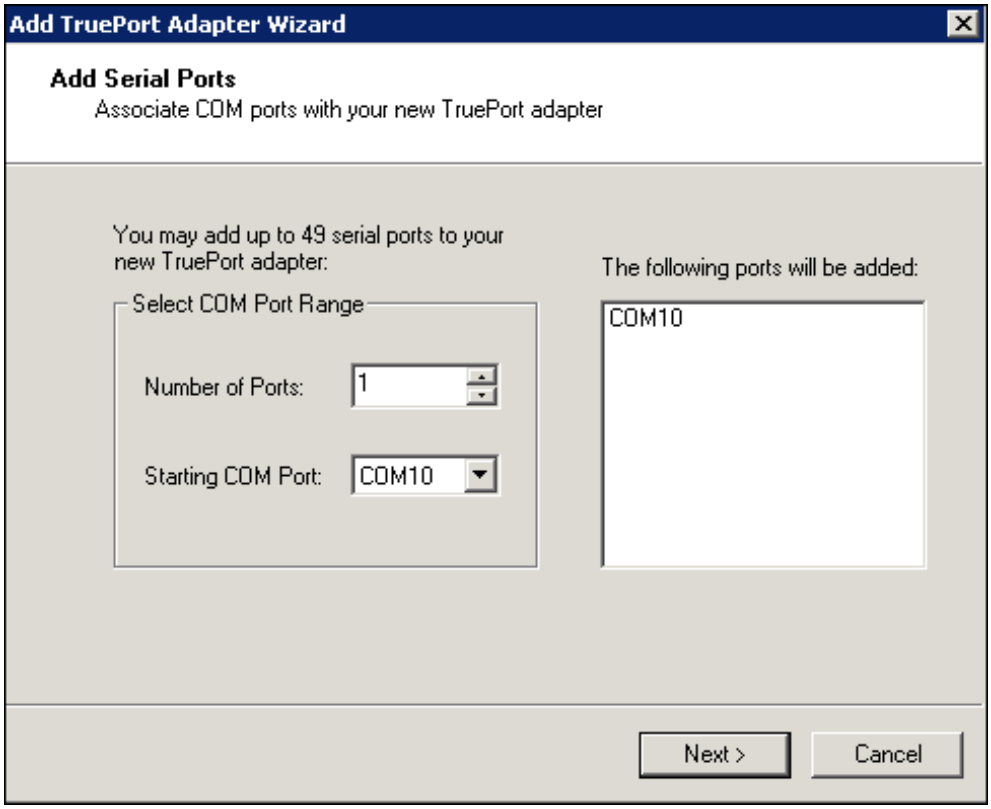
4. Enter a name for the TruePort Adapter.
   NOTE: This adapter will serve a particular device and therefore map to a specific COM port. Try to make the name descriptive so that the adapter can easily be tracked back to a particular device.
5. Enter the IP Address or the Hostname the device is using,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



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**.



⇨ 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**.

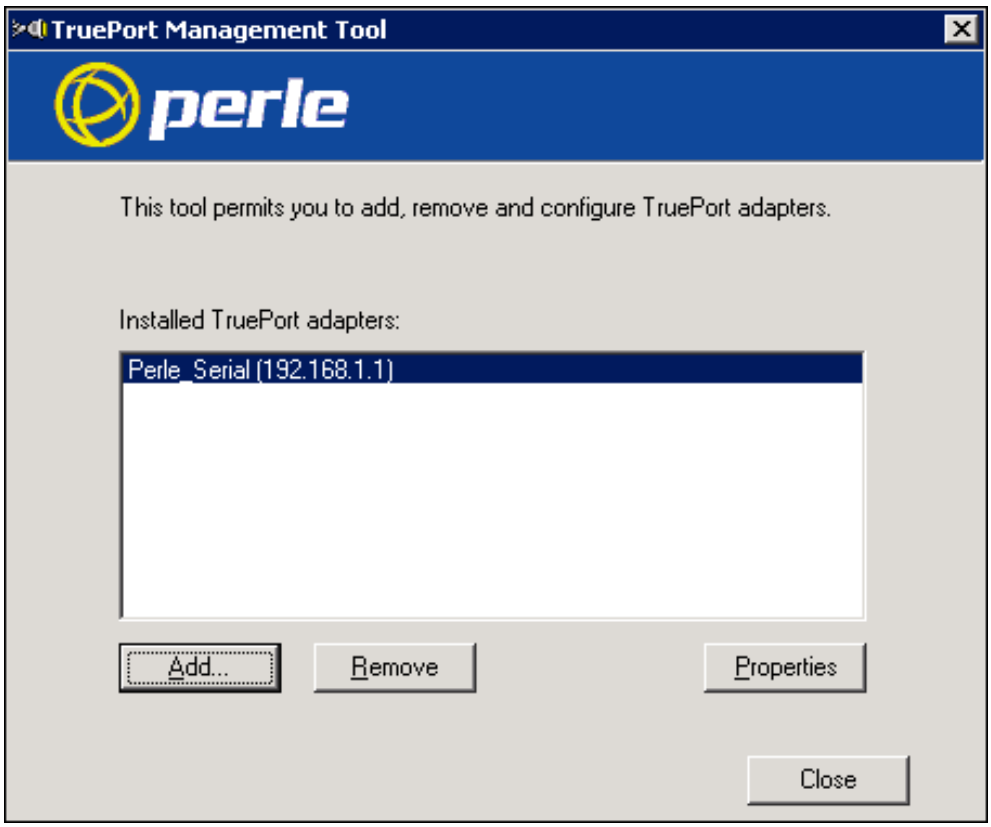
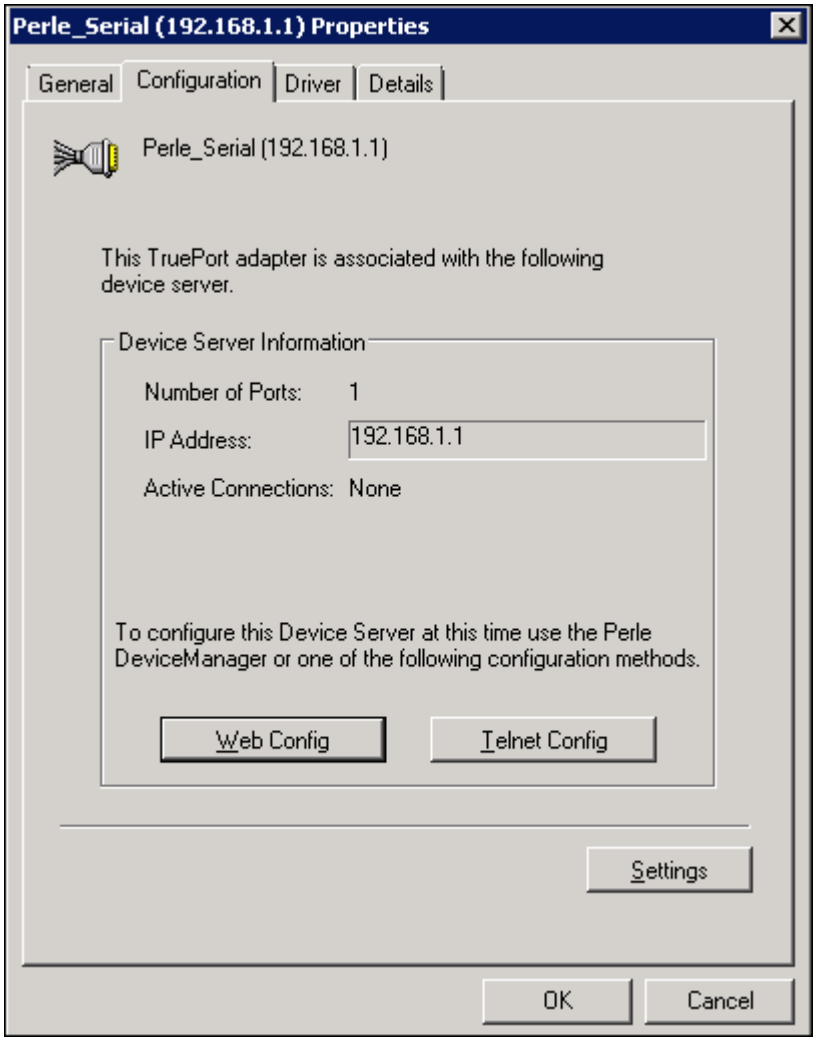


Fig. 18: Installed TruePort Adapters

ESPA Paging System - Serial Settings

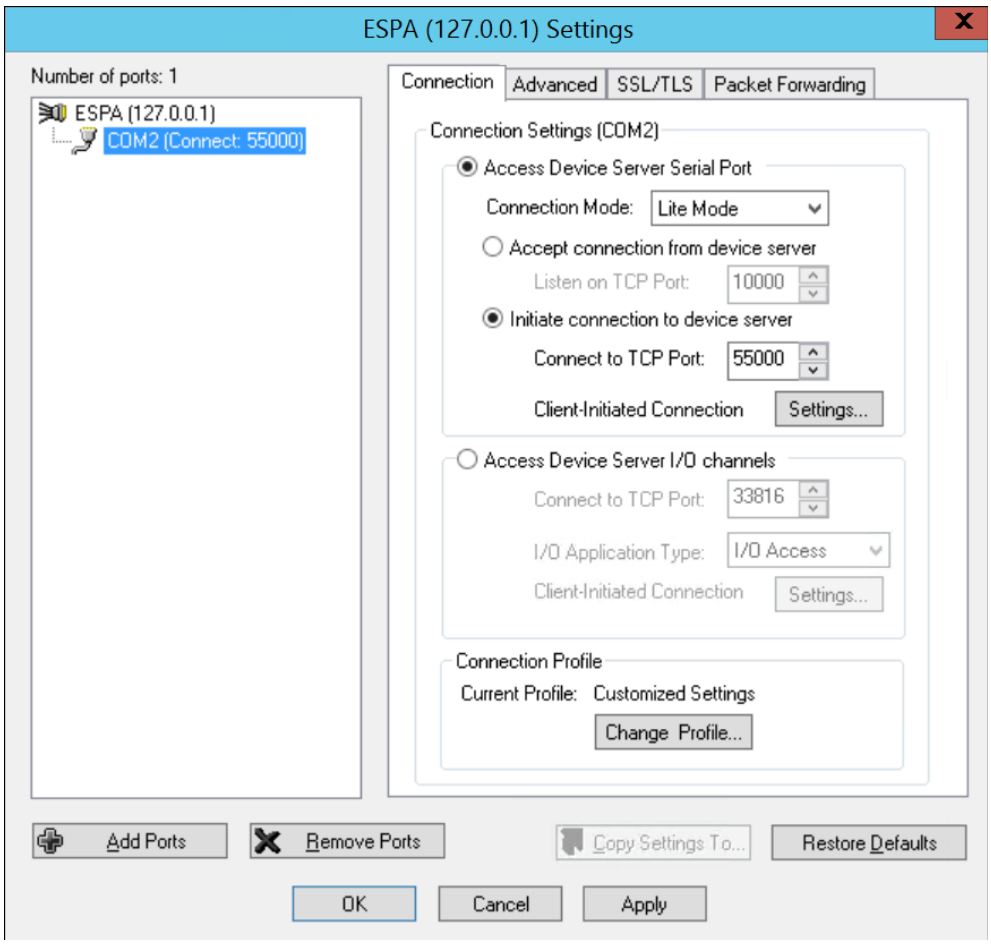
1. Select the Properties window of the device port to be configured, click the **Configuration** tab and then click **Settings**.



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

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

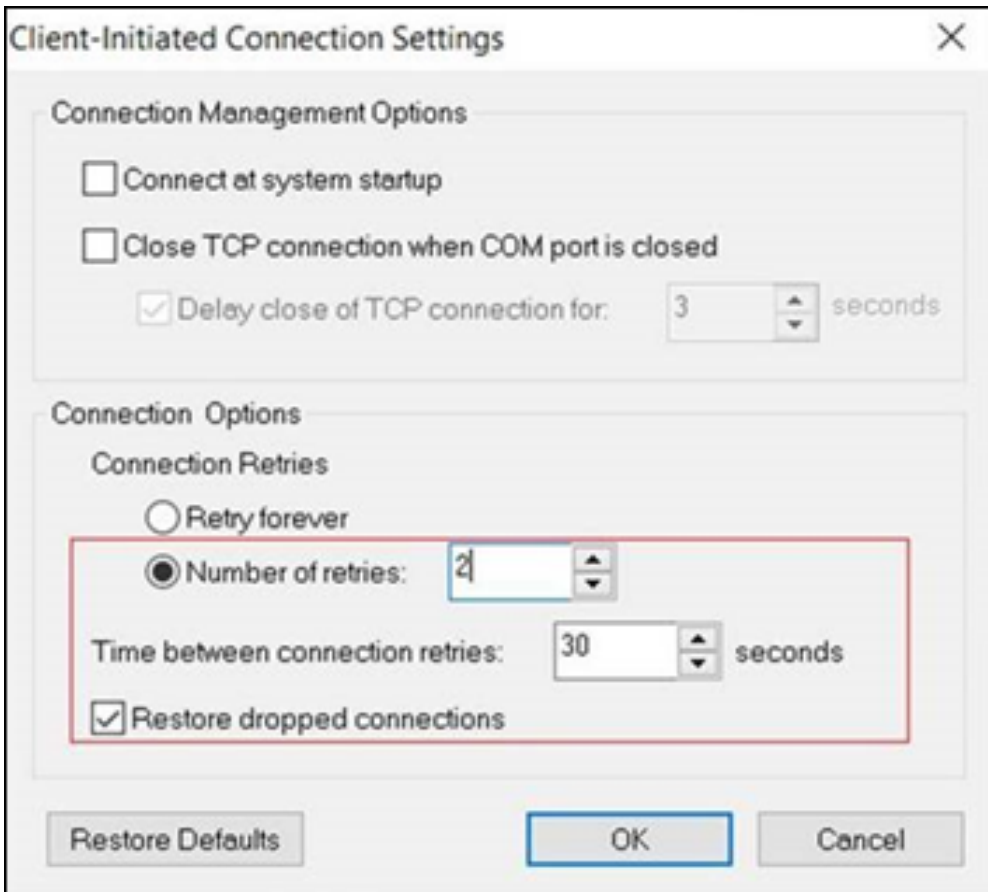
3. Select the **Connection** tab.
4. Select **Initiate connection to device server**.



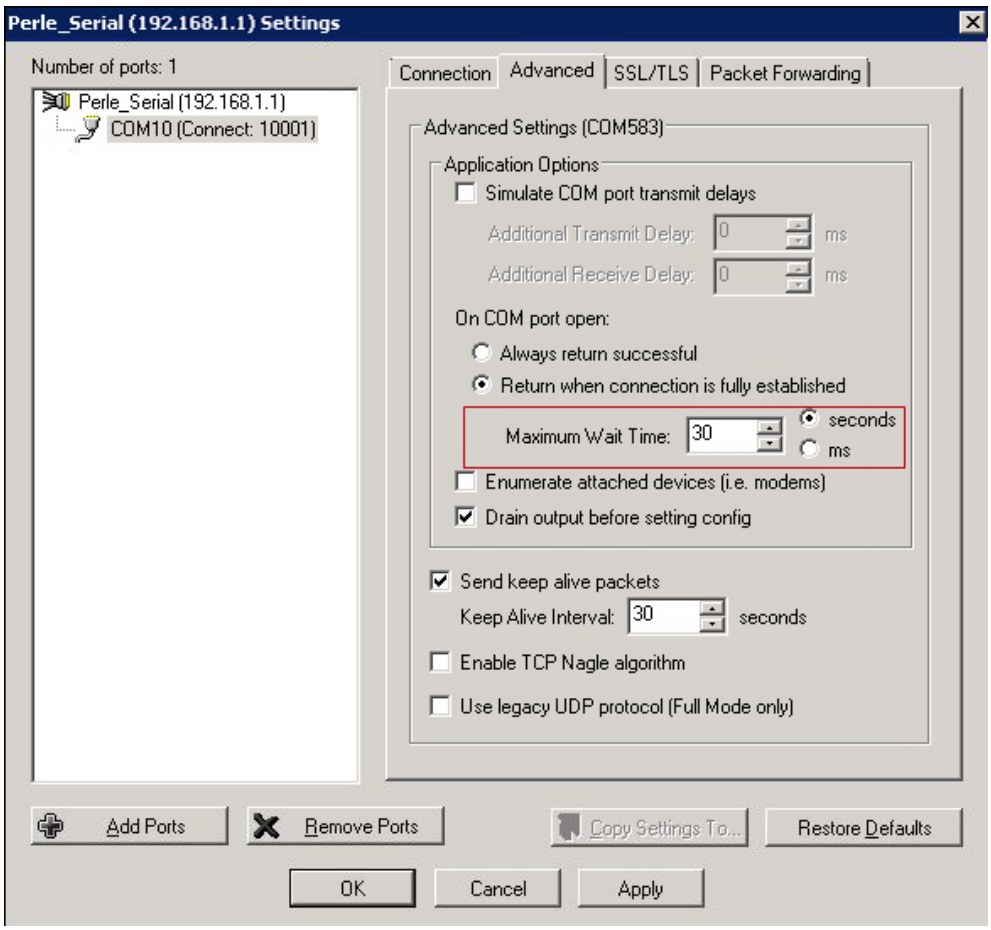
– Select **Connect to TCP Port**, enter the port number that was previously assigned to the device through the Perle DeviceManager.

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

   ⇨ The following window displays:

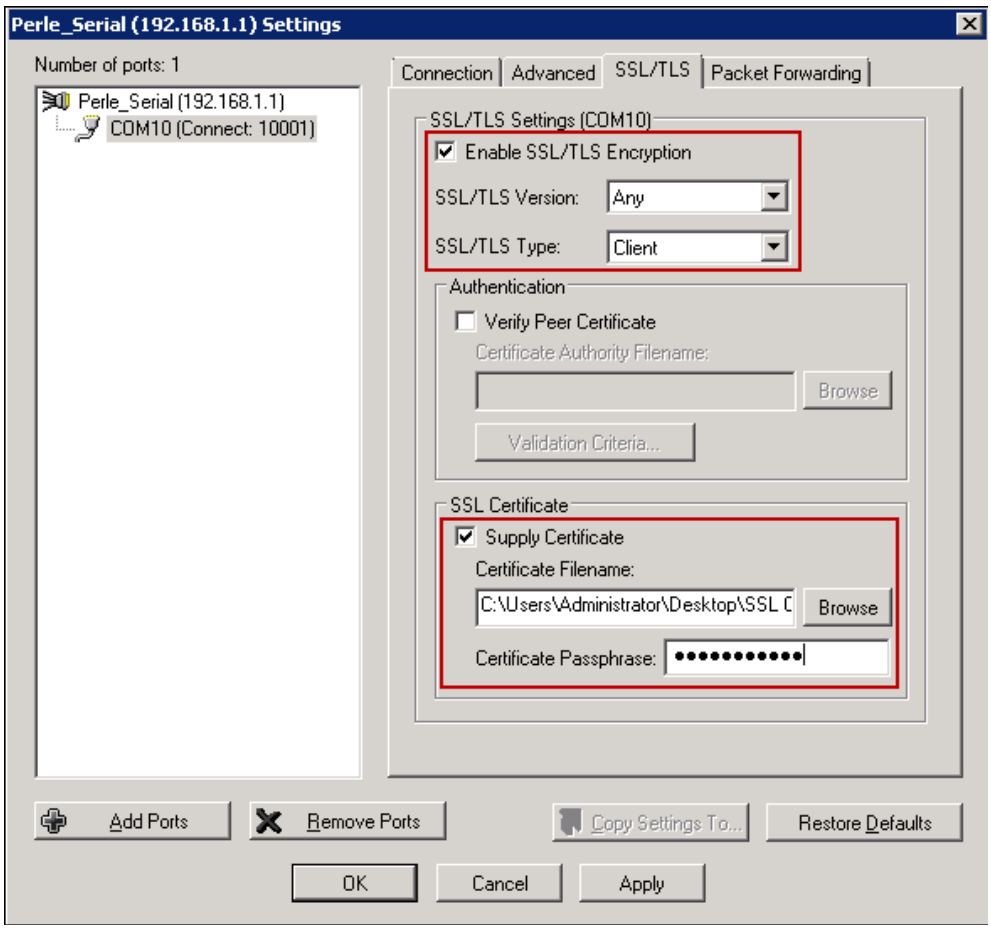


6. Select the **Connect at system startup** check box.
7. For **Connection Retries**, select **Retry forever**.
8. Click **OK**.
9. Click the **Advanced** tab.



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

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



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:

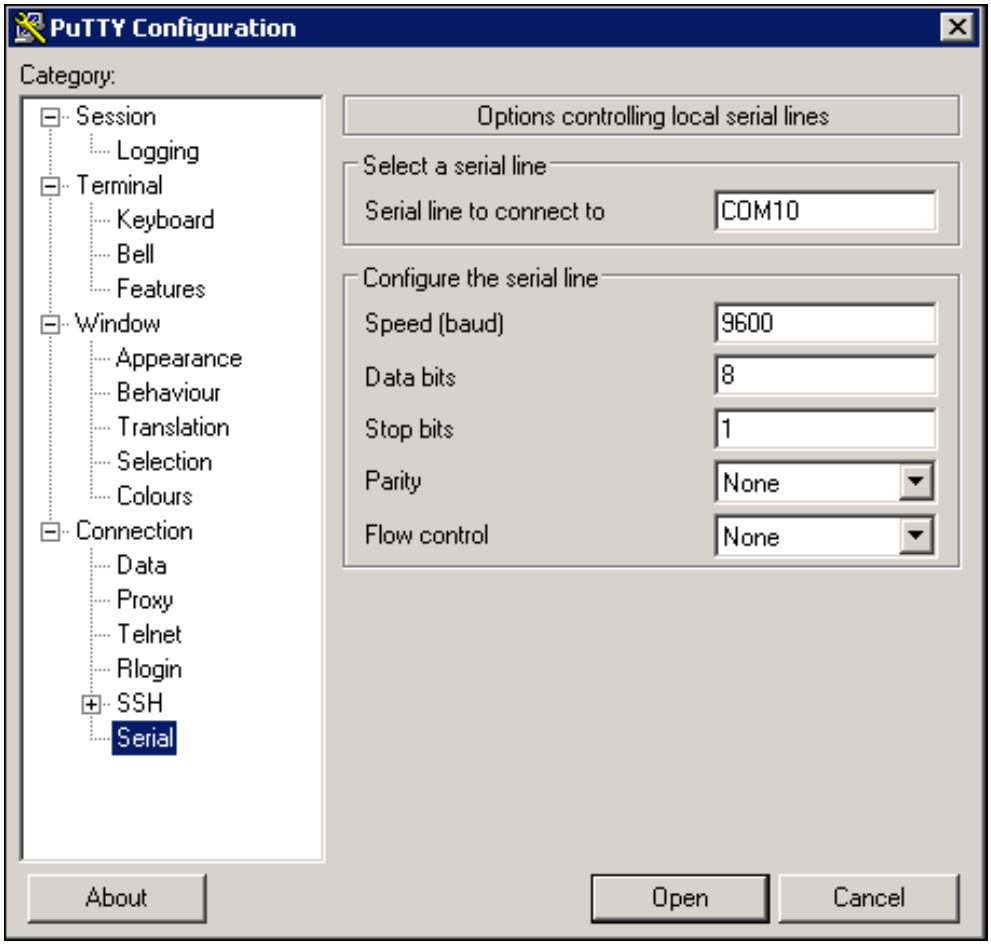
http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe

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.



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 *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.

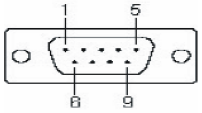
⇨ After a few seconds, the **Link/10/100** should be solid amber or green.
NOTE: Amber refers to a 100Mb connection. Green refers to a 10Mb connection.
NOTE:
The device does not have DHCP turned on as factory default. Configure the device to use DHCP or assign a static IP with a computer that is attached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

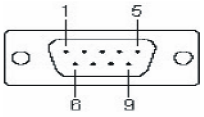
NOTE:
Keep the Console/Serial switches on the device in OFF position.



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. 19: 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			

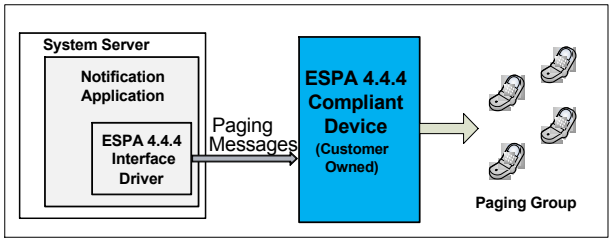
Fig. 20: TD2R2 Pinout

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.

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

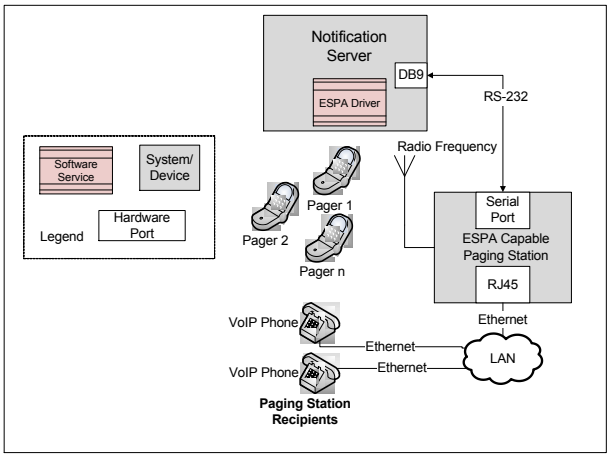


Note 1: The paging messages launched by cannot be canceled. only supports Launch operations for paging messages.

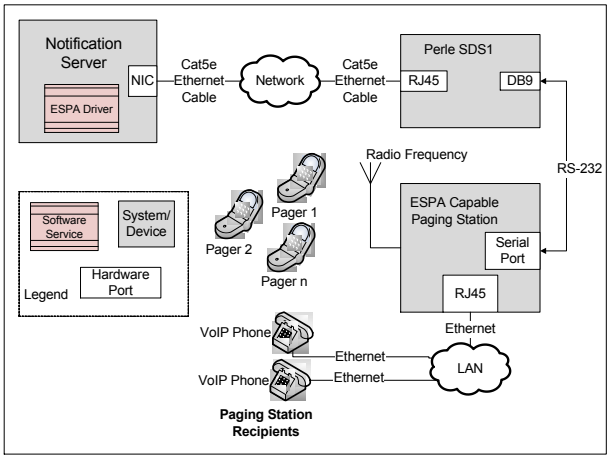
Note 2: The ESPA 4.4.4 protocol supports up to 128 characters. However, the ASCOM device currently tested with supports 120 characters.

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

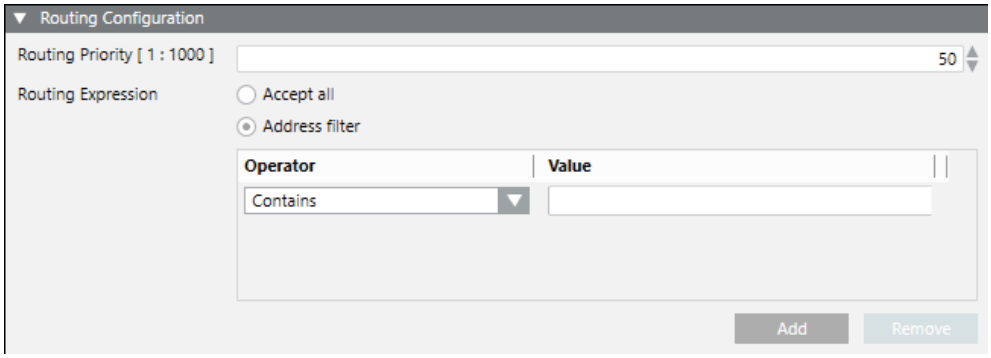
Configuration Properties

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 system. If the delivery is not successful, the ESPA managed device sends the negative acknowledgement to the 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 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, will search for either the value specified under **Starts with** or **Contains** operators.



- **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.

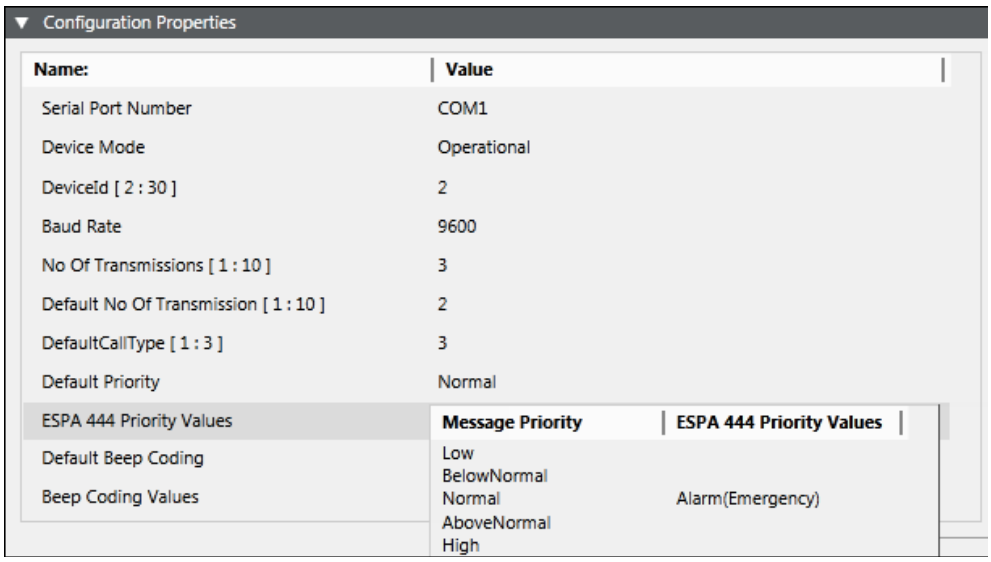
ESPA Paging System - Operator

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.

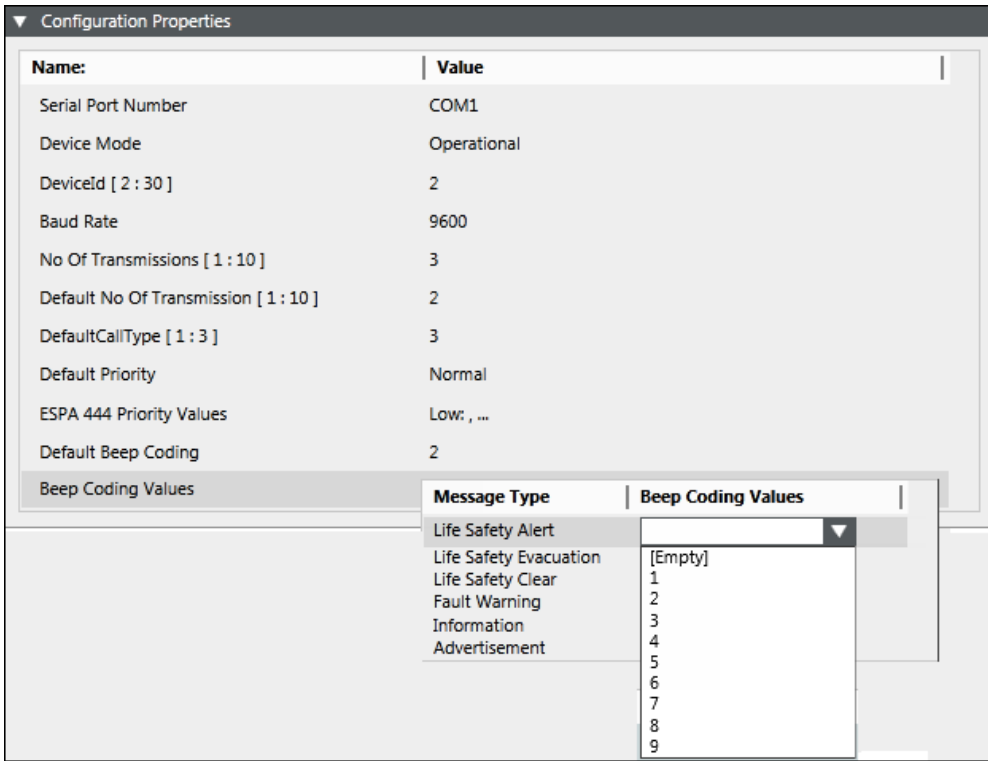
ESPA Paging System - Device Capability Mapping to Message Priorities

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.



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.



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.

1.9 Export DME File

Export DME File

The .dme is a binary file that consists of all the configuration settings for a particular Perle device. After completing the configuration, user can save the configuration values as a backup by creating a .dme file for a particular device. The .dme file can be used to restore the configuration of the perle device. The .dme file can also be used to configure similar Perle devices with minimal modifications in the configuration settings.

Complete the following steps to save a backup (.dme file) of the Perle device configuration file:

1. Open the **DeviceManager**.
   ⇨ A list of all the devices available in the network displays.
2. Select the device whose configuration setting is to be saved as a dme file.
3. In the **Establish Connection to** dialog box, click **OK**.
4. In the **Login** window, enter the device password. The factory default password is **superuser**.

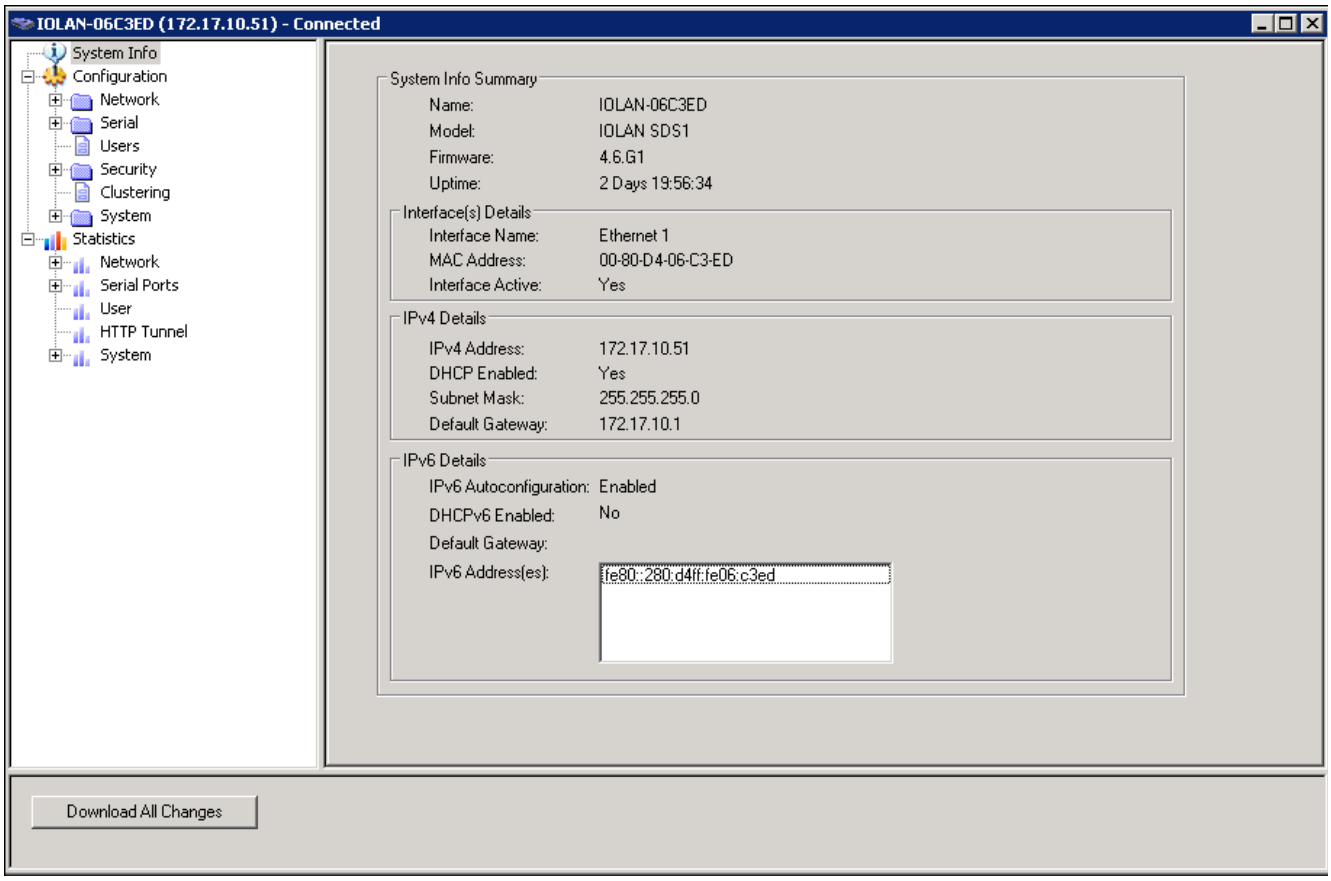


Fig. 21: System Info dialog box

5. From the menu, select **File**, and click **Save As**.
6. In the **Save As** dialog box, specify a name and format for the file.
   NOTE: Save the file as .dme file.

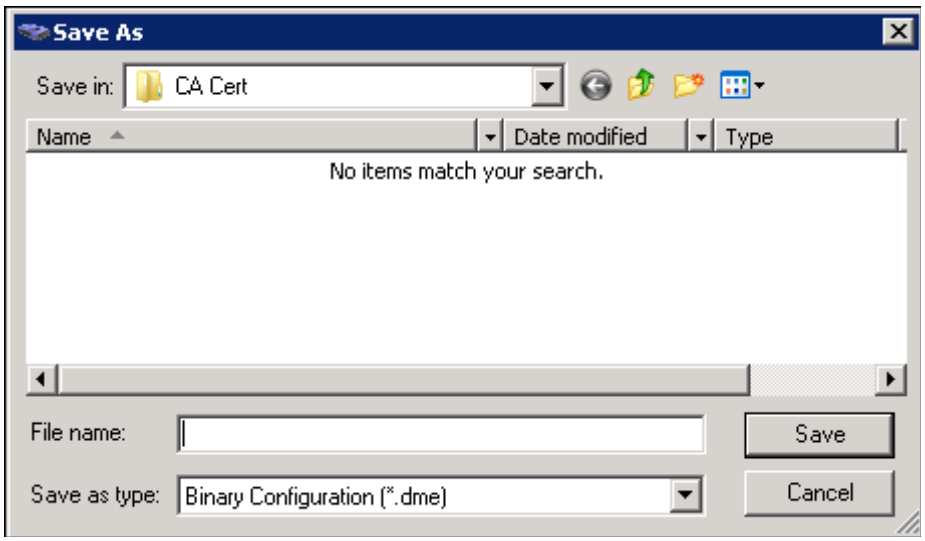


Fig. 22: Save As dialog box

7. Click **Save**.

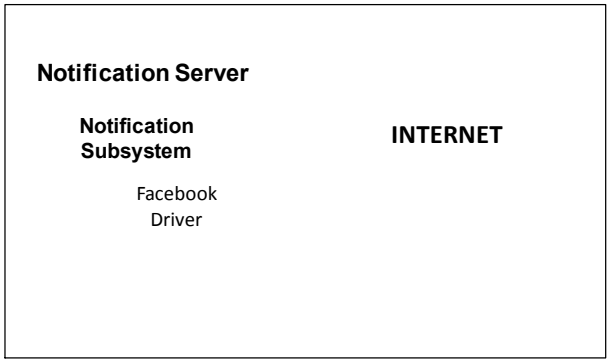
⇨ The Perle device configuration setting is successfully exported to the .dme file.

1.10 Facebook Device

Facebook Device

This section provides reference and background information for integrating the Facebook device. For procedures and workflows, see the step-by-step section.

has the capability to send messages to Facebook. The users can use an existing app or create a new app on Facebook for receiving the messages sent by . This occurs when incidents are initiated within targeting the Facebook device configured into the system. This will appear as a **Status Update** in the Facebook account configured with the device.



Other Facebook users **following** the app created on Facebook, for example, the app will then be able to receive these status updates on their Facebook accounts. In the case of message delivery failure due to network interruption, the system makes three attempts to successfully deliver a message to a Facebook account. If cannot successfully deliver a message to Facebook after three attempts, the message will be marked as failed in the user interface.

Facebook Device

This section provides additional procedures for integrating the Facebook device.

For workflows see the step-by-step section.

Facebook Account Creation and Registration

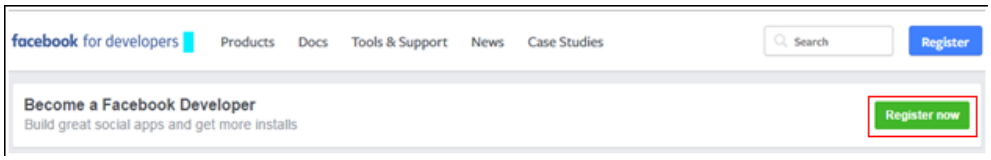
For to be able to post comments on Facebook, an account needs to be created. This should be followed by registering the system with the newly created account. It is then possible for the system to post comments using the registered account.

Notification Application Registration

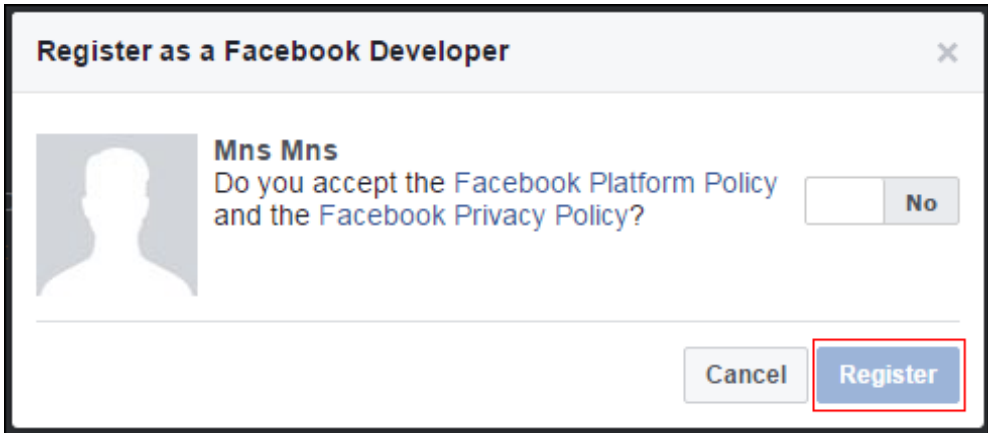
Follow the steps below to register with the Facebook account just created. The Facebook procedure requires validating the identity of the account and it may take up to two months before a Facebook app can be created with the account. This activity needs to be completed before proceeding further. Follow the steps detailed in the following section to complete this activity.

Register New App

1. If an app is not already available in the account, the account needs to be registered as a developer.
2. Select the URL https://developers.facebook.com/apps and enter the credentials to log on to the account.
3. In the **Become a Facebook Developer** dialog box, click **Register Now**.



4. If you agree to the terms and conditions, click **Yes** to accept the **Facebook Platform Policy** and **Facebook Privacy Policy**.



5. Click **Register**.
6. Follow the steps to verify the account.
   NOTE 1: Depending on the location, the user may be required to enter different means for confirmation, such as a mobile phone number or an email. Follow the steps presented by the Facebook site.

⇨ On successful registration, click **Create App** to create new application.

General Guidelines

Due to the dynamic nature of the Facebook User Interface, detailing every required step is beyond the scope of this document. This document is tested on Facebook API version v2.8.

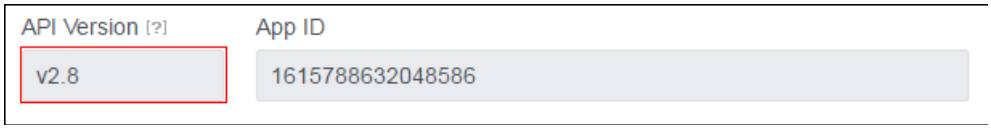
In case, the instructions given in the guide and the Facebook User Interface do not match, the user can create and configure the Facebook app for pages, by referring to the link https://developers.facebook.com/docs/apps/register. The user can also search for the below mentioned fields and set the required values.

The following table lists the field names along with the values:

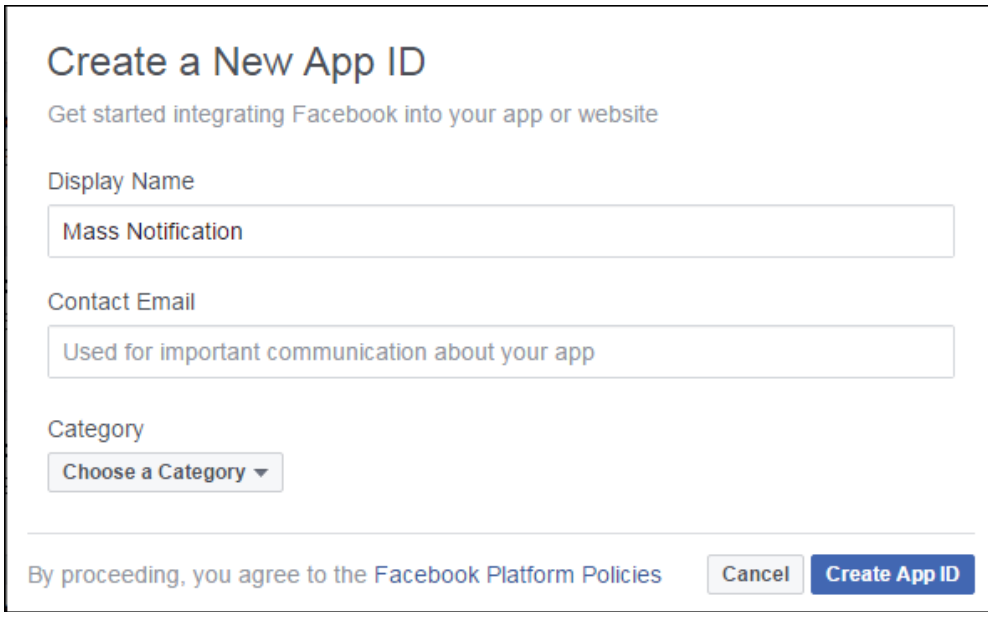
Field	Location (may vary depending on the Facebook version)	Value
Require App Secret	Settings>Advanced>Security	NO
Allow API Access to App Settings	Settings>Advanced>Security	NO
Client OAuth Login	Add Product	YES
Web OAuth Login	Add Product	NO
Embedded Browser OAuth Login	Add Product	YES

Create New App

▷ This document is tested with Facebook API Version **v2.8**.



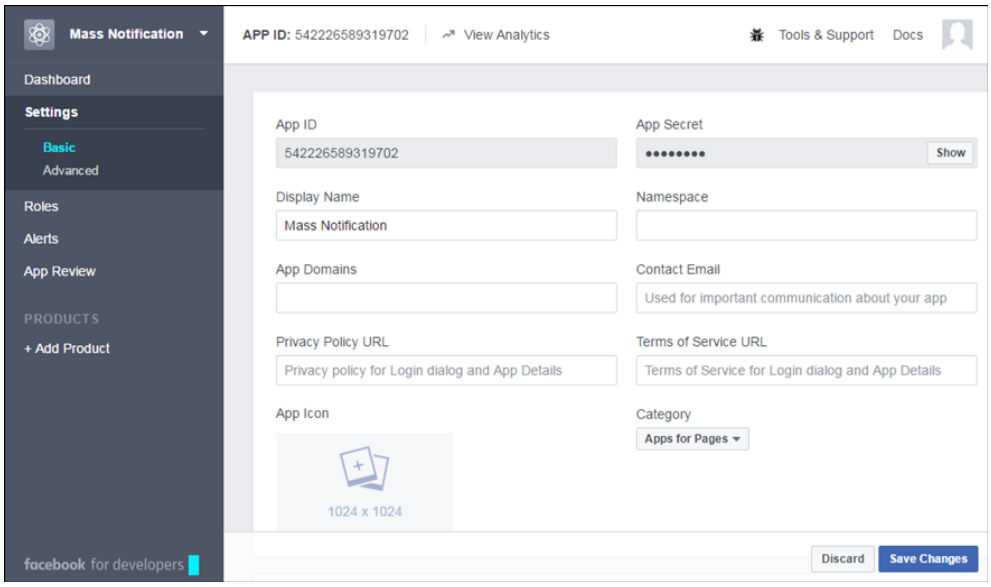
1. Select the URL https://developers.facebook.com/.
2. Log on to the Facebook Account using a valid user name and password.
3. Select **My Apps**, select **Add a New App**.
   ⇨ The **Create a New App ID** dialog box displays.



4. Enter a name for the App, for example, **Mass Notification**.
5. Enter contact email ID.
6. Select **Apps for Pages** from the **Category** drop-down list.
7. Click **Create App ID**.
8. Complete the **Security Check**.
   ⇨ The App is now created.
9. Click **Settings**. The page displaying the basic settings of the app should be visible.

   NOTE: Write down the values in the **App ID** and **App Secret** fields. The value

in the **App Secret** field is displayed after clicking **Show**. The values specified in the **App ID** and **App Secret** fields are needed for configuring the device in .



10. Click **Save Changes**.

Using an already existing app

If an app has already been created and is available for use, follow the steps below to select the application settings page. This is necessary before proceeding to the configuration step.

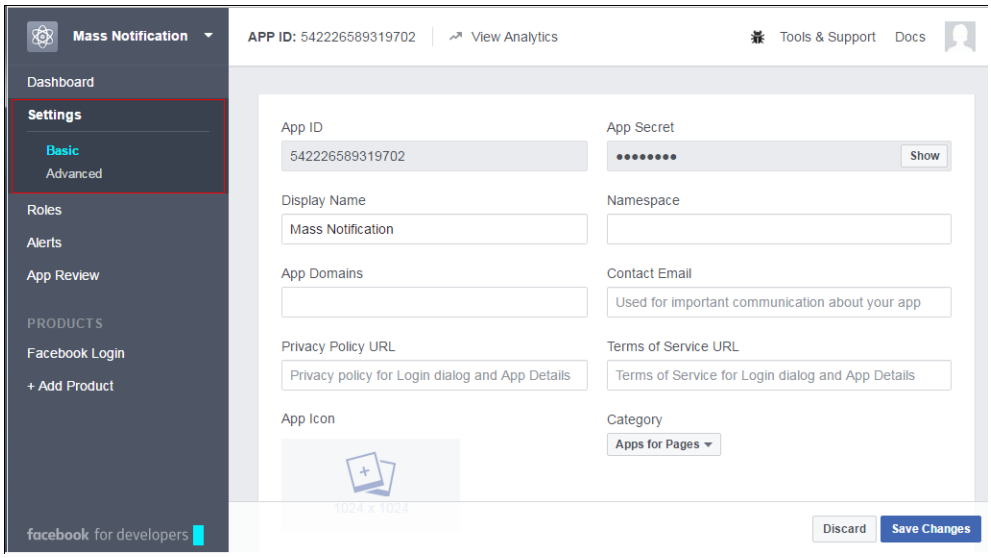
1. Select the URL https://developers.facebook.com/apps and enter the credentials to log on to the account.

   ⇨ The available apps display.

2. If more than one app is created, choose the app to be used with .

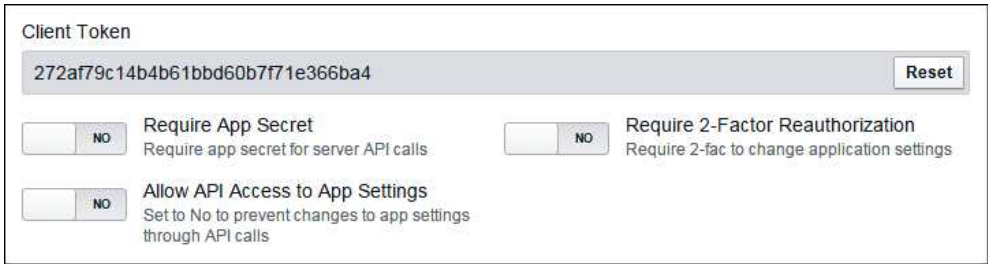
Configuring Application Settings

1. Click **Settings** to edit the configuration settings for the configured app.



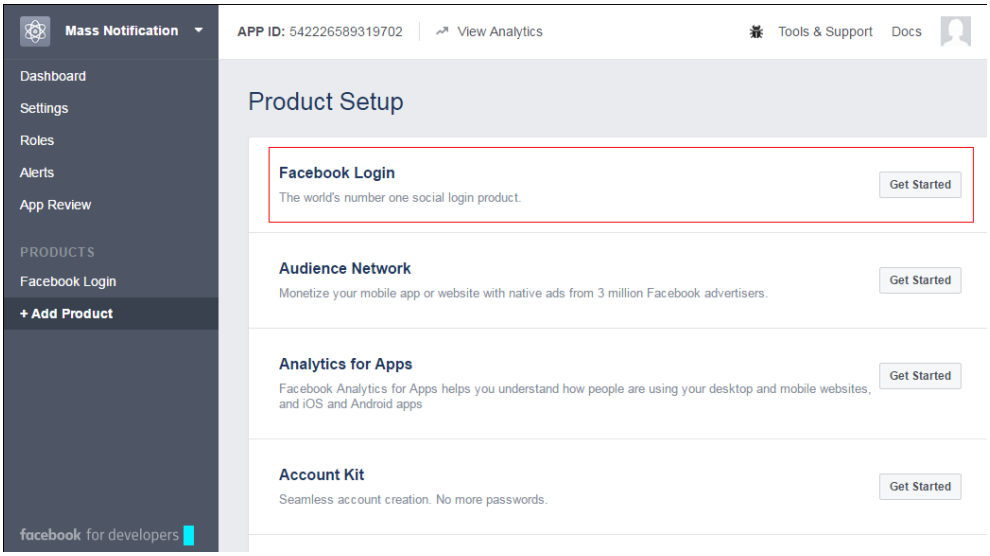
   ⇨ The values for the basic settings display.

2. Edit the **Display Name** and **Contact Email** fields.
3. Click **Save Changes**.
4. Select **Advanced**.
5. In the **Client Token** expander, do the following:
   a. Select **NO** for the **Require App Secret** field.
   b. Select **NO** for the **Allow API Access to App Settings** field.
   c. Leave the other fields as default.
   d. Leave the **Migrations** setting as default.



6. Click **Save Changes**.
7. Click **Add Product** from the left pane.

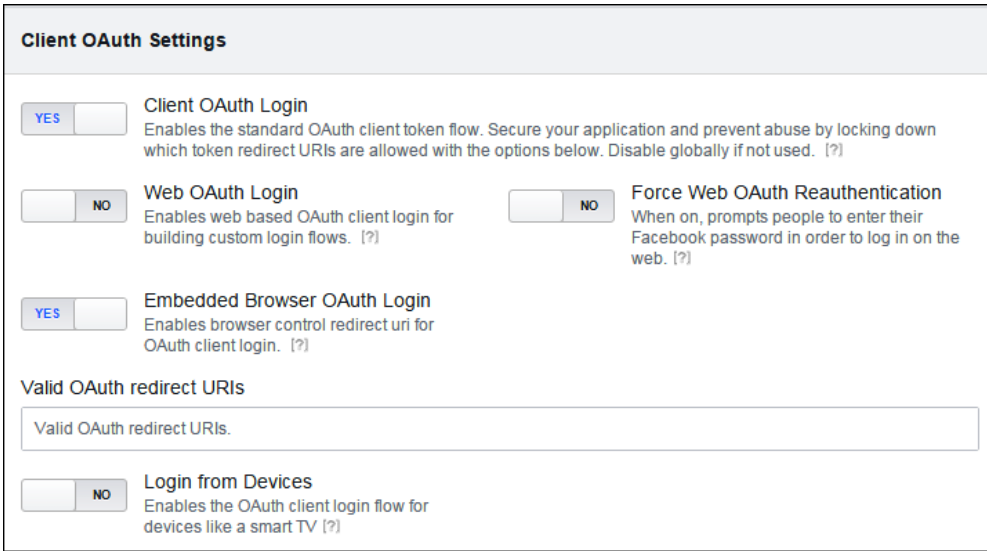
   ⇨ The **Product Setup** option displays.



8. Click **Get Started** next to **Facebook Login**.

   ⇨ The **Client OAuth Settings** option displays.

9. In the **Client OAuth Settings** expander, do the following:
   a. Select **YES** for the **Client OAuth Login** field.
   b. Select **NO** for the **Web OAuth Login** field.
   c. Select **YES** for the **Embedded Browser OAuth Login** field.
   d. Leave the other fields as default.



10. Click **Save Changes**.

⇨ The application settings have now been configured for the Facebook app.

EN - Facebook Account Creation

1. Select the Facebook homepage at https://www.facebook.com/.
2. Fill in the details in the **Sign up** section or **Create an account** section.
3. Click **Sign up** or **Create my account**.
4. Proceed to the next steps once the account is successfully created and post one or more status updates throughout the Facebook website interface.
   NOTE 1:
   The above workflow is only needed when a customer/organization does not

have a Facebook account that they want to use.
NOTE 2:
If all Internet traffic is to be routed through an authenticating proxy, then the Facebook driver needs to be deployed only on the main Server and not on the Front End Processor (FEP). If deployed on FEP, there can be authentication problems when the Facebook driver attempts to access the Internet. Refer to 's *Installation* section for more information on Server and FEP.
NOTE 3:
Go through Facebook's Terms of Use and follow the rules set forth by Facebook. The rules are still valid even when making posts to the Facebook account through .
NOTE 4:
The aim of this document is to familiarize the user with what to expect on the Facebook site.

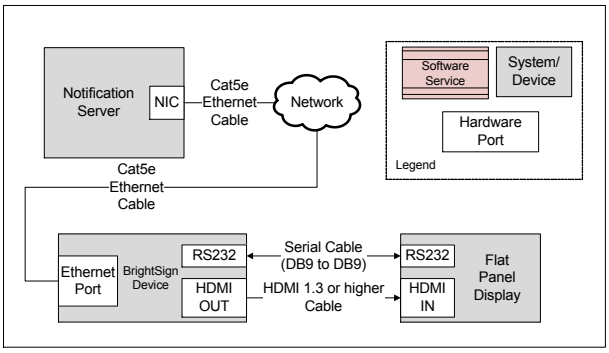
1. Select the Facebook homepage at https://www.facebook.com/.
2. Fill in the details in the **Sign up** section or **Create an account** section.
3. Click **Sign up** or **Create my account**.
4. Proceed to the next steps once the account is successfully created and post one or more status updates throughout the Facebook website interface

NOTE 1:
The above workflow is only needed when a customer/organization does not have a Facebook account that they want to use.
NOTE 2:
If all Internet traffic is to be routed through an authenticating proxy, then the Facebook driver needs to be deployed only on the main Server and not on the Front End Processor (FEP). If deployed on FEP, there can be authentication problems when the Facebook driver attempts to access the Internet. Refer to 's *Installation* section for more information on Server and FEP.
NOTE 3:
Go through Facebook's Terms of Use and follow the rules set forth by Facebook. The rules are still valid even when making posts to the Facebook account through .
NOTE 4:
The aim of this document is to familiarize the user with what to expect on the Facebook site.

1.11 Flat Panel Display Device

Flat Panel Display Device

The flat panel display is capable of receiving and displaying multimedia downloaded by the BrightSign devices. The flat panel display is connected to the media controller through a HDMI cable, for delivering multimedia, and a RS-232 cable. The RS-232 cable is used by the BrightSign device to control certain parameters of the flat panel display such as ON/OFF, volume adjustment, and video input selection.



All content delivered by the BrightSign device is downloaded from the server.

The BrightSign device can very easily support any type of flat panel display as long as the corresponding flat panel display meets the following criteria:

- 1920x1080 resolution
- HDMI video input
- External control through RS-232C

Flat Panel Display Device

This section provides additional procedures for integrating the Flat Panel Display device.

For workflows see the step-by-step section.

Installing Flat Panel Display Device

This section provides the user information on mounting the hardware and wiring / connection details for the device.

Prerequisites

- BrightSign XD1033 media controller, firmware version 6.2.94 or greater.
- RS232 communication cable (DB9 female controller end). Check the LCD model to determine whether the cable is straight through or null modem type, and whether the serial port requires a female or male end. Maximum cable length between the media controller and flat panel display should be 50 feet. **NOTE:** Check the LCD model to determine whether the cable is straight through or null modem type, and whether the serial port requires a female or male end.

Display Model	Connector on Monitor	Serial Cable for Commanding	Connector on Media Controller
Sharp PNE421	DB9-M (Input Port)	F----------F (Straight Through)	
Sharp LC42D69U	DB9-M	F----------F (Null Modem)	
Samsung LC-400FP3	DB9-M (Input Port)	F----------F (Null Modem)	
Samsung ED46D	Stereo 3.5 mm Jack	M----------F (TRS Connector)	

The following serial cable part numbers can be ordered from Siemens SAP:
52038 - Female to Female Null Modem Cable
52035 - Female to Female Straight Through Cable
52030 - Female to Male Straight Through Cable
52184 - Female to Male Null Modem Cable

- Line cord for AC power (included with flat panel display).
- HDMI Cable compatible with HDMI 1.3a or higher devices (included with the media controller).

NOTE: The Samsung models **ED32D**, **ED40D**, **ED55D**, **ED65D** and **ED75D** are also compatible with . Select **Samsung ED46D** in the **LCD Display Commanding** field to use the above models. Refer to the *Device Configuration Properties* section of the *Media Controller Integration Guide* for more information.

Disclaimer:
Prior to commissioning of system, a compatibility check should be performed for all devices and services to be integrated (refer to *System Description* document for compatibility information).

Mechanical Installation

To mount the flat panel display, follow the manufacturer's instructions for proper mounting and installation.

Electrical Installation

- Connect the HDMI cable to the HDMI port on both the flat panel display and the media controller. Refer to the TV manufacturer's operation manual to locate the HDMI port on the flat panel display.
  NOTE: Most flat panel displays contain multiple HDMI ports. Be sure to note which HDMI port will be used on the flat panel display, as this is required for remote control by and the media controller.
- Connect the RS-232 serial cable to the RS-232C port on the media controller. Refer to the flat panel display manufacturer's operation manual to locate the RS232C port on the flat panel display.
  NOTE: Check the LCD model to determine whether the cable is straight through or null modem type, and whether the serial port requires a female or male end. The media controller end of the RS-232 cable requires a female DB9 connector. The following table lists the serial cables required for some device models:

Display Model	Connector on Monitor	Serial Cable for Commanding	Connector on Media Controller
Sharp PNE421	DB9-M (Input Port)	F----------F (Straight Through)	
Sharp LC42D69U	DB9-M	F----------F (Null Modem)	
Samsung LC-400FP3	DB9-M (Input Port)	F----------F (Null Modem)	
Samsung ED46D	Stereo 3.5 mm Jack	M----------F (TRS Connector)	

- Connect the line cord to the power connector on the media controller. Refer to the flat panel display manufacturer's operation manual to locate the power connector on the flat panel display.

Installation Verification

Use the remote control included with the flat panel display to turn on the display. The flat panel display should display a **no signal** message.

Configuring and verifying Flat Panel Display Device

Follow the manufacturer's user manual on instructions for adjusting and configuring the flat panel display. Parameters that can be configured to the user's liking include the following:

- Brightness
- Tint
- Contrast

- Sharpness
- Color Intensity
- White Balance

1.12 GSM Modem Device

GSM Gateway

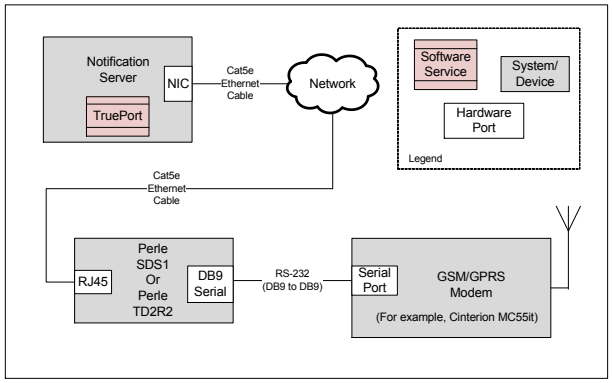
This section provides reference and background information for integrating the Global System for Mobile Communications (GSM) Gateway with the system. For procedures or workflows, see the step-by-step section.

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:

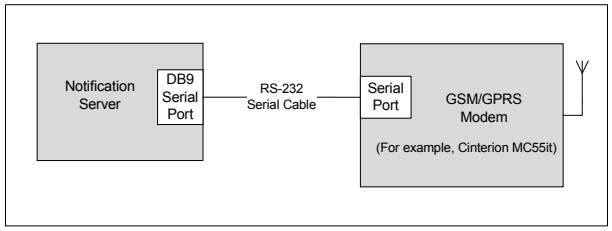


NOTE 1:
The GSM Terminal device accepts a SIM card that has SMS services enabled. Without enabling these services on a SIM card, you cannot send SMS through the device.

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:
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.

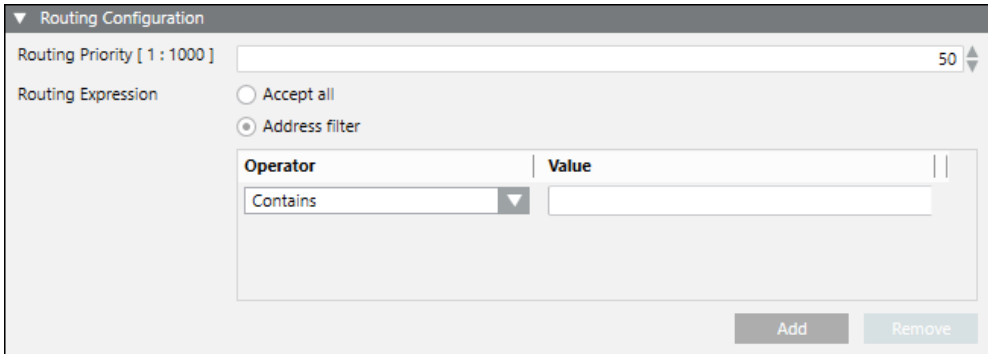
Below is an overview over the system using Serial Cable configuration:



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, will search for either the value specified under **Starts with** or **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 .

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

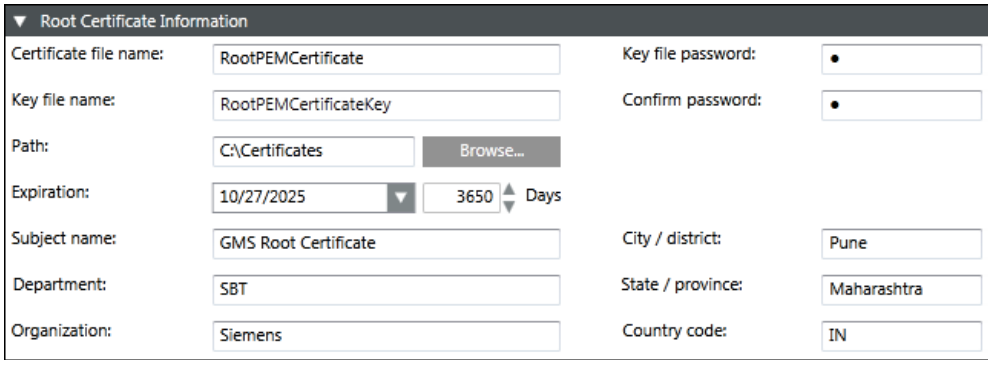
This section provides the steps linked with the configuration and verification of the device.

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.



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

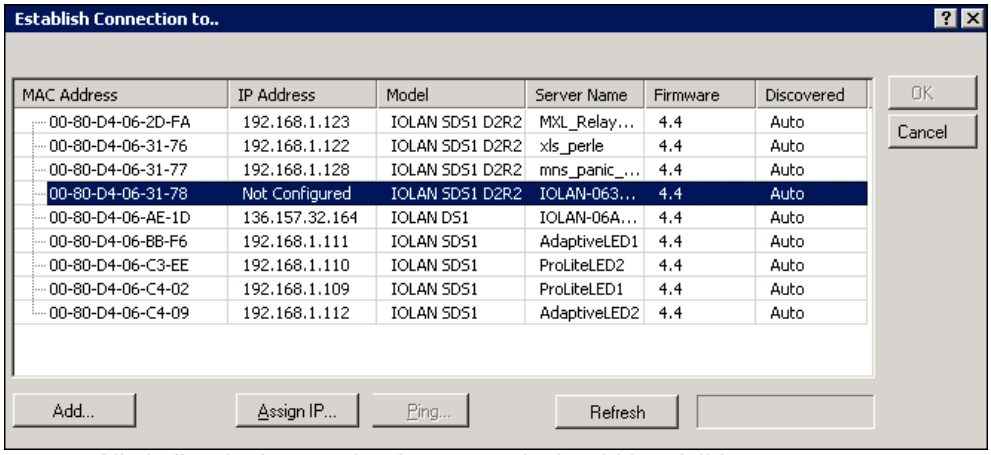
▷ Ensure that the DeviceManager is installed on a computer located under the same network as the device to configure.

▷ 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.

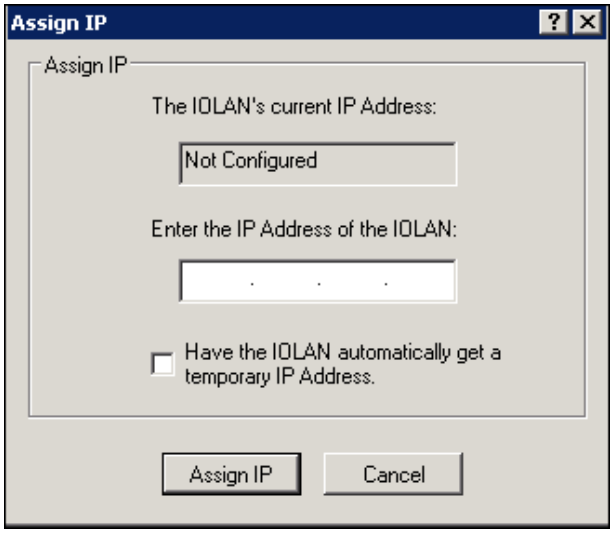
1. Start the DeviceManager.



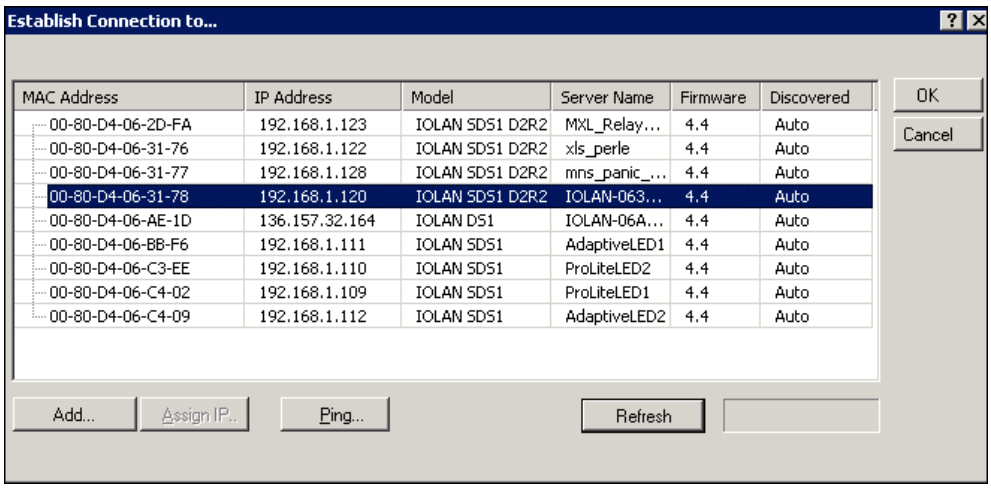
⇨ All similar devices under that network should be visible.

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**.



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



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**.

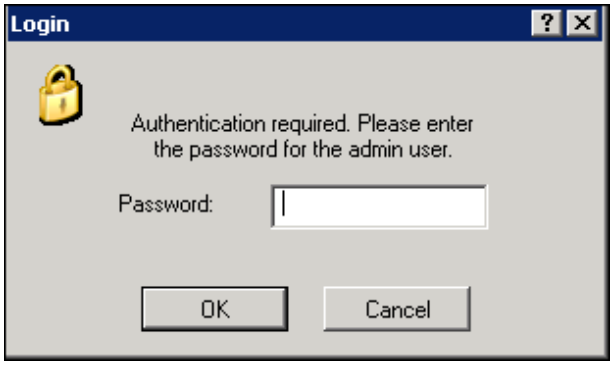
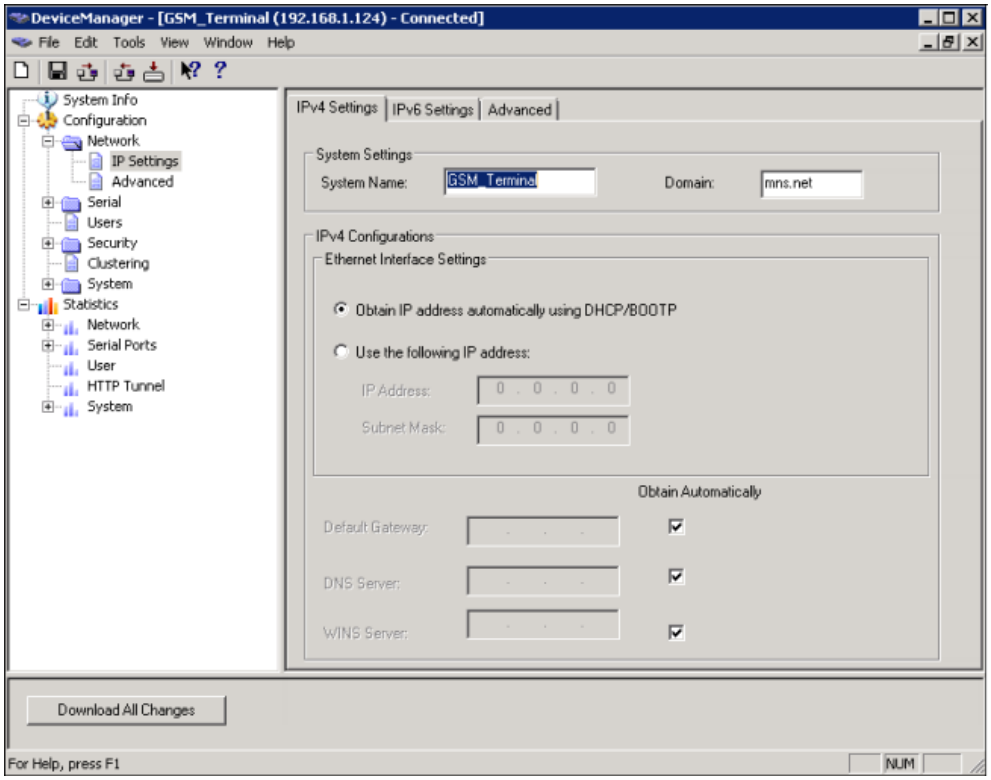


Fig. 23: Login window

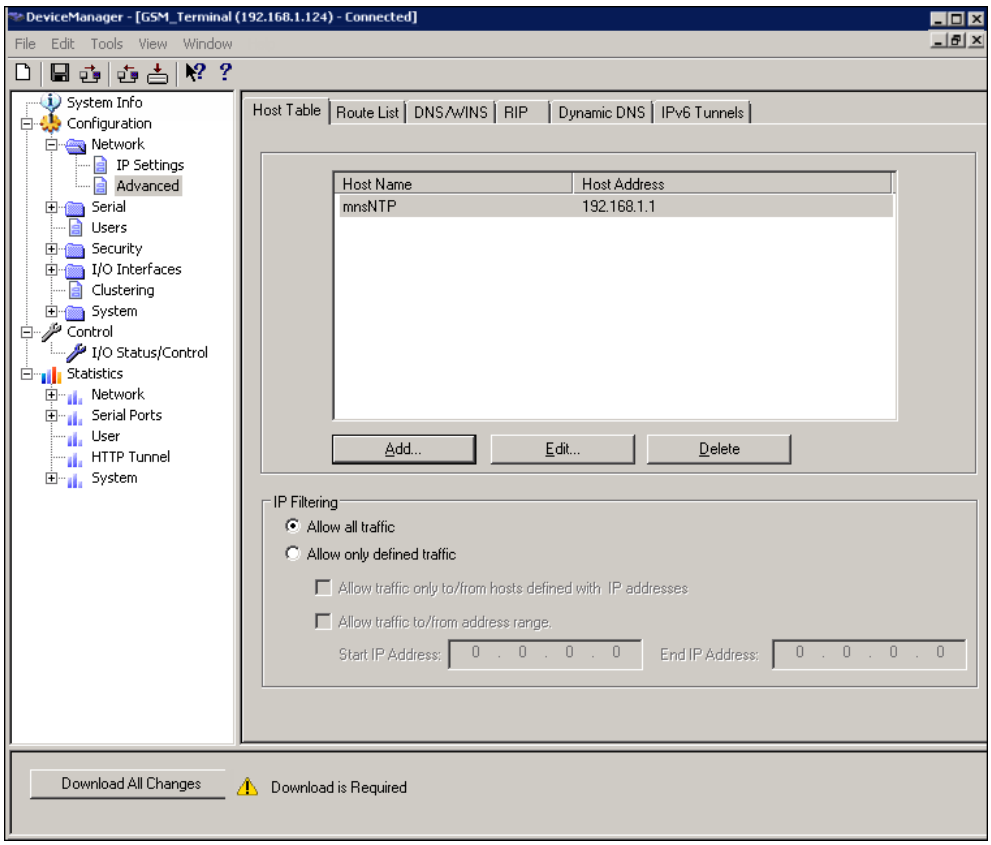
Network Setup

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**.



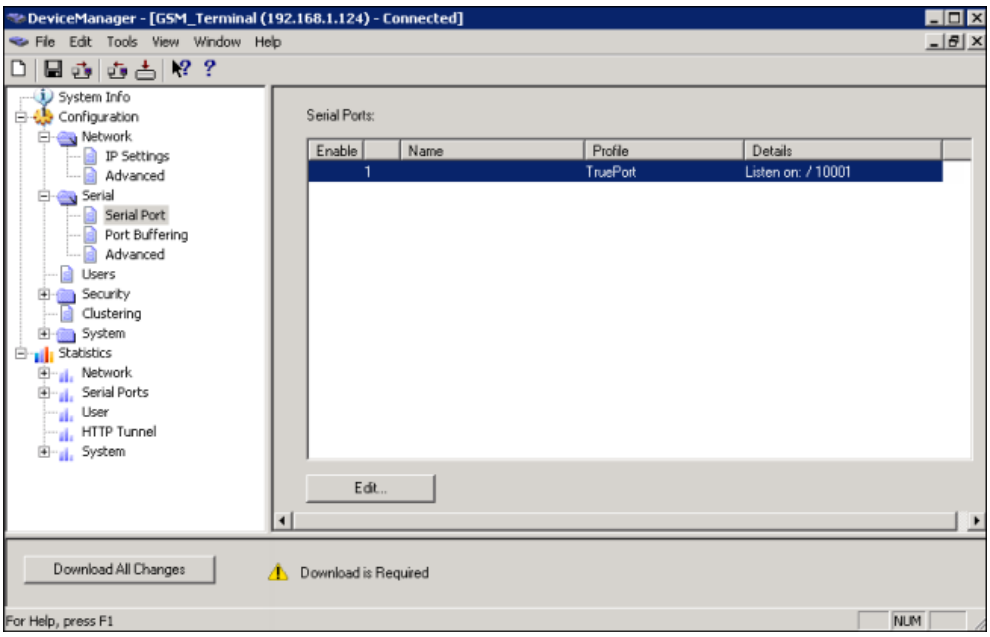
2. Select the **System Name** field, give the device a name that helps in distinguishing the corresponding device from other similar devices.
   NOTE 1: The System Name will also be used by the device to create a fully qualified domain name.
   NOTE 2: By default, the device is always **IOLAN** followed 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.



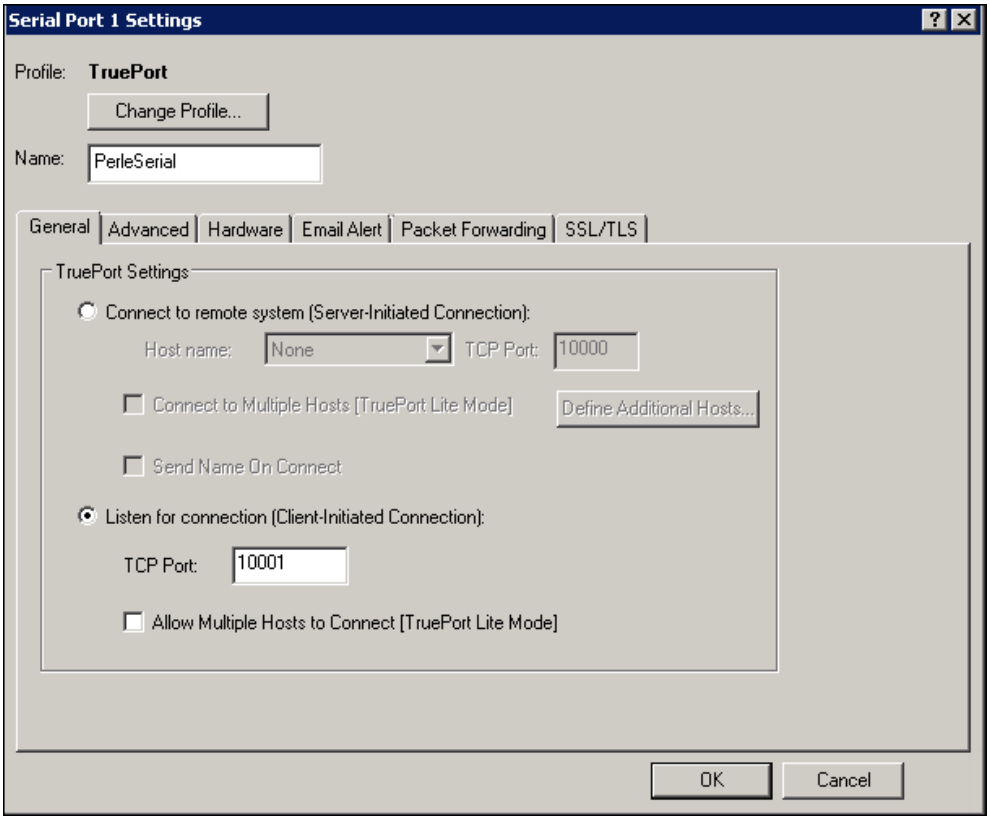
6. Select the **Host Table** tab, click **Add** to add an NTP host.
7. Enter a descriptive name for the NTP server. For example, **mnsNTP**.
8. Enter the IP address or the fully qualified domain name of an available NTP server.
   NOTE: An available NTP server is required to enable SSL on the device.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



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



⇨ 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)**.

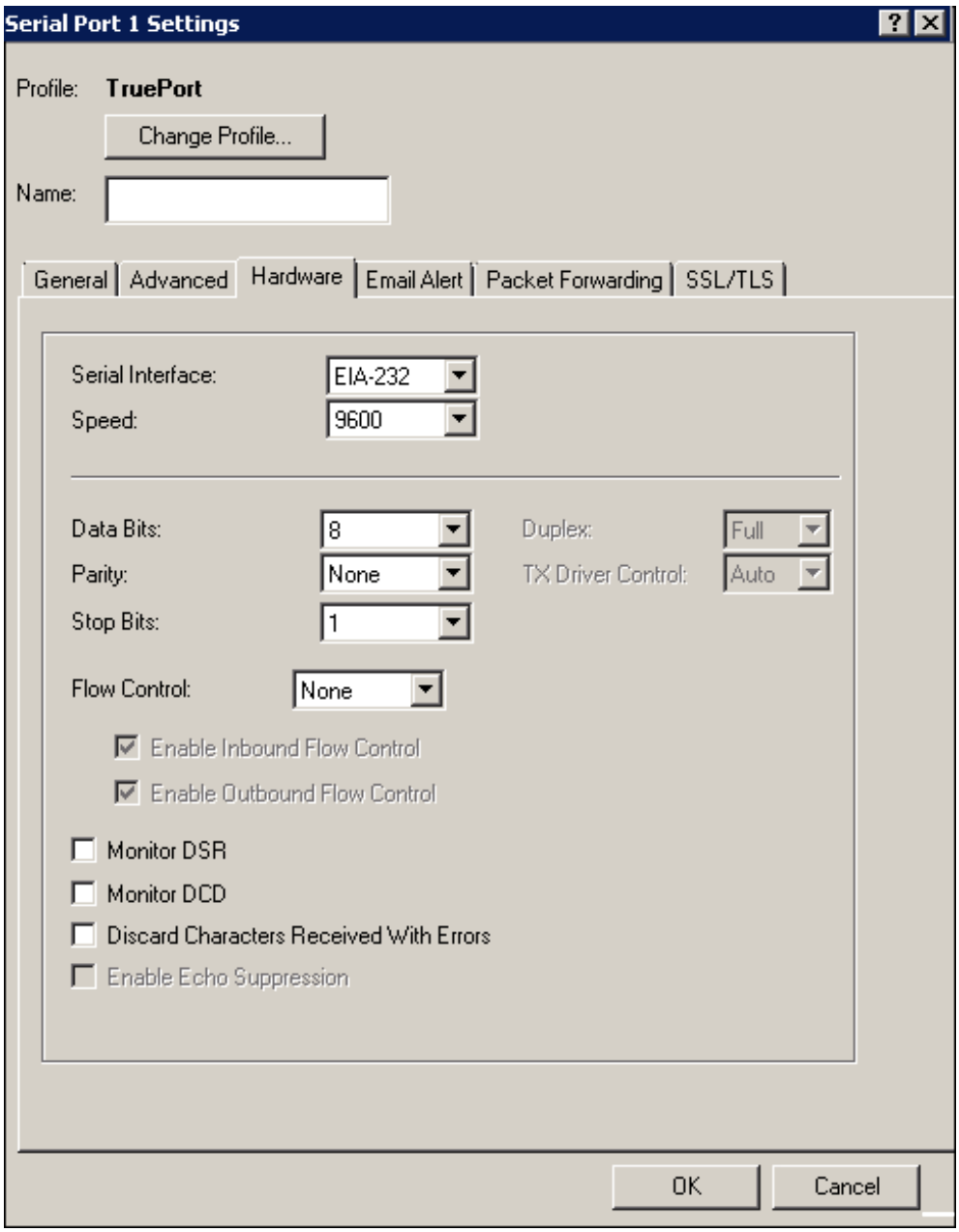
   ⇨ In this mode, the device will wait for the server to establish a connection.
8. Enter the TCP port needed to communicate to the device. By default, the TCP port is **10001**.

   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**.

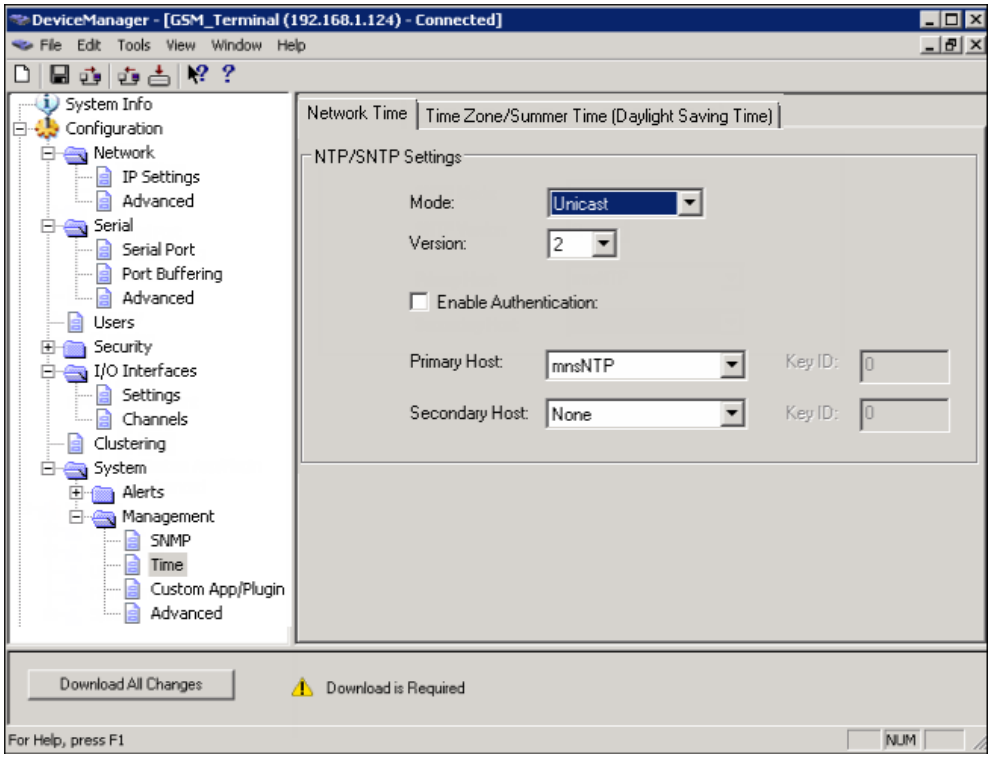
10. Select the **Hardware** tab.



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

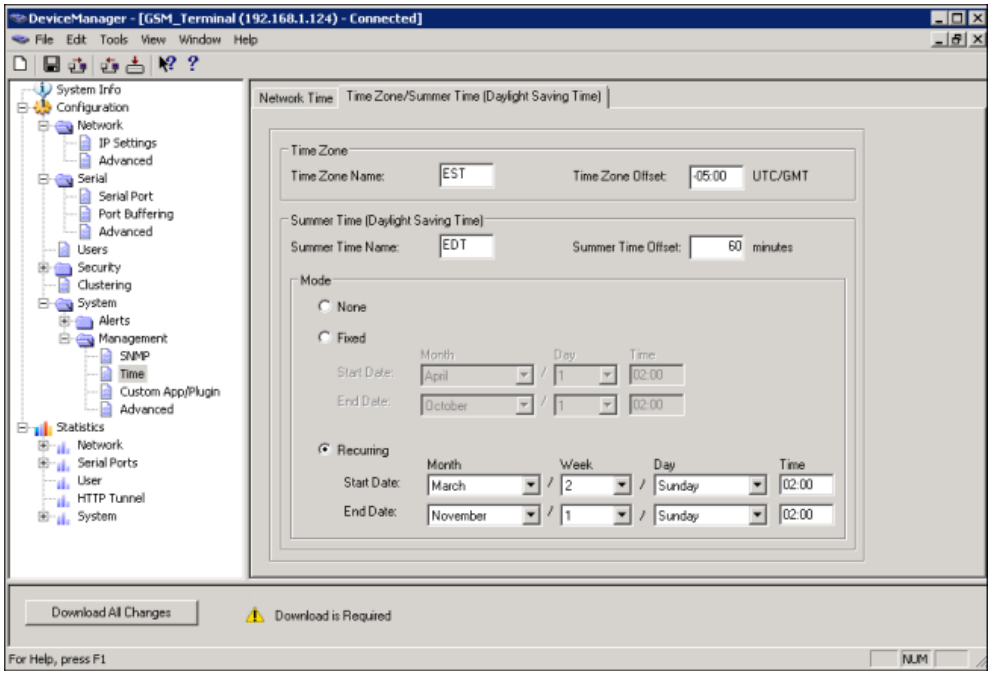
- Select **EIA-232** (RS-232) from the **Serial Interface** drop-down list.
- Select **9600** from the **Speed** drop-down list.
- Select **8** from the **Data Bits** drop-down list.
- Select **None** from the **Parity** drop-down list.
- Select **1** from the **Stop Bits** drop-down list.
- Set Flow 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**.

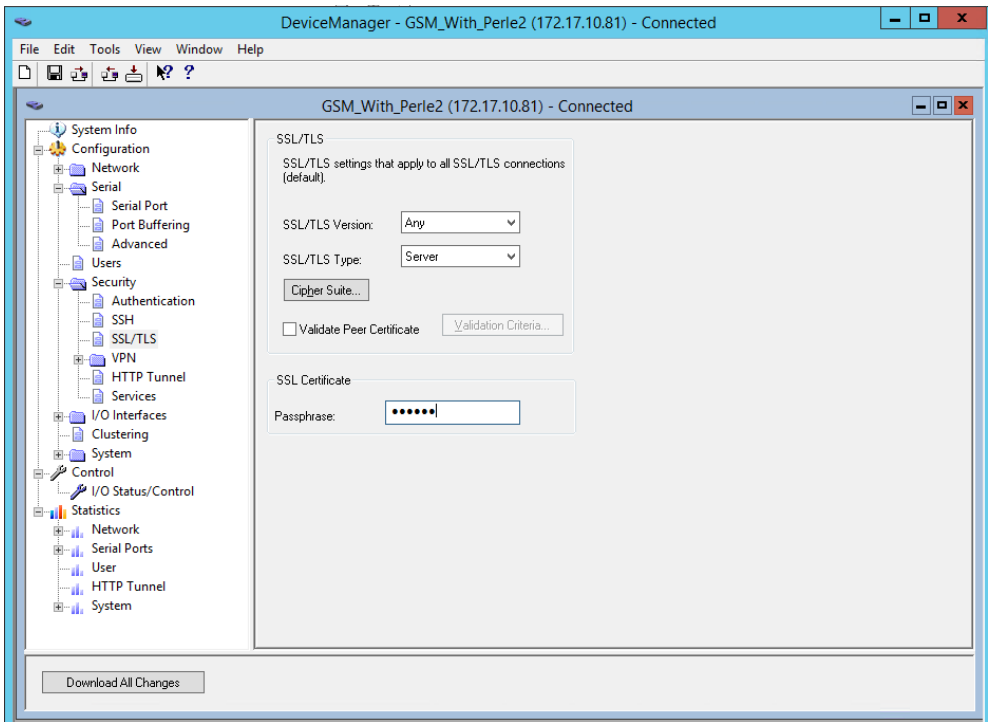


14. Select the **Network Time** tab, set the following parameters.
    - **Mode:** Unicast
    - **Version:** 2
    - Leave the **Enable Authentication** check box unselected.
    - **Primary Host:** Select the NTP server name created earlier.
    - **Secondary Host:** Select alternative NTP server name,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



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

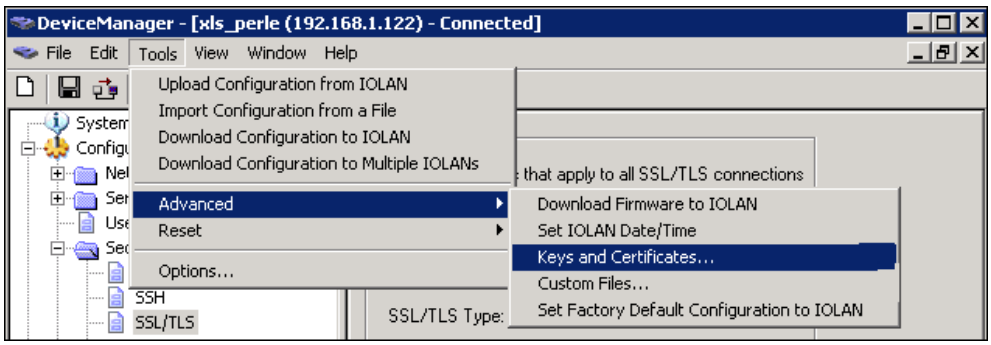


18. Set the **SSL/TLS Version** field to **Any**.

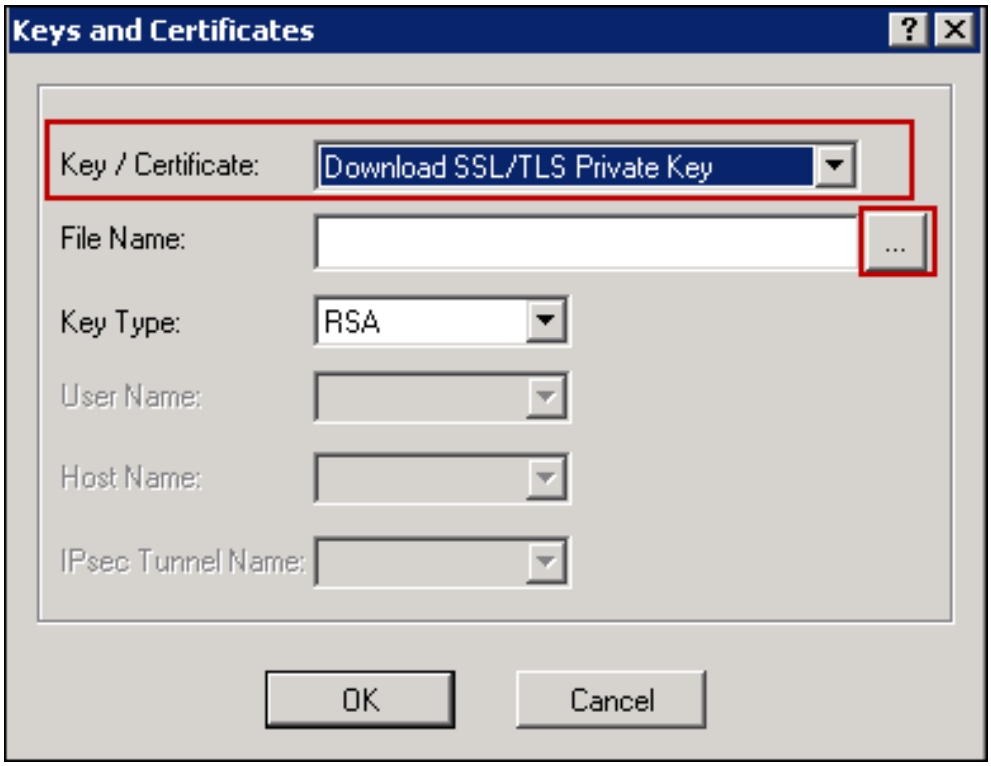
19. Set the **SSL/TLS Type** field to **Server**.

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.



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**.



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

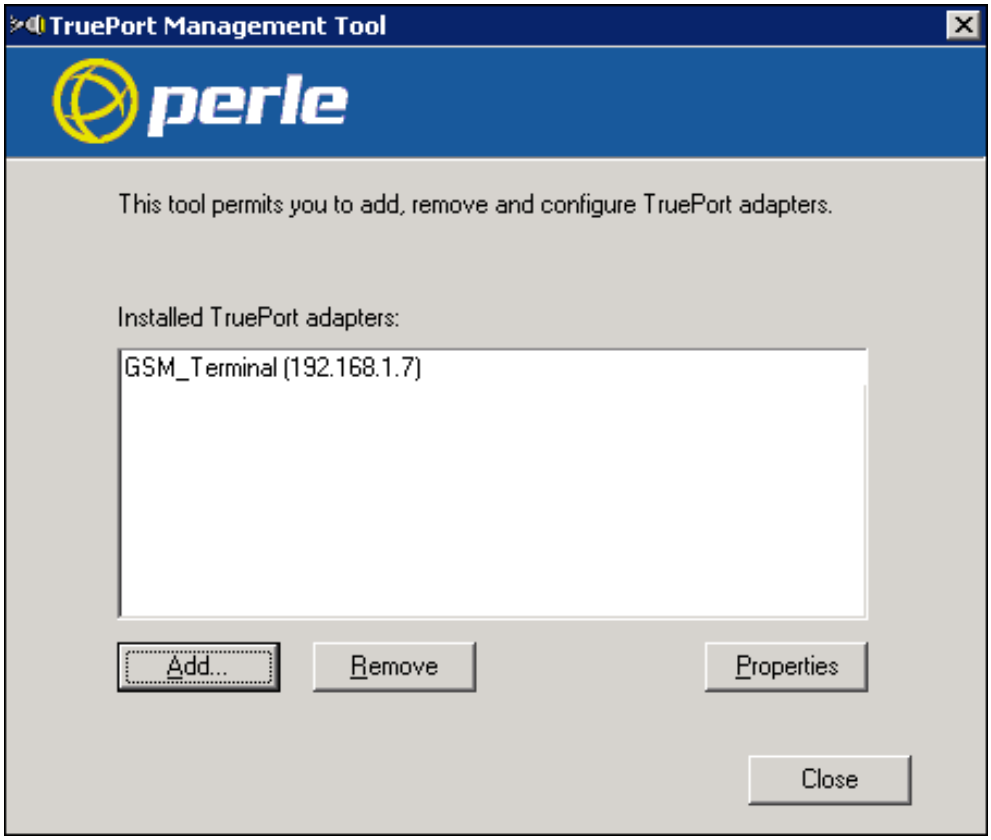
reconnected, it will take 90 seconds for the device to reboot and initialize. When ready, the Power LED will be a solid green color and the Link LED will be a solid orange or green.

⇨ The device is now configured.

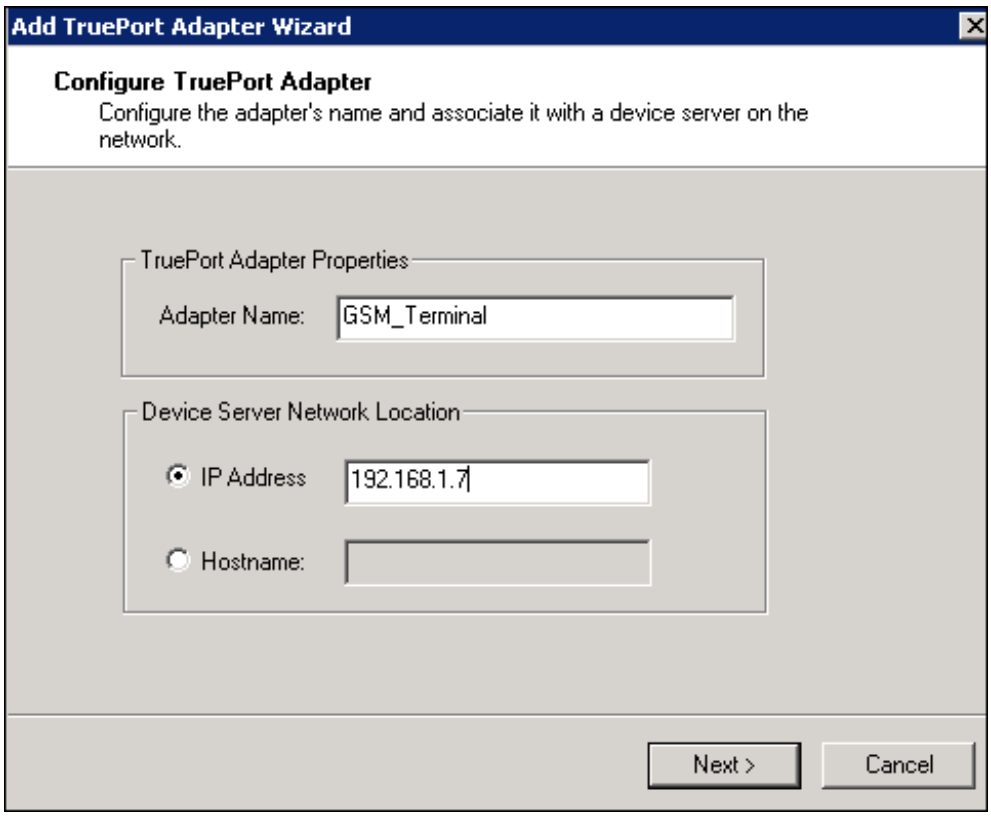
TruePort Driver Configuration

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.

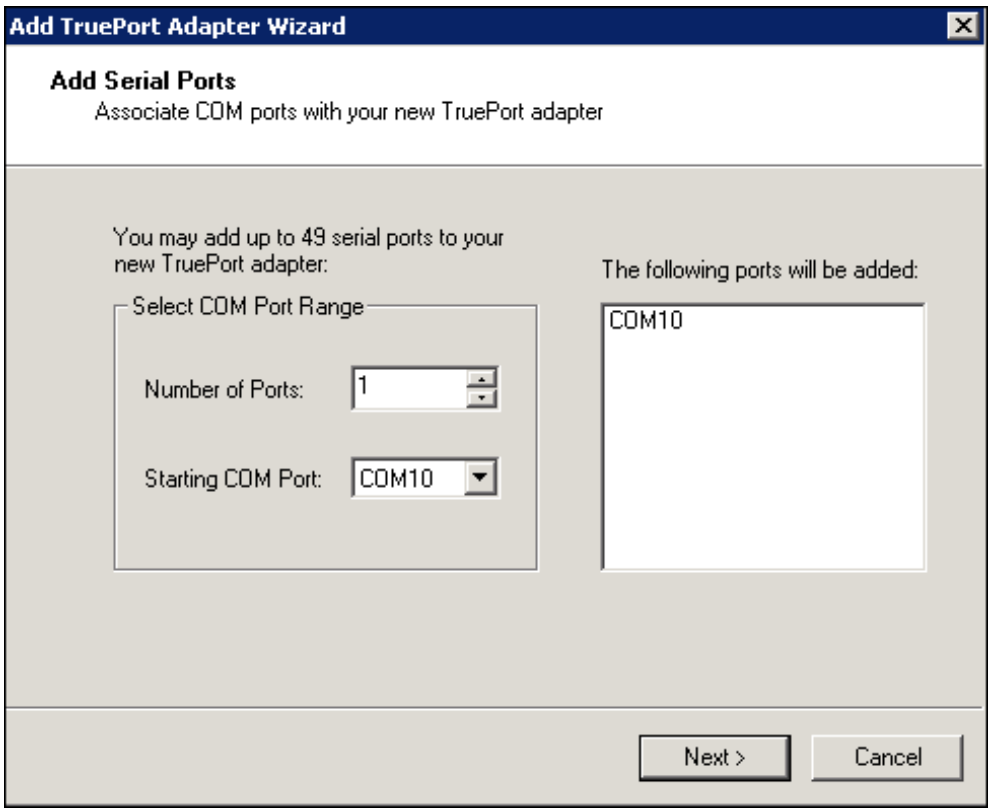
1. Install TruePort on the server.
2. Start the **TruePort Management Tool**.
3. In the **TruePort Management Tool** window, click **Add**.



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**.



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**.



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

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

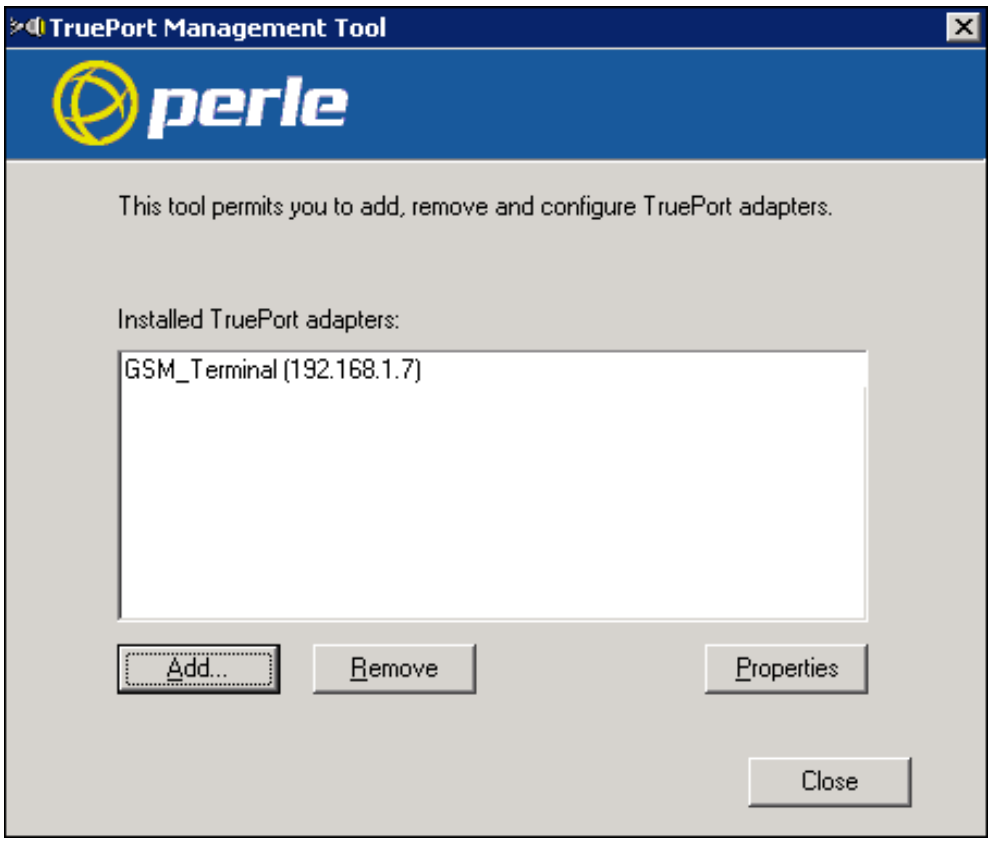
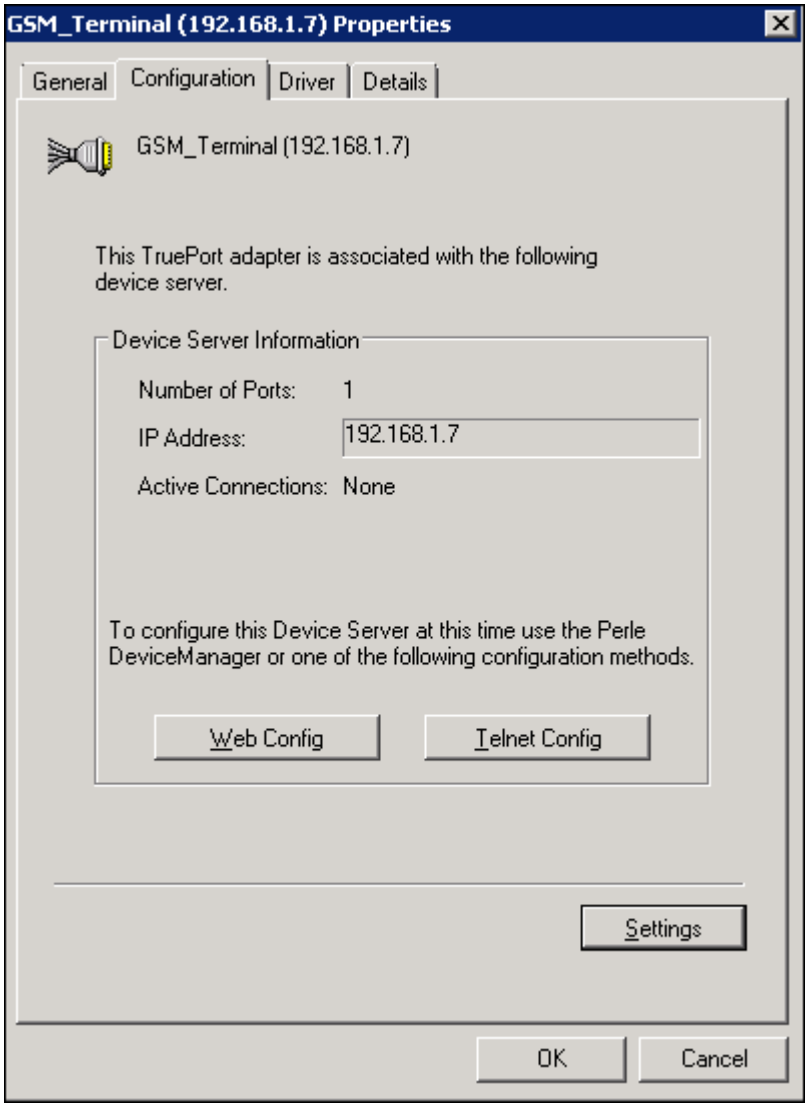


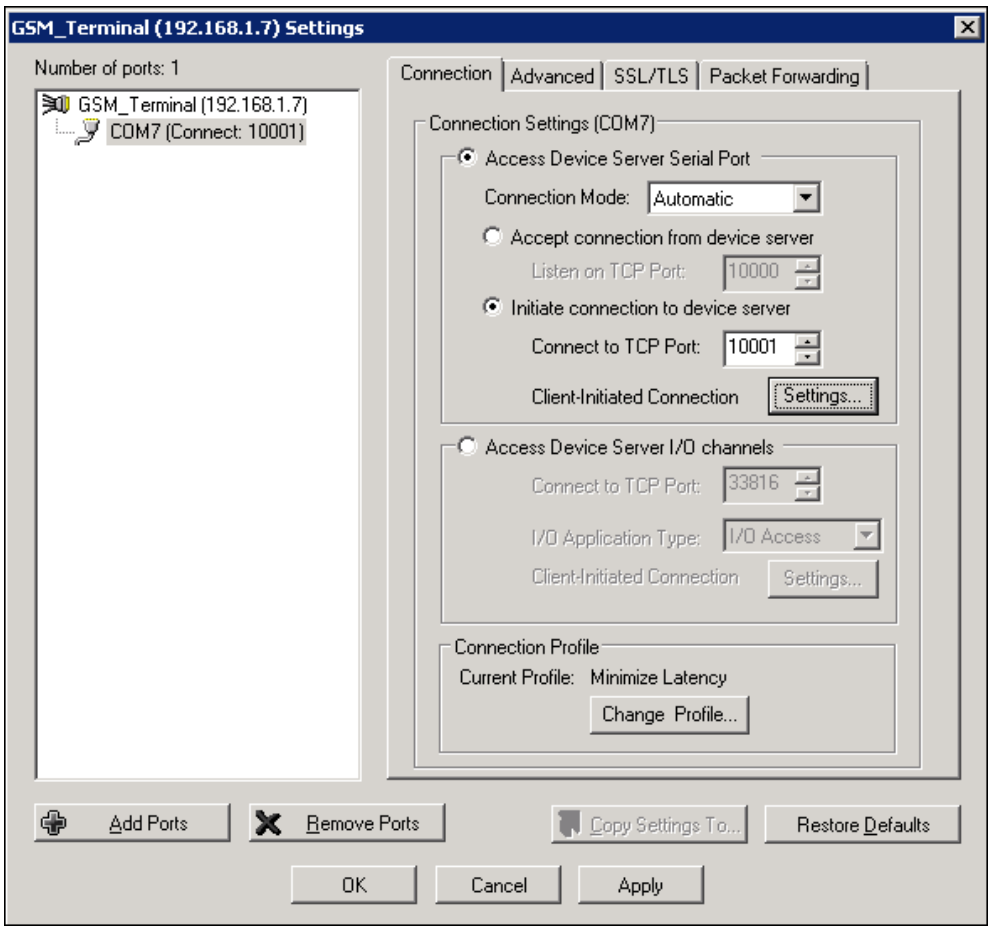
Fig. 24:

Serial Settings

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

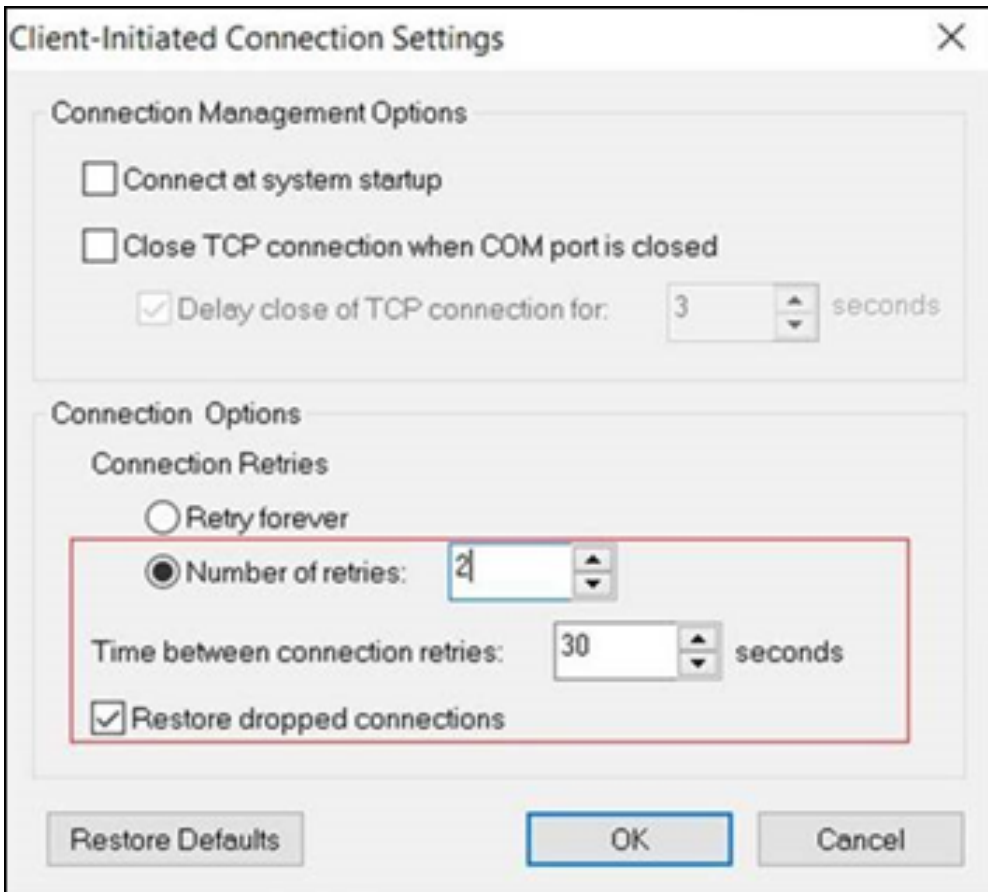


2. Click the COM port.
   ⇨ This will display the TruePort and COM port settings for this adapter.
3. Select the **Connection** tab.
4. Select **Initiate connection to device server**.

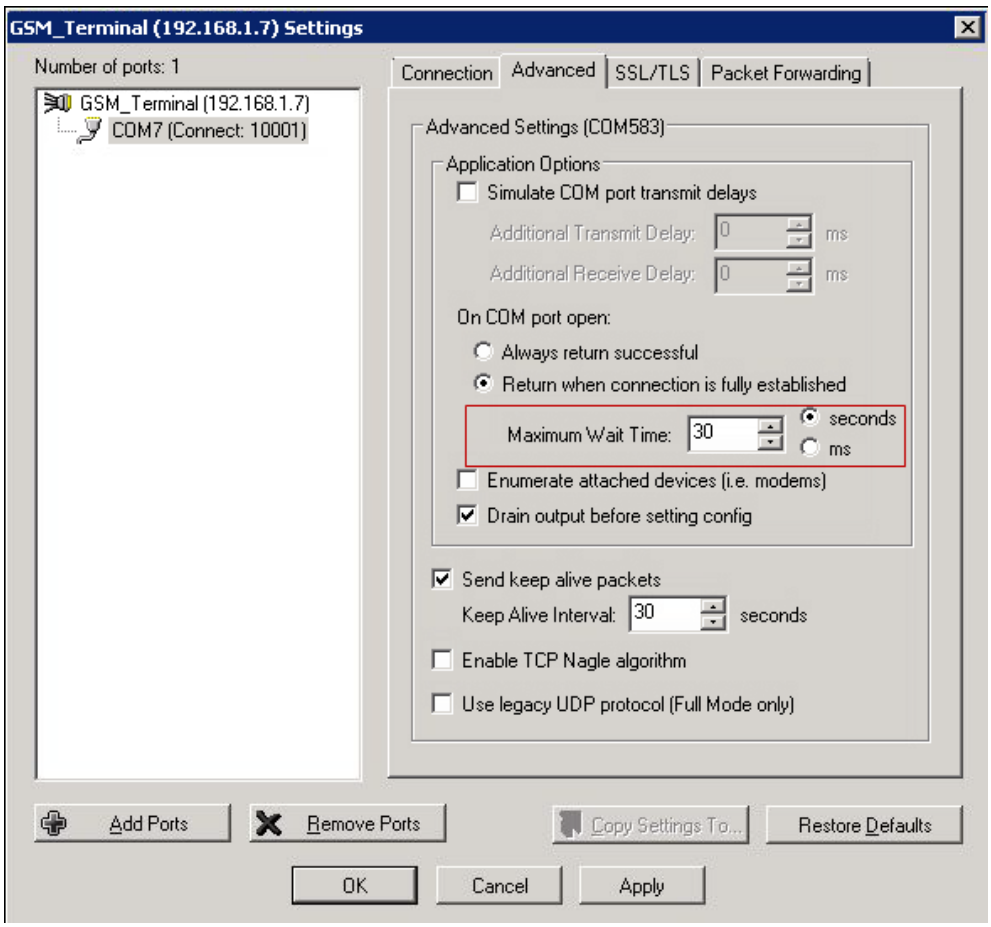


– Select **Connect to TCP Port**, enter the port number that was previously assigned to the device using the device manager.

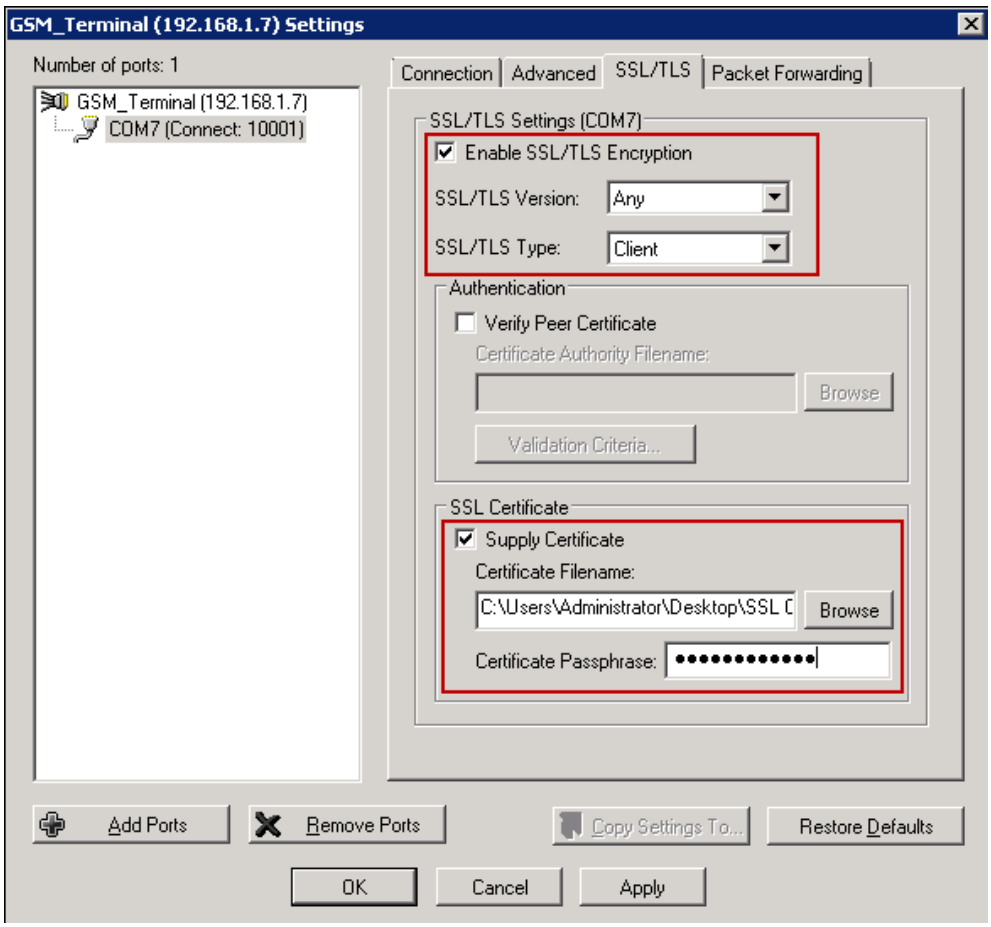
5. Click the **Settings** button next to **Client-Initiated Connection**.



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.



9. Set **Maximum Wait Time** to **30 seconds**.
10. Select the **SSL/TLS** tab.



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.

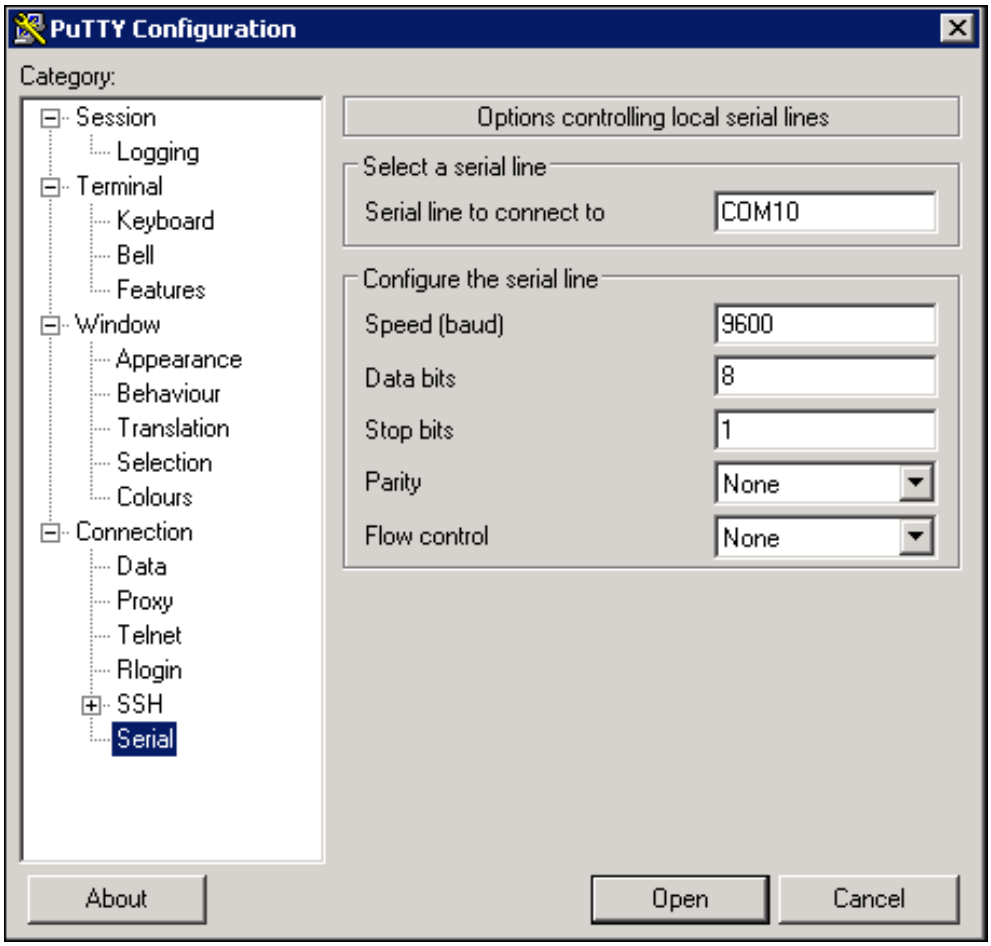
PuTTY can be downloaded from the following link:

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



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.

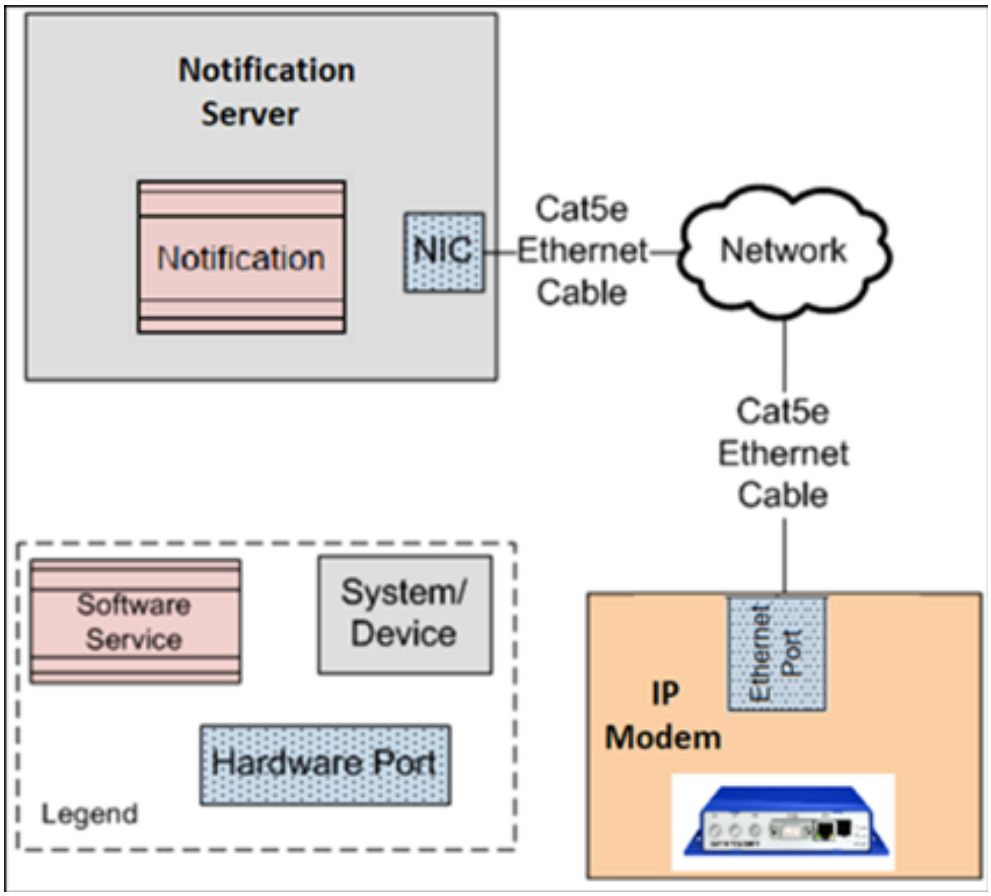
1.13 IP Modem Device

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:

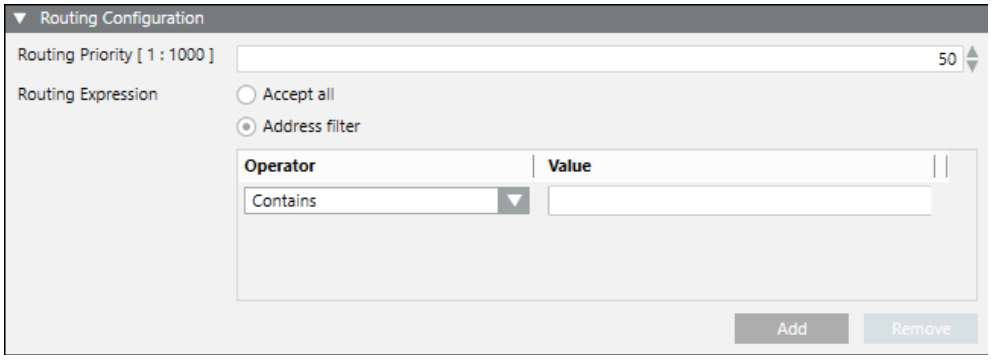


NOTE 1:
The GSM Terminal device accepts a SIM card that has the SMS services enabled. Without enabling these services on a SIM card, you cannot send SMS through the device.
NOTE 2:

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, will search for either the value specified under **Starts with** or **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.

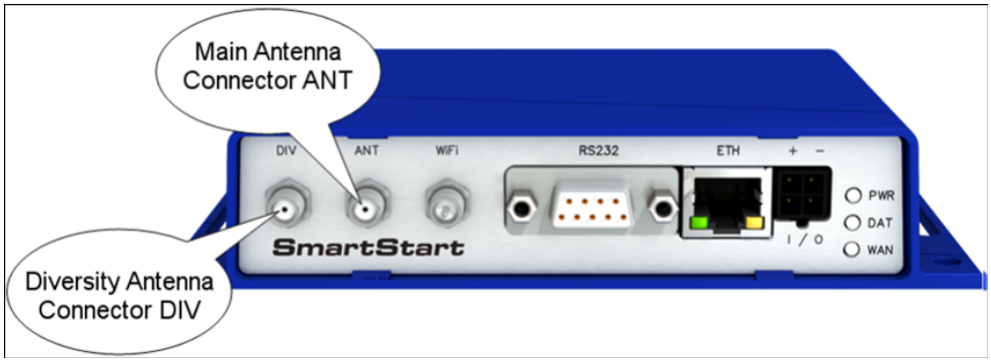
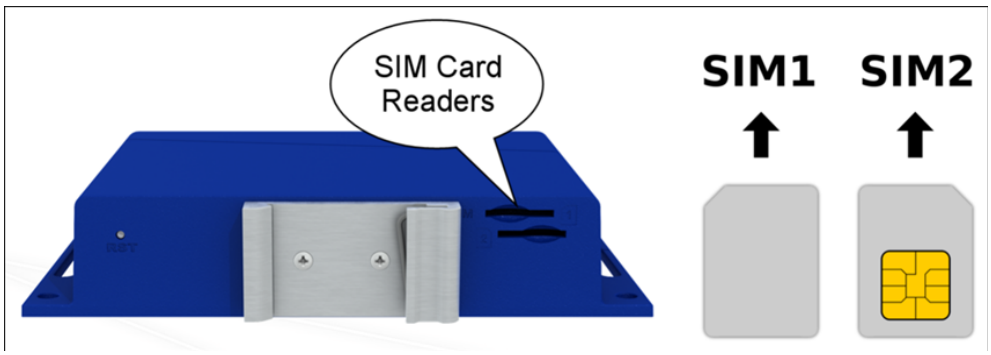


Fig. 25:

SIM Card

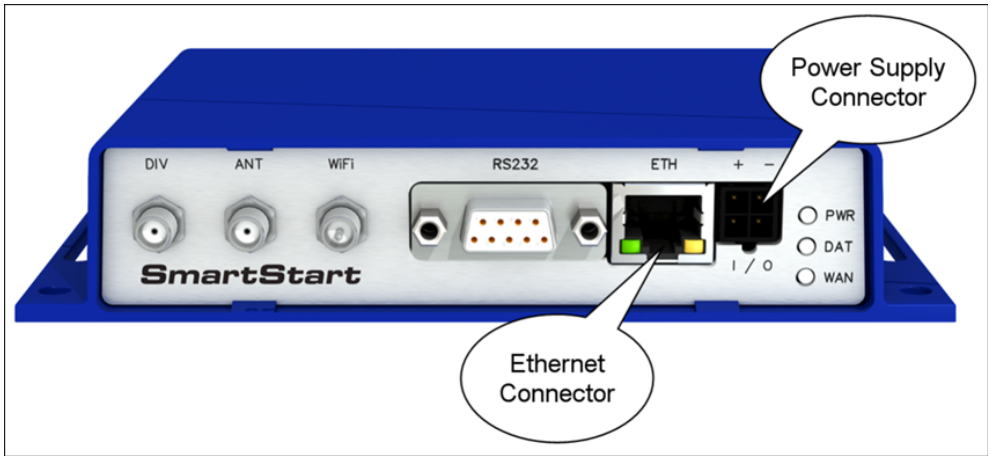
The SIM card readers, for 3 V and 1.8 V SIM cards, are located on the rear panel of the router. If you intend to use this device to communicate over a cellular network, place an activated data-provisioned SIM card into the SIM card reader. Push your SIM card into the SIM1 or SIM2 slot until it clicks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

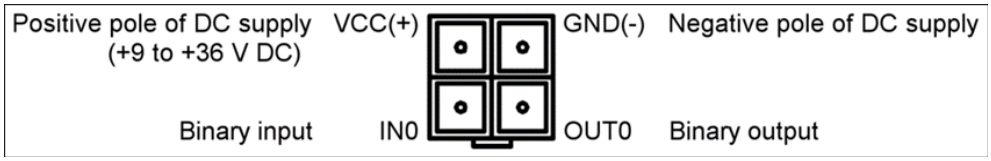
Note: Disconnect the router from the power supply, before handling the SIM card.



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.

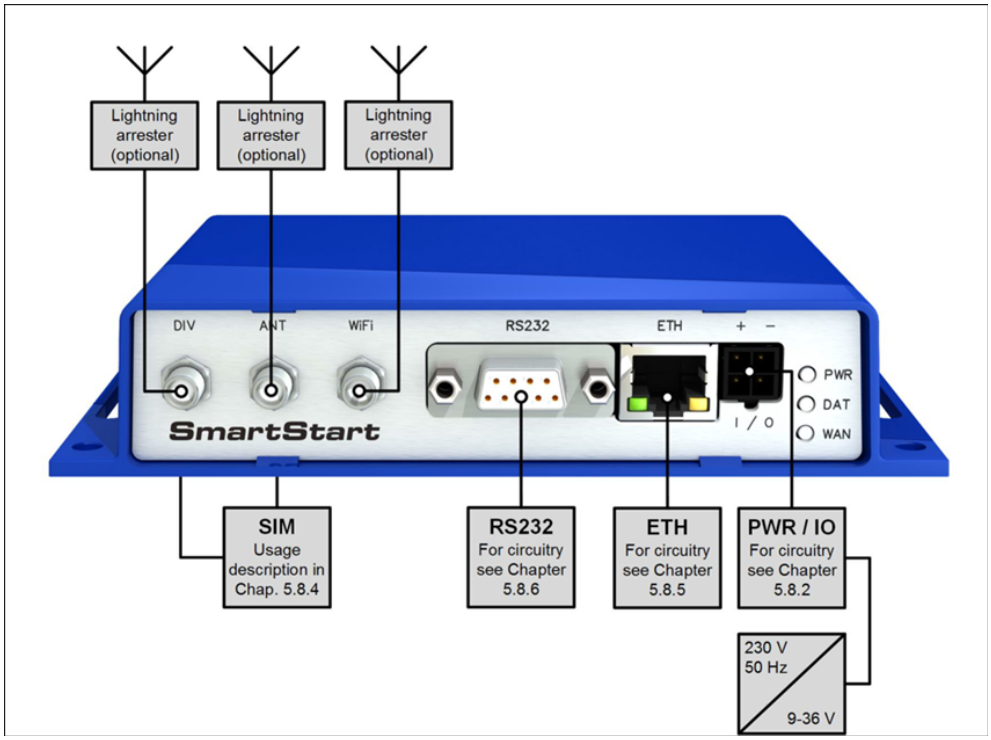
IP Modem Configuration

Configuration by Web Browser

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

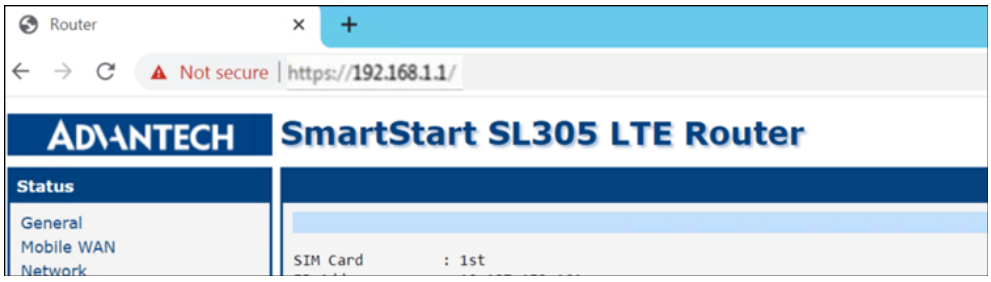
▷ Before putting the router into operation, it is necessary to connect all the components that are required to run your applications. Do not forget to insert a SIM card.
Note: The router cannot operate without a connected antenna, SIM card and power supply. The router may get damaged if the antenna is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

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

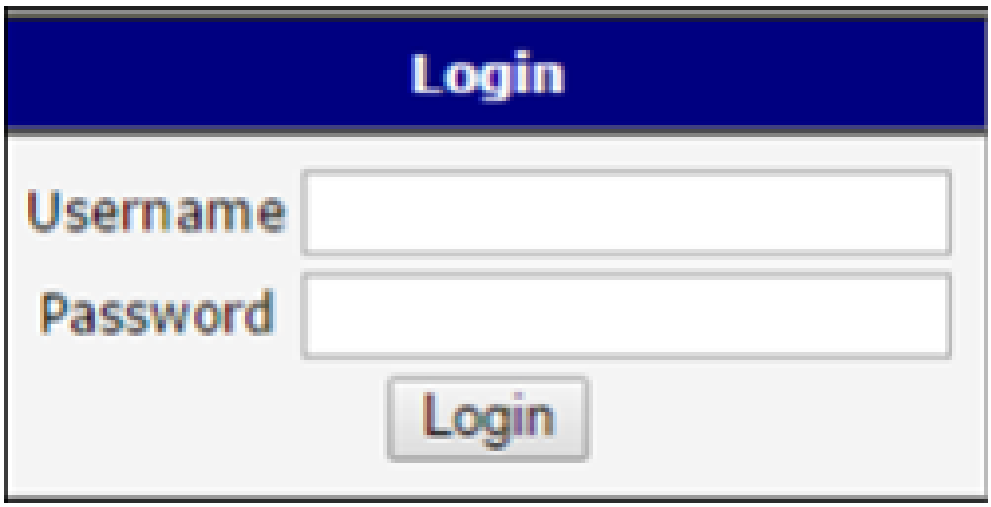


⇨ The router will start when a power supply is connected to the router. By default, the router will automatically start to log on to the default APN. These router behaviors can be changed via the web interface.
Note: If no SIM card is inserted in the router, it is not possible for the router to operate.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

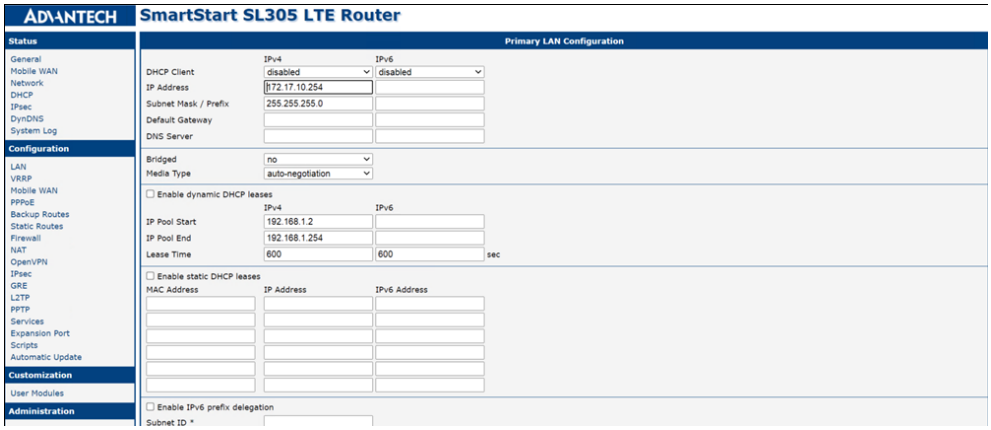
2. Enter the IP address of the router into the web browser. The default IP address of the router is 192.168.1.1. It is necessary to use HTTPS protocol for secure communication over a network.



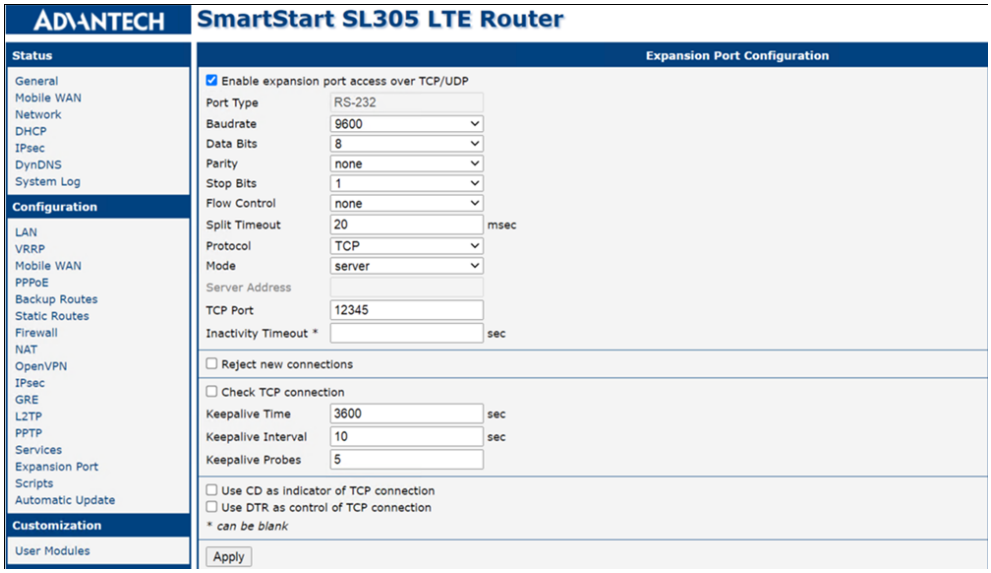
3. Enter the default username “root” and default password available on the back of the device for configuration.



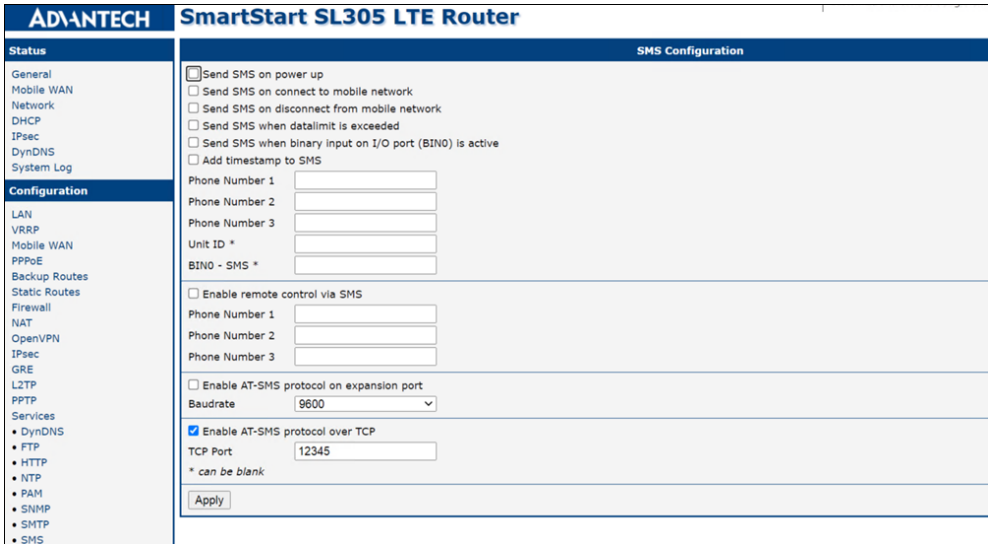
– Set the Primary LAN Configuration, if you are configuring the IP modem for the first time. If you have already configured the IP modem, then in this step you can update the Primary LAN Configuration.
Note: An IP address is required for the IP Modem before the device configuration process. After an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



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



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



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

1.14 Import DME File

Import DME File

Scenario: You want to import the .dme file.

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

▷ In System Browser, select **Management View**.

1. Open the **DeviceManager**.

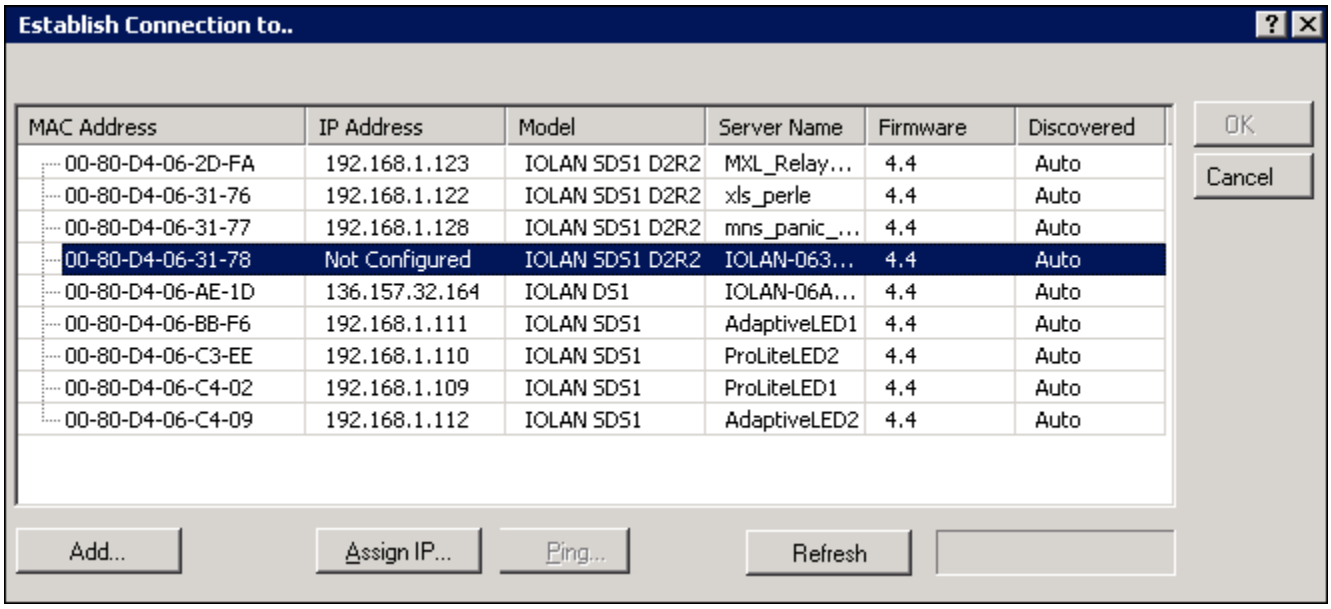


Fig. 26: Device Manager dialog box

⇨ All the perle devices in the network are displayed.

2. Select the device to configure and click **Assign IP**.
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**.

   ⇨ The IP address is assigned to the device now.
4. Select the device.
5. In the **Establish Connection to** dialog box, click **OK**, automatically login screen opens.
6. Enter the device password in the **Login** window. The factory default password is **superuser**.

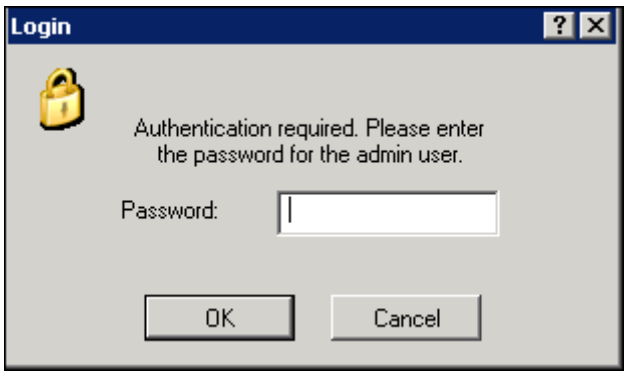


Fig. 27: Login dialog box

7. Select **Tools** > **Import Configuration from a File**.

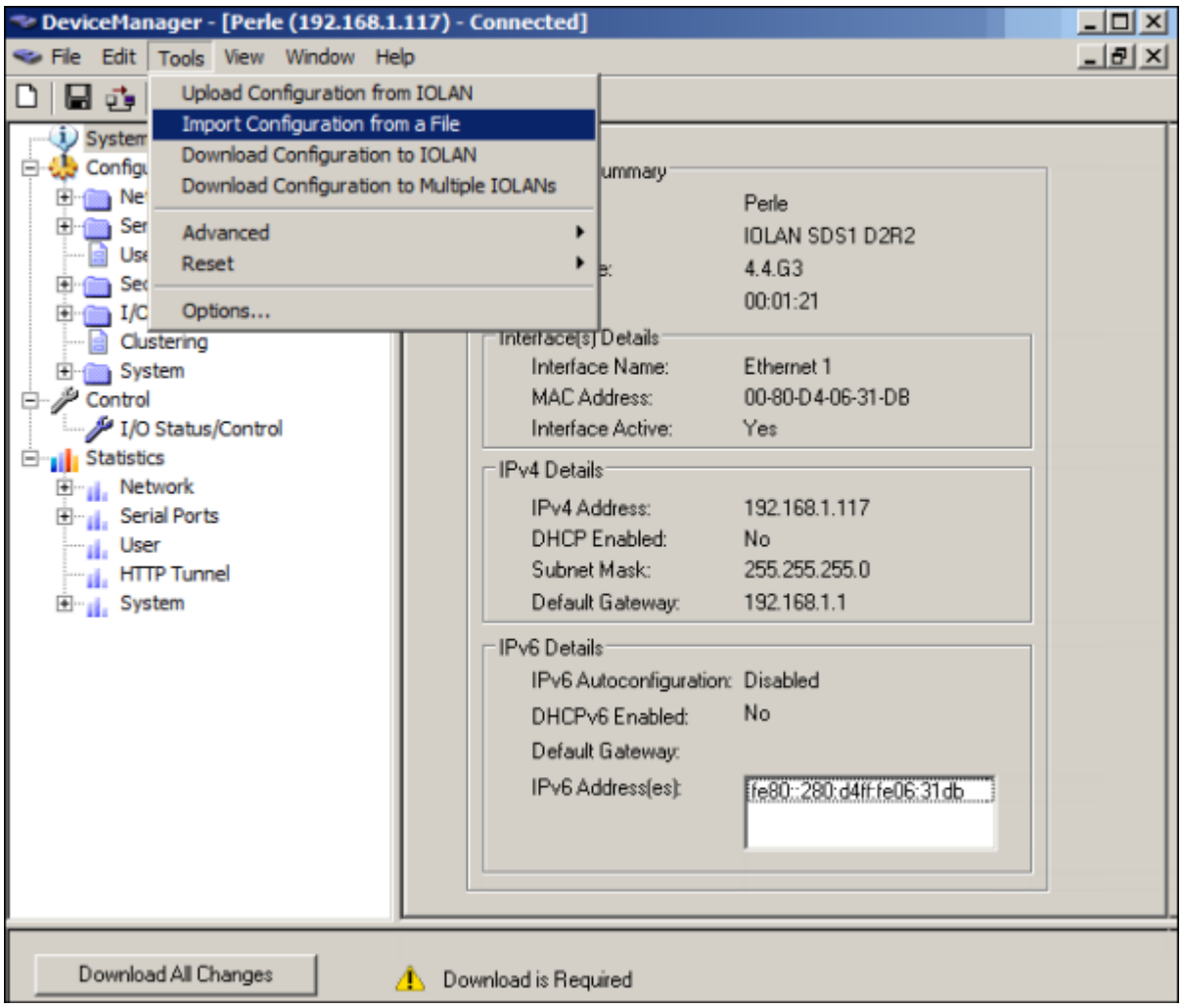


Fig. 28: Device Manager screen

8. Select the location of the preconfigured .dme file.
9. Click **Open**.
   ⇨ A confirmation message displays.

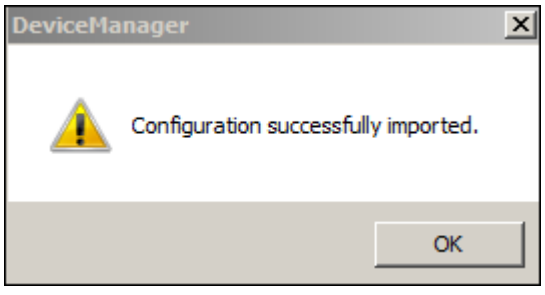


Fig. 29: Confirmation message dialog box

10. Click **OK**.
    NOTE: After importing the .dme file, verify the Perle device configuration with configuration settings as mentioned in the *Network Setup* and *Serial Settings* sections of Device Configuration.
11. In the **DeviceManager** dialog box, click **Download All Changes**.

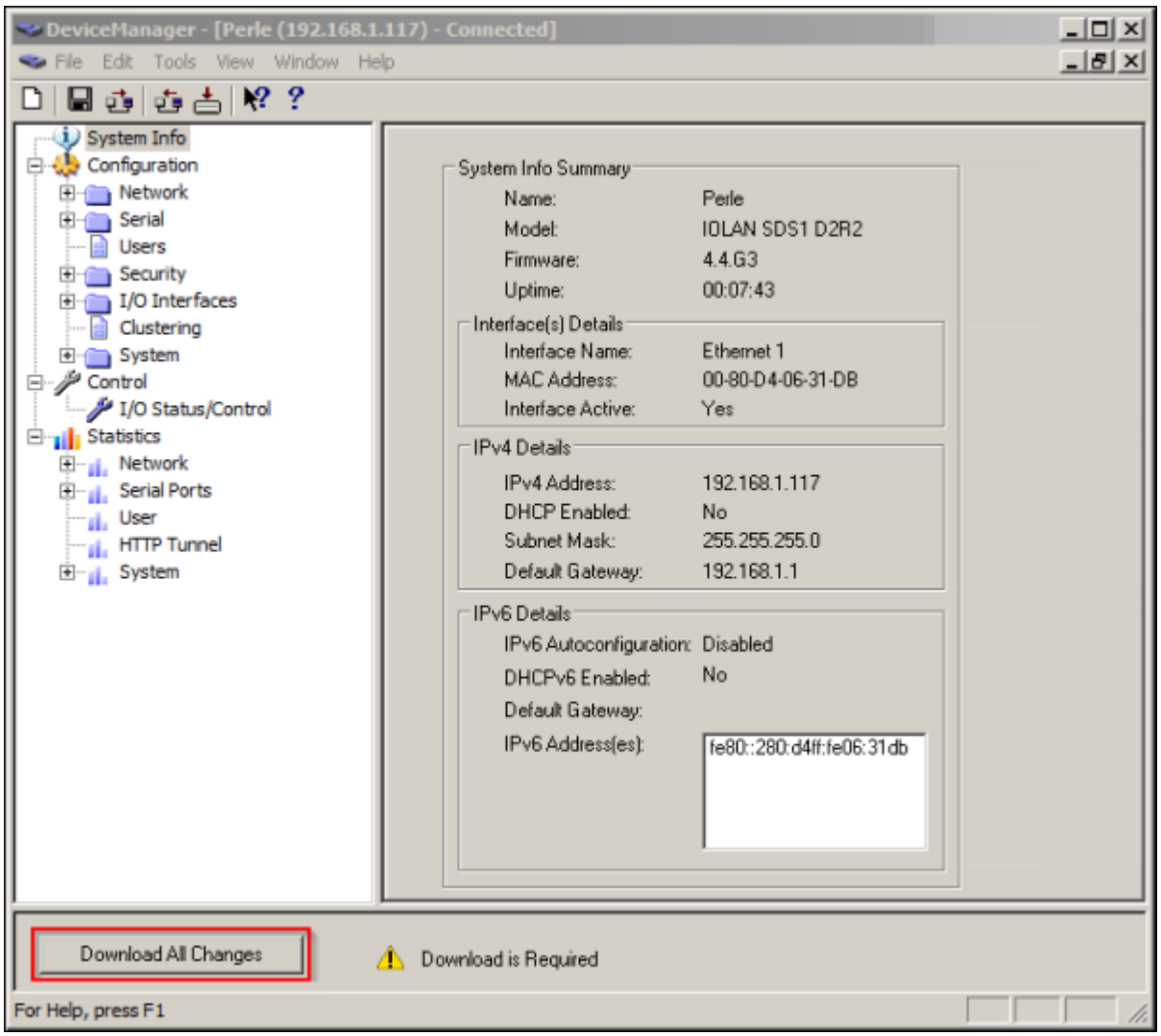


Fig. 30: Device Manager screen

12. Click **Yes**.

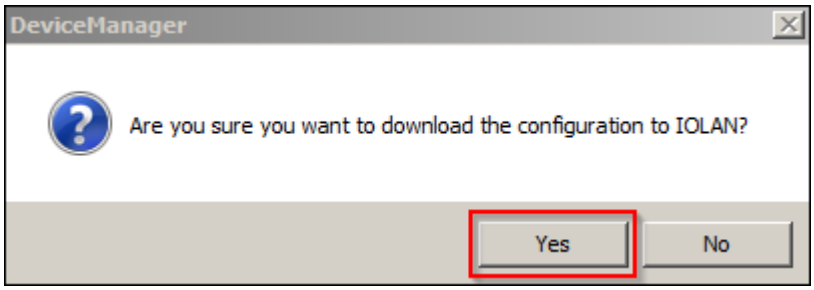


Fig. 31: Confirmation message dialog box

13. In the **DeviceManager** dialog box, click on **Reboot IOLAN**.

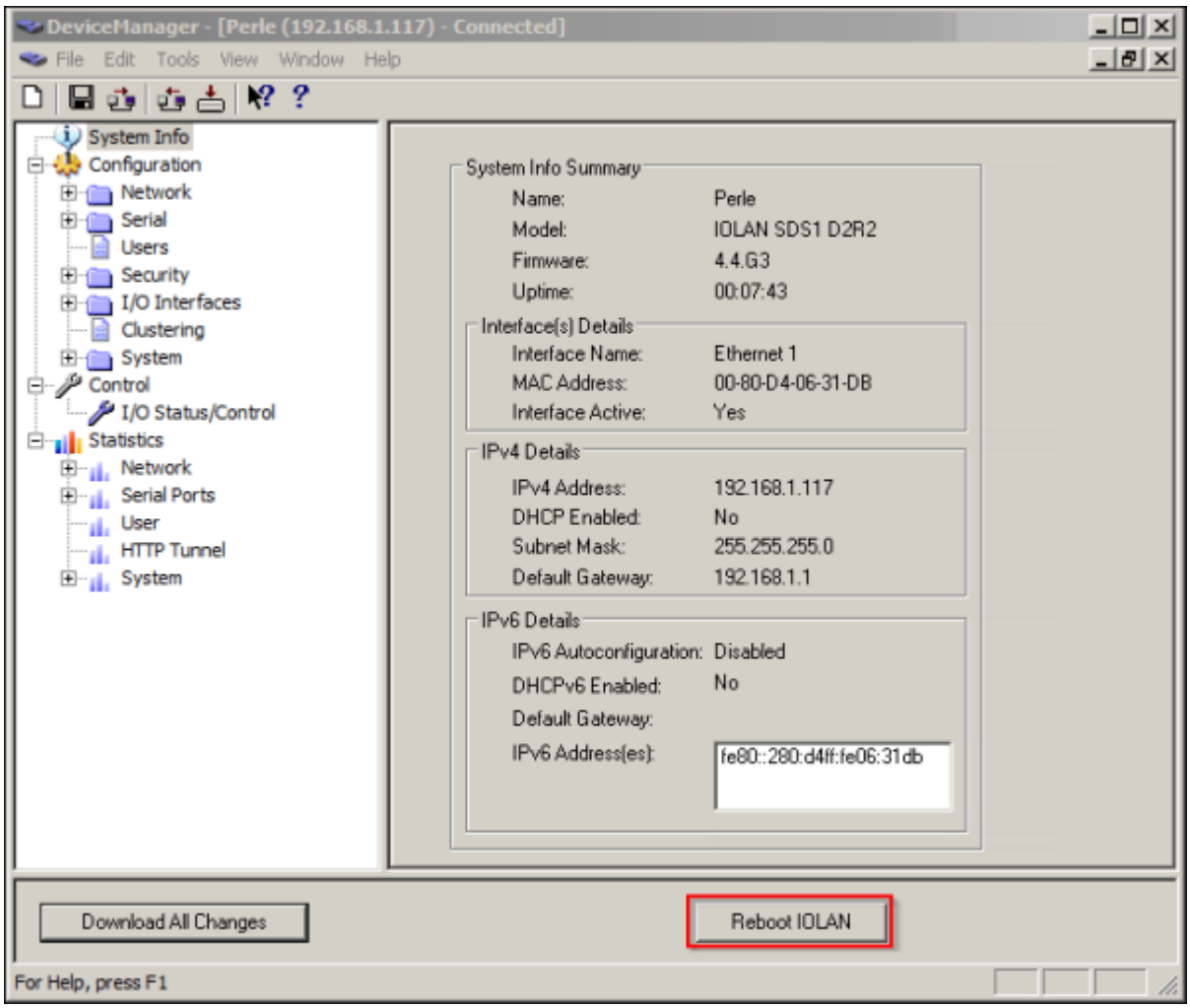


Fig. 32: Device Manager screen

14. A confirmation message displays.

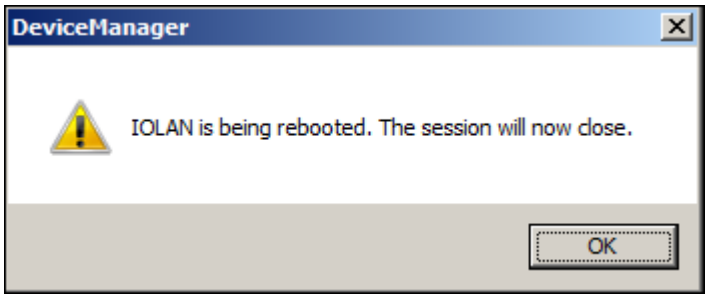


Fig. 33: Information messge dialog box

15. Click **OK**.

⇨ The configuration is complete.

NOTE:
The procedure must be repeated for each device that has to be configured.

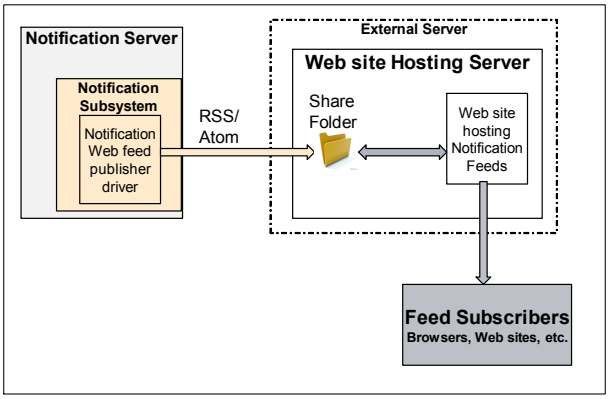
1.15 Interface to Website Device

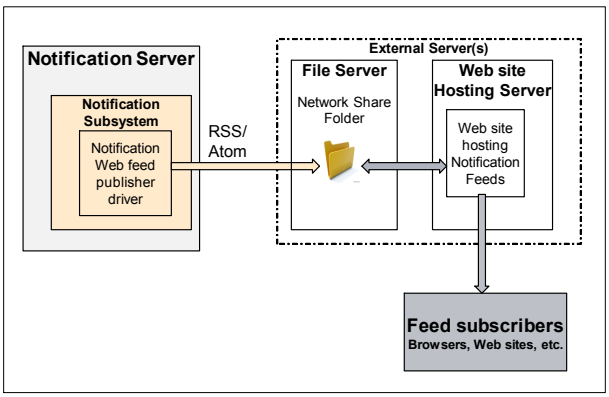
Interface to Website Device

This section provides reference and background information for integrating the Interface to Website Device. For procedures and workflows, see the step-by-step section.

has the capability to produce the following:

- Rich Site Summary (RSS) and Atom feeds as web feed documents
- CAP and XML message documents as web feed entries in RSS and Atom feed documents





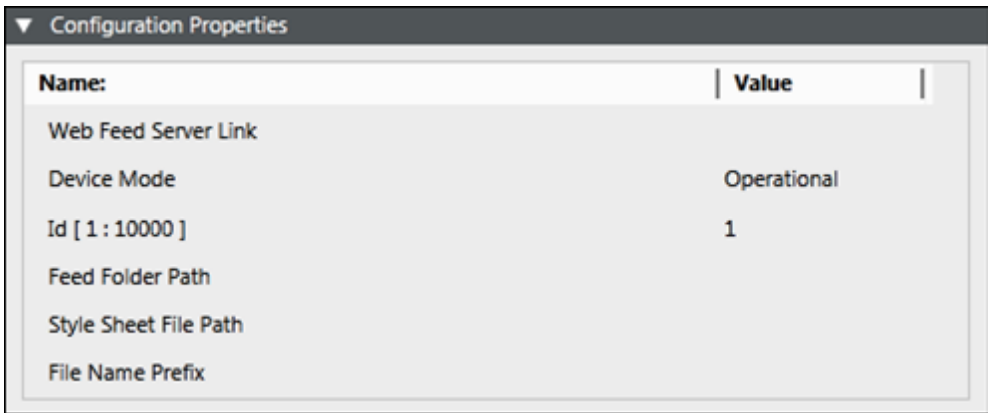
The feeds produced can be published to a website from which RSS / Atom readers and other applications or websites interested in feeds can subscribe to the feeds and access them.

generates both RSS and Atom feed XML files for all configured user languages. The user can decide which feed to use. The type of feed and the language is indicated in the file name of the feed. Some examples are listed below:

- 1_MNSFeeds_atom_en_US.xml is a feed file in Atom format in English
- 1_MNSFeeds_rss_es_ES.xml is a feed file in RSS format in Spanish

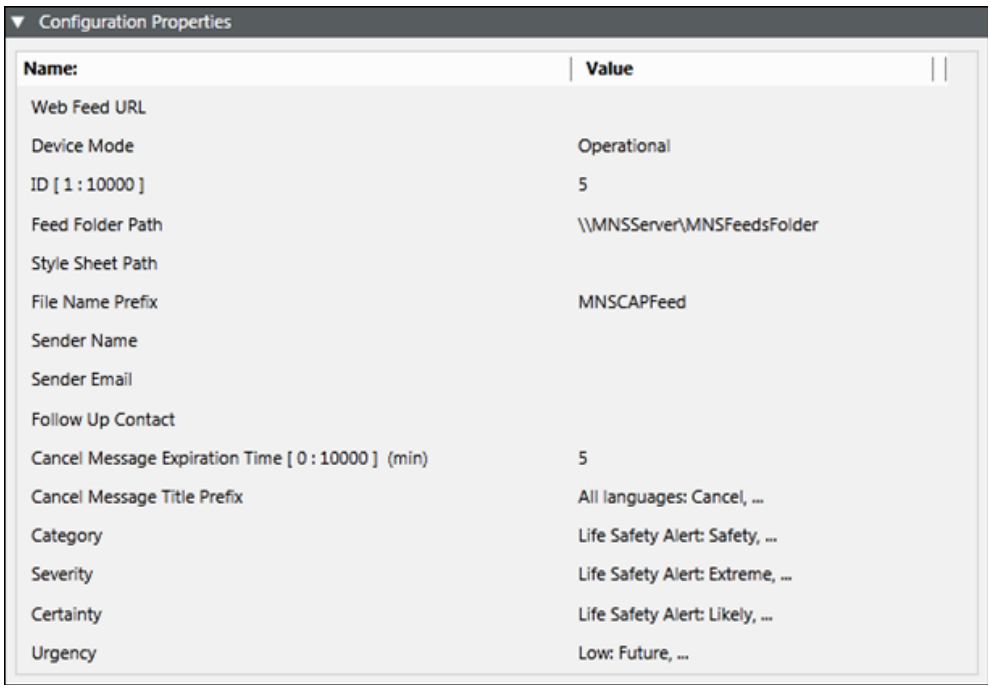
NOTE 1:
The RSS and Atom feeds are used to publish frequently updated content like blog entries and videos. Users can choose from a wide variety of applications (Web based applications, desktop applications, or mobile device applications) to access the RSS or Atom feeds. In either of the above cases, it should be noted that the services are running under an account that has write access to the share folder so that it can publish content. Websites can be configured to pick up content from a location on the same machine or from a network shared folder as depicted in the above images.
NOTE 2:
Abide by the terms of use mentioned on the hosting website.

Configuration Properties - Web Feed Device



- **Web Feed URL**: Enter the URL of the website where the feeds are to be published. This is needed to generate the correct hyperlinks to be associated with the RSS and Atom feeds generated.
- **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 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 status.
  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 status.
- **ID**: Enter a numeric ID for the feed. This is a numerical identifier for the feed file and the feed generated contains the ID as a part of the file name. For example, if the ID value entered is 555, then the generated feed file has the name **555_MNSFeed_atom_en_US.xml**. The value of the **ID** field should be unique across all configured Web Feed Publisher Devices.
- **Feed Folder Path**: Enter the full path of the folder where the feeds must be published.
  NOTE: This can also be a network share path. If this is the case, make sure that the system has write permissions to that folder. For example: \ **\MNSServer\MNSFeedsFolder**. The account used to run the services should have write access to the network share folder.
- **Style Sheet File Path**: Enter the full path of the style sheet file that must be used to view the feeds. For example, for emergency feeds, **[Installation Drive]: \GMSProjects\GMSMainProject\bin\MNSEmergencyFeedStylesheet.xsl** can be used. For informative feeds, **[Installation Drive]: \GMSProjects\GMSMainProject\bin\MNSInformationFeedStylesheet.xsl** can be used.
  NOTE: The value for this field is optional and can be left blank.
- **File Name Prefix**: Enter the prefix that needs to be used for the files that are generated. For example, If the value is set to **MNSFeed,** then the feed file is generated with a value in the field name such as **555_MNSFeed_atom_en_US.xml**.

Configuration Properties - CAP Feed Device



- **Web Feed URL**: Enter the URL of the website from which the feed files will be accessible to subscribing clients. This URL specifies a folder, for example: http://www.myalertfeed.com/publicfeeds/regioncentral. This information is needed to form the correct hyperlinks associated with the generated CAP message files.
- **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 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 status.
  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 status.
- **ID**: Enter a numeric ID for the feed. This is a numerical identifier for the feed file and the feed generated contains the ID as a part of the file name. For example, if the ID value entered is 555, then the generated feed file has the name **555_MNSFeed_atom_en_US.xml**. The value of the **ID** field should be unique across all configured CAP Feed devices.
- **Feed Folder Path**: Enter the full path of the folder where the feeds must be published.
  NOTE: This can also be a network share path. If this is the case, make sure that the system has write permissions to that folder. For example: \ **\MNSServer\MNSFeedsFolder**. The account used to run the services should have write access to the network share folder.
- **Style Sheet File Path**: Enter the full path of the style sheet file that must be used to view the feeds. The default style sheet is located at **[Installation Drive]\GMSProjects\GMSMainProject\bin\MNSEmergencyFeedStylesheet_CAP.xsl**.
  NOTE: The value for this field is optional and may be left blank.
- **File Name Prefix**: Enter the prefix that needs to be used for the files that are generated. For example, If the value is set to **MNSFeed**, then the feed file is generated with a value in the field name such as **555_MNSFeed_atom_en_US.xml**.
- **Sender Name**: Enter the name of the sender.
- **Sender Email**: Enter the email address of the sender.

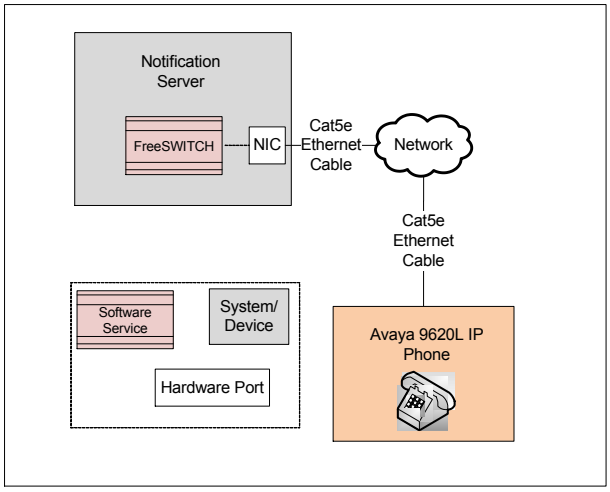
- **Follow Up Contact**: Enter the name of the contact person in case of any queries.
- **Cancel Message Expiration Time**: Enter the time period after which the canceled or suspended CAP messages must be removed from the generated feed.
  NOTE: When CAP messages are canceled or suspended before the original expiration time, the system generates CAP Cancel messages. These messages are present in the generated feed for the configured time period.
- **Cancel Message Title Prefix**: This prefix allows for the title of the message to be canceled or suspended in different languages.
- **Category**: Represents Feed item category as per the CAP protocol. Select a CAP Feed category for every message type. The selected category value is displayed in the CAP Feed's category element. For example, a message type Life Safety Alert can be mapped with the CAP Feed Category Safety.
- **Severity**: Represents Feed item severity as per the CAP protocol. Select a CAP Feed Severity for every message type. The selected severity value is displayed in the CAP Feed's severity element. For example, a Life Safety Alert message type can be mapped with the CAP Feed Severity Extreme.
- **Certainty**: Represents Feed item certainty as per the CAP protocol. Select a CAP Feed Certainty for every message type. The selected severity value is displayed in the CAP Feed's certainty element. For example, a Life Safety Alert message type can be mapped with a CAP Feed Certainty Likely.
- **Urgency**: Represents Feed item urgency as per the CAP protocol. Select a CAP Feed Urgency for every message priority. The selected urgency value is displayed in the CAP Feed's urgency element. For example, the message priority Low can be mapped with the CAP Feed Urgency Future.

1.16 IP Phone Avaya (9620L)

IP Phone Avaya (9620L)

This section provides reference and background information for integrating the IP Phone Avaya 9620L. For procedures or workflows, see the step-by-step section.

The Avaya 9620L phone is a VoIP telephone used by to make live announcements, listen to pre-recorded messages, record audio messages, or initiate incidents through an Interactive Voice Response (IVR) system. The phone communicates with ‘s VoIP Switch system. For more information on Avaya 9600 Series IP Phones, refer to https://support.avaya.com/products/P0553/9600-series-ip-deskphones/



The following subsections provide the user with a brief description of and how the Internet Protocol (IP) phone is integrated.

The system can integrate with the following Voice over Internet Protocol (VoIP) phones:

- Avaya 9620L
- Polycom SoundPoint 331
- Cisco CP-6921
- Stentofon IP Desktop Intercom Station
- Stentofon IP Dual Display Intercom Station

NOTE:
This guide provides detailed step-by-step instructions for configuring the Avaya 9620L IP phone. For information on configuring the other supported VoIP phones, refer to the respective VoIP phone integration guide.

IP Phone Avaya (9620L)

This section provides additional procedures related to IP Phone Avaya (9620L).

Installing IP Phone Avaya (9620L)

This section provides information on mounting the hardware and wiring / connection details for the device.

Prerequisites

- Avaya 9620L IP Phone with bundled accessories
- Software Version - SIP96xx_2_6_12_1.bin (Application); hb96xxua3_00.bin (Boot file)

Mechanical Installation

For mechanical installation and setup, follow the instructions mentioned in the installation manual provided by Avaya.

Electrical Installation

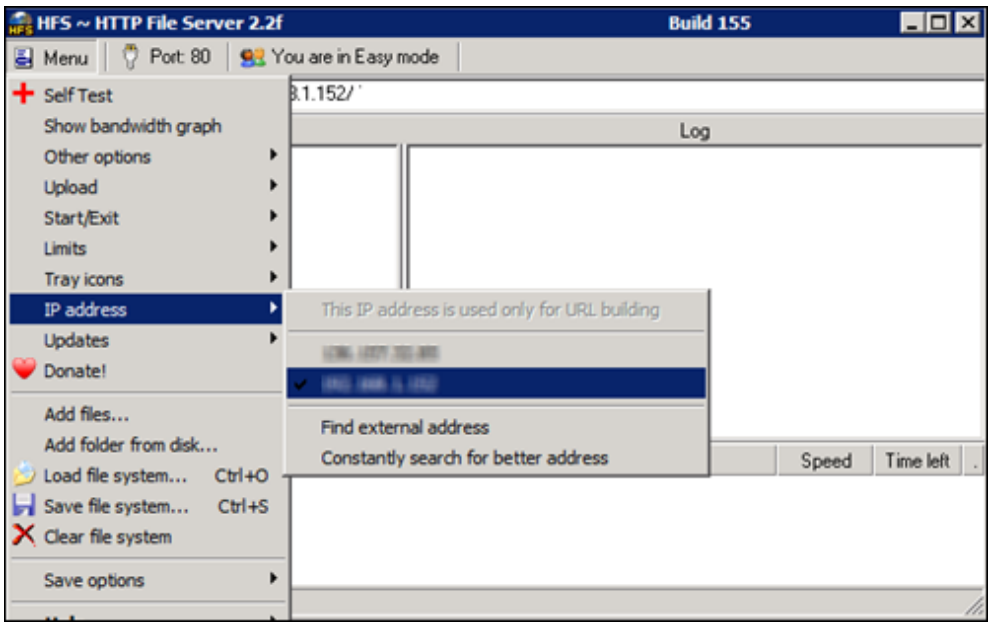
For electrical installation and setup, including power and Ethernet connections, follow the instructions mentioned in the installation manual provided by Avaya.

Configuring IP address

After mounting and wiring the IP phone, configure the phone to communicate with the software PBX included with .

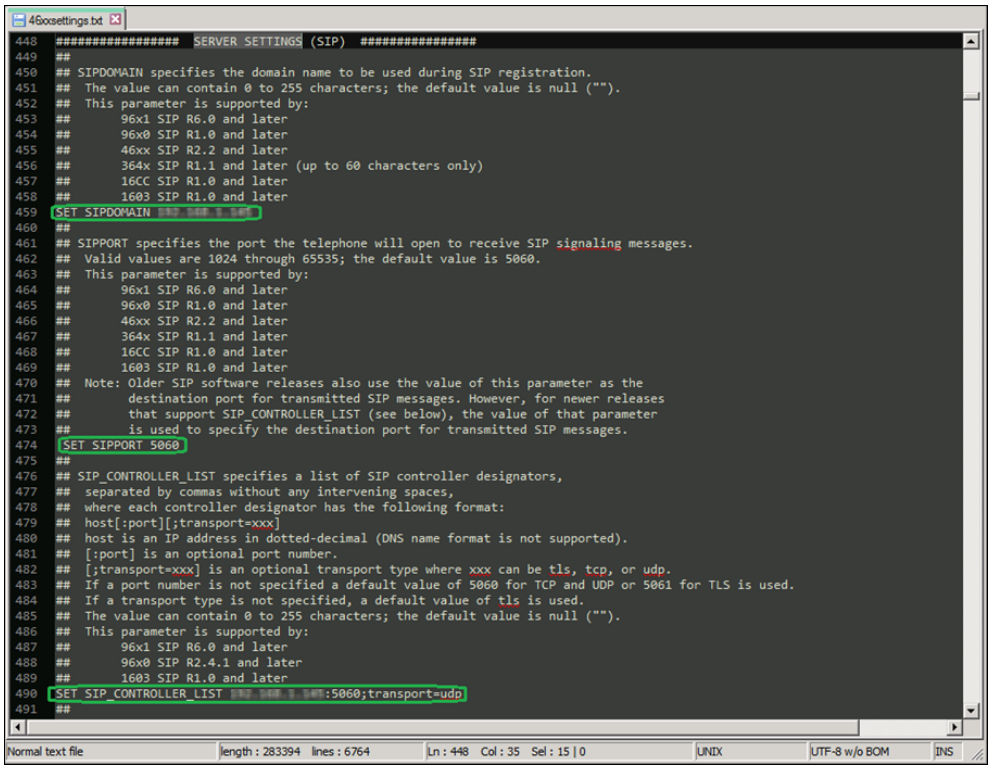
Prerequisites

1. Download the HTTP File Server hfs.exe application to the Host Machine.
   NOTE: The HTTP File Server may be running on the same machine where and FreeSwitch are installed or on a separate machine.
2. (*Optional*) Disable port 80 on the server.
3. Run the **hfs.exe** program.
4. Under **Menu**, select **IP Address**.
5. Select the corresponding IP address.



6. Copy the **46xxsettings.txt** file to the server machine. This file can be downloaded from the following link:
https://support.avaya.com/downloads/download-details.action?contentId=C2009071016160372125345&productId=P0553

   – In the **######### SERVER SETTINGS (SIP) #########** section of the **46xxsettings.txt** file, do the following:
   a. Enter the IP address for the server running the FreeSwitch in the **SET SIPDOMAIN** field.
   b. Enter **5060** in the **SET SIPPORT** field.
   c. Enter the IP address for the server running the FreeSwitch in the **SET SIP_CONTROLLER_LIST** field.
   d. Enter the IP address for the server running the HTTP File Server in the **SET CONFIG_SERVER** field.



7. Enter **0** in the **SET SIPSIGNAL** field.
8. Add the **46xxsettings.txt** file to the hfs tool.

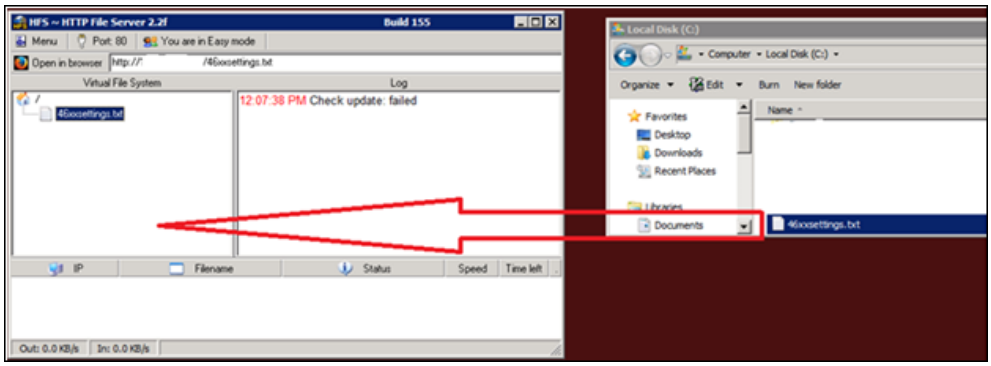


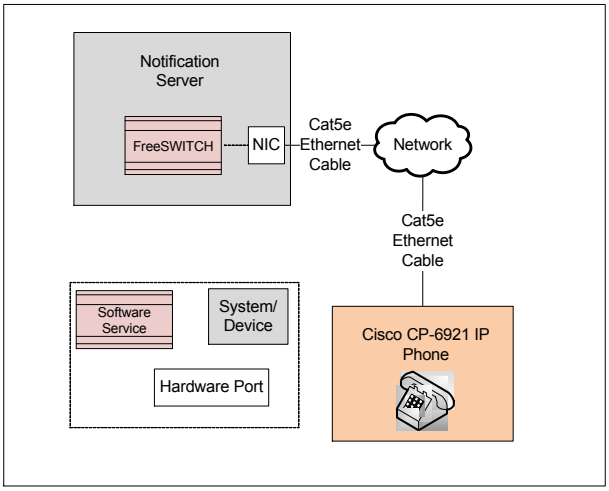
Fig. 34: Adding Text File

1.17 IP Phone Cisco (CP-6921)

IP Phone Cisco (CP-6921)

This section provides reference and background information for integrating the IP Cisco CP-6921 device. For procedures and workflows, see the step-by-step section.

The Cisco CP-6921 phone is a VoIP telephone used by to make live announcements, listen to pre-recorded messages, record audio messages, or initiate incidents through an Interactive Voice Response (IVR) system. The phone communicates with VoIP Switch system.



The following subsections provide the user with a brief description of and how the Internet Protocol (IP) phone is integrated.

The system can integrate with the following Voice over Internet Protocol (VoIP) phones:

- Cisco CP-6921
- Polycom SoundPoint 331
- Avaya 9620L
- Stentofon IP Desktop Intercom Station
- Stentofon IP Dual Display Intercom Station

NOTE:
This guide provides detailed step-by-step instructions on configuring the Cisco CP-6921 IP phone. For information on configuring the other supported VoIP phones, refer to the respective VoIP phone integration guide.

IP Phone Cisco (CP-6921)

This section provides additional procedures related to IP Phone Cisco (CP-6921).

Installing IP Phone Cisco (CP-6921)

This section provides information on mounting the hardware and wiring / connection details for the device.

Prerequisites

- Cisco CP-6921 IP phone with bundled accessories
- Software Version - 9.4.1.3

Mechanical Installation

For mechanical installation and setup, follow the instructions mentioned in the installation manual provided by Cisco.

Electrical Installation

For electrical installation and setup, including power and Ethernet connections, follow the instructions mentioned in the installation manual provided by Cisco.

Configuring IP Phone Cisco (CP-6921)

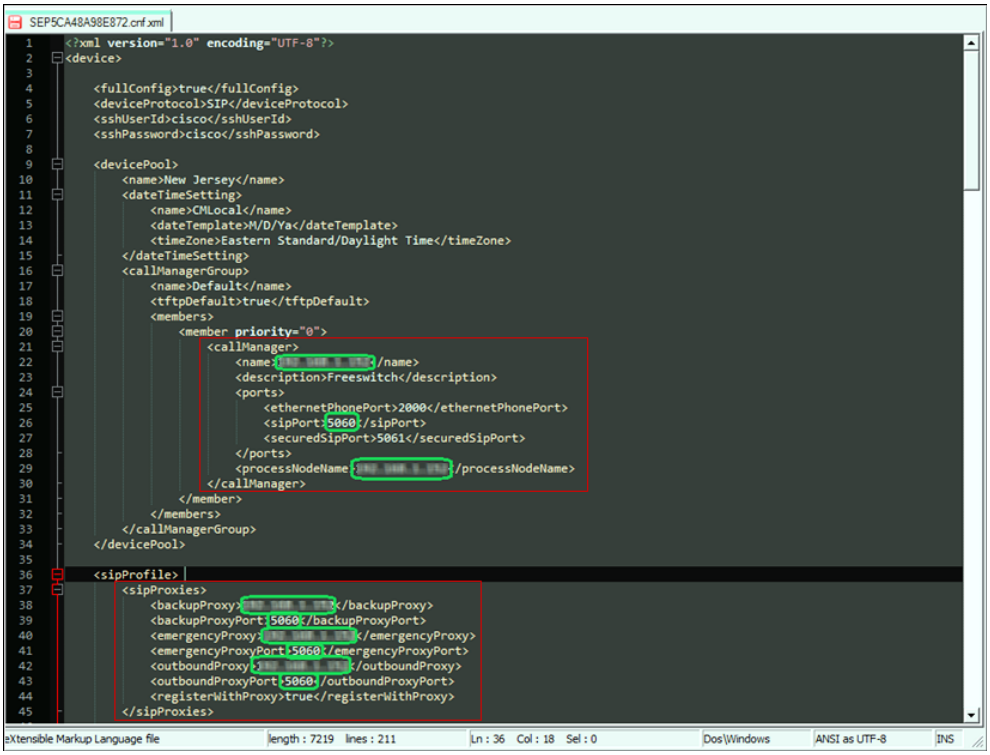
After mounting and wiring the IP phone, configure the phone to communicate with the software PBX included with .

Prerequisites

1. Install the Trivial File Transfer Protocol (TFTP) Server on the host machine (the same server where is installed).
2. Set up a directory containing the files that will be used by the TFTP Server to transfer configuration to the phone. The TFTP server should use this directory in the setup. For example, **C:\Program Files\Tftpd64**. The required files are **dialplan.xml** and **SEPxxxxxxxxxxxx.cnf.xml** (where xxxxxxxxxxxx is the phone's MAC address).

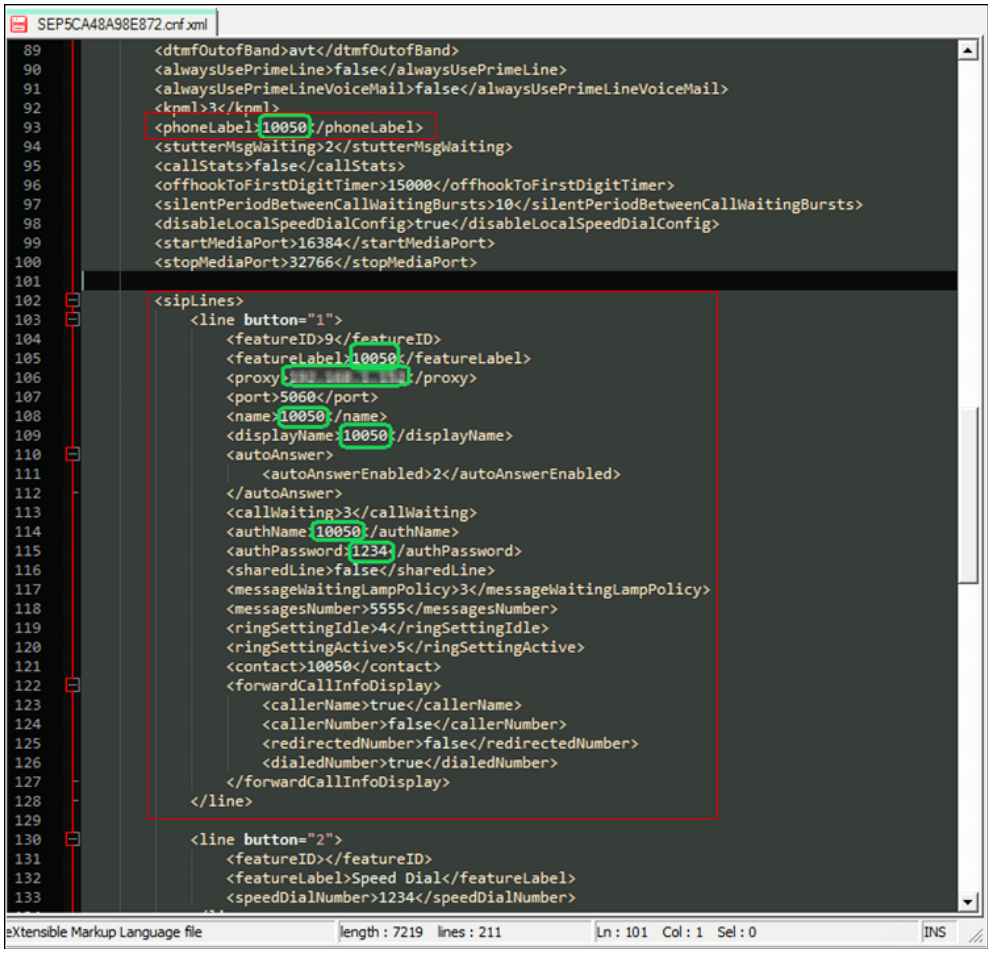
Configuring the SEPxxxxxxxxxxxx.cnf.xml File

1. Open the **SEPxxxxxxxxxxxx.cnf.xml** file.
2. In the **<callManager>** section, do the following:
   a. Enter the IP address for the Server running the FreeSwitch in the **<name>** field.
   b. Set the **<sipPort>** field to **5060**.
   c. Enter the IP address for the Server running the FreeSwitch in the **<processNodeName>** field.
3. Select **<sipProfile>**, in the **<sipProxies>** section, do the following:
   a. In the **<backupProxy>**, **<emergencyProxy>**, and **<outboundProxy>** fields, enter the IP address for the Server running FreeSwitch.
   b. Set the **<backupProxyPort>**, **<emergencyProxyPort>**, and **<outboundProxyPort>** fields to **5060**.



4. In the **<phoneLabel>** field, enter the FreeSwitch extension assigned to the Cisco CP-6921 IP phone.

5. In the **<sipLines>** section, do the following:
   a. Enter the FreeSwitch extension assigned to the Cisco CP-6921 IP phone in the **<featureLabel>** field.
   b. Enter the IP address for the server running the FreeSwitch in the **<proxy>** field.
   c. Enter the FreeSwitch extension assigned to the Cisco CP-6921 IP phone in the **<name>**, **<displayName>**, **<authName>**, and **<contact>** fields.
   d. Enter the password of the FreeSwitch extension assigned to the Cisco CP-6921 IP phone in the **<authPassword>** field.



6. Save the **SEPxxxxxxxxxxx.cnf.xml** file.

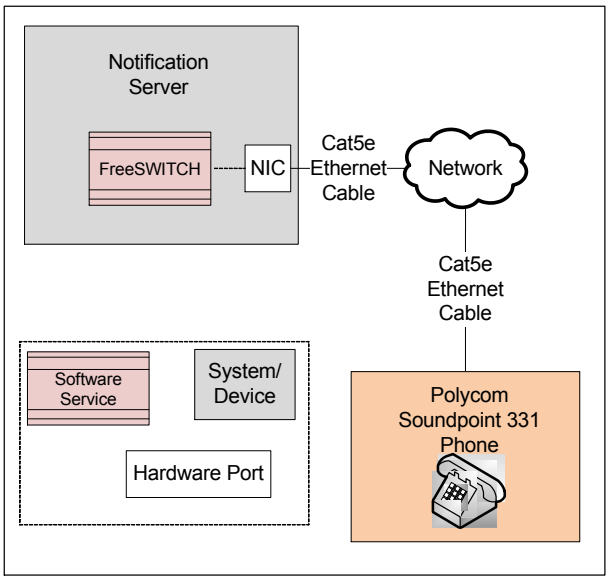
1.18 IP Phone Polycom (Soundpoint 331)

IP Phone Polycom (Soundpoint 331)

This section contains general reference information about Notification and how the Polycom (Soundpoint 331) Internet Protocol (IP) phone is integrated. For procedures and workflows, see step-by-step section.

The Polycom Soundpoint 331 phone is a VoIP telephone used by to make live announcements, listen to pre-recorded messages and record audio messages. The phone communicates with ‘s VoIP Switch system.

The IP Phone and allow the use of SSL through certificates. This is an optional configuration, but is recommended to prevent unwanted access or attacks from outside parties. The use of SSL certificates provide authentication, encryption, and integrity checking between and the IP Phone.



The system can integrate with the following Voice over Internet Protocol (VoIP) phones:

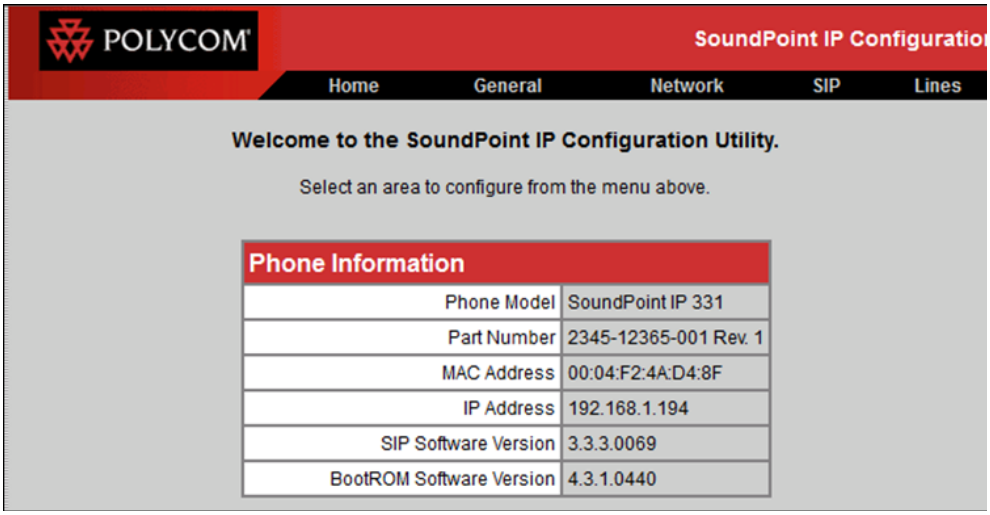
- Polycom SoundPoint 331
- Cisco CP-6921
- Avaya 9620L
- Stentofon IP Desktop Intercom Station
- Stentofon IP Dual Display Intercom Station

Provisioning Phone and Updating Software

Before configuring the IP phone, the recommendation for the user is to obtain the phone build configuration information. This data can be accessed through web interface after properly setting up the network configuration on the phone (once the phone IP address is known). The default user name and password are **Admin** and **456** respectively.

NOTE: For phones running on older software versions, the default user name is **Polycom**.

The following image provides the details of an IP phone running on an old software version:



The following image provides the details of an IP phone running on a new software version:

To set up the IP phone, follow the Polycom's Provisioning Guide located at **https://support.polycom.com/content/dam/polycom-support/products/voice/soundpointip/user/en/provisioning-guide-phones-ucs-4-0-1.pdf**.

The Polycom SoundPoint IP 331phone may have an old version of the SIP software. If the phone has a SIP software version prior to 4.0.1 (for example, 3.3.3.x), then there is a special procedure to update the software. This procedure provides instructions to upgrade to 4.0.1. Refer to the document located at **https://support.polycom.com/content/dam/polycom-support/products/Voice/polycom_uc/other-documents/en/Upgrade_Downgrade_UCS_v4_0_0_EA64731.pdf**.

To set up the Provisioning Server (FTP Server) to update the software to the phone, refer to the *Setting Up the Provisioning Server* section of the document located at the following link.

https://support.polycom.com/content/dam/polycom-support/products/voice/soundstation-ip-series/user/en/uc-ag-4--0--5.pdf.

The provisioning server may be set up on the same machine where is installed but in this configuration the phone should be assigned to a fixed IP (not a DHCP). If the phone is set up for DHCP, it is better to use the provisioning server on the same machine as the DHCP server.

The TFTP Server (tftpd64) was used in the verification. Appropriate setting on the phone should be selected to match the server type. Also, ensure that only TFTP related services are enabled in the TFTP tool and other services. For example, DHCP, Syslog are disabled unless they are needed.

The SIP Server address is the address of the machine where is installed. It is the same as the address of the provisioning boot server if the same machine is used for both purposes.

The steps for setting up provisioning boot server information to the phone may be done through the web interface or on the phone.

An XML editor may be replaced with a regular text editor assuming the user is familiar with the XML file fields.

IP Phone Polycom (Soundpoint 331)

This section provides additional procedures related to Polycom (Soundpoint 331) Internet Protocol (IP) phone.

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

Installing IP Phone Polycom (Soundpoint 331)

This section provides information on mounting hardware and wiring/connection details for the device.

Prerequisites

- Polycom SoundPoint IP 331 with bundled accessories
- Polycom Unified Communications Software (UCS) v4.1.1, installed on the Polycom 331
- OPTIONAL: CA Certificate in X.509 format with Privacy Enhanced Email (PEM) extension. This is only required if configuring the IP phone with the Transport Layer Security (TLS). Certificates are to be obtained from the site's IT administrator. Siemens and Polycom will not supply security certificates.

Mechanical Installation

- For mechanical installation and setup, follow the instructions on the *Polycom SoundPoint IP 321/331/335 Quick Start Guide*.

Electrical Installation

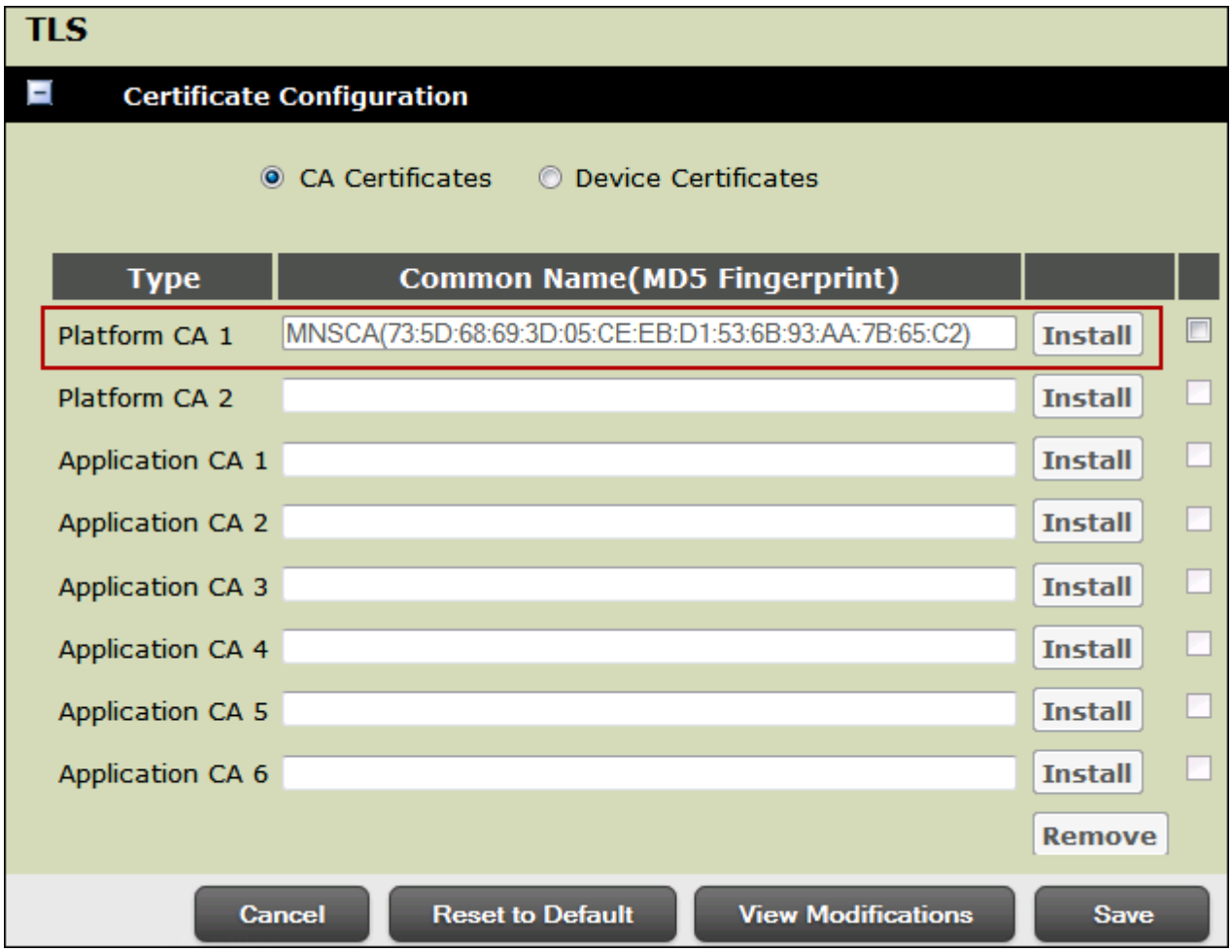
- For electrical installation and setup, including power and Ethernet connections, follow the instructions on the *Polycom SoundPoint IP 321/331/335 Quick Start Guide*.

Configuring TLS/SSL

▷ CA Certificate in X.509 format with Privacy Enhanced Email (PEM) extension.

▷ HTTP website to host the CA certificate. The CA certificate can only be uploaded to the IP phone through a HTTP website.

1. From the home page, select **Settings > Network > TLS**.
2. Selectr the **Certificate Configuration** section.
3. Select **CA Certificates**.
4. Select the Platform CA 1, enter the HTTP address where the IP Phone will download the CA certificate from and click **Install**.
   NOTE: The HTTP address should contain the full path to the certificate including the certificate name. For example, **http://website_ip_address/certificate_folder/myCA.pem**.



5. Select **TLS Profiles**, verify that **Default** is selected from the Type for all Profile Names. Platform 1 or Platform CA 1 should be selected for the CA certificate. The Platform Credential 1 should be selected for Device Credentials.

6. Click **Save**.
7. Change the transport type to TLS.
8. Select **Utilities > Reboot Phone**.
   NOTE: When TLS is enabled, change all SIP port numbers on the IP Phone to 5061.

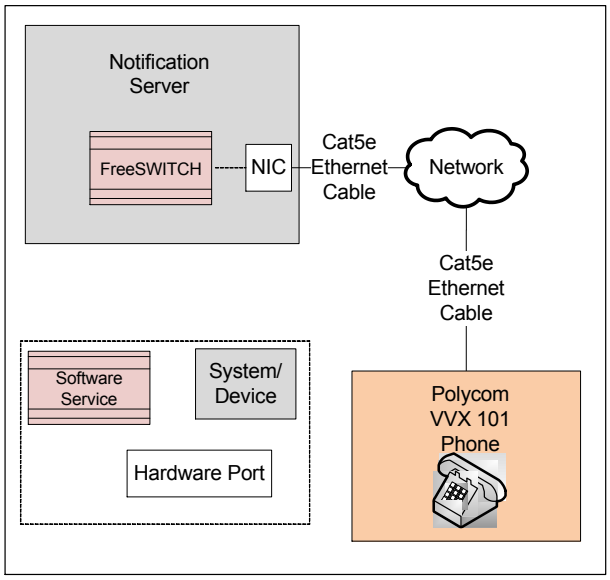
1.19 IP Phone Polycom (VVX 101)

IP Phone Polycom (VVX 101)

This section contains general reference information about Notification and how the Polycom (VVX 101) Internet Protocol (IP) phone is integrated. For procedures and workflows, see step-by-step section.

The Polycom VVX 101 phone is a VoIP telephone used by to make live announcements, listen to pre-recorded messages and record audio messages. The phone communicates with ‘s VoIP Switch system.

The IP Phone and allow the use of SSL through certificates. This is an optional configuration, but is recommended to prevent unwanted access or attacks from outside parties. The use of SSL certificates provide authentication, encryption, and integrity checking between and the IP Phone.



The system can integrate with the following Voice over Internet Protocol (VoIP) phones:

- Polycom VVX 101
- Polycom SoundPoint 331
- Cisco CP-6921
- Avaya 9620L
- Stentofon IP Desktop Intercom Station
- Stentofon IP Dual Display Intercom Station

Provisioning Phone and Updating Software

Before configuring the IP phone, the recommendation for the user is to obtain the phone build configuration information. This data can be accessed through web interface after properly setting up the network configuration on the phone (once the phone IP address is known). The default user name and password are **Admin** and **456** respectively.

The following image provides the details of an IP phone running on a new software version:

To set up the IP Phone, refer the document located at following link. Also to set up provisioning Server (FTP Server) to update the software to the phone, refer to the Setting Up the Provisioning Server section of the document located at the following link.

https://www.polycom.fr/content/dam/polycom-support/products/Voice/business_media_phones/user/en/uc-admin-5-4-1.pdf

The provisioning server may be set up on the same machine where is installed but in this configuration the phone should be assigned to a fixed IP (not a DHCP). If the phone is set up for DHCP, it is better to use the provisioning server on the same machine as the DHCP server.

The TFTP Server (tftpd64) was used in the verification. Appropriate setting on the phone should be selected to match the server type. Also, ensure that only TFTP related services are enabled in the TFTP tool and other services. For example, DHCP, Syslog are disabled unless they are needed.

The SIP Server address is the address of the machine where is installed. It is the same as the address of the provisioning boot server if the same machine is used for both purposes.

The steps for setting up provisioning boot server information to the phone may be done through the web interface or on the phone.

An XML editor may be replaced with a regular text editor assuming the user is familiar with the XML file fields.

IP Phone Polycom (VVX 101)

This section contains additional procedures related to Polycom (VVX 101) Internet Protocol (IP) phone.

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

Installing IP Phone Polycom (VVX 101)

This section provides information on mounting hardware and wiring/connection details for the device.

Prerequisites

- Polycom VVX 101 with bundled accessories
- Polycom Unified Communications Software (UCS) v4.1.1, installed on the Polycom VVX 101
- OPTIONAL: CA Certificate in X.509 format with Privacy Enhanced Email (PEM) extension. This is only required if configuring the IP phone with the Transport Layer Security (TLS). Certificates are to be obtained from the site's IT administrator. Siemens and Polycom will not supply security certificates.

Mechanical Installation

For mechanical installation and setup, follow the instructions on the *Polycom VVX 101 Quick Start Guide*.

Electrical Installation

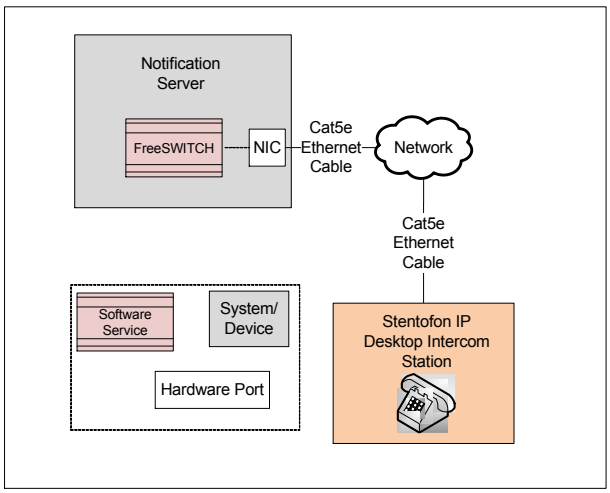
For electrical installation and setup, including power and Ethernet connections, follow the instructions on the *Polycom VVX 101 Quick Start Guide*.

1.20 IP Phone Stentofon (IP Desktop Intercom Station)

IP Phone Stentofon (IP Desktop Intercom Station)

This section provides reference and background information for integrating IP Phone Stentofon (IP Desktop Intercom Station) phone. For procedures and workflows, see step-by-step section.

The Stentofon IP Desktop Intercom Station is a VoIP telephone used by to make live announcements, listen to pre-recorded messages, record audio messages, or initiate incidents through an Interactive Voice Response (IVR) system. The phone communicates with VoIP Switch system.



The system can integrate with the following Voice over Internet Protocol (VoIP) phones:

- Stentofon IP Desktop Intercom Station
- Cisco CP-6921
- Polycom SoundPoint 331
- Avaya 9620L
- Stentofon IP Dual Display Intercom Station

IP Phone Stentofon (IP Desktop Intercom Station)

This section provides additional procedures for integrating IP Phone Stentofon (IP Desktop Intercom Station) phone.

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

Installing IP Phone Stentofon (IP Desktop Intercom Station)

This section provides information on mounting the hardware and wiring / connection details for the device.

Prerequisites

- Stentofon IP Desktop Intercom Station (Manufacturer Item #1008000000.0102) with bundled accessories
- Software Version - 02.03.3.3

Mechanical Installation

For mechanical installation and setup, follow the instructions mentioned in the installation manual provided by Stentofon.

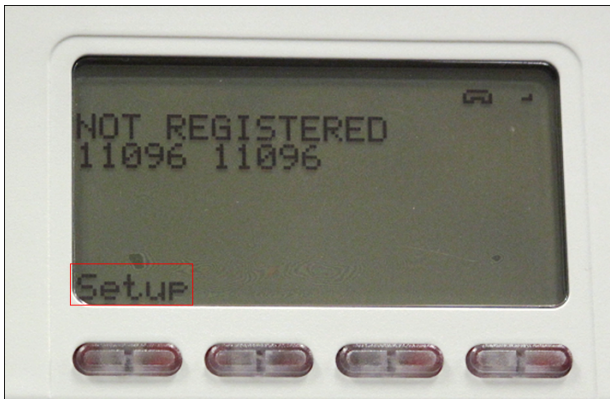
Electrical Installation

For electrical installation and setup, including power and Ethernet connections, follow the instructions mentioned in the installation manual provided by Stentofon.

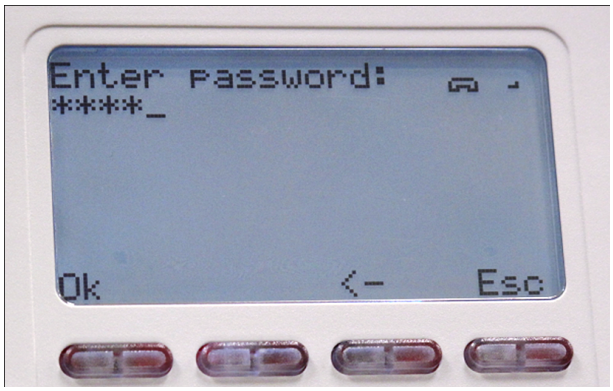
Configuring IP Address

For determining how the IP address is assigned to the phone, do the following:

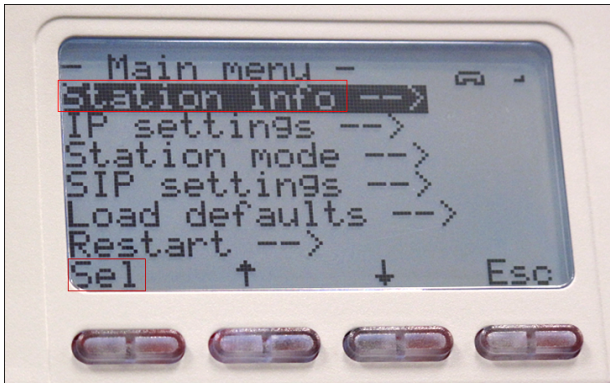
1. Press **Menu** > **Setup** > **Sel** on the phone.



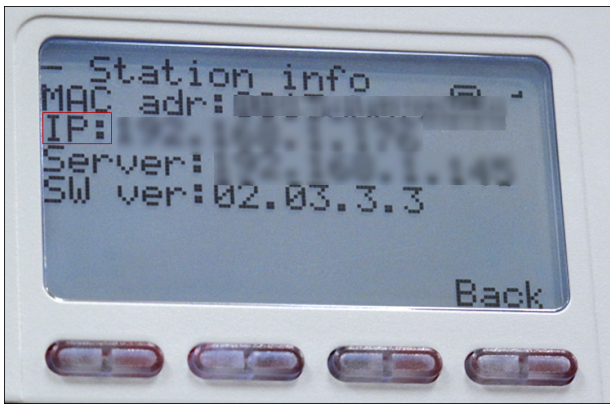
2. Enter the password in the **Enter password** field. The default password is **1851**.



3. Press **OK**.
4. Select **Station Info** and press **Sel**.



⇨ The IP address is displayed in the **IP** field.

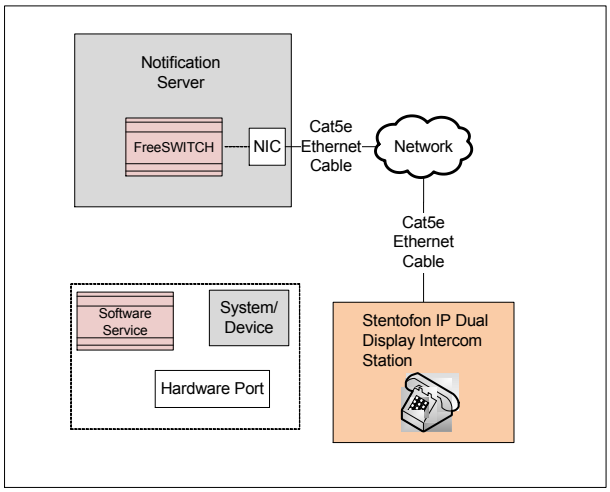


1.21 IP Phone Stentofon (IP Dual Display Intercom Station)

IP Phone Stentofon (IP Dual Display Intercom Station)

This section provides reference and background information for integrating the IP Phone Stentofon (IP Dual Display Intercom Station) phone. For procedures and workflows, see step-by-step section.

The Stentofon IP Dual Display Intercom Station is a VoIP telephone used by to make live announcements, listen to pre-recorded messages, record audio messages, or initiate incidents through an Interactive Voice Response (IVR) system. The phone communicates with ‘s VoIP Switch system.



The system can integrate with the following Voice over Internet Protocol (VoIP) phones:

- Stentofon IP Dual Display Intercom Station
- Cisco CP-6921
- Polycom SoundPoint 331
- Avaya 9620L
- Stentofon IP Desktop Intercom Station

IP Phone Stentofon (IP Dual Display Intercom Station)

This section provides additional procedures for integrating the IP Phone Stentofon (IP Dual Display Intercom Station) phone.

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

Installing IP Phone Stentofon (IP Dual Display Intercom Station)

This section provides information on mounting the hardware and wiring / connection details for the device.

Prerequisites

- Stentofon IP Dual Display Station (Manufacturer Item #1008007000.0200) with bundled accessories
- Software Version - 02.03.3.3

Mechanical Installation

For mechanical installation and setup, follow the instructions mentioned in the installation manual provided by Stentofon.

Electrical Installation

For electrical installation and setup, including power and Ethernet connections, follow the instructions mentioned in the installation manual provided by Stentofon.

Configuring IP Address

For determining how the IP address is assigned to the phone, do the following:

1. Press **Menu** > **Setup** > **Sel** on the phone.

2. Enter the password in the **Enter password** field. The default password is **1851**.

3. Press **OK**.
4. Select **Station Info** and press **Sel**.

⇨ The IP address is displayed in the **IP** field.

Fig. 35: IP Address of Stentofon IP Dual Display Station

1.22 Manually Importing Device Support Libraries

Manually Importing Device Support Libraries

Perform the following steps if the Device Support Libraries are not imported automatically by the system.

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

1. In System Browser, select **Management View**.
2. Select **Project** > **System Settings** > **Libraries**.
   ⇨ The **Library Configurator** tab displays.
3. Click **Import**.
   ⇨ The **Import Libraries** dialog box displays.
4. Select **GMSMainProject >** L**ibraries** > **Exports** to import an already existing library, or browse to the location where the library file is located.
   ⇨ A list of libraries display.
5. Select the library file to add.
   NOTE 1: Select all the device specific **.gms** files with naming format **MassNotification_[DeviceType]_HQ_1.gms**.
   NOTE 2: It is not recommended to import

MassNotification_Common_HQ_1.gms, **MassNotification_CommonTelephony_HQ_1.gms**, and **(MassNotification_[DeviceType]_OM_HQ_1.gms)** libraries as System automatically imports these libraries.

6. Click **Open**.

⇨ The library is imported.
NOTE: Manually Importing Device Support Libraries is applicable for all the devices.

1.23 Media Controller Device

Media Controller Device

This section provides additional procedures for integrating the Media Controller device.

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

Configuring Media Controller Device

Certificate Creation From System Management Console

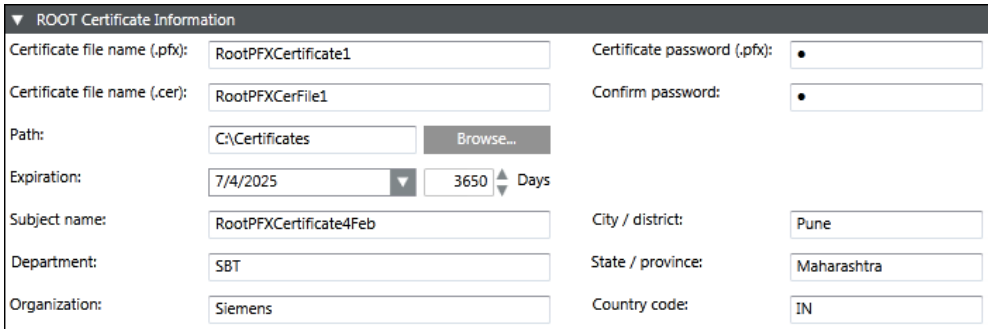
To establish a secure communication between the Media Controller device and the Web Server, certificates need to be configured.

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

1. Create a root certificate Windows store based (.pfx and .cer).
2. Using that root certificate, create a host certificate Windows store based (.pfx).

Create a Root Certificate (.pfx)

1. Double-click **SMC** or right-click **SMC** and select the **Run as administrator** option.
   ⇨ The **System Management Console** window displays.
2. In the **Console** tree, select the **Certificate** node.
   ⇨ The **Certificates** tab displays.
3. Click **Create Certificate** and then select **Create ROOT Certificate (.pfx)** .
   ⇨ The **ROOT Certificate Information** expander displays.



4. In the **ROOT Certificate Information** section, provide the details as follows:

- *(Mandatory field)* Enter the **Certificate file name (.pfx).**
- *(Mandatory field)* Enter the **Certificate file name (.cer).**
- *(Mandatory field)* Enter the **Certificate password (.pfx)** and **confirm** the corresponding password.
- *(Mandatory field)* Browse for the location to store the root certificate on the disk. By default, the path of the last-created root certificate is selected.
- Set the **Expiration** (validity period) duration in days. By default, the certificate expires after 3650 days.
- Enter the following information about the subject:
  a) *(Mandatory field)* **Subject name**: (default) GMS Root Certificate
  b) *(Optional field)* **Department**
  c) *(Optional field)* **Organization**
  d) *(Optional field)* **City / district**
  e) *(Optional field)* **State / province**
  f) *(Optional field)* **Country code** (only two characters)

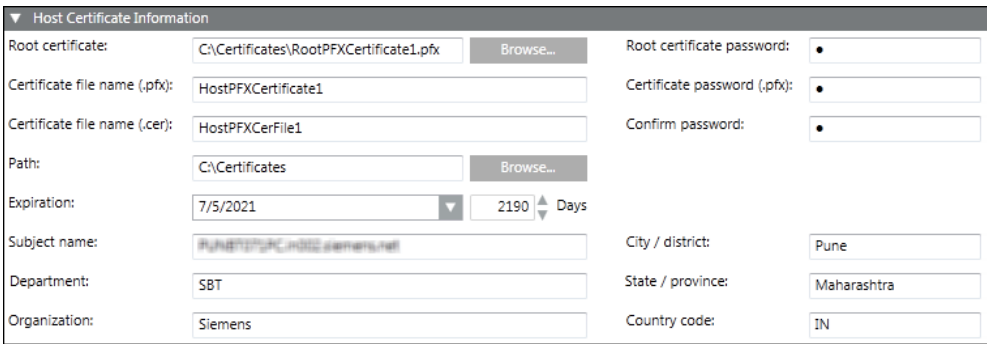
5. Click **Save** to initiate root certificate creation.

⇨ If confirmed, the data entered during the root certificate creation is validated and on successful root certificate creation, two new root certificate files, one with .pfx extension and another with .cer extension, are created at the specified location on the disk.
NOTE 1:
When a root certificate is created for the first time, all the fields are blank. For all subsequent root certificate creation (.pfx or .pem based), by default, the last created root certificate information for some fields, such as **Path**, **Organization** displays.
NOTE 2:
The root certificate (.pfx file) is used to create a host certificate (.pfx file).
NOTE 3:
The **Subject name** should not be set as the full computer name because the host certificate's **Subject name** is required to be set as the full computer name and the host and root certificate's **Subject name** cannot be same, otherwise the Client/Server communication does not work.
NOTE 4:
After the root certificate is imported, the **Subject name** appears in the **Issued To** field of the Windows Certificate store. Provide a unique Subject name. If multiple root certificates are created with the default **Subject name** (GMS Root Certificate), identifying and selecting the correct root certificate from the Windows Certificate store would be difficult.
NOTE 5:
Create multiple host certificates using one root certificate (.pfx file).

Create a Host Certificate (.pfx)

▷ The user must have the root certificate (.pfx file) and the password with which a host (.pfx) certificate needs to be created.

1. Double-click or right-click **SMC** and select the **Run as administrator** option.
   ⇨ The **System Management Console** window displays.
2. In the **Console** tree, select the **Certificate** node.
   ⇨ The **Certificates** tab displays.
3. Click **Create Certificate** and then select **Create Host Certificate (.pfx)** .
   ⇨ The **Host Certificate Information** expander displays.



4. In the **Host Certificate Information** expander, do the following:
   - Browse for the **Root certificate** (.pfx file) from the disk. By default, the last created root certificate (.pfx file) is selected.
   - *(Mandatory field)* Enter the **Root certificate password**.
   - *(Mandatory field)* Enter the **Certificate file name (.pfx)** of the host certificate.
   - *(Mandatory field)* Enter the **Certificate password (.pfx)** for the host certificate and **confirm** the corresponding password.
   - *(Mandatory field)* Enter the **Certificate file name (.cer)** of the host certificate.
   - *(Mandatory field)* Browse for the location to store the certificate on the disk. By default, the path of the last-created root certificate is selected.
   - Set the **Expiration** (validity period) duration in days. By default, the certificate expires after 2190 days.
   - Enter the following information about the subject:
     a) *(Mandatory field)* **Subject name:** (default) the Full computer name of the host machine (including the domain name if the host machine is in a domain), for example, ABCXY022PC.dom01.company.net. However, change this according to where this host certificate will be imported or used.
     b) *(Optional field)* **Department**
     c) *(Optional field)* **Organization**
     d) *(Optional field)* **City / district**
     e) *(Optional field)* **State / province**
     f) *(Optional field)* **Country code** (only two characters)
5. Click **Save** to initiate the file (.pfx) based host certificate creation.
   ⇨ A message displays if the Subject name of the host certificate is same as that of its root certificate.
6. Click **OK**.
7. Click **Save** to initiate the file (.pfx) based host certificate creation.

⇨ The data entered during certificate creation, is validated and on successful certificate creation, the two new host certificate files, one with extension .pfx and another with extension .cer, are created at the specified location on the disk.
NOTE 1:
By default, the subject's identifier information (except for the **Subject name**) is pre-populated with the information of the last root certificate subject.
NOTE 2:
The **Subject name** of the host certificate must not be the same as the **Subject name** of its root certificate.

Importing a Root Certificate in the Windows Store

The following procedure applies only to importing certificates using the SMC. For the non-SMC workstations, import the root certificate (.cer file) using Microsoft Management Console (MMC 3.0).

1. Double-click or right-click **SMC** and select the **Run as administrator** option.
   ⇨ The **System Management Console** window displays.
2. In the **Console** tree, select the **Certificate** node.
   ⇨ The **Certificates** tab displays.
3. Click **Import Certificate** .
   ⇨ The **Import Certificate** expander displays.
4. In the **Import Certificate** expander, do the following:
   – In the **Certificate type** field, select the **Root certificate** option.
   – In the Certificate field, click **Browse** and select the **Certificate file**. Import the appropriate certificate for the selected Certificate type to be able to use them. SMC displays a message if the selected certificate does not match the selected Certificate type.
   To import the root certificate , import the root certificate (.cer file) of the root .pfx certificate.
   – *(Optional)* Clear the **Set as default** check box, if the selected certificate is not needed to be set as default. By default, the **Set as default** check box is selected, if the selected **Certificate type** is not already set as default.
5. Click **Save** .

⇨ The selected certificate is imported successfully in the certificate store. The **Certificate Type - Root Certificate** is imported in the Store location, **Local machine Certificates and User Certificates > Trusted Root Certificate Authorities**.

Website Creation

The media works in conjunction with a HTTPS Web Server. The media controller downloads all content from an accessible HTTPS server.

Media Controller - Device Engineering

This section provides the steps necessary to configure a device.

Before the BrightSign device can play media content on the flat panel display, the device needs to be configured to connect to a HTTPS website. To connect securely to a website, the media controller needs to be preloaded with the Certificate Authority (CA) of that website. This allows the media controller to establish a trusted connection with the website so that media can be downloaded.

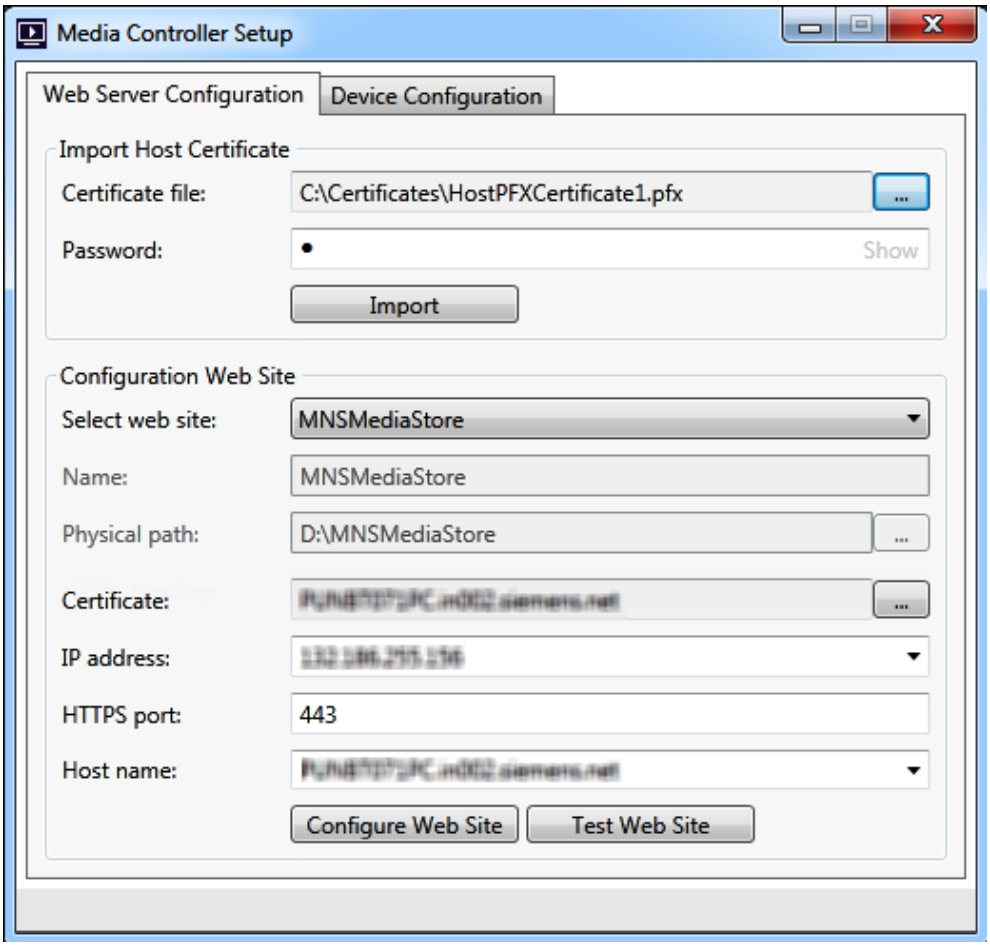
Media Controller Device Set Up

This section describes the setup process for the Media Controller device on a server or a dedicated Web Server.

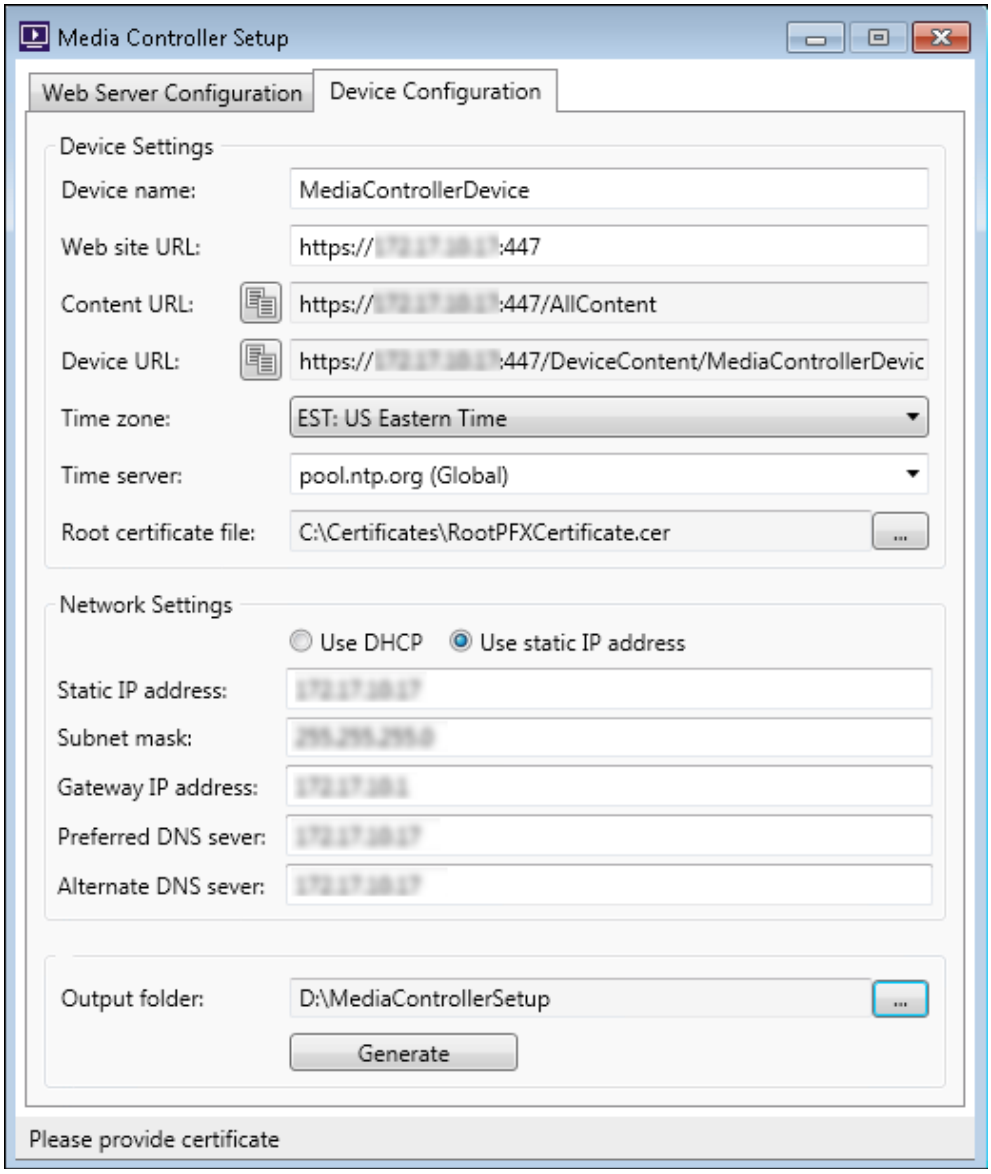
Notification Server

1. Select **(Installation Drive):** > **GMSProjects** > **GMSMainProject** > **bin** > **MNSTools** > **MediaController** folder.
2. Double-click the **MediaControllerSetup.exe** or right-click the **MediaControllerSetup.exe** and select the option **Run as administrator**.

   ⇨ The **Media Controller Setup** dialog box displays.



3. Select the **Device Configuration** tab.



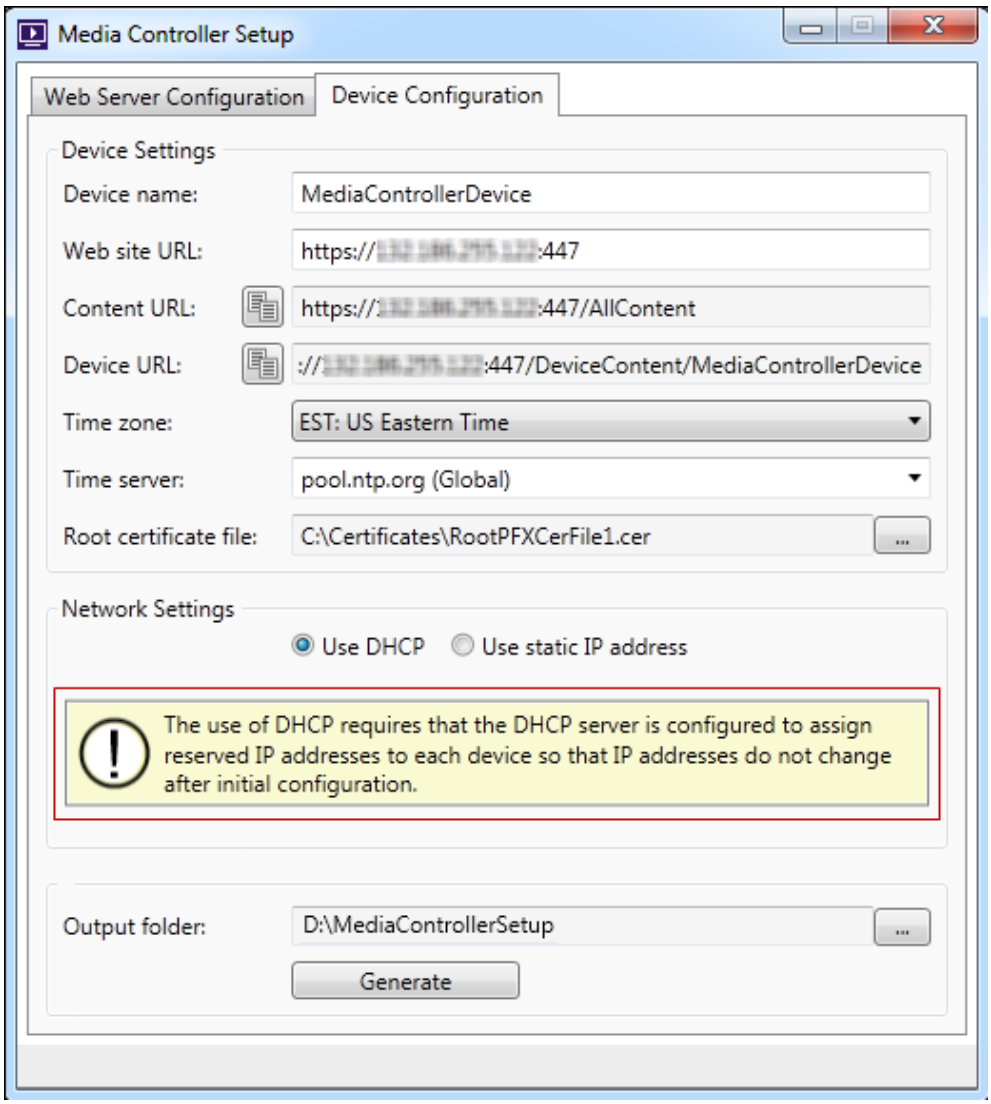
4. In the **Device Settings** section, do the following:
   - In the **Device name** field, enter the folder name for the device. This name is used to access the device. For example, **MediaControllerDevice**. **NOTE:** The **Media Controller Setup** utility automatically creates a folder named **DeviceContent** in the website folder. For example if the name of the website folder is **MNSMediaStore** and if the physical path of this folder is **D:\MNSMediaStore**, then the **Media Controller Setup** utility will create the **DeviceContent** folder inside the **MNSMediaStore** folder and the physical path of the **DeviceContent** folder will be **D:\MNSMediaStore\DeviceContent**. Create a folder of the same name as specified in the **Device name** field in the **DeviceContent** folder manually. For example, a folder named **MediaControllerDevice** at the location **D:\MNSMediaStore\DeviceContent\MediaControllerDevice**. The media controller will download the content in this folder.
   - The **Website URL** field is automatically populated with the URL of the website configured in the **Web Server Configuration** tab. For example, **https://[IPAdress]:[PortName]**
   - The **Content URL** field is automatically populated with the URL of the Content folder from which the media controller downloads the media content. For example, **https://[IPAdress]:[PortName]/AllContent**

NOTE: This Content URL must be specified in the **Media Storage Web Folder URL field** of the System Configuration (Field Network and Device) section. Click  to copy the Content URL.

– The **Device URL** field is automatically populated with the URL of the Device folder from where the media controller downloads the content. The name specified in the **Device name** field is used as the name of the Device folder by the **Media Controller Setup** utility. For example, **https://[IPAdress]:[PortName]/DeviceContent/MediaControllerDevice**
NOTE 1: Ensure that the folder with the same name as specified in the **Device name** field is present in the **DeviceContent** folder, otherwise the media controller will not be able to download the content. For example, **MediaControllerDevice**.
NOTE 2: This Device URL must be specified in the **Web Server Link** field of the Device Configuration Properties section. Click  to copy the Device URL.
– Select the time zone from the **Time zone** drop-down list.
– Select the time server from the **Time server** drop-down list.
NOTE: The above is a prerequisite for the device to have the right time set so that the device can securely download content from the website.
– In the **Root certificate file** field, click  and select the **Root certificate (.cer)**.
NOTE: The **Media Controller Setup** utility allows the import of **Root certificate (.crt) and Root certificate (.pem) also.**

5. In the **Network Settings** section, do the following:

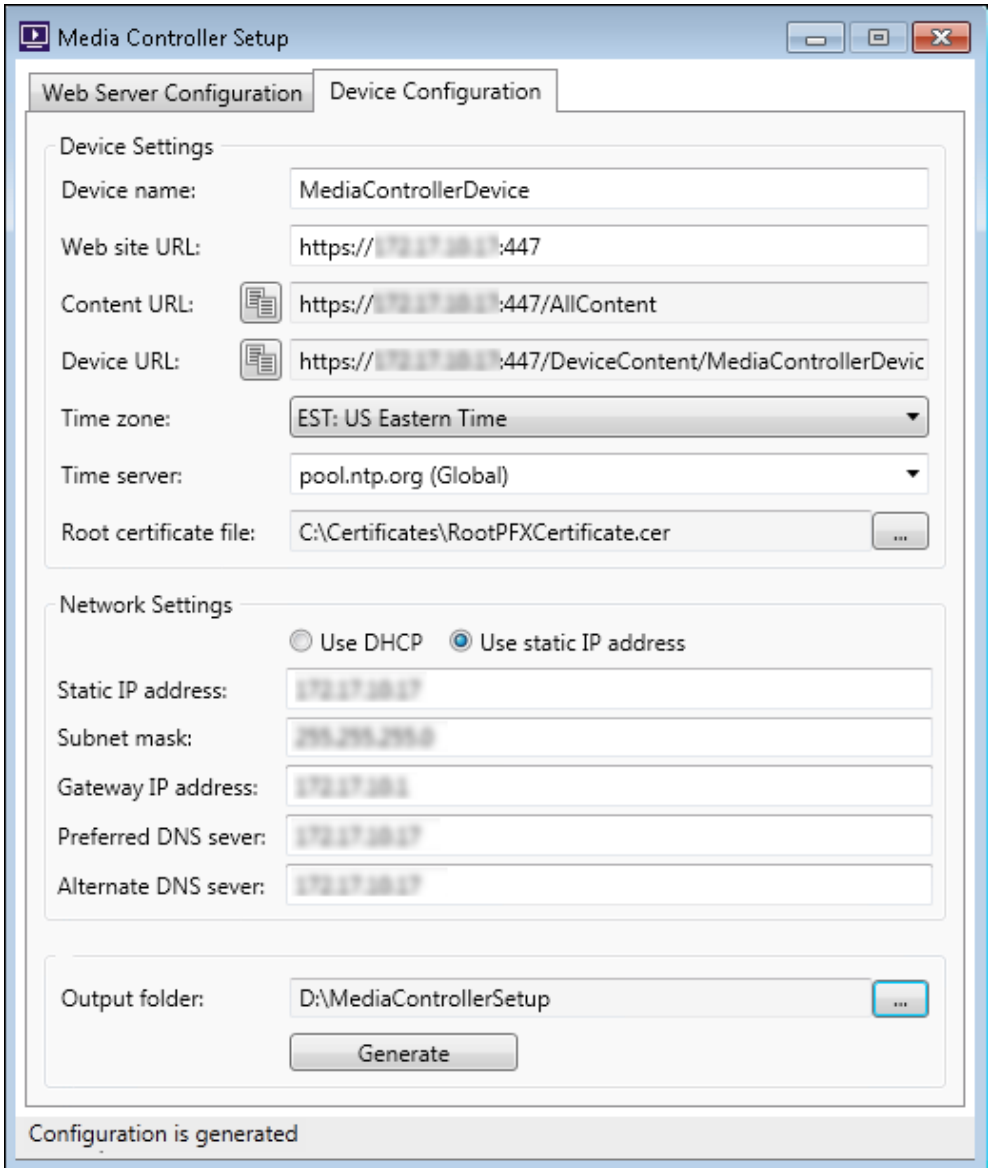
– Select the **Use DHCP** option if the device needs to be set in DHCP mode. If selected the other fields cannot be edited, but can be ignored.
⇨ A message displays if the **Use DHCP** option is selected.



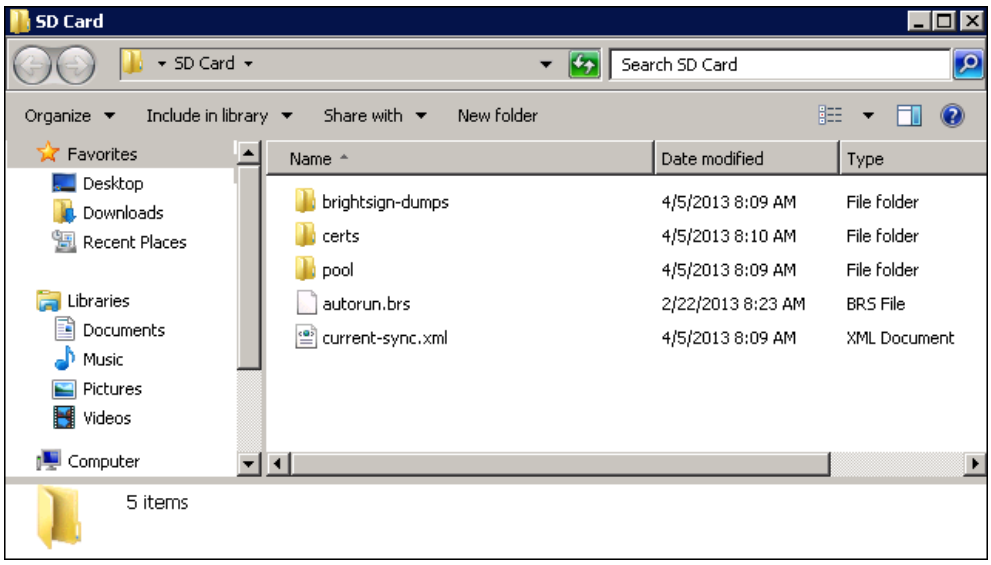
– Select the **Use static IP address** option if the device needs to be configured with a static IP address. Ensure that the remaining fields under network settings are filled out if this option is selected.
– For **static IP address** option, enter the following data in the respective fields:
  a) In the **Static IP address** field, enter the IP address to be used for the device. Ensure that there are no IP address conflicts.
  NOTE: For more details on Network Settings, see the --- MISSING LINK --- section.
  b) In the **Subnet mask** field, enter value for the subnet mask. The value for the subnet mask can be obtained by executing the **ipconfig** command in the command prompt.
  NOTE: In the case of website being on a different machine other than the server, enter the subnet mask of the machine on which the corresponding website is present.
  c) In the **Gateway IP address** field, enter the value for the IP address of the gateway. The value for the subnet mask can be obtained by executing the **ipconfig** command in the command prompt.
  NOTE: In the case of website being on a different machine other than the server, enter the Gateway IP Address of the machine on which the corresponding website is present.
  d) [Optional] In the **Preferred DNS server** field, enter the value for the preferred DNS server. The value for the preferred DNS server can be obtained by executing the **ipconfig** command in the command prompt.

e) [Optional] In the **Alternate DNS server** field, enter the value for alternate DNS server. The value for the alternate DNS server can be obtained by executing the **ipconfig** command in the command prompt.

6. In the **Output folder** field, click ... .
   ⇨ The **Browse For Folder** dialog box displays.
7. Select the location where the setup files need to be copied. It is recommended to select the SD card which will be loaded into the media controller.
8. Click **Generate** to create the setup files.
   ⇨ Upon successful generation of the Device Setup files, a message **Configuration is generated** displays at the bottom of the **Media Controller Setup** dialog box.



9. Once generation is complete, ensure that the files and folders listed in the following image are available on the SD card.



10. Verify that the **Root certificate** is available under the **certs** folder. Connection to the website is not possible without this certificate.

Web Server Installed on a Machine Other Than Notification Server

Do the following if IIS is installed on a different server than the server on which is installed.

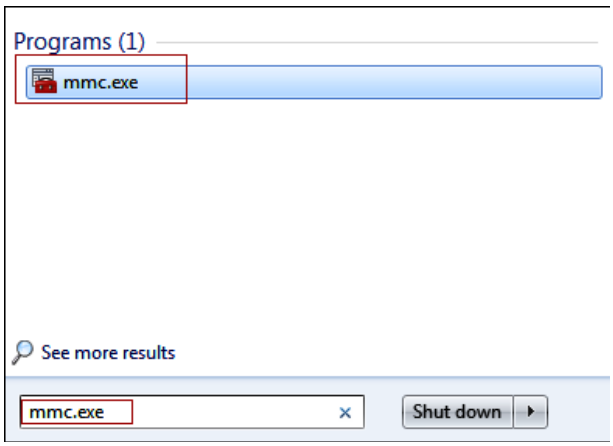
▷ Ensure that the Media Controller device and the Web Server are in the same network (same IP range).

▷ The certificates for the Web Server configuration should be created through SMC as per the steps mentioned in the Creating a Root Certificate (.pfx) and the Creating a Host Certificate (.pfx) sections. The details of the Web Server, for example, the full computer name including the domain name if the Web Server is in a domain, must be entered in the corresponding fields of the certificates.

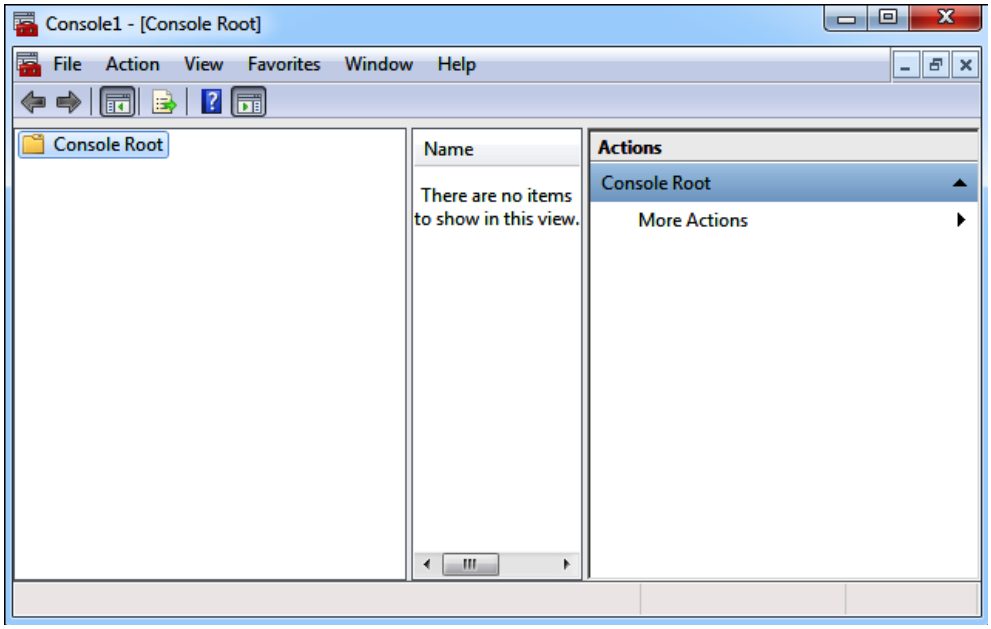
1. Store the certificates in a .zip file and copy the corresponding .zip file to the Web Server.

2. After copying the .zip file, import the root certificate (.cer file) using the Microsoft Management Console (mmc.exe) by performing the following tasks:

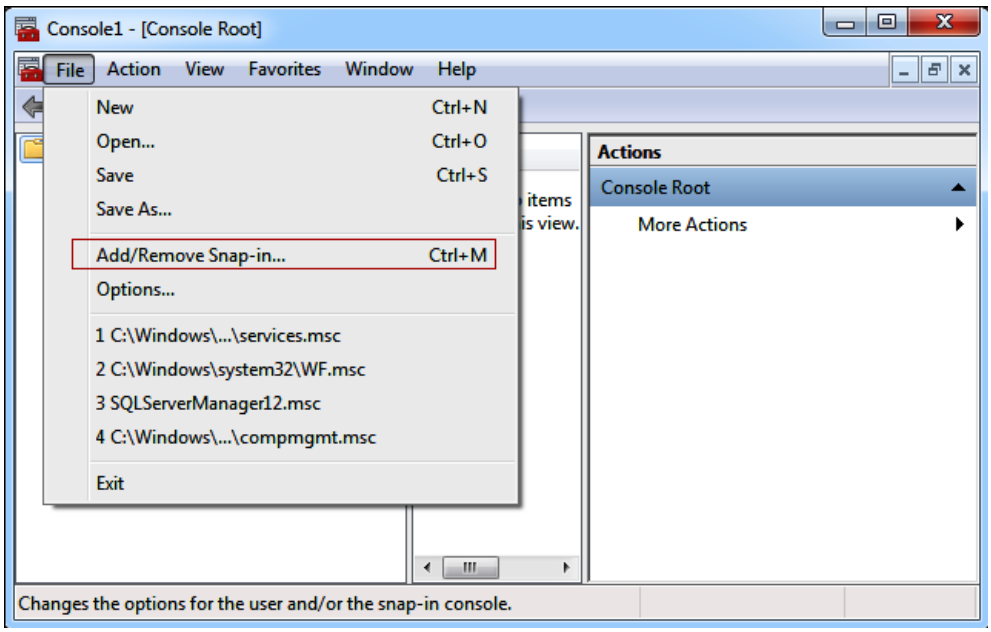
– Open the Windows **Start** Menu and enter **mmc.exe** in the **Search programs and files** field.



– Right-click the **mmc.exe** and select the option **Run as administrator**.
⇨ The **Console Root** dialog box displays.

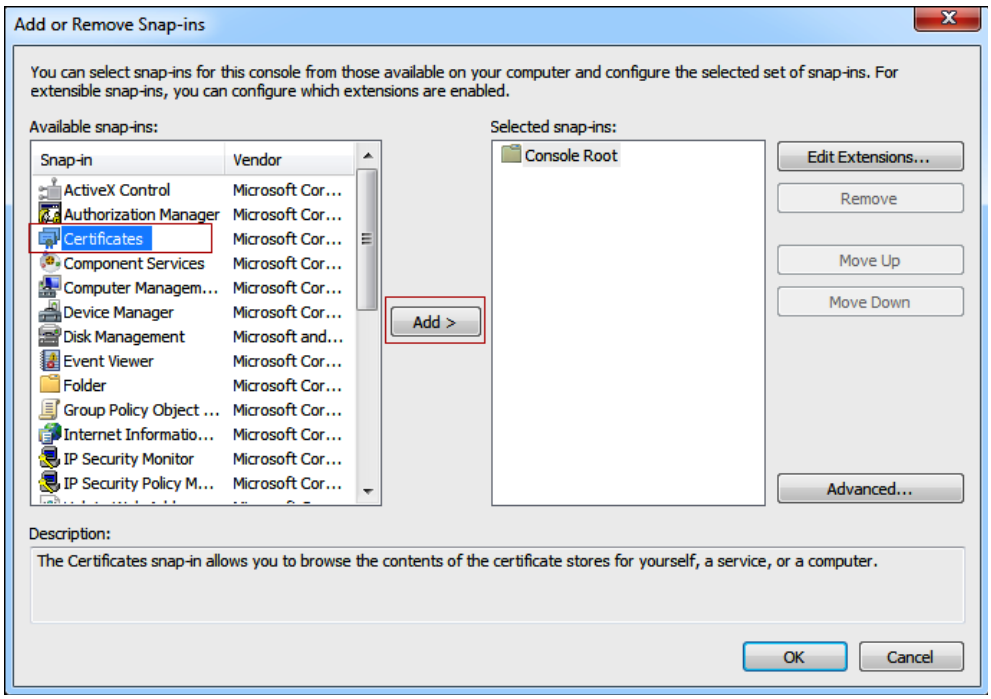


3. Select **File > Add/Remove Snap-in**.



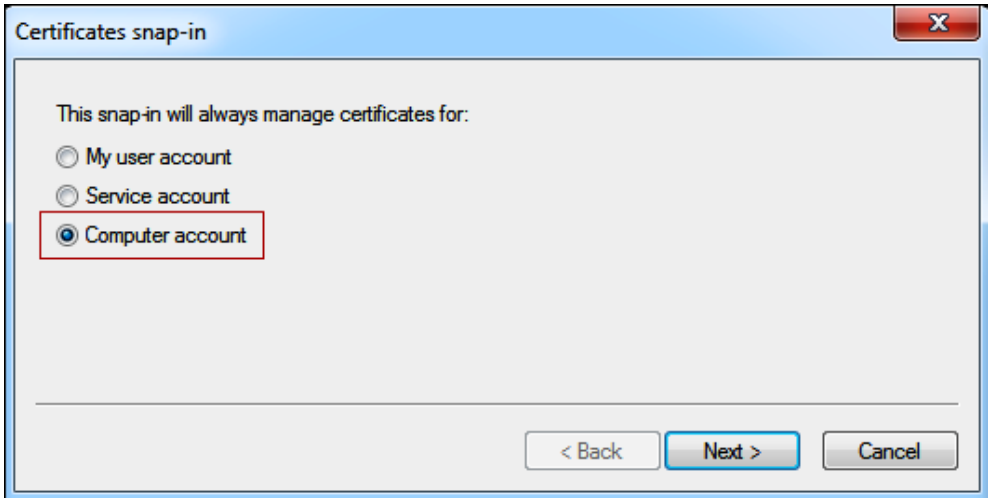
⇨ The **Add or Remove Snap-ins** dialog box displays.

4. Select **Certificates** and click **Add**.



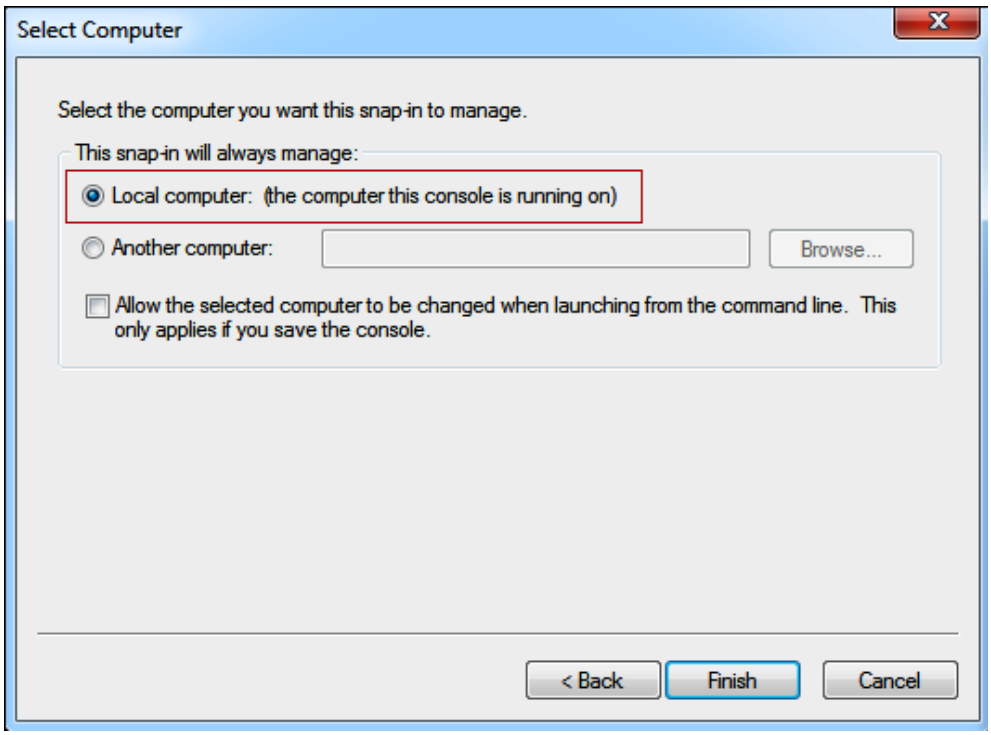
⇨ The **Certificates snap-in** dialog box displays.

5. Select **Computer account** option and click **Next**.

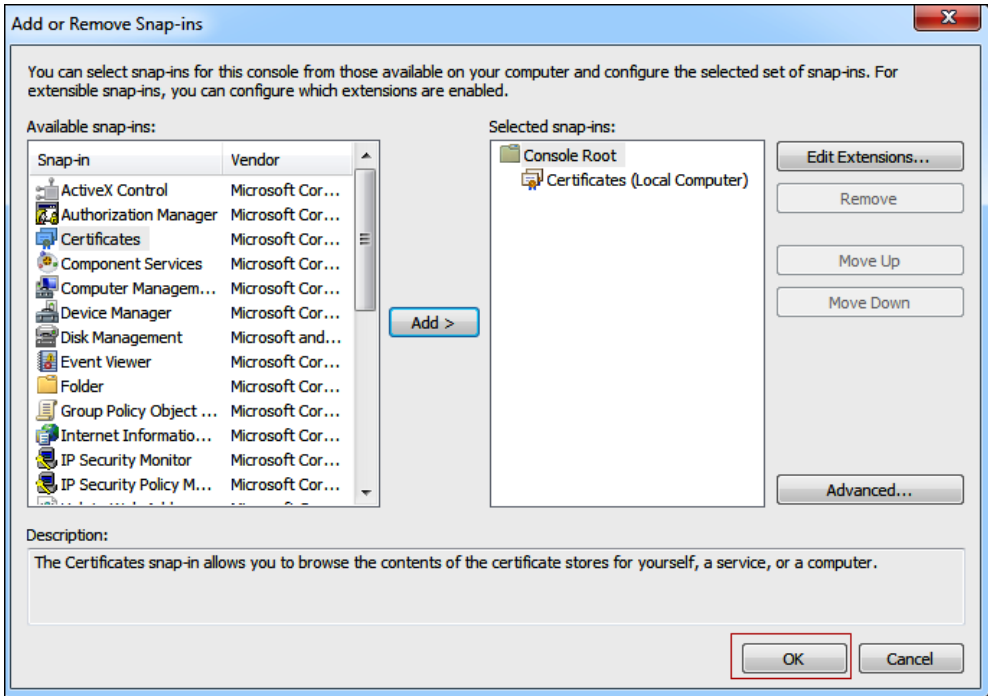


⇨ The **Select Computer** dialog box displays.

6. Select the **Local computer: (the computer this console is running on)** option.

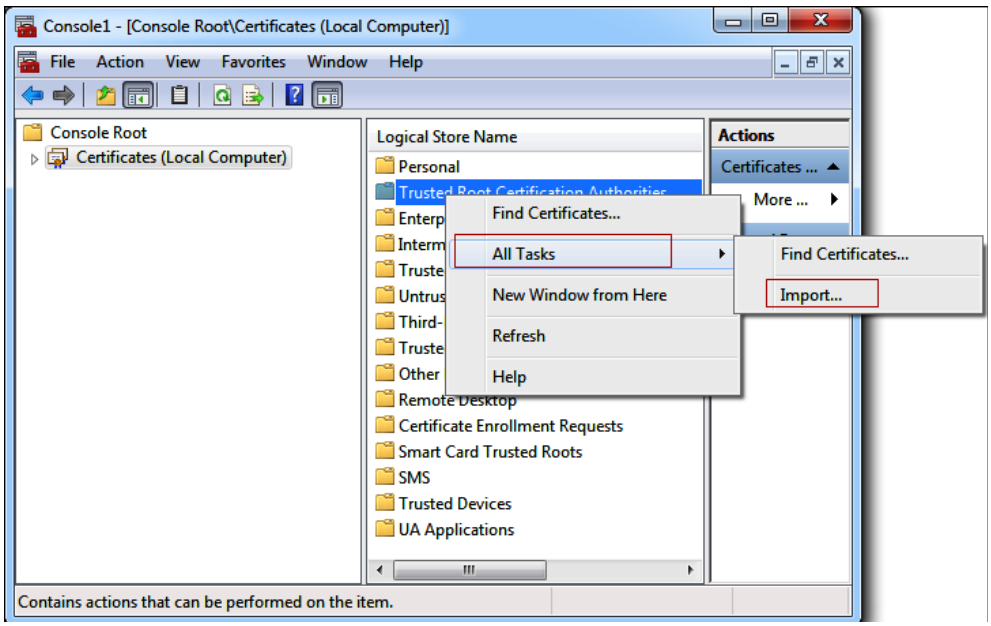


7. Click **Finish**.
8. Click **OK** in the **Add or Remove Snap-ins** dialog box.



⇨ The **Certificates** snap-in is added to the list of **Selected snap-ins**.

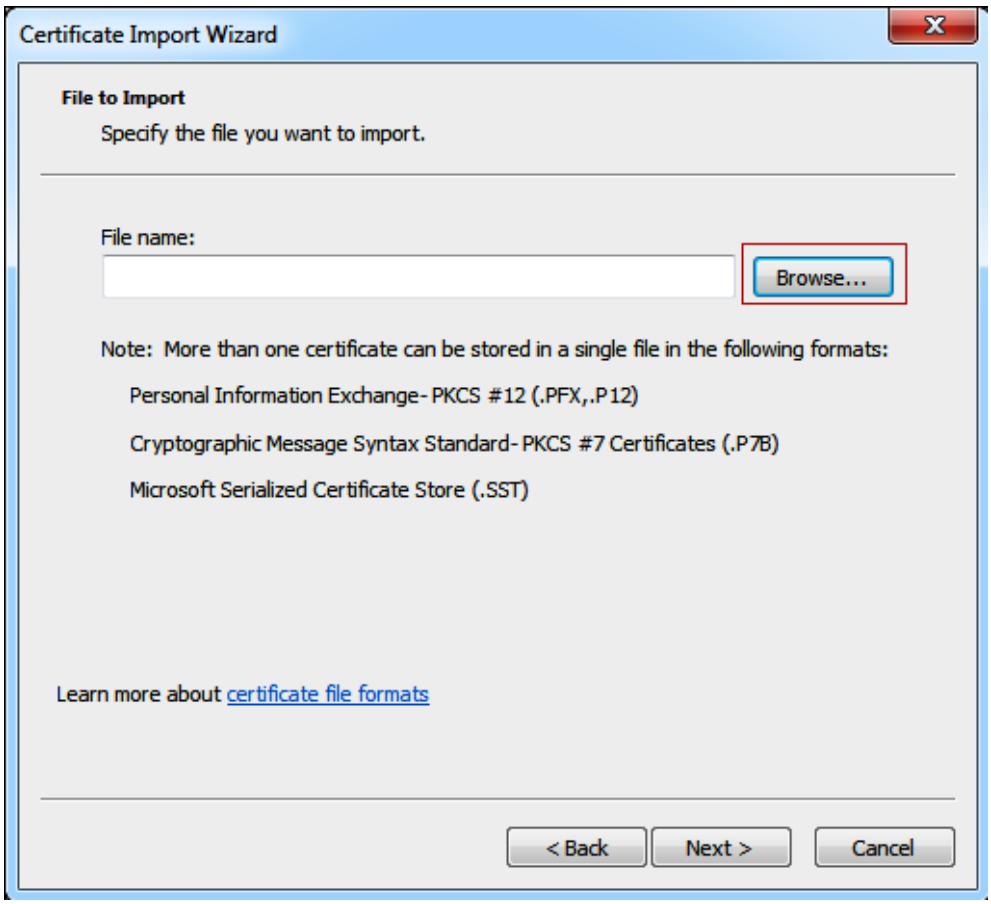
9. Select **Console Root >Certificates (Local Computer)**.
10. Right-click the **Trusted Root Certification Authorities** option in the **Logical Store Name** section and select **All Tasks** > **Import**.



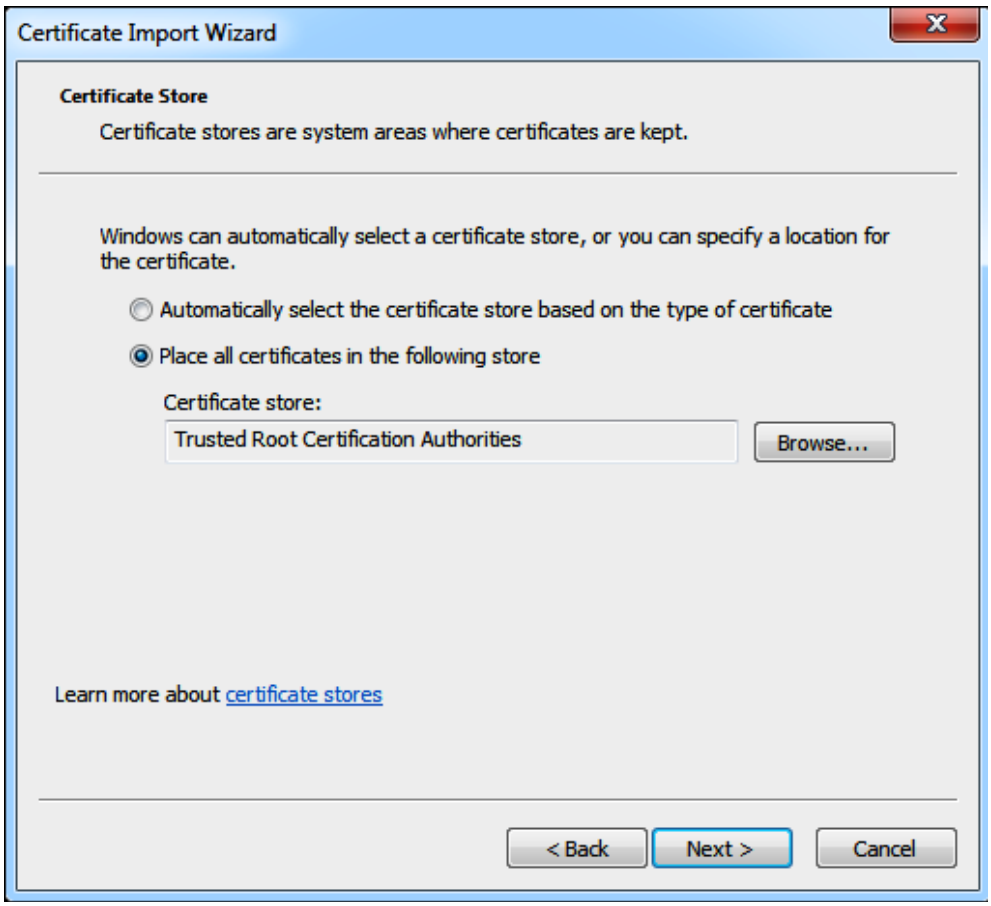
➪ The **Certificate Import Wizard** dialog box displays.

11. Click **Next**.

12. The **File to Import** window displays. Click **Browse** and select the location where the certificates are stored.

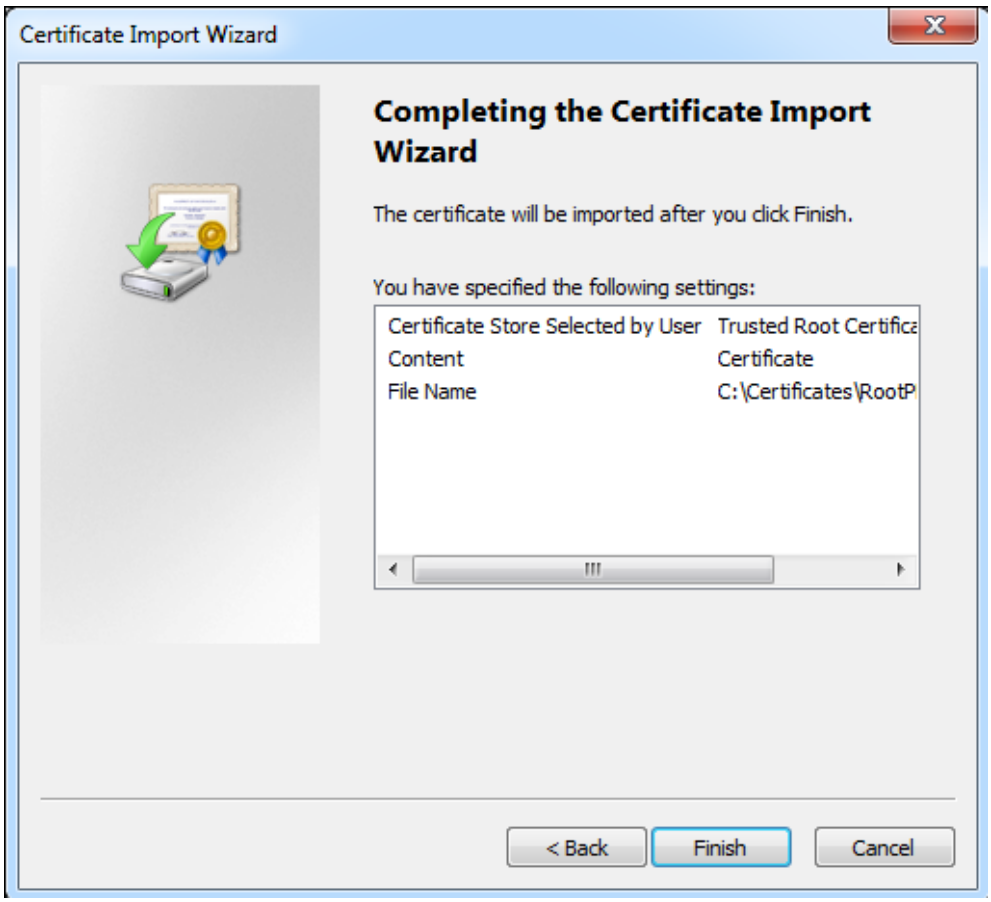


13. Select the root certificate (.cer file).
14. Click **Open**.
    ⇨ The path of the certificate file displays in the **File name** field of the **File to Import** window.
15. Click **Next**.
16. The **Certificate Store** window displays.
17. Select **Place all certificates in the following store** option.



18. Click **Next**.

19. The **Completing the Certificate Import Wizard** window displays.



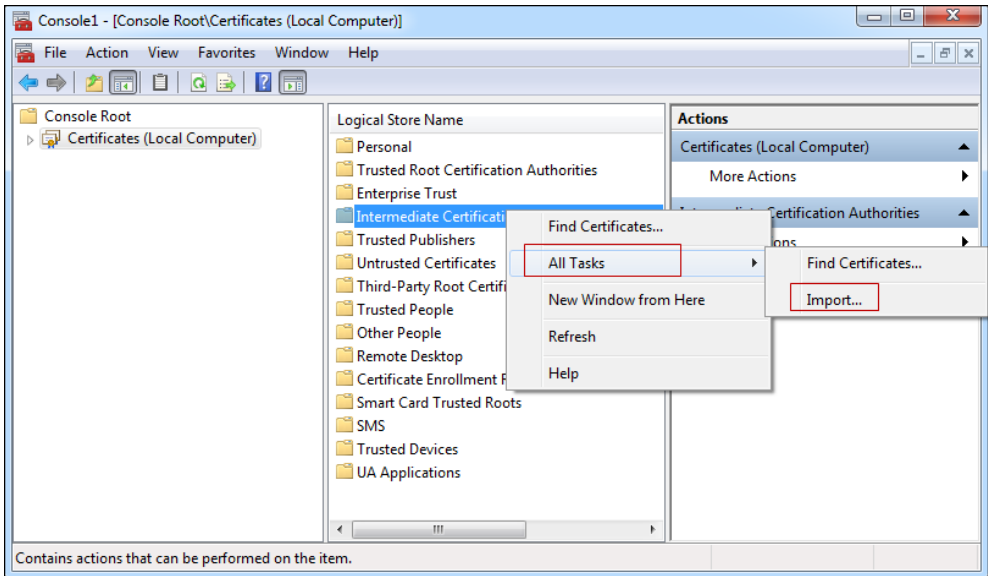
20. Click **Finish**.

⇨ Upon successful import of certificate, a message box displays.

21. Click **OK**.

⇨ The certificate import process for the **Trusted Root Certification Authorities** is complete.

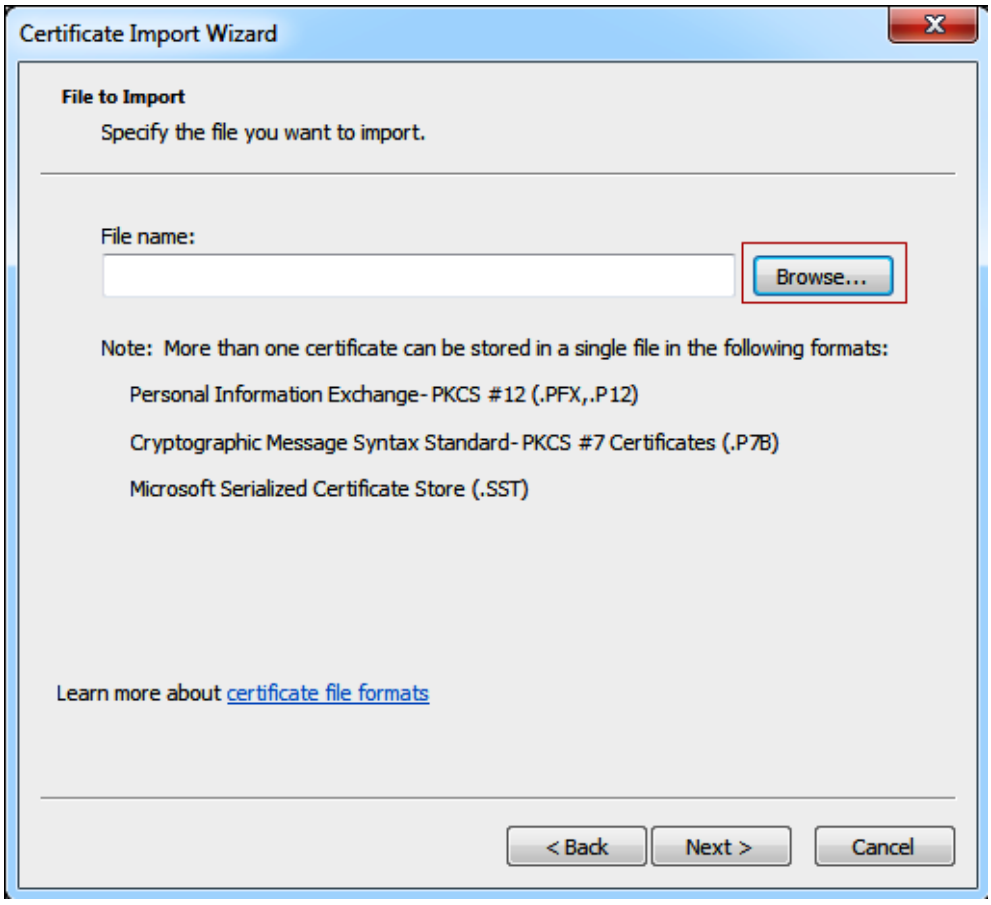
22. Right-click the **Intermediate Certification Authorities** option in the **Logical Store Name** section and select **All Tasks** > **Import**.



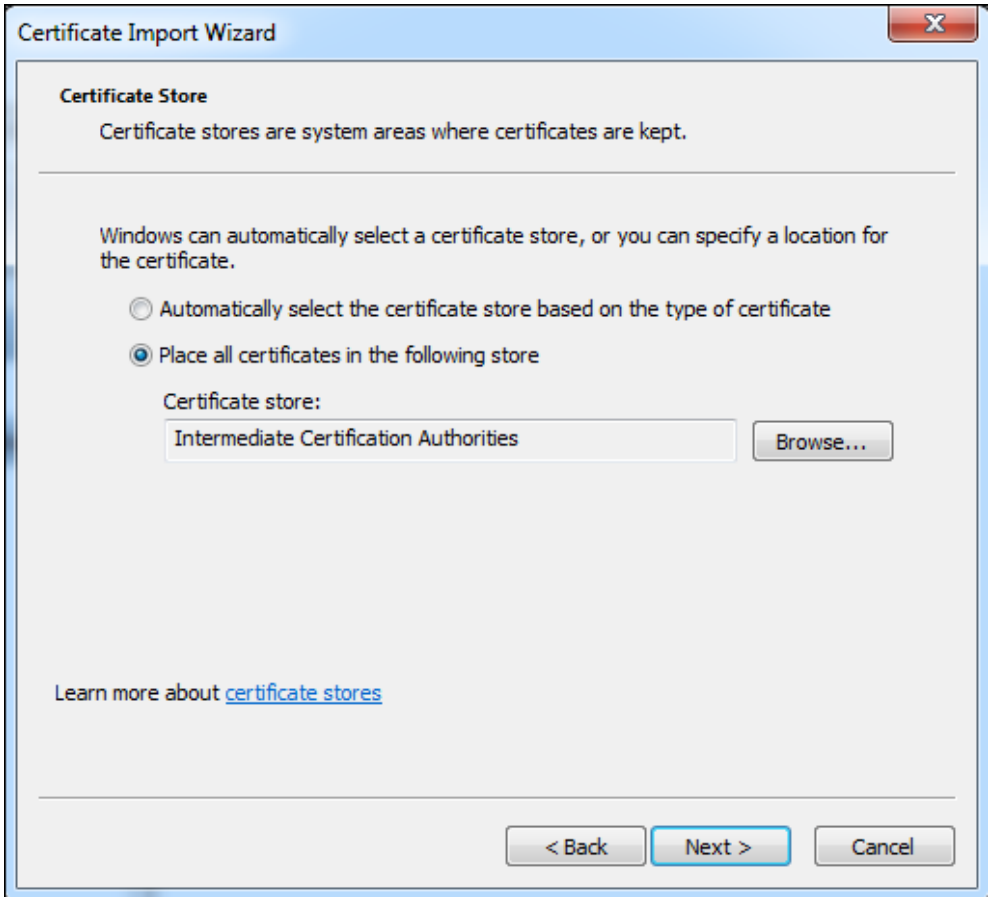
⇨ The **Certificate Import Wizard** dialog box displays.

23. Click **Next**.

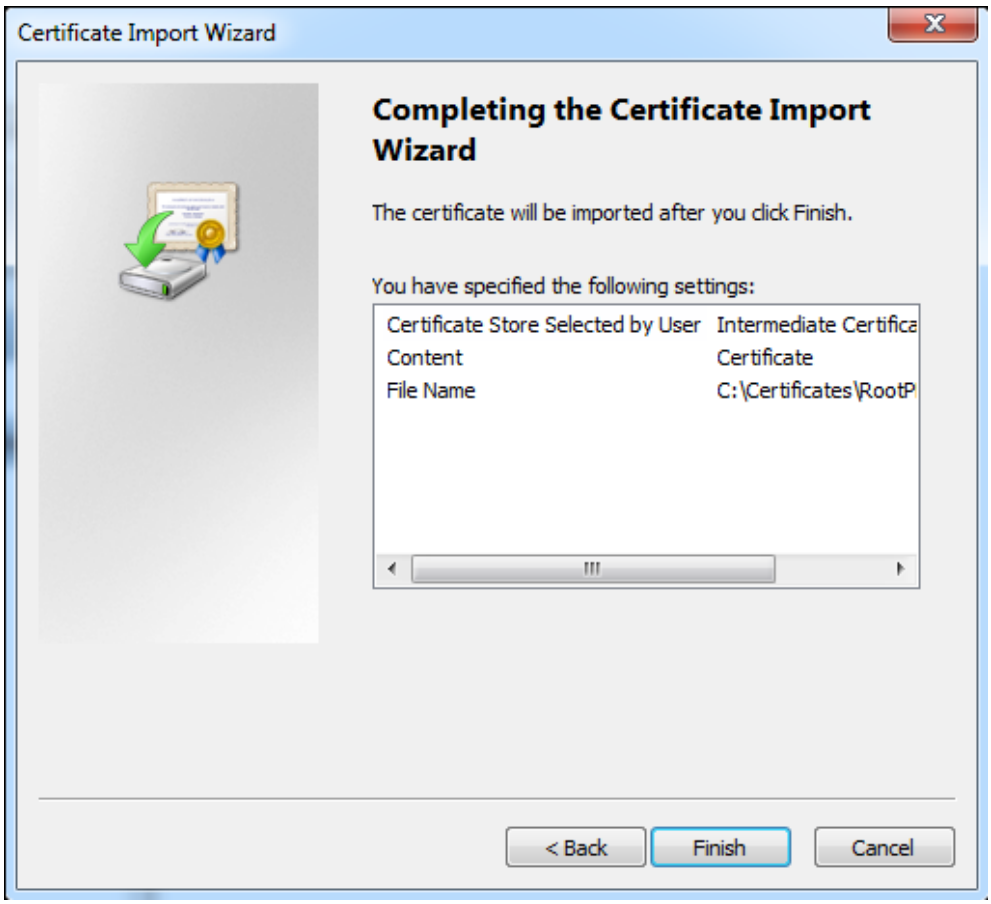
24. The **File to Import** window displays. Click **Browse** and select the location where the certificates are stored.



25. Select the root certificate (.cer file).
26. Click **Open**.
    ⇨ The path of the certificate file displays in the **File name** field of the **File to Import** window.
27. Click **Next**.
28. The **Certificate Store** window displays.
29. Select **Place all certificates in the following store** option.



30. Click **Next**.
31. The **Completing the Certificate Import Wizard** window displays.



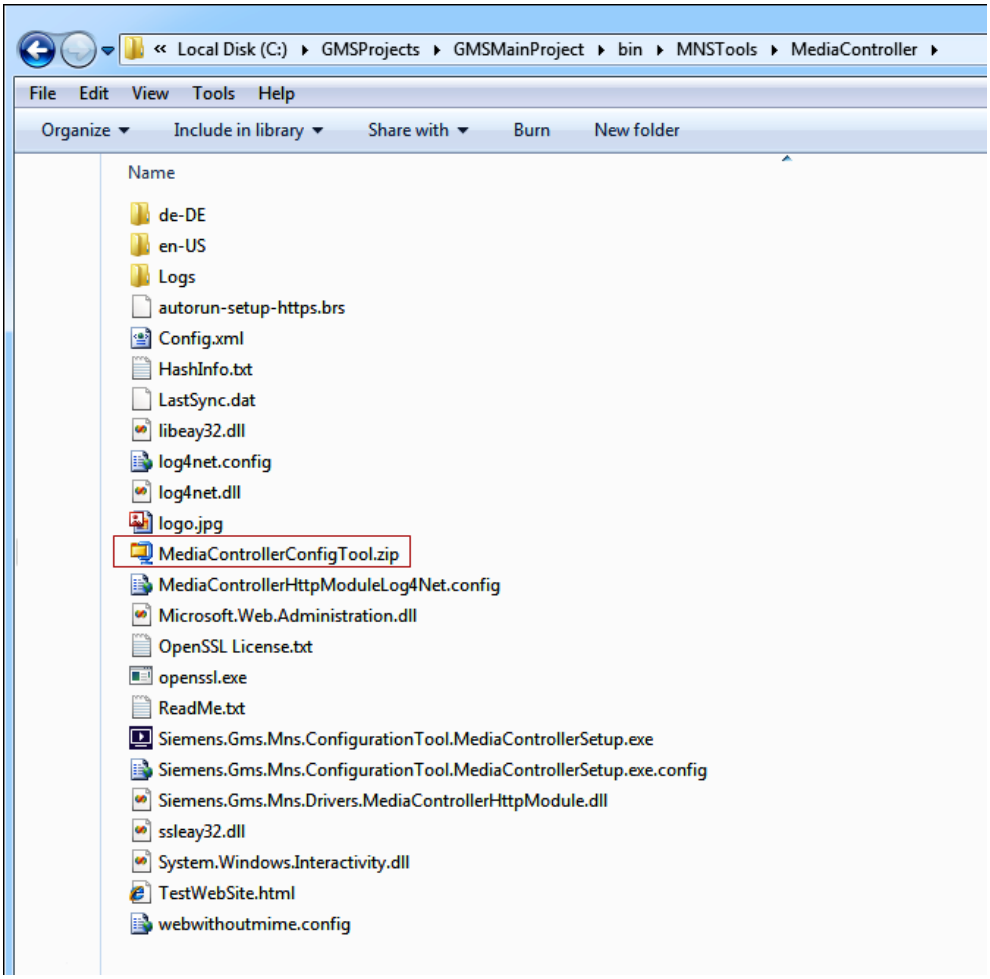
32. Click **Finish**.

⇨ Upon successful import of certificate, a message box displays.

33. Click **OK**.

⇨ The certificate import process for the **Intermediate Certification Authorities** is complete.

34. Select **(Installation Drive):** > **GMSProjects** > **GMSMainProject** > **bin** > **MNSTools** > **MediaController**.



35. Select **MediaControllerConfigTool.zip** file.
36. Copy the .zip file to the dedicated Web Server.
37. Extract the content of the .zip file in a desired location.
38. Right-click the **MediaControllerSetup.exe** and select the option **Run as administrator**.
39. For **Web Server Configuration**, select one of the following options:
    - For creating a new website, follow the steps mentioned in Creating a New Web Site section.
    - For selecting an existing website, follow the steps mentioned in Selecting an Existing Web Site section.
40. After the Web Server configuration, follow steps 3 to 9 of --- MISSING LINK --- section for **Device Configuration**.

Device Verification of Media Controller

To verify the device IP address when configured for DHCP, do the following:

1. After loading the setup files onto the SD card using the **Media Controller Setup** utility, insert the SD card into the BrightSign device and wait for five minutes.
2. After five minutes, remove power from the BrightSign device by unplugging the AC adapter from the device.
3. Remove the SD card from the device.
4. Insert the AC adapter back into the device.

5. When the device has booted up (approximately one to two minutes), the device model will display on the LCD along with the MAC address, IP address, and firmware version.
6. After verifying the IP address on the LCD, re-insert the SD card and reboot the device.

Additional Workflows

This section of the Media Controller Device explains the customization levels, preloading of content onto Media Controllers, network setting scenarios and automatic switching to emergency Notification.

Customization Levels

Basic system libraries (such as, **Headquarter > Global > Base**) are provided with the installation. Additional libraries can be imported, created or edited. How experts can work with libraries depends on the customization level that indicates what type of libraries authorized experts can customize (Headquarter, Zone, Region, or Project).

The customization level displays in the **Extended Operation** tab of the Contextual pane when selecting **System Settings** in the **Management View** of System Browser. The customization level is set to **Project** and cannot be changed.

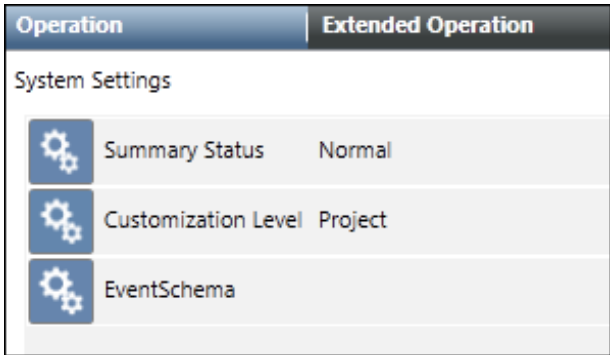


Fig. 36: Customization Level

NOTE:
If it is necessary to work with a customization level different from the **Project**, contact the Customer Support center that is authorized to modify this setting.

For the allowed customization level, authorized experts can do the following:

- Edit libraries according to the following schema.

Experts	Tasks
Headquarter experts	Edit libraries belonging to any level (**Headquarter**, **Zone**, **Region**, or **Project**)
Customer Support	
Zone librarians	Edit libraries belonging to the **Zone**, **Region**, or **Project** level only.
Region librarians	Edit libraries belonging to the **Region** or **Project** level only.
Project engineers	Edit libraries belonging to the **Project** level only.

- Customize libraries (create new libraries by cloning the structure of a library from a higher to a lower library level) to better meet the customer's needs, according to the following schema.

Customization Level	Task
Project	Customize **Headquarter**, **Zone**, or **Region** libraries under the Project level.

Region	Customize **Headquarter** or **Zone** libraries under the **Region** level.
Zone	Customize only **Headquarter** libraries under the **Zone** level.
Headquarter	N/A

Navigation Through Customized Libraries

By clicking any customized library-related item contained in the **Extended items** tab area of the Contextual pane, the Secondary pane opens next to the Primary pane where the **Library Configurator** displays the settings for the selected related item. This workflow can be helpful for example to compare libraries data across customizations. Customization of the library displayed in the Secondary pane is also possible.

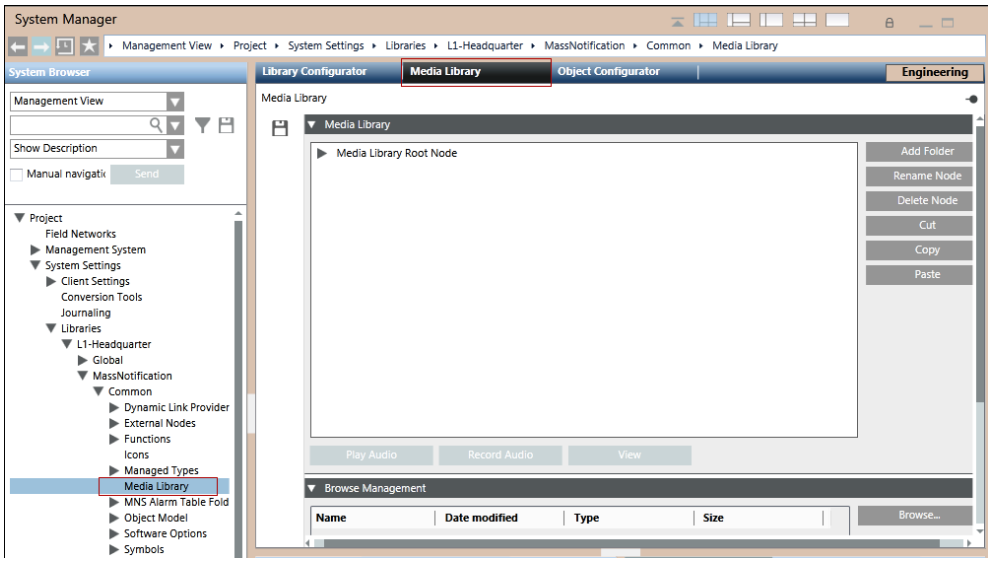
Preload

allows preloading of content onto Media Controllers. This scheduled activity copies large audio and multimedia content files onto the media controllers to guarantee timely playing of audio and multimedia messages on those devices, even when large files are involved.

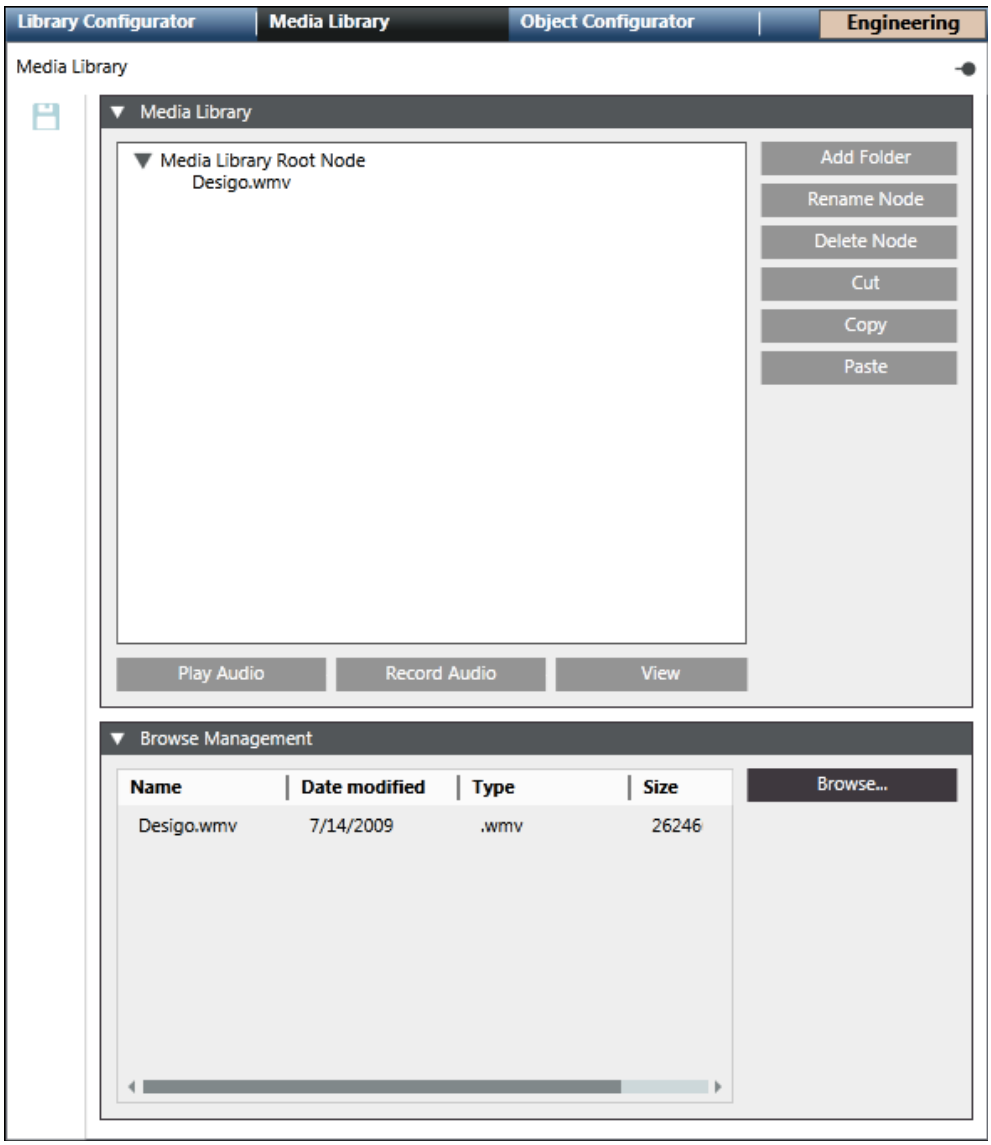
Preloading Content onto Media Controllers

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

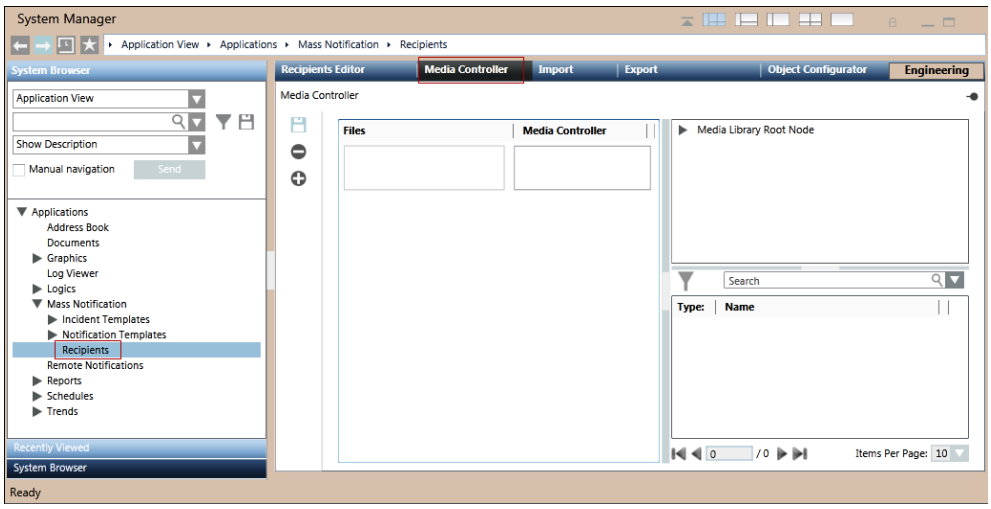
1. In System Browser, select **Management View**.
2. Select **Project** > **System Settings** > **Libraries** > **L1-Headquarter** > **Notification** > **Common** > **Media Library**.
3. Select the **Media Library** tab.



4. Seelct the **Browse Management** expander.
5. Click **Browse** and select the folder that contains the media content.
6. Drag and drop the media content from the **Browse Management** expander on to the **Media Library Root Node** of the **Media Library** expander.

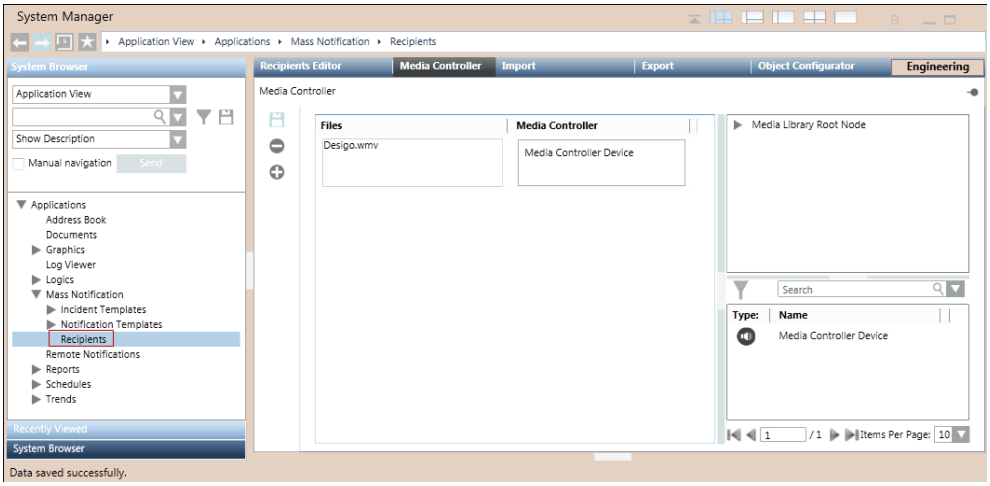


7. Select **Applications** > **Notification** > **Recipients**
8. Select the **Media Controller** tab.
9. Click **Add new item** to add preloaded content to a specific media controller device.



10. Drag and drop the media file on to the **Files** column.

11. Drag and drop the media controller device on to the **Media Controller** column.

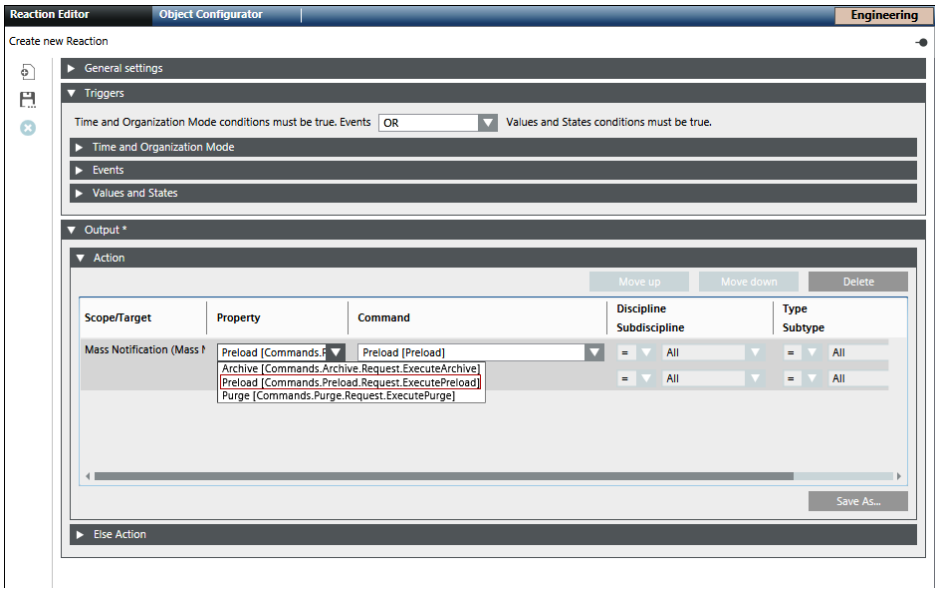


12. For preloading the media files using the **Preload** feature, do the following:
- **a.** Select **Applications** > **Notification**.
- **b.** Select the **Extended Operation** tab.
- **c.** Click **Preload**.

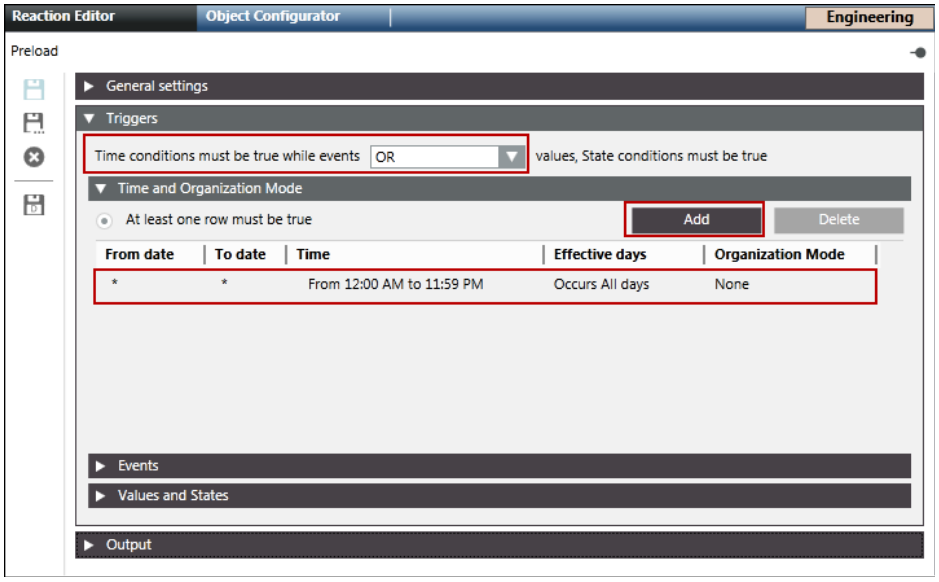
⇨ A message **Preload successful** displays if the content preload is successful.

13. For preloading the media files using the **Reaction** feature, do the following:
- **a.** Click the **Operation** button.
- **b.** Select **Applications** > **Logics** > **Reactions**.
- **c.** Drag and drop the **Notification** node on the **Action** expander under the **Output** expander of the **Reaction Editor** tab.
- **d.** Select **Preload [Commands.Preload.Request.ExecutePreload]** from the **Property** drop-down list.

14.



15. Open the **Triggers** expander. Do the following:
    a. Change the Time condition to **OR**.
    b. Open the **Time and Organization Mode** expander.
    c. Click **Add** to add a new time row and leave all values as default or enter a time or schedule that will periodically trigger the **MnsPreloadExecute** command.



16. Click **Save As** and name the reaction **Preload**. For more information on the **Reaction** feature, refer to the *Reaction* section.

Network Settings Scenarios

When configuring a secure, encrypted connection between a media controller device and the publishing web server it is critical that the **Issued to** field of the server certificate exactly matches the host name of the web server. The following scenarios describe three common types of network environments with regards to availability of DHCP and DNS services. Each scenario then describes how to configure media controller devices and the network to ensure proper communication and functioning.

Scenario #1:

The web server and media controller device reside on a network where they can make use of DHCP and DNS servers.

1. Configure the DHCP server reserve an IP address for the media controller device.
2. Configure the Field Network in as per the System Configuration (Field Network and Device) section.
3. Create the server certificate by using the web server's host name for the **Issued to** field.
4. Configure the media controller to acquire its IP address through DHCP and use the corresponding IP address to the web server's hostname in web server URLs.

Scenario #2:

The web server and media controller device reside on a private network or an VLAN with no access to DHCP and DNS servers.

1. Configure a Windows Server machine with DHCP and DNS server roles for the VLAN.
2. Configure the DHCP server reserve an IP address for the media controller device.
3. Configure the Field Network in as per the System Configuration (Field Network and Device) section.
4. Create the server certificate by using the web server's host name for the **Issued to** field.
5. Configure the media controller to acquire its IP address through DHCP and use the corresponding IP address to the web server's hostname in web server URLs.

Scenario #3:

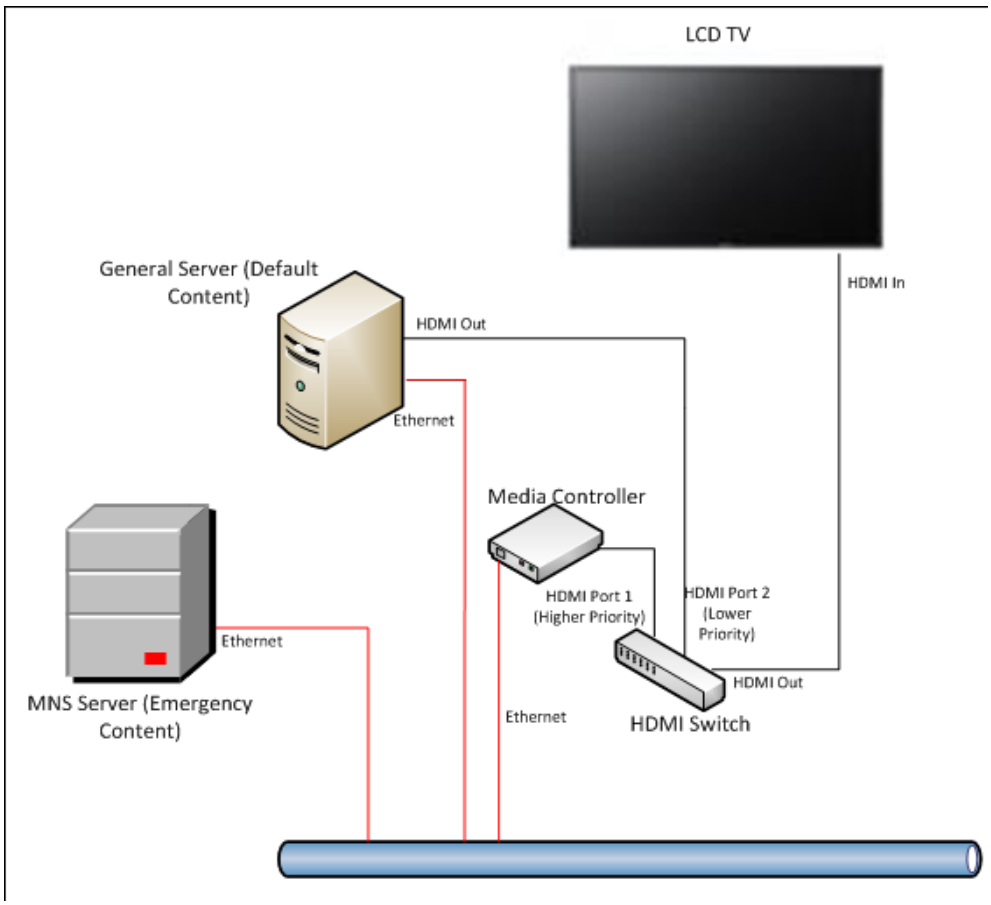
The web server and media controller device are not allowed to use a DHCP or DNS server, and running a local DHCP and DNS server is prohibited.

1. Create the server certificate by using the web server's IP address for the "Issued to" field.
2. Configure the Field Network in as per the System Configuration (Field Network and Device) section, except, use the IP addresses in place of the host names in device addresses and web server URLs.
3. Configure the media controller to acquire its IP address through DHCP and use the corresponding IP address to the web server's hostname in web server URLs.

Automatic Switching to Emergency Notification Content From the Default Content Using the HDMI Switch

There is a need from customers and organizations to use one LCD monitor to show default content in normal daily operations as well as MNS alert content in case of emergency situation. For example, the LCD monitor is configured to actively display current facility news updates, cafeteria menu, or presentations. When an emergency event occurs, the default contents displaying on the LCD monitor will be automatically interrupted and MNS alert content shall be displayed to notify and update building occupants about the situation. The default content restores when the emergency event has been cleared.

For this purpose, an HDMI switch with the ability to assign priority level to HDMI ports can be used. The switch must support HDMI channel prioritization. This means, for a 2-port HDMI switch, port 1 has the higher priority and port 2 has a lower priority. The following diagram shows a sample setup.

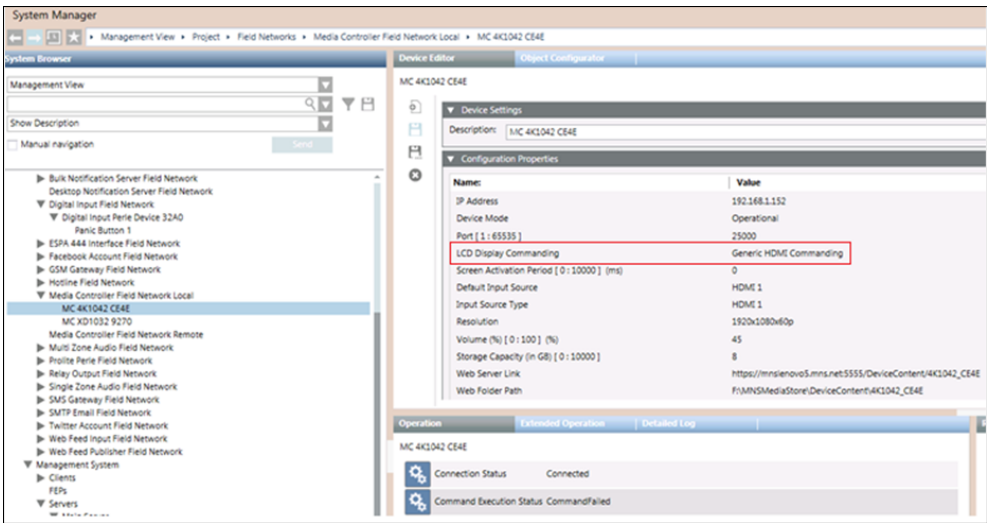


This set up has been tested with the following hardware:

- StartTech 2-port HDMI Auto Switch - 1080p VS221HDQ
- Media Controller - BrightSign 4K1042
- LCD TV - Samsung 400FP-3

Steps to configure to utilize the HDMI switch for automatic content switching:

1. To configure the StarTech 2-Port HDMI Switch VS221HDQ, do the following:
   a. EDID port selection switch - 1 (off)
   b. Mode selection switch - 3 (Priority Mode)
2. Connect the default content source output to HDMI Switch Port #2 (lower priority).
3. Connect the Media Controller output to HDMI Switch Port #1 (higher priority).
4. Connect the HDMI switch output to the LCD TV HDMI 1 input port.
5. Select System Manager, select the **Generic HDMI Commanding** option from the **LCD Display Commanding** field.



Use Case Example:

- Default content (for example, presentation) is playing on the LCD TV connected to port 2 of the HDMI switch.
- An Emergency Incident occurs at the facility. Incident is triggered and sent to the Media Controller connected to port 1 of the HDMI switch.
- The HDMI switches to port 1 after detecting the signal on it.
- The Emergency content displays on the LCD TV through Media Controller.
- The Emergency Incident is resolved, Incident is cancelled.
- The HDMI switch switches to port 2 after detecting the signal on port 1 is no longer present. Default content returns to play on the LCD TV.

Installing Media Controller

This section provides the user with information on mounting the hardware and connection details for the device.

Prerequisites

The following are the prerequisites for the Media Controller installation:

- BrightSign XD1033 with firmware version 6.2.94 or greater, or BrightSign 4K1042 with firmware version 5.0.22 or greater.
- RS232 communication cable (DB9 female controller end).
  NOTE: Check the LCD model to determine whether the cable is straight through or null modem type and whether the serial port requires a female or male end.

Display Model	Connector on Monitor	Serial Cable for Commanding	Connector on Media Controller
Sharp PNE421	DB9-M (Input Port)	F----------F (Straight Through)	DB9-M
Sharp LC42D69U	DB9-M	F----------F (Null Modem)	
Samsung LC-400FP3	DB9-M (Input Port)	F----------F (Null Modem)	
Samsung ED46D	Stereo 3.5 mm Jack	M----------F (TRS Connector)	

The following serial cable part numbers can be ordered from Siemens SAP:

52038 - Female to Female Null Modem Cable

52035 - Female to Female Straight Through Cable

52030 - Female to Male Straight Through Cable

52184 - Female to Male Null Modem Cable

- AC Power adapter (bundled with media controller)
- Cat5e Ethernet Cable
- HDMI Cable compatible with HDMI 1.3a or higher devices (bundled with media controller)
- SD/SDHC flash card, class 4 or higher, 4GB or higher, with only FAT32 (File Allocation Table) file system
- HTTPS website to host content for the media controller devices. The website should be configured to ignore client certificates. Only the Certificate Authority (CA) certificate is used for security.
  - The website can be an external Web Server hosted by the customer or third party. In this scenario, a web folder from the website needs to be accessible to the server either as a mapped driver or a network shared folder.
  - The website can be hosted on the system server along with .
  - For instructions on how to create a HTTPS website using Media Controller Setup utility and incorporating the CA certificate, refer to the --- MISSING LINK --- section.

Disclaimer:
Prior to commissioning of system, a compatibility check should be performed for all devices and services to be integrated (refer to the *System Description* document for compatibility information).

Mechanical Installation

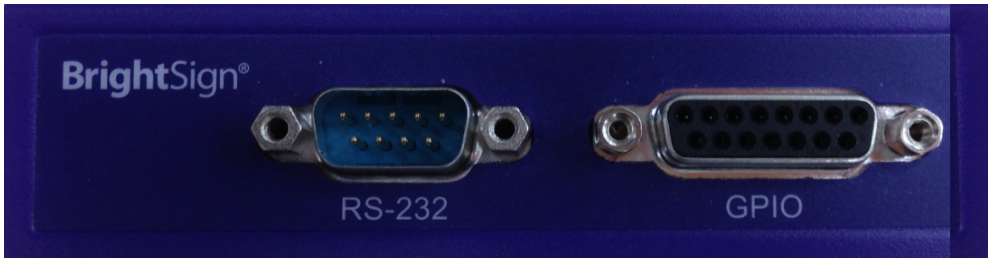
For Wall Mounting, the housing of the BrightSign device has flanges on the side with slot cutouts for mounting. Using screws fasten the BrightSign device to a wall or flat surface using the flanges.

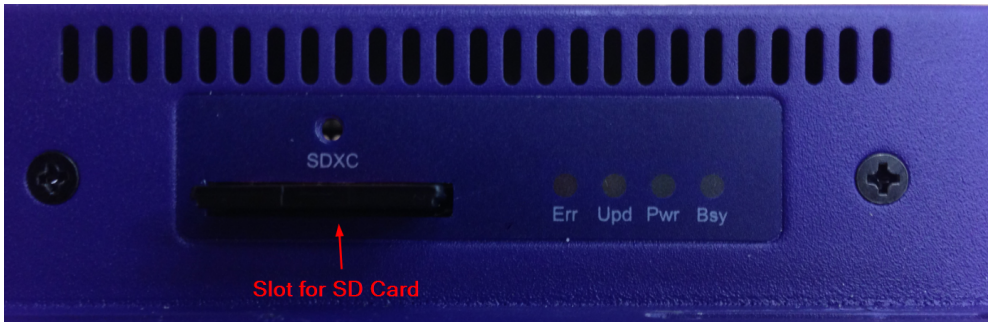
NOTE:
Users must supply their own screws to fasten the bracket to the wall. Use an appropriate screw type for the wall type (concrete, wood, dry wall and so on).

For VESA Mounting, using the VESA mounting kit offered by the distributor *Insight Direct*, mount the BrightSign device to the backside of the flat panel display using the instructions included with the mounting kit.

Electrical Installation

Use the following images of the BrightSign device as a reference:





- Connect the HDMI cable to the HDMI port on both the flat panel display and BrightSign device. Refer to the TV manufacturer's operation manual to locate the HDMI port on the flat panel display.
- If the flat panel display supports control commands through a RS232 port, connect the RS-232 serial cable to the RS-232 port on both the flat panel display and BrightSign device. Refer to the TV manufacturer's operation manual to locate the RS232 port on the flat panel display.
  NOTE: Check with the flat panel display manufacturers to determine what type of RS232 serial cable is required. The following table lists the serial cables required for some device models:

Display Model	Connector on Monitor	Serial Cable for Commanding	Connector on Media Controller
Sharp PNE421	DB9-M (Input Port)	F----------F (Straight Through)	DB9-M
Sharp LC42D69U	DB9-M	F----------F (Null Modem)	
Samsung LC-400FP3	DB9-M (Input Port)	F----------F (Null Modem)	
Samsung ED46D	Stereo 3.5 mm Jack	M----------F (TRS Connector)	

- Insert the SD card, loaded with the configuration files and script, into the SD card slot of the BrightSign device. See the --- MISSING LINK --- section for details on loading the configuration file.
- Connect the power adapter to the power connector on the BrightSign device. When supplied with power, the media immediately turns on and begins the boot-up process. The boot-up process may take up to five minutes depending on configuration.

Installation Verification

1. If installed properly, the **Pwr** LED should be lit on the BrightSign device.
2. Verify the input selection for the flat panel display is set for **HDMI**.

Media Controller Device Troubleshooting

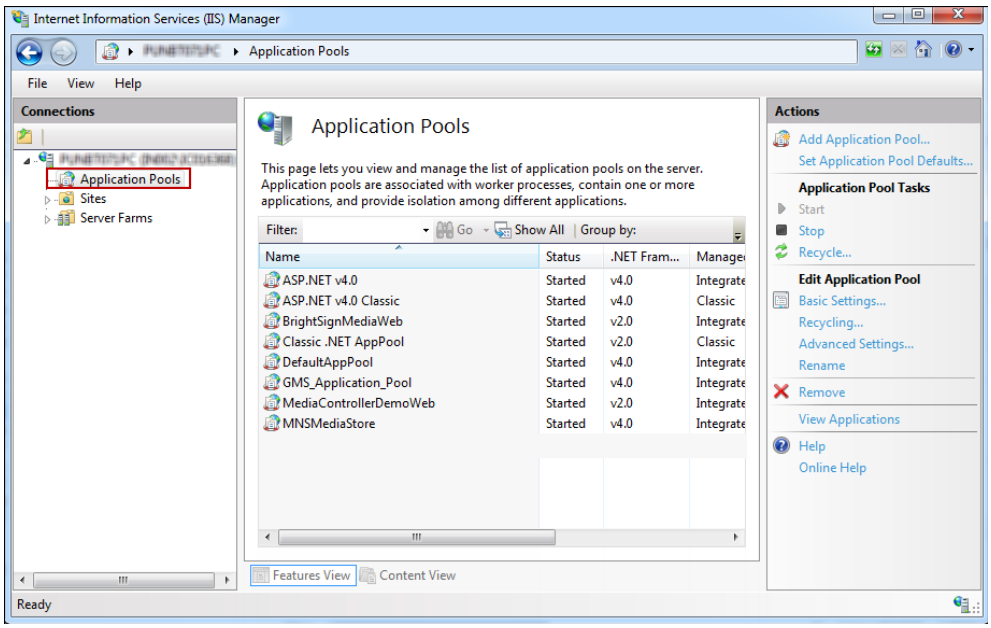
This section provides solutions to some common problems, the user may encounter during Media Controller device configuration.

Media Controller Web Site Displays Service Unavailable Error

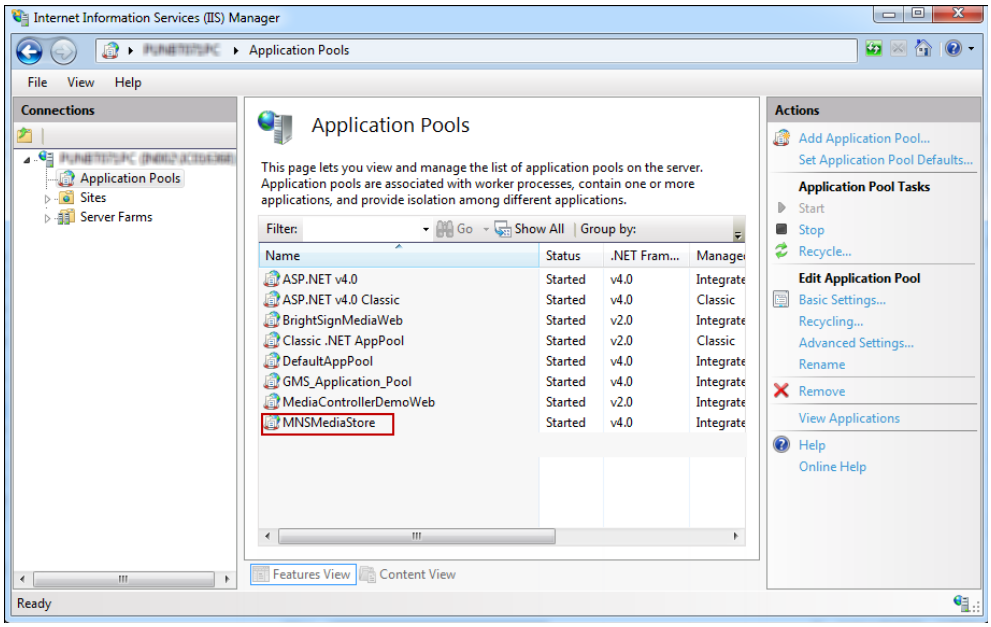
Problem: While browsing the Web site created through **Media Controller Setup** utility, if the **Service Unavailable** error is displayed.

Solution: Perform the following steps to rectify the corresponding error:

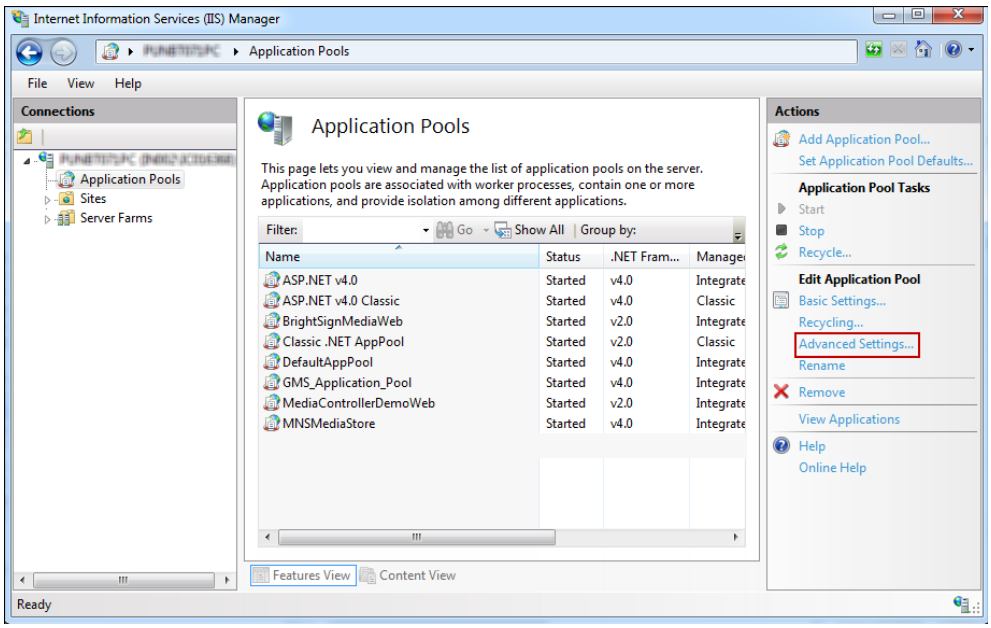
1. From the Windows **Start** menu, type **inetmgr** and press **ENTER**.
   ⇨ The Internet Information Services (IIS) Manager window displays.
2. Select **Application Pools**.



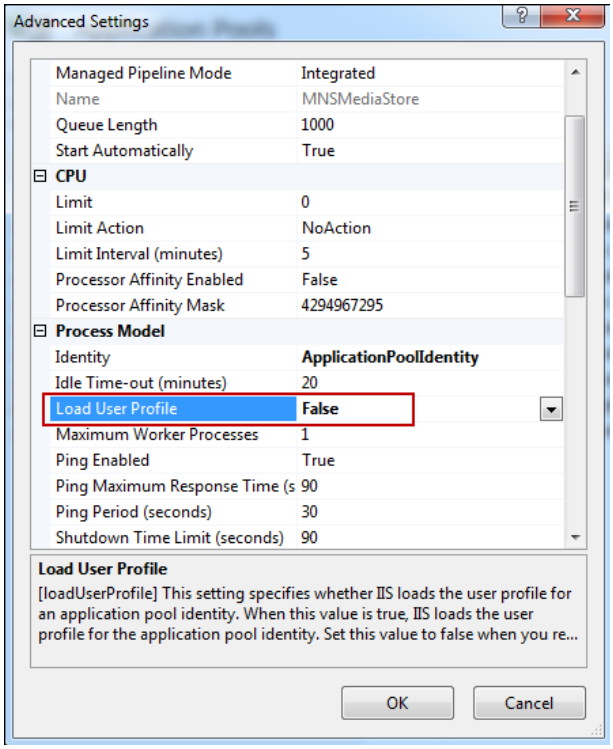
3. Select the Web site from the Application Pools list.



4. Right-click the created Web site and select the **Advanced Settings** option or click **Advanced Settings** under **Edit Application Pool** section.



➪ The **Advanced Settings** dialog box displays.



5. Select **Process Model**, verify that the value specified in the **Load User Profile** field must be **False**. If not, select **False** from the drop-down list.
6. Click **OK**.
7. Right-click the **Application Pools** node and select the **Refresh** option.

Compatibility Issue With New Media Controller Firmware Version 6.0.51

Problem: Version 4.2 supports Bright Sign Media controller models XD1033, and 4K1042. These devices are now shipped from the manufacturer with firmware version 8.0.48. The following issues have been observed on media controller models XD1033 with firmware version 8.0.48:

- It takes approximately 5 minutes to get the device into **Connected** state after the initial configuration.
- It takes approximately 4 minutes for the first launch of 80 MB non preloaded multimedia file. Subsequent delivery times for the same multimedia content are shorter (15-20 seconds).
- Sporadically, the device connection status becomes disconnected in window. However, message Launch / Suspend / Resume / Cancel / Expire operations will succeed.

Solution: For resolving these issues, downgrade to the corresponding tested firmware version. The listed tested firmware can be requested directly from Bright Sign support site.

Apart from the listed models, the firmware version 6.0.51 is not tested on other media controller models

Volume Issue on LCD Device in Standby Mode

Problem: When the following two conditions are met on sending a message to a LCD device, the device volume does not follow the volume level configured in :

- **Condition 1** - LCD device is in standby mode
- **Condition 2** - Media controller device is configured with any device specific commanding for LCD Display Commanding setting under device configuration properties in

Solution: If the Standby mode is required for a LCD device, ensure that the LCD device's volume is audible and verified.

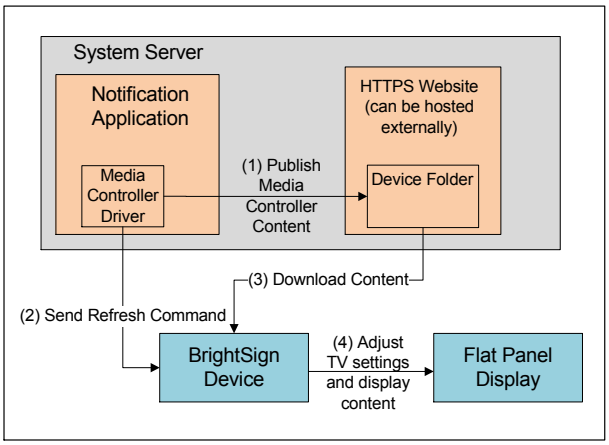
Command Execution Status Issue For Media Controller Devices

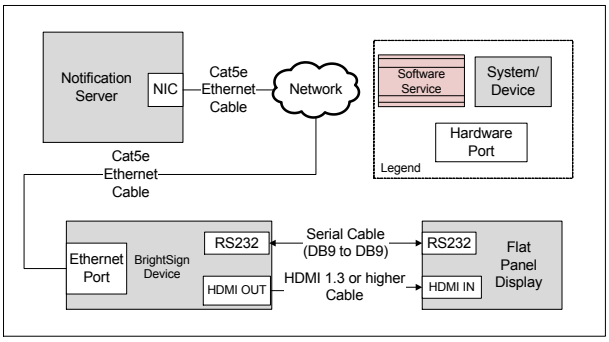
In some tests, it is observed that the Command Execution Status seen on the device configuration screen in the **Operation** tab shows failed whereas the actual message delivery succeeds, and is shown as `Delivered` in the **Browse** screen.

Media Controller Device

This section contains general reference information about Notification and how the Media Controller device is integrated. For procedures and workflows, see step-by-step section.

has the capability to publish multimedia content, part of the notification, which will then be displayed on a flat panel display by the BrightSign device. The BrightSign device is a media controller that handles the actual presentation and content on the flat panel display.





The BrightSign Media Controller supports the following file formats.

- **Audio Files**
  - AAC (LC - Low complexity profile) at a Constant Bit Rate, as part of a video file (.mp4, .mov, or .ts) at 44.1 KHz, 48 KHz
  - MP2 (MPEG-1 Layer 2) at a Constant Bit Rate, as part of a video file (.mpg or .ts) at 44.1 KHz, 48 KHz
  - MP3 at a Constant Bit Rate (44.1 KHz, 48 KHz, or 32 KHz at up to a bit rate of 224 Kbps) as a standalone file (not encoded as an audio track in a video file)
  - AC3 5.1 passed through (un-decoded, RAW data) HDMI. Audio streams in this format are supported by BrightSign players, but will require an AC3 decoder (HDMI AV receiver)
  - WAV
- **Video Files**
  - MPEG-2 - Can be saved as an .mpg, .ts, .m2ts or .vob container.
  - MPEG-1 - Can be saved as an .mpg container.
  - (4K models only) H.265 (HEVC) - Can be saved as a .ts, .mov, or .mkv container
  - H.264 (MPEG-4, Part 10) - Can be saved as a .mp4, .mov, or .ts container
  - WMV - .wmv video only files (.wma audio files are not supported). Support includes videos exported from PowerPoint

NOTE: The .mov files with compressed **atoms** (metadata) are not currently supported.

- **Image Files**
  - JPG
  - BMP
  - PNG

The maximum supported resolution is 1920x1080.

NOTE: BrightSign players do not support JPG image files with CMYK color profiles.

The following figure provides an overview of how the content is displayed.

1. A notification message with content is sent to the media controller. The media controller publishes that content onto a web folder on a HTTPS website.
2. The media controller driver instance sends a refresh command over Ethernet to the media controller.
3. The media controller receives this refresh command and immediately goes to the HTTPS folder and downloads all content. Additionally, the media controller is configured to poll the website for new content.
4. Based on the content, the media controller will do any necessary serial control on the flat panel display and display the content published by .

There will be different delays after the message is sent and before the content plays on the device for the following cases:

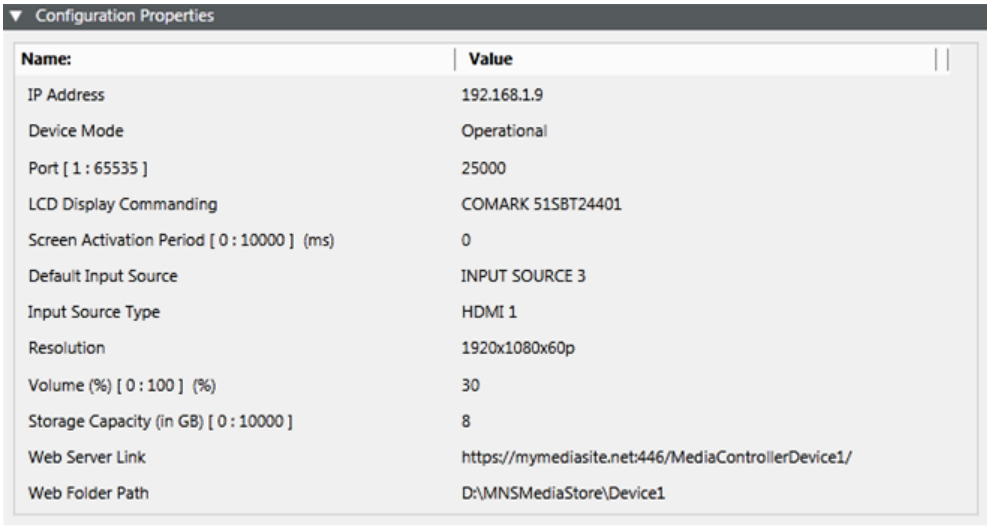
- Freshly configured Secure Digital (SD) card
- Device has previously played a media file but no preload is used
- Preload feature is used

also allows preloading of content onto Media Controllers. This scheduled activity copies large audio and multimedia content files onto the media controllers to guarantee timely playing of audio and multimedia messages on those devices, even when large files are involved.

The following specific models of Media Controller devices are supported by :

- BrightSign® XD1030
- BrightSign® XD1032
- BrightSign® 4K1042

Configuration Properties for Media Controller Device



- **IP Address**: Enter the hostname or IP address of the device. This field is editable.
- **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 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 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.
- **Port**: Enter the port number used to send UDP commands to the media controller.
  UDP commands are used by to trigger immediate downloads by the media controller.
- **LCD Display Commanding**: Select the display type (brand and model) connected to the media controller from the drop-down list.
  No Commanding: The media controller does not send any commands to the LCD display.
  Generic HDMI Commanding: The media controller will turn off its HDMI signal when no message is active. If an LCD display with automatic stand-by mode is directly connected to the media controller, the display will switch into stand-by mode. This option may also be used with a two-port HDMI switch device between the controller and the display, in order to switch between an alternative, non-emergency HDMI input and MNS content. This option cannot control volume on the display.
  All other display models: The media controller will switch between default input and media controller input as well as control the volume via the RS232 connection.
  NOTE: The Samsung models **ED32D**, **ED40D**, **ED55D**, **ED65D** and **ED75D** are also compatible with . Select the **Samsung ED46D** drop-down option in the **LCD Display Commanding** field to use the above models.

- **Window Activation Period**: Specify a period that the media controller will delay playing a new message when no message was active before. Use this setting in combination with **Generic HDMI Commanding** in order to give the display enough time to power up from power-save mode so that the beginning of new messages, for example, a video does not get cut off.
- Default Input Source: Select the default input source that is the standard input of the device. For example, Camera.
- Input Source Types: Select the input source on the display from the drop-down menu. supports connections through HDMI only. LCD displays typically contain multiple HDMI ports and the port numbers are labeled accordingly. When this is set, the system automatically changes the input source on the display at the start of the presentation.
- **Resolution**: Select the value for the flat panel display. Recommended value is 1920x1080x60 pixels.
- **Volume (%)**: Enter the percentage value between 1 and 100 for the volume to be used when the presentation displays.
- **Storage Capacity**: Enter the storage capacity in Gigabytes (GB) of the SD card on the media controller.
- **Web Server Link**: Enter the Device URL from the **Device URL** field of the **Media Controller Setup** utility. Refer to the Mass Notification Server section for more information.
- **Web Folder Path**: Enter the folder path where presentations and media content to be displayed by the media controller device are published. This folder's name is mentioned in the **Device URL** field of the **Media Controller Setup** utility. For example, in the **Device URL**, **https://mymediasite.net:447/DeviceContent/MediaControllerDevice**, the name of the folder is **MediaControllerDevice**. The folder path to be entered can be the full path to a folder on the local machine or a network share folder.
  For example: **D:\MNSMediaStore\DeviceContent\MediaControllerDevice or \\MNSMediaStore\DeviceContent\MediaControllerDevice**.
  NOTE 1: This can be the full path to a folder on the local machine or a network share folder.
  NOTE 2: A network share folder must be accessible to . Each device must have its own specific folder where can publish device-specific content. Unlike the common folder, uses this location to publish content such as RS232 commands and presentation format that are device-specific.

Default Input Source

The following table lists the mapping of Default Input Sources and the available drop-down options.

For example, if **Samsung 400FP3** Multimedia Device Type is selected and the user wants to select **HDMI 1** as a Default Input Source. For this case, **HDMI 1** must be selected in the drop-down list. Similarly, if **DVI** needs to be selected as a Default Input Source, select **Input Source 1** in the drop-down list.

Multimedia Device Type	Default Input Source	Drop-down option for Default Input Source
Samsung 400FP3	HDMI 1	HDMI 1
	HDMI 2	HDMI 2
	DVI	Input Source 1
	VGA	Input Source 2
Samsung ED46D	HDMI	HDMI 1
	DVI	Input Source 1
	VGA	Input Source 2
	Component	Input Source 3

LG 42LD450	HDMI 1	HDMI 1
	HDMI 2	HDMI 2
	HDMI 3	HDMI 3
	HDMI 4	HDMI 4
	Component	Input Source 1
	DTV (Antenna)	Input Source 2
	Analog (Antenna	Input Source 3
	Analog (Cable)	Input Source 4
	AV 1	Input Source 5
	AV 2	Input Source 6
	RGB-PC	Input Source 7
Sharp PNE421	AV HDMI	HDMI 1
	PC D-SUB	Input Source 1
	PC HDMI	Input Source 2
Sharp LC42D69U	HDMI 1	HDMI 1
	HDMI 2	HDMI 2
	HDMI 3	HDMI 3
	HDMI 4	HDMI 4
	Component 1	Input Source 1
	Component 2	Input Source 2
	AV	Input Source 3
Sharp LC80LE632U	HDMI 1	HDMI 1
	HDMI 2	HDMI 2
	HDMI 3	HDMI 3
	HDMI 4	HDMI 4
	TV	Input Source 1
	Component	Input Source 2
	Video 1	Input Source 3
	Video 2	Input Source 4
Sharp LC70LE640U	HDMI 1	HDMI 1
	HDMI 2	HDMI 2
	HDMI 3	HDMI 3
	HDMI 4	HDMI 4
	TV	Input Source 1
	Component	Input Source 2
	Video 1	Input Source 3
	Video 2	Input Source 4
	PC	Input Source 5

Sharp LC46E77UN	HDMI 1	HDMI 1
	HDMI 2	HDMI 2
	HDMI 3	HDMI 3
	HDMI 4	HDMI 4
	HDMI 5	HDMI 5
	Component 1	Input Source 1
	Component 2	Input Source 2
	AV	Input Source 3
	PC	Input Source 4

For example, if **Samsung 400FP3** is selected as a display device (having maximum HDMI input source value of HDMI 2 and maximum input source value of Input Source 2). In **Input Source Type** field, if the user selects **HDMI 5** option, in this case, the system by default selects **HDMI 2** as the maximum value since **HDMI 5** option is not available for **Samsung 400FP3**.

Depending on the value selected in the **Default Source Type** field, the system selects the maximum value.

- If the user selects **HDMI 5** option, in this case, the system by default selects **HDMI 2** as the maximum value since **HDMI 5** option is not available for **Samsung 400FP3**.
- If the user selects **Input Source 4** option, but the maximum available option is **Input Source 2**; the system by default selects **Input Source 2** as the maximum value since **Input Source 4** option is not available for **Samsung 400FP3**.
- If no option is selected, the system by default selects **HDMI 2** as the maximum value.

Input Source Types

The following table lists the mapping of Input Source type and the available drop-down options.

For example, if **Comark 51SBT24401** Multimedia Device Type is selected and the user wants to select **HDMI** as an Input Source Type. For this case **HDMI 1** must be selected in the drop-down list. Similarly, if **Sharp PNE421** Multimedia Device Type is selected and the user wants to select **AV HDMI** as a Default Input Source. For this case, **HDMI 1** must be selected in the drop-down list.

For example, if **Samsung 400FP3** Multimedia Device Type is selected and the user wants to select **HDMI 1** as an Input Source Type. For this case **HDMI 1** must be selected in the drop-down list. Similarly, if **Sharp PNE421** Multimedia Device Type is selected and the user wants to select **AV HDMI** as a Default Input Source. For this case, **HDMI 1** must be selected in the drop-down list.

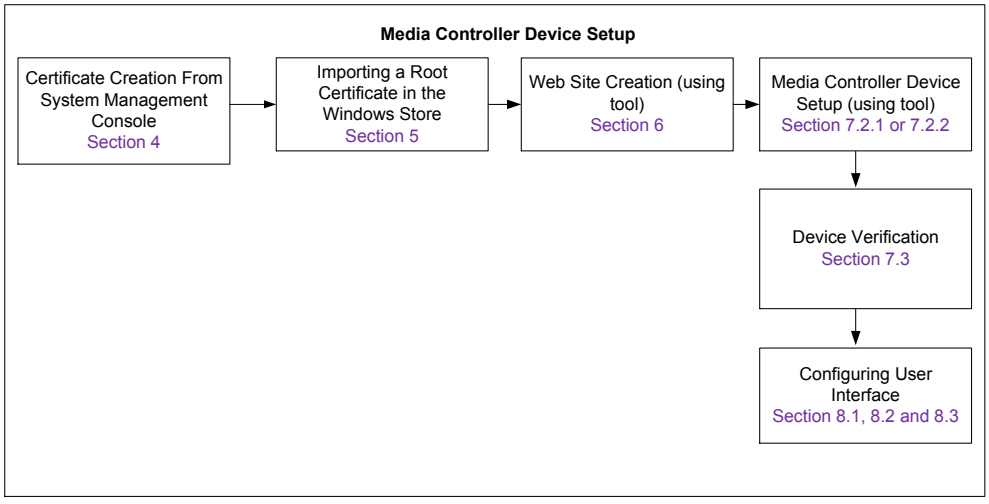
Multimedia Device Type	Input Source Type	Drop-down option for Input Source Type
Samsung 400FP3	HDMI 1	HDMI 1
	HDMI 2	HDMI 2
Samsung ED46D	HDMI	HDMI 1
LG 42LD450	HDMI 1	HDMI 1
	HDMI 2	HDMI 2
	HDMI 3	HDMI 3
	HDMI 4	HDMI 4
Sharp PNE421	AV HDMI	HDMI 1

Sharp LC42D69U	HDMI 1	HDMI 1
	HDMI 2	HDMI 2
	HDMI 3	HDMI 3
	HDMI 4	HDMI 4
Sharp LC80LE632U	HDMI 1	HDMI 1
	HDMI 2	HDMI 2
	HDMI 3	HDMI 3
	HDMI 4	HDMI 4
Sharp LC70LE640U	HDMI1	HDMI 1
	HDMI 2	HDMI 2
	HDMI 3	HDMI 3
	HDMI 4	HDMI 4
Sharp LC46E77UN	HDMI 1	HDMI 1
	HDMI 2	HDMI 2
	HDMI 3	HDMI 3
	HDMI 4	HDMI 4
	HDMI 5	HDMI 5

In the **Input Source Type** field, if the user selects any available option that is not compatible with the display device; the system automatically selects the maximum available value.

For example, if **Samsung 400FP3** is selected as a display device (having maximum input source value HDMI 2). In **Input Source Type** field, if the user selects **HDMI 5** option, in this case, the system by default selects **HDMI 2** as the maximum value since **HDMI 5** option is not available for **Samsung 400FP3**.

Media Controller Device Set Up Flow Diagram



1.24 Multi Zone Audio Device

Multi Zone Audio Device

This section provides reference and background information for integrating the Multi Zone Audio device. For procedures or workflows, see the step-by-step section.

The multi zone audio interface allows the user to assign multiple relays to a common audio source. Each relay can correspond to an individual audio zone. For example, a practical deployment would be a site that has four audio zones. If the user wishes to control four zones independently with the same audio source, then multi zone would be require.

The Multi Zone Driver utilizes the following devices to deliver audio and to activate the audio circuits.

- **Line Level Audio Device (LLA) (Barix Annuncicom 200 and CyberData SIP Adapter)**

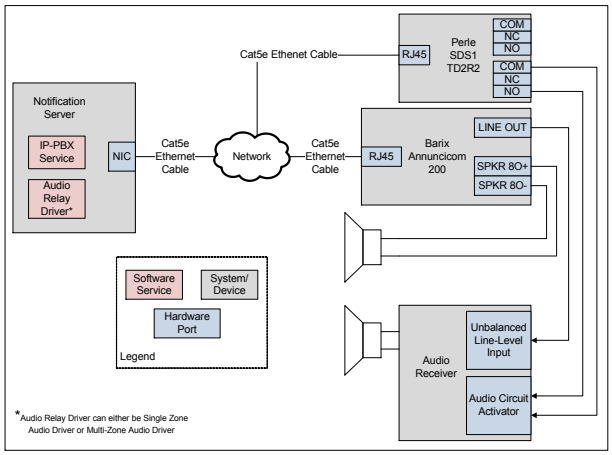
The Line Level Audio device (LLA), integrates with through an IP-PBX service using the SIP protocol over TCP/IP. The LLA converts the SIP audio session into a line-level audio signal. This signal can be used as an external input source for any generic audio receiver that meets the requirements of the LLA.

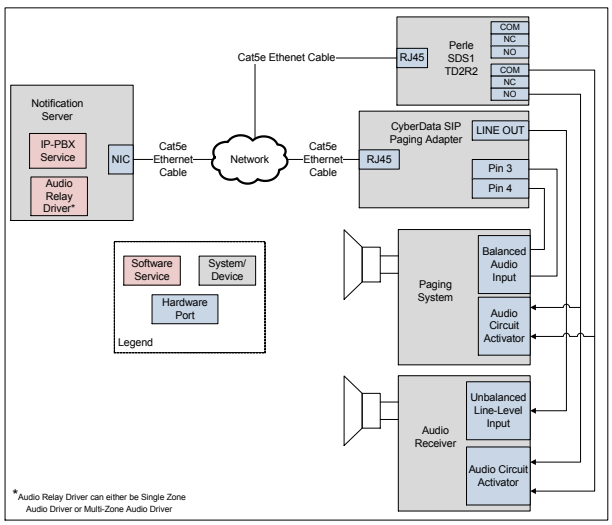
For details on wiring and the LLA output specifications for Barix Annuncicom 200, refer to the Audio Output section.

For details on wiring and the LLA output specifications for CyberData SIP Adapter, refer to the Audio Output section.

- **IP Relay (Perle IOLAN SDS1 TD2R2)**

The Perle SDS1 TD2R2 provides relays for contact closing. Prior to sending audio, the appropriate relay on the TD2R2 will be activated providing a closed relay contact. External audio receivers are expected to recognize this change and perform the steps required to allow audio to pass through and be amplified.





provides the following additional features when playing audio messages through Single and Multi-Zone Audio drivers:

- **Repetitions and intervals**: will repeatedly play the audio content of messages on the targeted audio devices, up to the number of repetitions configured in the audio content, and spaced out as specified through the configured interval.
- **Synchronized playing**: When the audio content of a single message needs to be played on multiple audio devices, ensures that the played audio content is synchronized across all devices. Listeners will then hear the resulting output as if the sound was coming from a single speaker.

NOTE 1:
The capability to play audio content in a highly synchronized fashion on multiple SIP-based audio devices can only be guaranteed for devices from the same manufacturer and possibly the same series or model. The audio content played on devices from different manufacturers might result in a slight but noticeable lag in the output heard by listeners. This can be due to the differences in device-internal processing speed of the participating devices.
NOTE 2:
During a live announcement or audio messaging, if any SIP-based audio device gets disconnected due to connectivity issues, system makes three attempts to rejoin the SIP-based audio device.

When multiple messages are active and share some or all of the targeted audio devices, will suppress playing audio content of messages with lower priority based on the priority tolerance rules.

Multi Zone Audio Device

This section provides additional procedures for integrating the Multi Zone Audio device.

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

Installing Multi Zone Audio

Line Level Audio Device

Barix Annuncicom 200

Hardware Prerequisites

Before proceeding, ensure that the following items are available:

- Barix Annuncicom 200 Line Level Audio device
- 9-30 VDC or 12-24 VAC, 500mA minimum
- Category 5 Ethernet cable

Power

Power to the device can either be supplied by the barrel connector or the terminal block labeled as PWR (refer image below), but not both. Both inputs are internally connected, so one can be used as an output for other devices.

Pin 1 of the terminal connector is ground. Pin 2 is power.
NOTE: For Barix Annuncicom 200 LLA, Power over Ethernet (PoE) is also an option for supplying power to the device.

Ethernet

1. Plug one end of the Ethernet cable into the RJ45 jack on the LLA.
2. Connect the other end of the Ethernet cable to the network jack.
   NOTE:
   The LLA obtains an IP address using DHCP by default. To assign a static IP address or if DHCP is not present, refer to the *Obtaining an IP Address Manually* section and the *Changing the IP Address* section.

Audio Output

An audio receiver is a device that amplifies an external analog audio signal and distributes that signal to one or more speakers. Examples are an audio/video receiver, a voice-enabled fire panel system, a radio-base station, and an intercom/public announcement system.

There are two methods to supply audio from the LLA:

Method 1: Use the LINE-OUT RCA socket.
NOTE 1: The tip of the RCA plug is a signal.
NOTE 2: The Line Out has 50Ω output impedance with a range of 1-3 Vp-p

Cable requirements are as follows:

1. >= 22 awg shielded, stranded cable wire
2. < 6ft length

Method 2: Use the “SPKR +” and “SPKR –“ terminals on the LLA.
NOTE: This interface can deliver 1 Watt into an 8Ω load.

Cable requirements are as follows:

1. >= 22 awg shielded, stranded cable wire
2. < 6ft length
3. Twisted wire pair

NOTE:
Refer to the Diagram 1 in the Device Overview section for an illustration regarding how the various components are connected for Barix Annuncicom 200 with Perle

device. Refer to the Diagram 2 in the Device Overview section for an illustration regarding how the various components are connected for Barix Annuncicom 200 without Perle device.

Hardware Verification

After completing the mechanical and electrical installations, verify the status LED is solid green color. If not, do the following outlined in the following sections:

- Obtaining an IP Address Manually
- Upgrading the LLA Firmware
- Changing the IP Address
- Configuring the SIP Endpoint

Obtaining an IP Address Manually

The Barix Annuncicom 200 device is configured for DHCP. If the device is unable to obtain an IP address, do the following to assign a temporary IP address:

1. Either use a network cable to link the Barix Annuncicom 200 device and the computer directly, or connect the Barix Annuncicom 200 device to the computer through the network switch and power the device.
   NOTE: Ensure that there is a valid static IP address configured. For example, a computer having subnet mask as 192.168.0.0 can have a static IP as 192.168.0.2.
2. Open the Windows Command prompt (cmd.exe).
3. Use the **Ping** command to ensure the usage of a free IP address (one not already used by another device in the network).
   NOTE: For example, if the computer has the IP address 192.168.0.2, and there is a need to check if 192.168.0.6 is free. Type Ping 192.168.0.6. If there is no reply, then it means that 192.168.0.6 is available.
4. Look for the Barix Annuncicom 200's MAC address printed on a label on the bottom of the device (12 hex digits, separated by a hyphen every 2 digits). For example, if the MAC address is 00-08-E1-00-B1-77, type in the following in the Windows command prompt: **arp -s 192.168.0.6 00-08-E1-00-B1-77.**
5. Enter the command window **telnet 192.168.0.6 1** to make the Barix Annuncicom 200 listen to the IP address **192.168.0.6**.

   NOTE: The Barix Annuncicom 200 will immediately refuse the connection on port 1, but will be available for browser access as long as the device stays powered on.
6. To check if the Barix Annuncicom 200 is responding, use the Ping command again. Type **Ping 192.168.0.6**. If there is no reply, the IP address **192.168.0.6** can access the Barix Annuncicom 200 using a web browser. If the device is unreachable through the **Ping** command, refer to the manufacturer's manual for additional methods.

Upgrading LLA Firmware

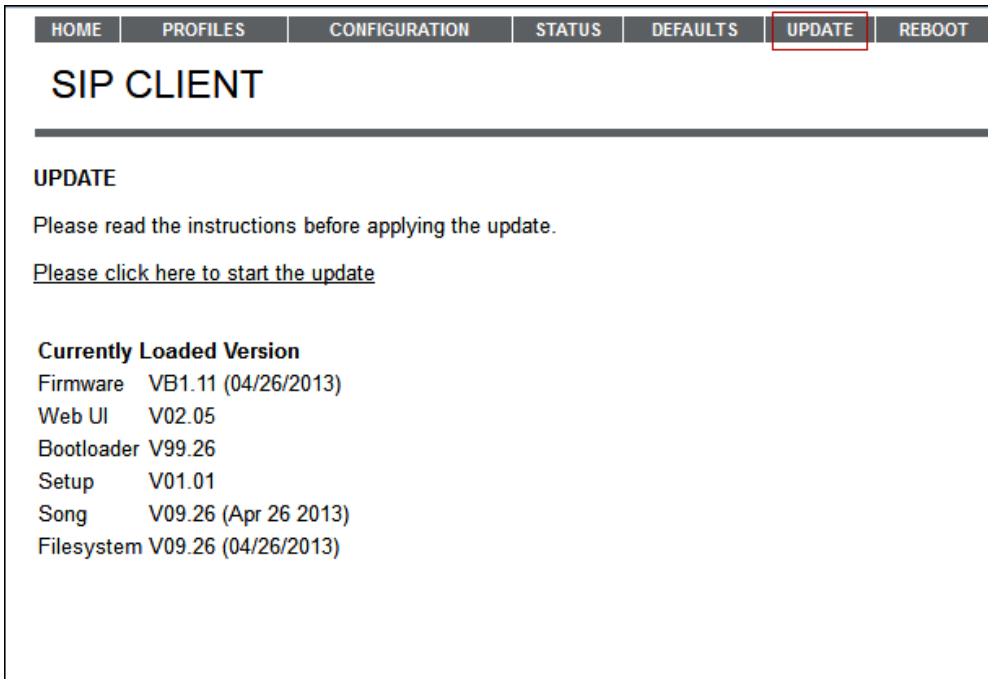
The latest SIP firmware can be found on the Barix website:

http://www.barix.com/downloads/downloads-firmware/sip-client-application/

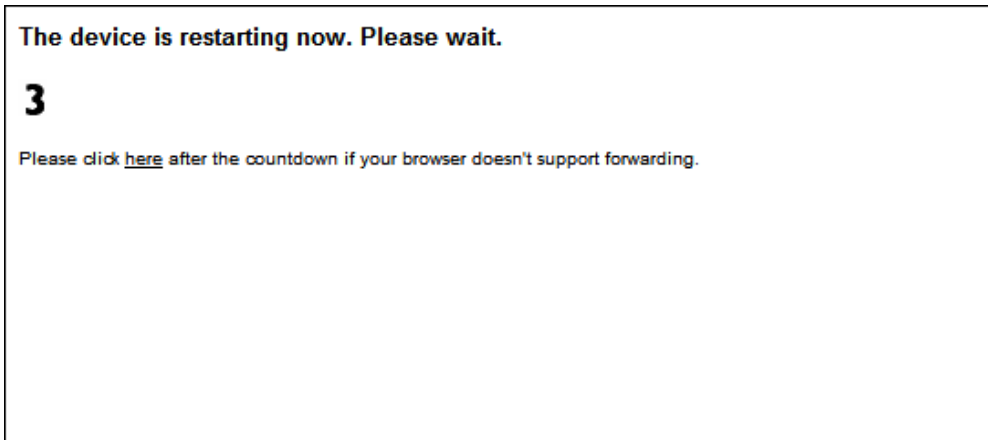
This document has been tested with firmware version 2.12.

Disclaimer:
Prior to the commissioning of a 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.

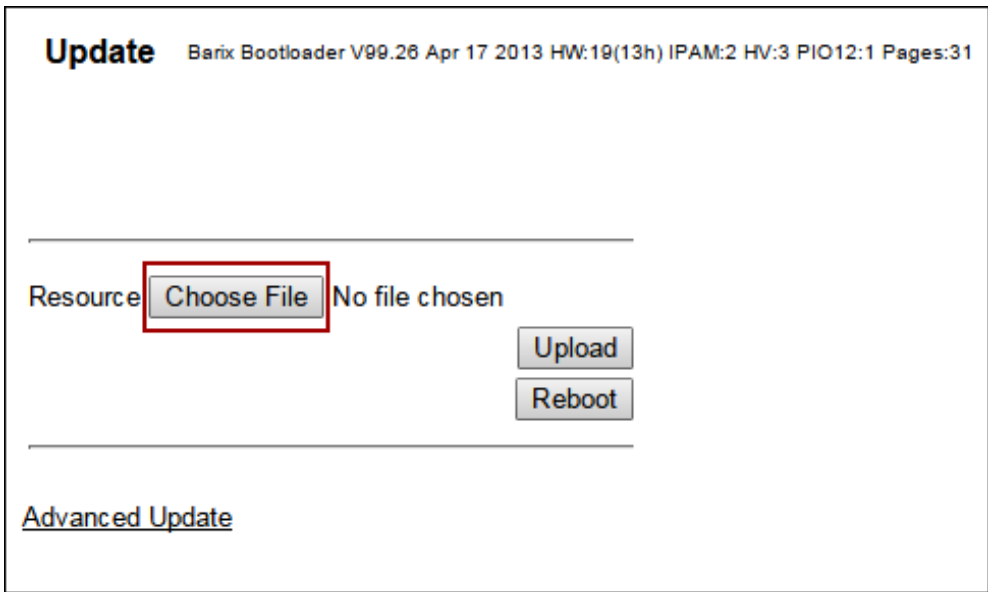
1. In a web browser, enter the IP address of the Barix Annuncicom 200 in the URL.
2. Select the **UPDATE** tab.



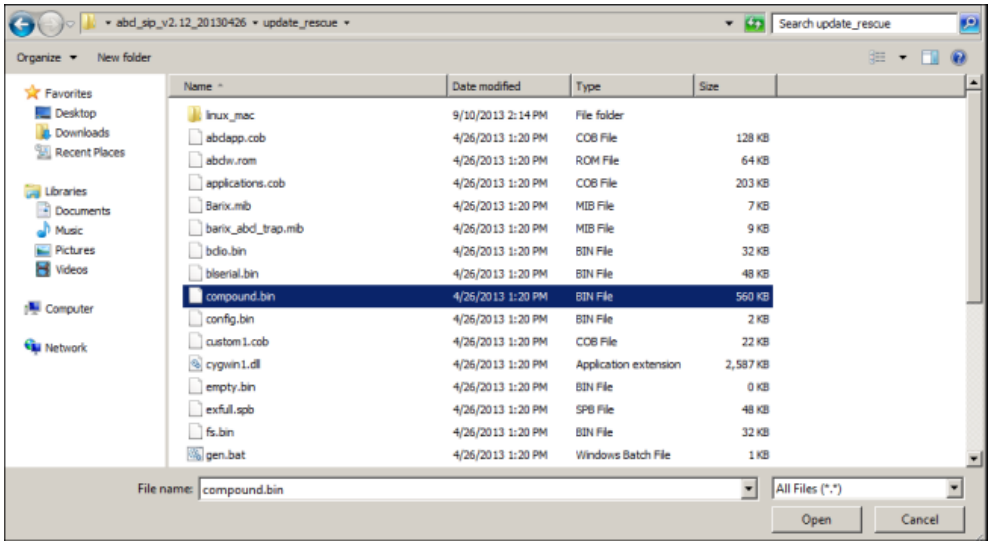
3. On the **UPDATE** window, click the **Please click here to start the update** link.
   ⇨ The device resets and a countdown displays.



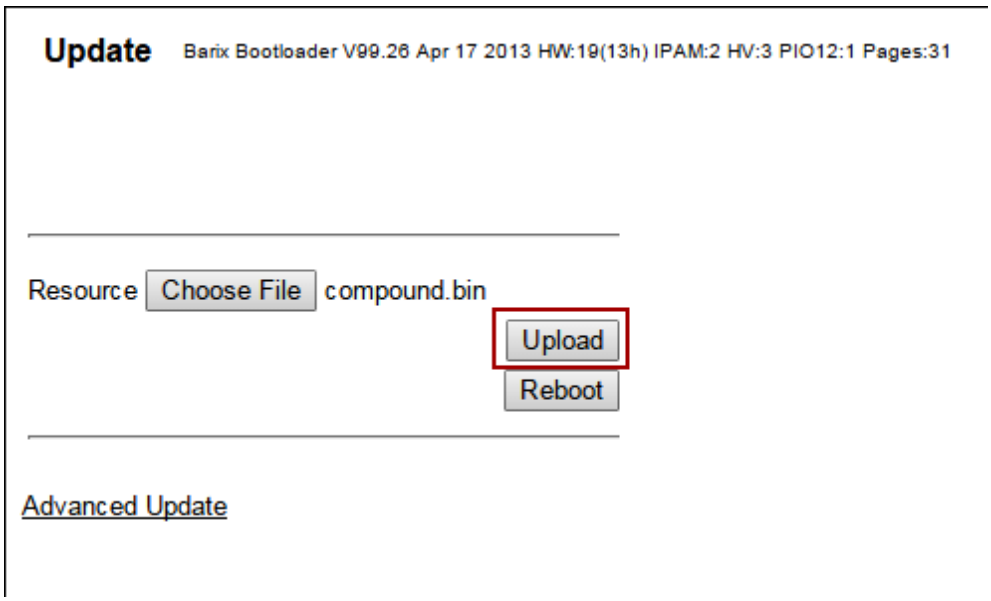
4. Once complete, the **Update** window displays, click **Choose File** to upload the new firmware bin file.



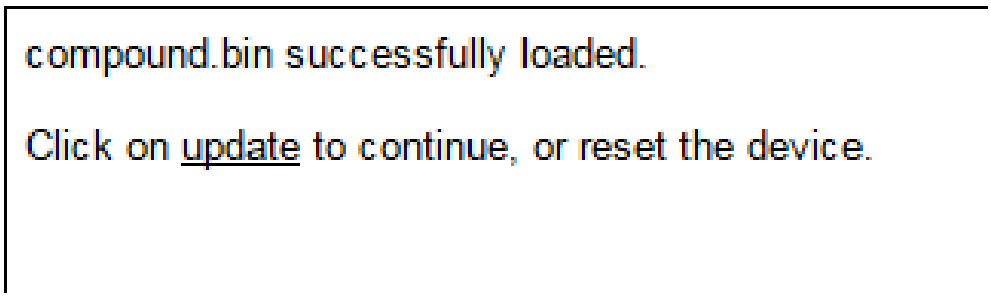
5. Select **abcl_sip_vXXXXX** > **update_rescue** and select **compound.bin** file.
6. Click **Open**.:



7. Click **Upload**.
   ⇨ The device may take up to a minute to upload and flash the new firmware.



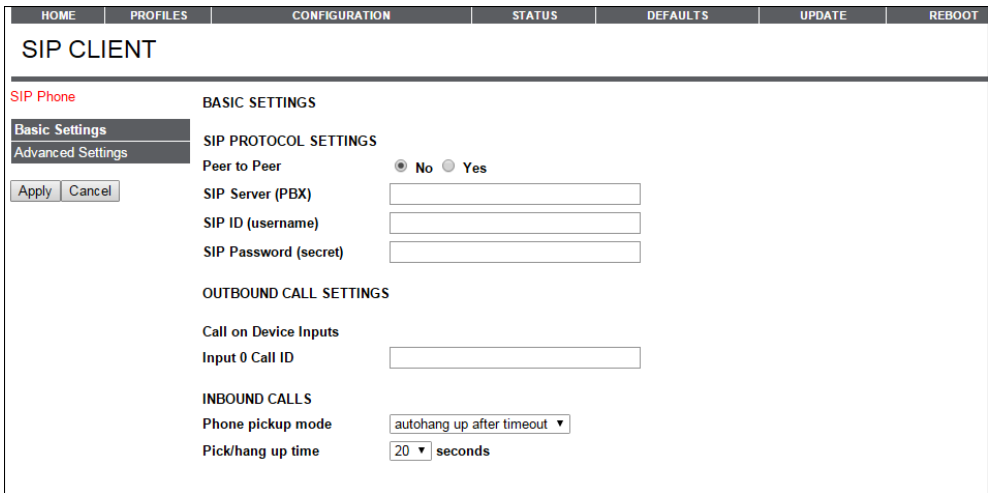
⇨ A message displays as successfully loaded once the firmware upload is complete.



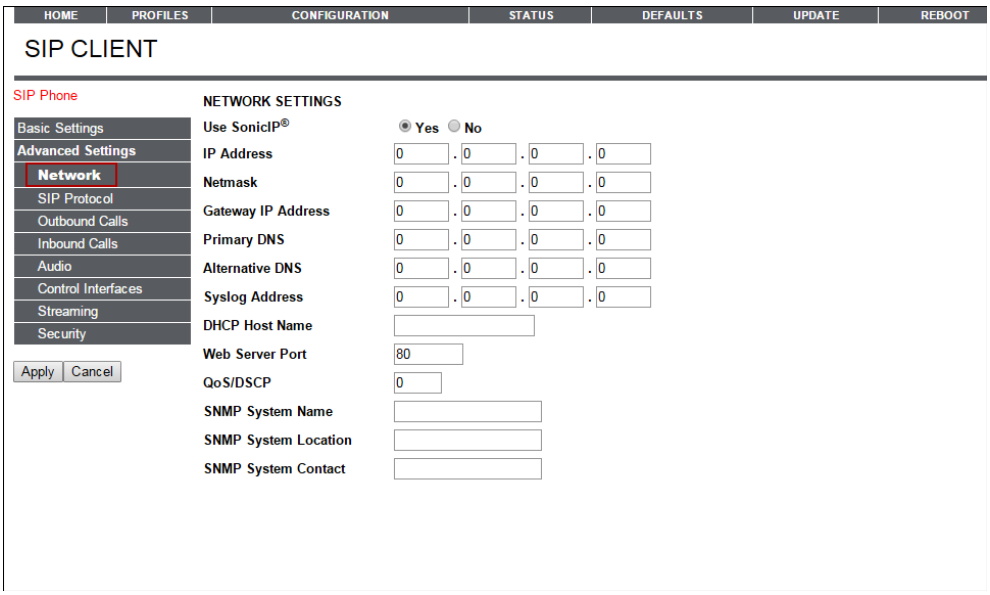
8. Reboot Barix Annuncicom 200 by disconnecting and then reconnecting the DC power supply.

Changing the IP Address

1. In a web browser, enter the IP Address of the Barix Annuncicom 200 in the URL.
2. Select the **CONFIGURATION** tab.



3. Click **Advanced Settings** > **Network**.



4. Enter the appropriate values for the **IP Address** and **Netmask** as per the IT infrastructure.
   NOTE 1: It is strongly recommended to specify a Gateway IP Address to ensure proper routing of the SIP call.
   NOTE 2: For DHCP, the required settings will automatically be populated by the DHCP server. By default, entering an **IP Address** value of 0.0.0.0 defaults to DHCP. Use the **Help** menu on the right-hand side of each configuration window for details on all the parameter fields.
5. Click **Apply**.
6. Select the **REBOOT** tab.

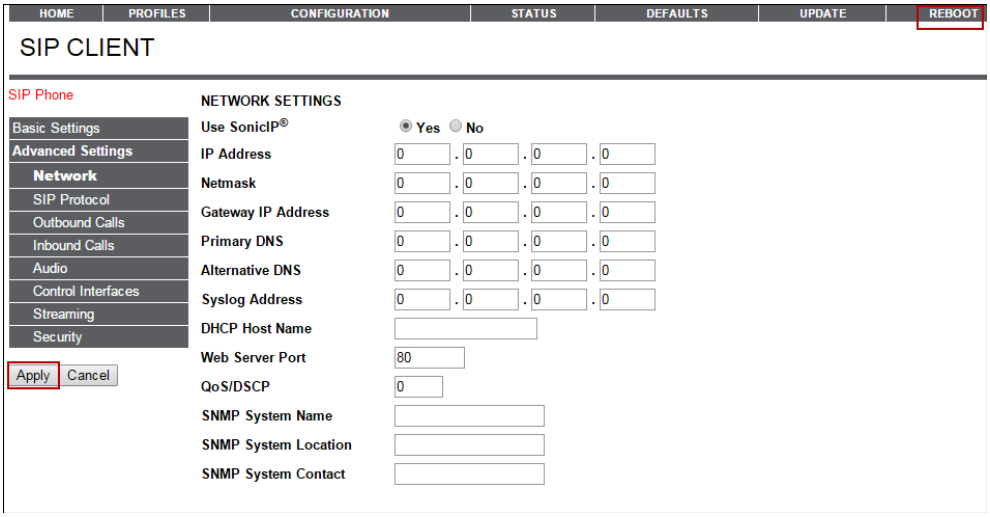
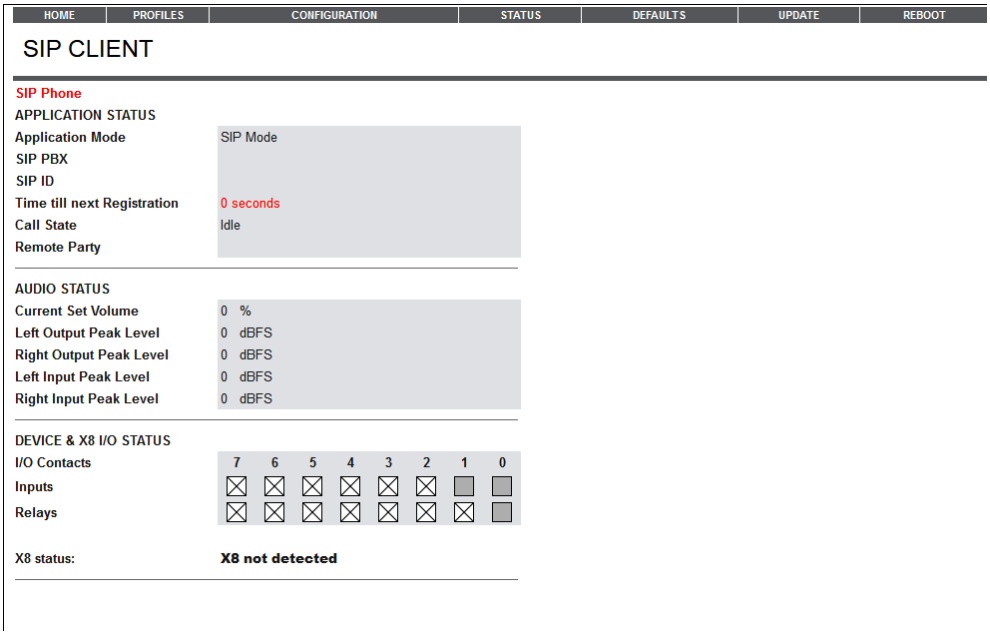


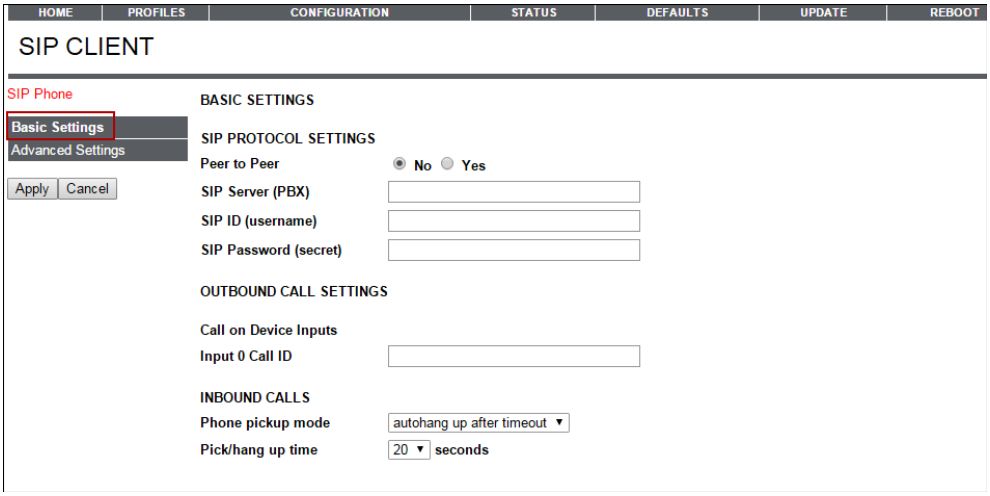
Fig. 37: Reboot Tab

Configuring the SIP Endpoint

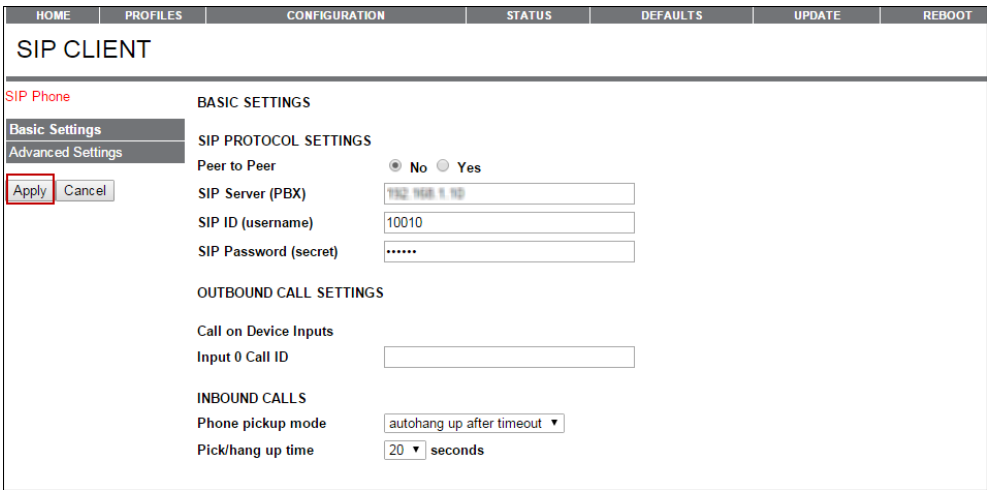
1. In a web browser, enter the IP Address of the Barix Annuncicom 200 in the address bar.



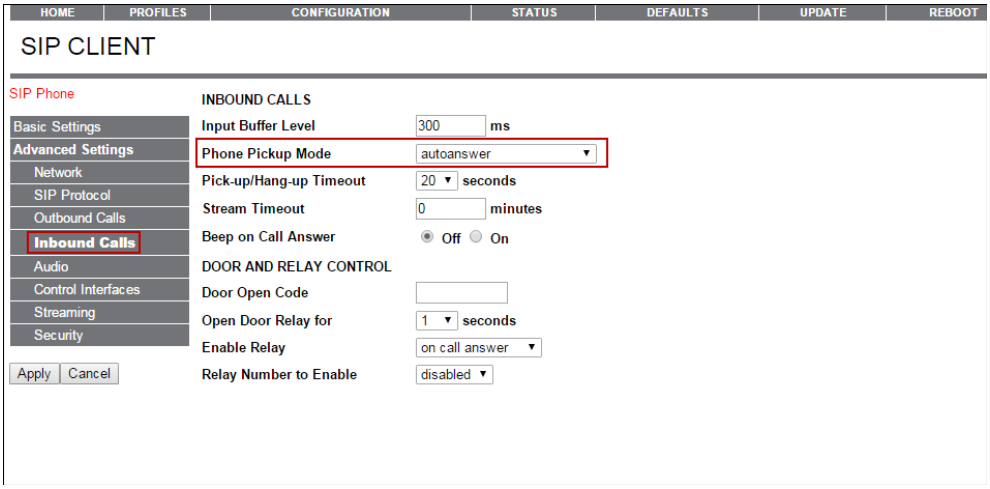
2. Select the **CONFIGURATION** tab.
3. Click **Basic Settings**.



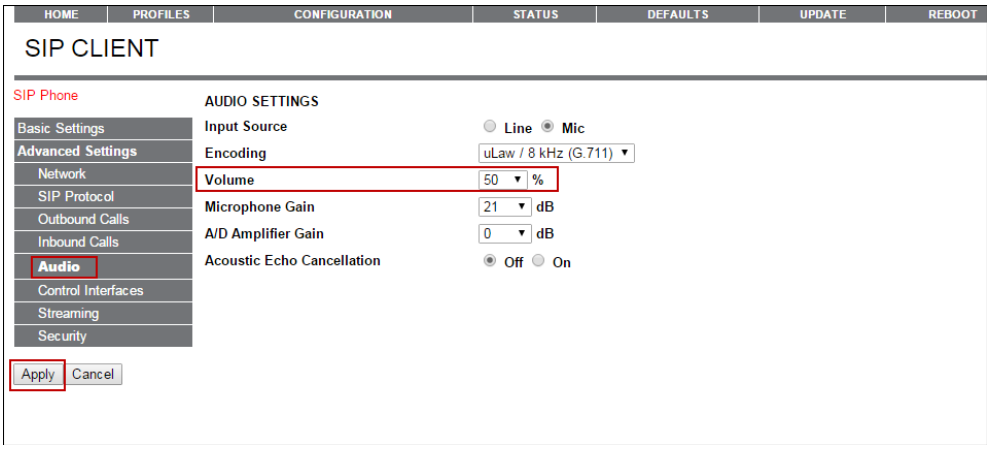
4. Select **No** for **Peer to Peer** and enter the following values for the fields given below:
   - **SIP Server (PBX)** – IP Address of the server running FreeSwitch
   - **SIP ID (username)** – The extension number for the device in the telephony server using the Telephony Configuration Tool
   - **SIP Password (secret)** – The Password used for SIP registration assigned to the extension in the **SIP ID (username)** field



5. Leave the other fields with default and click **Apply**.
6. Select **Advanced settings** > **Inbound Calls**.
7. Set the **Phone Pickup Mode** to **autoanswer**.



8. Select **Advanced Settings** > **Audio**.
9. Select the appropriate volume level.

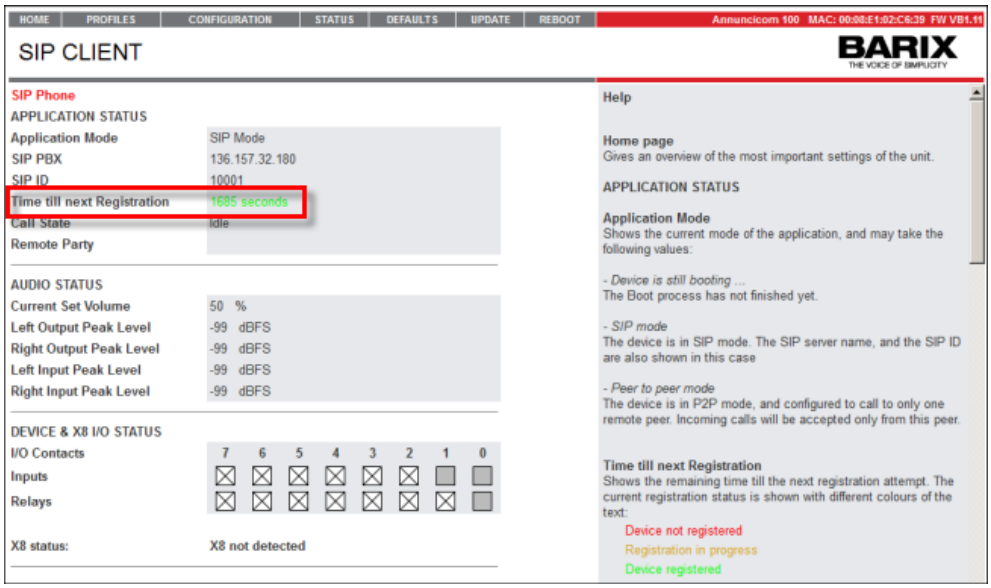


10. Click **Apply**.
11. Select the **REBOOT tab**.
12. Click the **Reboot the device** link.

➪ SIP client reboots.

13. Select the **HOME** tab.

14. Check the field **Time till next Registration**. If the time is in Green color, then the device is successfully registered with the server.
NOTE: Click on **Help** on the right hand side of the configuration window if the registration time displays in a different color.



NOTE:
When the network connection between a Barix Annuncicom 200 device and the server is interrupted, the device becomes disconnected from the telephony subsystem. The disconnected device periodically attempts to reconnect, and that frequency is determined by the time until the next registration configured on the device. The time until the next registration determines how quickly a Barix Annuncicom 200 device reconnects to the telephony subsystem once the network connection has been reestablished.

Device Verification

After successful installation and configuration, the device announces the IP Address while rebooting and the status LED remains green.

NOTE:
Verify that the device is registered using the Telephony Configuration utility. Refer to the *Telephony Configuration Guide*, P/N for details.

CyberData SIP Adapter

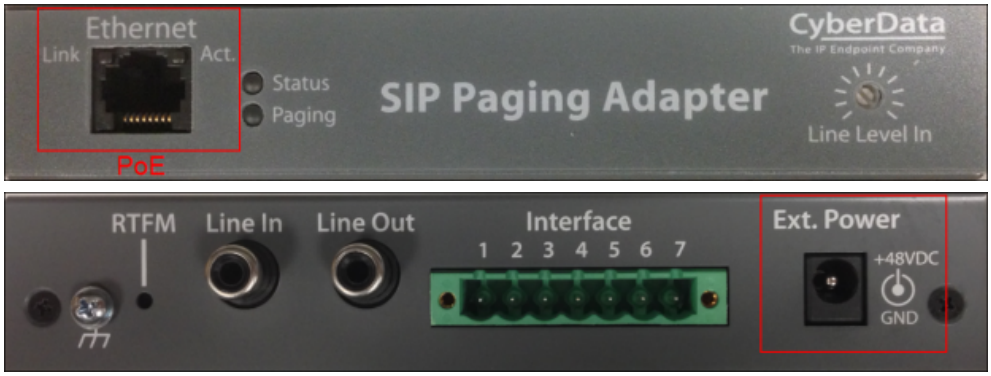
Hardware Prerequisites

Before proceeding, ensure that the following items are available:

- CyberData SIP Paging Adapter (P/N 011233)
- PoE 802.3af or 48VDC, 500mA (minimum) DC power supply
- Category 5 Ethernet cable

Power

Power to the device can either be supplied by the barrel connector or through Ethernet using a Power over Ethernet (PoE) equipped switch or power injector.



Ethernet

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

Audio Output

An audio receiver is a device that amplifies an external analog audio signal and distributes that signal to one or more speakers. Examples are an audio/video receiver, a voice-enabled fire panel system, a radio-based station, and an intercom/public announcement system.

There are two methods to supply audio from the LLA:

Method 1: Use the LINE-OUT Radio Corporation of America (RCA) socket.
NOTE 1: The tip of the RCA plug is a signal.
NOTE 2: Line Out has a 10kΩ output impedance with Voltage Peak-to-Peak (VPP) of 2V maximum.

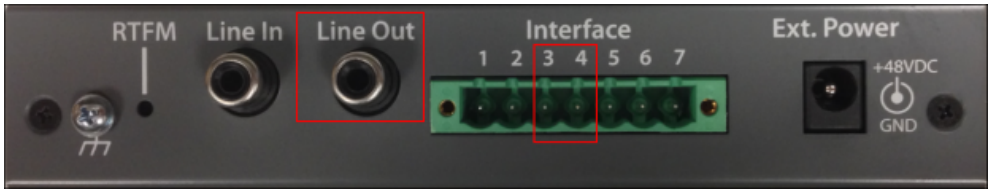
Cable requirements are as follows:

1. >= 22 awg shielded, stranded cable wire
2. < 6ft length

Method 2: Use pins 3 and 4 on the terminal block for a balanced 600Ω output with a 10V peak-to-peak.

Cable requirements are as follows:

1. >= 22 awg shielded, stranded cable wire
2. < 6ft length
3. Twisted wire pair



NOTE:
Refer to the image in Device Overview section for an illustration regarding how the various components are connected.

Hardware Verification

After completing the mechanical and electrical installations, verify that the status LED is a solid green color. If not, do the following outlined in the following sections:

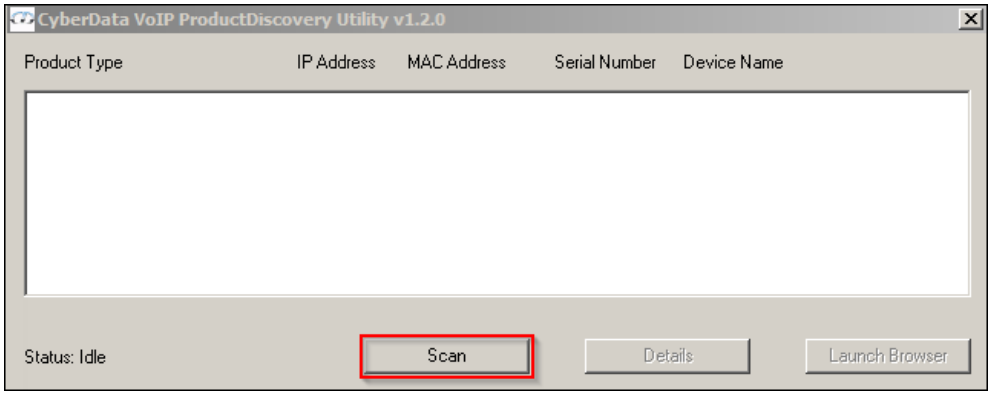
- IP Address Assignment
- Configuring a SIP End Point
- Upgrading the LLA Firmware

IP Address Assignment

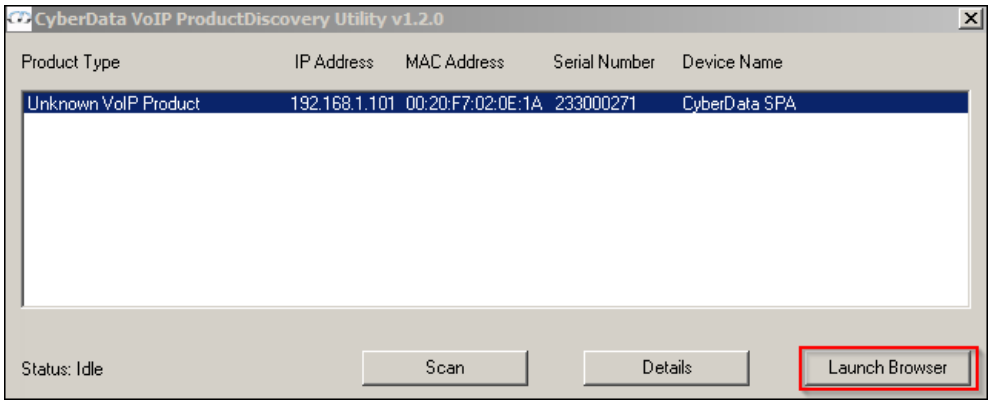
The CyberData SIP Adapter device can be configured either for DHCP or static IP.

To determine the IP address or change the IP address of the device, do the following:

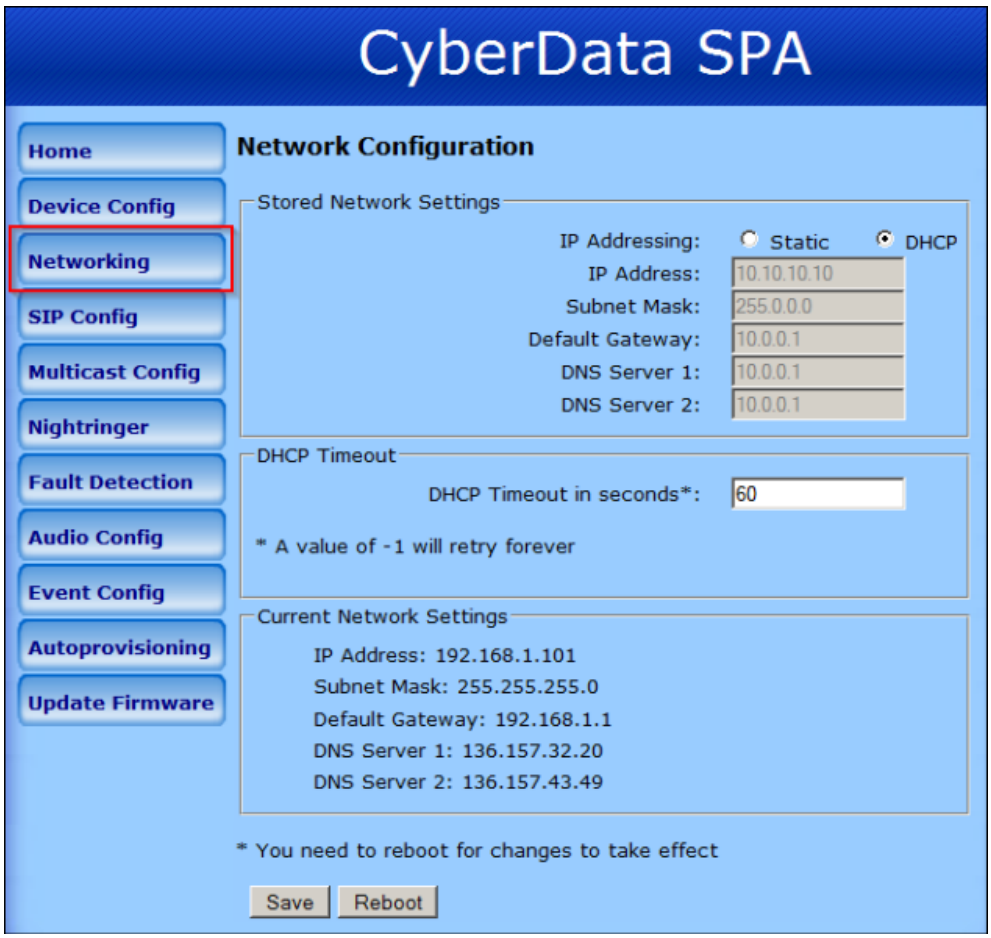
1. Connect a computer to the same switch as the CyberData SIP Adapter device.
2. Use the CyberData Discovery Utility program to locate the device on the network.
   NOTE: The Discovery Utility program can be downloaded from the following website:
   http://www.cyberdata.net/support/voip/discovery_utility.html
3. Run the utility and **Scan** for devices.
   NOTE: Ensure that the computer is on the same subnet as the device to be configured.



4. Select the device from the utility and click **Launch Browser**.
   NOTE 1: Alternatively, manually enter the IP address into a browser's URL.
   NOTE 2: The IP address of the CyberData device can also be derived by connecting an 8Ω speaker directly to pins 3 and 4 on the terminal block and pressing the Reset Test Function Management (RTFM) button on the device. The device will announce the IP address.



5. When prompted, enter **admin** for both Username and Password.
6. In **CyberData SPA** window, click **Networking**.



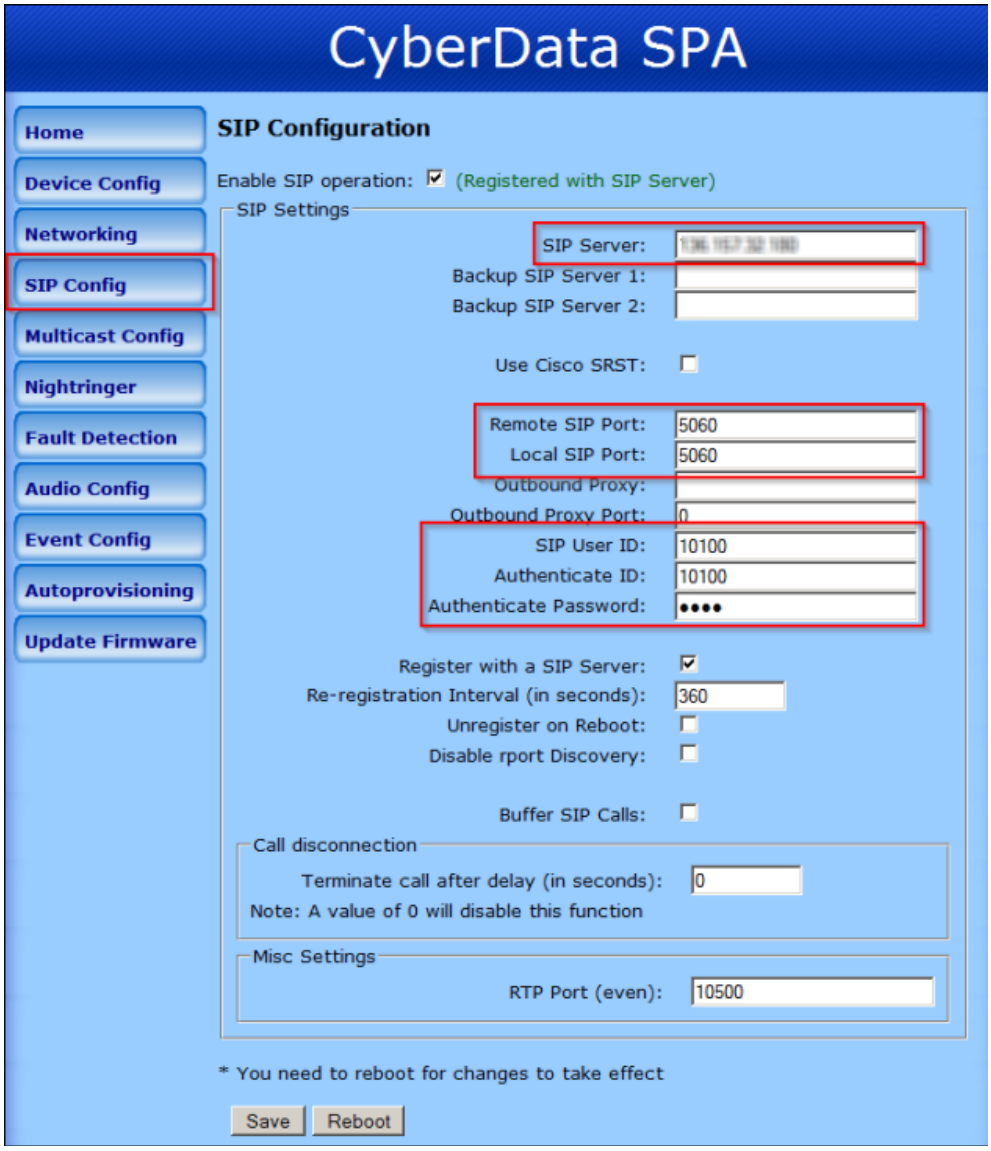
7. In the **IP Addressing** section, select either **Static** or **DHCP** option based on the device usage.
   NOTE 1: For a Static IP, enter the appropriate values for **IP Address** and **Subnet Mask**. Configure **Default Gateway** and **DNS Servers** as per the IT infrastructure procedures. It is strongly recommended to specify a **Default Gateway** to ensure proper routing of the SIP call.
   NOTE 2: For DHCP, the required settings will automatically be populated by the DHCP server.
8. Click **Save**.
9. Click **Reboot**.

Configuring the SIP End Point

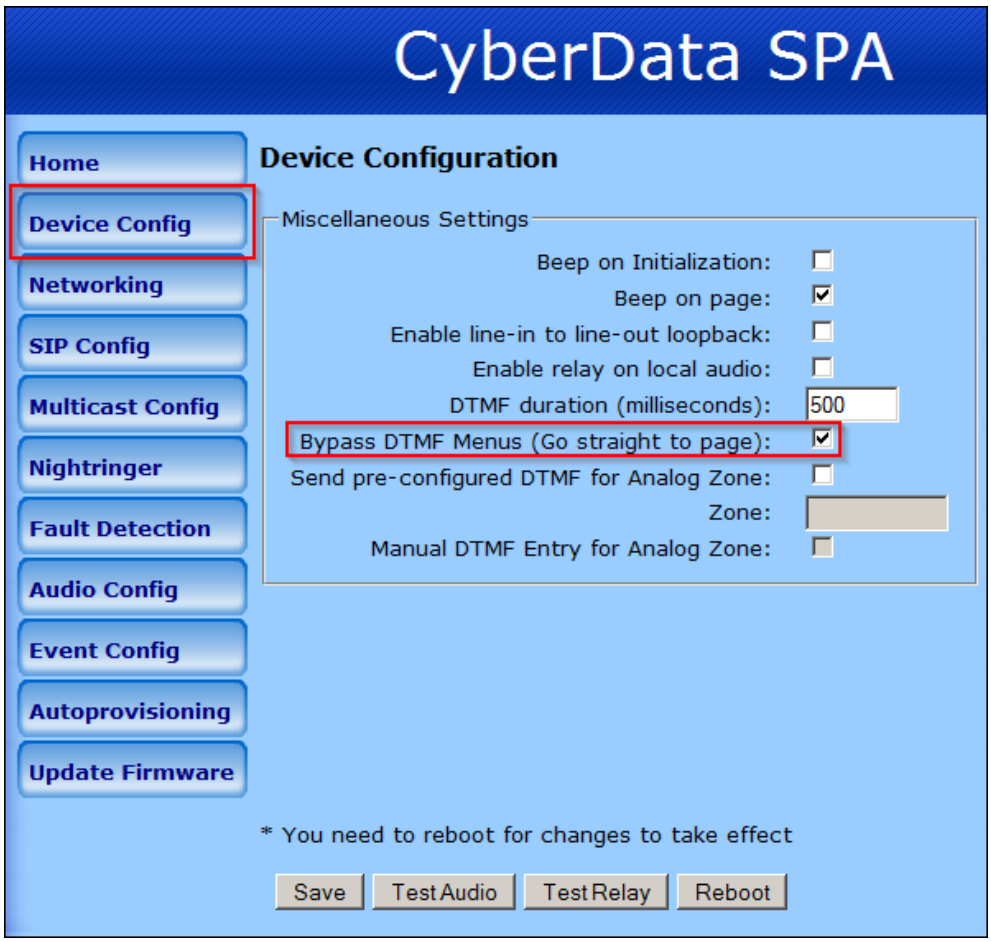
This document has been tested with firmware version 7.0.0. If an earlier version is present, before configuring the device for SIP, do the following mentioned in the *Upgrading LLA Firmware section of* Installing Multi Zone Audio.

1. In a web browser, enter the IP Address of the CyberData SIP Adapter device in the address bar.
2. Click **SIP Config**.
3. Enter the following values for the fields given below:
   - **SIP Server** – IP Address of the server running the telephony server.
   - **Remote SIP Port** - Enter 5060.
   - **Local SIP Port** - Enter 5060.
   - **SIP User ID** - Extension number for the device in the telephony server using the Telephony Configuration Tool.
   - **Authenticate ID** - Extension number for the device in the telephony server using the Telephony Configuration Tool.
     Authenticate Password - The password used for the SIP registration

assigned to the extension above.
NOTE: For more information on the Telephony Configuration Tool, refer to the *Telephony Configuration Guide,* P/N .



4. Leave the other fields with default and click **Save**.
   NOTE: When the network connection between a CyberData SIP Adapter and the server is interrupted, the device becomes disconnected from the telephony subsystem. The disconnected device periodically attempts to reconnect, and that frequency is determined by the re-registration interval configured on the device. The re-registration interval determines how quickly a CyberData SIP Adapter device reconnects to the telephony subsystem once the network connection has been re-established.
5. Click **Device Config**.
6. Enable the **Bypass DTMF Menus (Go straight to page)**.



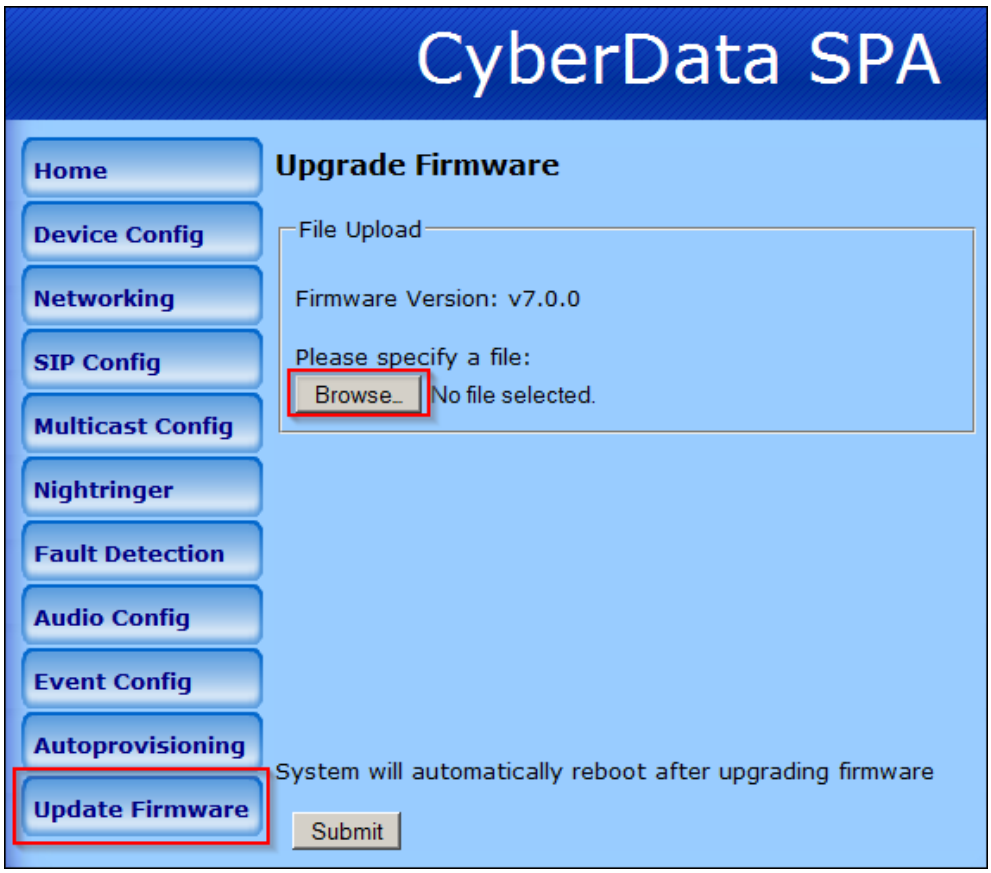
7. Click **Save**.
8. Click **Reboot**.

Upgrading LLA Firmware

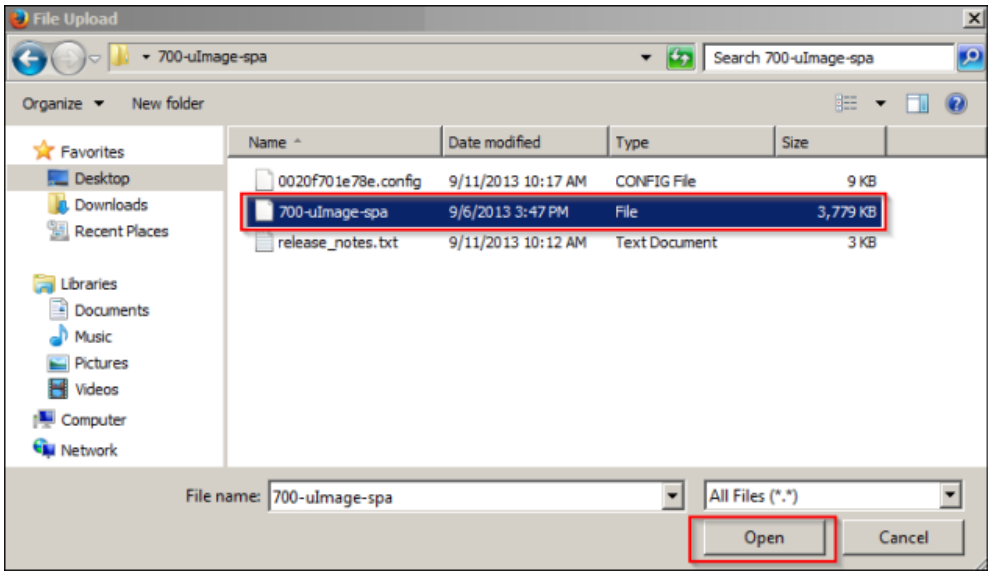
The latest firmware can be obtained from the CyberData website.

Disclaimer:
Prior to the commissioning of a 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.

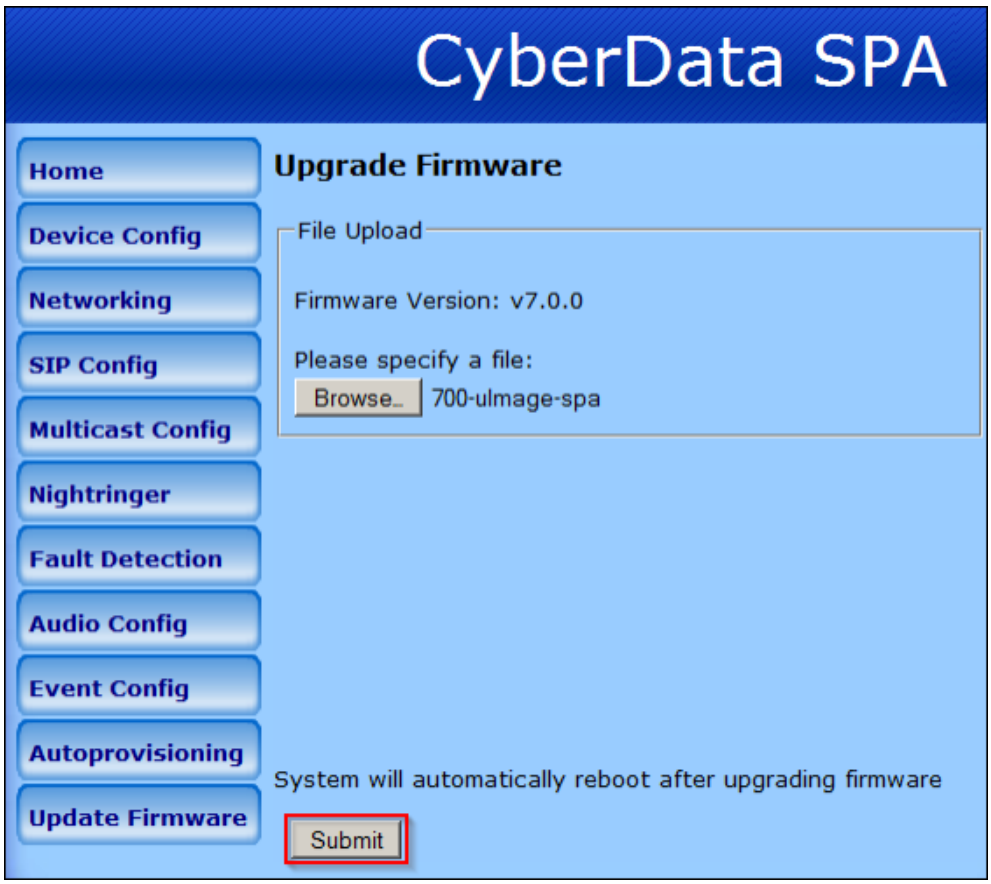
1. In a web browser, enter the IP Address of the CyberData SIP Adapter device in the address bar.
2. Click **Update Firmware**.
3. Click **Browse**.



4. Select the folder containing the firmware upgrade file.
5. Select the firmware upgrade file.
6. Click **Open**.



7. Click **Submit**.
   NOTE: The device may take up to two minutes to upgrade.



Device Verification

After successful installation and configuration, the status LED turns blue.

NOTE:
Verify that the device is registered using the Telephony Configuration utility. Refer to the *Telephony Configuration* section.

Perle TD2R2 Device

The following subsections describe the steps necessary to wire, mount, and configure the Perle TD2R2, the Ethernet I/O Relay device. There are two areas of configuration. The first is to configure the TD2R2 device to allow remote access to the relays. The second area of configuration is the TruePort driver which the server uses to communicate with the TD2R2 device.

Configuring the TD2R2 requires Perle's DeviceManager software. Install DeviceManager on a computer that is connected to the same subnet network as the Perle device being configured.

Prerequisites

Before proceeding, ensure that the following items are available:

- Perle IOLAN SDS1 TD2R2
- 9-30VDC (400mA minimum) power supply, if not included with device
- Category 5 Ethernet cable
- Computer or server to communicate with the device
- Device Installation CD or a computer with network access
- Hookup wire – when using the I/O and relay pins
  NOTE 1:
  The driver (TruePort) that is used to communicate with the device must be installed on the same server/machine that runs the application.
  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 DHCP.
NOTE 3:
To configure the device, a computer located in the same network is required.

Mounting

The Perle TD2R2 has two brackets on the side of the mounting holes. The installer should fasten the device to a flat surface by placing screws through mounting holes

Power

▷ For the Perle TD2R2, use a power adaptor capable of 9-30VDC output and 400mA.

1. 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** LED should be a solid green color.
NOTE:
Connecting the power supply to the device with incorrect polarity can permanently damage the device and pose a fire risk.

Ethernet

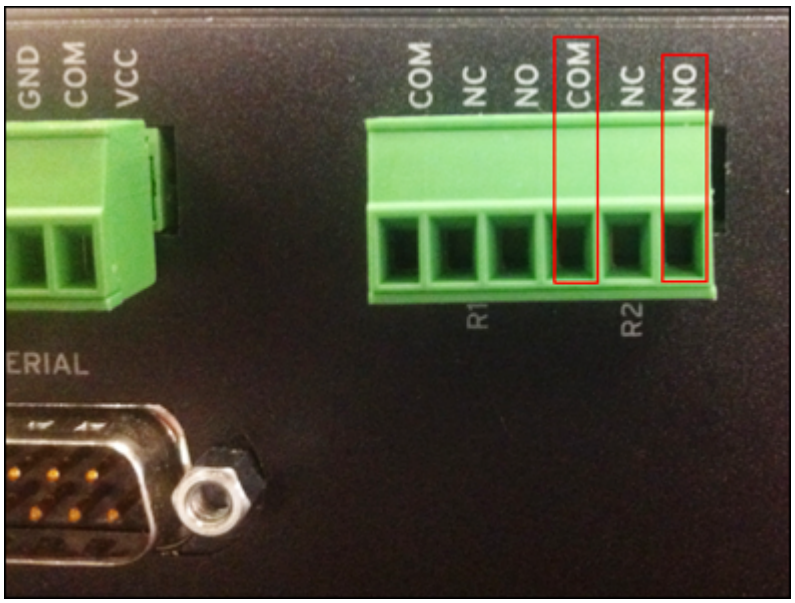
1. Plug one end of the Ethernet cable to the RJ45 jack on the device.
2. Connect the other end of the Ethernet cable to the network jack.

⇨ After a few seconds, the **Link/10/100** should be a solid amber or green color.
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.

Relay Output

The relay outputs are generally used to switch higher power speaker arrays or zone selection circuits on fire panels. In addition, relay outputs differ from digital outputs in that electrical isolation between the two devices are provided.

Generally, these external circuits require a closed dry contact for activation. The Perle TD2R2 includes two relays each with separate COM terminals. When hooking the device relays to external circuits, use the COM and NO (normally open) terminals. This will provide a closed switch activation to any external circuit.



Configuring Multi Zone Audio Device

Certificate Creation From System Management Console

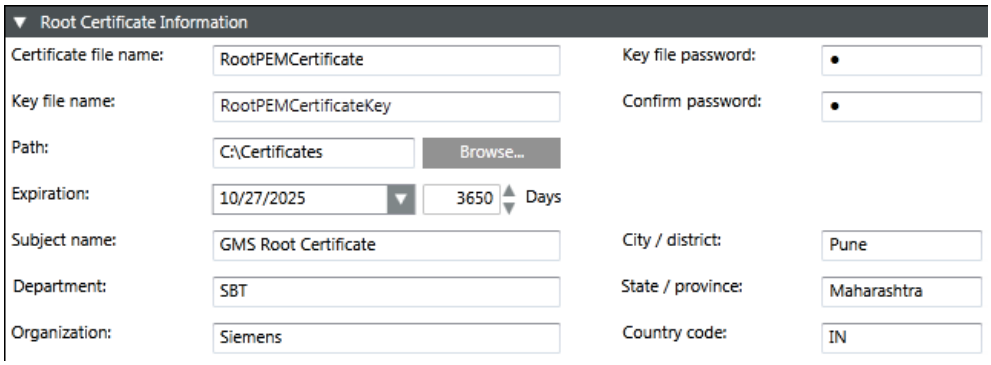
To establish a secure communication, certificates must be configured.

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

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

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.



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** to initiate root certificate creation.

⇨ 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.

Device Configuration

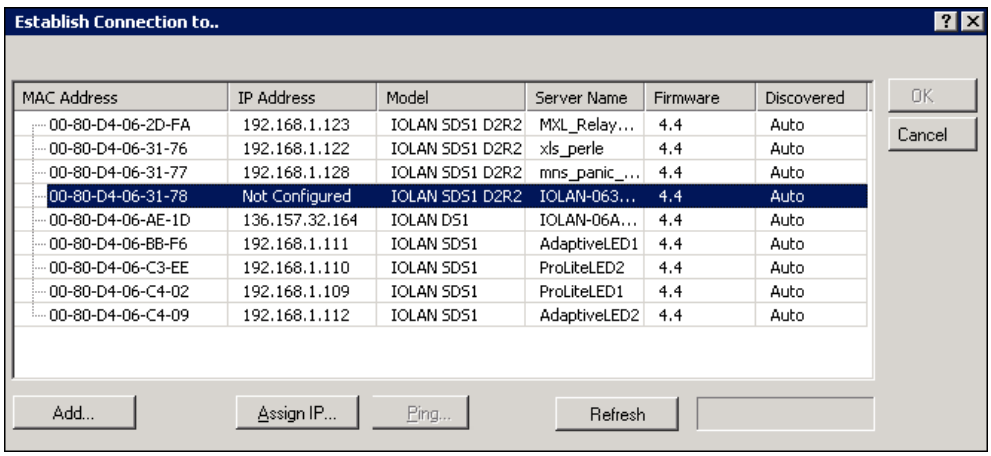
▷ The **DeviceManager** is installed on a computer located in the same network as the device to configure.

▷ 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**.

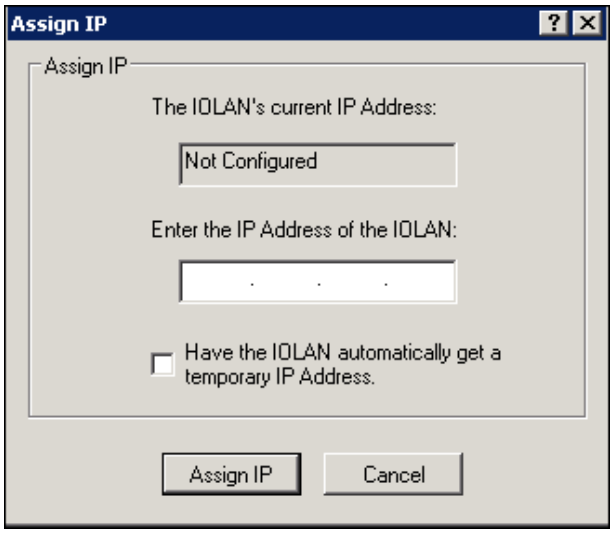
▷ If preconfigured .dme file is available, then refer Import DME File section.

1. Start **DeviceManager**.



⇨ All similar devices under that network are visible.

2. Select the device to configure and click **Assign IP**.
   NOTE 1: If unable to see the device in the window, verify that the device has power and is connected to the network. Check the LEDs on the device; the power LED should be a solid green color and the link LED should be a solid amber / green color.
   NOTE 2: If issues persist, unplug the Ethernet cable and power. Wait for five 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 a solid amber color and then release. Wait for 90 seconds for device to reboot and initialize. If resetting 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**.



⇨ The connection window displays with an IP address.

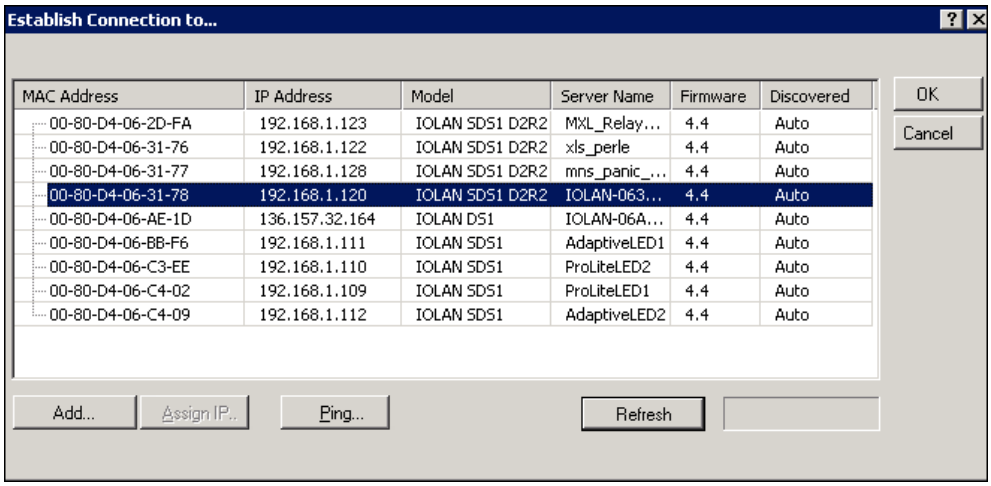
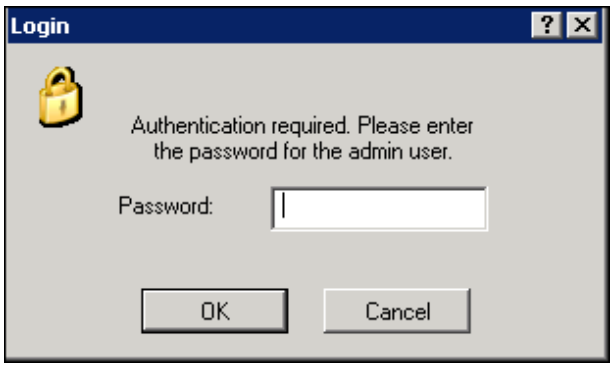


Fig. 38: Establish Connection To

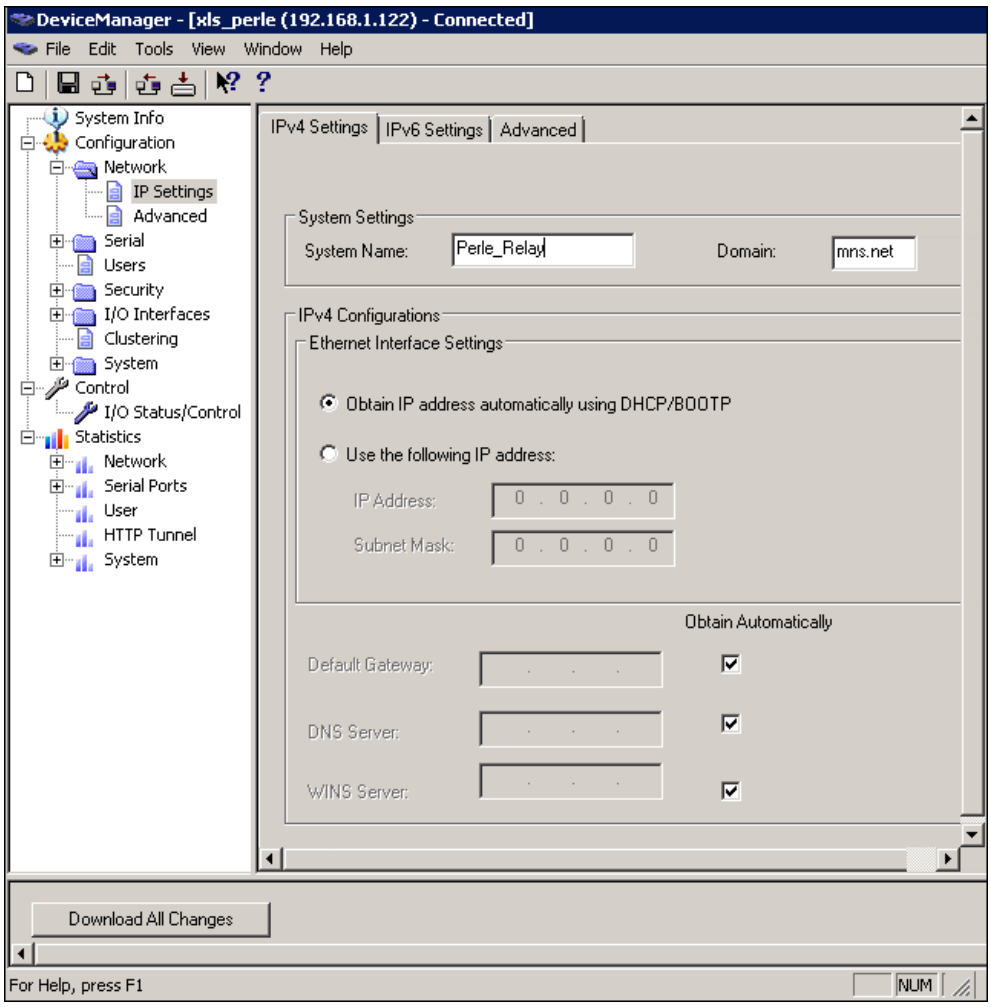
4. Select the device again, and click **OK** to log into the device for configuring.
5. At the login window, type in the device password. The factory default password is: **superuser**.



Network Set Up

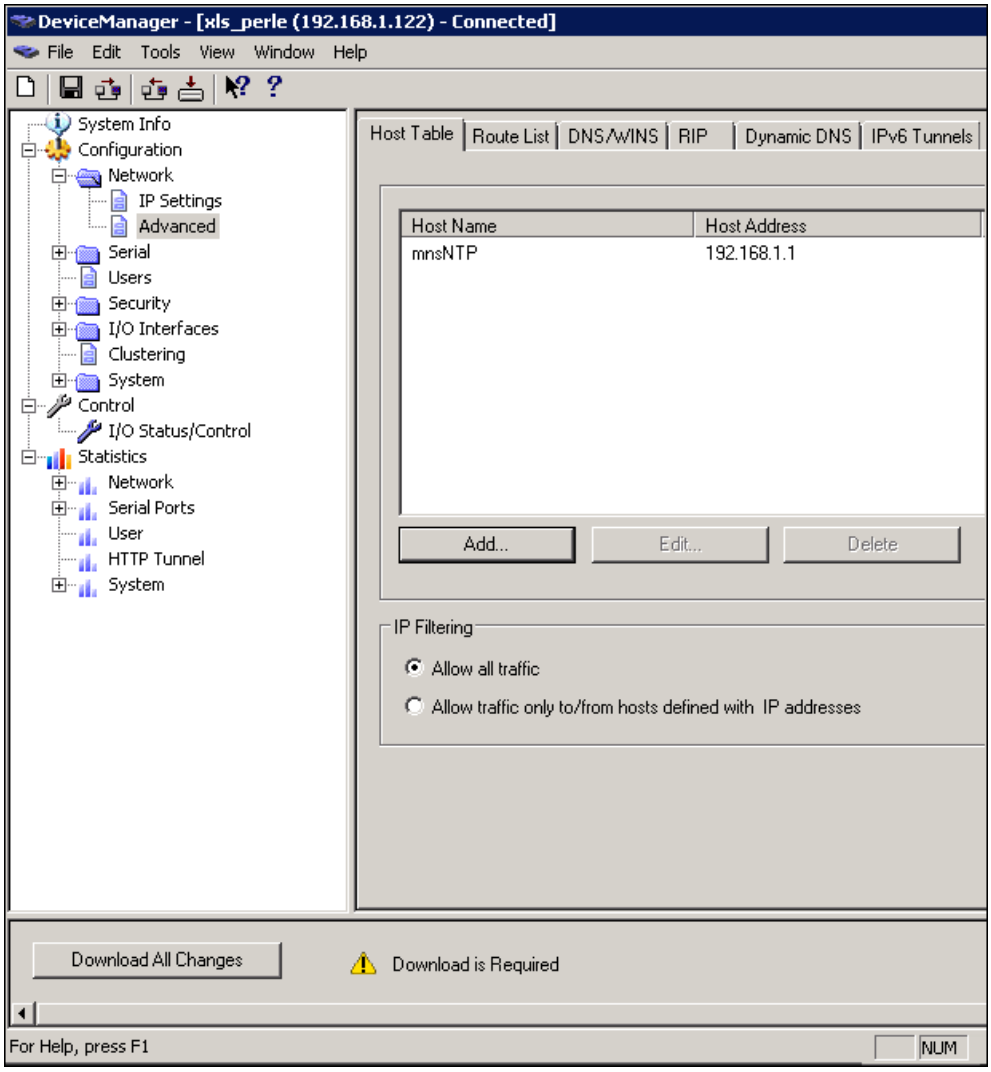
▷ Log in to the device using the DeviceManager.

1. In the Device Manager window, click on the **Network folder** and then on **IP Settings**.
   NOTE: In this area, it is possible to configure additional parameters for the network settings, such as configuring a **static IP address** or a **DHCP**.



2. In the **System Name** field, provide a name that helps distinguish the device from other similar devices.
   NOTE 1: The System Name is 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.

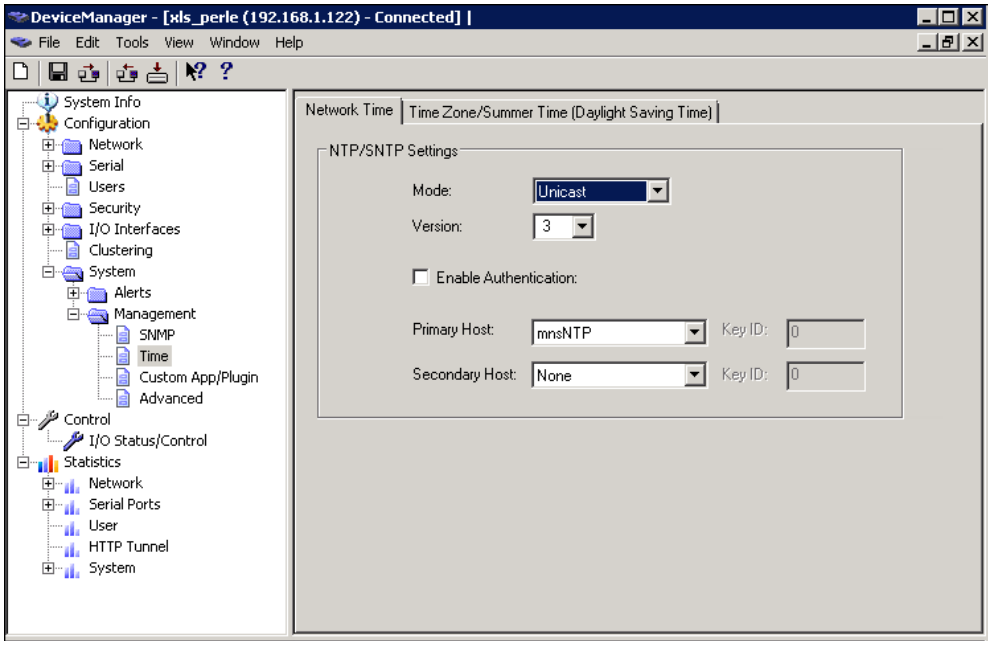
3. Select the **Domain** field, enter the domain name used on the client's network. For example, **AmericaUniversity.net**.
   NOTE: The device is capable of receiving the domain automatically from DHCP. However, DHCP would have to be configured to set the domain as a parameter.
4. Select **Network>IP Settings**.
5. Select the **Advanced** tab.
6. Select the **Register Address in DNS** check box.
7. Select the **Advanced** option from the left-hand side of the window.
8. Select the **Host Table** tab.
9. Click **Add** to add an NTP host.



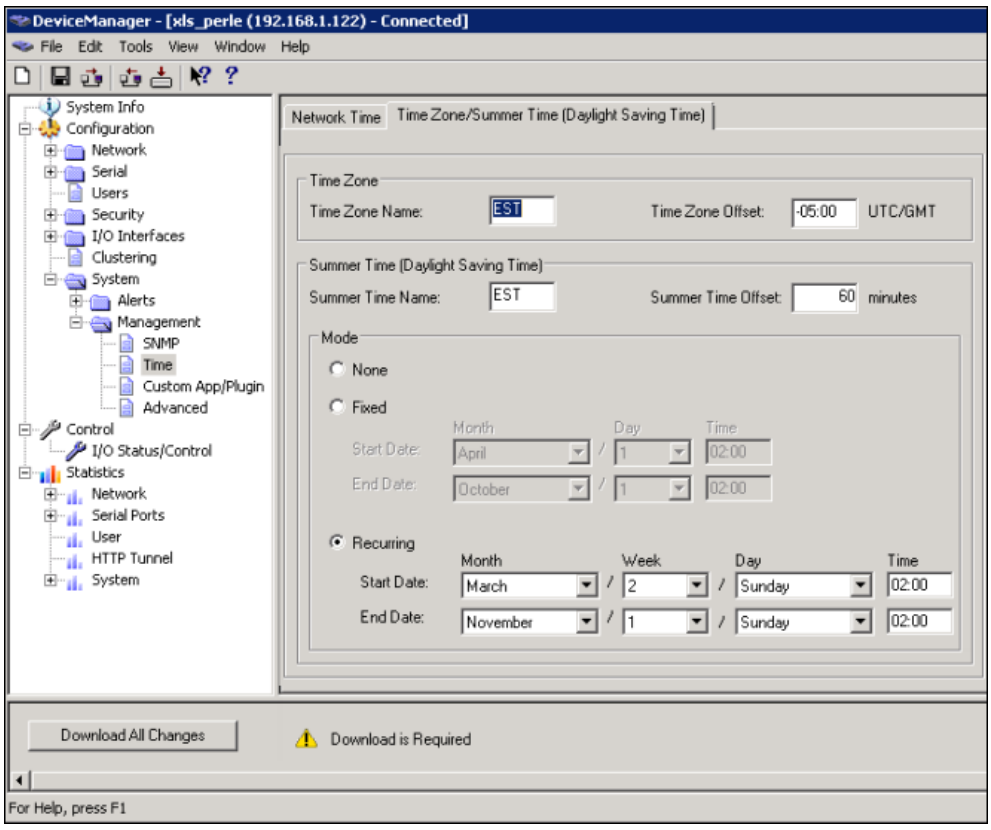
10. On the window, enter a descriptive name for the NTP server (for example, **mnsNTP**).
11. Enter the IP address or the fully qualified domain name of an available NTP server.
    NOTE: An available NTP server is required to enable SSL on the device.
12. Click **OK**.

Time and Security Settings

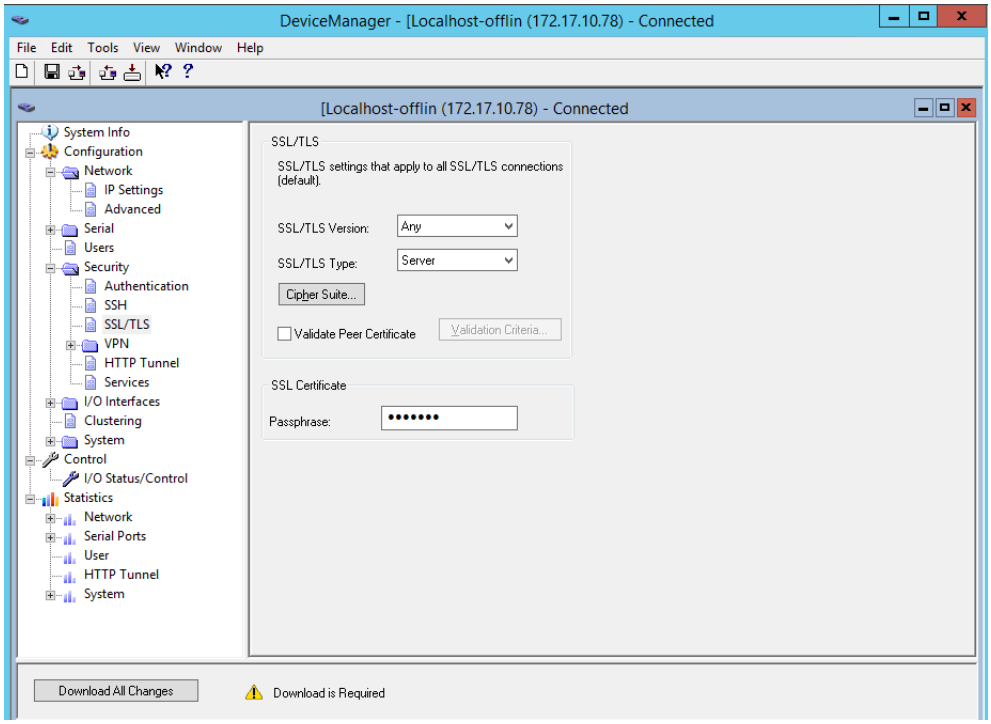
1. Select **Configuration > System > Management > Time**.
2. Select the **Network Time** tab.
3. Set the following parameters:
   - **Mode**: Unicast.
   - **Version**: 3.
   - Leave the **Enable Authentication** check box unselected.
   - **Primary Host**: Select the NTP server name created earlier.
   - **Secondary Host**: Select an alternative NTP server name, otherwise set the name as the 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 if there are any questions.



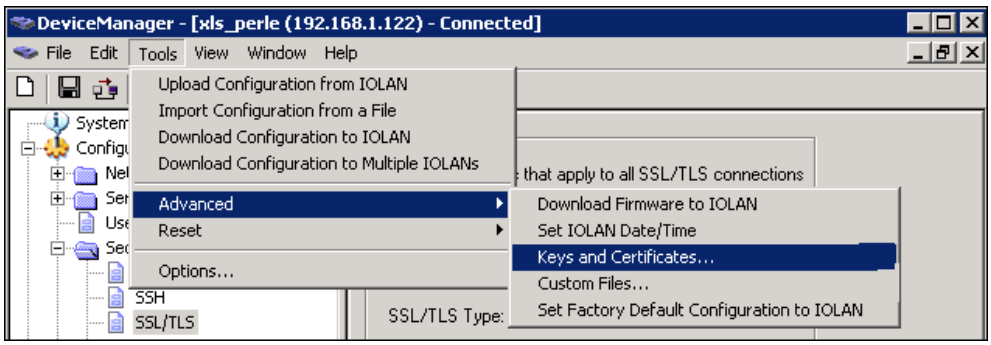
4. Select the **Time Zone/Summer Time (Daylight Saving Time)** tab.
5. Configure the parameters as per the details mentioned in the Time Zone/ Summer Time (Daylight Saving Time) Parameters section.



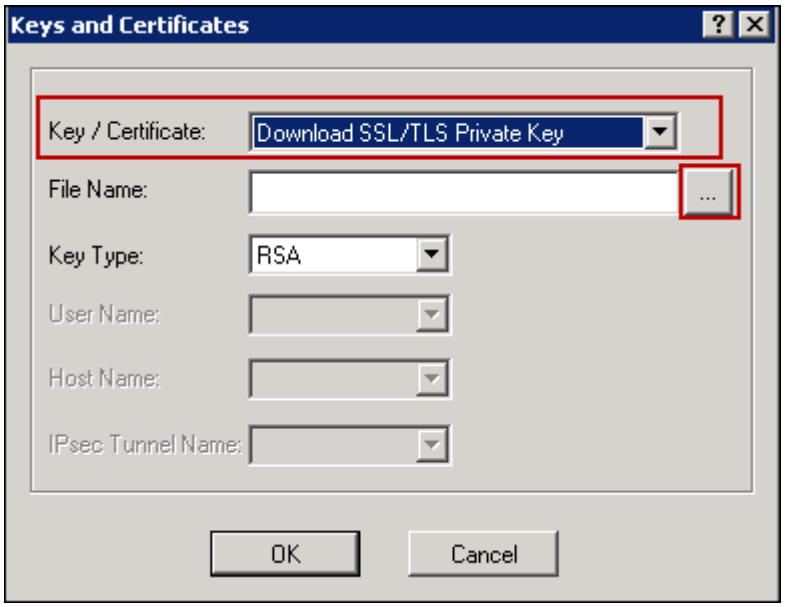
6. Select **Configuration > Security > SSL/TLS**.



7. Set **SSL/TLS Version** field to **Any**.
8. Set **SSL/TLS Type** field to **Server**.
9. Select the **SSL Certificate** section.
10. Enter the password of the SSL certificate in the **Passphrase** field.
11. Select **Tools > Advanced > Keys and Certificates**.



12. In the **Key/Certificate** drop-down list, select **Download SSL/TLS Private Key**.
13. Click the browse button and upload the private key for your Root certificate (.pem).
14. Click **OK**.



15. Select **Tools > Advanced > Keys and Certificates**.
16. In the **Key/Certificate** drop-down list, select **Download SSL/TLS Certificate**.
17. 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.
18. Click **OK**.
19. Select **Tools > Advanced > Keys and Certificates**.
20. In the **Key/Certificate** drop-down list, select **Download SSL/TLS CA**.
21. Click the browse button and upload the upload the Root certificate (RootCertificate.pem file).
22. Click **OK**.

Time Zone/Summer Time (Daylight Saving Time) Parameters

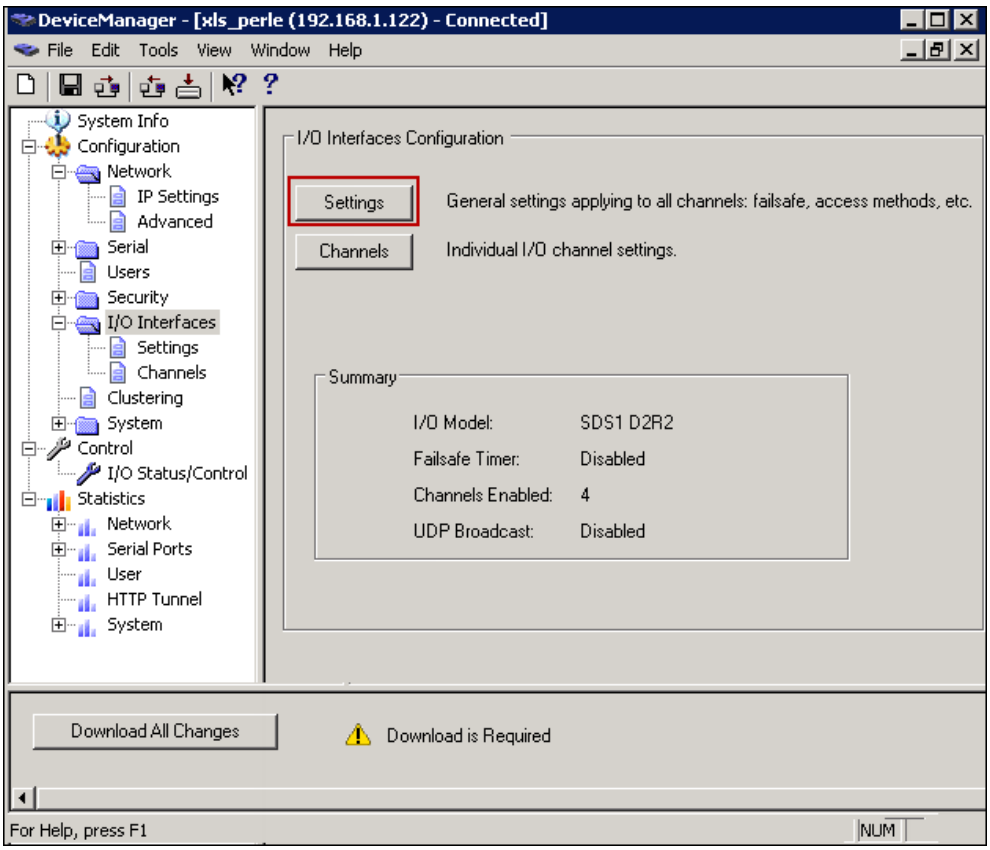
Field	Description

Time Zone Name	The name of the time zone to be displayed during standard time. **Field Format:** Maximum four characters and minimum three characters (do not use angle brackets <>)
Time Zone Offset	The offset from Coordinated Universal Time (UTC) for the local time zone. **Field Format:** Hours *hh* (valid -12 to +24) and minutes *mm* (valid 0 to 59 minutes)
Summer Time Name	The name of the configured summer time zone will be displayed during the summer time setting. If this parameter is not set, then the summertime feature will not work. **Field Format:** Maximum four characters and minimum three characters (do not use angle brackets <>)
Summer Time Offset	The offset from standard time in minutes. Valid values are 0 to 180. **Range:** 0-180 **Default:** 60
Summer Time Mode	Use this mode to configure when the summer time will take effect. **None** – No summer time change **Fixed** – The summer time change goes into effect at the specified time every year. For example, April 15 at 1:00 P.M. **Recurring** – The summer time change goes into effect every year at the same relative time. For example, on the third week in April on a Tuesday at 1:00 P.M. **Default** – None
Fixed Start Date	The exact date and time in which the IOLAN's clock will change to summer time (daylight saving time) hours.
Fixed End Date	The exact date and time in which the IOLAN's clock will end summer time hours and change to standard time.
Recurring Start Date	The relative date and time in which the IOLAN's clock will change to summer time (daylight saving time) hours. Sunday is considered the first day of the week.
Recurring End Date	The relative date and time in which the IOLAN's clock will end summer time hours and change the standard time. Sunday is considered the first day of the week.

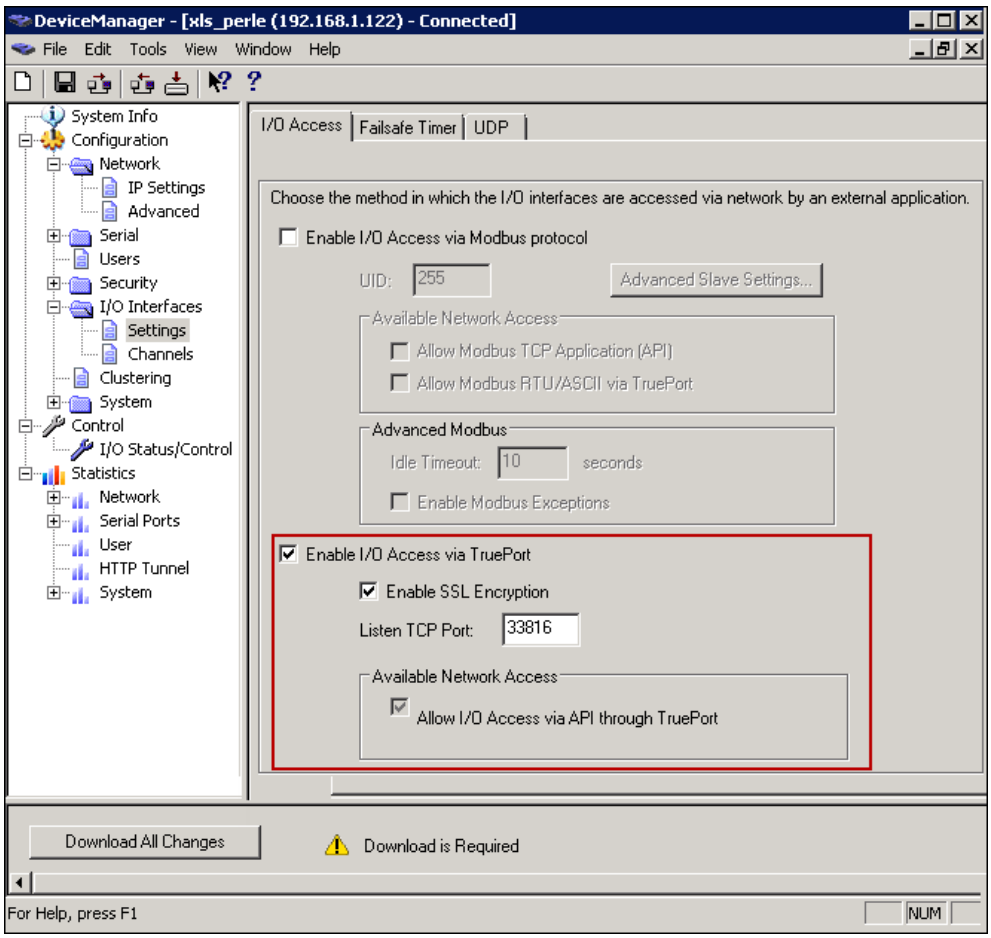
I/O Access Settings

▷ Log in to the device using the DeviceManager.

1. In the **DeviceManager** window, click **I/O Interfaces** on the left-hand side of the window.
2. Click **Settings**.



3. Select the **I/O Access** tab.
4. Select the **Enable I/O Access via TruePort** check box.
   NOTE 1: By default, the device monitors I/O commands on TCP port 33816. If there is a need to change the I/O TCP port, it can be changed as long as the change does not conflict with other services or TruePort ports.
   NOTE 2: 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.



5. Select the **Enable SSL Encryption** check box.

   ⇨ Configuration is now complete.

6. Click **Download All Changes**.

7. Click **Reboot IOLAN**.
   NOTE: Any time you reboot the device, or power is reconnected, wait 90 seconds for the device to reboot and initialize. When the device is ready, the Power LED will be solid green and the Link LED will be solid amber/green.

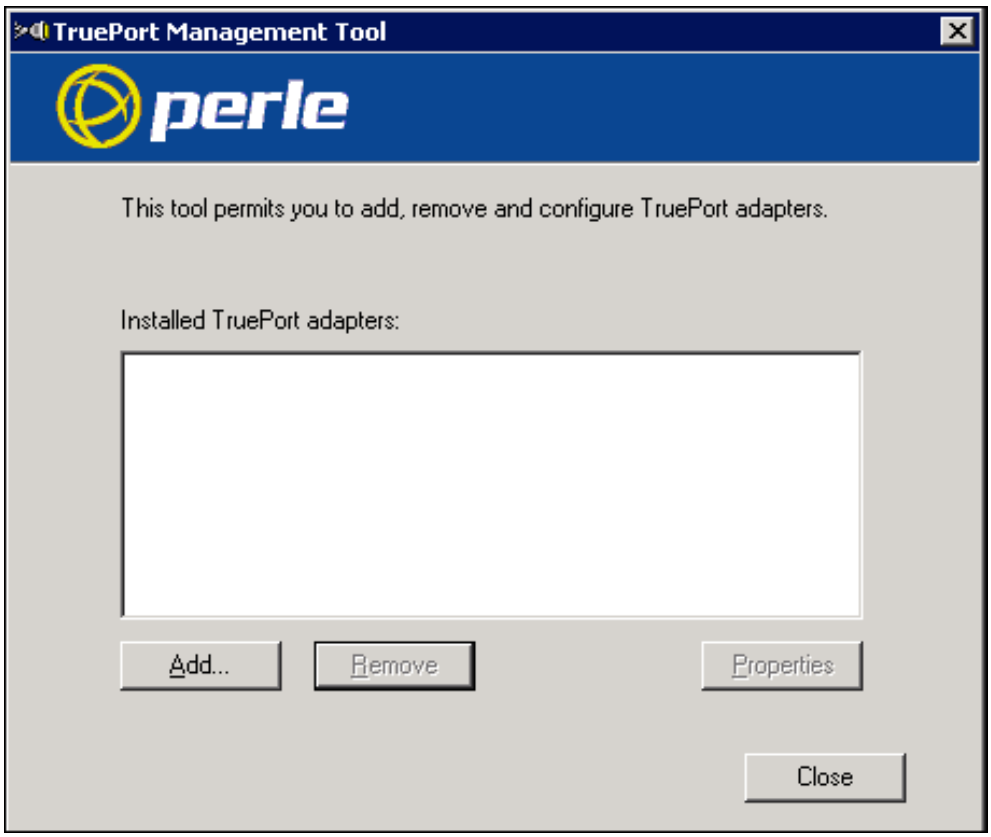
TruePort Driver Configuration

The TruePort driver is the second part of the process to link the device to the server. The TruePort driver is designed to manage all similar devices communicating with the server. Since TruePort creates a virtual COM port, each device should have a COM port for each service.
NOTE: Serial communication and I/O access are each considered a separate service and therefore require separate COM ports.

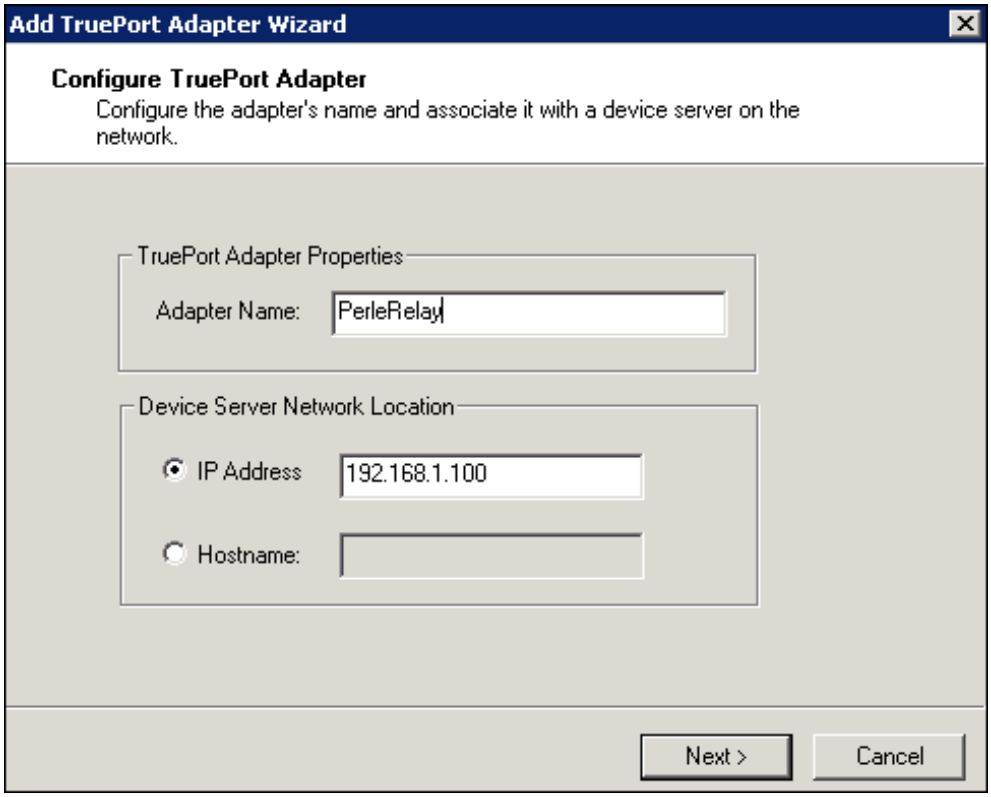
▷ Ensure that the TruePort is installed on the server.

1. Start the **TruePort Management Tool**.

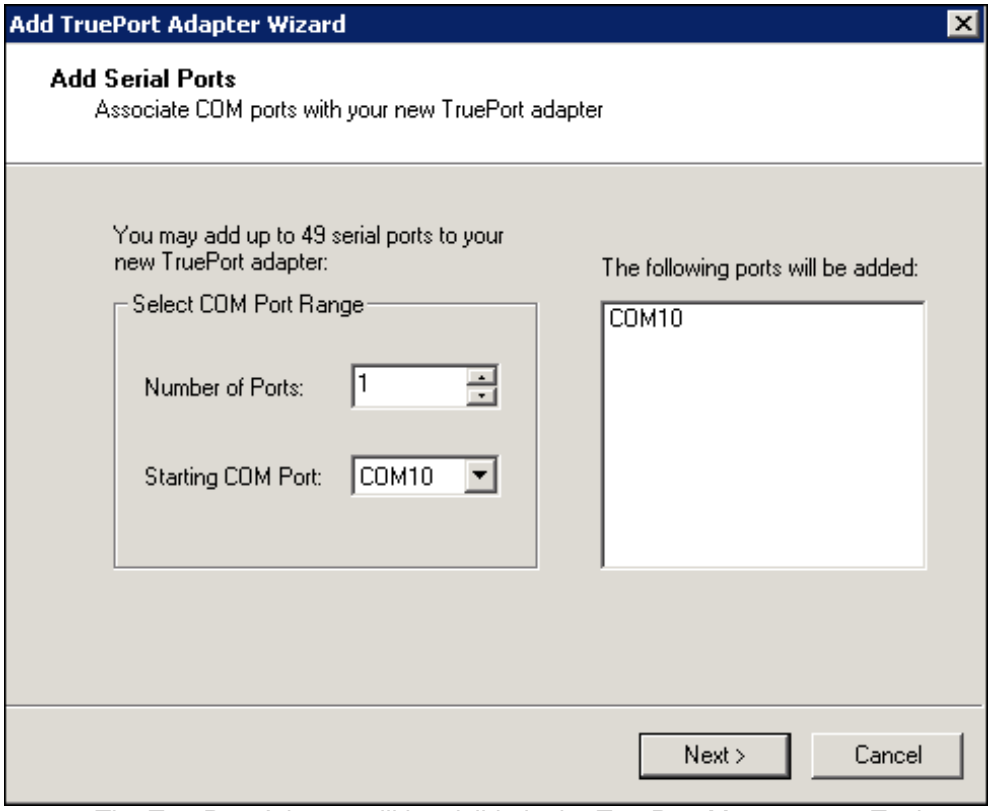
2. Click **Add**.



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



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

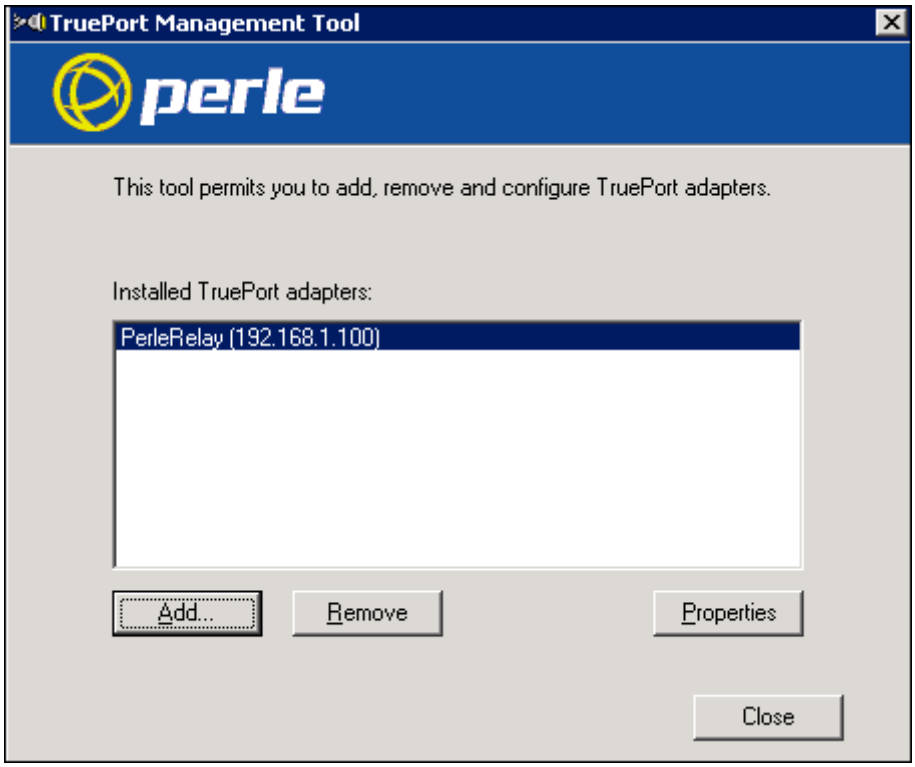


⇨ The TruePort Adapter will be visible in the TruePort Management Tool.

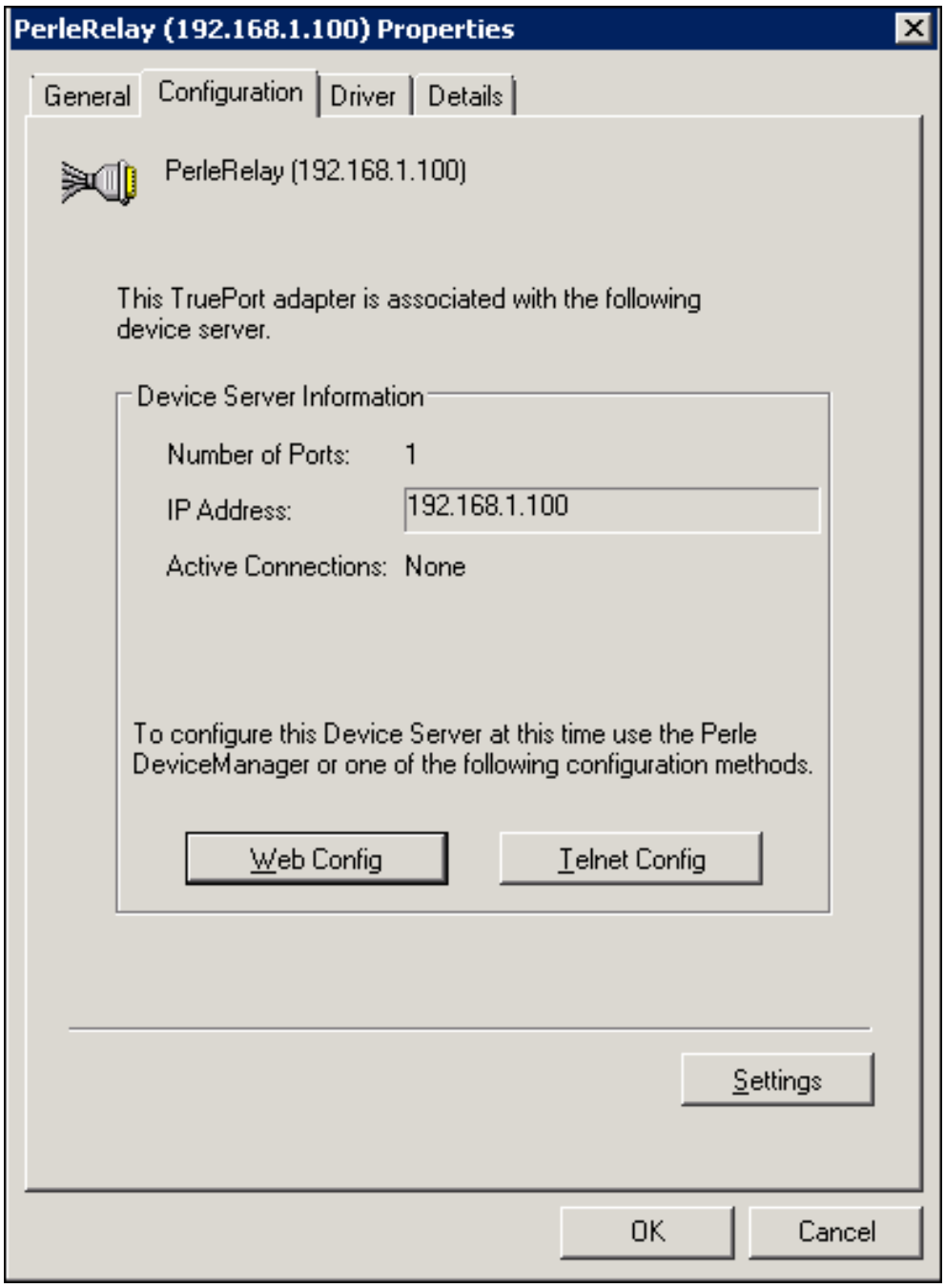
I/O Access Settings

To configure the I/O access settings, do the following:

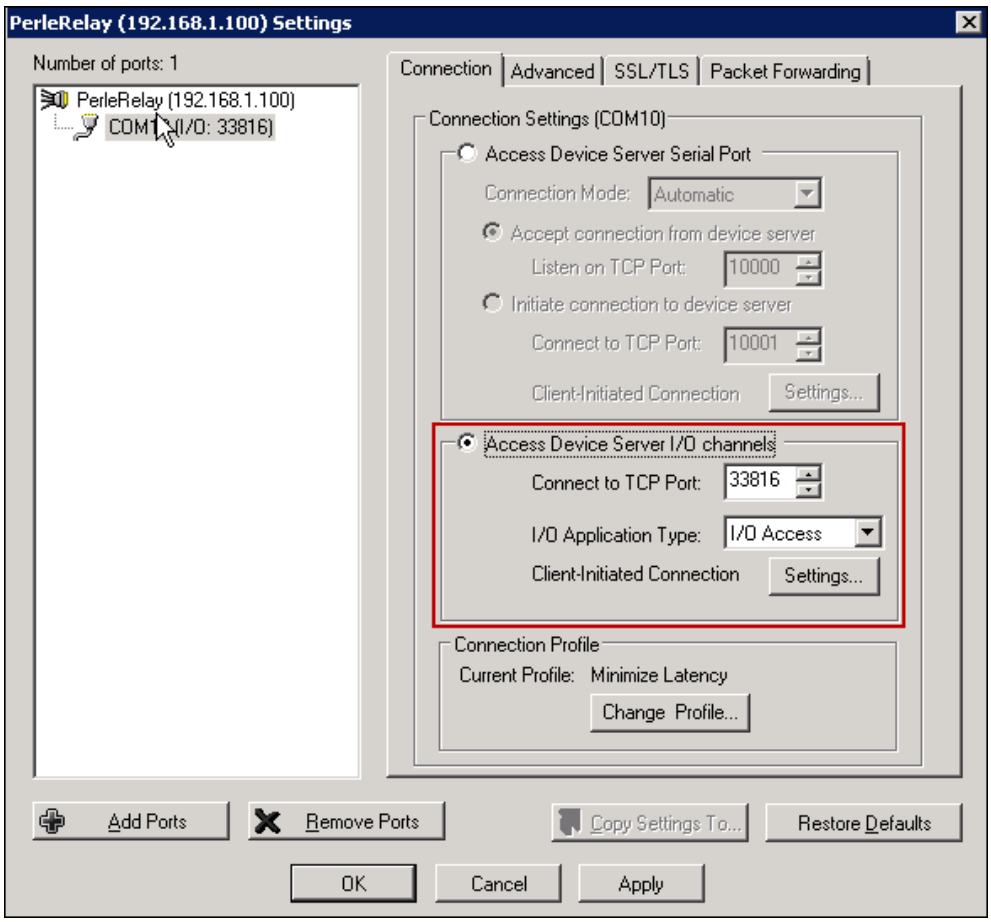
1. Start the **TruePort Management Tool**, select the Perle device to configure, and click **Properties**.



2. Select the **Configuration** tab
3. Click **Settings**.

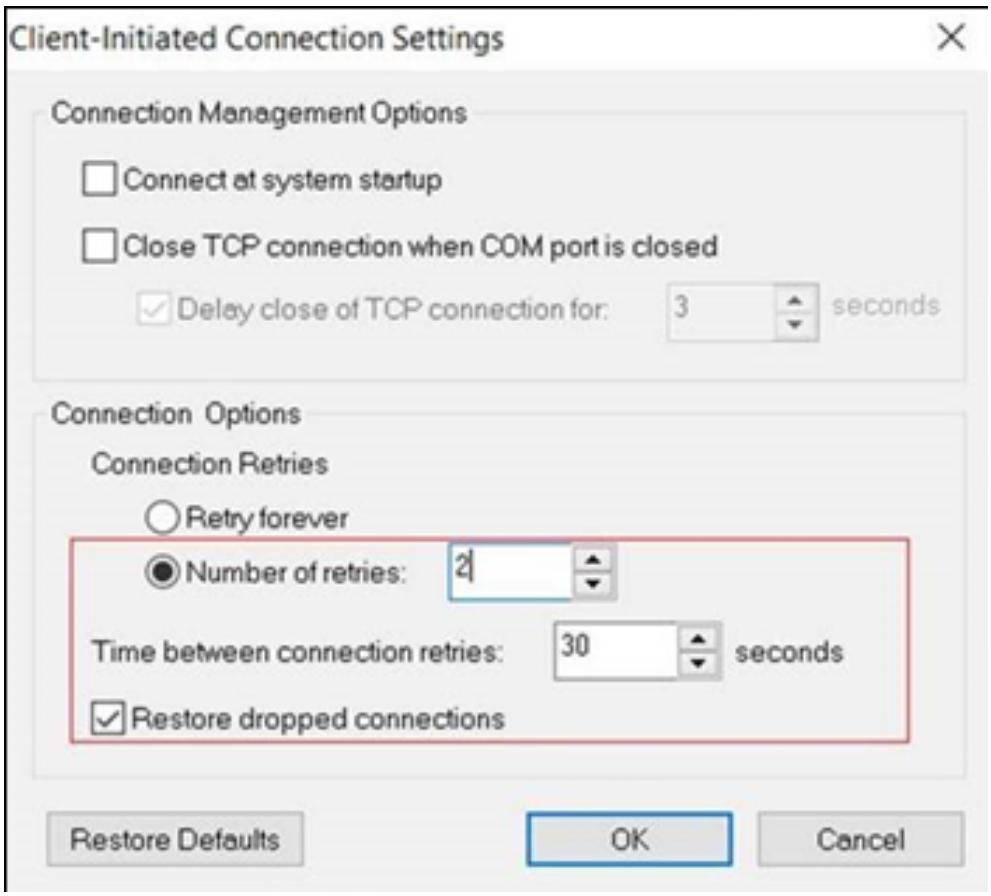


4. If there were two COM ports originally created for this device, select one to use for I/O access. If the COM port selected is being used, the other COM port should be reserved for serial communication. If a second COM port was not created, click the **Add Ports** button at the bottom of the window.
5. Select the **Connection** tab.
6. Select the **Access Device Server I/O channels** option.
7. Select the **Connect to TCP Port** that was configured on the device for I/O access.
8. In the **I/O Application Type** drop-down lsit, select **I/O Access**.

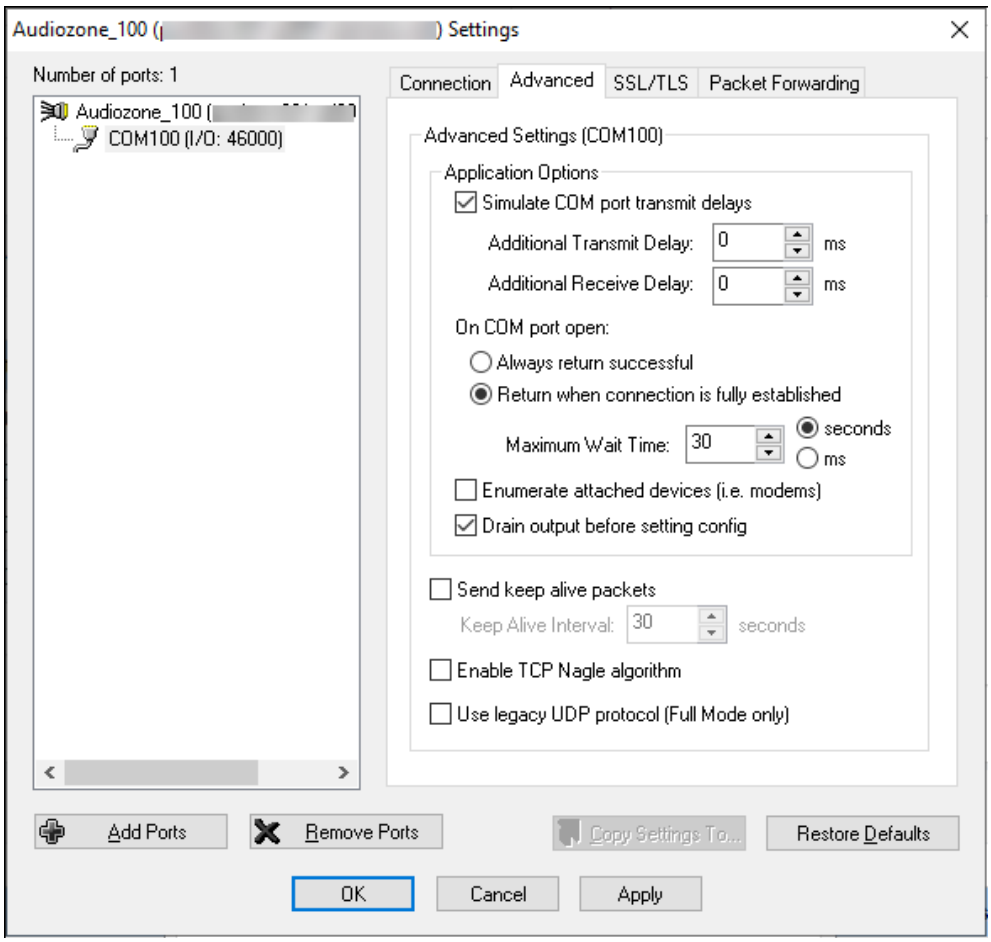


9. Click the **Settings** button next to **Client-Initiated Connection**.

   ⇨ The following window displays:

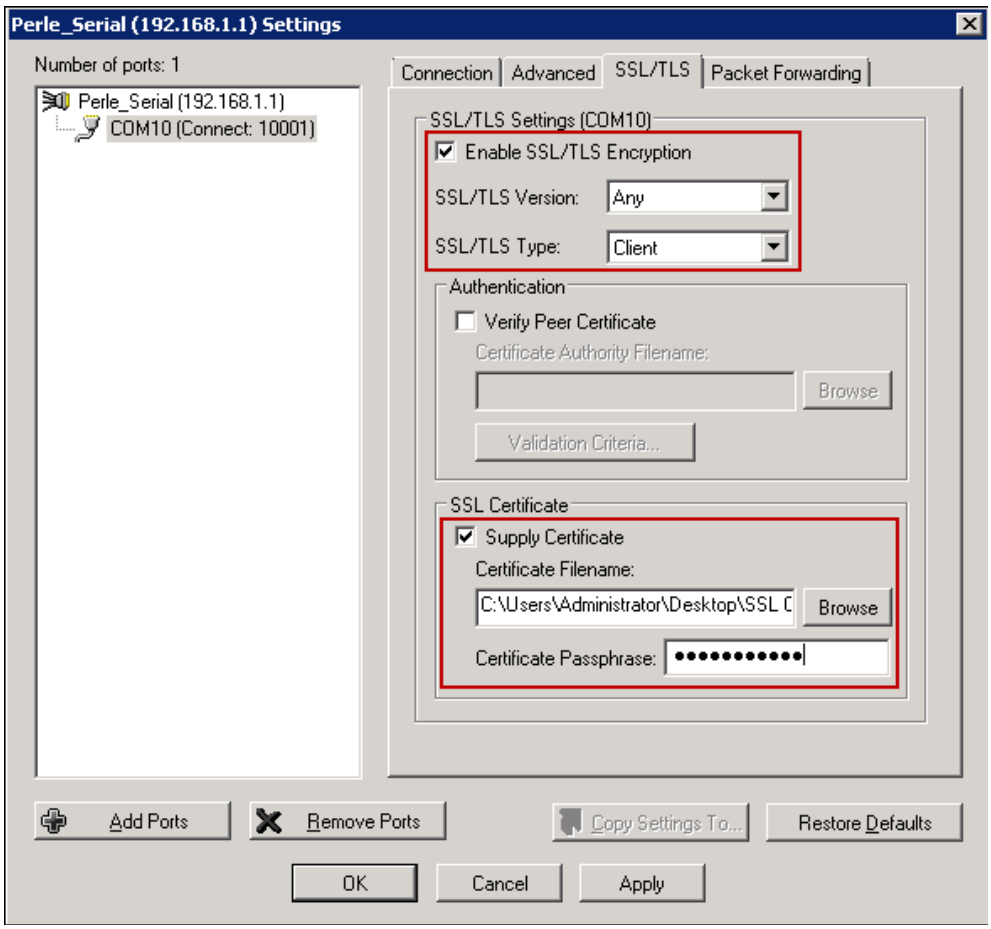


10. In the **Connection Options** section, do the settings only for the following parameters:
    - **Number of retries**: 2.
    - **Time between connection retries**: 30.
    - Select the **Restore dropped connections** check box.
11. In the **Connection Management Options** section, ensure that you do not select **Connect at system startup** and the **Close TCP connection when COM port is closed**.
12. Select the **Advanced** tab.



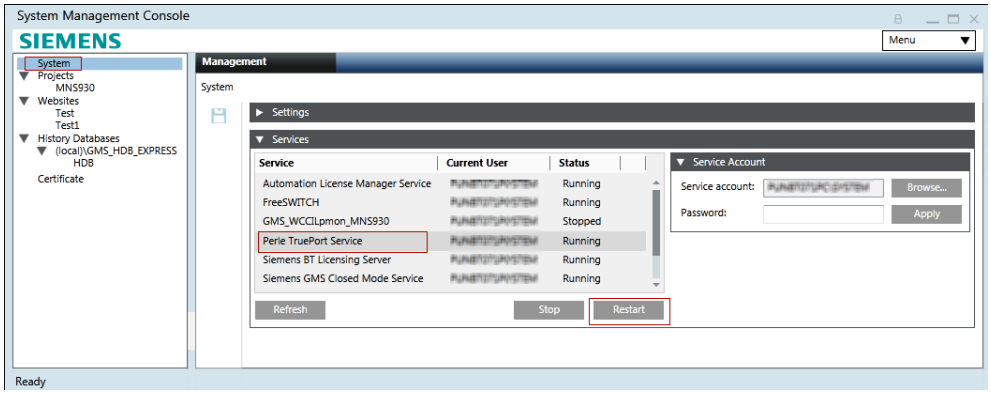
13. Set **Maximum Wait Time** to **30 seconds**.

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



15. Select the **Enable SSL/TLS Encryption** check box.
16. Set the **SSL/TLS Version** field to **Any**.
17. Set the **SSL/TLS Type** field to **Client**.
18. Select the **Supply Certificate** check box.
19. Click the browse button and select the combined Root certificate. Refer to the Device Configuration section for more information on combining a Root certificate.
20. Enter the password in the **Certificate Passphrase** field.
21. Click **Apply** and then **OK**.
22. Restart the **Perle TruePort Service** from the SMC.

⇨ The TruePort driver is ready for I/O access



Device Verification

I/O and Relays

A procedure for testing relays and I/O from the server without is yet to be determined.

Multi Zone Audio Device Troubleshooting

Device not getting Connected

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 if the device does not get connected after the **Check Status Rate** duration.

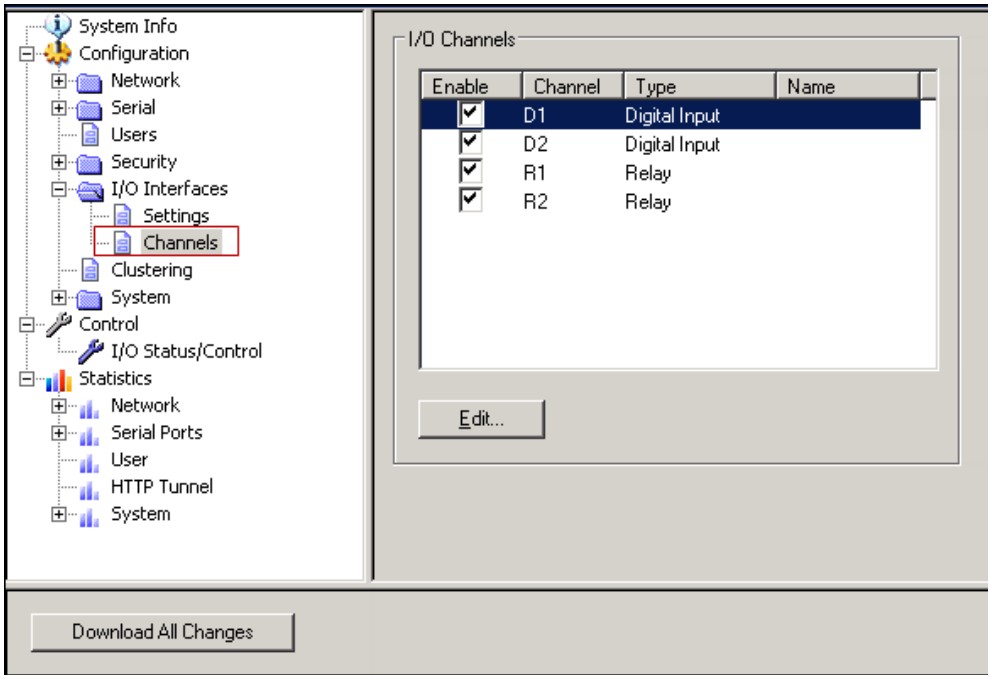
Solution: Perform the following steps in sequence until the device gets connected after a particular step. After each step, wait for the **Check Status Rate** duration and monitor the device connection status:

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.

Messages not Delivered on Audio Device

Problem: Messages are not delivered to the audio device.

Solution: Ensure that the corresponding I/O Channels are selected. To select the I/O Channels, select **I/O Interfaces > Channels** in the Device Manager of the Perle Device.



See also

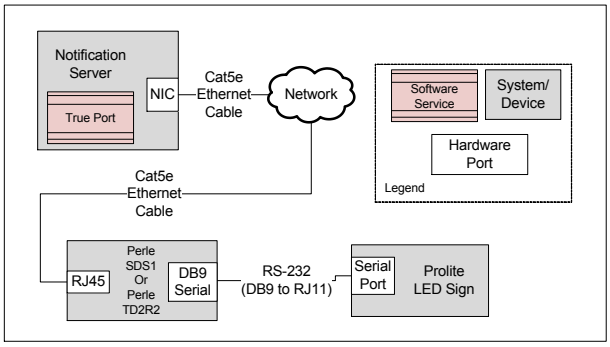
Multi Zone Audio Device [→ 263]

1.25 Pro-Lite TrucolorII LED Display

Pro-Lite TrucolorII LED Display

This section provides reference and background information for integrating the Pro-lite TrucolorII LED Display device. For procedures and workflows, see step-by-step section.

The Pro-Lite TrucolorII LED Display device provides on-premise, text-based messaging as part of the solution. It communicates serially over RS-232. Therefore, the deployment requires an IP-to-serial device to bridge the gap between the IP-based system and the serial-based LED sign.



NOTE: Currently, special characters other than ASCII are not supported by the Prolite Perle device.

Pro-Lite TrucolorII LED Display

This section provides additional procedures for integrating the Pro-lite TrucolorII LED Display device.

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

Installing Pro-Lite TrucolorII LED Display

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 present:

- Perle IOLAN SDS1
- 9-30VDC (400mA min) Power Supply, if not included with Perle IOLAN SDS1
- Category 5 Ethernet cable
- Computer or Server to communicate with the device
- The device Installation CD or a computer with network access
- DB9 RS-232 serial cable – included with Pro-Lite TrucolorII LED Display device.
  NOTE 1:
  The driver (TruePort) that is used to communicate with the device must be installed on the same server / machine that runs .
  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 DHCP.

NOTE 3:
To configure the device, a computer located on the same network is needed.
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 that the installer fasten the device to a flat surface by placing screws through mounting holes.

Power

1. For the Perle SDS1, use a power adapter capable of 9-30VDC output and 400mA. If the 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 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 the network jack.

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

Serial Connector

Plug one end of the serial cable in to the DB9 connector on the device. Connect the other end of the serial cable to the Pro-Lite TrucolorII LED Display device for serial communication.

NOTE: Keep the Console/Serial switch(s) present on the device in OFF position.

Pro-Lite TrucolorII LED Display device Installation

Prerequisites

The prerequisites for the installation of Pro-Lite TrucolorII LED Display device are as mentioned below:

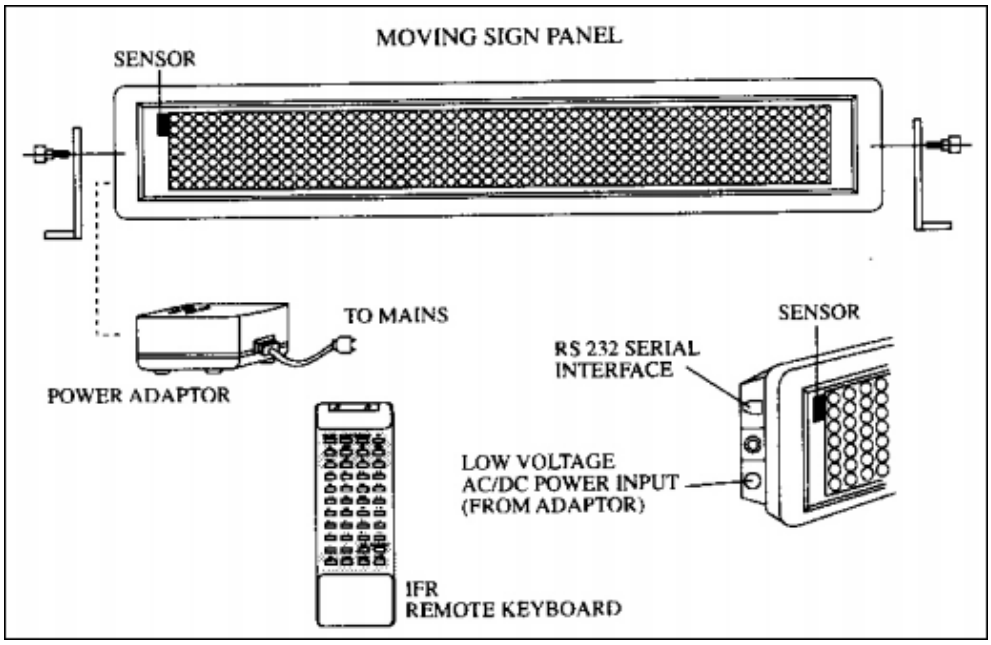
- Pro-Lite TrucolorII LED Display device with included mounting brackets
- Screws
  NOTE:
  The screw type and length should be carefully chosen based on the surface medium the device will be mounted on.

Mechanical Installation

This section includes details about the installation of the mechanical components of the device.

▷ The user must have a set of mounting brackets included in the purchase of the LED Display.

1. Measure the width between the LED Display's mounting holes.
2. Fasten the mounting brackets to the wall with a pair of screws using the width between the LED Display's mounting holes.
   NOTE: Use an appropriate screw type for the wall type (concrete, wood, dry wall, and others). The user should provide the screws to fasten the bracket to the wall.
3. Mount the LED Display to the bracket using the screws that came with the LED Display.
   NOTE: To adjust the angle of the LED Display, slightly unscrew the brackets from the LED Display, adjust the angle, and retighten the bracket.



Electrical Installation

1. Mount the LED Display to a flat surface using the two mounting brackets included with the LED Display.
2. Loosen the screw connecting the LED Display and bracket, reposition the LED Display, and then fasten the screw to adjust the angle.
3. Plug the RJ11 connector of the serial cable to the port marked **RS232** on the LED Display.
4. Connect the DB9 side of the serial cable to the **DB9** connector on the SDS1.
5. Connect the power adapter to the port marked **DC IN** on the LED Display.
6. Plug the adapter into an AC outlet.
   NOTE: If the LED Display is factory default, the user will see demo text and graphics on the LED Display.

Installation Verification

If installed and wired correctly on boot up, the LED Display details information such as baud rate, LED Display device address, and a welcome message.

NOTE: If any activity is not visible, verify that power is present.

Configuring Pro-Lite TrucolorII LED Display

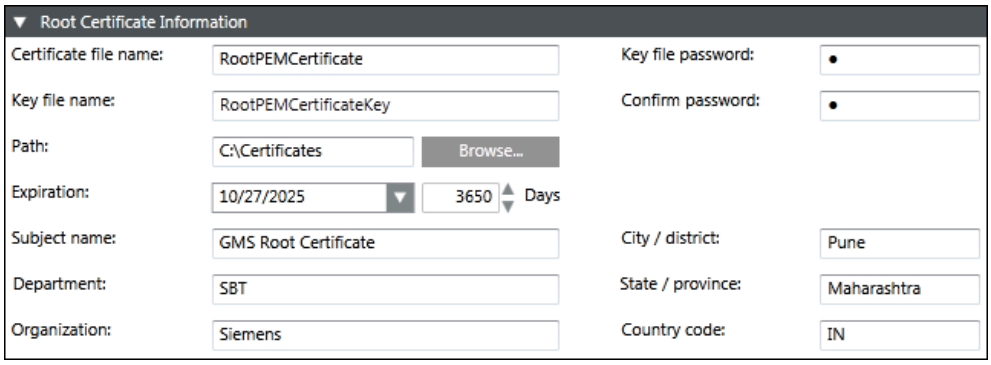
This section provides the steps linked with the configuration and verification of the device.

Certificate Creation From System Management Console

To establish a secure communication, certificates must 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.



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** to initiate root certificate creation.

⇨ 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 are 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

Configuration to communicate to the device requires two main steps. 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.

The other 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 is through the TruePort driver.

NOTE:
TruePort is a COM port re-director driver utility that is installed on the server. It 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 the remote device.

Device Configuration

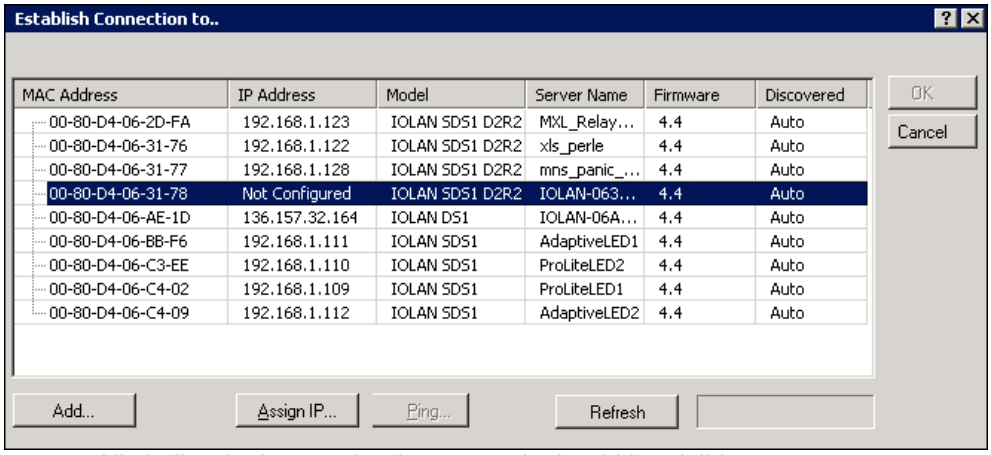
▷ Ensure that the DeviceManager is installed on a computer located under the same network as the device that will be configured.

▷ 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 cat command in command prompt, for example, **cat RootCertificateKey.pem RootCertificate.pem > RootCombineCert.pem**.

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

1. Start **DeviceManager**.

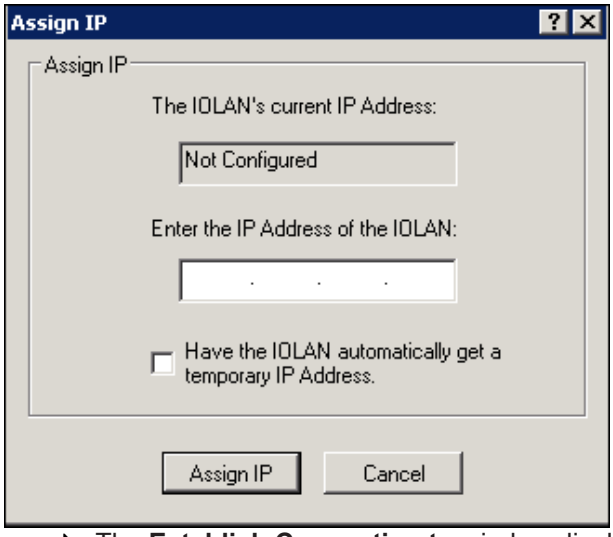


⇨ All similar devices under that network should be visible.

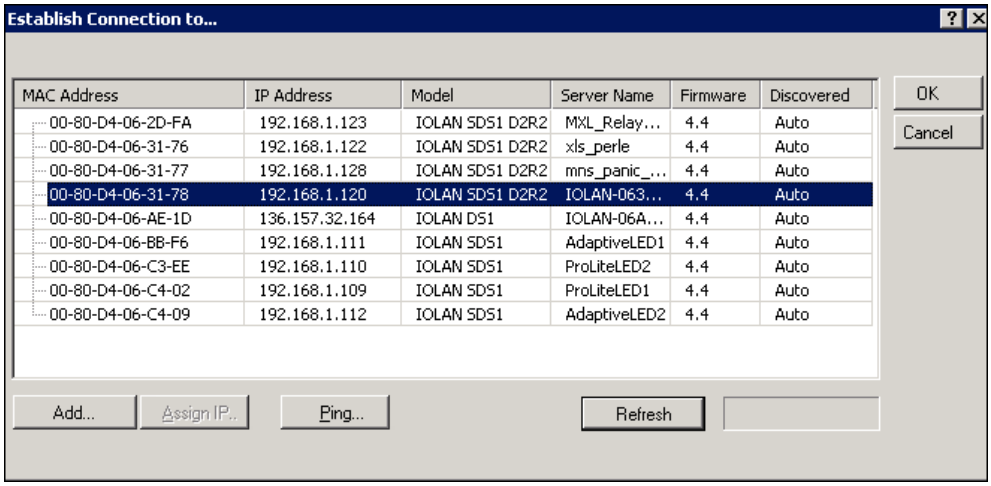
2. Select the device to configure and click **Assign IP**.
NOTE 1: If the device is not visible in the window, verify that the device has power and is connected to the network. Check the LEDs on the device; the power LED should be solid green and the link LED should be solid amber / green.
NOTE 2: If 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 device to reboot and initialize. If still unsuccessful, replace the unit or check the network.

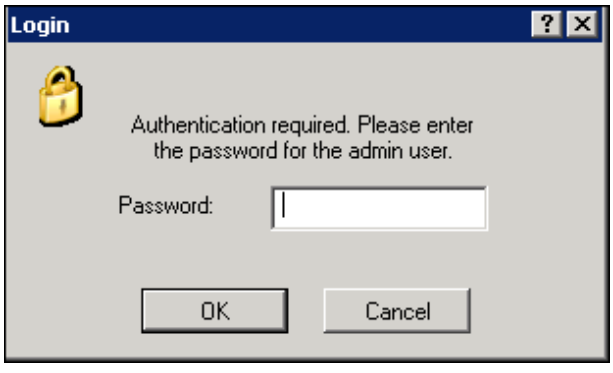
3. Manually enter an IP address or select the **Have the IOLAN automatically get a temporary IP Address** check box below to have the DHCP assign one automatically. Then click **Assign IP**.



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



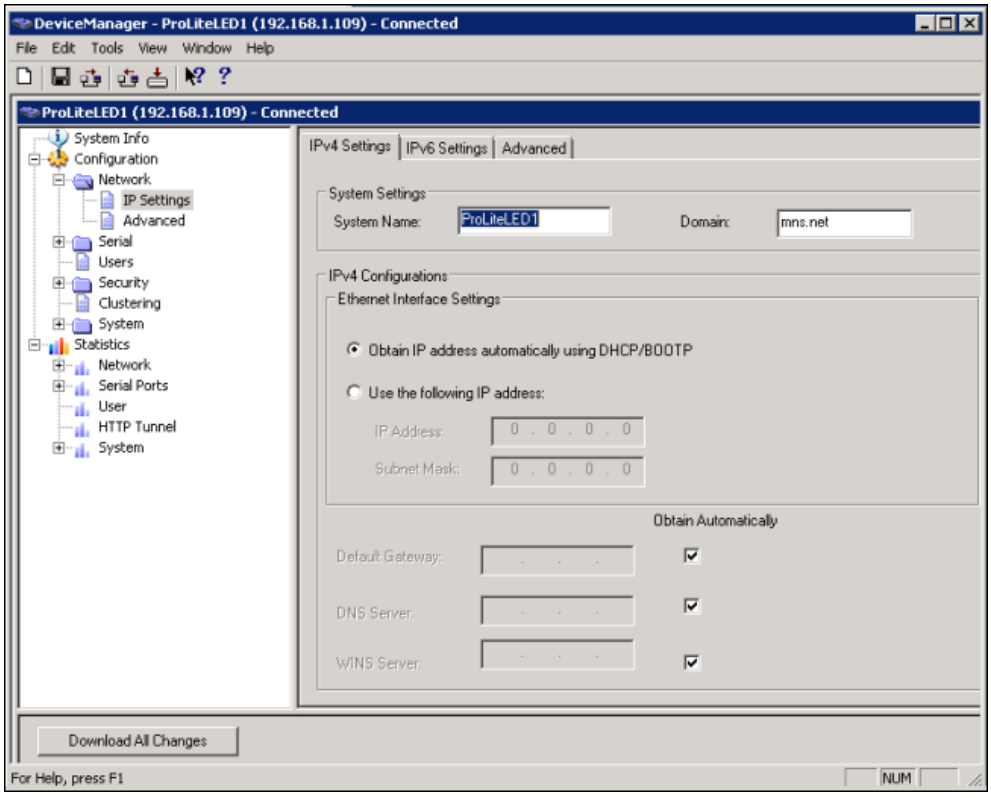
4. Select the device again, and click **OK** to log into the device for configuring.
5. At the login window, type in the device password. The factory default password is: **superuser**.



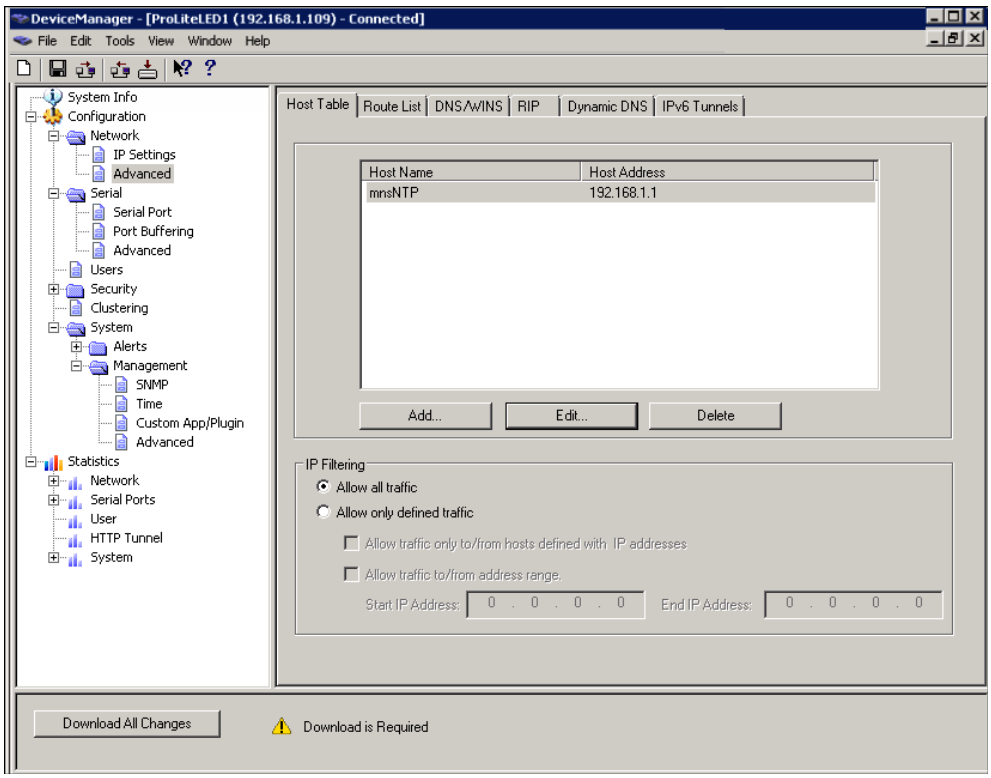
Network Setup

To further configure the network settings of the device, log into the device using DeviceManager. Proceed with 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**.



2. Select the **System Name** field, give the device a distinguishable name to help identify it 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, under the domain name used on 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**.
5. Select the **Advanced** tab.
6. Select the **Register Address in DNS** check box.
7. Select the **Advanced** tab on the left-hand side menu.



8. Select the **Host Table** tab.
9. Click **Add** to add an NTP host.
10. On the widoow, enter a descriptive name for the NTP server (for example, **mnsNTP**).
11. 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.
12. Click **OK**.

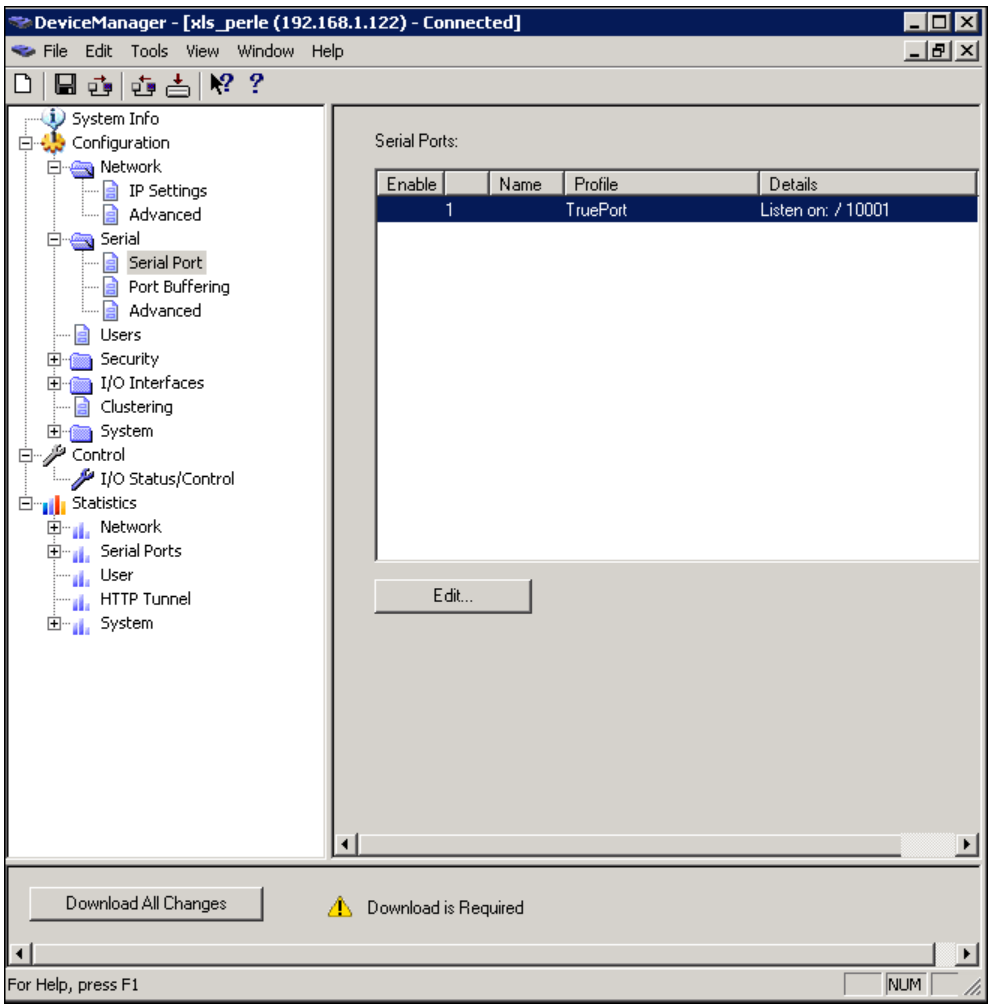
Serial Settings

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

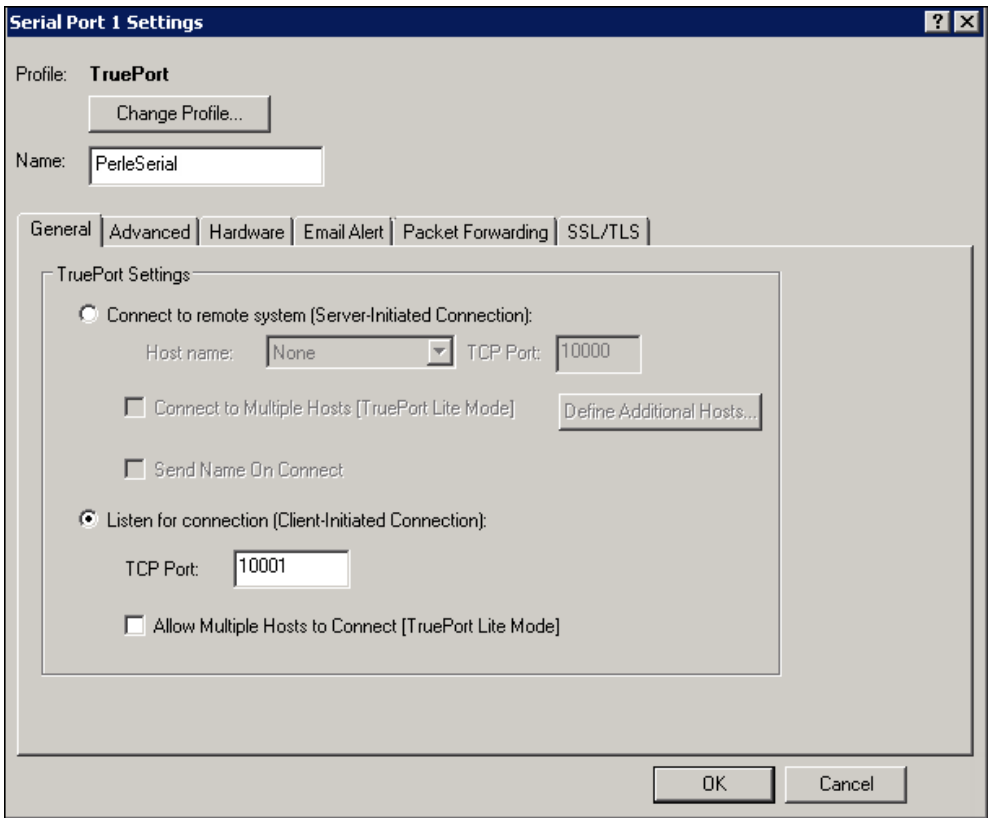
1. In the device manager window, click the **Serial** folder on the left and then **Serial Port**.

   ⇨ Begin configuring the number of serial ports and the device profile. Only one serial port per device is required for serial communication.

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



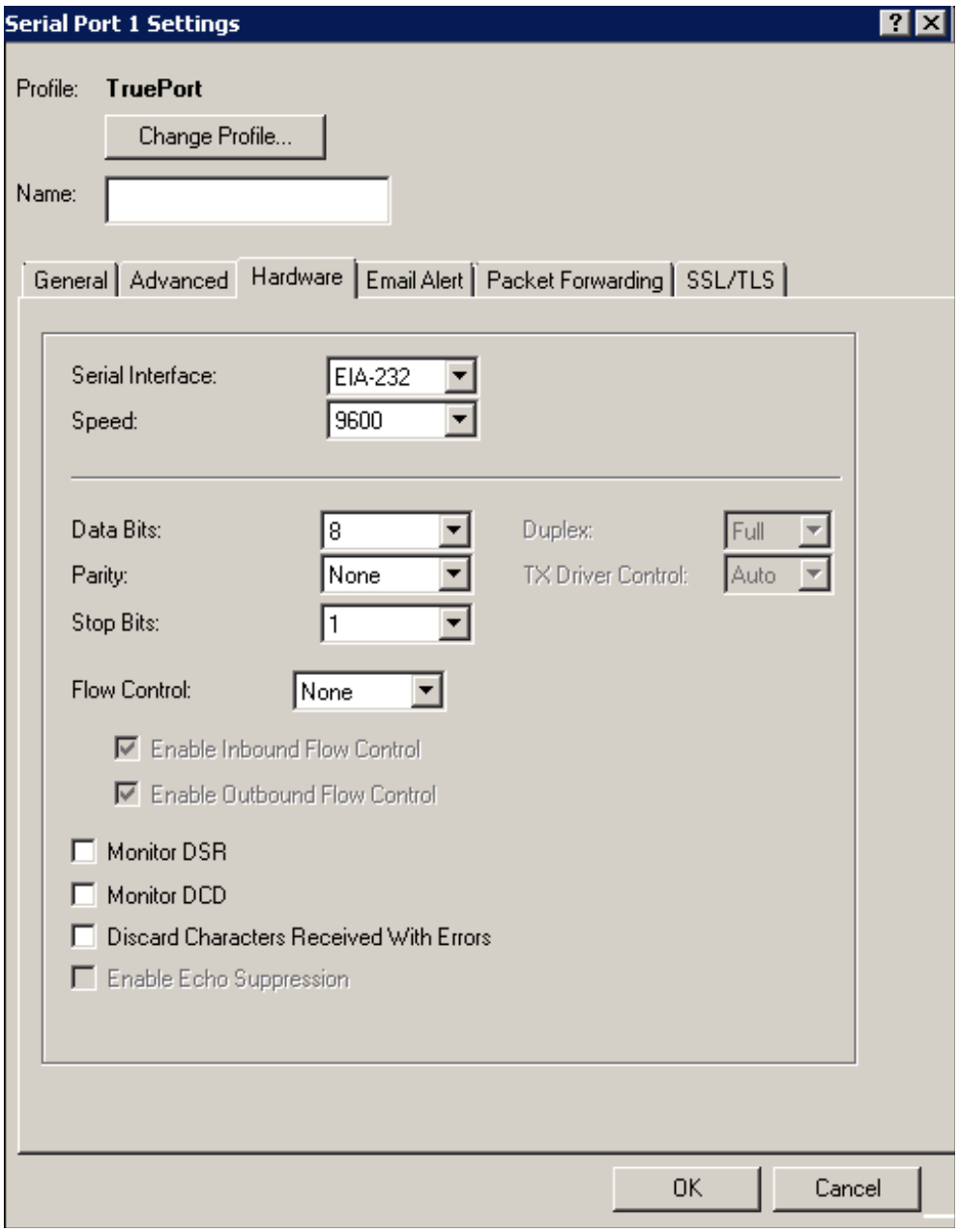
3. In the **Serial Port settings** window, click **Change Profile**. Select the **TruePort** profile and click **OK**.



⇨ The serial port settings window will change to reflect the new profile.

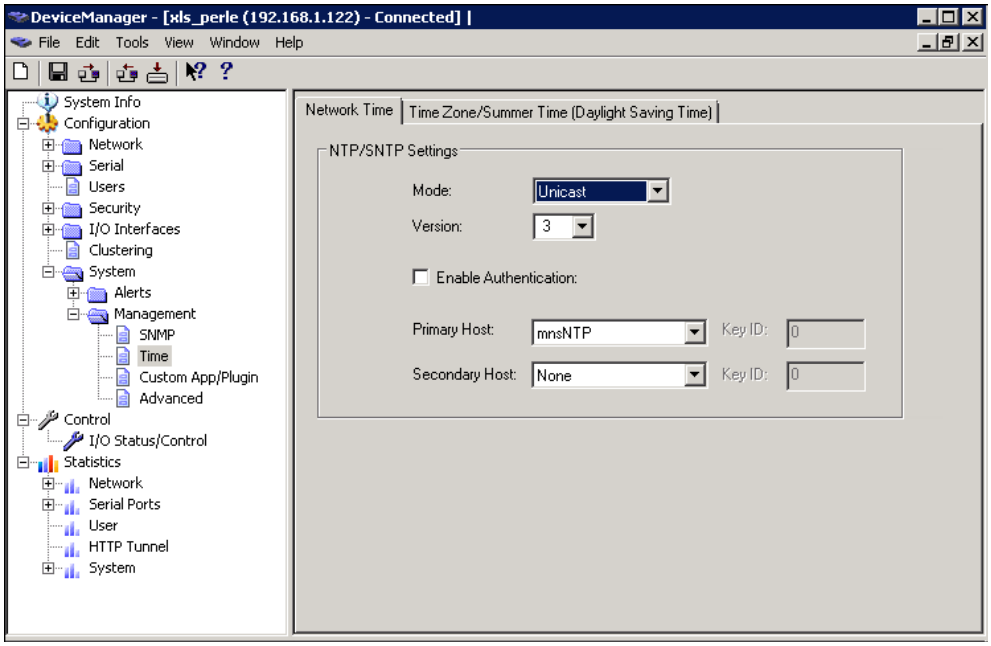
4. Select the **General** tab.
5. Click the **Listen for connection (Client-Initiated Connection)** option.

   ⇨ In this mode, the device will wait for the server to establish a connection.
6. Enter the TCP port that will communicate 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.
7. Ensure that the **Allow Multiple Hosts to Connect [TruePort Lite Mode]** check box is unselected. Click **OK**.
8. Select the **Hardware** tab.

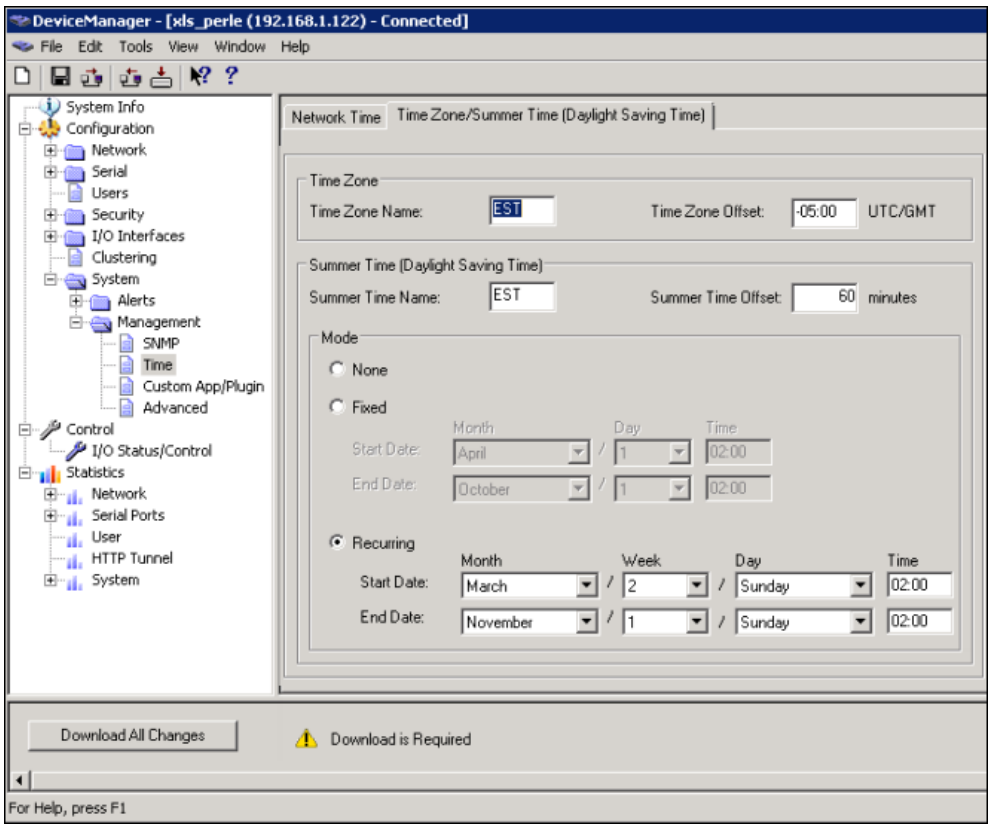


9. Select **EIA-232** (RS-232).
10. Set Speed to **9600**.
11. Set Data Bits to **8**.
12. Set Parity to **None**.
13. Set Stop Bits to **1**.
14. Set Flow Control to **None**.
15. Do not select the **Monitor DSR** check box.
16. Do not select the **Monitor DCD** check box.
17. Do not select the **Discard Characters Received With Errors** check box.
18. Select the **SSL/TLS** tab.
19. Select the following check boxes:
    Enable SSL/TLS
    Use Global settings (**Security > SSL/TLS**)
20. Click **OK**.

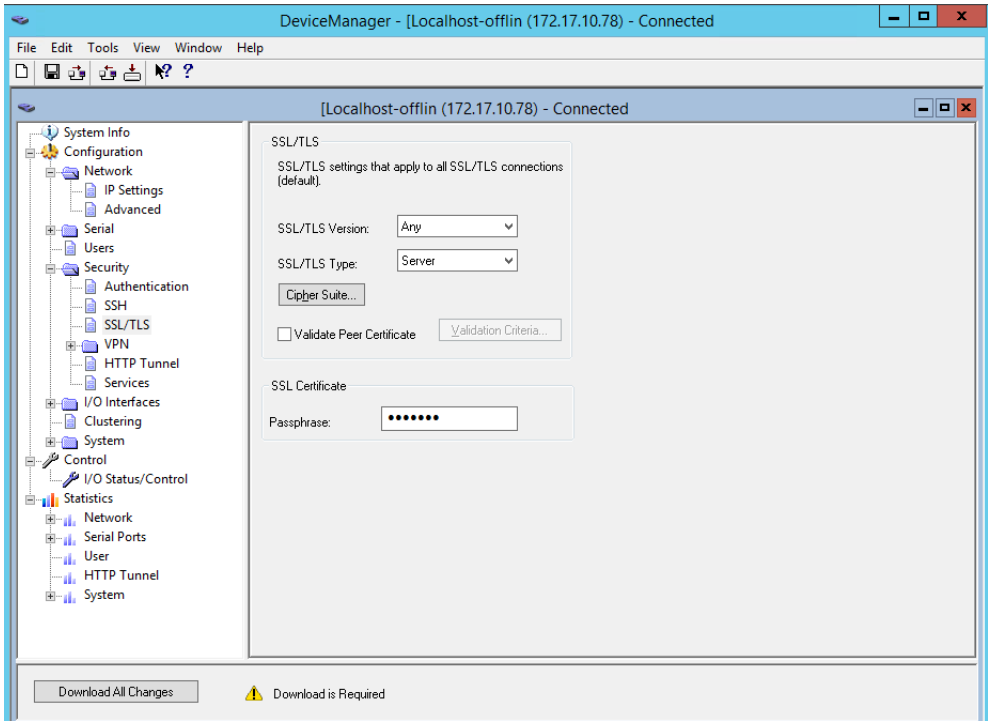
21. Select **Configuration > System > Management > Time**.
22. Select the **Network Time** tab.
23. Set the following parameters.
    - **Mode:** Unicast
    - **Version:** 3
    - Leave the **Enable Authentication** check box unselected.
    - **Primary Host:** Select the NTP server name created earlier.
    - **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. If unsure, then verify with the client's network administrator.



24. Select the **Time Zone/Summer Time (Daylight Saving Time)** tab.
25. Configure the parameters as per the details mentioned in Time Zone/Summer Time (Daylight Saving Time) parameters.



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

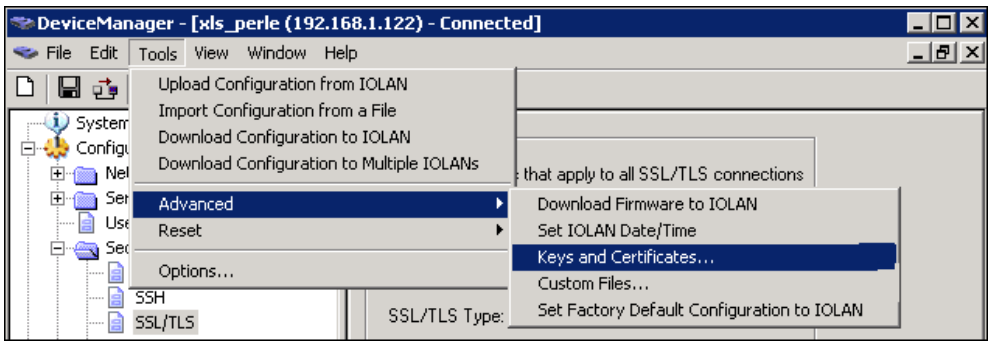


27. Set **SSL/TLS Version** field to **Any**.

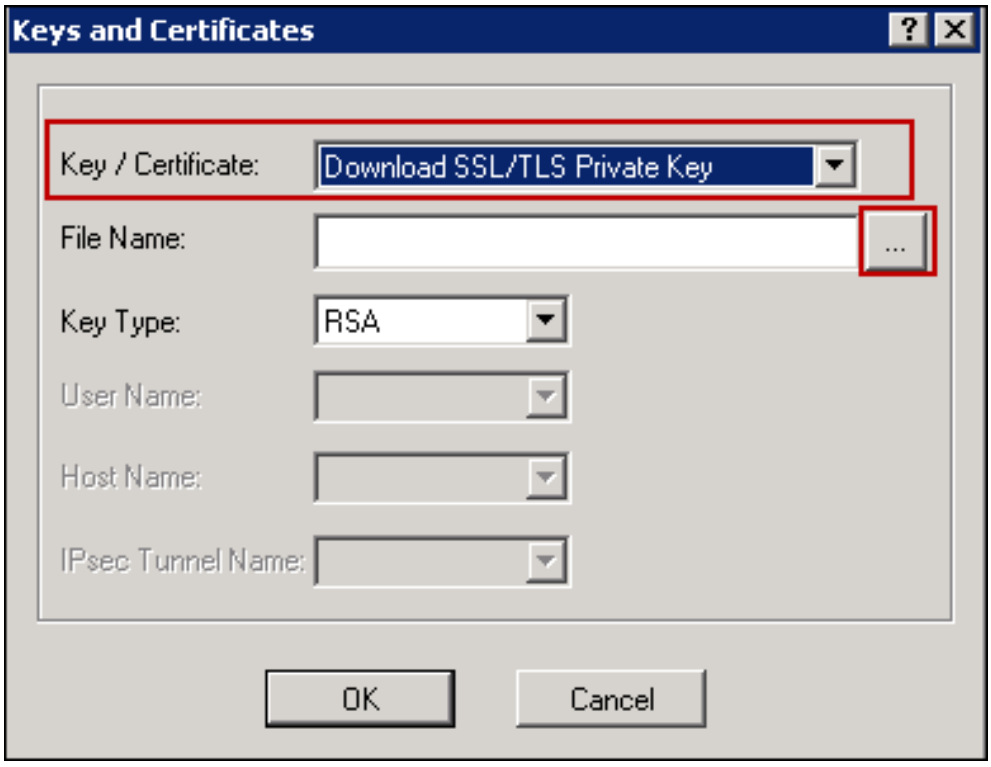
28. Set **SSL/TLS Type** field to **Server**.

29. Select the **SSL Certificate** section, enter the password of the SSL certificate in the **Passphrase** field.

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



31. In the **Key/Certificate** drop-down list, select **Download SSL/TLS Private Key**.
32. Click the browse button and upload the private key for the root certificate(pem).
33. Click **OK**.



34. Select **Tools > Advanced > Keys and Certificates**.
35. In the **Key/Certificate** drop-down list, select **Download SSL/TLS Certificate**.
36. 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.
37. Click **OK**.
38. Select **Tools > Advanced > Keys and Certificates**.
39. In the **Key/Certificate** drop-down list, select **Download SSL/TLS CA**.
40. Click the browse button and upload the upload the root certificate (RootCertificate.pem file).
41. Click **OK**.

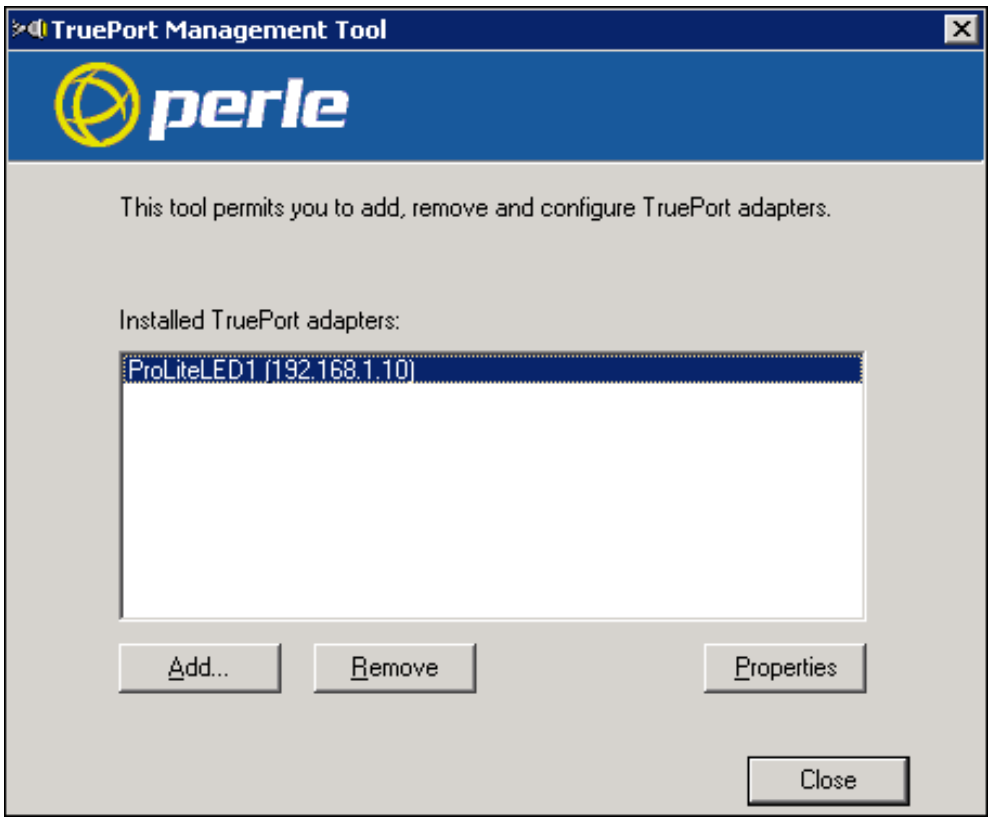
42. Click **Download All Changes** to make the changes to the device.
43. Click **Reboot IOLAN**.
    NOTE: Any time a reboot of the device is needed, or power is reconnected, the user must wait 90 seconds for the device to reboot and initialize. When ready, the Power LED will be solid green and the Link LED will be solid amber or green.

⇨ The device is now configured.

TruePort Driver Configuration

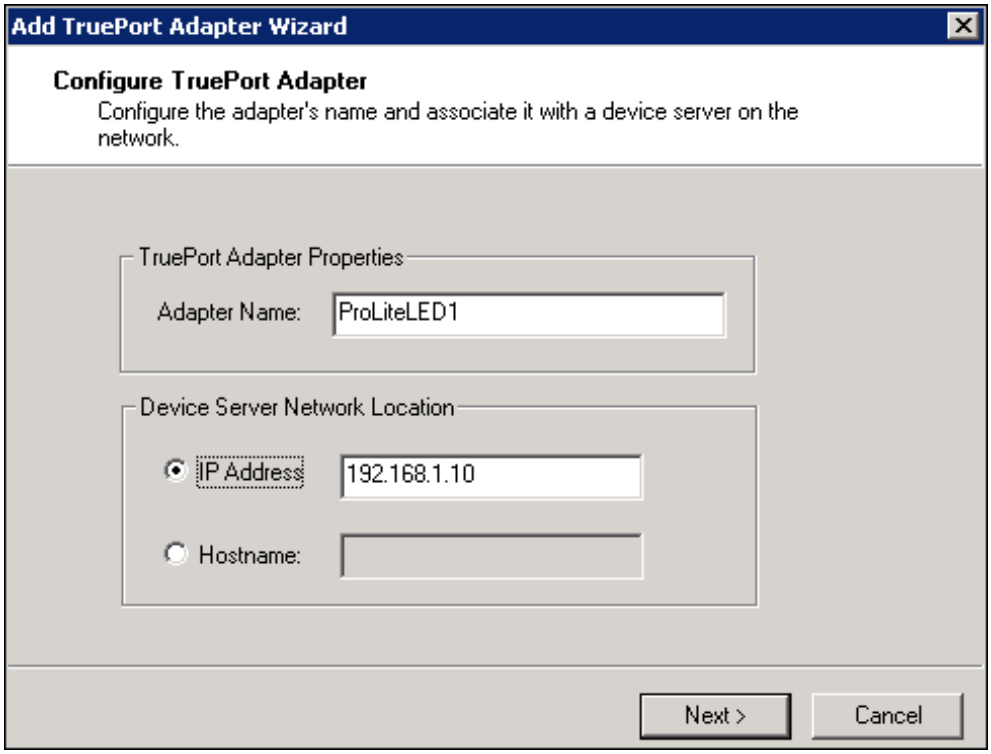
▷ The TruePort driver is the second part of the process to link the device to the server. TruePort is only used when the device is configured to use the TruePort profile. The TruePort driver is designed to manage all similar devices communicating with the server. Since TruePort creates a virtual COM port, it is recommended that each device has its own and 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 **Management Tool** window, click **Add**.

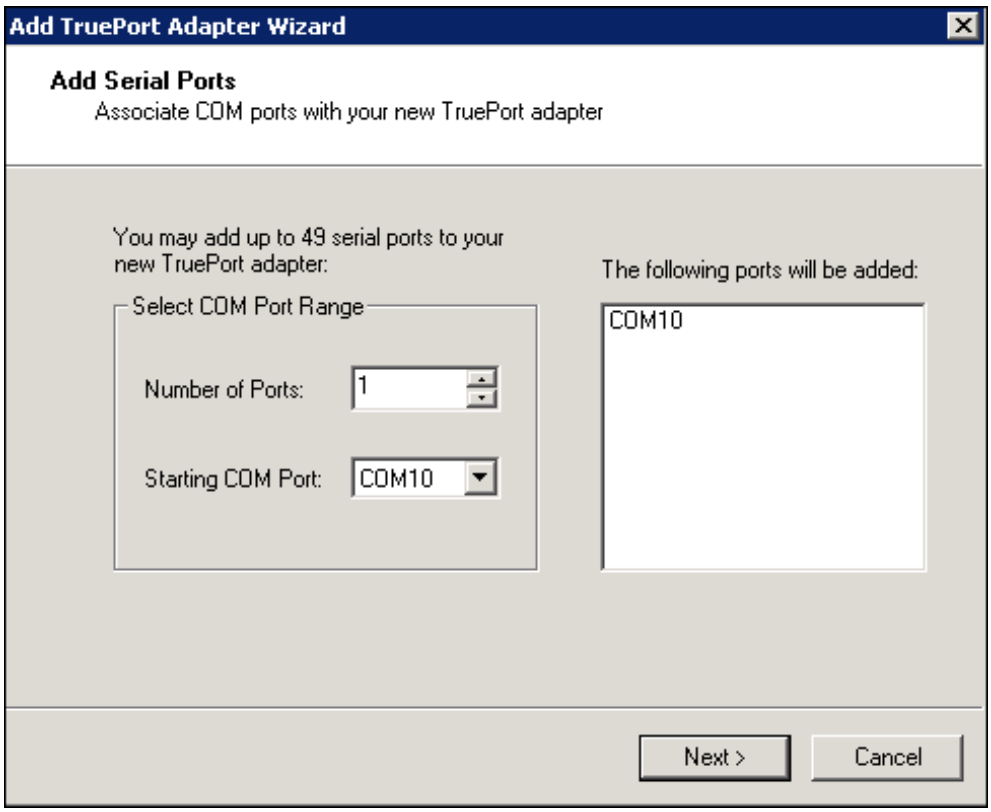


4. Enter a name for the TruePort Adapter.
   NOTE: This Adapter will serve a particular device and therefore map to a specific COM port. Try to make the name descriptive so that the Adapter can easily be tracked back to a particular device.

5. Enter the IP address or the hostname the device is using, and click **Next**.



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 add incrementally for each device and service configured. This will help to avoid any conflicts with existing COM ports or other devices. TruePort allows creation of up to 4,096 COM ports.
7. Click **Next**.



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

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

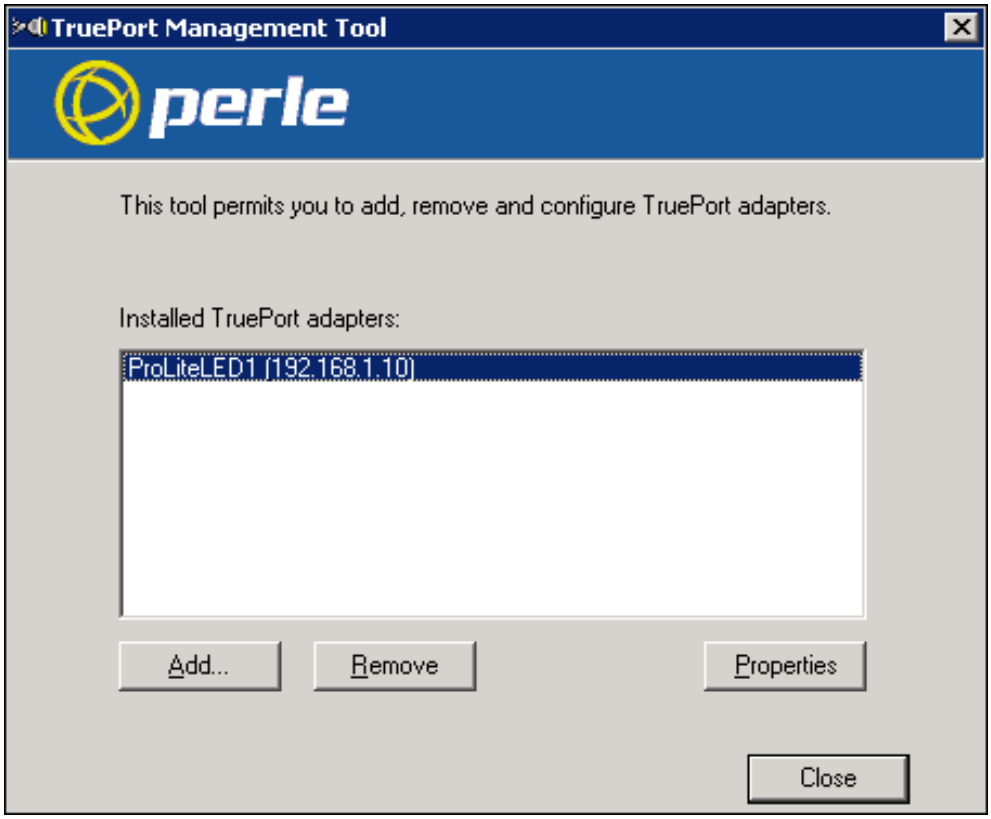
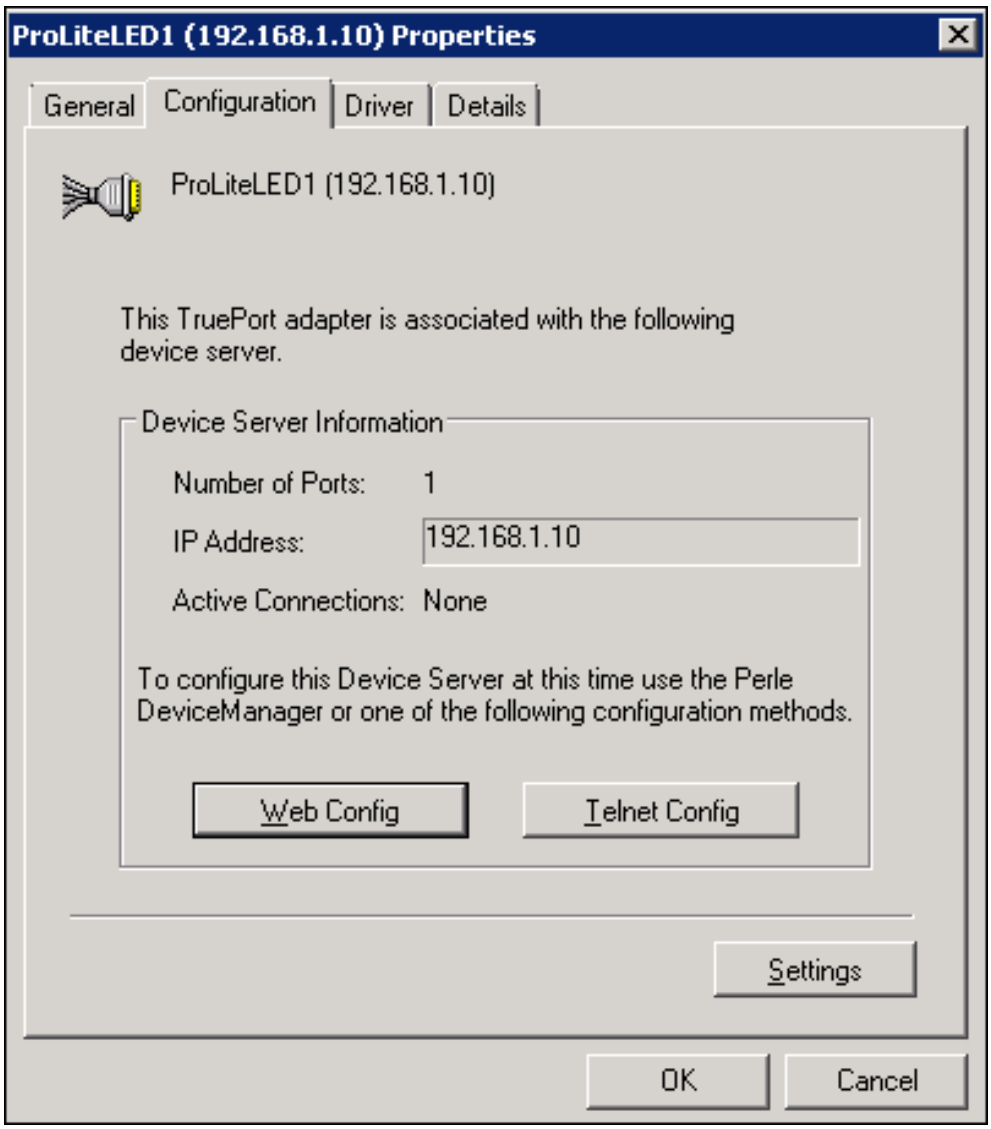


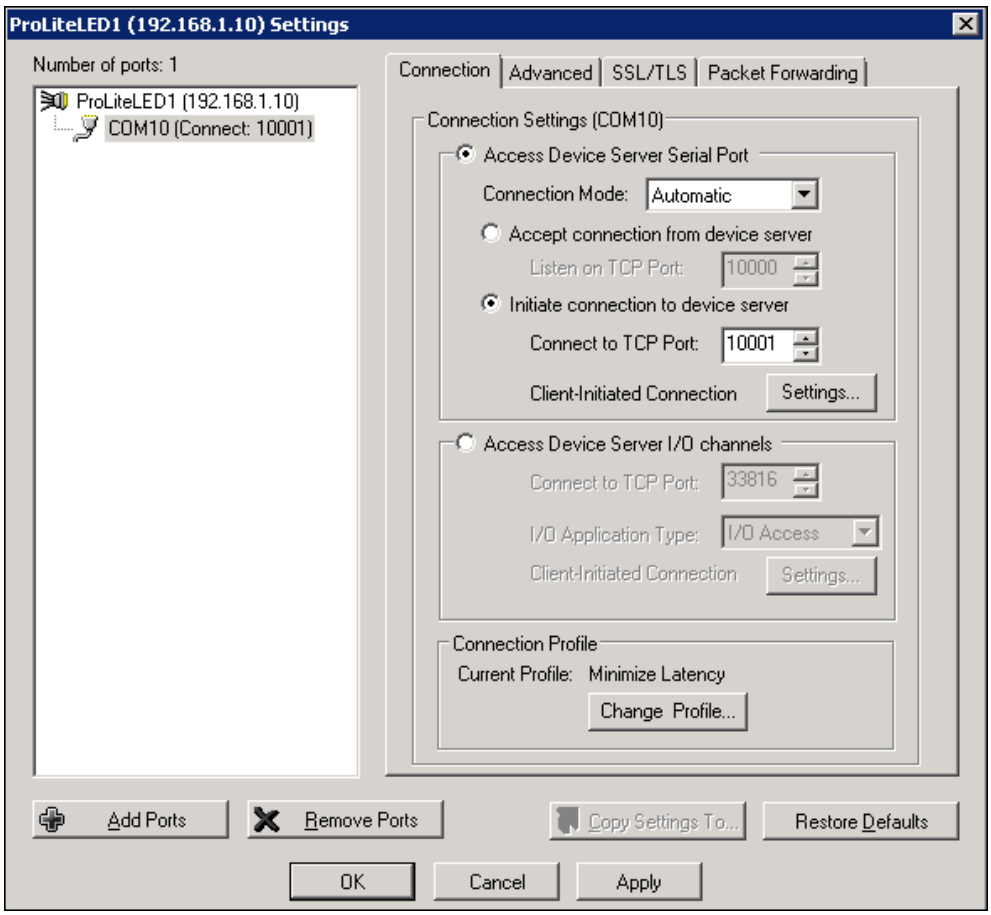
Fig. 39: TruePort Management Tool

Serial Settings

1. Select the properties window of the device port to be configured.
2. Select the **Configuration** tab.
3. Click **Settings**.



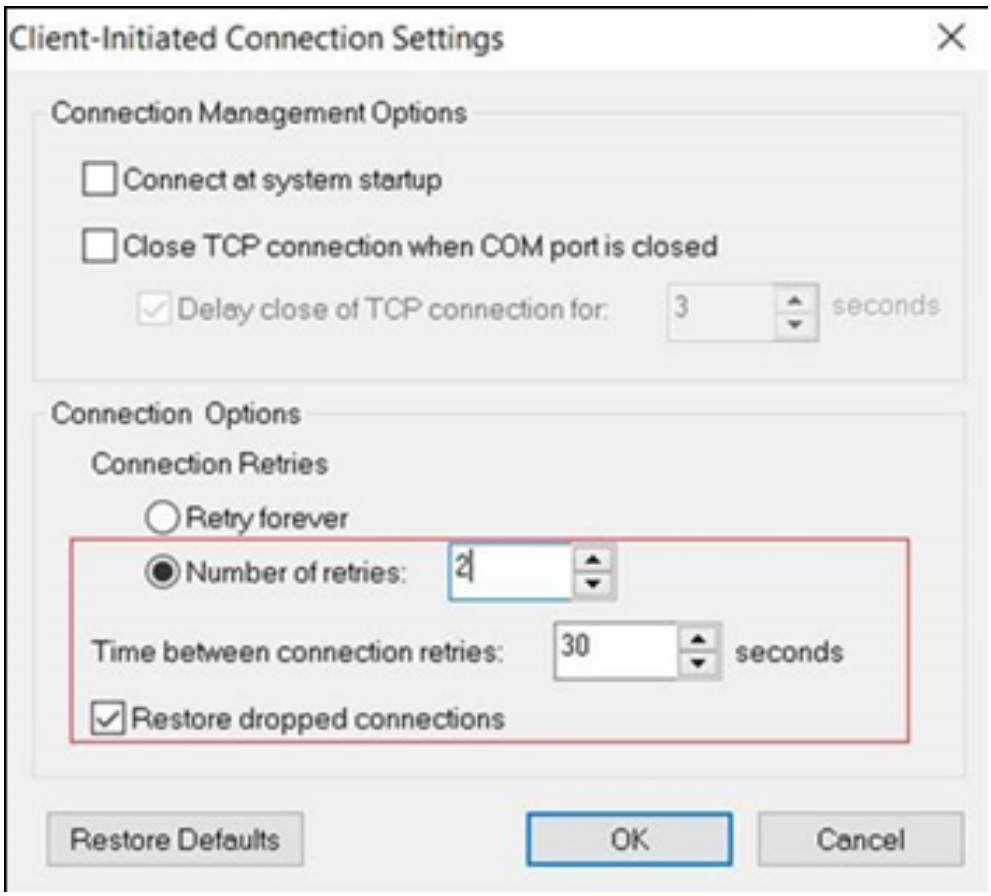
4. Click the COM port on the left-hand side.
   ⇨ This will display the TruePort and COM port settings for this adapter.
5. Select the **Connection** Tab.
6. Select the **Initiate connection to device server** option.



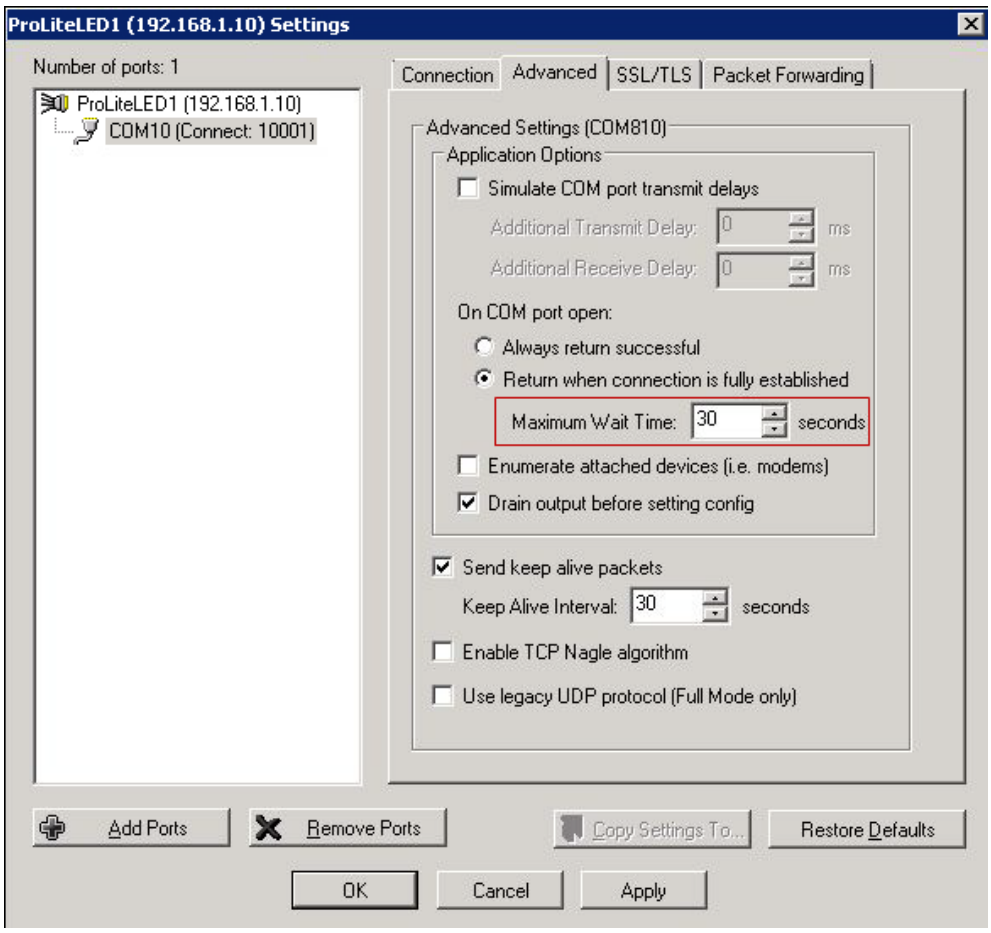
– Select **Connect to TCP Port**, enter the port number that was previously assigned to the device using the device manager.

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

   ⇨ The following window displays.

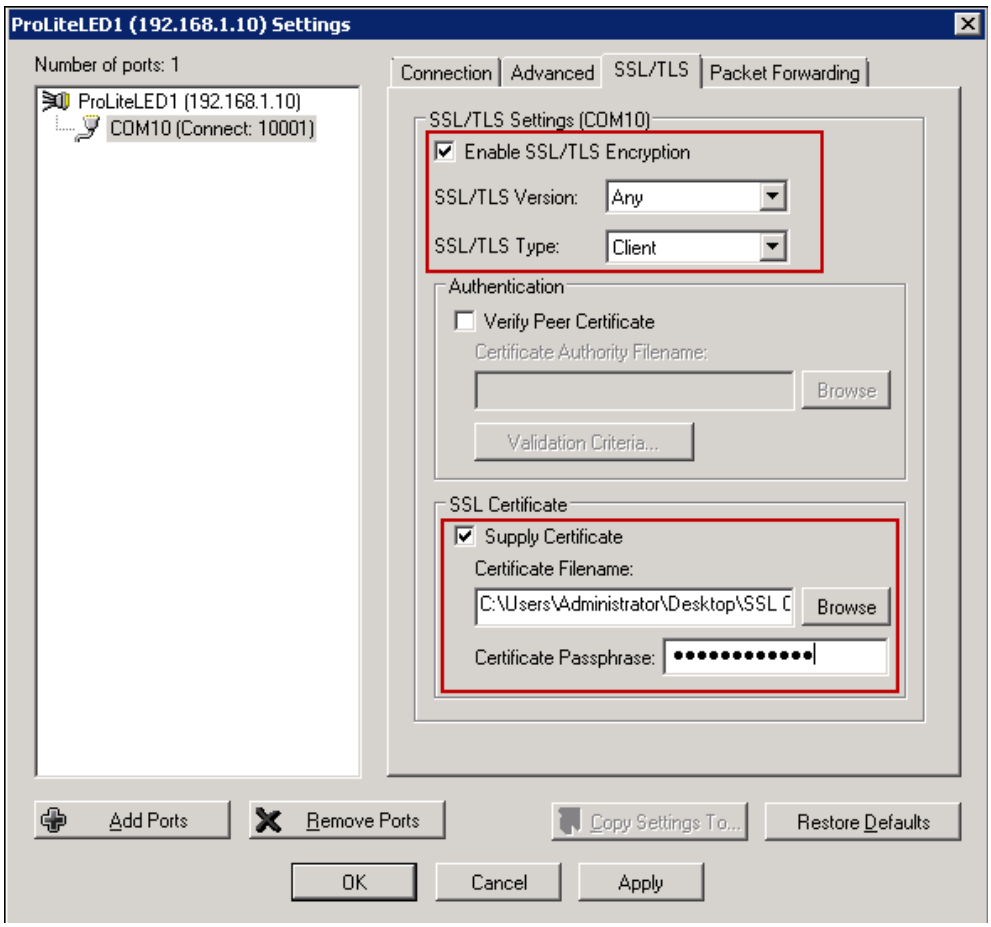


8. Select the **Connect at system startup** check box.
9. For **Connection Retries**, select the **Retry forever** option.
10. Click **OK**.
11. Select the **Advanced** tab.

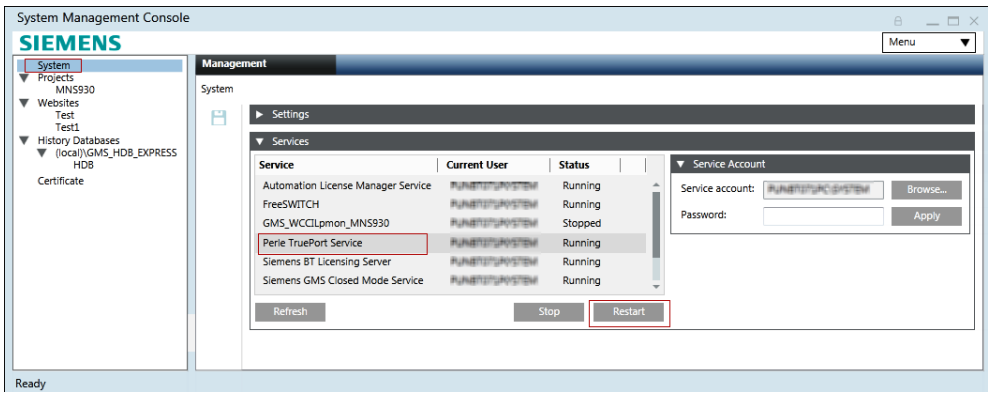


12. Set **Maximum Wait Time** to **30 seconds**.

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



14. Select the **Enable SSL/TLS Encryption** check box.
15. Set the **SSL/TLS Version** field to **Any**.
16. Set the **SSL/TLS Type** field to **Client**.
17. Select the **Supply Certificate** check box.
18. Click the browse button and select the combined Root certificate. Refer to the Device Configuration section for more information on combining a Root certificate.
19. Enter the password in the **Certificate Passphrase** field.
20. Click **Apply** and then **OK**.
21. Restart the **Perle TruePort Service** from the SMC.



Device Verification

Test the settings of the TruePort application and Perle SDS1 device by connecting the device to the Pro-Lite TrucolorII LED Display and sending a message directly using a serial terminal, such as PuTTY.

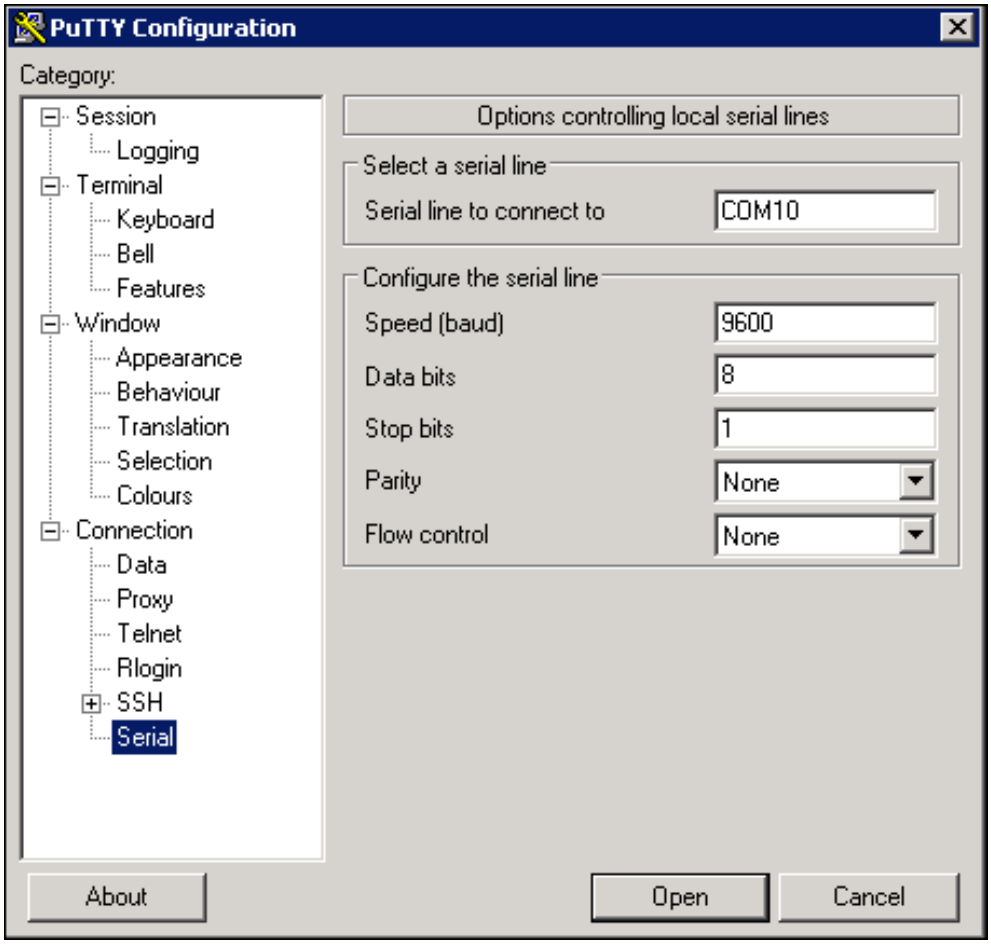
PuTTY can be downloaded from the following link:

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

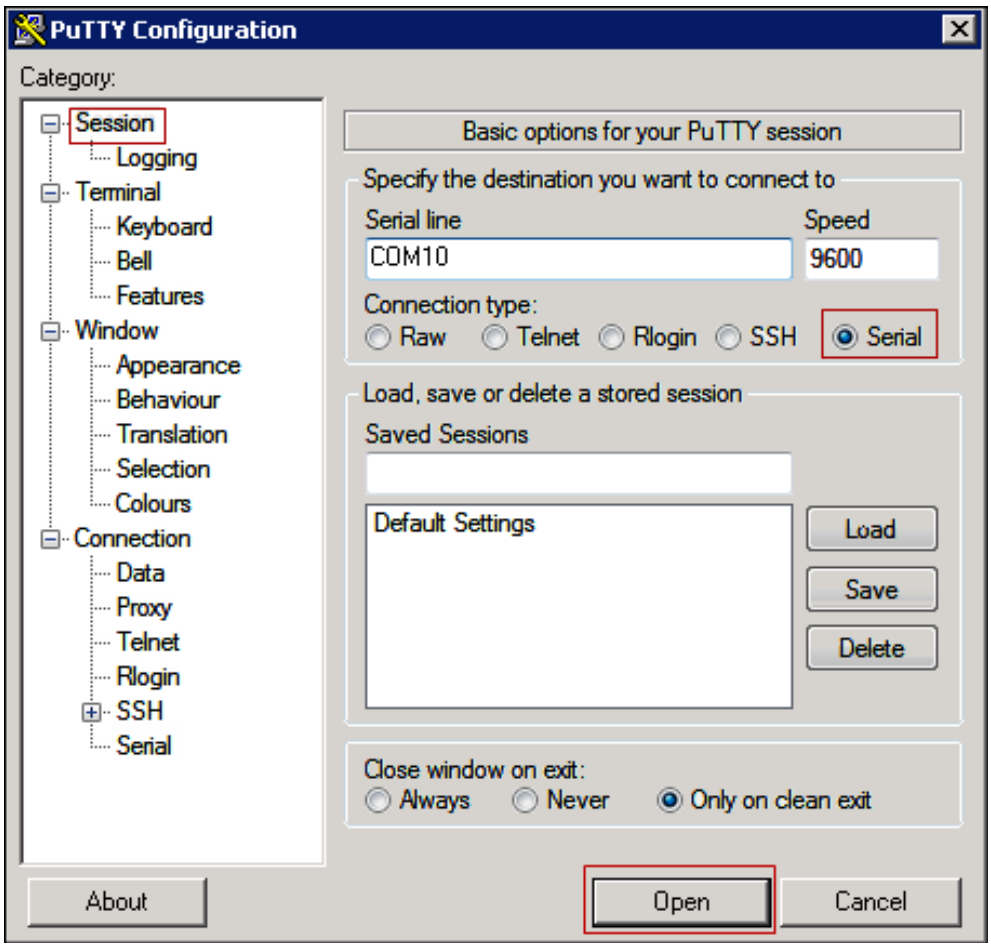
To test the serial port, open up a HyperTerminal or PuTTY session from the server on the serial COM port. If the COM port can be opened, the TruePort driver is working properly.

The steps for testing Pro-Lite 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 the TruePort Driver Configuration section.
3. Enter the parameters for Baud rate, data bits, stop bits, parity, and flow control for the external device that will be transmitting ASCII data.
   - **Baud Rate:** 9600
   - **Data Bits:** 8
   - **Stop Bits:** 1
   - **Parity:** None
   - **Flow Control:** None



4. Click **Session**, select the **Serial** option.
5. Click **Open**.



6. Enter the command **<ID00><PA>Test** and send the command through the terminal application.
   NOTE 1: Ensure that the terminal application is configured to send a character return and line feed when the user presses **Send** or **Enter**.
   NOTE 2: If a message similar to **<ID01>E** is received without any messages appearing on the sign, then an error has occurred. Check the COM port settings and message syntax.

Pro-Lite TrucolorII LED Display 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.

1.26 Prolite with Ethernet Support

Prolite with Ethernet Support

This section provides additional procedures for Prolite with Ethernet Support.

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

Installing AND 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:

- Advanced Network Device (AND) IP Display or IP Speaker
- Cat5e Ethernet Cable

The optional prerequisite includes:

- Ethernet Power Injector

Mechanical Installation

1. Remove the back frame by removing the four Torx screws on the side of the device.
2. Mount the back frame to a flat surface by placing screws through the eight mounting holes located on the frame.

⇨ The mechanical installation of the device is now complete.

Electrical Installation

1. Connect the Ethernet cable to the Ethernet port on the back of the device.
2. Connect the other end to the power injector or a PoE capable switch/hub/router.
   NOTE: The AND IP Displays and IP Speakers are Power over Ethernet (PoE) only devices. They receive all of their power over the Ethernet cable.
3. Verify that the network is PoE ready.
   NOTE: If the network is not PoE ready, a power injector must be purchased and installed.

⇨ The device boot process is started.

Installation Verification

On successful connection, the LED sign will display the following in sequence:

- Advanced Network Devices
- Firmware
- MAC
- IP Address
  NOTE 1:
  If nothing is displayed when Ethernet cable is connected, verify that PoE is available.
  NOTE 2:
  If the Dynamic Host Configuration Protocol (DHCP) with a rotating bar is displayed, then the device is unable to obtain an IP address. Check with the local site administrator for the DHCP availability. A DHCP server is required during the first reboot in order for the AND sign to obtain an initial IP address. After an initial IP address is obtained, the sign can be reconfigured with a static IP address.

Configuring AND Device

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:

- Computer connected to the same subnet as the IP Display or IP Speaker.
- Web browser for accessing the IP Display‘s or IP Speaker‘s internal web server.

Device Configuration

After the completion of the boot up process, the device will request an IP address through DHCP. Upon receiving the IP address, the device will display it before returning to the normal operation.

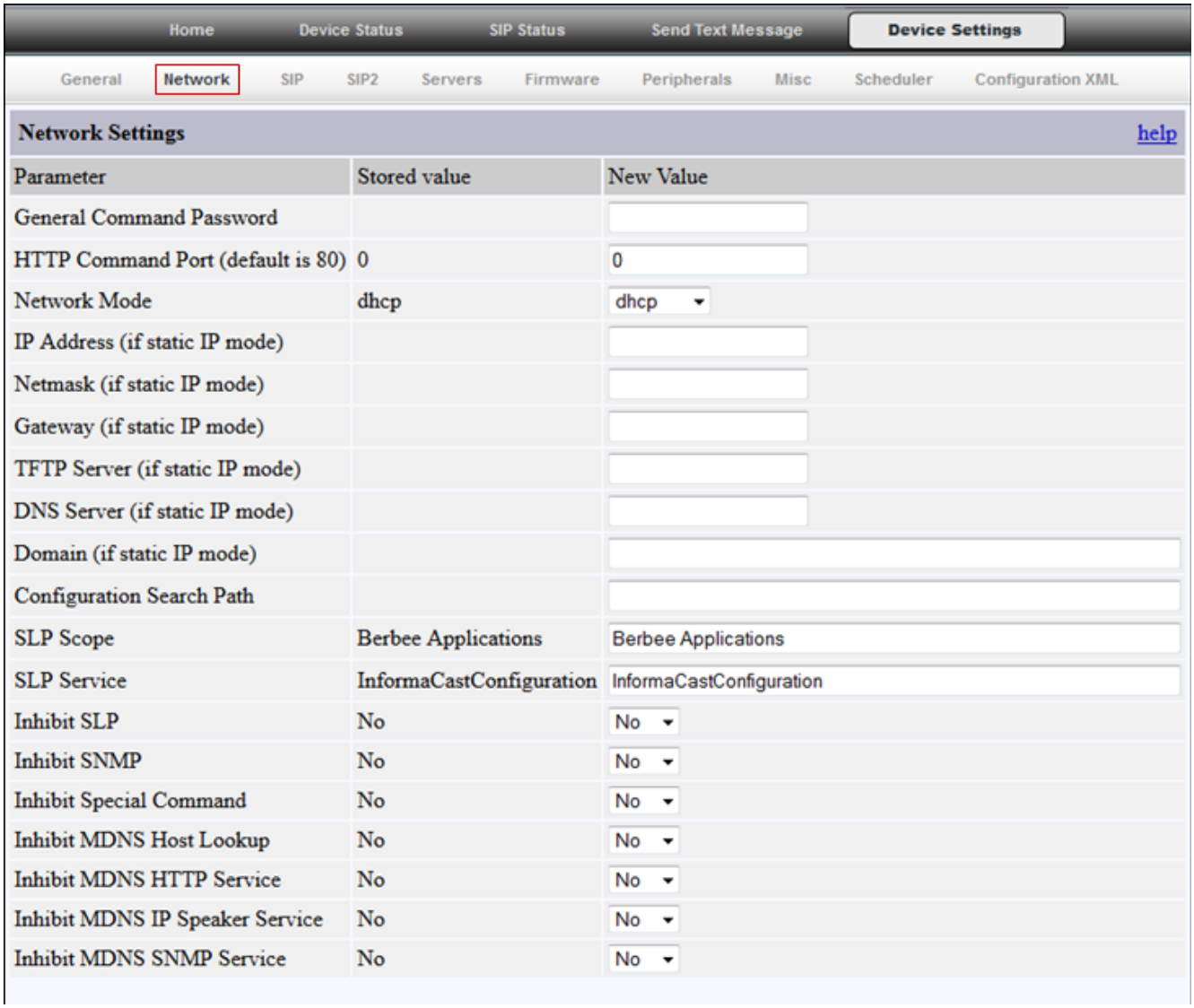
NOTE:
An IP address is required for the Advanced Network Devices before the device installation process. If the device is unable to receive an IP address, the device will continue to reboot and search again. A DHCP server is required during the first reboot in order for the AND sign to obtain an initial IP address. After an initial IP address is obtained, the sign can be reconfigured with a static IP address.

◈ After receiving the IP address, log on to the device using a web browser on a computer attached to the same subnet as the sign.
URL: http://sign_ip_address

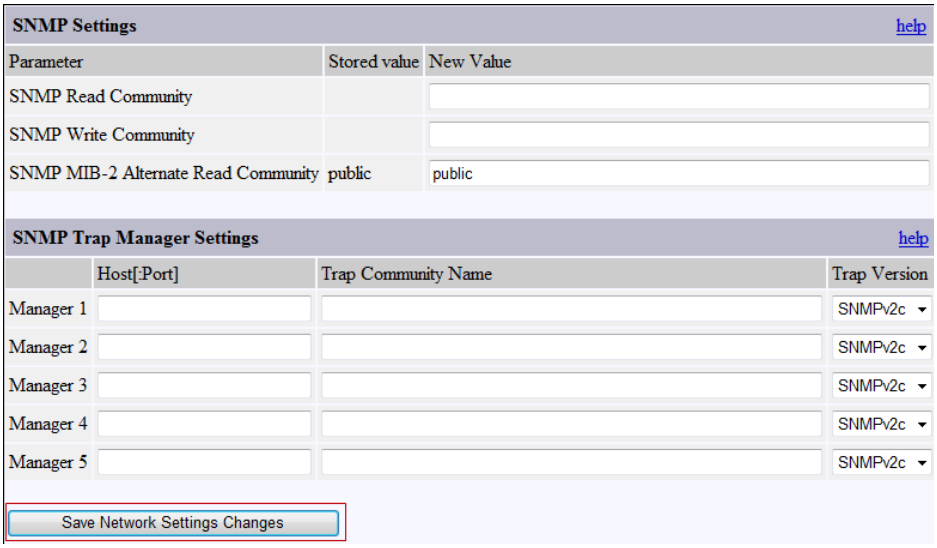
Display Configuration

1. Click **Device Settings**.
2. Select **Network**.

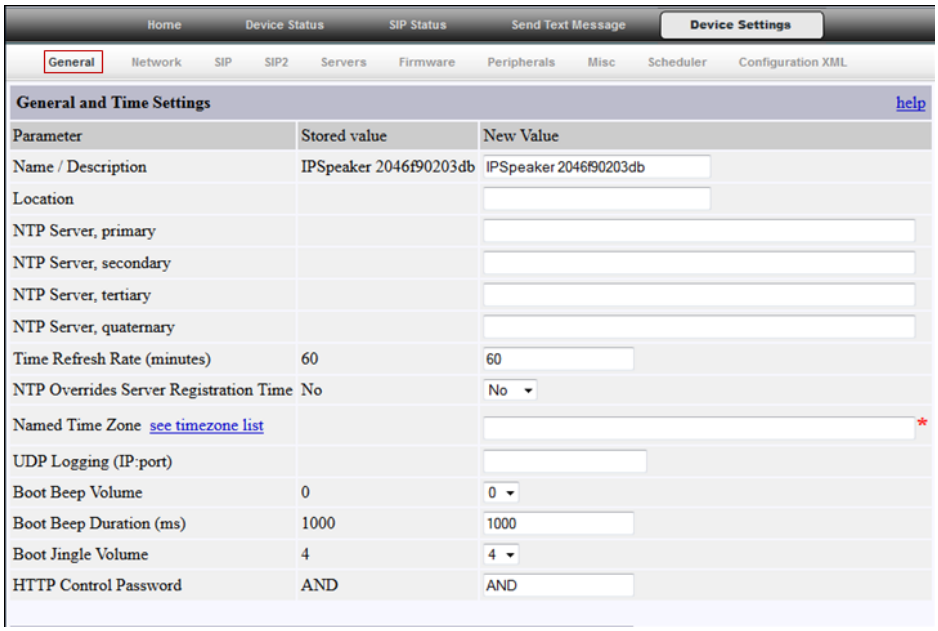
   ⇨ The **Network Settings** section displays.



3. Enter the network settings in the **Network Settings** field.
   NOTE: To assign a static IP address, select the **static IP value** under **Network Mode** and enter the **IP address**, **Netmask**, and **Gateway underneath**.
4. Select **Save Network Settings Changes**.



5. Click **General** and do the following:

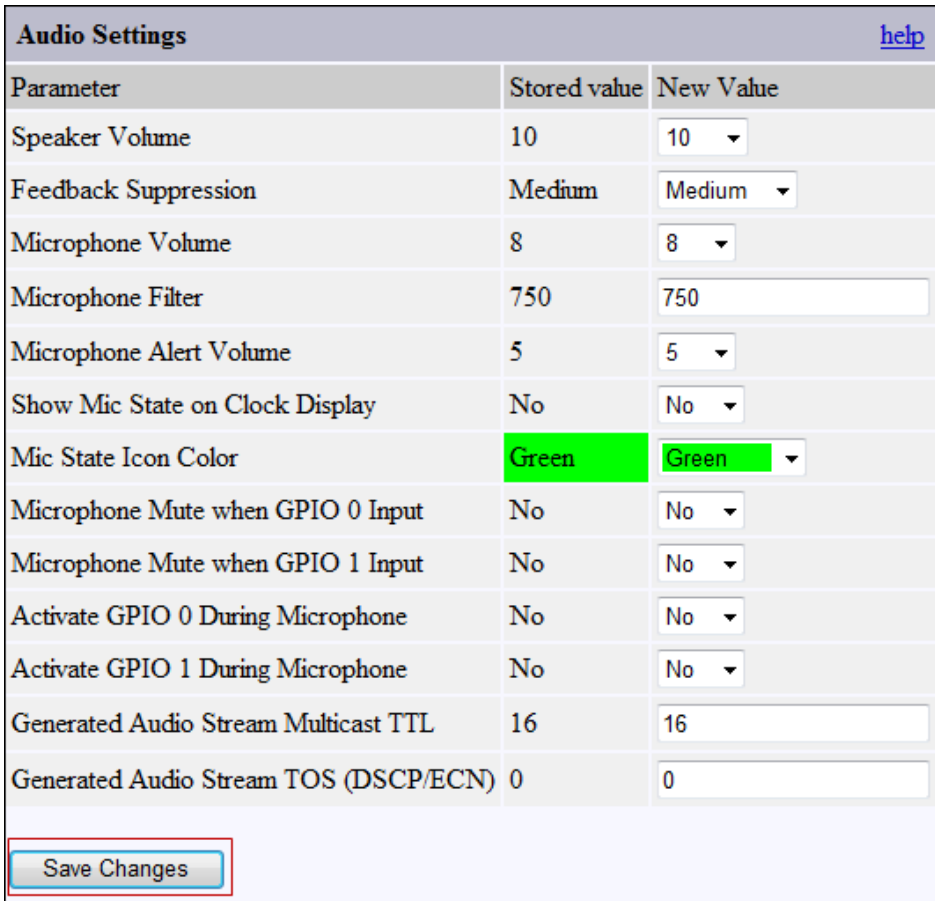


– Enter a name for the sign in the **Name** field.
– Enter the IP address of the main NTP server in the **NTP Server, primary** field.
  NOTE 1: This is required while using the sign as a clock during normal operation. It is also important in order to have accurate time stamps for the internal device logging.
  NOTE 2: It is recommended to use the NTP server.
– Enter the IP address of the Backup NTP server in the **NTP Server, secondary** field.
  NOTE: In the case of primary NTP server failure, the device will access the secondary NTP server. This is optional but recommended.
– Enter the appropriate string for your Time Zone in the **Named Time Zone** field.
– Leave the **HTTP Control Password** (default) password as it is or set a new password in case the user wants to change the default password.

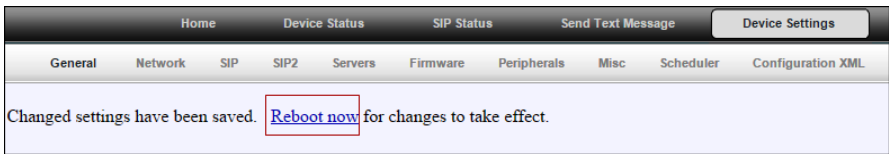
– In the **Display Settings** section, set value to **100** in the **Display Brightness** field.

Display Settings		help
Parameter	Stored value	New Value
Time Format	12 hour	12 hour
Show Leading Zero	No	No
Show Seconds	Off	Off
Keep Clock Seconds Smaller	No	No
Blink Colon	Yes	Yes
Clock Font Note: The date field is shown only when the clock is using a multi-line font.	BatangChe Bold	BatangChe Bold
Clock Color	Cranberry	Cranberry
Seconds Color	Tan	Tan
AM Color	Olive	Olive
PM Color	Sienna	Sienna
Date Color Note: Use multi-line clock font to enable	Olive	Olive
Date Format Note: Use multi-line clock font to enable	%a, %b %e	%a, %b %e
Date Shown as Tiny Note: Use multi-line clock font to enable	Yes	Yes
Clock Above Small Text	No	No
Minute Progress Critical Start Second	0	0
Minute Progress Color	Hunter	Hunter
Minute Progress Critical Color	Cranberry	Cranberry
Text Font	Arial Bold	Arial Bold
Text Color	Cranberry	Cranberry
Timer Font	Retro 7 Narrow	Retro 7 Narrow
Countdown Timer Color	Green	Green
Countdown Timer Critical Color	Vermillion	Vermillion
Count Up Timer Color	Green	Green
Count Up Timer Critical Color	Vermillion	Vermillion
Display Brightness (0-100)	100	100

6. Set the **Speaker Volume** to the required level.



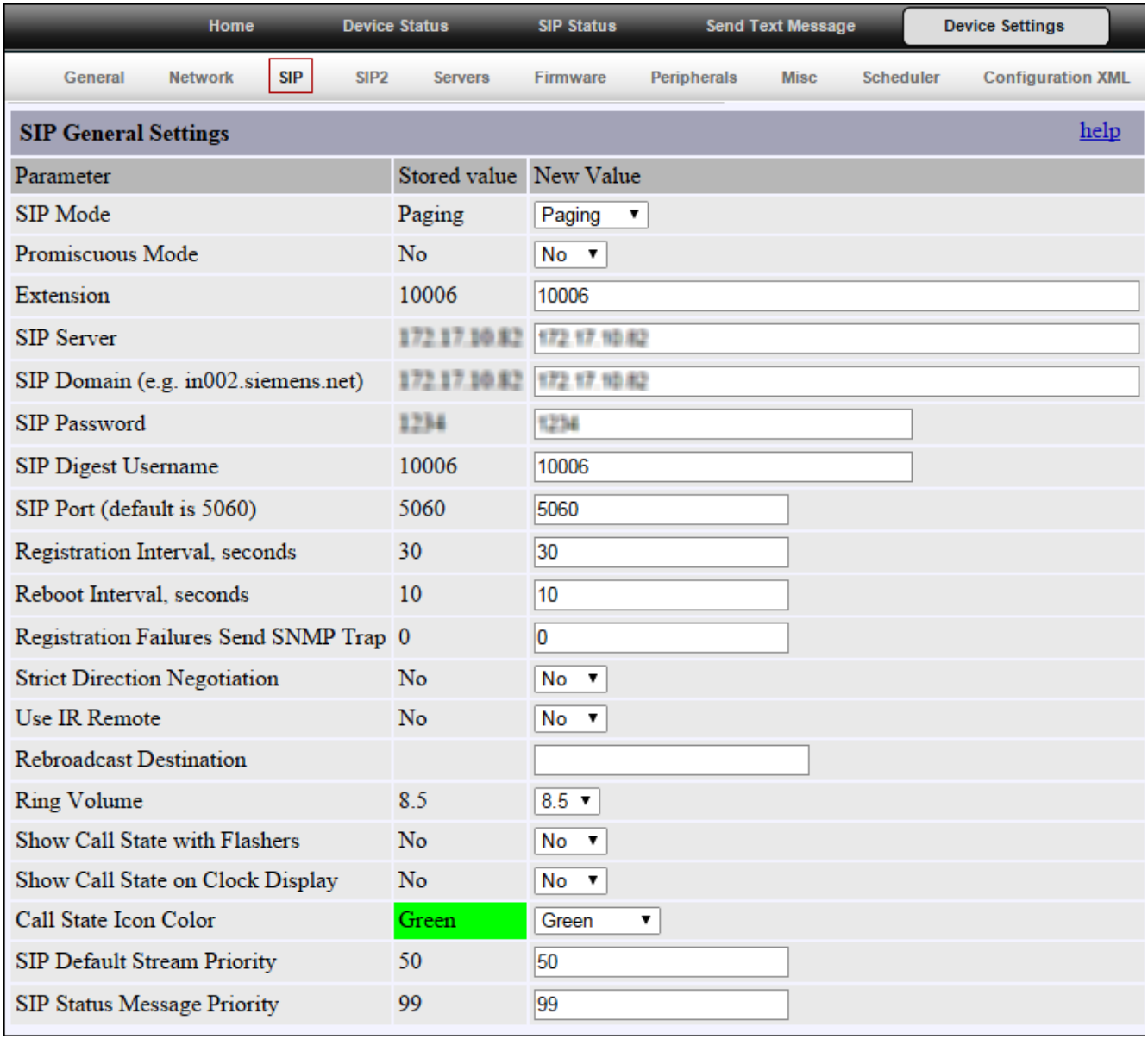
7. All other values are optional and can be left as default.
8. Click **Save Changes**.
   ⇨ A message displays for rebooting the device.



9. Click **Reboot now**.

Speaker Configuration

1. For configuring an AND IP Speaker, do the following:
   – Click **Device Settings**.
   – Select **SIP**.
   ⇨ The **SIP General Settings** section displays.



- In the **SIP Mode** field, select **Paging**.
- Enter the FreeSwitch extension number configured for the corresponding AND IP Speaker in the **Extension** field.
- In the **SIP Server** field, enter the IP Address of the SIP Server.
- In the **SIP Domain** field, enter the IP Address of the SIP Server.
- In the **SIP Password** field, enter the password of the FreeSwitch extension.
- Set the **Ring Volume** to the required level.
- All other values are optional and can be left as default.

SIP GPIO Input Action Settings help

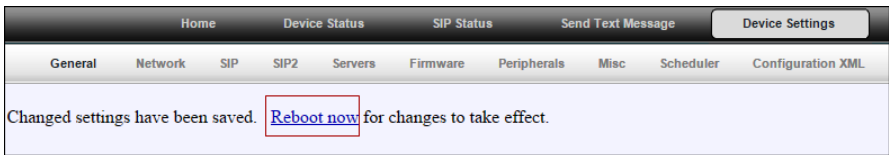
Parameter	Stored value	New Value
Push-to-Talk 1 (GPIO 0 Outgoing)		
Push-to-Talk 1 Alternate (Hold)		
Push-to-Talk 1 Alternate Hold Time (ms)	0	0
Push-to-Talk 1 Trigger Only	No	No
Push-to-Talk 2 (GPIO 1 Outgoing)		
Push-to-Talk 2 Alternate (Hold)		
Push-to-Talk 2 Alternate Hold Time (ms)	0	0
Push-to-Talk 2 Trigger Only	No	No
GPIO Control of Non-GPIO Calls	No	No

SIP GPIO Output Control Settings help

Parameter	Stored value	New Value
Keypad GPIO 0 'On' Password		
Keypad GPIO 0 'Off' Password		
Keypad GPIO 0 'Transient' Password		
GPIO 0 Transient Time (ms)	0	0
Keypad GPIO 1 'On' Password		
Keypad GPIO 1 'Off' Password		
Keypad GPIO 1 'Transient' Password		
GPIO 1 Transient Time (ms)	0	0
Activate GPIO 0 During Active Call	No	No
Activate GPIO 1 During Active Call	No	No
Activate GPIO 0 When Ringing	No	No
Activate GPIO 1 When Ringing	No	No

Save SIP Changes

2. Click **Save SIP Changes**.
   ⇨ A message displays for rebooting the device.



3. Click **Reboot now** to reboot the device.

Device Verification

To test the configuration of the device, follow the steps below:

◈ Open a web browser and enter the following URL:
http://SIGN_IP_ADDRESS/signmsg?text=This+is+a+test+message&loops=3&maxseconds=0&pauseseconds=0&speed=5&color=red&font=arial_bold&human=1&button=Send+New+Text+Message
NOTE: Computer must be connected to the same subnet as the IP LED sign.

⇨ On successful device configuration, the sign will display `This is a test message` three times as per the configured color.

1.27 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.

provides a redundancy feature using an off-the-shelf redundancy solution from Stratus Technologies called everRun 7.2. 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 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

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

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 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. 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 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**:

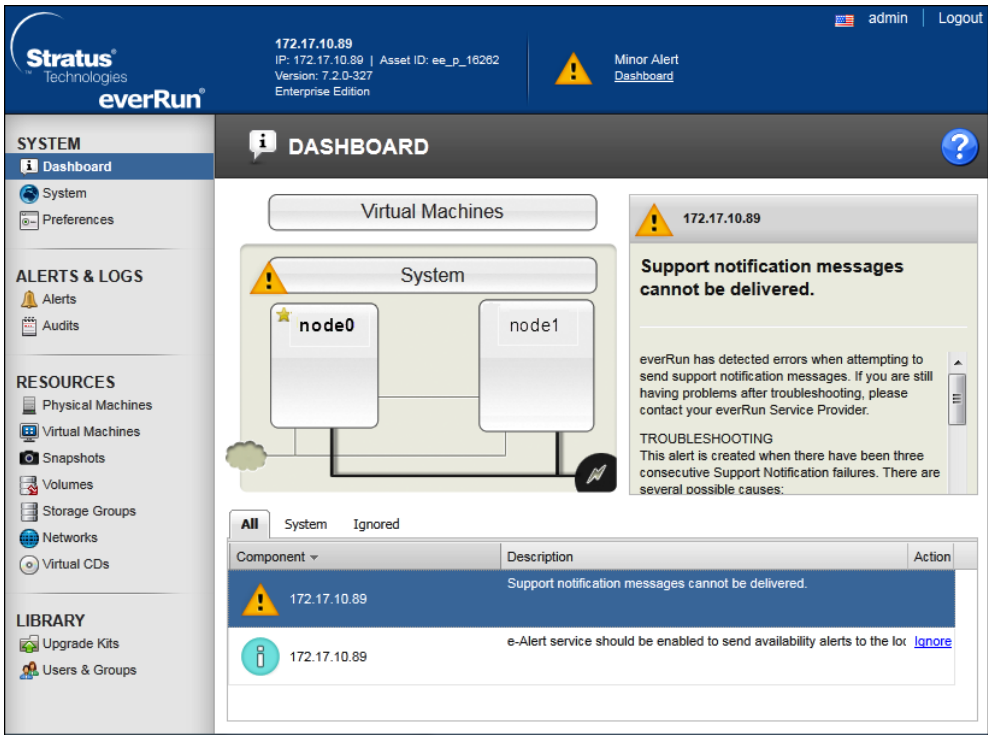
   – IPv4 address
   – Netmask
   – Default gateway address
   – Domain name server address
     NOTE 1: Contact your network administrator for this information.
     NOTE 2: If you enter invalid information, the window redisplays until you enter valid information.

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

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

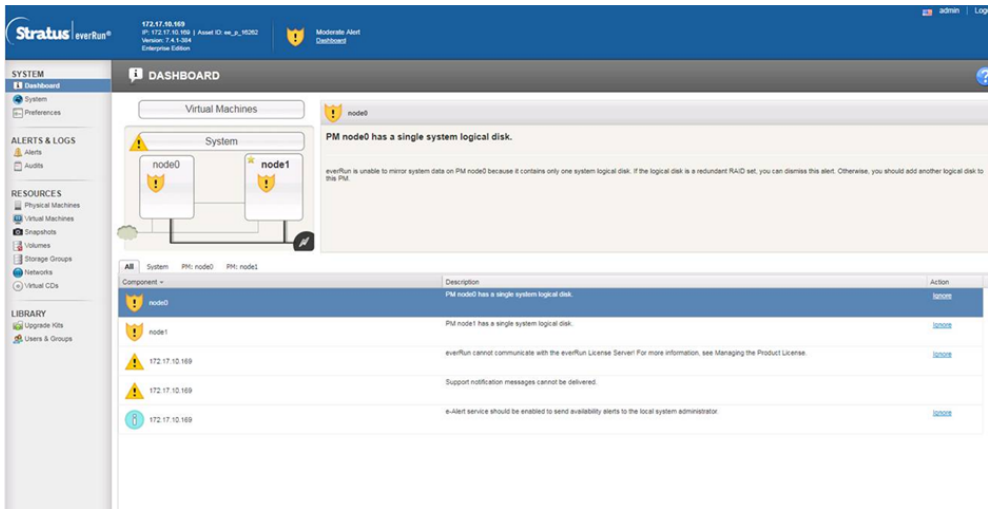


Troubleshooting the Physical Machine

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.



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 installation.

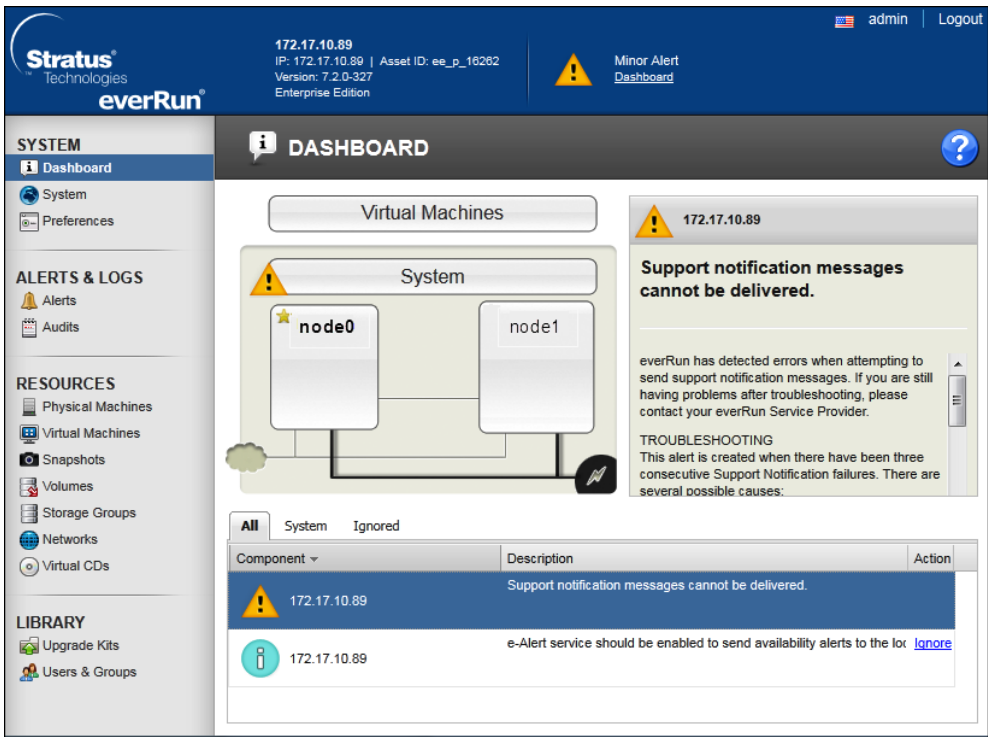
For background information on Server Failover, see Server Failover.

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

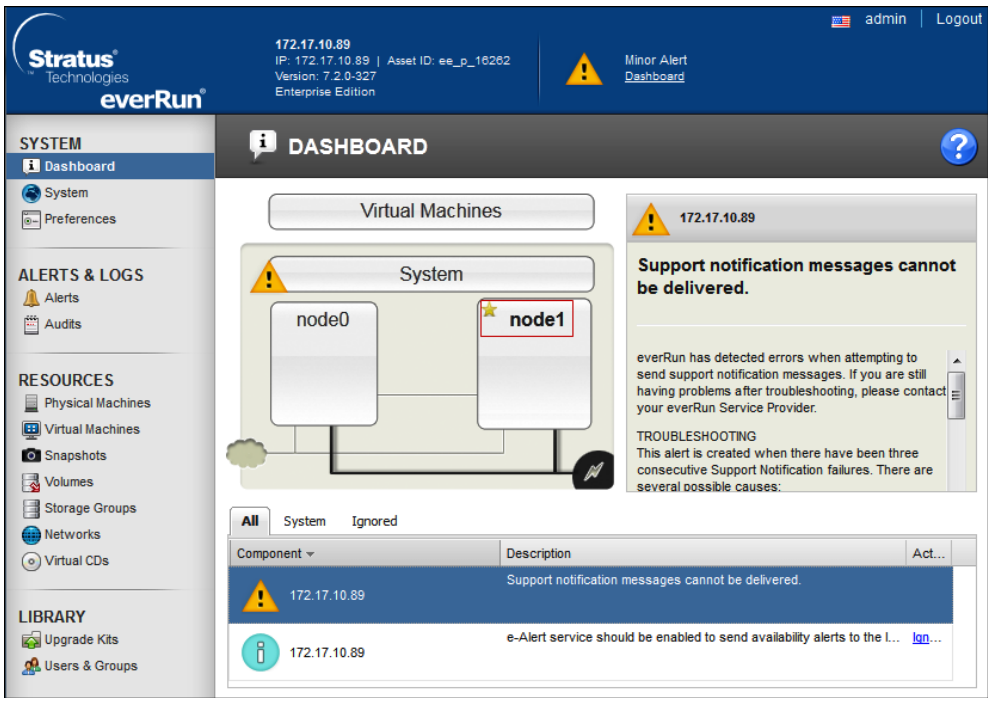
Verification Before Installing Notification

▷ 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.



➪ 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.



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

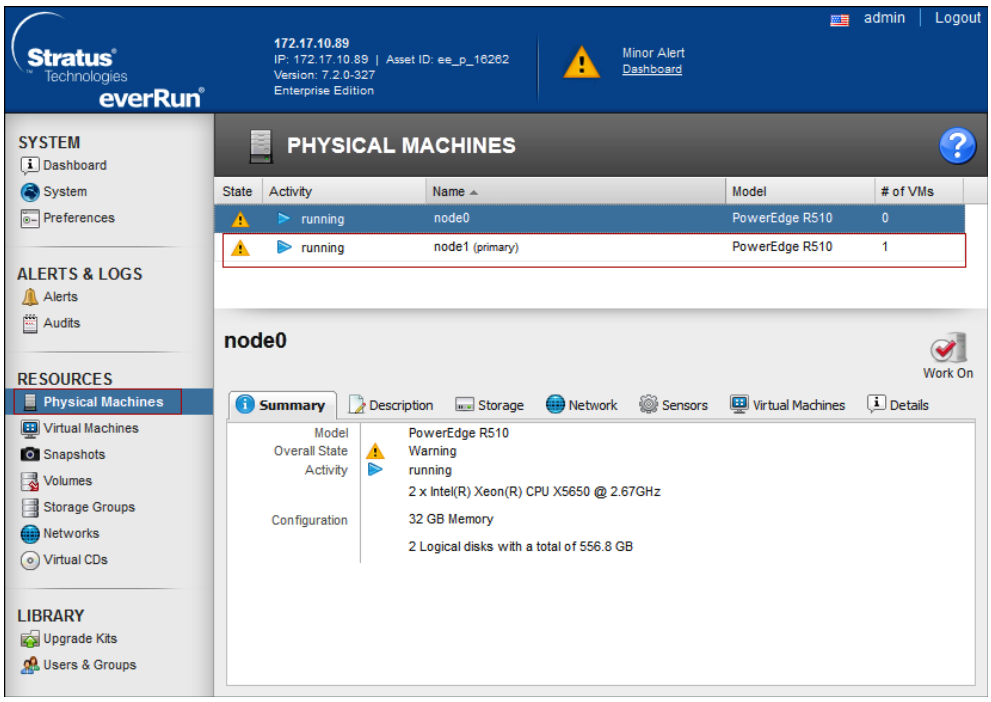


Fig. 40: Verification for the Primary Physical Machine

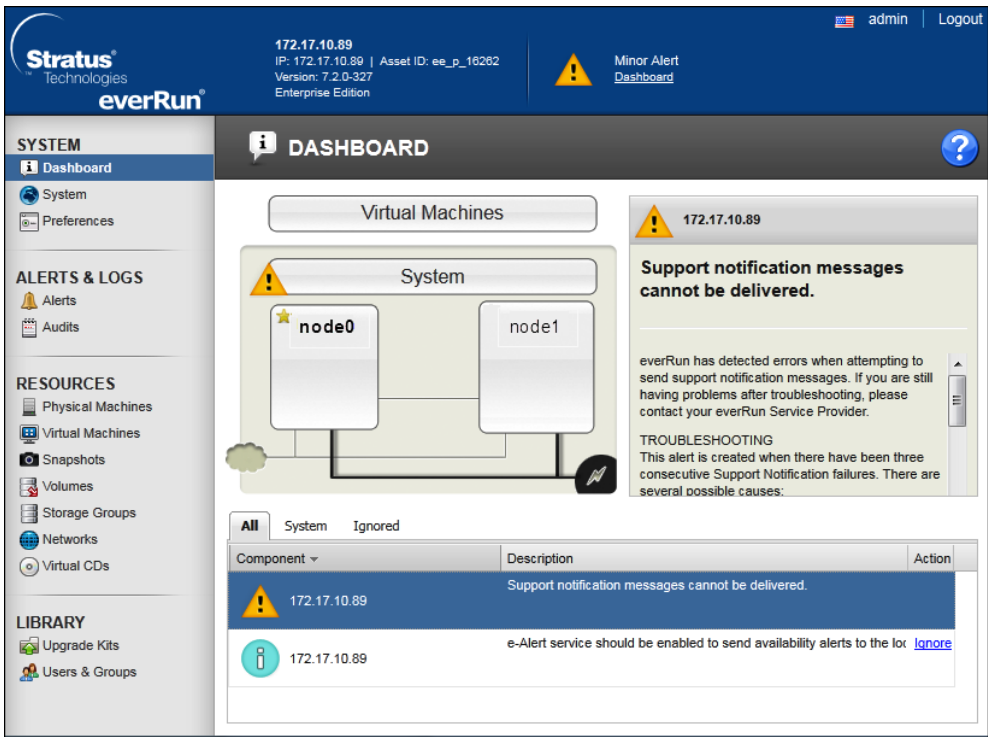
Verification After Installing Notification

▷ Virtual Machines are created and protected with everRun 7.2.

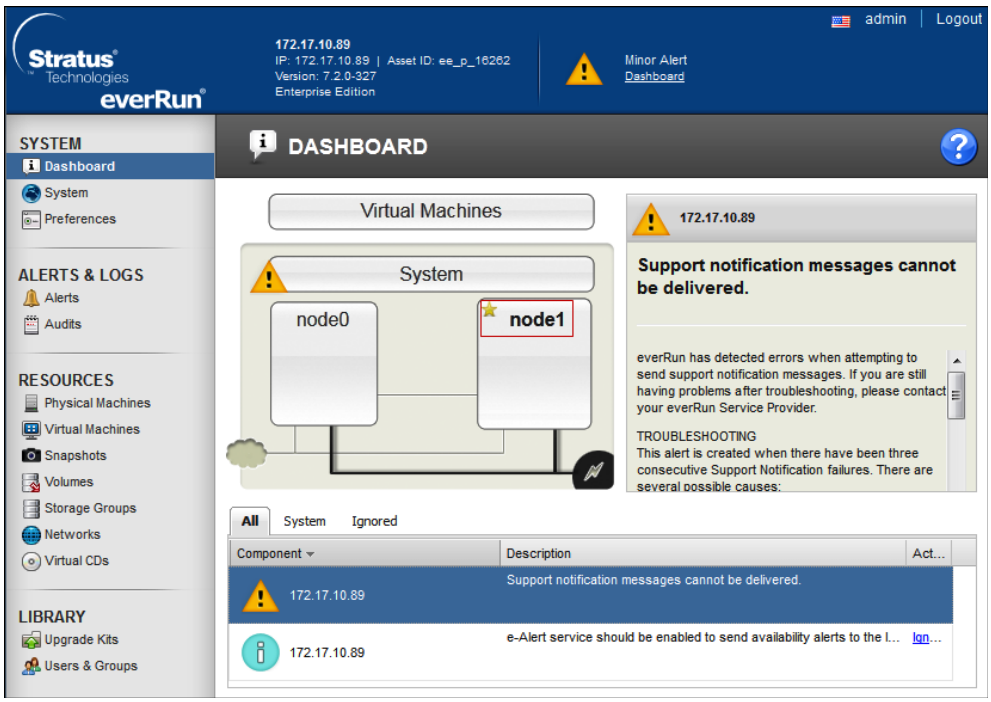
▷ is installed on the client machines.

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.



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



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

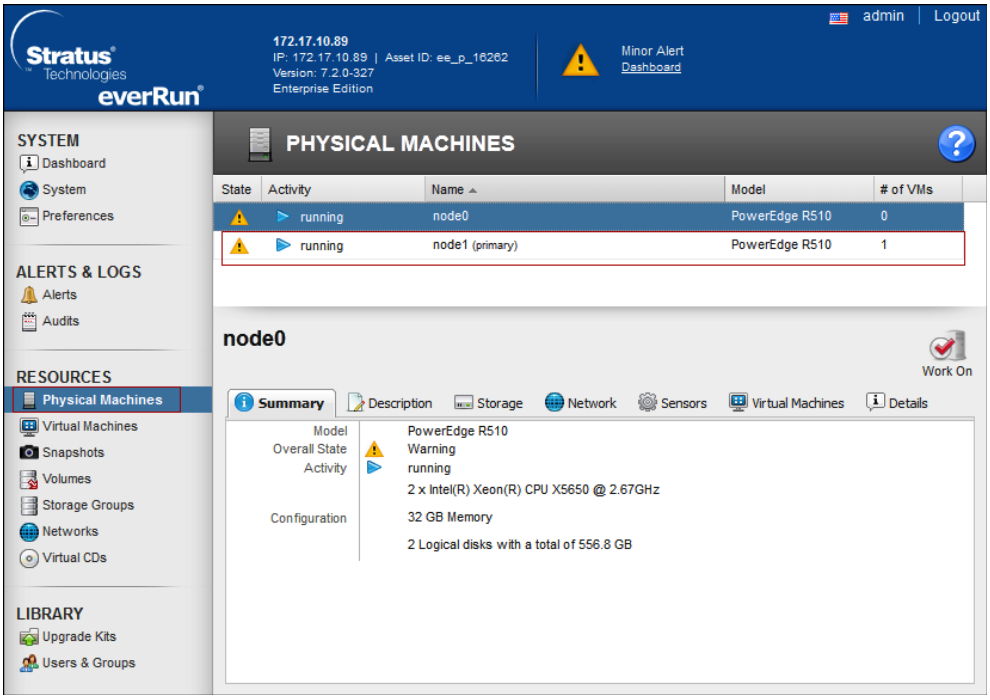


Fig. 41: Verification for the Primary Physical Machine

1.28 Relay Output Device

Relay Output Device

This section contains additional procedures for integrating the Relay Output device.

Installing Relay Output

This section provides information on mounting the hardware and connection details for each device.

Perle TD2R2 Installation

This section describes the prerequisites and steps to mount the device to a flat surface, supply power to the device, add an Ethernet network, and properly wire the device to allow a dry contact to be read.

Prerequisites

Before proceeding, ensure that the following items are available:

- Perle IOLAN SDS1 TD2R2
- 9-30 Vdc (400 mA minimum) Power Supply, if not included with device
- Category 5 Ethernet cable
- Computer or Server to communicate with the device
- The device Installation CD or a computer with network access
- Hookup wire of at least 20 AWG is necessary when using the I/O and relay pins
- STI emergency button, model SS-2*69E, is used in conjunction with the digital inputs

⚠ WARNING	
	**WARNING:** If configuring the Perle device for dry-contact detection, do not use the same device for relay control.

NOTE 1:
The TruePort Driver that is used to communicate with the device must be installed on the same server/machine that runs .
NOTE 2:
Make sure to have an RJ45 jack available that is connected to a properly configured IP network. The network must allow IP addresses to be assigned statically or through Dynamic Host Configuration Protocol (DHCP).
NOTE 3:
To configure the device, you must have a computer connected to the same network.

Mounting

The Perle SDS1 TD2R2 has two brackets on the side of the mounting holes. The installer is recommended to fasten the device to a flat surface by placing screws through mounting holes.

Power

This section describes the steps necessary to supply power to the device.

1. For the Perle TD2R2, use a power adaptor capable of 9-30VDC output and 400mA. If there is a barrel connector, cut off the connector 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** LED should be solid green.

⚠ WARNING	
	**WARNING:** Connecting the power supply to the device with incorrect polarity can permanently damage the device and pose a fire risk.

Ethernet

The Ethernet section describes the steps necessary to provide ethernet network connectivity to the device.

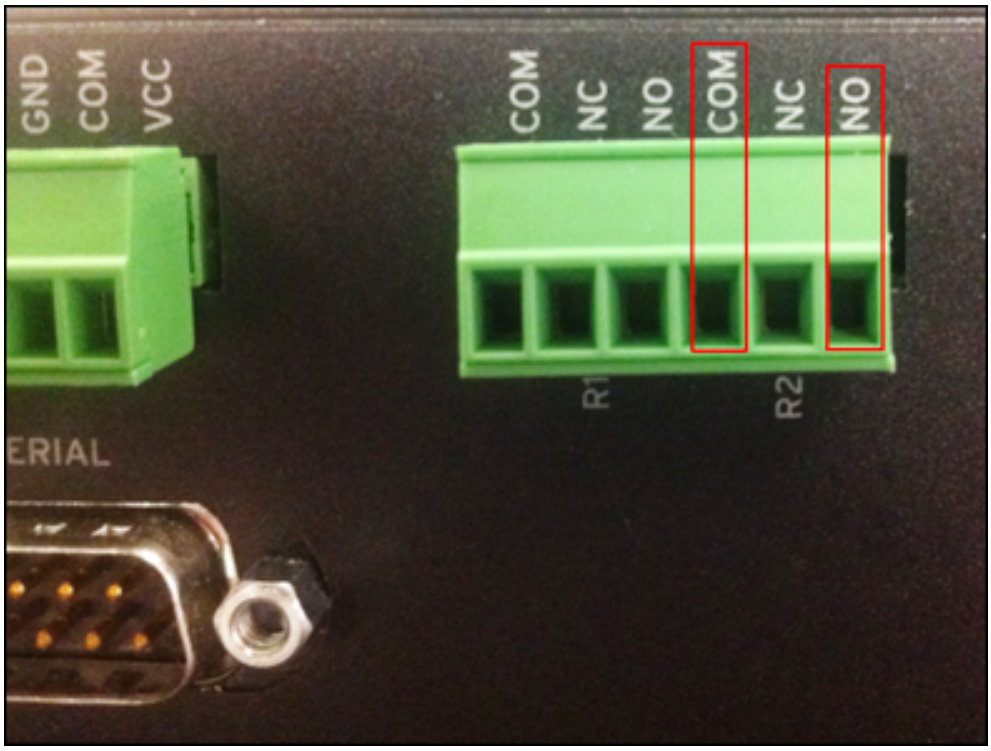
1. Plug one end of the Ethernet cable to the RJ45 jack on the device.
2. Connect the other end of the Ethernet cable to your network jack.

⇨ 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. You need to configure the device to use DHCP or assign a static IP with a computer that is attached to the same subnetwork.

Relay Output

The relay outputs are generally used to switch higher power speaker arrays or zone selection circuits on fire panels. In addition, relay outputs differ from digital outputs in that they provide electrical isolation between the two devices.

Generally, these external circuits require a closed dry contact for activation. The Perle TD2R2 includes two relays each with their own COM terminals. When hooking the device relays to external circuits, use the COM and NO (normally open) terminals. This will provide a closed switch activation to any external circuit.



⚠ WARNING	
⚠	**WARNING**: The maximum load for the relay channel is 1A @ 30 Vdc or 0.5A @ 120 Vac.

Configuring Relay Output

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

NOTE:

TruePort is a COM port re-director driver utility that is installed on the server. It 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.

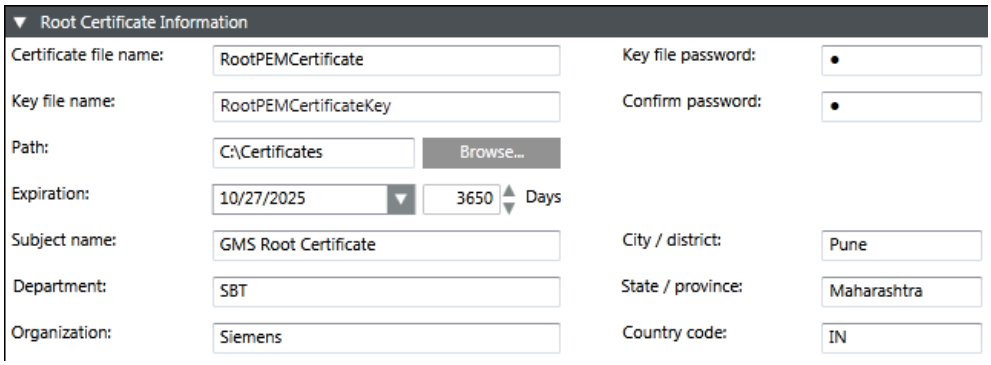
The following is the recommended workflow for working with the **Certificates** in System Management Console (SMC).

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

Create 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.



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.

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 are 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.

Relay Device Configuration

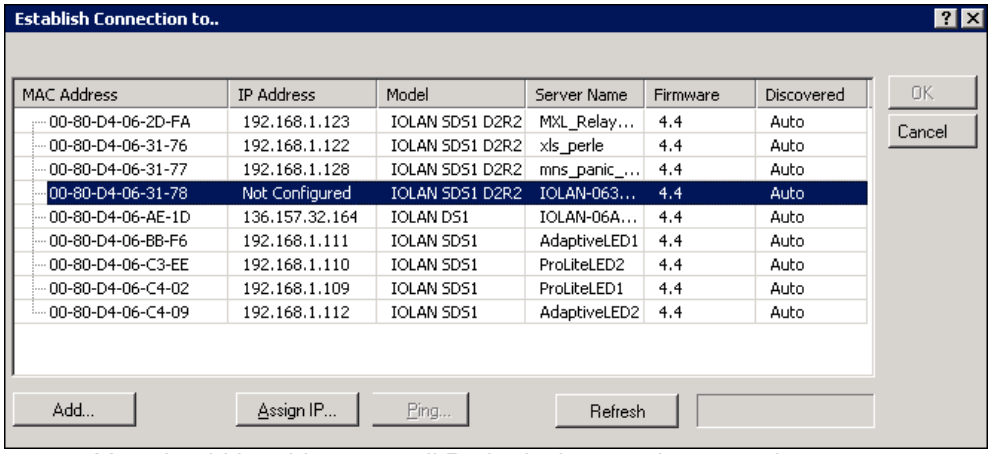
▷ You have installed **DeviceManager** on a computer located in the same network as the device to configure.

▷ 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 Import DME File.

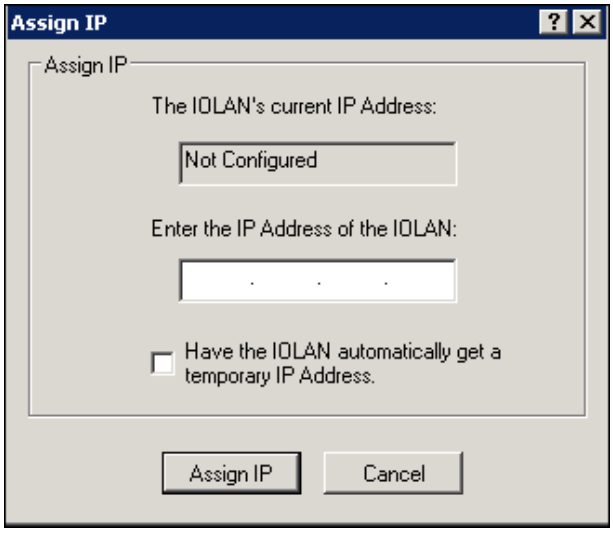
1. Start **DeviceManager**.



⇨ You should be able to see all Perle devices on the network.

2. Select the device you want to configure and click **Assign IP**.
NOTE 1: If you are unable to see the device in the window, 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 you are still having 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 device to reboot and initialize. If resetting 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**.



⇨ You should now be back to the connection window. The device should now have an IP address.

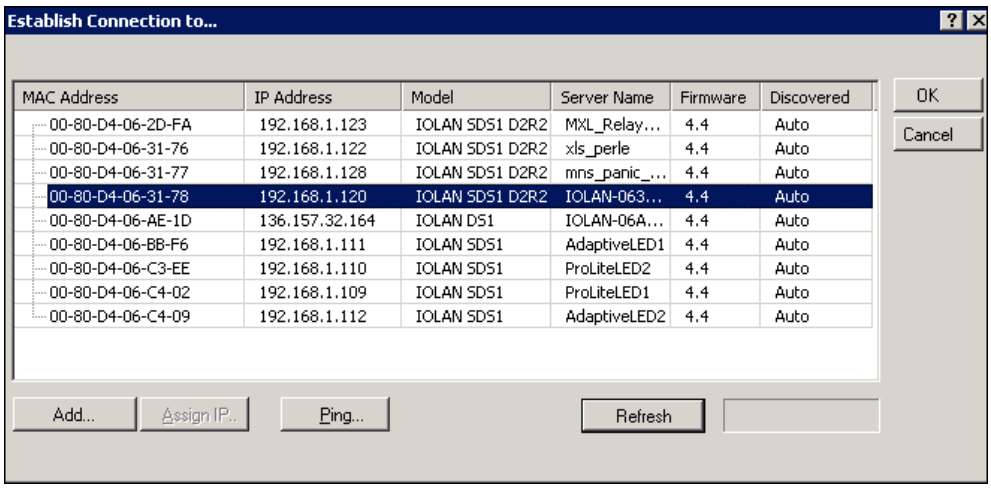


Fig. 42: Establish Connection To

4. Select the device again, and click **OK**.
5. At the login window, type in the device password. The factory default password is: **superuser**.

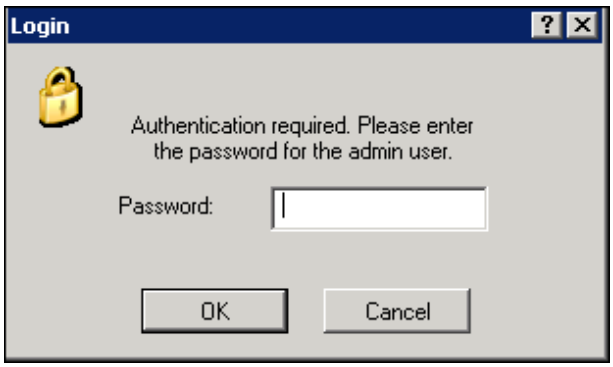
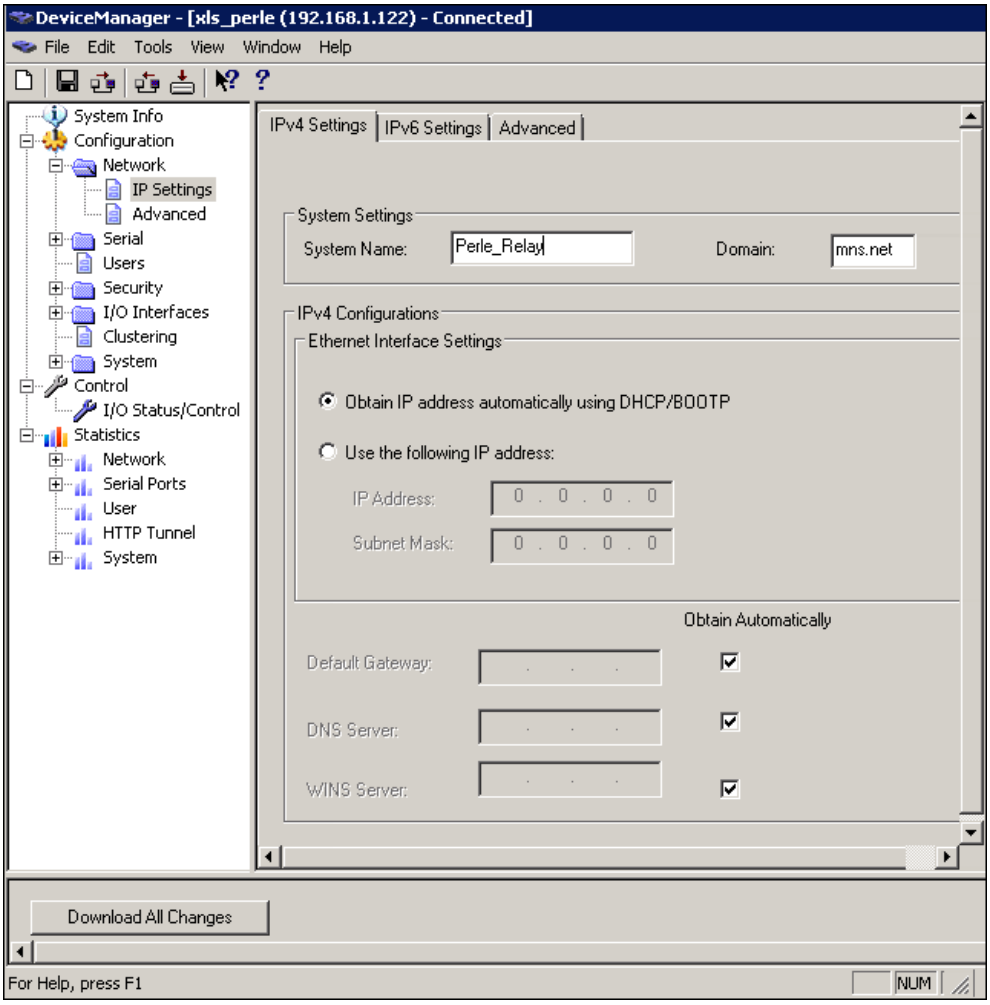


Fig. 43: Login Window

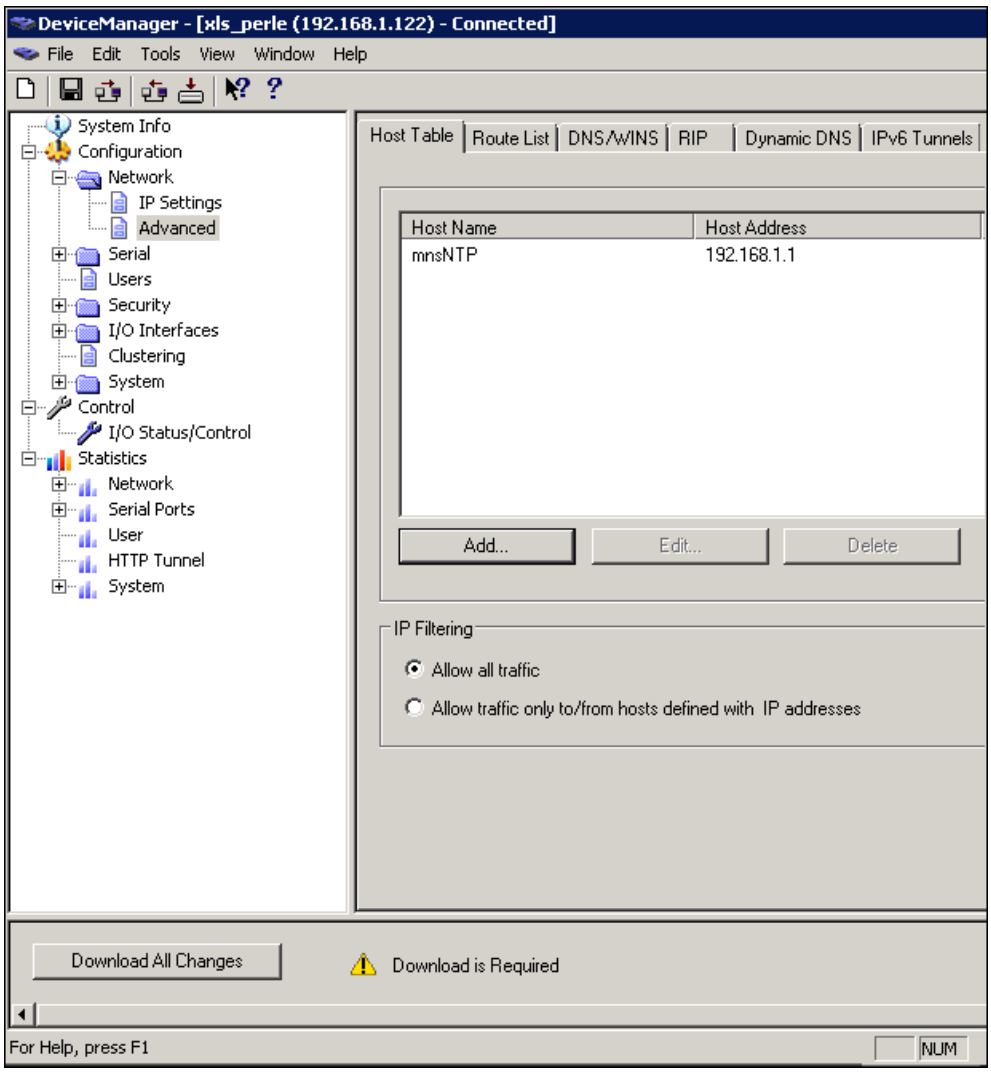
Network Set Up

▷ You have logged in to the device using DeviceManager.

1. In the **DeviceManager** window, click on 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**.



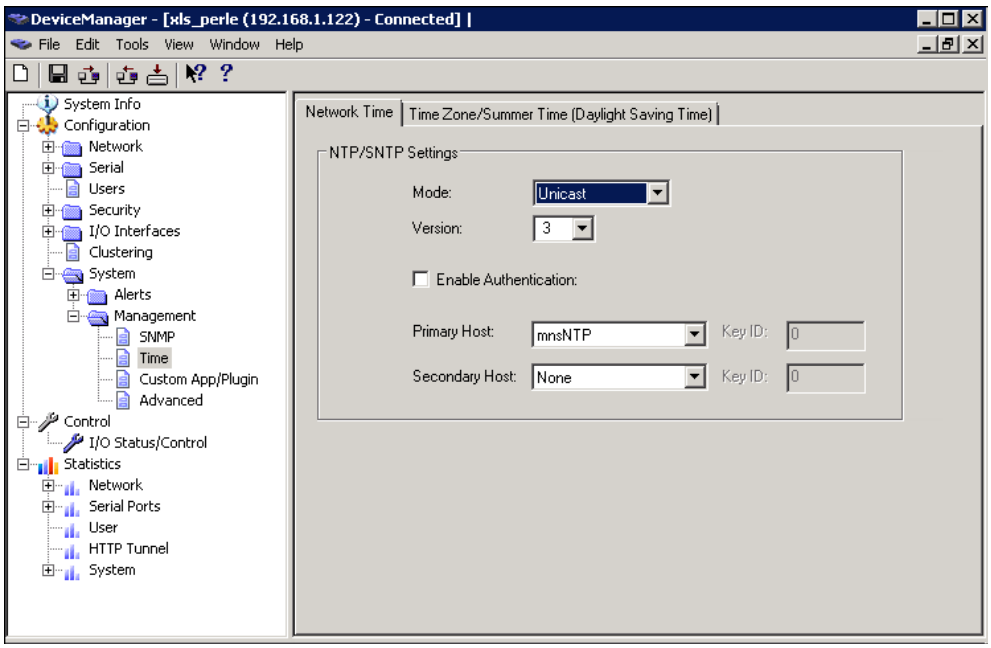
2. In the **System Name** field, provide a name that helps distinguish that device from other similar devices.
   NOTE 1: The System Name is used by the device to create a fully qualified domain name.
   NOTE 2: By default, the device is always **IOLAN** followed by the last three bytes of the device MAC address.
3. Select the **Domain** field, enter the domain name used on the client's network (for example, **AmericaUniversity.net**).
   NOTE: The device is capable of receiving the domain automatically from the Dynamic Host Configuration Protocol (DHCP). However, the DHCP would have to be configured to set the domain as a parameter.
4. Select **Network>IP Settings**.
5. Select the **Advanced** tab.
6. Select the **Register Address in DNS** check box.
7. Select the **Advanced** option from the left-hand side of the window.
8. Select the **Host Table** tab.
9. Click **Add**.



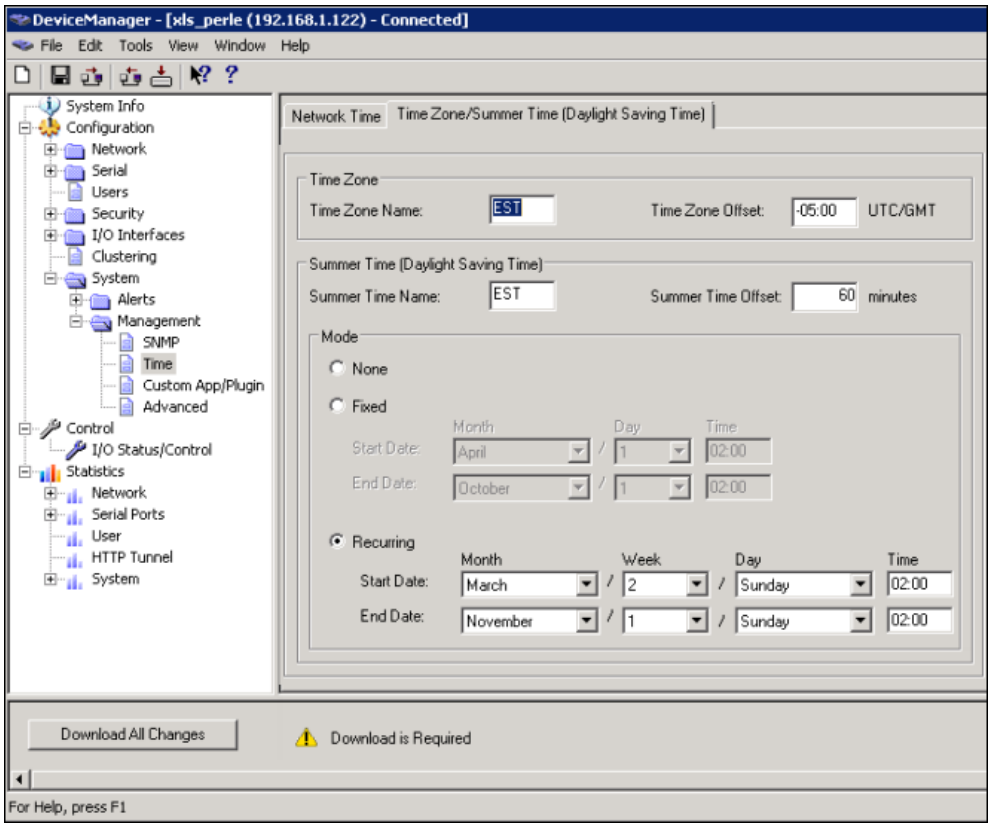
10. On the window, enter a descriptive name for the Network Time Protocol (NTP) server (for example, **mnsNTP**).
11. Enter the IP address or the fully qualified domain name of an available NTP server.
    NOTE: An available NTP server is required to enable SSL on the device.
12. Click **OK**.

Time and Security Settings

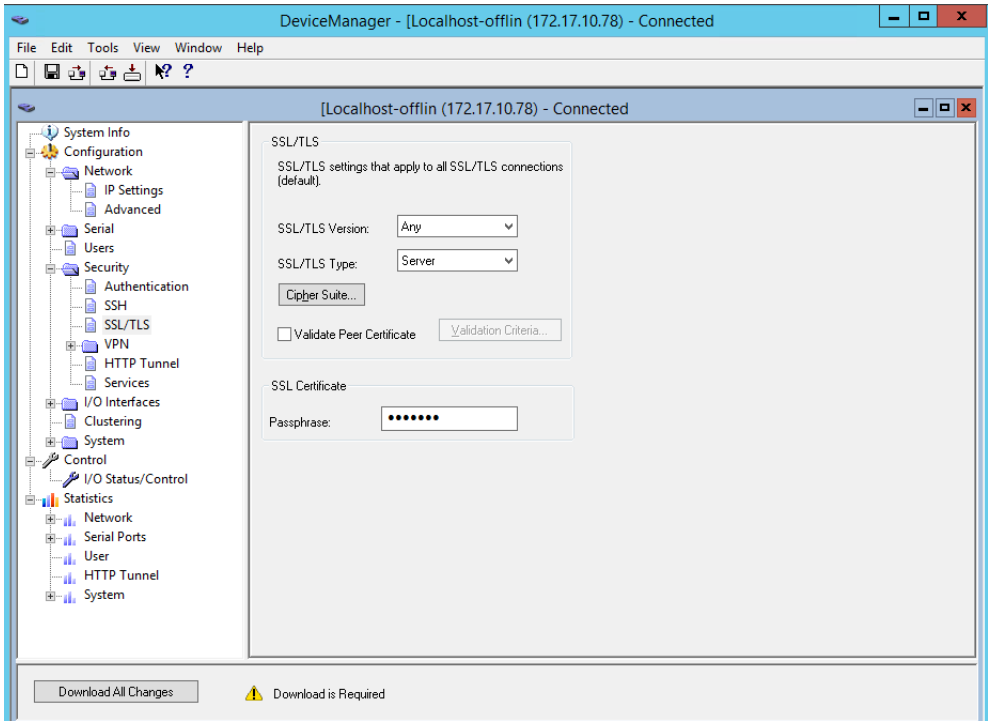
1. Select **Configuration > System > Management > Time**.
2. Select the **Network Time** tab.
3. Set the following parameters.
   - **Mode**: Unicast.
   - **Version**: 3.
   - Leave the **Enable Authentication** check box unselected.
   - **Primary Host**: Select the NTP server name created earlier.
   - **Secondary Host**: Select alternative NTP server name, otherwise set the name as the 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 you are not sure, verify with the client's network administrator.



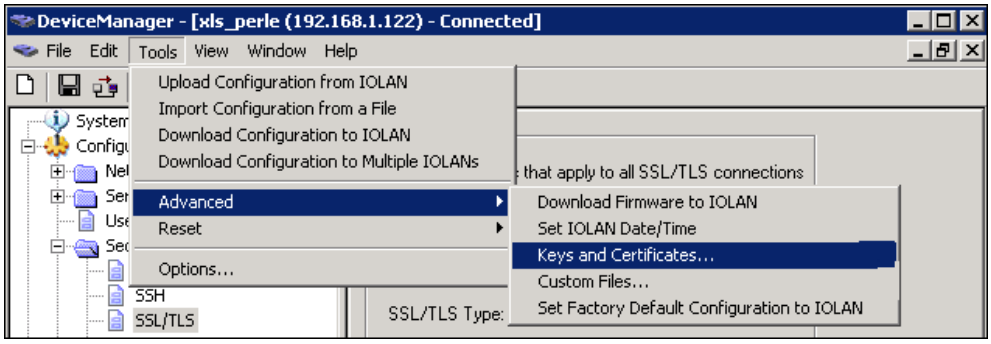
4. Select the **Time Zone/Summer Time (Daylight Saving Time)** tab.
5. Configure the parameters as per the details mentioned in Time Zone/Summer Time (Daylight Saving Time) Parameters.



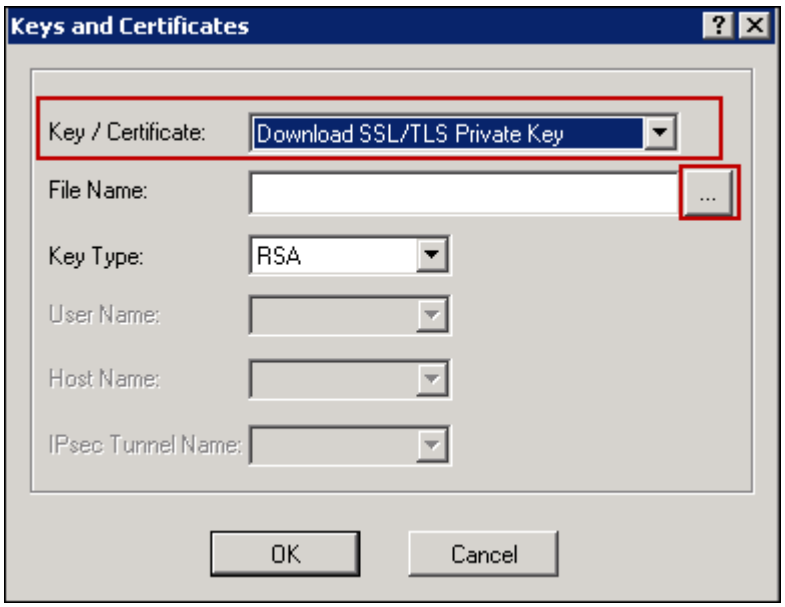
6. Select **Configuration > Security > SSL/TLS**.



7. Set **SSL/TLS Version** field to **Any**.
8. Set **SSL/TLS Type** field to **Server**.
9. Select the **SSL Certificate** section.
10. Enter the password of the SSL certificate in the **Passphrase** field.
11. Select **Tools > Advanced > Keys and Certificates**.



12. In the **Key/Certificate** drop-down list, select **Download SSL/TLS Private Key**.
13. Click the browse button and upload the private key for your Root certificate (.pem).
14. Click **OK**.



15. Select **Tools > Advanced > Keys and Certificates**.
16. In the **Key/Certificate** drop-down list, select **Download SSL/TLS Certificate**.
17. 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.
18. Click **OK**.
19. Select **Tools > Advanced > Keys and Certificates**.
20. In the **Key/Certificate** drop-down list, select **Download SSL/TLS CA**.
21. Click the browse button and upload the upload the root certificate (RootCertificate.pem file).
22. Click **OK**.

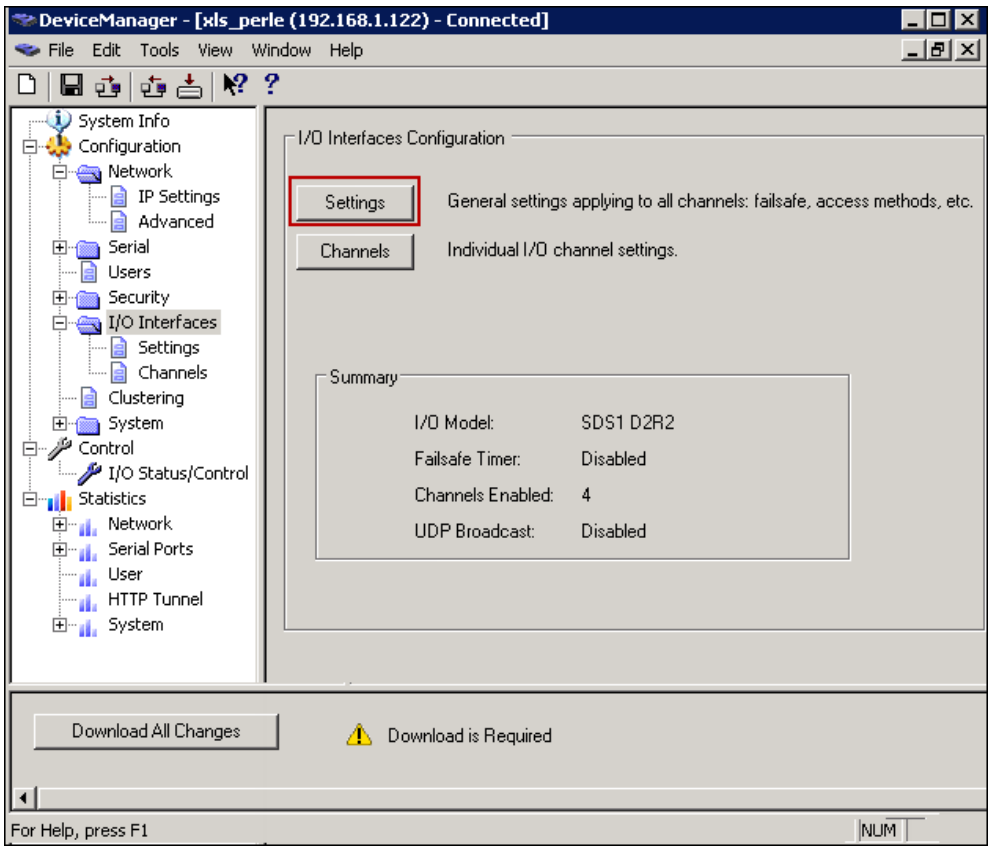
Time Zone/Summer Time (Daylight Saving Time) Parameters

Field	Description
Time Zone Name	The name of the time zone to be displayed during standard time. **Field Format:** Maximum 4 characters and minimum 3 characters (do not use angled brackets <>)
Time Zone Offset	The offset from UTC (Coordinated Universal Time) for your local time zone. **Field Format:** Hours *hh* (valid -12 to +24) and minutes *mm* (valid 0 to 59 minutes)
Summer Time Name	The name of the configured summer time zone; this will be displayed during the summer time setting. If this parameter is not set, then the summertime feature will not work. **Field Format:** Maximum 4 characters and minimum 3 characters (do not use angled brackets <>)
Summer Time Offset	The offset from standard time in minutes. Valid values are 0 to 180. **Range:** 0-180 **Default:** 60

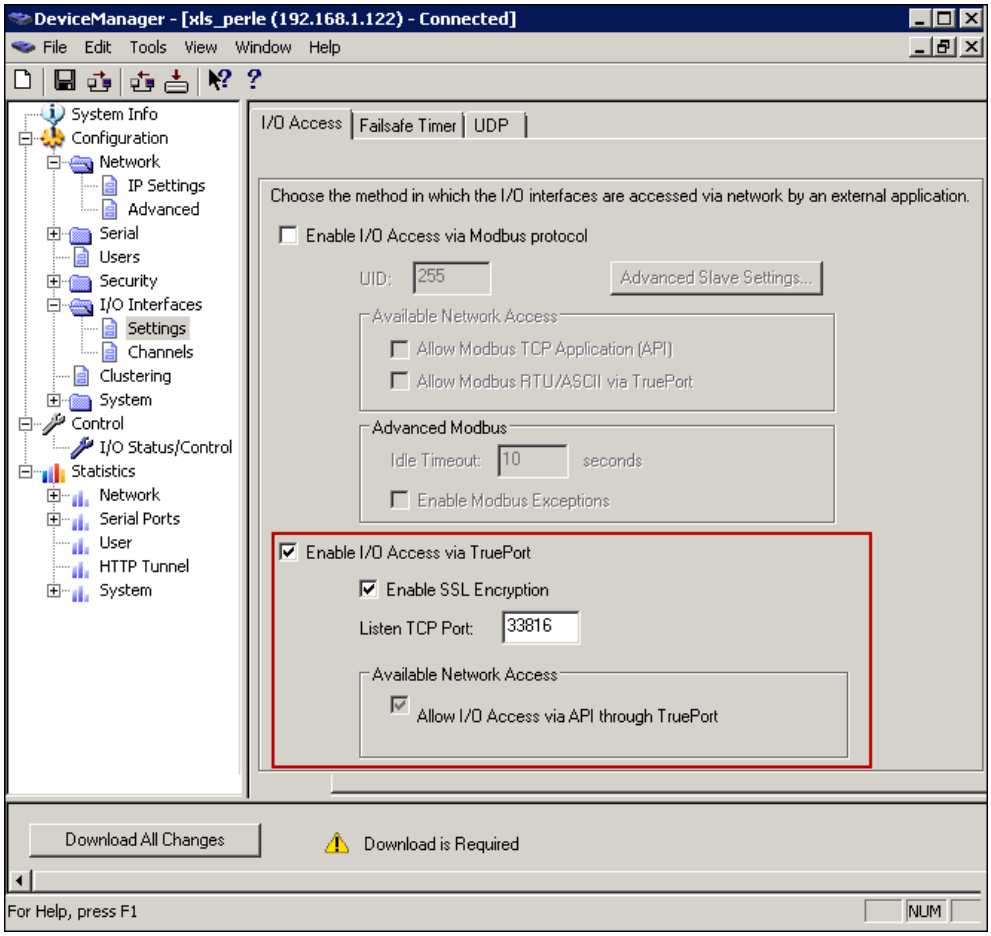
Summer Time Mode	Configure the summer time to take effect. **None** – No summer time change **Fixed** – The summer time change goes into effect at the specified time every year. For example, April 15 at 1:00pm. **Recurring** – The summer time change goes into effect every year at the same relative time. For example, on the third week in April on a Tuesday at 1:00pm. **Default** – None.
Fixed Start Date	The exact date and time in which the IOLAN's clock will change to summer time (daylight saving time) hours.
Fixed End Date	The exact date and time in which the IOLAN's clock will end summer time hours and change to standard time.
Recurring Start Date	The relative date and time in which the IOLAN's clock will change to summer time (daylight saving time) hours. Sunday is considered the first day of the week.
Recurring End Date	The relative date and time in which the IOLAN's clock will end summer time hours and change the standard time. Sunday is considered the first day of the week.

I/O Access Settings

1. You have logged in to the device using DeviceManager.
2. In the DeviceManager window, click **I/O Interfaces** on the left-hand side of the window, and then click **Settings**.



3. On the **I/O Access** tab, select the **Enable I/O Access via TruePort** checkbox.
   NOTE 1: By default, the device monitors I/O commands on TCP port 33816. If you wish to change the I/O TCP port, you may as long as the change does not conflict with other services or TruePort ports.
   NOTE 2: 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.



4. Select the **Enable SSL Encryption** checkbox.

⇨ The configuration is now complete. Click **Download All Changes** to make the changes to the device or continue with other settings.

◈ Click **Reboot IOLAN**.
NOTE: Any time you reboot the device, or power is reconnected, wait 90 seconds for the device to reboot and initialize. When the device is ready, the Power LED will be solid green and the Link LED will be solid amber or green.

Perle TD2R2 Device

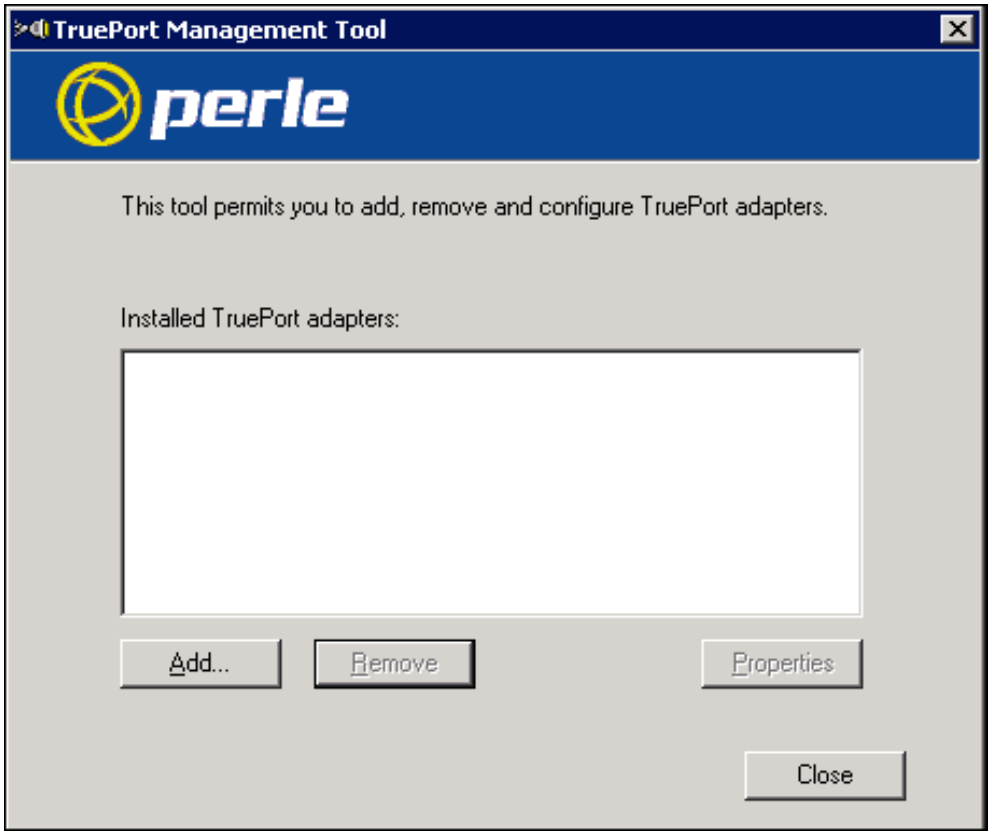
There are two areas of configuration. The first is to configure the TD2R2 device to allow remote access to the relays. The second area of configuration is the TruePort driver which the server uses to communicate with the TD2R2 device.

Configuring the TD2R2 requires Perle's DeviceManager software. Install DeviceManager onto a computer that is connected to the same subnet network as the Perle device you are trying to configure.

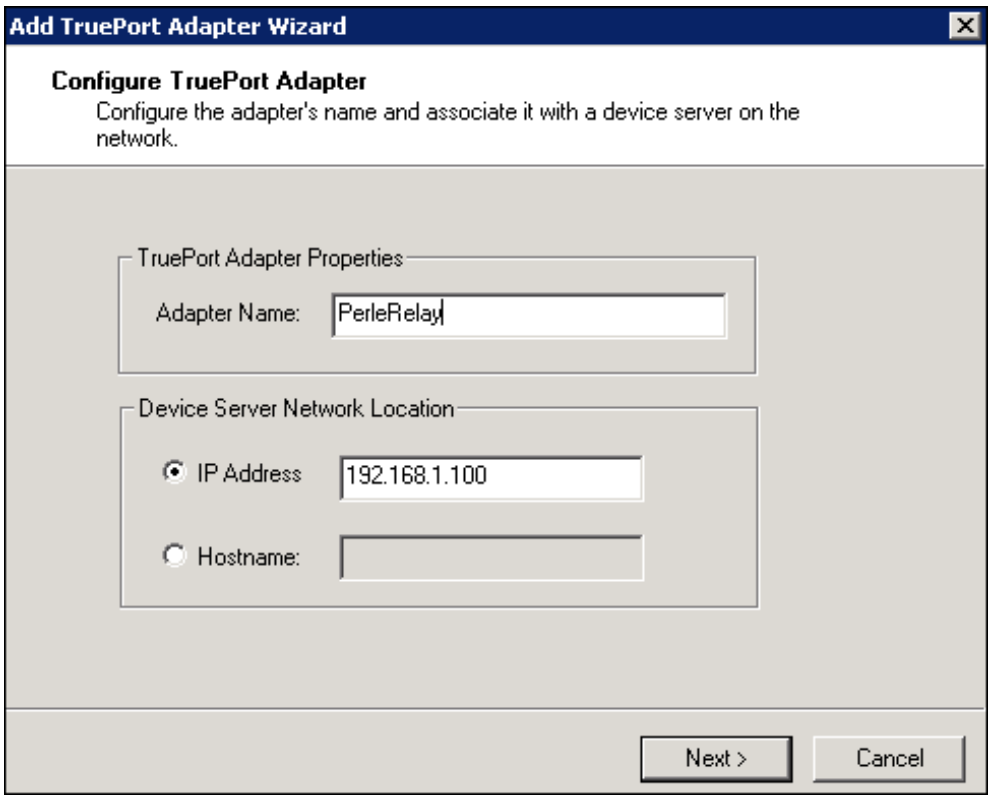
TruePort Driver Configuration

▷ The TruePort Driver is the second part of the process to link the device to your 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, each device should have a COM port for each service.
NOTE: Serial communication and I/O access are each considered a separate service and therefore require separate COM ports. Each device requires a unique and separate COM port.

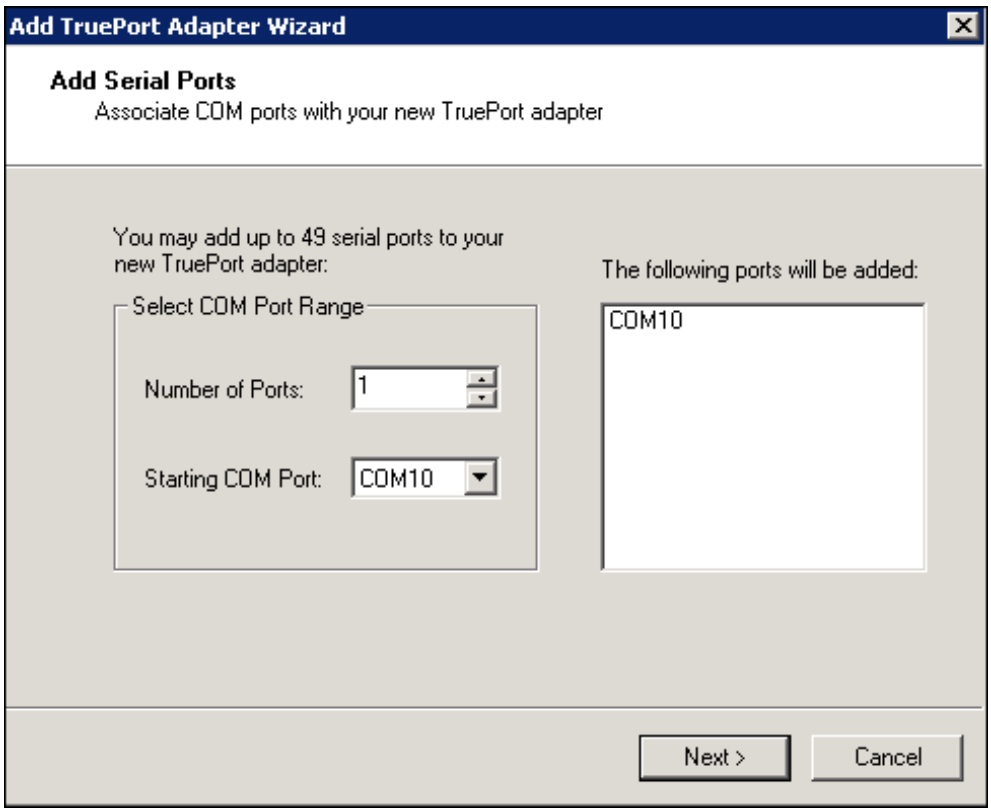
1. If you have not already done so, install TruePort on your server.
2. Start the **TruePort Management Tool**.
3. At the management window, click **Add**.



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



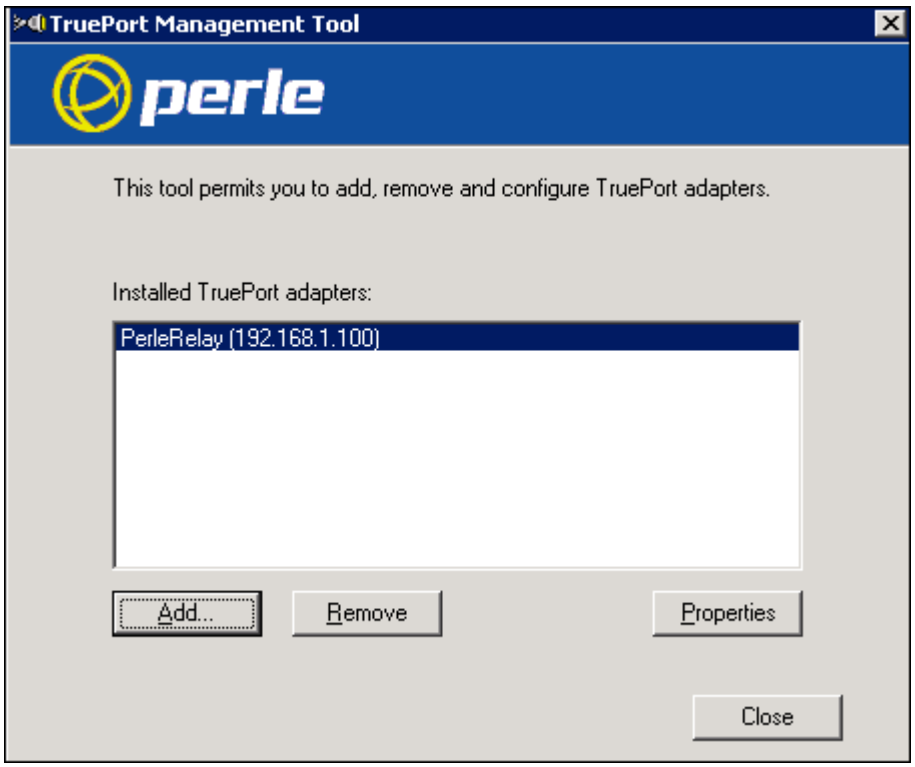
6. Leave the number of ports set to **1** (if you are also using I/O access, you may set ports to **2**, or add another later). Select the COM port you wish to assign to that particular device. By convention, start at COM100 and increment for each device and service configured. This will help to avoid any conflicts with existing COM ports or other devices. TruePort allows you to create up to 4096 COM ports.
7. Click **Next**.



⇨ You should now see the TruePort Adapter in the TruePort Management Tool.

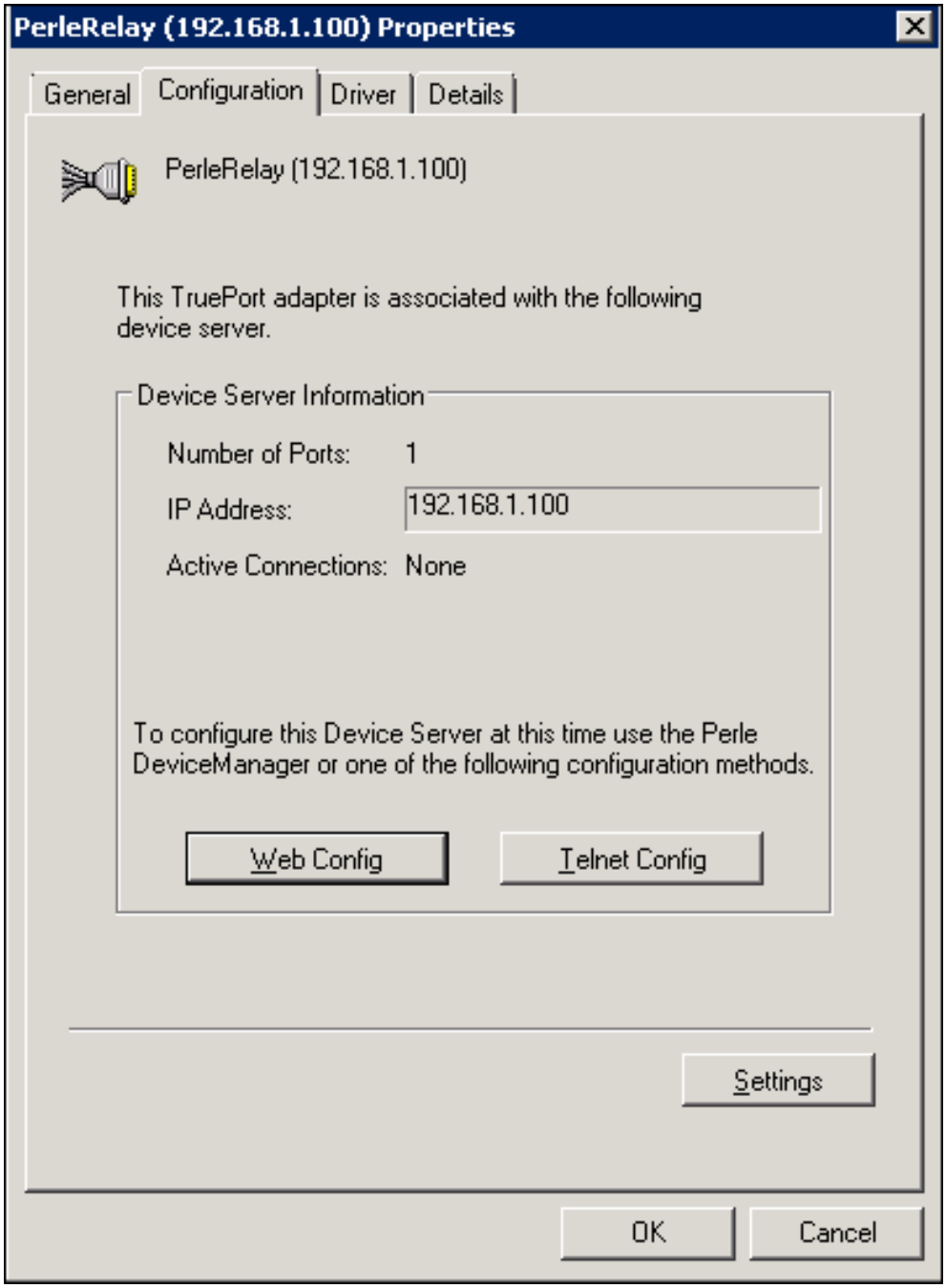
I/O Access Settings

1. Start the **TruePort Management Tool**, select the Perle device you want to configure, and click **Properties**.

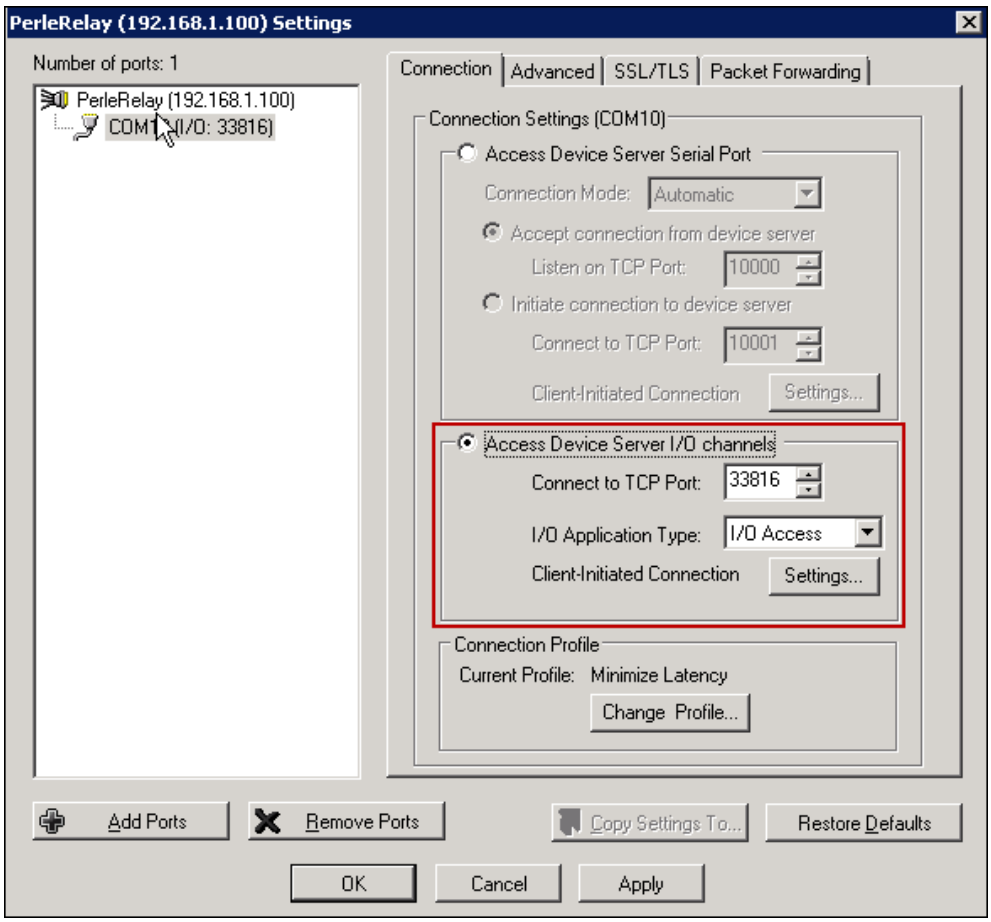


2. Select the **Configuration** tab.

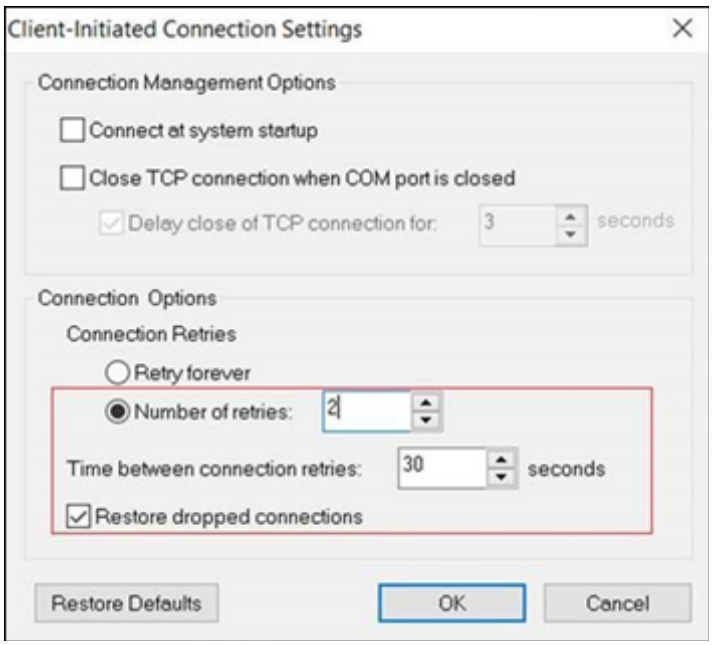
3. Click **Settings**.



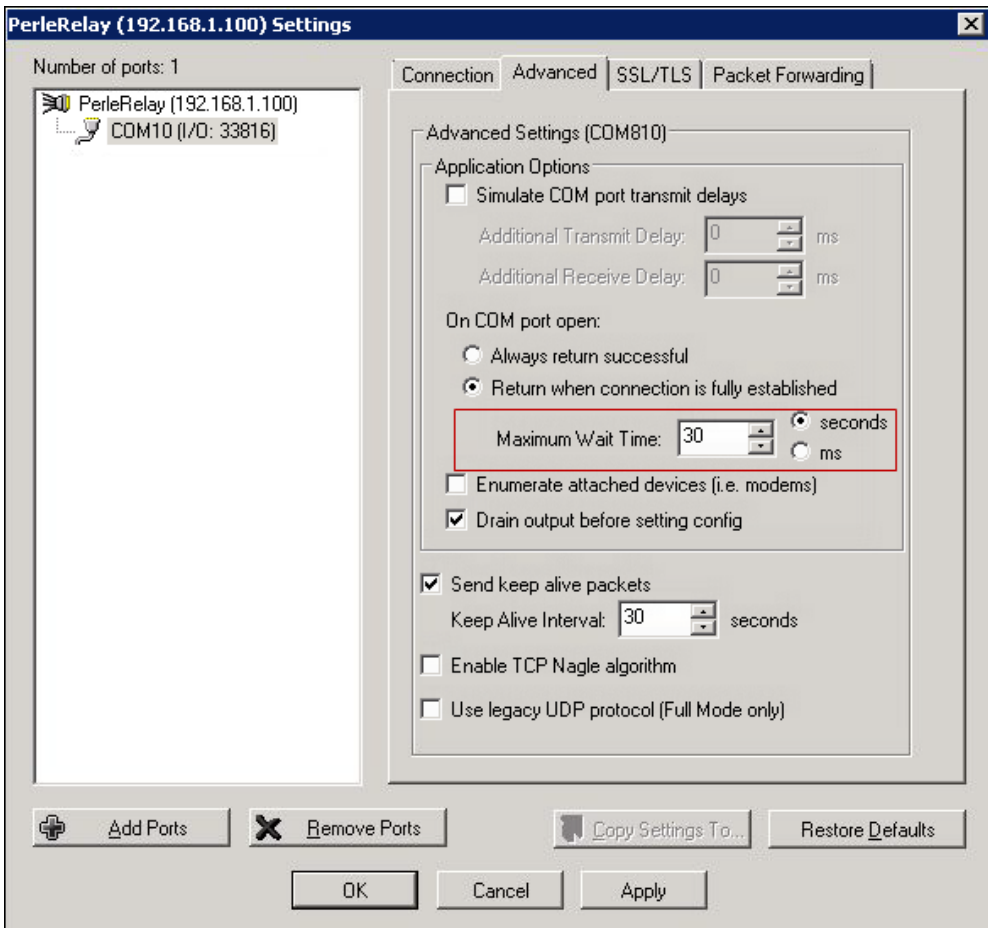
4. If you originally created two COM ports for this device, select one to use for I/O access. If the COM port you selected is being used, the other COM port should be reserved for serial communication. If you have not added a second COM port, you may do so by clicking the **Add Ports** button at the bottom of the window.
5. Select the **Connection** tab.
6. Select the **Access Device Server I/O channels** option.
   - Select the TCP port that was configured on the device for I/O access.
   - In the **I/O Application Type** drop-down list, select **I/O Access**.



7. Click the **Settings** button next to **Client-Initiated Connection**.
   ⇨ The following window displays:

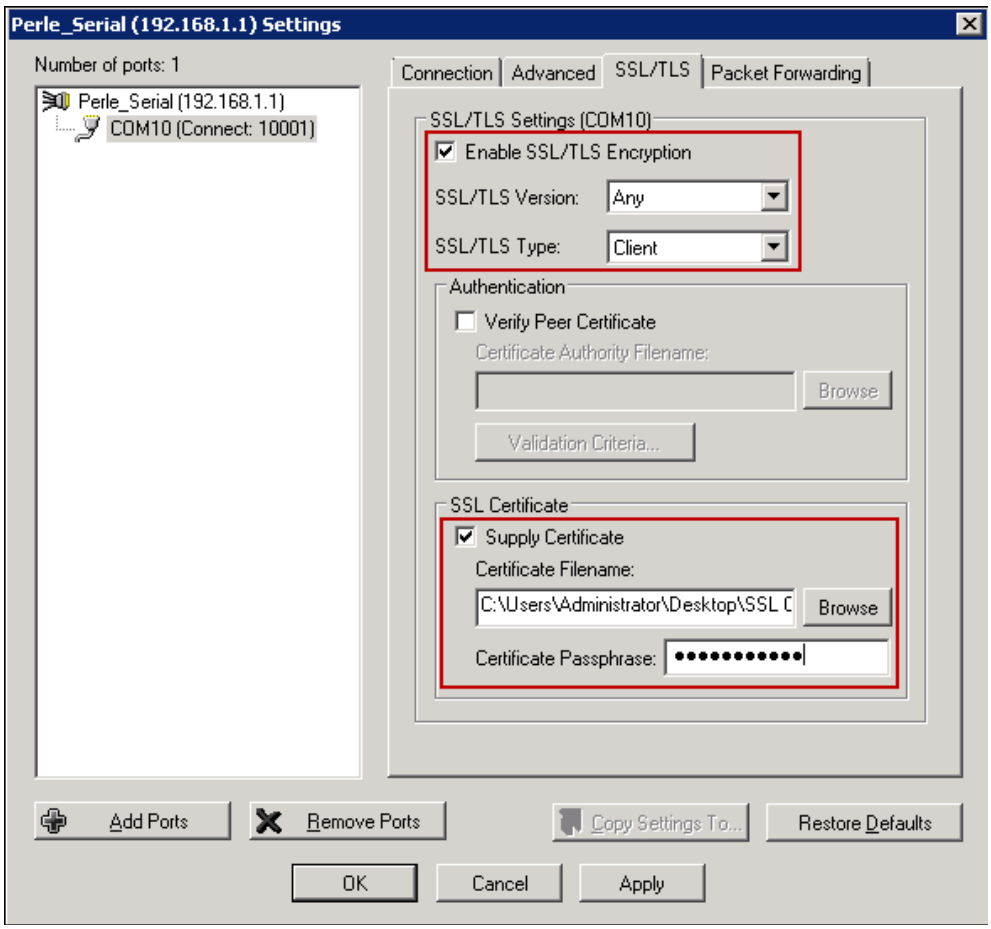


8. Select the **Connect at system startup** check box.
9. For **Connection Retries**, select the **Retry forever** option.
10. Click **OK.**
11. Select the **Advanced** tab.



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

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



14. Select the **Enable SSL/TLS Encryption** check box.
15. Set the **SSL/TLS Version** field to **Any**.
16. Set the **SSL/TLS Type** field to **Client**.
17. Select the **Supply Certificate** check box.
18. Click the browse button and select the combined root certificate. Refer to the Device Configuration section for more information on combining a root certificate.
19. Enter the password in the **Certificate Passphrase** field.
20. Click **Apply** and then **OK**.
21. Restart the **Perle TruePort Service** from the SMC.

⇨ The TruePort driver is ready for I/O access.

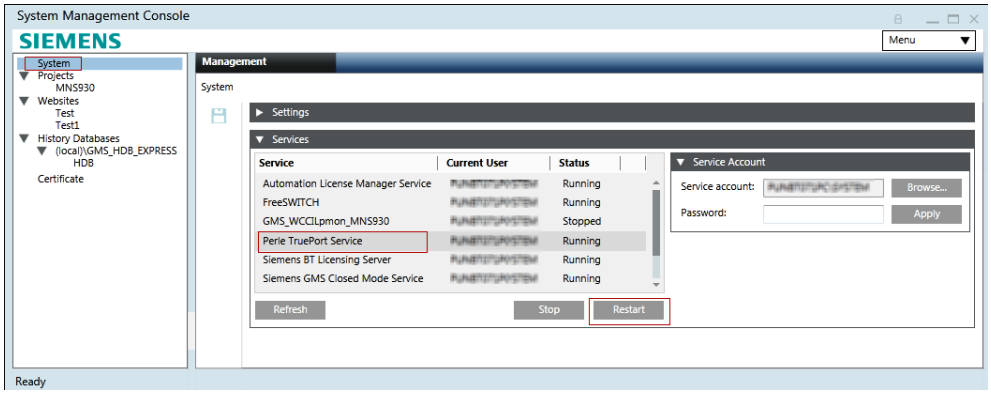


Fig. 44: Restarting the Perle TruePort Service

Relay Output Device 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, if the device does not get connected after the **Check Status Rate** duration.

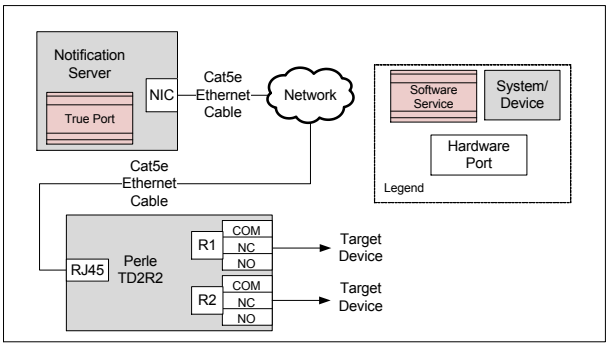
Solution: Perform the following steps in sequence until the device gets connected after a particular step. After each step, wait for the **Check Status Rate** duration and monitor the device connection status.

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

Relay Output Device

This section contains general reference information about Notification and how the Relay Output device is integrated. For procedures and workflows, see step-by-step section.

The Perle TD2R2 device serves as an SSL-encoded relay output enabling messages to trigger any target device, such as a siren or a strobe light. When a incident is initiated the Perle relay activates for the duration of the message lifecycle or deactivates after a specified time according to settings established by the operator.



1.29 RSS CAP

RSS CAP

This section contains additional procedures for integrating the RSS CAP device.

For workflows, see the Creating and Configuring Web Feed Input Device section.

Event Triggers Configuration

This section describes the configuration of event triggers for the Web Feed Input. Note that the event triggers can be configured both at the driver level and also when configuring the Web Feed input device under the Field Network. In either case, rules are set to analyze different parts of the feed item. An example of the XML feed is listed in the CAP feed XML Sample section. This example will be used as a basis for the different configurations in the following sections.

Configuring an Event Trigger

▷ The user must have added either the **ASCII Input Perle** or **Web Feed Input** device.
For more information on adding devices, refer to the Notification Devices section.

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

1. In System Browser, select **Management View**.
2. Select **Project** > **Management System** > **Servers** > **Main Server** > **Drivers**.
3. Select the **Driver Instance** (ASCII Input or Web Feed Input) for the desired Input Rules creation.
4. Select the **MNS Driver Editor** tab.
5. Open the **Event Triggers** expander.
6. Click **Add** on the bottom left corner of the expander.
7. Enter a **Name** for the Event Trigger.
8. Click **Add** under **Input message filter rules** and do the following:
   a. Enter a **Name** for the Input message filter rule.
   b. (*Optional*) Select the **Negated** check box to prevent certain text patterns that must not be present in the Input Data for the Event Trigger to trigger the event.
   c. (*Optional*) Specify an **Xpath** expression to narrow down the scope for the subsequent **Regular expression** match.
   d. Enter the **Regular expression** for text matching in the Input Data.
9. Select the **Event trigger settings** expander, do the following:
   a. Select the **Trigger enabled** check box to analyze and filter data.
   b. Select the **Event category of triggered event** from the drop-down list.
10. Select the **Event field mappings for triggered event** expander, do either of the following:
    a. Specify a static **Default value** OR
    b. Specify a **Regular expression**, plus optionally an **Xpath** expression (for XML documents) that dynamically extract data from input messages.
    NOTE: **Name**, **Xpath**, **Regular expression**, and **Default value** are case-sensitive.
11. Click **Save**  .

⇨ The Event Trigger is saved.

Updating an Event Trigger

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

1. In System Browser, select **Management View**.
2. Select **Project** > **Management System** > **Servers** > **Main Server** > **Drivers**.
3. Select the **Driver Instance** requiring Input Rule updating.
4. Select the **MNS Driver Editor** tab.
5. Open the **Event Triggers** expander.

6. Update the required fields.
   For more information on the fields, please refer to the *Configuring an Event Trigger* section.
7. Click **Save** .

⇨ The Input Rule is saved with the updates.

Deleting an Event Trigger

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

1. In System Browser, select **Management View**.
2. Select > **Project** > **Management System** > **Servers** > **Main Server** > **Drivers**.
3. Select the **Driver Instance** with the target Input Rule to be deleted.
4. Select the **MNS Driver Editor** tab.
5. Open the **Event Triggers** expander.
6. Click **Remove** at the bottom left corner of the expander.
7. A confirmation message displays.
8. Click **Yes**.
9. Click **Save** .

⇨ The Input Rule is deleted.

Raw Input Data Analysis

▷ The user must have added either the **ASCII Input Perle** or **Web Feed Input** Device.
For more information on adding devices, please refer to the Notification Devices section.

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

1. In System Browser, select **Management View**.
2. Select **Project** > **Management System** > **Servers** > **Main Server** > **Drivers**.
3. Select the **Driver Instance** (ASCII Input or Web Feed Input) for which the user wants to analyze input data.
4. Select the **MNS Driver Editor** tab.
5. Open the **Input Message Analysis** expander.
6. Click **Start** next to **Start/stop capturing input messages** to start capturing messages from the Input Devices.
   ⇨ A preview of the captured message displays in **Message preview**.
   ⇨ Under **Captured messages**, the **Timestamp** at when the message was captured displays.
7. Click the **Stop** button to stop capturing messages.

Input Message Filter Rules

1. Click **Add** to create a new message filter.
   NOTE: Multiple filter rules can be added to each trigger rule but even if one of the filter rules matches the input feeds, the event is generated.
2. Enter a name for the filter rule in the **Name** field.
3. Select the **Negated** check box if a negative rule is being set.
4. Enter the XML path of the field for patterns to be matched by the regular expression in the **Xpath (Optional)** field. For example, for the sample XML Feed in CAP feed XML Sample, look for text in the event field, and then enter the value **alert/info/event/text()**.
   NOTE 1: When xpath is not defined, the value specified in the **Regular Expression** field is applied on the entire feed content.
   NOTE 2: Configuration of an XPath must not be done if the Web Feed item is in HTML format. This will not result in the alarms and automatic incident triggering.
5. Enter the text pattern to search for a match within the feed item in the **Regular Expression** field. A simple example can be the occurrence of a word or a phrase. For example, for the sample XML feed in CAP feed XML Sample where Xpath is set to look in the event field. To check if the event is of the type Winter Weather Advisory, enter the value **(?<ValueToExtract>Winter Weather Advisory)**. For the sample HTML feed in Practical Example of HTML and to check if the input feed is of Wal-Mart, enter the value **(?<ValueToExtract> Wal-Mart)**.

Event Trigger Settings

1. Select the **Trigger Enabled** check box to enable triggering of the management station alarm if conditions set in message filter rules are satisfied.
2. Select the category of the triggered event from the **Event Category** drop-down list.
   NOTE:
   Set the rules based on which content is extracted from the feed item and added to the alarm that is being raised.

Event Field Mappings for Triggered Text

When triggering is enabled, the management station alarms are raised. Configurations can be set to extract content from the feed item and fill in the **Event Cause** and **the Additional Information** fields of the management station alarm.

Event values can be configured that will eventually be passed into the management station alarm. The text passed can then be used to match against the rules set for incident triggers.

Event Cause

- **Default Value:** Set the default value for the event cause. For example, Winter Weather advisory message received. Refer to the table in the *System Usage of Configurations* section for the information on when the value defined in this field is used.
- **Xpath (Optional):** Set the Xpath for the XML document from which text needs to be extracted. For example, for the sample XML in the CAP feed XML Sample section the value **alert/info/ headline/text()** will fetch the text from the **headline** field of the feed. Refer to the table in the *System Usage of Configurations* section for the information on when the value defined in this

field is used.
NOTE: Configuration of an XPath must not be done if the Web Feed item is in HTML format. This will not result in the alarms and automatic incident triggering.

- **Regular Expression (Optional):** Set the regular expression to extract the text from the feed item to be passed along to the management station alarm. Refer to the table in the *System Usage of Configurations* section for the information on when the value defined in this field is used.

Additional Information

The **Additional Information** field is configured similar to the **Event Cause** field. The only difference is that the extracted values are used to fill the **Additional Information** field of the alarm being raised.

System Usage of Configurations

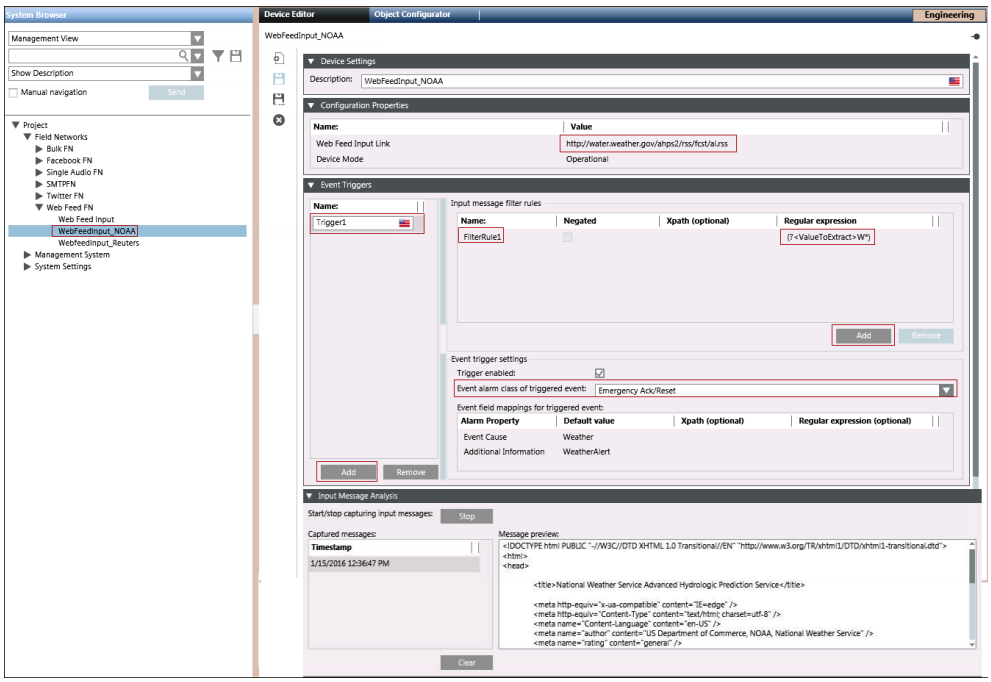
The table below details the behavior of the system when one or more fields described above are configured. An **X** indicates a value defined in that field.

Default Value	XPath	Regular Expression	Behavior
X			The text in Default value is set as the value for the respective field of the Alarm.
	X		The text contained in the field defined by the XPath is used to fill in the respective value in the alarm. The default value, if set, is ignored.
X	X		
		X	The Regular expression is applied to the whole feed item and the resulting text is used to fill in the respective value in the alarm. The default value, if set, is ignored.
X		X	
	X	X	The regular expression is applied only to the text in the field defined by the XPath expression. The resulting value is used to fill the appropriate field in the alarm. The default value, if set, is ignored.
X	X	X	

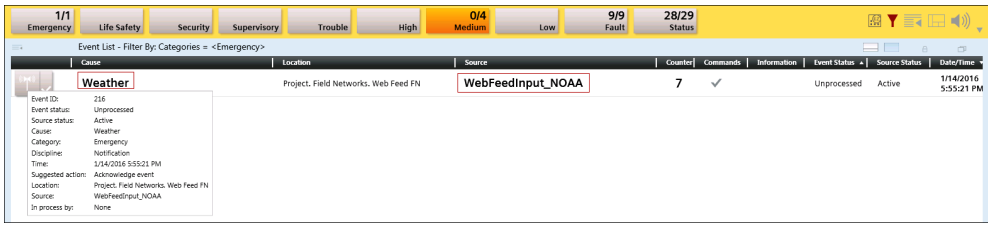
Event Triggering Example

Scenario: Configure an Event Trigger for a weather feed from NOAA or a CAP feed.

1. Configure a Web Feed Input Device. For example, **WebFeedInput_NOAA**.
2. Select the **Configuration Properties** of the device, enter the URL of the NOAA site or the URL of the CAP Feed.



3. Select **Operational** from the **Device Mode** drop-down list.
4. Select the **Input Message Analysis** expander, click **Start** to capture the input message.
5. Select the **Event Triggers** expander, click **Add** and enter a name for the Event Trigger. For example, **Trigger1**.
6. Select **Input message filter rules**, click **Add**.
7. Enter a name for the filter rule in the **Name** field. For example, **FilterRule1**.
8. Enter a regular expression in the **Regular expression** field.
9. Select the **Trigger enabled** check box.
10. Select the event alarm class from the **Event alarm class of triggered event** drop-down list. For example, **Emergency Ack/Reset**.
11. Enter the event cause in the **Event Cause** field.
12. Enter the additional information about the event in the **Additional Information** field.
13. Click **Save** .
    ⇨ Event will be raised when the feed is captured from the configured URL.



1.30 Single Zone Audio Device

Single Zone Audio Device

This section provides reference and background information for integrating the Single Zone Audio device. For procedures and workflows, see the step-by-step section.

The Single Zone Audio Driver is intended for interfaces that require a single audio source with or without relay. Currently, for DTMF devices, the Single Zone Audio Driver is used without relay.

Below is the general overview of how delivers SIP-based audio for deployments in which Notification must deliver audio to an external speaker system. The Single Zone Audio Driver can utilize the following devices to deliver audio and to activate audio circuits.

- **Line Level Audio (LLA) device (Barix Annuncicom 200 and CyberData SIP Adapter)**
- **IP Relay (Perle IOLAN SDS1 TD2R2)**

The Line Level Audio (LLA) device, integrates with through an IP-PBX service using the SIP protocol over TCP/IP. The LLA converts the SIP audio session to a line-level audio signal. This signal can be used as an external input source for any generic audio receiver that meets the requirements of the LLA.

For details on wiring and the LLA output specifications for the Barix Annuncicom 200 device, refer to the Audio Output section.

For details on wiring and the LLA output specifications for the CyberData SIP Adapter, refer to the Audio Output section.

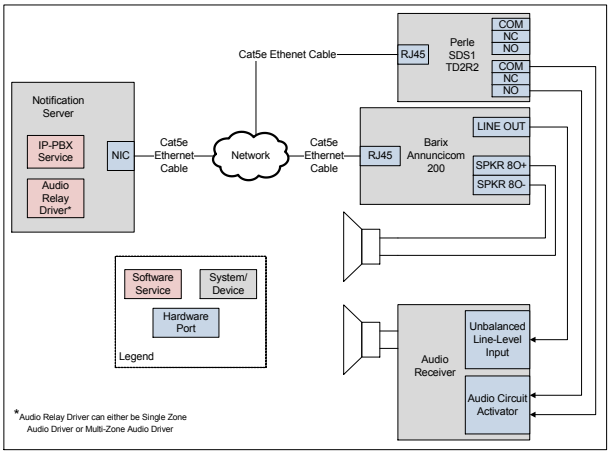
The optional Perle SDS1 TD2R2 provides relays for contact closing. Prior to sending audio, the appropriate relay on the TD2R2 will be activated providing a relay contact closure. External audio receivers are expected to recognize this change and perform the necessary steps to allow audio to pass through and be amplified. If the deployment requires relay contact closure, refer to the Perle TD2R2 Device section.

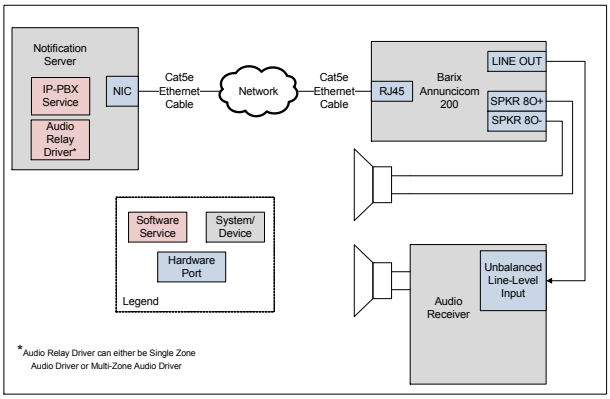
In addition to delivering audio to an external speaker system using the optional IP relay, the single zone audio driver can also deliver audio to a pure SIP device that has auto-answer capabilities.

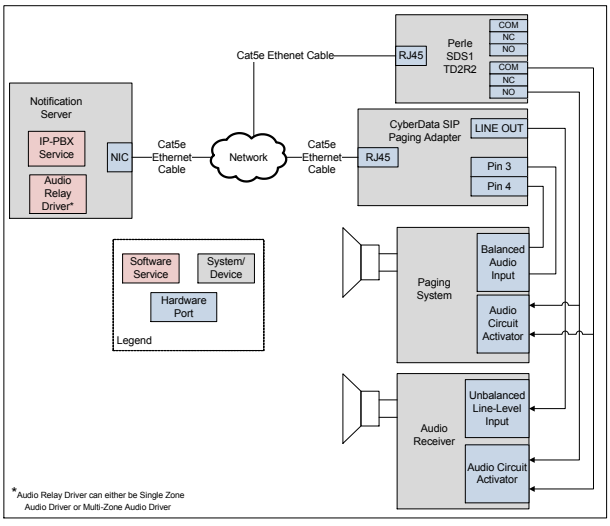
The ability to send a DTMF sequence prior to audio is also available. Details on using this feature are provided in the Generating DTMF Sequences section.

In summary, the following configurations are supported by the single zone audio driver:

Deployment	Audio Device Used	IP Relay
Audio through LLA with IP relay	Barix (Barix Annuncicom 200)	Perle TD2R2 Device
	CyberData SIP Adapter (CyberData SIP Adapter)	
Audio through LLA without IP replay	Barix (Barix Annuncicom 200)	None
Audio through SIP auto-answer	CyberData IP Speaker (CyberData IP Speaker)	None
Audio through SIP with DTMF	None. Skip to section Generating DTMF Sequences	None

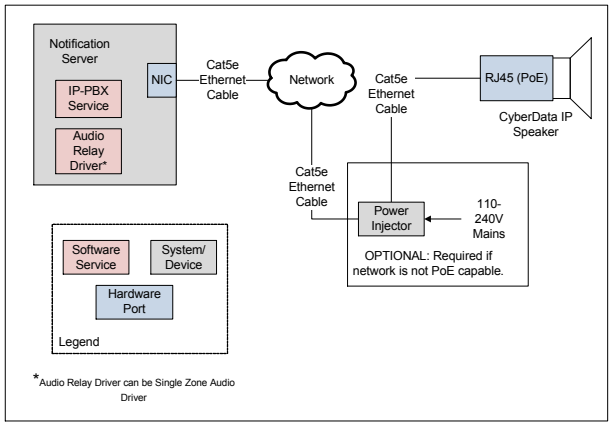






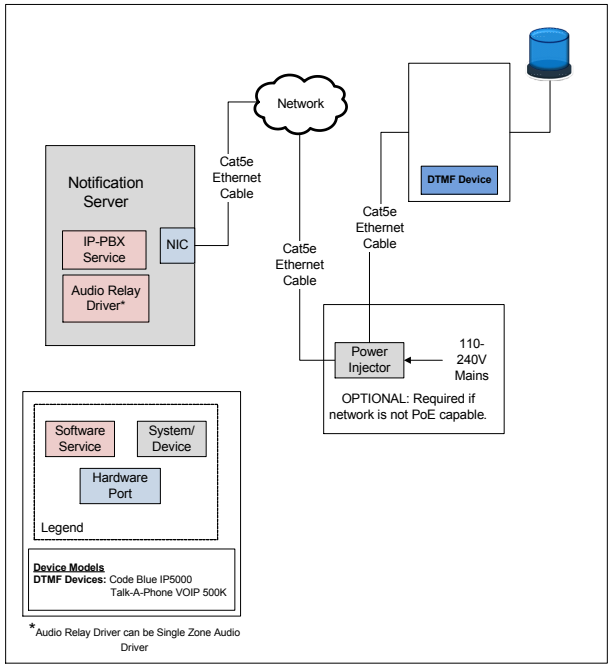
- **CyberData IP Speaker**

The Single Zone Driver provides the status of the CyberData IP Speaker extension to the system. The CyberData IP Speaker integrates with through an IP-PBX service using the Session Initiation Protocol (SIP) over Transmission Control Protocol / Internet Protocol (TCP/IP).



- **Dual-tone multi-frequency (DTMF) Device**

provides an additional way to perform activations on telephone audio devices using Dual-tone multi-frequency signaling (DTMF tones), for Voice-over-Internet Protocol (VoIP) telephone devices. Telephone audio devices may be SIP devices directly connected to and registered with FreeSwitch. However, this feature also applies to telephone devices that FreeSwitch reaches through a telephony gateway or a customer private branch exchange (PBX). Such telephone devices can be VoIP devices. The user configures a DTMF activation and/or deactivation sequence for individual audio zone device nodes. will automatically play these sequences whenever a Live Announcement or an audio message is sent to the audio zone device.



provides the following additional features when playing audio messages through Single Zone Audio drivers:

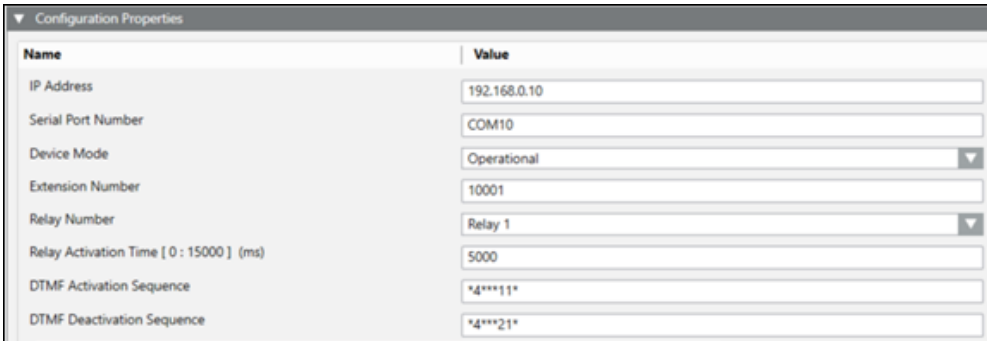
- **Repetitions and intervals**: will repeatedly play the audio content of messages on the targeted audio devices, up to the number of repetitions configured in the audio content, and spaced out as specified through the configured interval.
- **Synchronized playing**: When the audio content of a single message needs to be played on multiple audio devices, ensures that the played audio content is synchronized across all devices. This allows listeners to hear the resulting output as if it were coming from a single speaker.

NOTE 1:
The capability to play audio content in a highly synchronized fashion on multiple SIP-based audio devices can only be guaranteed for devices from the same manufacturer and possibly the same series or model. The audio content played on devices from different manufacturers might result in a slight but noticeable lag in the output heard by listeners. This can be due to the differences in device-internal

processing speed of the participating devices.
NOTE 2:
During a Live Announcement or audio message, if any SIP-based audio device gets disconnected due to connectivity issues, the system makes three attempts to rejoin that SIP-based audio device.
NOTE 3:
It is the responsibility of the user to find out the DTMF sequences that are required to interact with the connected DTMF-capable telephone devices. For example, from device documentation provided by the specific device manufacturer.

When multiple messages are active and share some or all of the targeted audio devices, will suppress playing audio content of messages with lower priority based on the priority tolerance rules.

Single Zone Audio Zone Workspace



- **IP Address :** Enter the IP address of the Perle device, if Perle device is used to activate Single Audio Zone. In case of a Single Audio Zone without a Perle device, enter value as -1.
- **Serial Port Number**: Enter the number of Serial COM port created by TruePort for a particular Perle device.
- **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.
- **Extension Number**: Set the **Extension Number** to the extension of the Line Level Audio device connected to the fire panel.
  NOTE: For details on creating extensions for the Line Level Audio device, refer to the Configuring Telephony Device.
- **Relay Number**: Set **Relay Number** to the relay used for this particular audio interface.
  NOTE 1: There is no need to set the Relay Number when the Serial Port Number is set to **-1**. For others, it can be set to either **1** or **2**. For using a **Single Audio Zone** with a Perle device, set the **Serial Port Number** to the COM port that was configured for IO access for the Perle device (for example, **COM100**). For using a **Single Audio Zone** without a Perle device, set the **Serial Port Number** to **-1**.
  NOTE 2: For DTMF devices, a **Single Audio Zone** is used without a Perle device. Set the **Serial Port Number** to **-1**, if using a DTMF device.
  NOTE 3: To check the COM ports that were used by the device, open the TruePort Management Tool.
- **Relay Activation Time**: Enter the relay activation time in the **Relay Activation Time** field.

- **DTMF Activation Sequence**: If using a DTMF device, set the DTMF activation sequence in the **DTMF Activation Sequence** field. For more information, refer to Generating DTMF Sequences.
- **DTMF Deactivation Sequence**: If using a DTMF device, set the DTMF deactivation sequence in the **DTMF Deactivation Sequence** field.

Single Zone Audio Device

This section provides additional procedures for integrating the Single Zone Audio device.

Installing Single Zone Audio Device

Line Level Audio Device

Barix Annuncicom 200

Hardware Prerequisites

Before proceeding, ensure that the following items are available:

- Barix Annuncicom 200 Line Level Audio device
- 9-30 VDC or 12-24 VAC, 500mA minimum
- Category 5 Ethernet cable

Power

Power to the device can either be supplied by the barrel connector or the terminal block labeled as PWR (refer image below), but not both. Both inputs are internally connected, so one can be used as an output for other devices.

Pin 1 of the terminal connector is ground. Pin 2 is power.

NOTE:
For Barix Annuncicom 200 LLA, Power over Ethernet (PoE) is also an option for supplying power to the device.

Ethernet

1. Plug one end of the Ethernet cable into the RJ45 jack on the LLA.
2. Connect the other end of the Ethernet cable to the network jack.
   NOTE:
   The LLA obtains an IP address using DHCP by default. To assign a static IP address or if DHCP is not present, refer to the *Obtaining an IP Address Manually* and the *Changing the IP Address* sections.

Audio Output

An audio receiver is a device that amplifies an external analog audio signal and distributes that signal to one or more speakers. Examples are an audio/video receiver, a voice-enabled fire panel system, a radio-base station, and an intercom/ public announcement system.

There are two methods to supply audio from the LLA:

Method 1: Use the LINE-OUT RCA socket.
NOTE 1: The tip of the RCA plug is a signal.
NOTE 2: The Line Out has 50Ω output impedance with a range of 1-3 Vp-p

Cable requirements are as follows:

1. >= 22 awg shielded, stranded cable wire
2. < 6ft length

Method 2: Use the “SPKR +” and “SPKR –“ terminals on the LLA.
NOTE: This interface can deliver 1 Watt into an 8Ω load.

Cable requirements are as follows:

1. >= 22 awg shielded, stranded cable wire
2. < 6ft length
3. Twisted wire pair
   NOTE:
   Refer to the Diagram 1 in the Device Overview section for an illustration regarding how the various components are connected for Barix Annuncicom 200 with Perle device. Refer to the Diagram 2 in the Device Overview section for an illustration regarding how the various components are connected for Barix Annuncicom 200 without Perle device.

Hardware Verification

After completing the mechanical and electrical installations, verify the status LED is solid green color. If not, perform the steps outlined in the following sections:

- Obtaining an IP Address Manually
- Upgrading the LLA Firmware
- Changing the IP Address
- Configuring the SIP Endpoint

Obtaining an IP Address Manually

The Barix Annuncicom 200 device is configured for DHCP. If the device is unable to obtain an IP address, do the following steps to assign a temporary IP address:

1. Either use a network cable to link the Barix Annuncicom 200 device and the computer directly, or connect the Barix Annuncicom 200 device to the computer through the network switch and power the device.
   NOTE: Ensure that there is a valid static IP address configured. For example, a computer having subnet mask as 192.168.0.0 can have a static IP as 192.168.0.2.
2. Open the Windows Command prompt (cmd.exe).

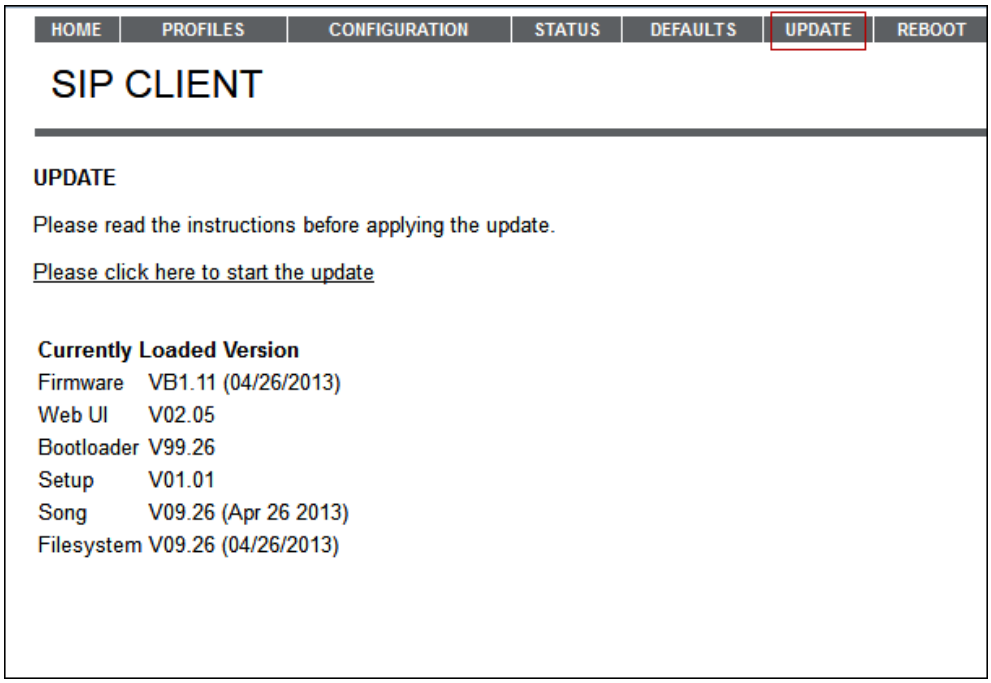
3. Use the **Ping** command to ensure the usage of a free IP address (one not already used by another device in the network).
   NOTE: For example, if the computer has the IP address 192.168.0.2, and there is a need to check if 192.168.0.6 is free. Enter Ping 192.168.0.6. If there is no reply, then it means that 192.168.0.6 is available.
4. Look for the Barix Annuncicom 200's MAC address printed on a label on the bottom of the device (12 hex digits, separated by a hyphen every 2 digits). For example, if the MAC address is 00-08-E1-00-B1-77, enter the following in the Windows command prompt: **arp -s 192.168.0.6 00-08-E1-00-B1-77.**
5. In the command window, enter **telnet 192.168.0.6 1** to make the Barix Annuncicom 200 listen to the IP address **192.168.0.6**.
   NOTE: The Barix Annuncicom 200 will immediately refuse the connection on port 1, but will be available for browser access as long as the device stays powered on.
6. To check if the Barix Annuncicom 200 is responding, use the Ping command again. Enter **Ping 192.168.0.6**. If there is no reply, the IP address **192.168.0.6** can access the Barix Annuncicom 200 using a web browser. If the device is unreachable through the **Ping** command, refer to the manufacturer's manual for additional methods.

Upgrading LLA Firmware

The latest SIP firmware can be found on the Barix website:
http://www.barix.com/downloads/downloads-firmware/sip-client-application/
This document has been tested with firmware version 2.12.

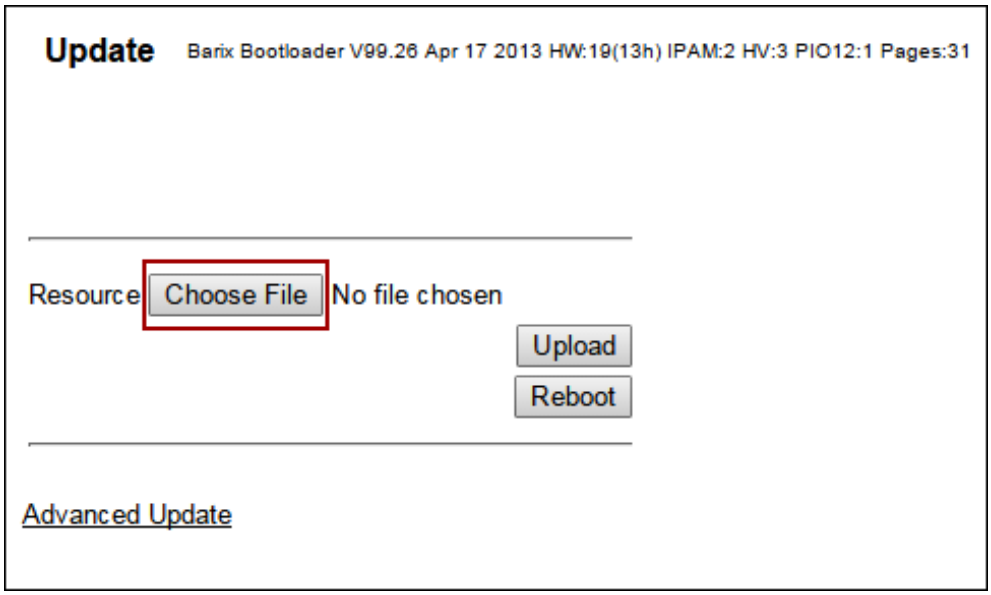
Disclaimer:
Prior to the commissioning of a system, a compatibility check should be performed for all devices and services to be integrated. Refer to the *Notification System Description* document for compatibility information.

1. In a web browser, enter the IP address of the Barix Annuncicom 200 in the URL.
2. Select the **UPDATE** tab.

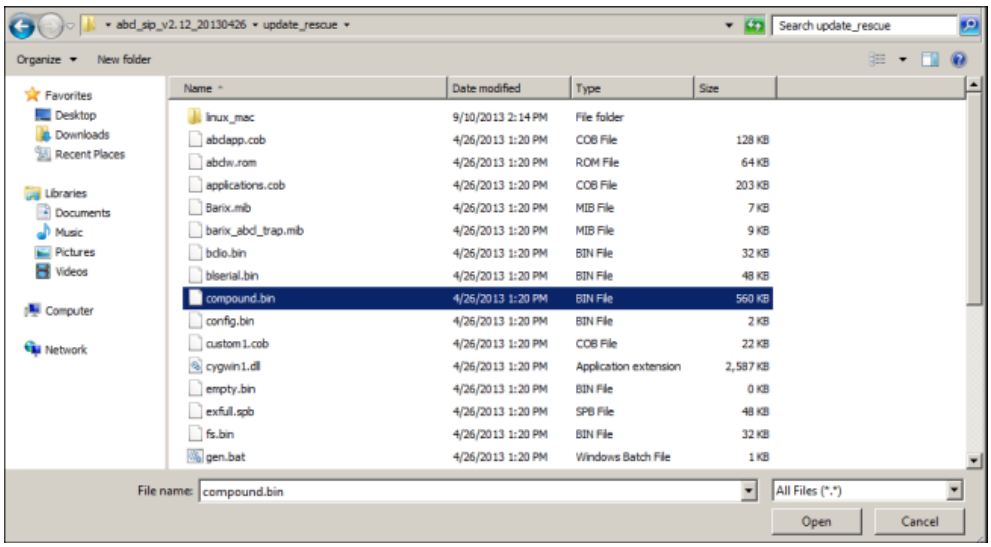


3. In the **UPDATE** window, click **Please click here to start the update**.
   ⇨ The device resets and a countdown is displayed.

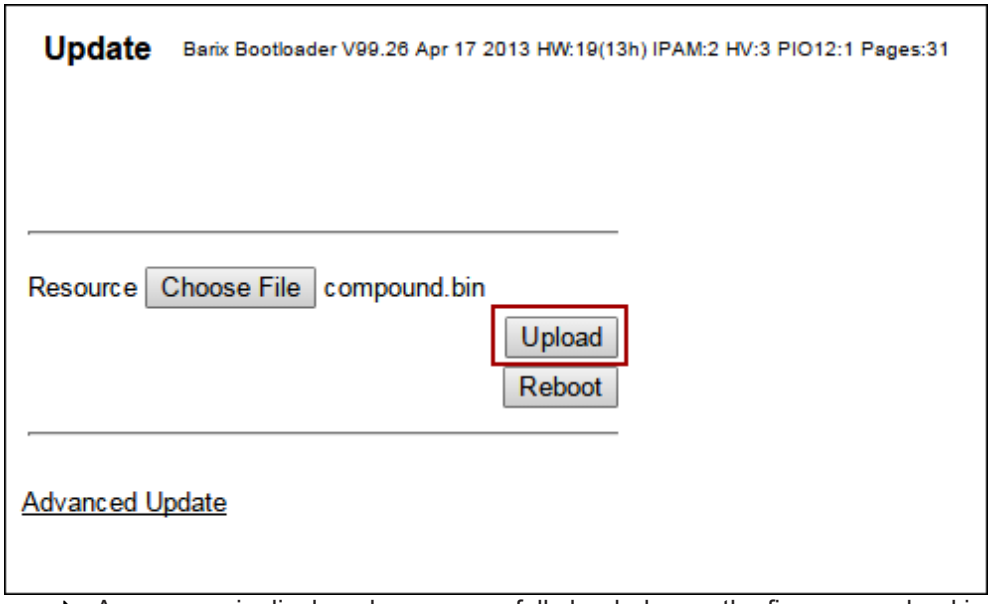
4. Once complete, the **Update** window is displayed, click **Choose File**.



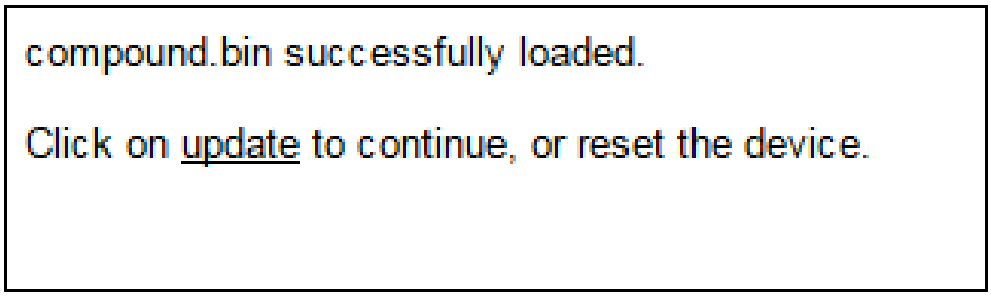
5. Select **abcl_sip_vXXXXX** > **update_rescue** and select **compound.bin** file.
6. Click **Open** as shown in the example below:



7. Click **Upload**.
   ⇨ The device may take up to a minute to upload and flash the new firmware.



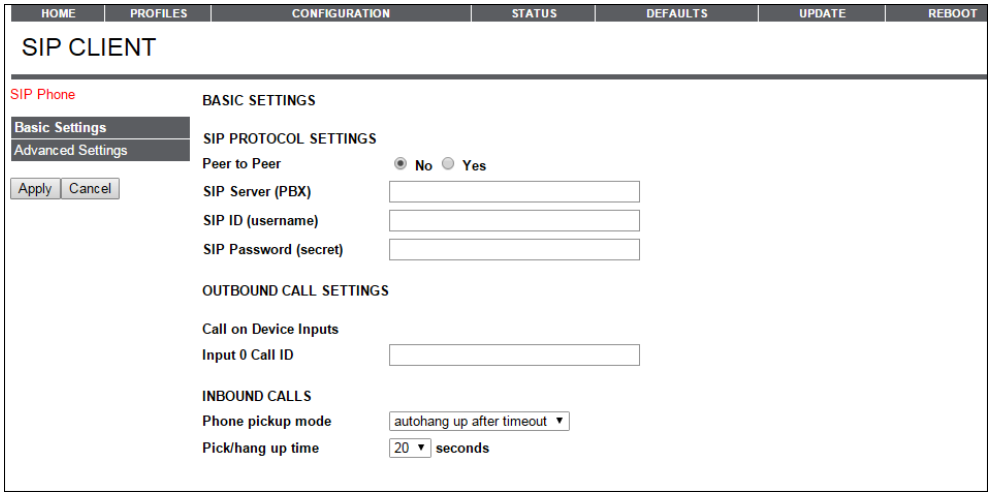
   ⇨ A message is displayed as successfully loaded once the firmware upload is complete.



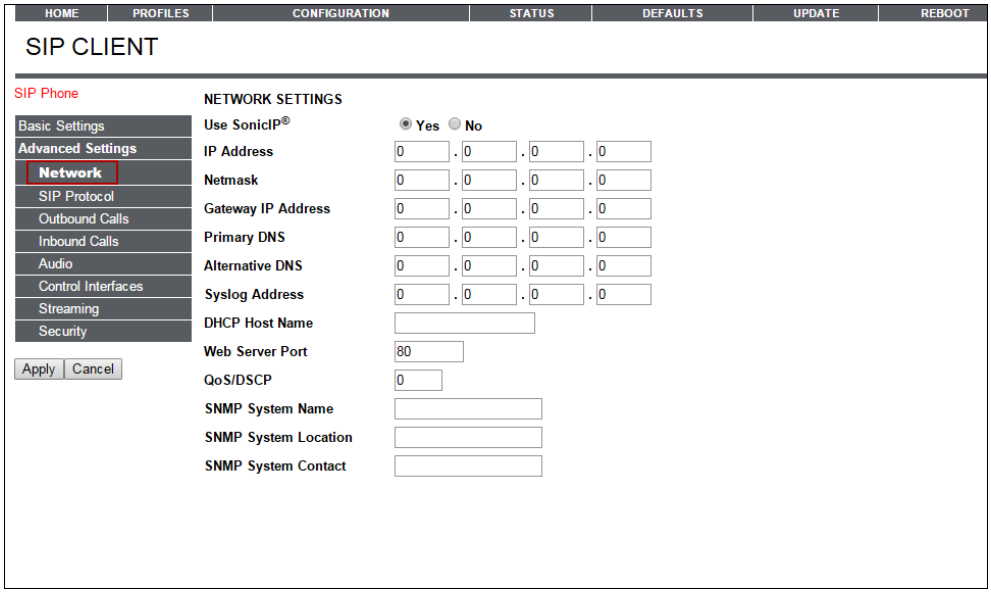
8. Reboot Barix Annuncicom 200 by disconnecting and then reconnecting the DC power supply.

Changing the IP Address

1. In a web browser, enter the IP Address of the Barix Annuncicom 200 in the URL.
2. Select the **CONFIGURATION** tab.



3. Select **Advanced Settings > Network**.



4. Enter the appropriate values for the **IP Address** and **Netmask** as per the IT infrastructure.
   NOTE 1: It is strongly recommended to specify a Gateway IP Address to ensure proper routing of the SIP call.
   NOTE 2: For DHCP, the required settings will automatically be populated by the DHCP server. By default, entering an **IP Address** value of 0.0.0.0 defaults to DHCP. Use the **Help** menu on the right-hand side of each configuration window for details on all the parameter fields.
5. Click **Apply**.
6. Select the **REBOOT** tab.

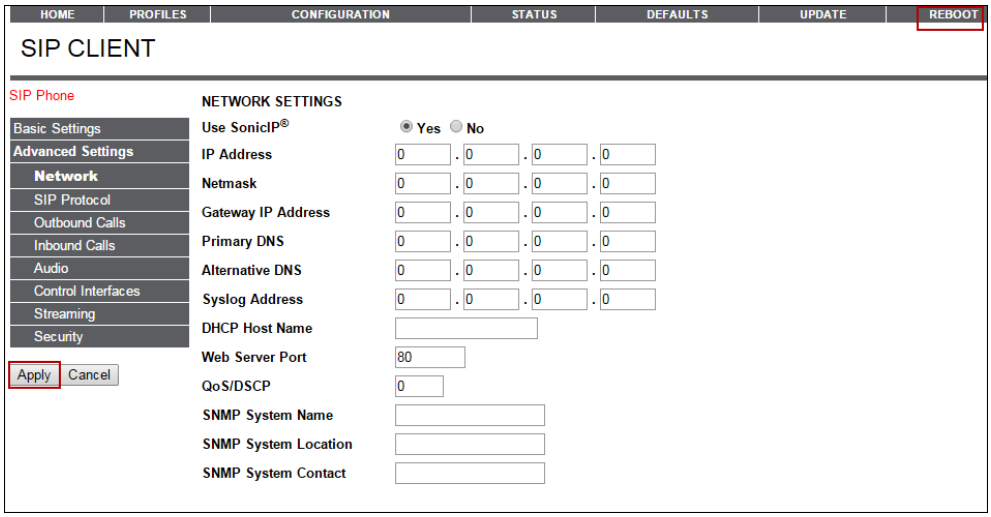
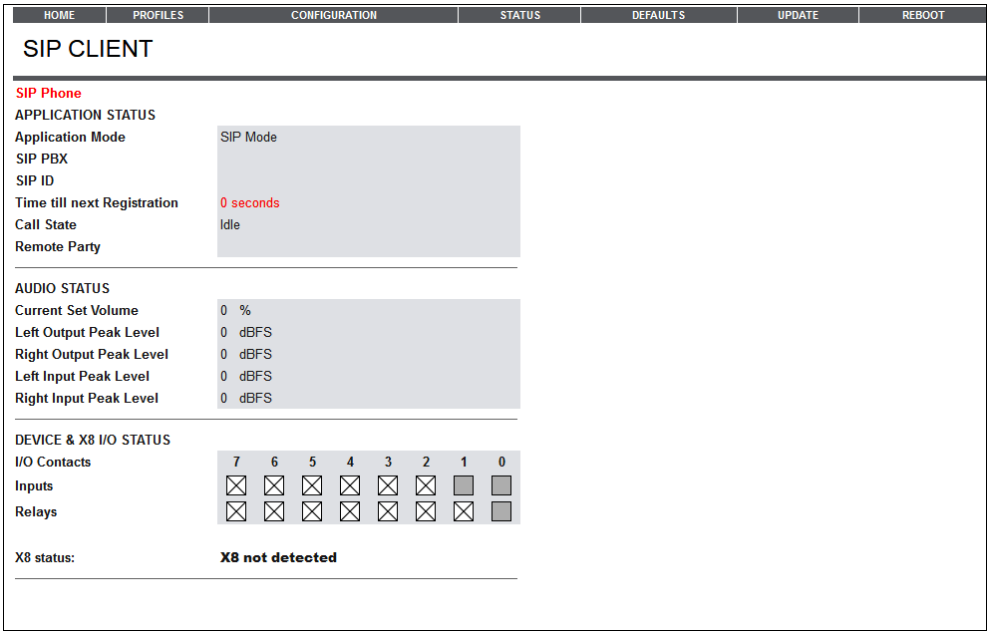


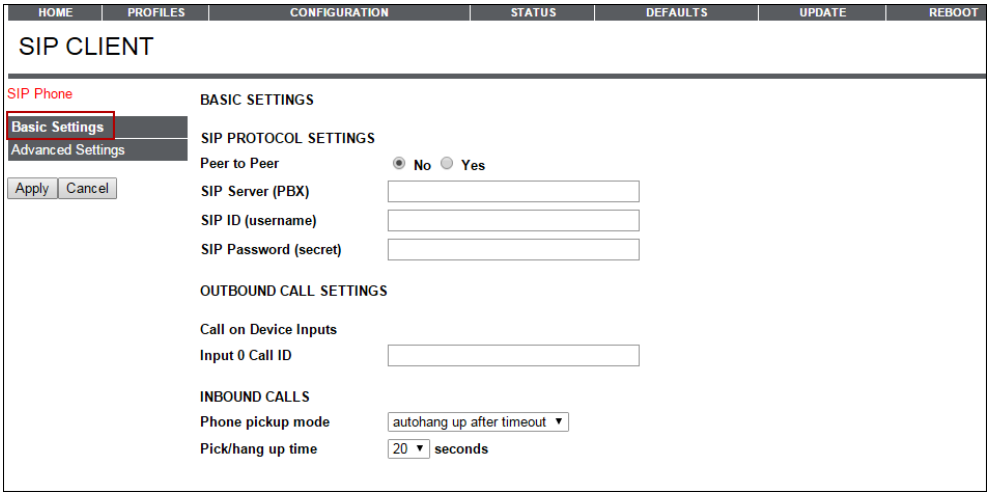
Fig. 45: Reboot Tab

Configuring the SIP Endpoint

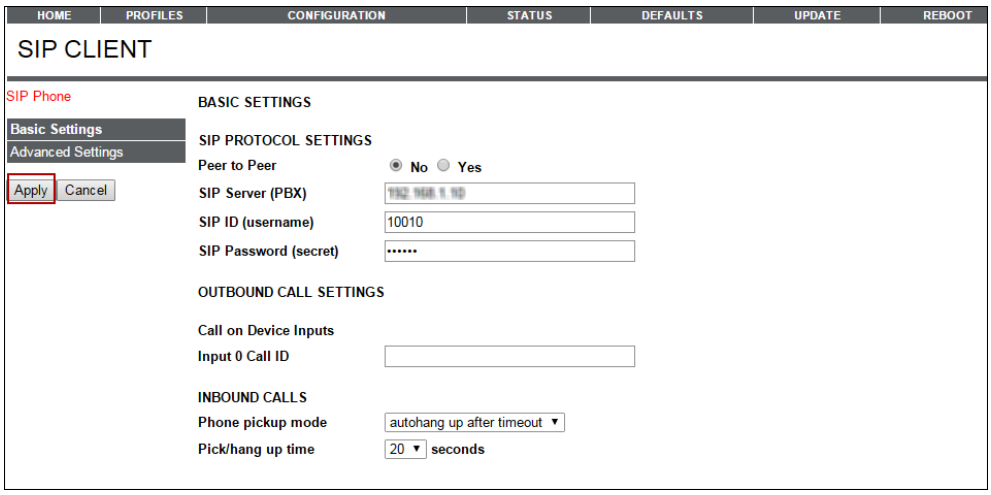
1. In a web browser, enter the IP Address of the Barix Annuncicom 200 in the address bar.



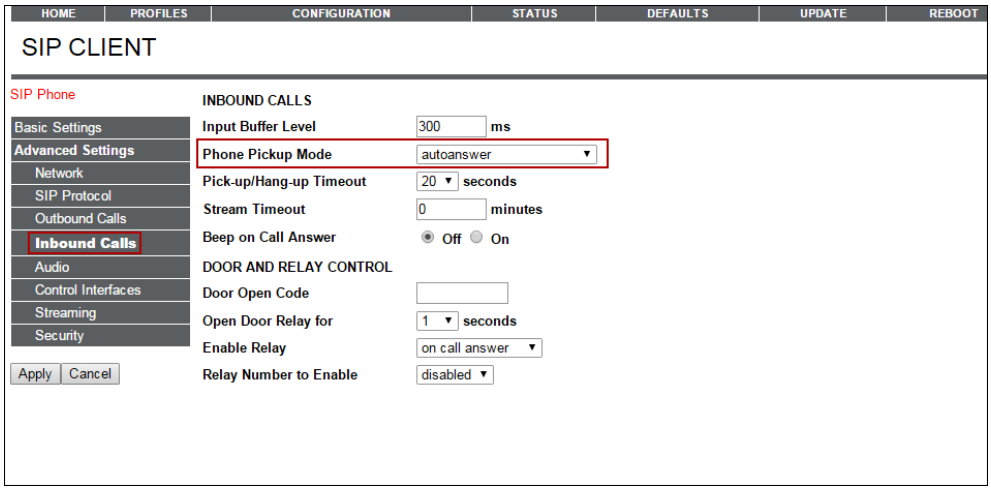
2. Select the **CONFIGURATION** tab.
3. Click **Basic Settings**.



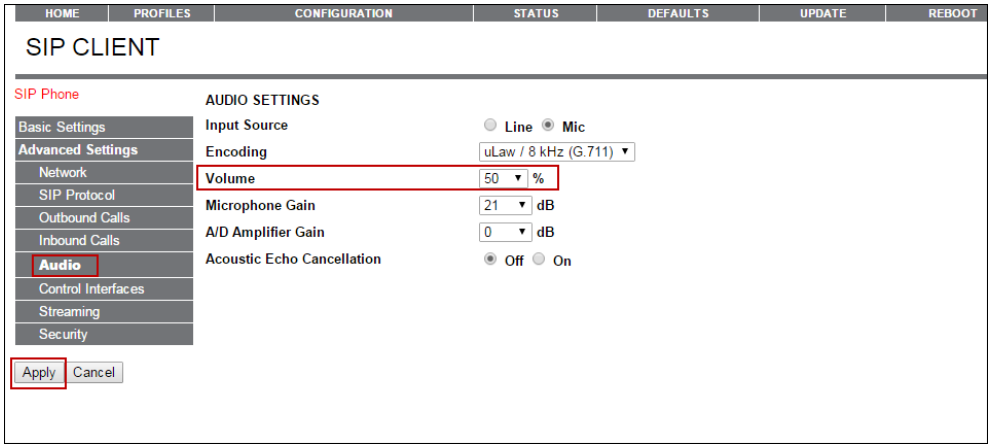
4. Select **No** for **Peer to Peer** and enter the following values for the fields given below:
   - **SIP Server (PBX)** – IP Address of the server running FreeSwitch
   - **SIP ID (username)** – The extension number for the device in the telephony server using the Telephony Configuration Tool
   - **SIP Password (secret)** – used for SIP registration assigned to the extension in the **SIP ID (username)** field



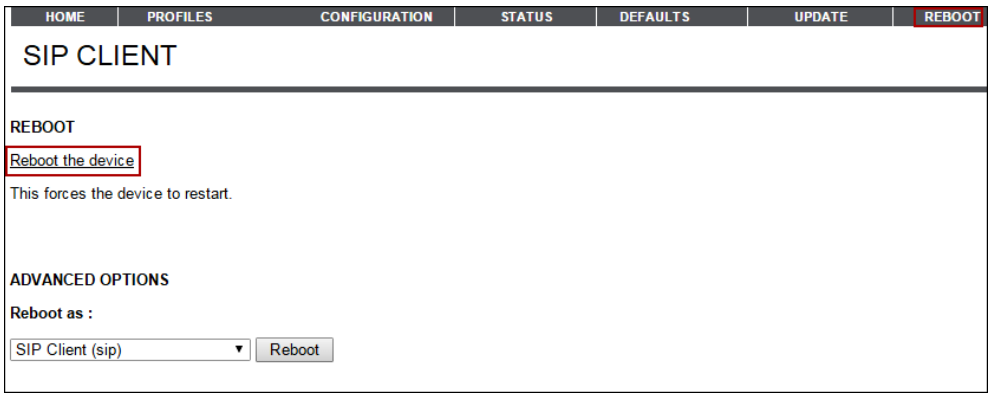
5. Leave the other fields with default and click **Apply**.
6. Select **Advanced settings** > **Inbound Calls**
7. Set the **Phone Pickup Mode** to **autoanswer**.



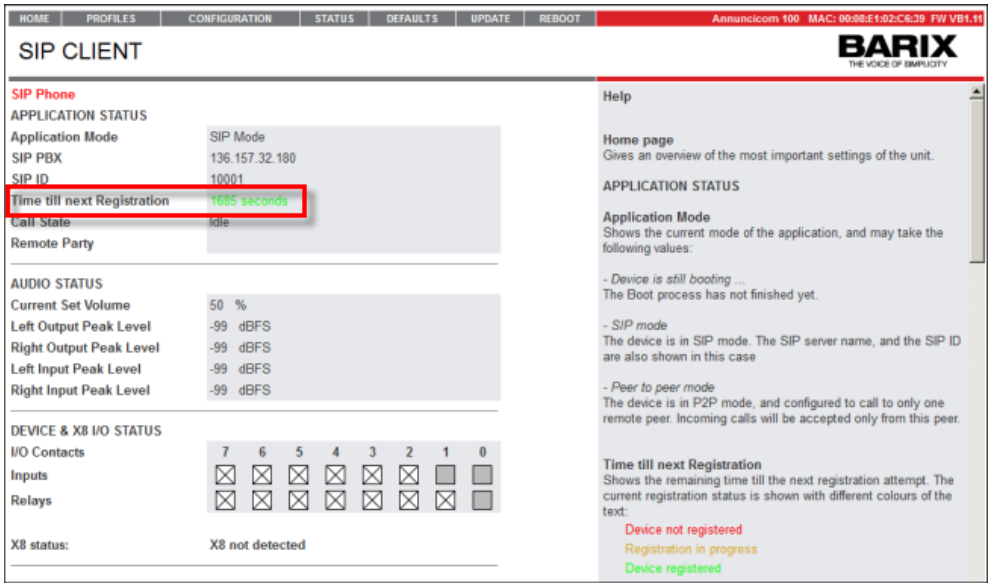
8. Select **Advanced Settings** > **Audio**.
   a. Select the appropriate volume level.
   b. Click **Apply**.



9. Select the **REBOOT tab**.
10. Click the **Reboot the device** link.



11. SIP client reboots.
12. Select the **HOME** tab.
13. Check the field **Time till next Registration**. If the time is in Green color, then the device is successfully registered with the server.
    NOTE: Click **Help** on the right hand side of the configuration window if the registration time is displayed in a different color.



NOTE:
When the network connection between a Barix Annuncicom 200 device and the server is interrupted, the device becomes disconnected from the telephony subsystem. The disconnected device periodically attempts to reconnect, and that frequency is determined by the time until the next registration configured on the device. The time until the next registration determines how quickly a Barix Annuncicom 200 device reconnects to the telephony subsystem once the network connection has been reestablished.

Device Verification

After successful installation and configuration, the device announces the IP Address while rebooting and the status LED remains green.

NOTE:
Verify that the device is registered using the Telephony Configuration utility. Refer to the *Telephony Configuration* section.

CyberData SIP Adapter

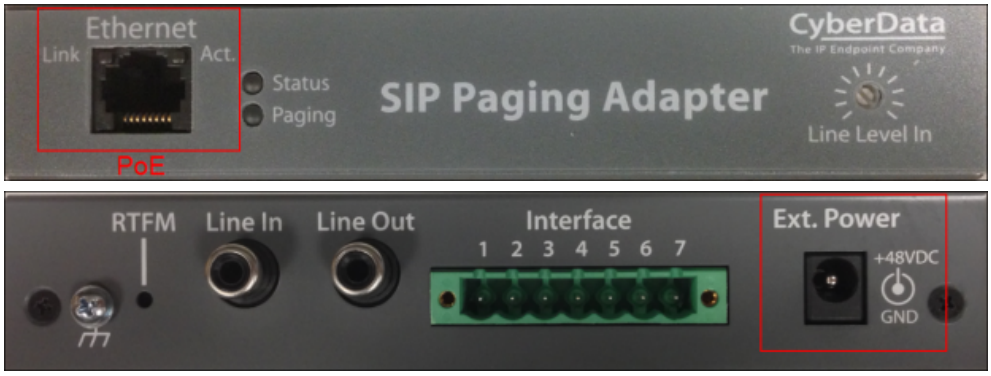
Hardware Prerequisites

Before proceeding, ensure that the following items are available:

- CyberData SIP Paging Adapter (P/N 011233)
- PoE 802.3af or 48VDC, 500mA (minimum) DC power supply
- Category 5 Ethernet cable

Power

Power to the device can either be supplied by the barrel connector or through Ethernet using a Power over Ethernet (PoE) equipped switch or power injector.



Ethernet

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

Audio Output

An audio receiver is a device that amplifies an external analog audio signal and distributes that signal to one or more speakers. Examples are an audio/video receiver, a voice-enabled fire panel system, a radio-based station, and an intercom/public announcement system.

There are two methods to supply audio from the LLA:

Method 1: Use the LINE-OUT Radio Corporation of America (RCA) socket.
NOTE 1: The tip of the RCA plug is a signal.
NOTE 2: Line Out has a 10kΩ output impedance with Voltage Peak-to-Peak (VPP) of 2V maximum.

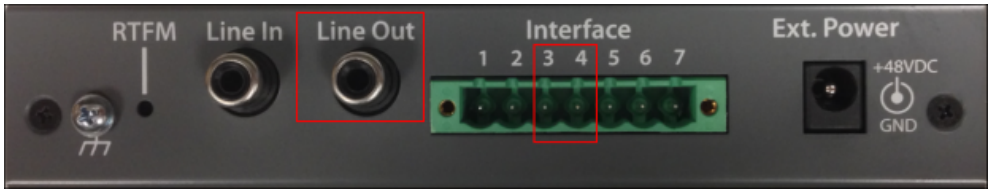
Cable requirements are as follows:

1. >= 22 awg shielded, stranded cable wire
2. < 6ft length

Method 2: Use pins 3 and 4 on the terminal block for a balanced 600Ω output with a 10V peak-to-peak.

Cable requirements are as follows:

1. >= 22 awg shielded, stranded cable wire
2. < 6ft length
3. Twisted wire pair



NOTE:
Refer to the image in Device Overview section for an illustration regarding how the various components are connected.

Hardware Verification

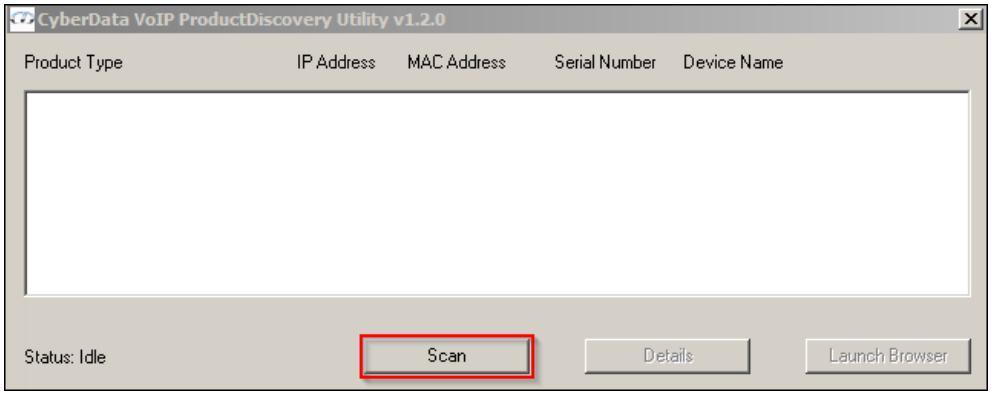
After completing the mechanical and electrical installations, verify that the status LED is a solid green color. If not, perform the steps outlined in the following sections:

IP Address Assignment

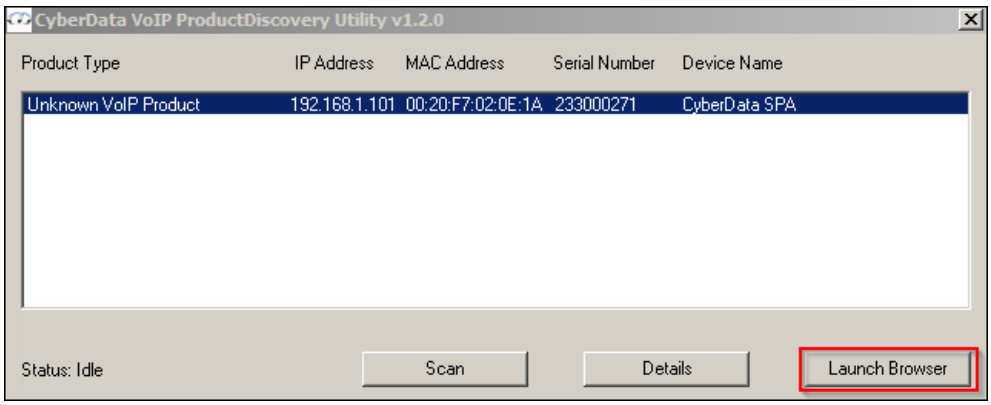
The CyberData SIP Adapter device can be configured either for DHCP or static IP.

To determine the IP address or change the IP address of the device, do the following:

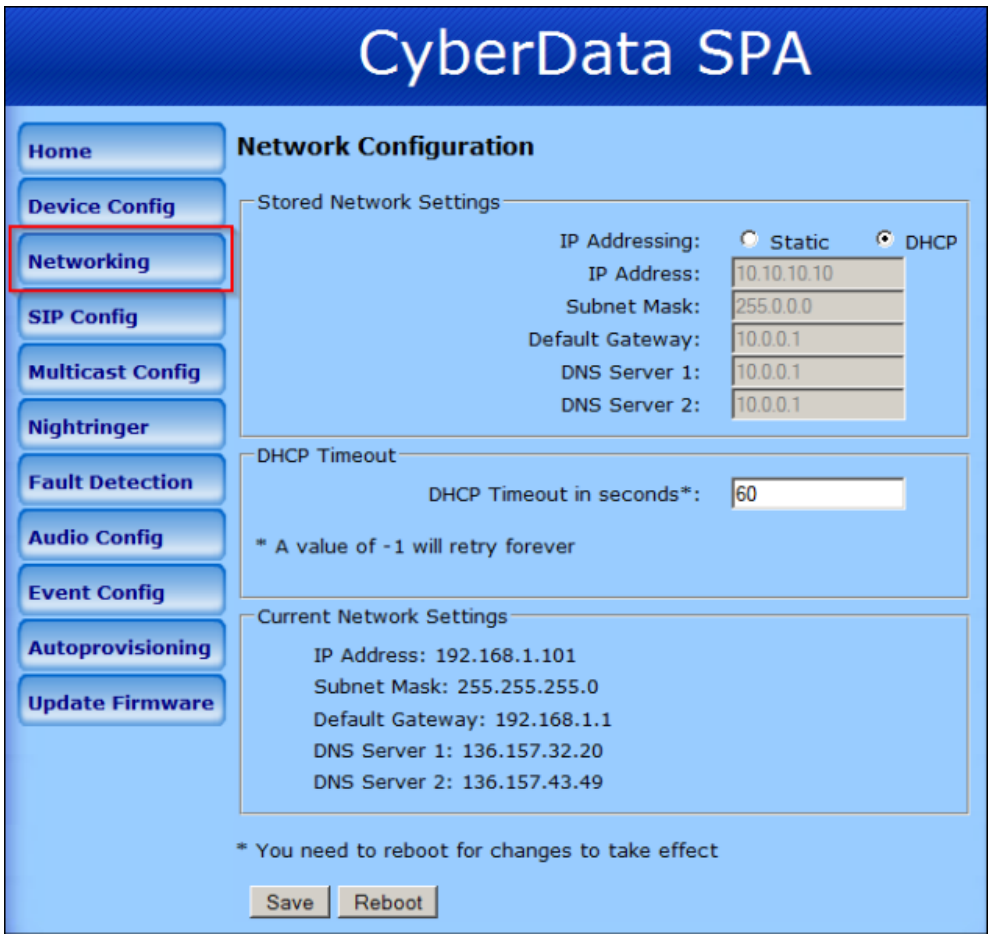
1. Connect a computer to the same switch as the CyberData SIP Adapter device.
2. Use the CyberData Discovery Utility program to locate the device on the network.
   NOTE: The Discovery Utility program can be downloaded from the following website:
   http://www.cyberdata.net/support/voip/discovery_utility.html
3. Run the utility and **Scan** for devices.
   NOTE: Ensure that the computer is on the same subnet as the device to be configured.



4. Select the device from the utility and click **Launch Browser**.
   NOTE 1: Alternatively, manually enter the IP address into a browser's URL.
   NOTE 2: The IP address of the CyberData device can also be derived by connecting an 8Ω speaker directly to pins 3 and 4 on the terminal block and pressing the Reset Test Function Management (RTFM) button on the device. The device will announce the IP address.



5. When prompted, enter **admin** for both Username and Password.
6. In **CyberData SPA** window, click **Networking**.



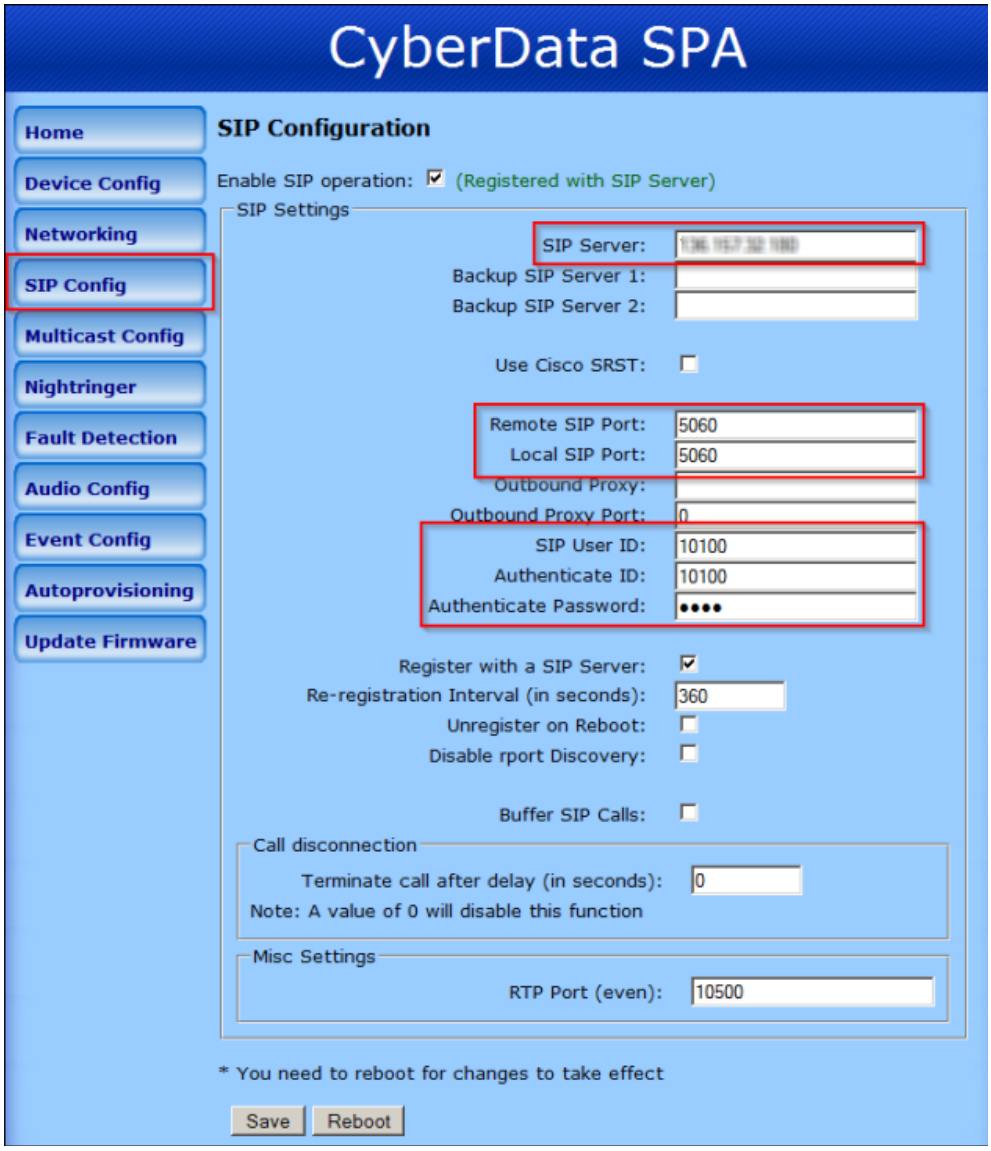
7. In the **IP Addressing** section, select either **Static** or **DHCP** based on the device usage.
   NOTE 1: For a Static IP, enter the appropriate values for **IP Address** and **Subnet Mask**. Configure **Default Gateway** and **DNS Servers** as per the IT infrastructure procedures. It is strongly recommended to specify a **Default Gateway** to ensure proper routing of the SIP call.
   NOTE 2: For DHCP, the required settings will automatically be populated by the DHCP server.
8. Click **Save**.
9. Click **Reboot**.

Configuring the SIP End Point

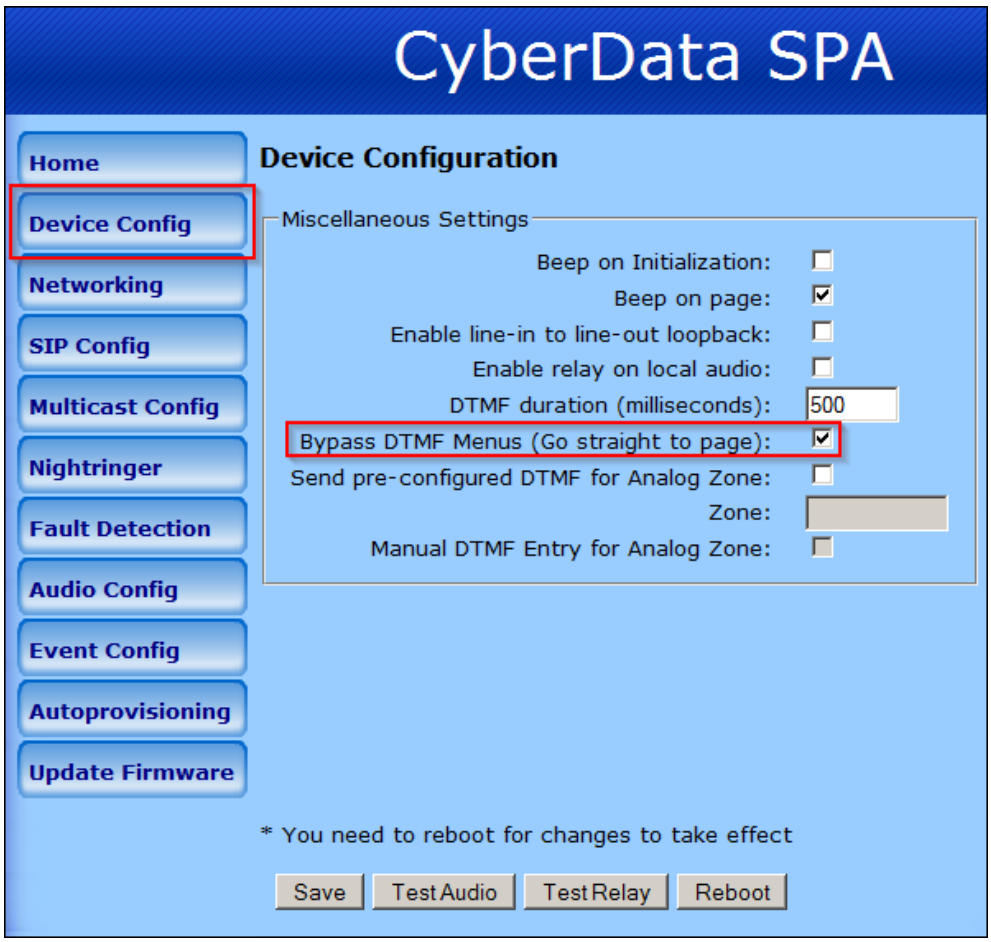
This document has been tested with firmware version 7.0.0. If an earlier version is present, perform the steps mentioned in the *Upgrading LLA Firmware* section before configuring the device for SIP.

1. In a web browser, enter the IP Address of the CyberData SIP Adapter device in the address bar.
2. Click **SIP Config**.
3. Enter the following values for the fields given below:
   - **SIP Server** – IP Address of the server running the telephony server.
   - **Remote SIP Port** - Enter 5060.
   - **Local SIP Port** - Enter 5060.
   - **SIP User ID** - Extension number for the device in the telephony server using the Telephony Configuration Tool.
   - **Authenticate ID** - Extension number for the device in the telephony server using the Telephony Configuration Tool.
     Authenticate Password - The password used for the SIP registration

assigned to the extension above.
NOTE: For more information on the Telephony Configuration Tool, refer to the *Telephony Configuration* section.



4. Leave the other fields with default and click **Save**.
   NOTE: When the network connection between a CyberData SIP Adapter and the server is interrupted, the device becomes disconnected from the telephony subsystem. The disconnected device periodically attempts to reconnect, and that frequency is determined by the re-registration interval configured on the device. The re-registration interval determines how quickly a CyberData SIP Adapter device reconnects to the telephony subsystem once the network connection has been re-established.
5. Click **Device Config**.
6. Enable the **Bypass DTMF Menus (Go straight to page)**.



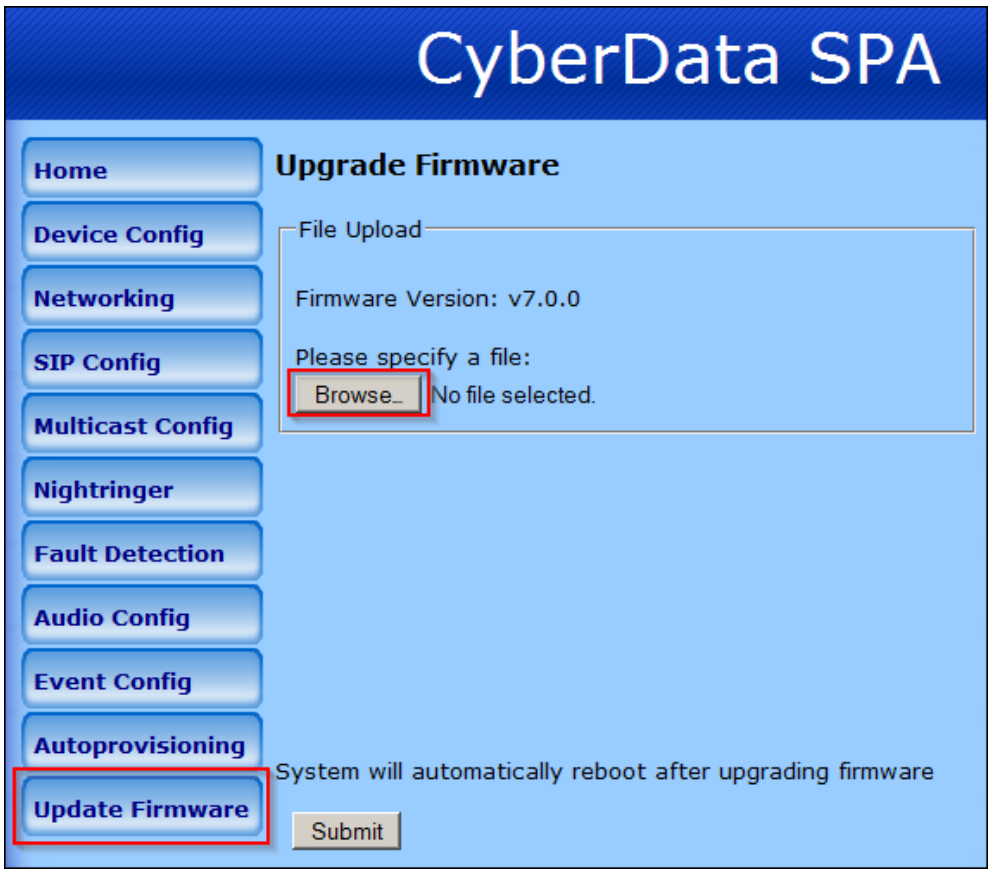
7. Click **Save**.
8. Click **Reboot**.

Upgrading LLA Firmware

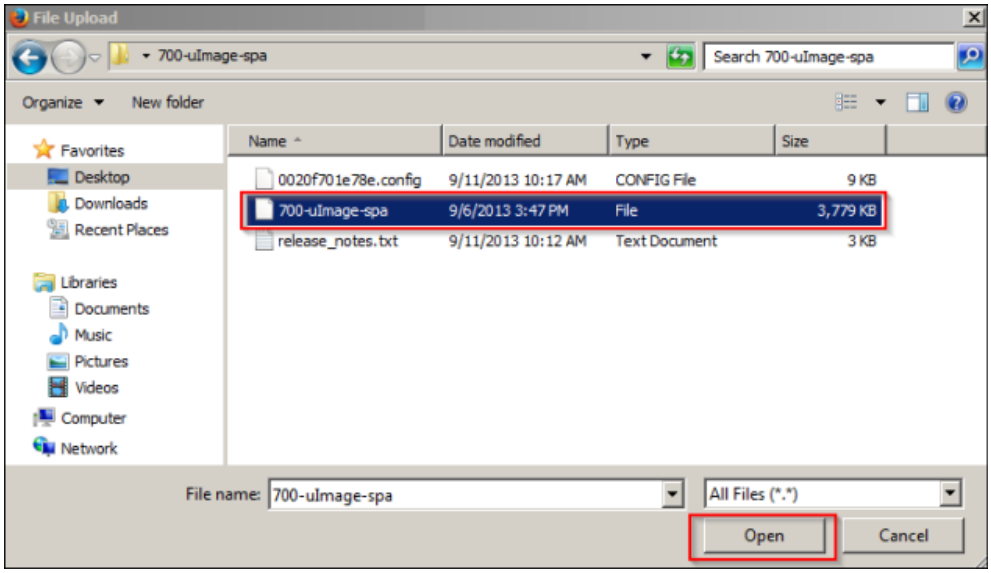
The latest firmware can be obtained from the CyberData website.

Disclaimer:
Prior to the commissioning of a 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.

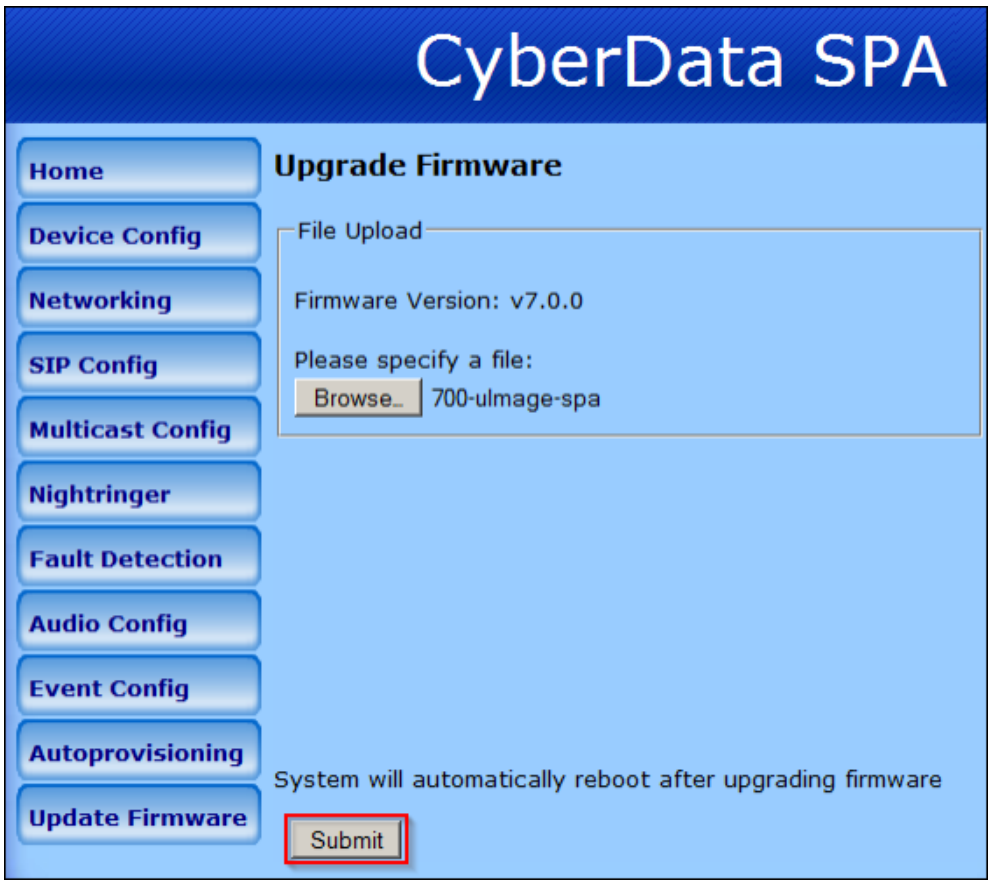
1. In a web browser, enter the IP Address of the CyberData SIP Adapter device in the address bar.
2. Click **Update Firmware**.
3. Click **Browse**.



4. Select the folder containing the firmware upgrade file.
5. Select the firmware upgrade file and click **Open**.



6. Click **Submit** to confirm the upgrade.
   NOTE: The device may take up to two minutes to upgrade.



Device Verification

After successful installation and configuration, the status LED turns blue.

NOTE:
Verify that the device is registered using the Telephony Configuration utility. Refer to the *Telephony Configuration* section.

Perle TD2R2 Device

The following subsections describe the steps necessary to wire, mount, and configure the Perle TD2R2, the Ethernet I/O Relay device. There are two areas of configuration. The first is to configure the TD2R2 device to allow remote access to the relays. The second area of configuration is the TruePort driver which the server uses to communicate with the TD2R2 device.

Configuring the TD2R2 requires Perle's DeviceManager software. Install DeviceManager on a computer that is connected to the same subnet network as the Perle device being configured.

Prerequisites

Before proceeding, ensure that the following items are available:

- Perle IOLAN SDS1 TD2R2
- 9-30VDC (400mA minimum) power supply, if not included with device
- Category 5 Ethernet cable
- Computer or server to communicate with the device
- Device Installation CD or a computer with network access
- Hookup wire – when using the I/O and relay pins
  NOTE 1:
  The driver (TruePort) that is used to communicate with the device must be installed on the same server/machine that runs the application.
  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 DHCP.
NOTE 3:
To configure the device, a computer located in the same network is required.

Mounting

The Perle TD2R2 has two brackets on the side of the mounting holes. The installer should fasten the device to a flat surface by placing screws through mounting holes.

Power

▷ For the Perle TD2R2, use a power adaptor capable of 9-30VDC output and 400mA.

1. 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** LED should be a solid green color.
NOTE:
Connecting the power supply to the device with incorrect polarity can permanently damage the device and pose a fire risk.

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 the network jack.

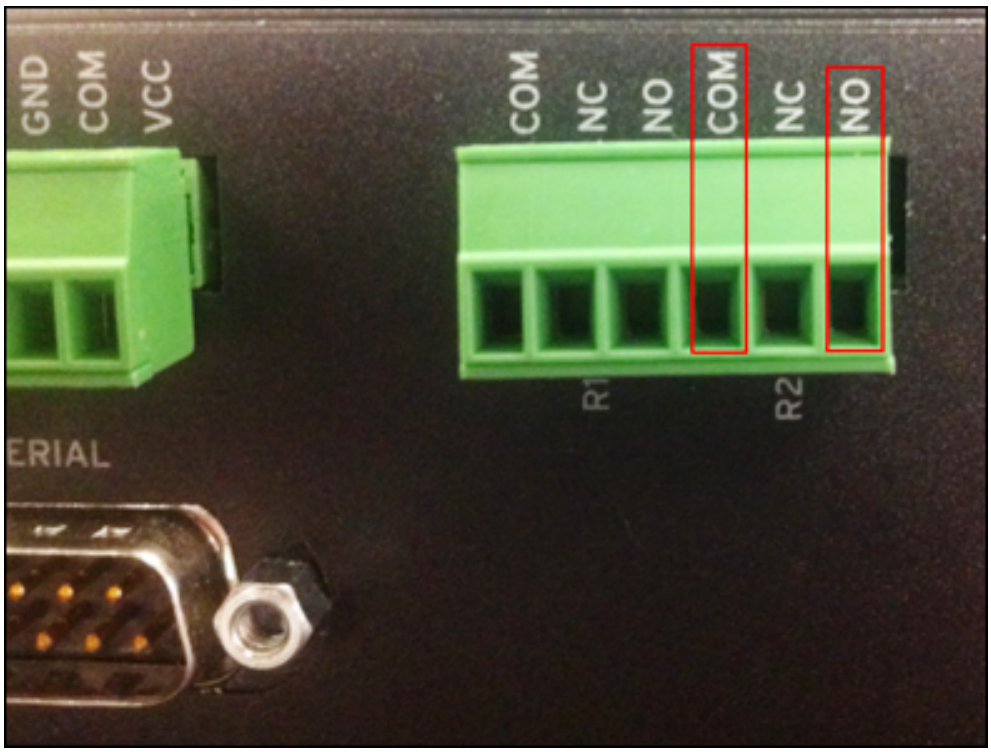
⇨ After a few seconds, the **Link/10/100** should be a solid amber or green color.

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.

Relay Output

The relay outputs are generally used to switch higher power speaker arrays or zone selection circuits on fire panels. In addition, relay outputs differ from digital outputs in that electrical isolation between the two devices are provided.

Generally, these external circuits require a closed dry contact for activation. The Perle TD2R2 includes two relays each with separate COM terminals. When hooking the device relays to external circuits, use the COM and NO (normally open) terminals. This will provide a closed switch activation to any external circuit.



CyberData IP Speaker

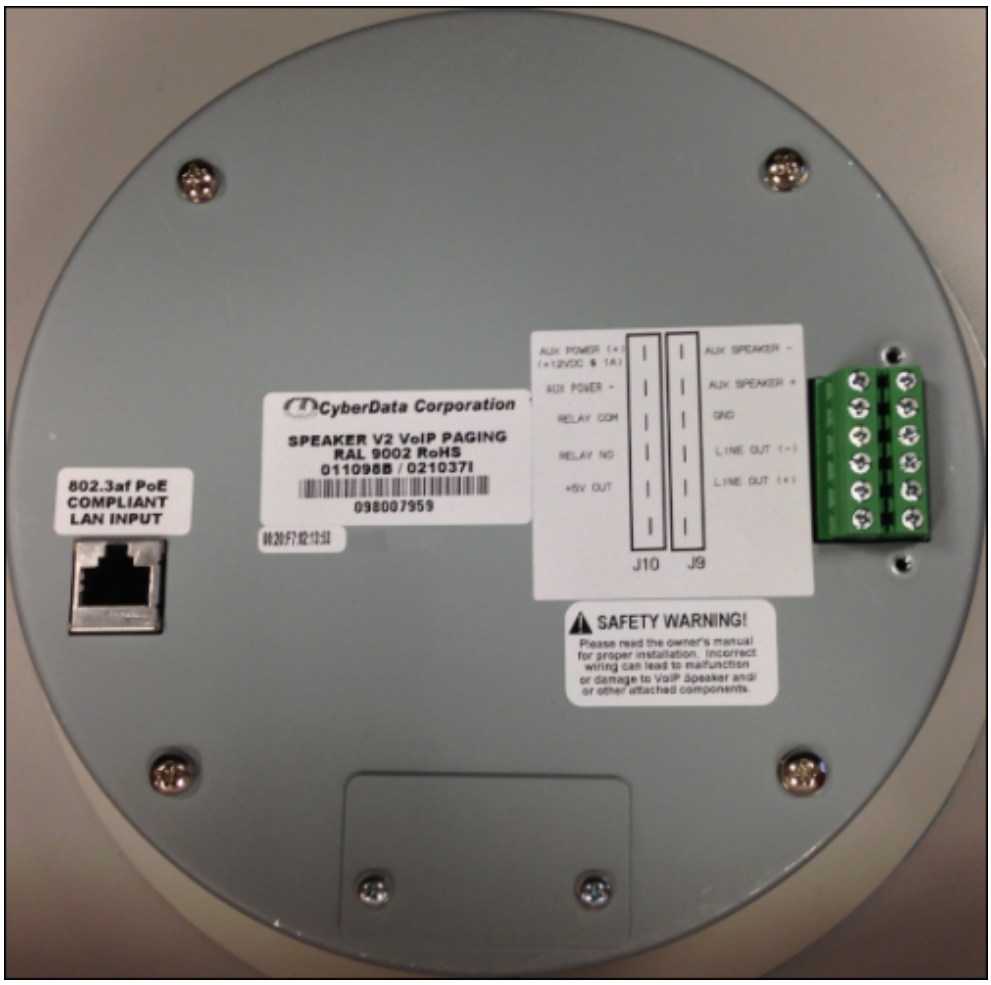
Hardware Prerequisites

Before proceeding, ensure that following items are available:

- CyberData IP Speaker
- PoE 802.3af or 48VDC, 500mA (minimum) DC power supply
- Category 5 Ethernet cable

Power

Power to the device is supplied by the RJ45 connector.



Ethernet

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

Hardware Verification

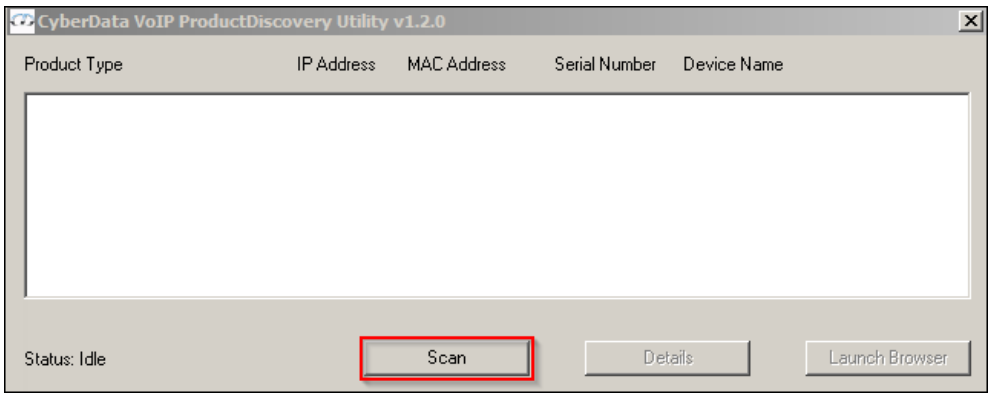
After completing the mechanical and electrical installations, verify the status LED is a solid green color. If not, perform the steps outlined in the following sections:

- IP Address Assignment
- Configuring a SIP End Point
- Upgrading the IP Speaker Firmware

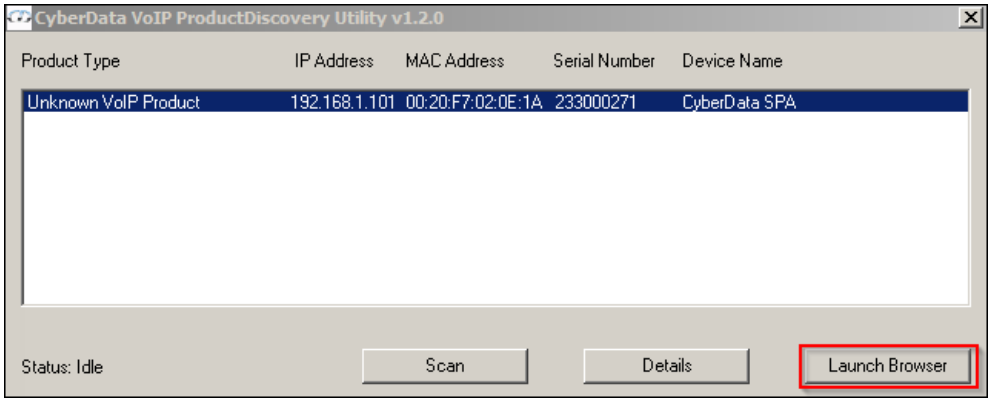
IP Address Assignment

The CyberData IP Speaker device is configured for Dynamic Host Configuration Protocol (DHCP). To determine the IP address or change the IP address of the device, do the following:

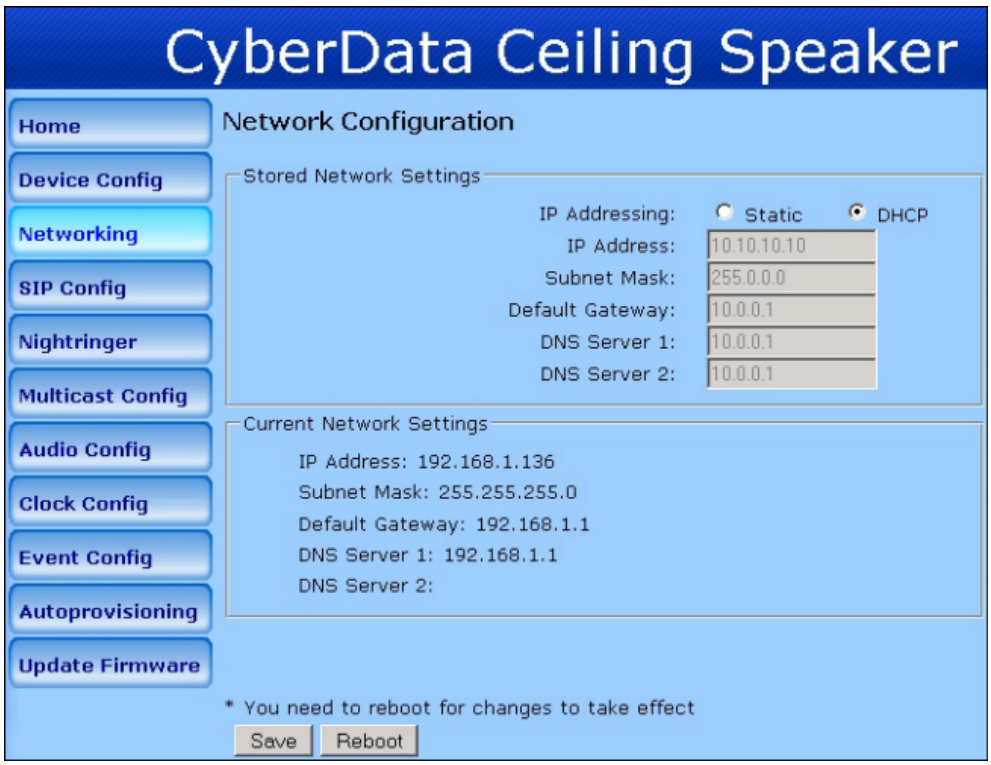
1. Connect a computer to the same switch as the CyberData IP Speaker device.
2. Use the CyberData Discovery Utility program to locate the device on the network.
   NOTE: The Discovery Utility program can be downloaded from the following website:
   http://www.cyberdata.net/support/voip/discovery_utility.html
3. Run the utility and **Scan** for devices.
   NOTE: Ensure that the computer is on the same subnet as the device that needs to be configured.



4. Select the device from the utility and click **Launch Browser**.
   NOTE 1: Alternatively, manually enter the IP address into a browser's URL.
   NOTE 2: The IP address of the CyberData IP Speaker device can be derived alternatively by pressing the **RTFM** button on the device. The device will announce the IP address.



5. Enter **admin** for both Username and Password when prompted.
6. Click **Networking**.

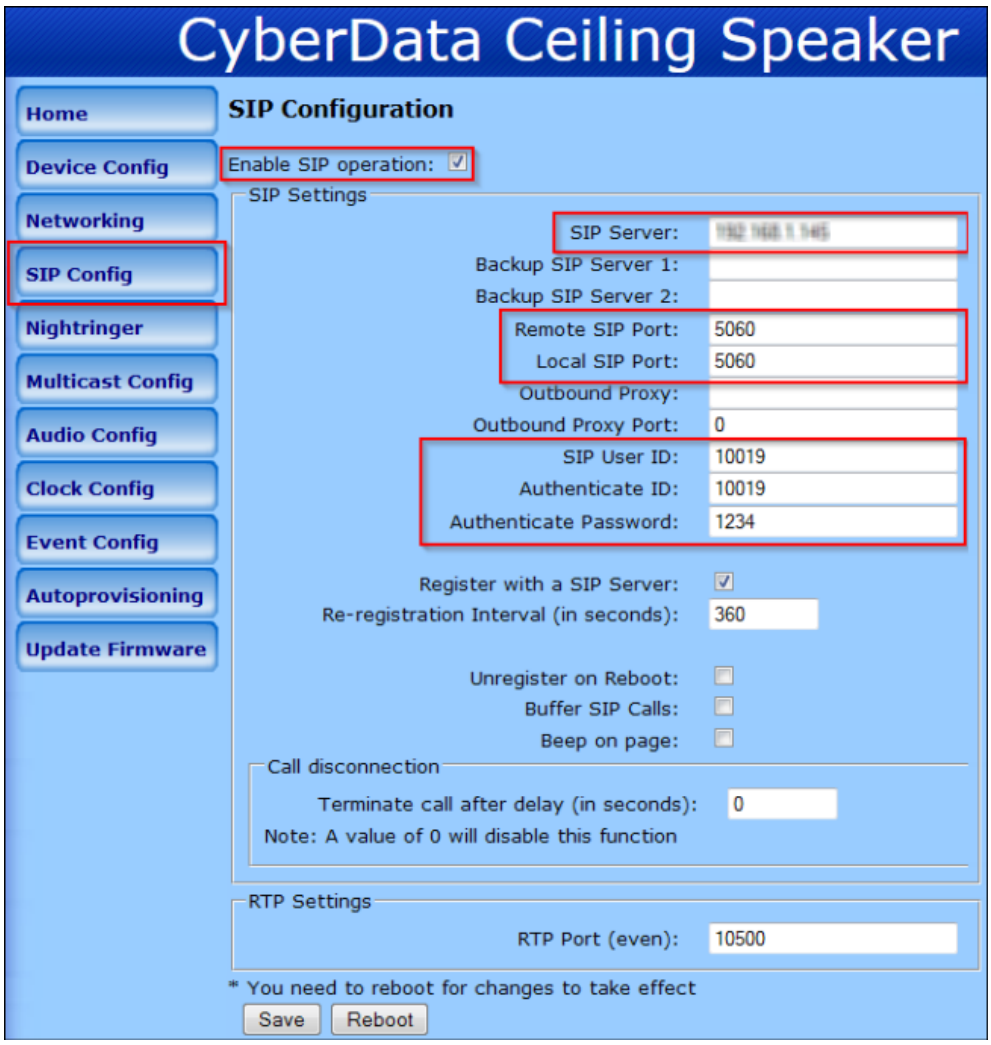


7. In the **IP Addressing** section, select either **Static** or **DHCP** based on the device usage.
   NOTE 1: For Static IP, enter appropriate values for **IP Address** and **Subnet Mask**. Fill **Default Gateway** and **DNS Servers** as per your IT infrastructure. It is strongly recommended to specify a **Default Gateway** to ensure proper routing of the SIP call.
   NOTE 2: For DHCP, the required settings will automatically be populated by the DHCP server.
8. Click **Save**.
9. Click **Reboot**.

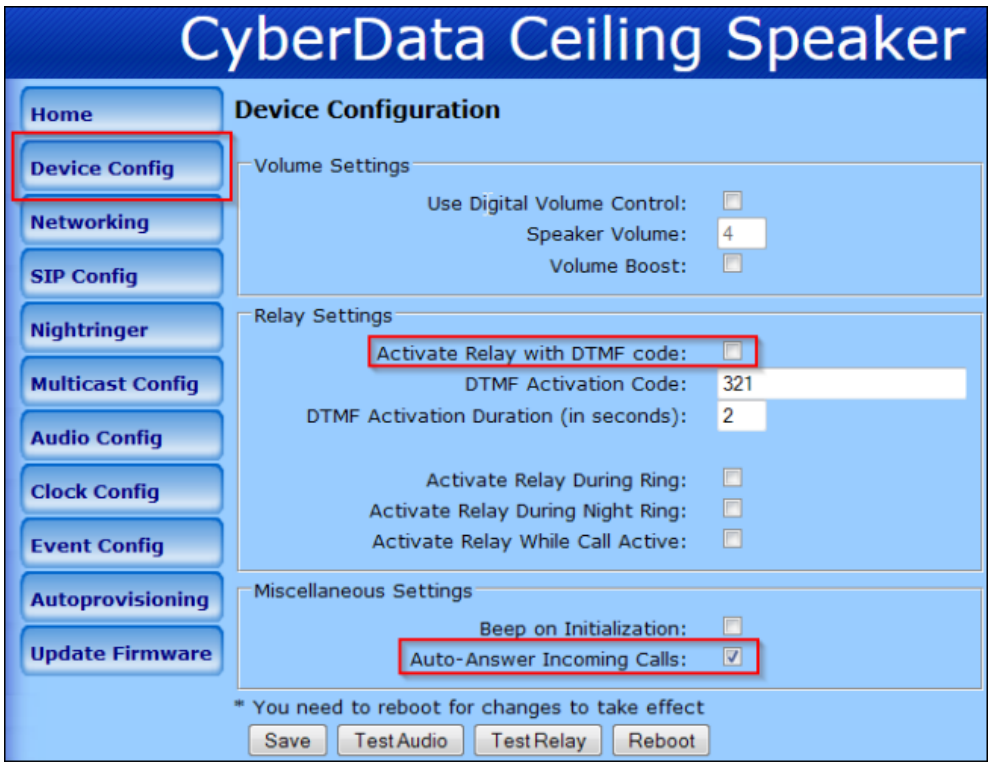
Configuring the SIP Endpoint

This document has been tested with SIP firmware version 6.3.0. If this is an earlier version, perform the steps mentioned in the Upgrading LLA Firmware section before configuring the device for SIP.

1. In a web browser, enter the IP Address of the CyberData IP Speaker device in the address bar.
2. Click **SIP Config**.
3. Confirm that **Enable SIP Operation** is enabled.
4. Enter the following values for the fields given below:
   - **SIP Server** – IP Address of the server running on the telephony server
   - **Remote SIP Port** - Enter **5060**.
   - **Local SIP Port** - Enter **5060**.
   - **SIP User ID** - Extension number for the device on the telephony server using the Telephony Configuration Tool.
   - **Authenticate ID** - Extension number for the device on the telephony server using the Telephony Configuration Tool.
   - **Authenticate Password** - Password used for SIP registration assigned to the extension above.



5. Leave the other fields with the default values and click **Save**.
   NOTE: When the network connection between a CyberData IP Speaker and the server is interrupted, the device becomes disconnected from the telephony subsystem. The disconnected device periodically attempts to reconnect, and that frequency is determined by the re-registration interval configured on the device. The re-registration interval determines how quickly a CyberData IP Speaker device reconnects to the telephony subsystem once the network connection has been reestablished.
6. Click **Device Config**.
7. Disable **Active Relay with DTMF code**.
8. Enable **Auto-Answer Incoming Calls**.



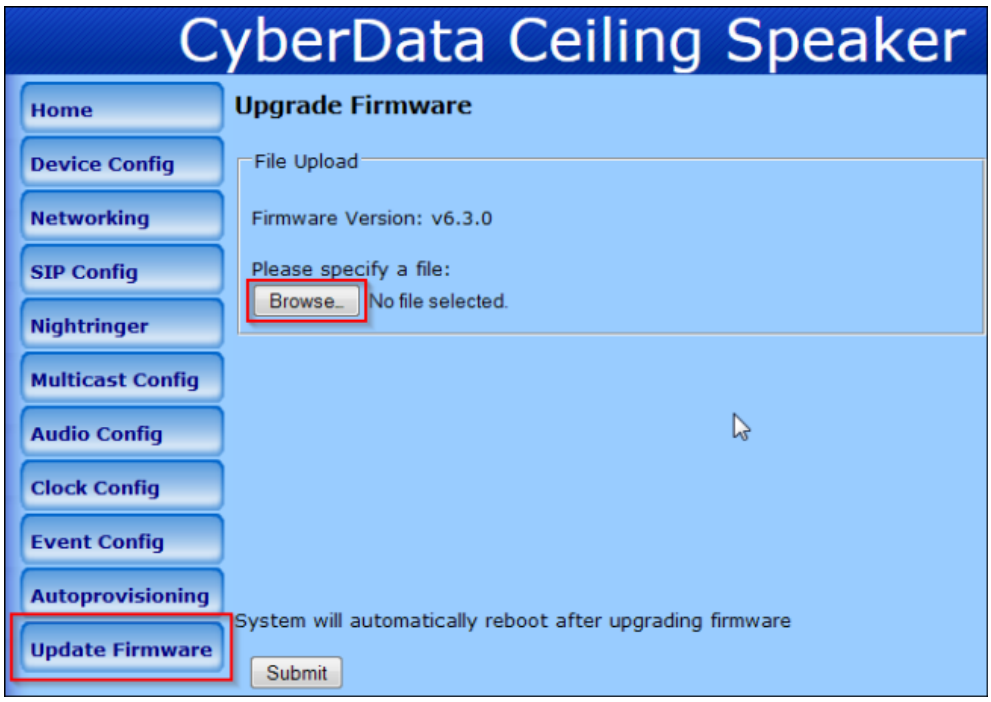
9. Click **Save**.
10. Click **Reboot**.

Upgrading the IP Speaker Firmware

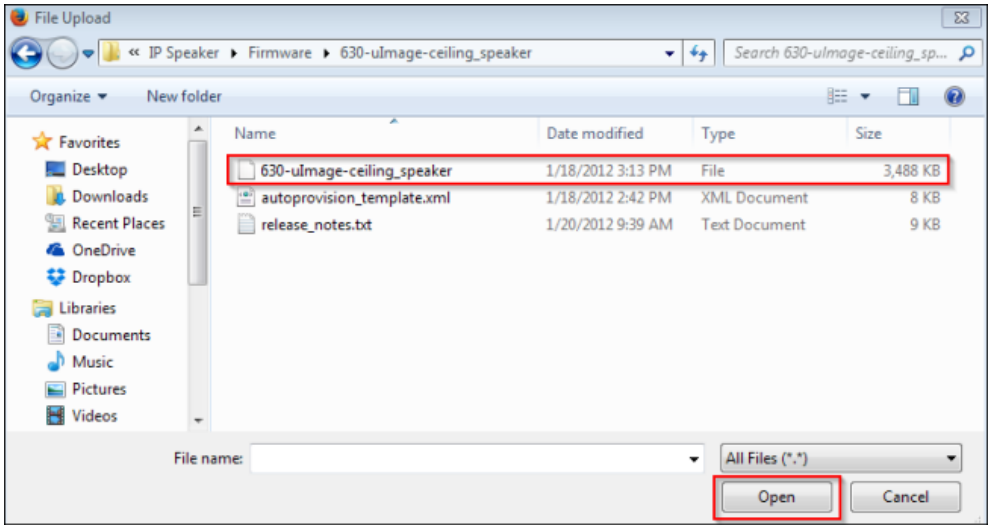
The latest firmware can be obtained from the CyberData website.

Disclaimer:
Prior to the commissioning of 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.

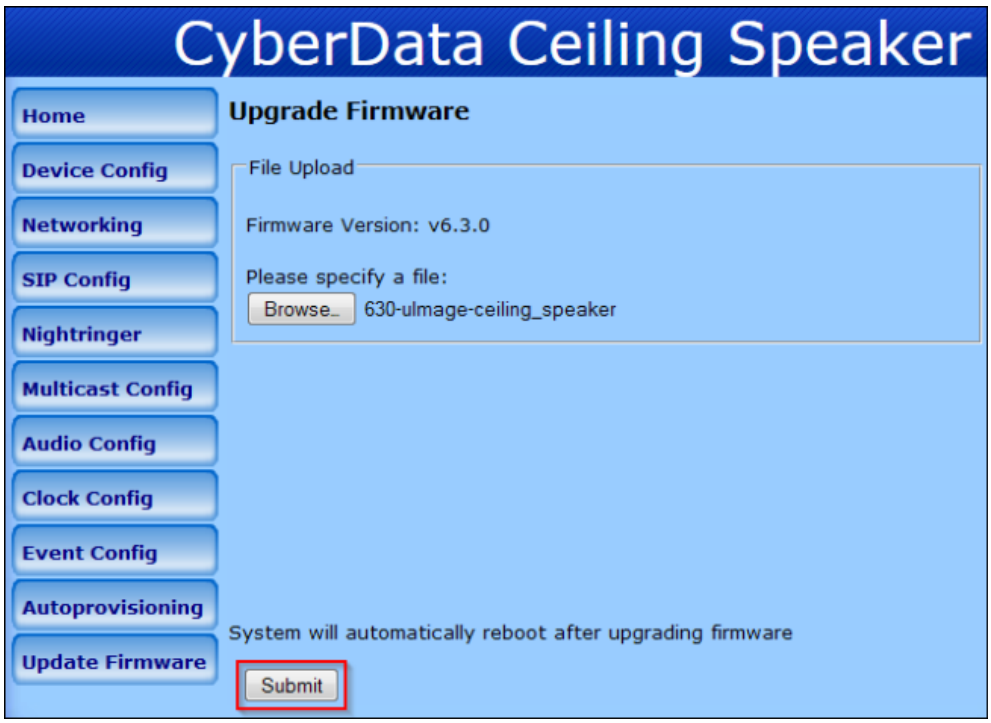
1. In a web browser, enter the IP Address of the CyberData IP Speaker device in the address bar.
2. Click **Update Firmware**.
3. Click **Browse**.



4. Select the folder containing the firmware upgrade file.
5. Select the firmware upgrade file and click **Open**.



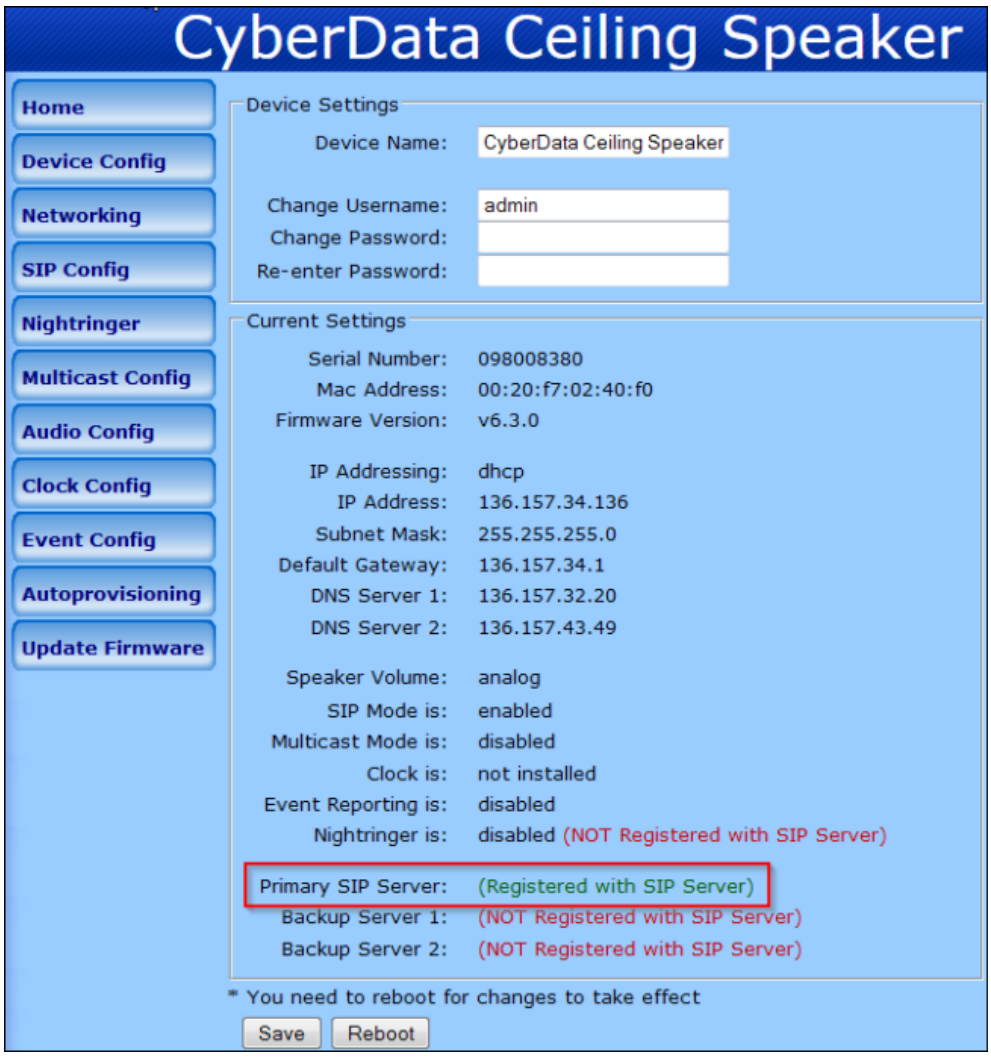
6. Click **Submit** to confirm the upgrade.
   NOTE: The device may take up to two minutes to upgrade.



Device Verification

After successful installation and configuration, the device announces the IP Address while rebooting and the status LED remains green.

To verify successful SIP configuration, log into the device. In the **Home** window, **Registered with SIP Server** message displays.



NOTE:
Verify that the device is registered using the Telephony Configuration utility. Refer to the Configuring Telephony Device for details.

Configuring Single Zone Audio 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).

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.

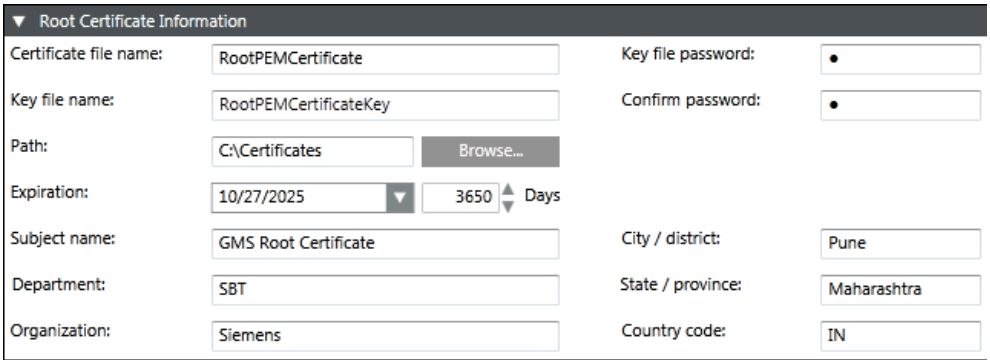


Fig. 46:

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.

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 are 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

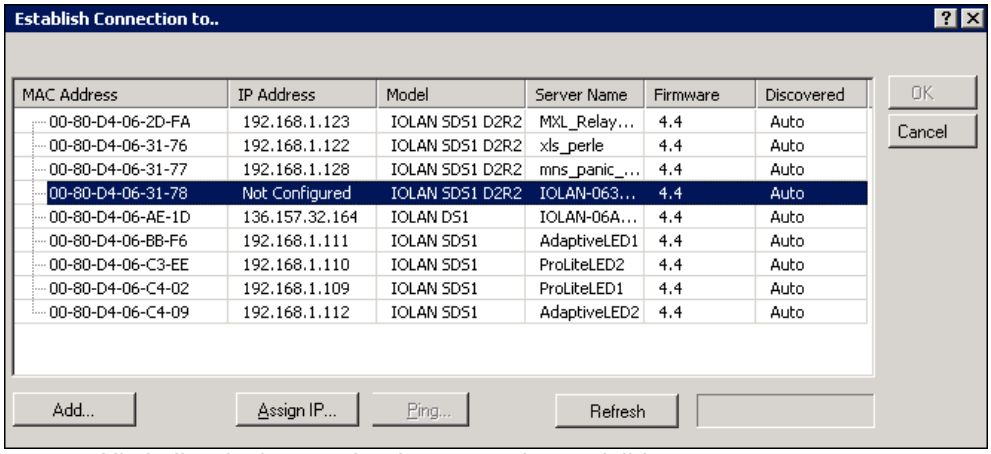
▷ The **DeviceManager** is installed on a computer located in the same network as the device to configure.

▷ 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 Import DME File section.

1. Start **DeviceManager**.



⇨ All similar devices under that network are visible.

2. Select the device to configure and click **Assign IP**.

   NOTE 1: If unable to see the device in the window, verify that the device has power and is connected to the network. Check the LEDs on the device; the power LED should be a solid green color and the link LED should be a solid amber / green color.

   NOTE 2: If issues persist, unplug the Ethernet cable and power. Wait for five 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 a solid amber color and then release. Wait for 90 seconds for device to reboot and initialize. If resetting 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**.

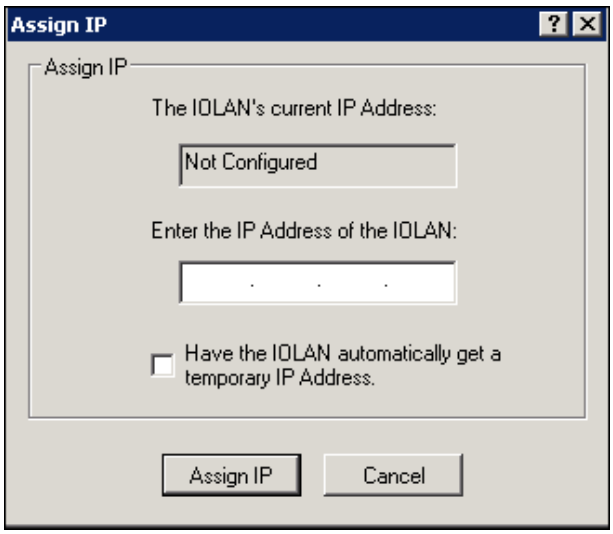


Fig. 47:

⇨ The **Establish Connection to** window displays an IP address.

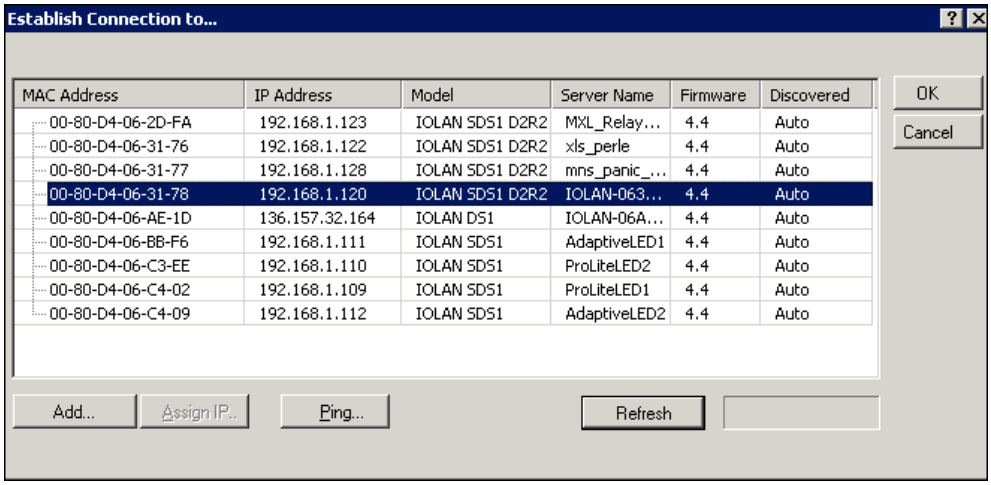
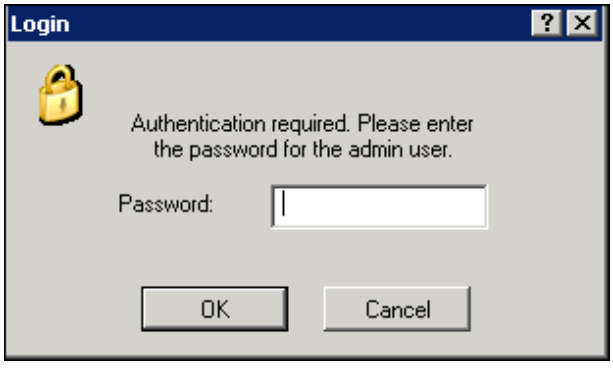


Fig. 48:

4. Select the device again, and click **OK** to log into the device for configuring.
5. In the **Login** window, enter the device password. The factory default password is: **superuser**.



Network Set Up

▷ Log in to the device using the DeviceManager.

1. In the **DeviceManager** window, click on the **Network** folder and then on **IP Settings**.
   NOTE: In this area, it is possible to configure additional parameters for the network settings, such as configuring a **static IP address** or a **DHCP**.

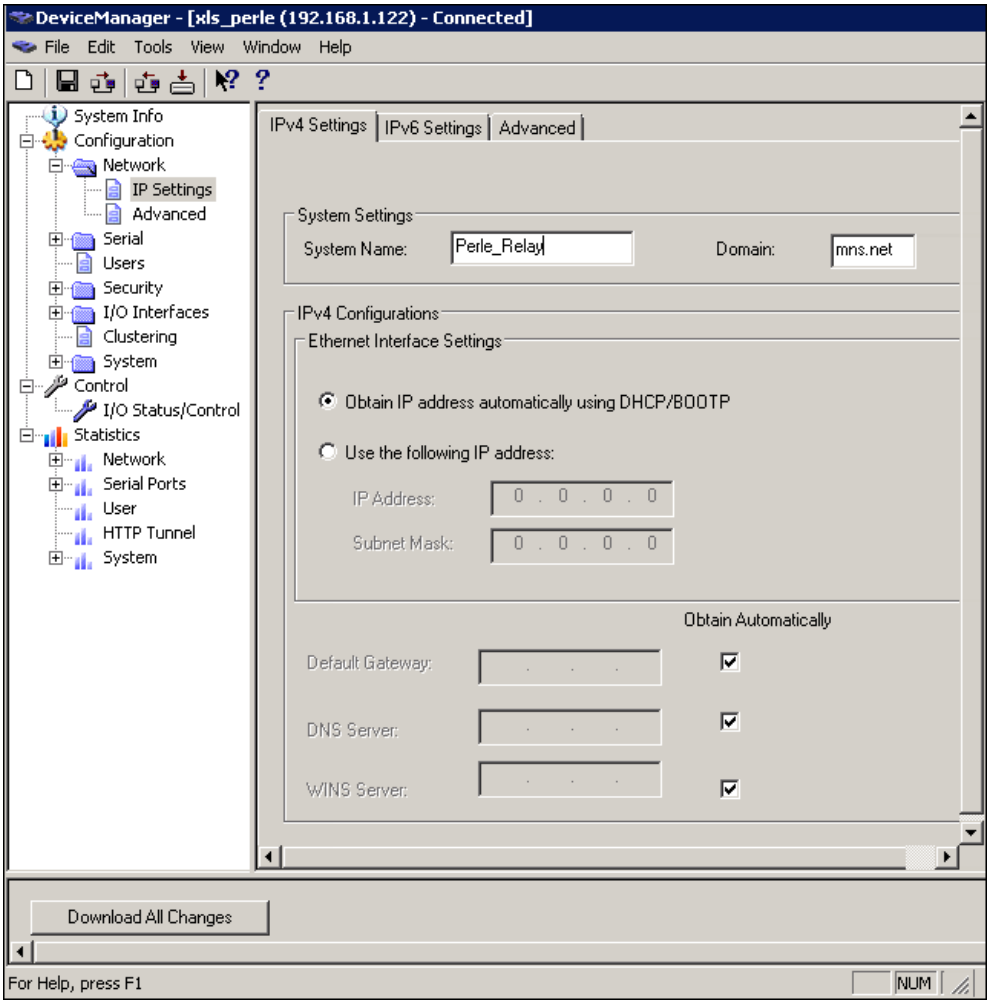


Fig. 49: IPv4 Settings Tab

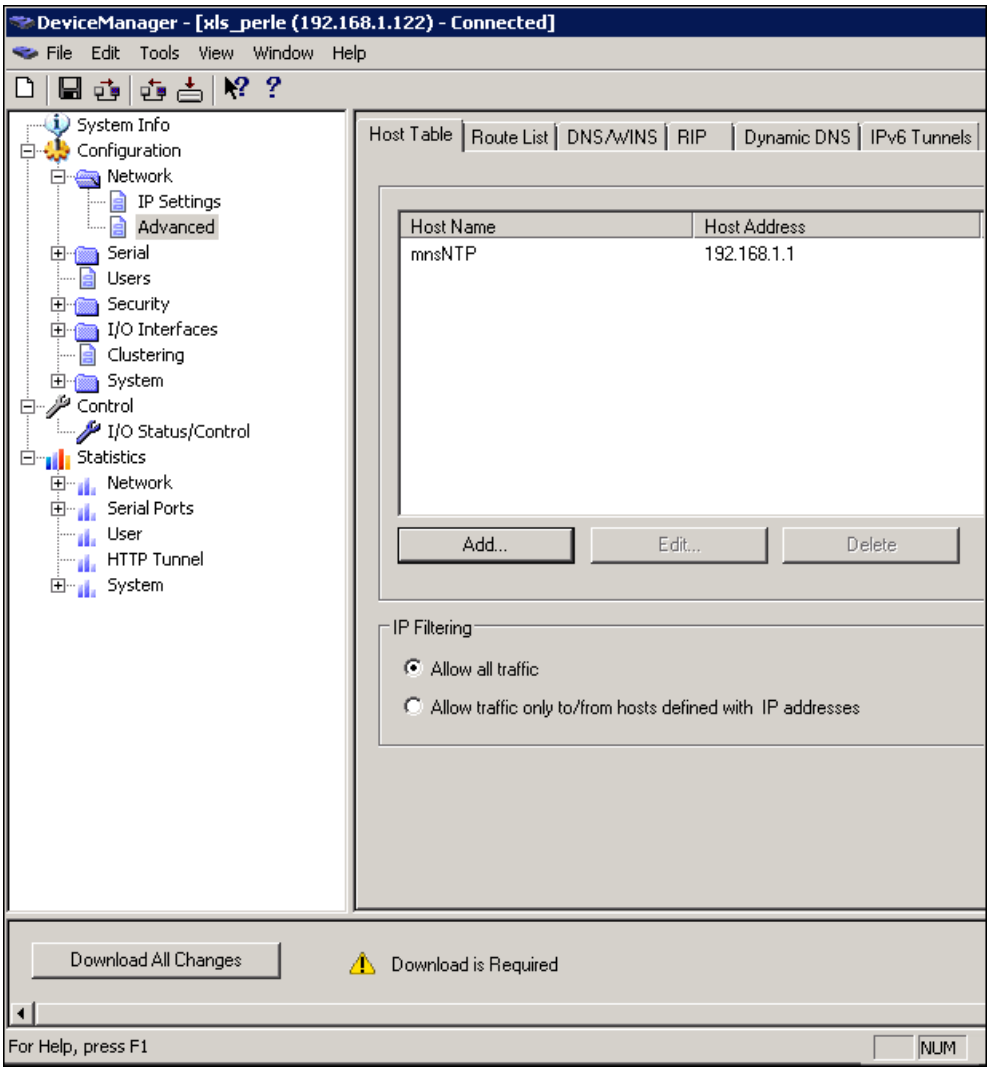
2. In the **System Name** field, provide a name that helps distinguish the device from other similar devices.

   NOTE 1: The System Name is 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.
4. Enter the domain name used on 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.
5. Select the **Network>IP Settings**.
6. Select the **Advanced** tab.
7. Select the **Register Address in DNS** check box.

8. Select **Advanced** from the left-hand side menu.
9. Select the **Host Table** tab.
10. Click **Add**.

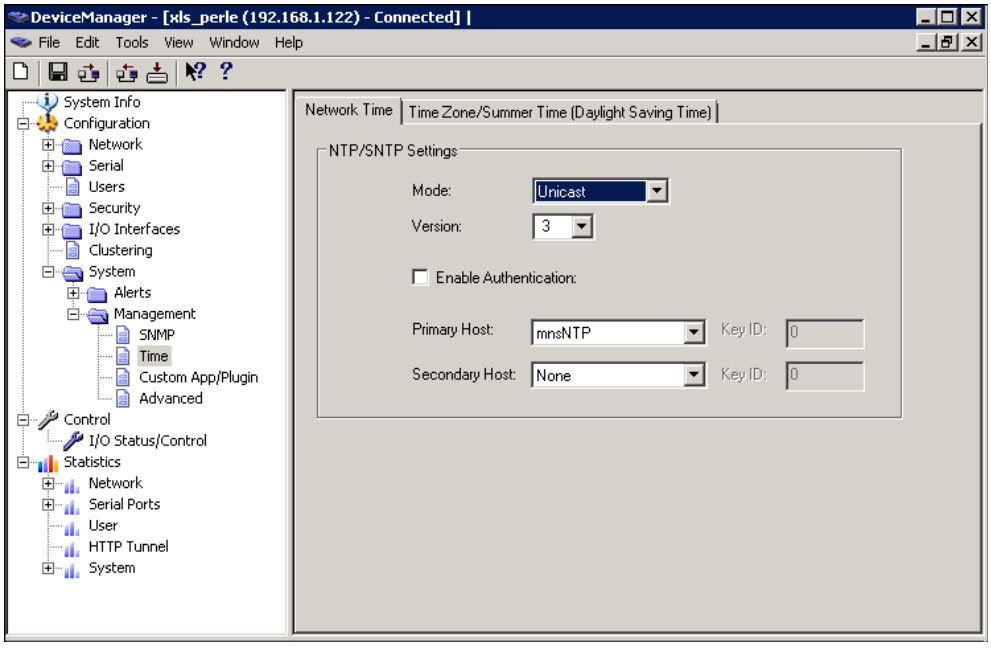


11. Enter a descriptive name for the NTP server, for example, **mnsNTP**.
12. Enter the IP address or the fully qualified domain name of an available NTP server.
    NOTE: An available NTP server is required to enable SSL on the device.
13. Click **OK**.

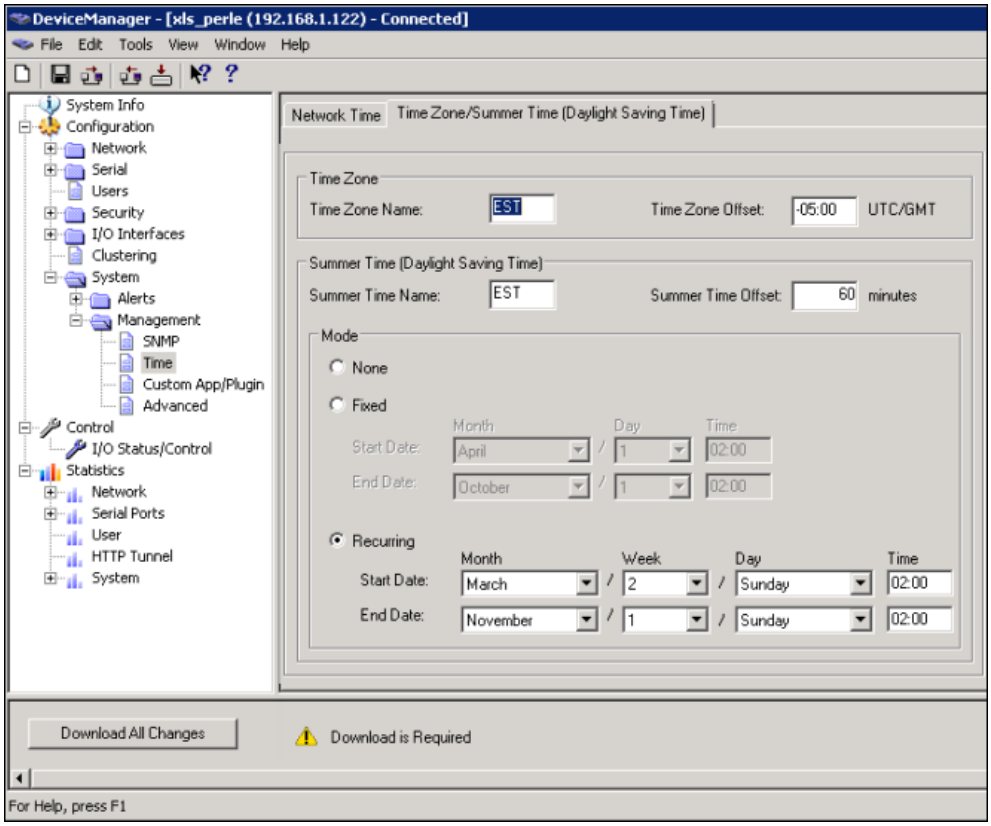
Time and Security Settings

1. Select **Configuration > System > Management > Time**.
2. Select the **Network Time** tab.
3. Set the following parameters:
   - **Mode**: Unicast.
   - **Version**: 3.
   - Leave the **Enable Authentication** check box unselected.
   - **Primary Host**: Select the NTP server name created earlier.
   - **Secondary Host**: Select an alternative NTP server name, otherwise set the name as the primary host.
     NOTE: Network time works best when the version matches that of the NTP

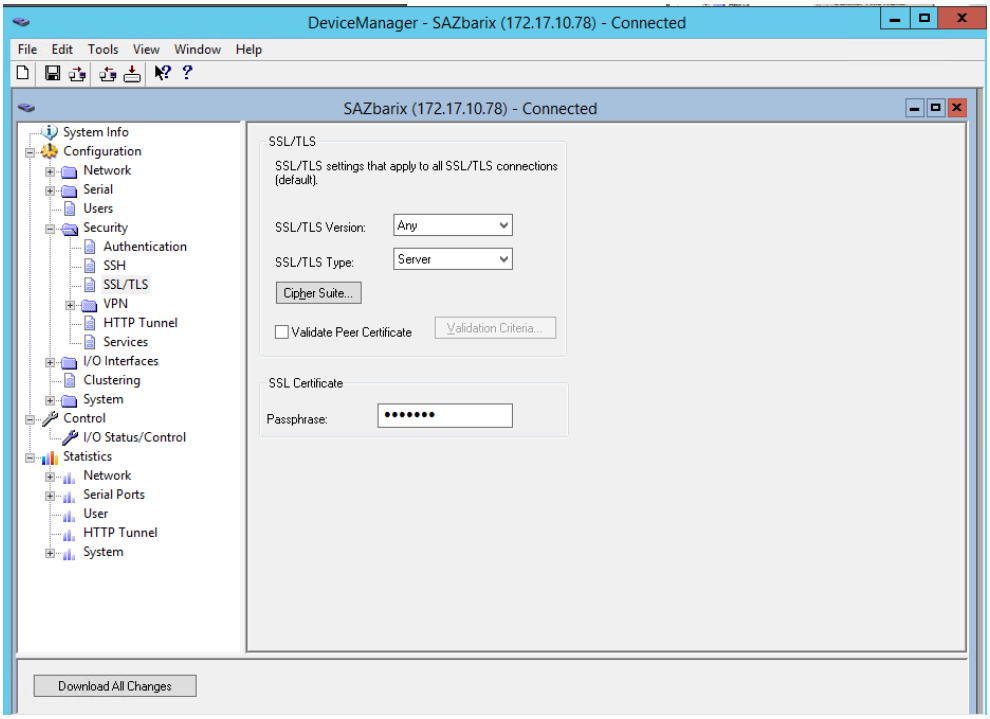
server. Windows time servers generally default to Version 2. External NTP servers generally work with Version 3. Verify with the client's network administrator if there are any questions.



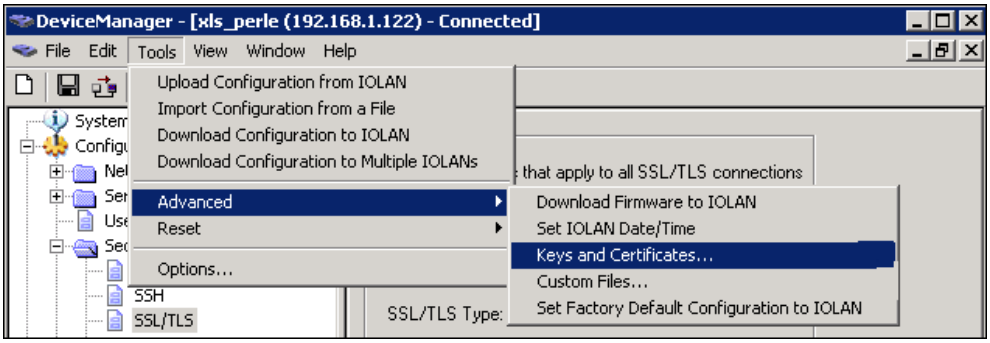
4. Select the **Time Zone/Summer Time (Daylight Saving Time)** tab.
5. Configure the parameters as per the details mentioned in Time Zone/Summer Time (Daylight Saving Time) Parameters.



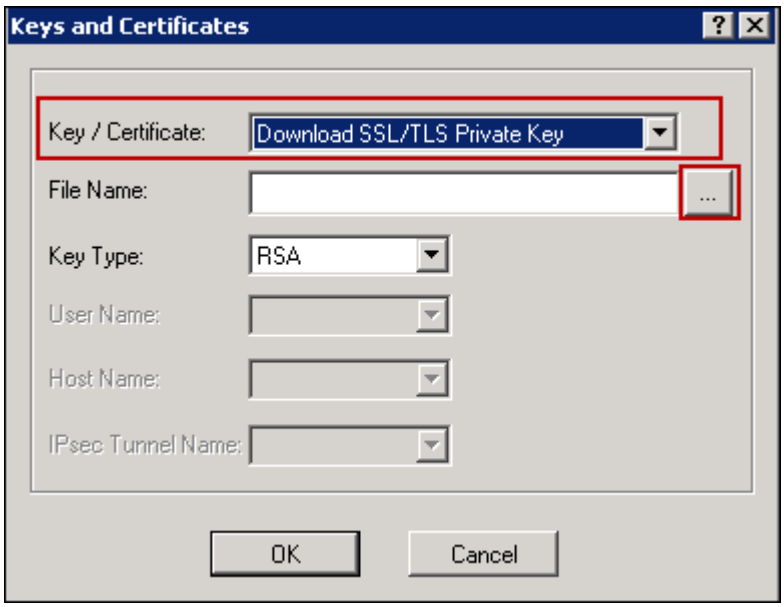
6. Select **Configuration > Security > SSL/TLS**.



7. Set **SSL/TLS Version** field to **Any**.
8. Set **SSL/TLS Type** field to **Server**.
9. Select the **SSL Certificate** section.
10. Enter the password of the SSL certificate in the **Passphrase** field.
11. Select **Tools > Advanced > Keys and Certificates**.



12. In the **Key/Certificate** drop-down list, select **Download SSL/TLS Private Key**.
13. Click the browse button and upload the private key for your Root certificate (.pem).
14. Click **OK**.



15. Select **Tools > Advanced > Keys and Certificates**.
16. In the **Key/Certificate** drop-down list, select **Download SSL/TLS Certificate**.
17. 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.
18. Click **OK**.
19. Select **Tools > Advanced > Keys and Certificates**.
20. In the **Key/Certificate** drop-down list, select **Download SSL/TLS CA**.
21. Click the browse button and upload the upload the Root certificate (RootCertificate.pem file).
22. Click **OK**.

Time Zone/Summer Time (Daylight Saving Time) Parameters

Field	Description
Time Zone Name	The name of the time zone to be displayed during standard time. **Field Format:** Maximum four characters and minimum three characters (do not use angle brackets <>)
Time Zone Offset	The offset from Coordinated Universal Time (UTC) for the local time zone. **Field Format:** Hours *hh* (valid -12 to +24) and minutes *mm* (valid 0 to 59 minutes)
Summer Time Name	The name of the configured summer time zone will be displayed during the summer time setting. If this parameter is not set, then the summertime feature will not work. **Field Format:** Maximum four characters and minimum three characters (do not use angle brackets <>)
Summer Time Offset	The offset from standard time in minutes. Valid values are 0 to 180. **Range:** 0-180 **Default:** 60

Summer Time Mode	Use this mode to configure when the summer time will take effect. **None** – No summer time change **Fixed** – The summer time change goes into effect at the specified time every year. For example, April 15 at 1:00 P.M. **Recurring** – The summer time change goes into effect every year at the same relative time. For example, on the third week in April on a Tuesday at 1:00 P.M. **Default** – None
Fixed Start Date	The exact date and time in which the IOLAN's clock will change to summer time (daylight saving time) hours.
Fixed End Date	The exact date and time in which the IOLAN's clock will end summer time hours and change to standard time.
Recurring Start Date	The relative date and time in which the IOLAN's clock will change to summer time (daylight saving time) hours. Sunday is considered the first day of the week.
Recurring End Date	The relative date and time in which the IOLAN's clock will end summer time hours and change the standard time. Sunday is considered the first day of the week.

I/O Access Settings

▷ Log in to the device using the DeviceManager.

1. In the **DeviceManager** window, click **I/O Interfaces** on the left-hand side menu, and then click **Settings**.

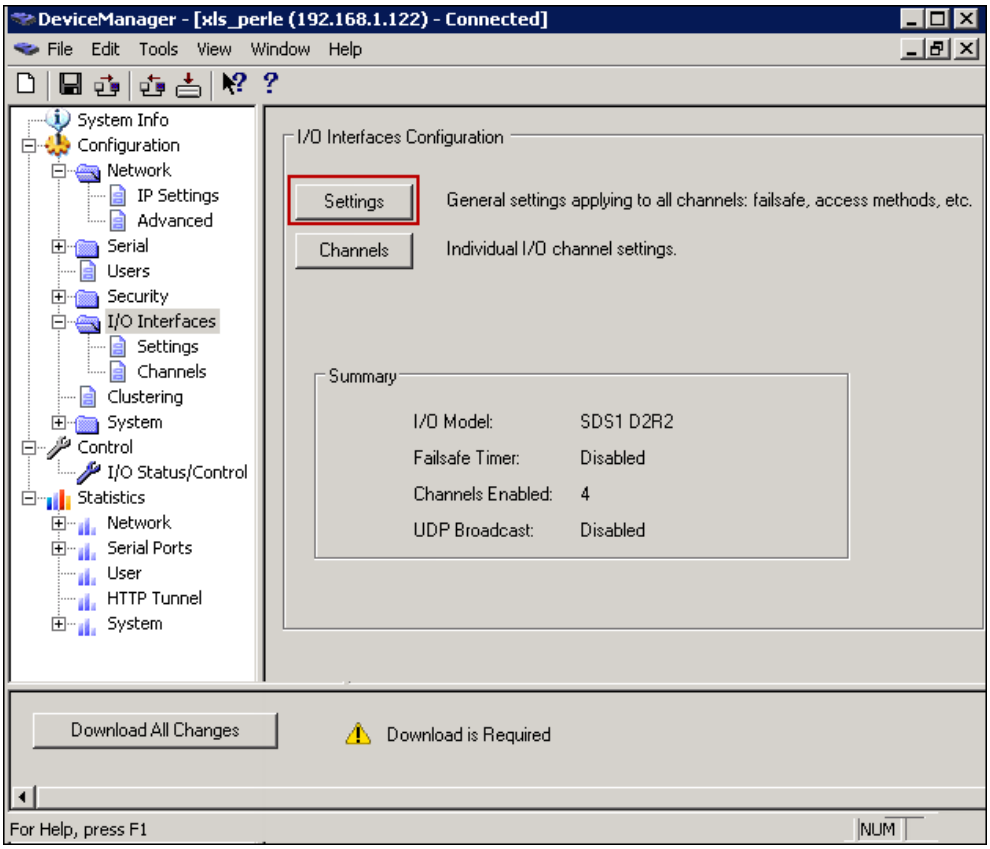


Fig. 50: I/O Interfaces Configuration

2. On the **I/O Access** tab, select the **Enable I/O Access via TruePort** check box.

   NOTE 1: By default, the device monitors I/O commands on TCP port 33816. If there is a need to change the I/O TCP port, it can be changed as long as the change does not conflict with other services or TruePort ports.

   NOTE 2: 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.

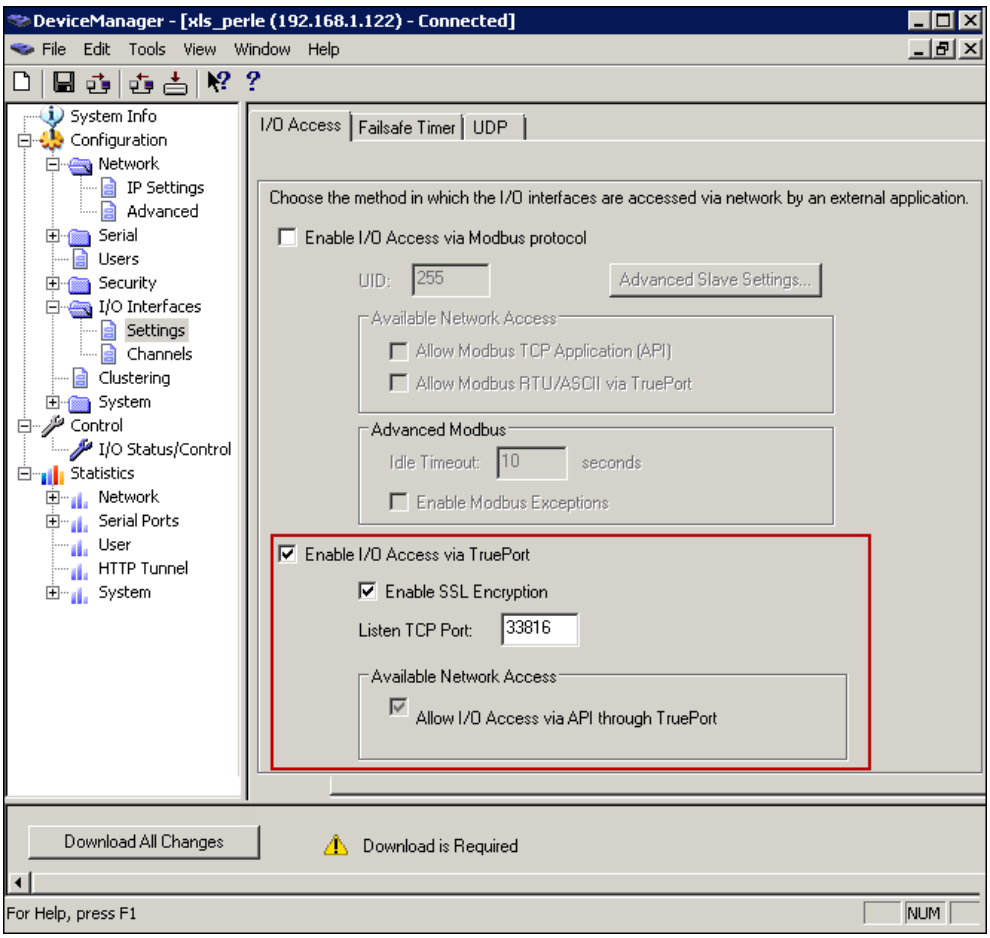


Fig. 51: I/O Access Tab

3. Select the **Enable SSL Encryption** check box.

⇨ Configuration is now complete. Click **Download All Changes** to make the changes to the device or continue with other settings.C

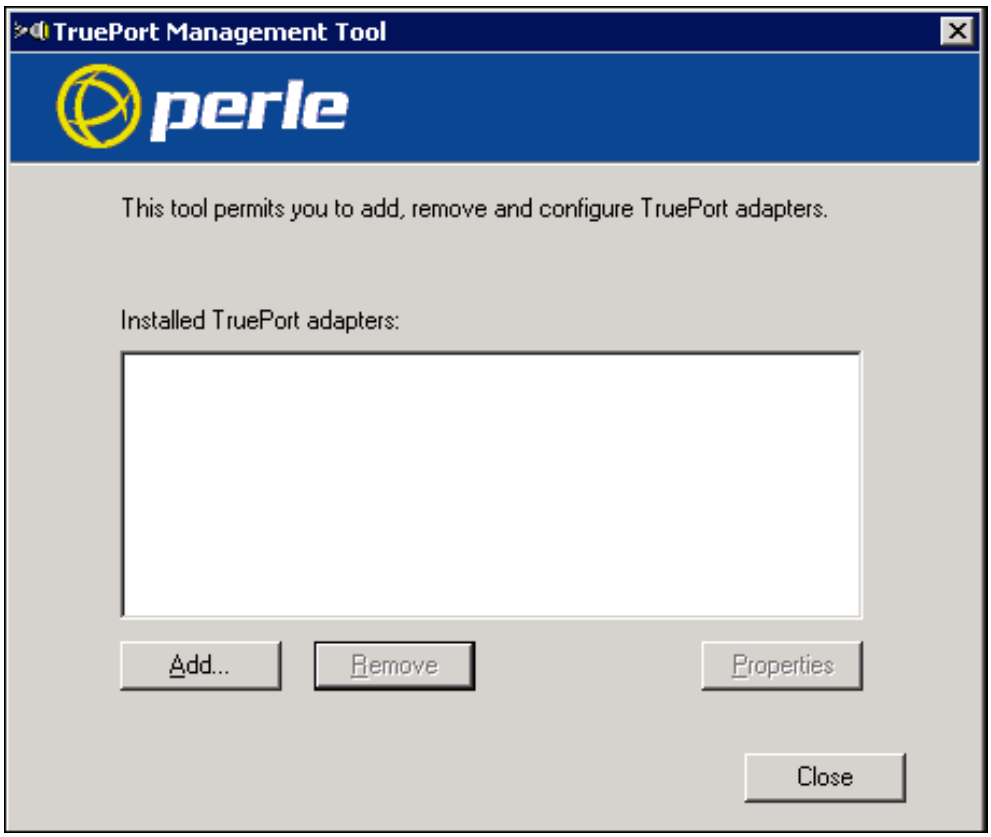
◈ Click **Reboot IOLAN**.
NOTE: Any time you reboot the device, or power is reconnected, you must wait 90 seconds for the device to reboot and initialize. When the device is ready, the Power LED will be solid green and the Link LED will be solid amber/green.

TruePort Driver Configuration

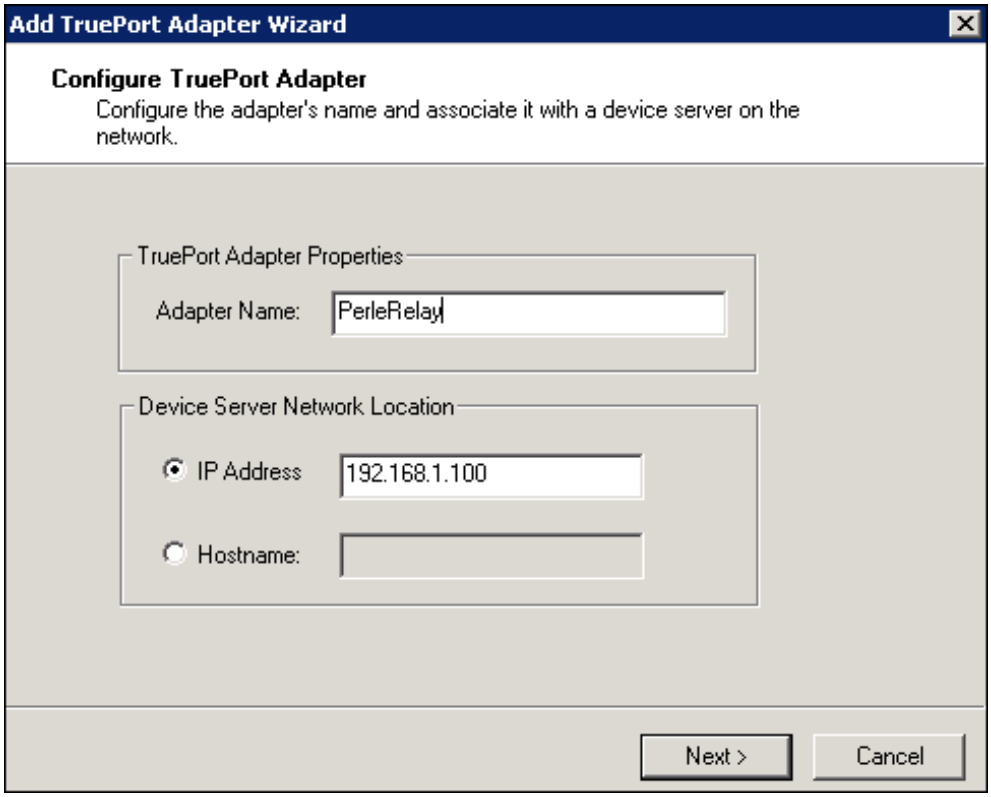
The TruePort driver is the second part of the process to link the device to the server. The TruePort driver is designed to manage all similar devices communicating with the server. Since TruePort creates a virtual COM port, each device should have a COM port for each service.
NOTE: Serial communication and I/O access are each considered a separate service and therefore require separate COM ports.

▷ Ensure that the TruePort is installed on the server.

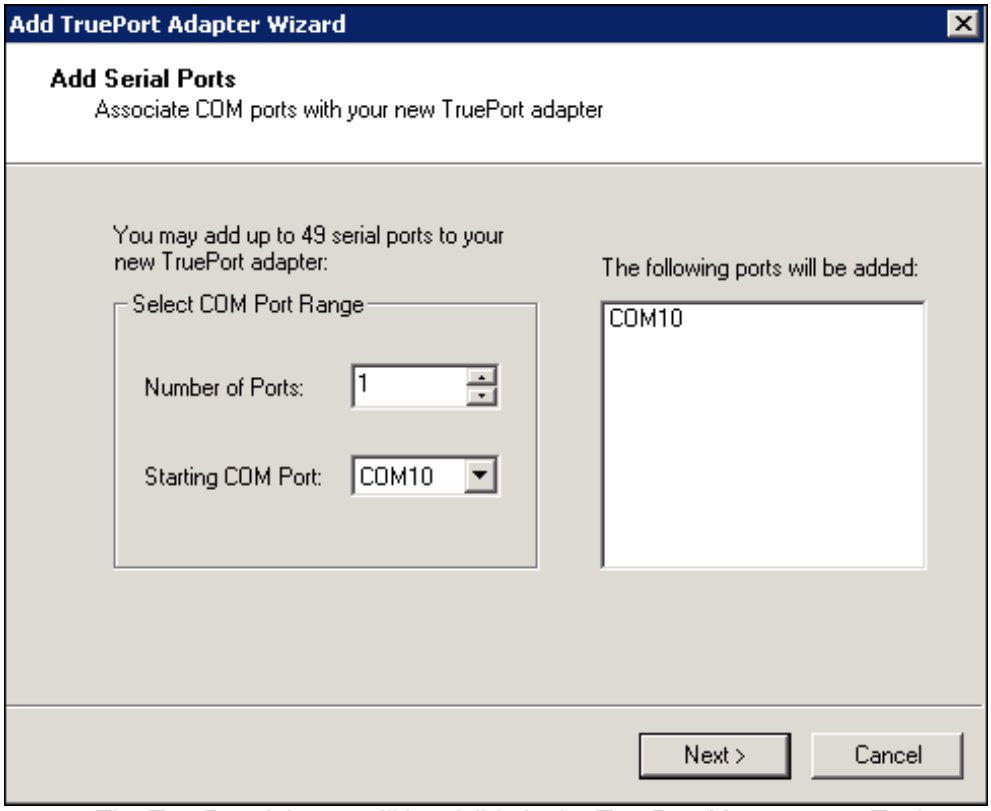
1. Start the **TruePort Management Tool**.
2. In the **Management Tool** window, click **Add**.



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



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

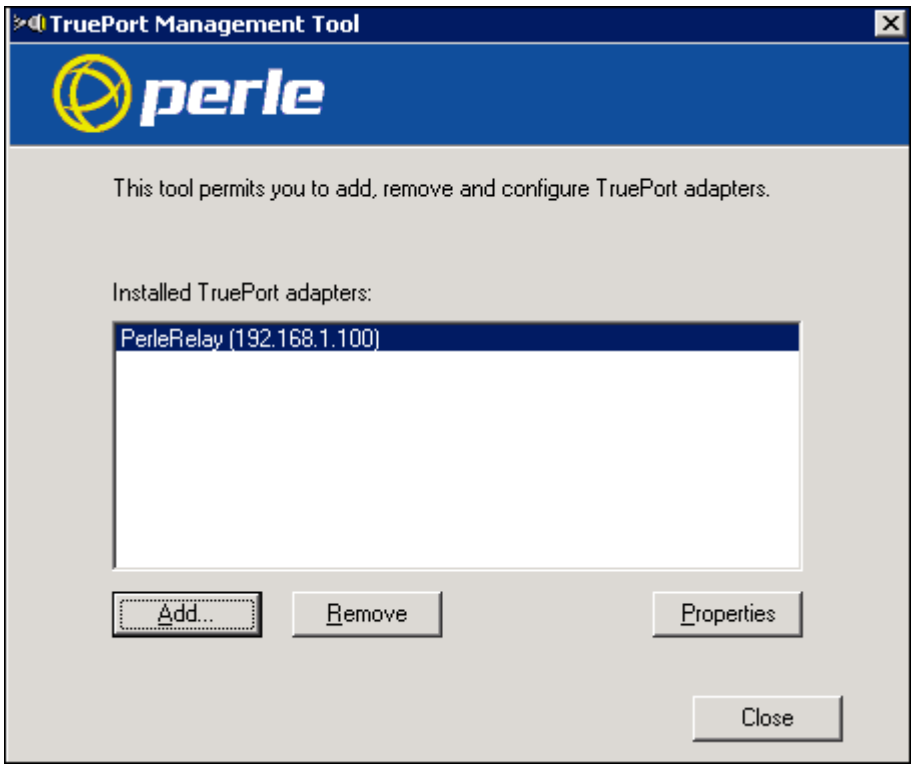


⇨ The TruePort Adapter will be visible in the TruePort Management Tool.

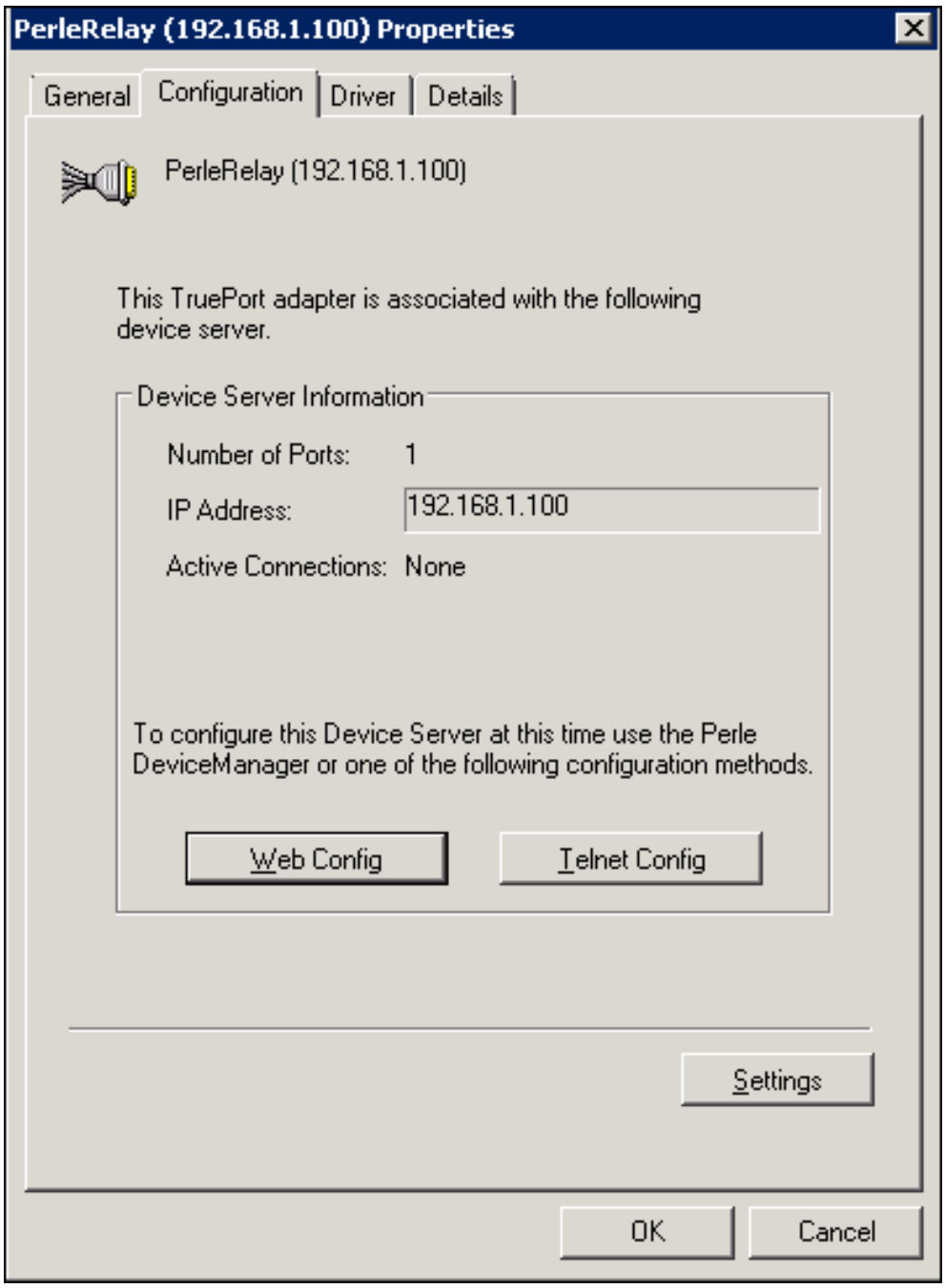
I/O Access Settings

To configure the I/O access settings, do the following steps:

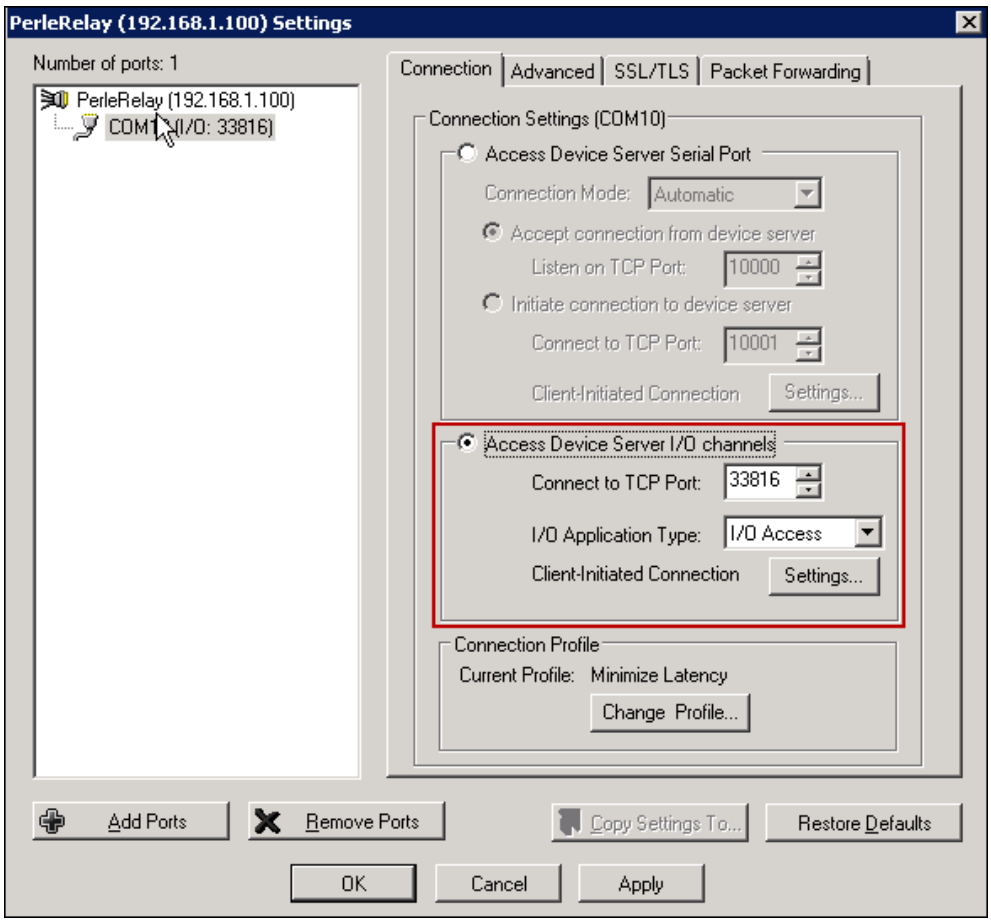
1. Start the **TruePort Management Tool**.
2. Select the Perle device to configure.
3. Click **Properties**.



4. Select the **Configuration** tab.
5. Click **Settings**.

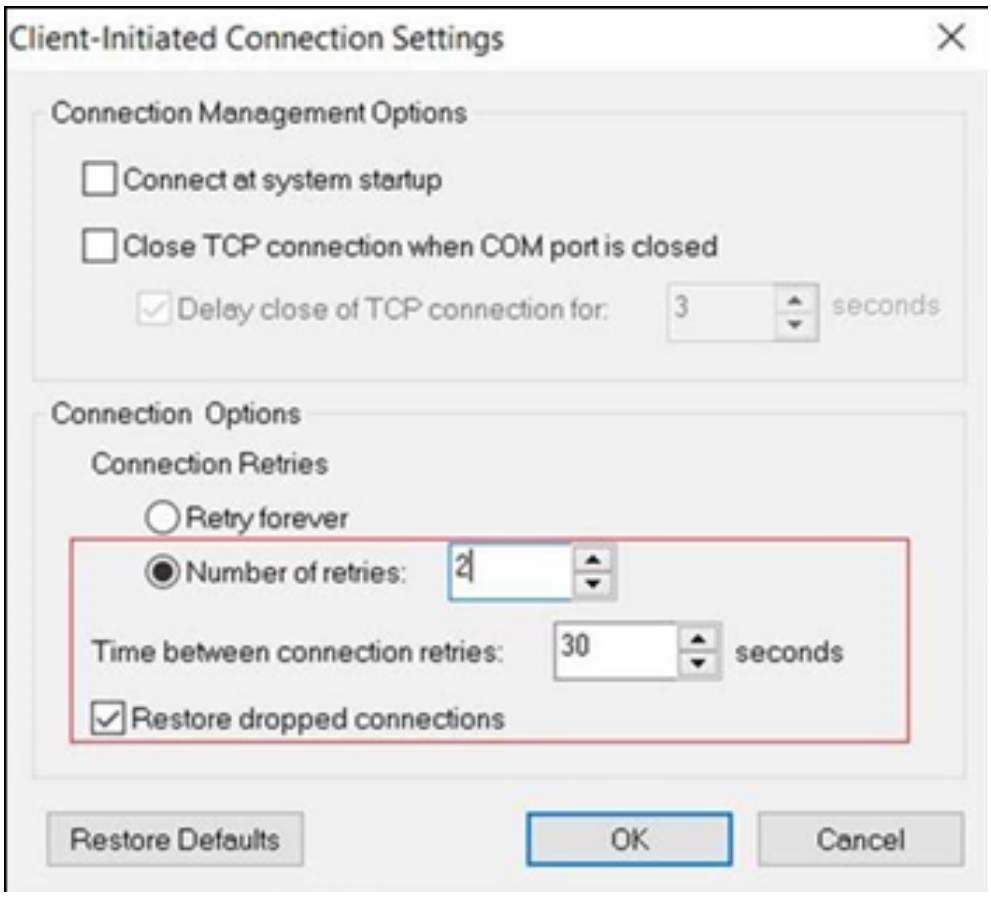


6. If there were two COM ports originally created for this device, select one to use for I/O access. If the COM port selected is being used, the other COM port should be reserved for serial communication. If a second COM port was not created, click the **Add Ports** button at the bottom of the window.
7. Select the **Connection** tab.
8. Select **Access Device Server I/O channels**.
9. Select the **Connect to TCP Port** that was configured on the device for I/O access.
   – In the **I/O Application Type** drop-down lsit, select **I/O Access**.

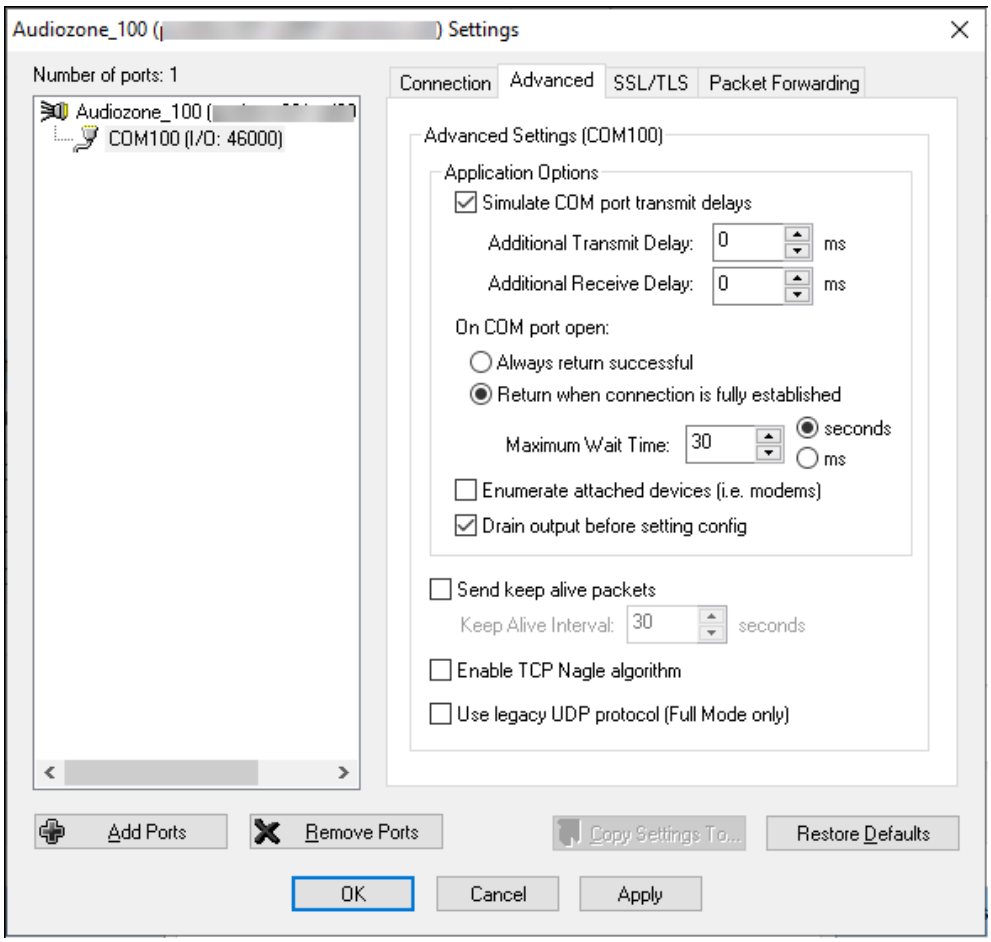


10. Click the **Settings** button next to **Client-Initiated Connection**.

⇨ The **Client-Initiated Connection Settings** window displays:



11. In the **Connection Options** section, do the settings only for the following parameters:
    - **Number of retries**: 2.
    - **Time between connection retries**: 30.
    - Select the **Restore dropped connections** check box.
12. In the **Connection Management Options** section, ensure that you do not select **Connect at system startup** and the **Close TCP connection when COM port is closed**.
13. Select the **Advanced** tab.



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

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

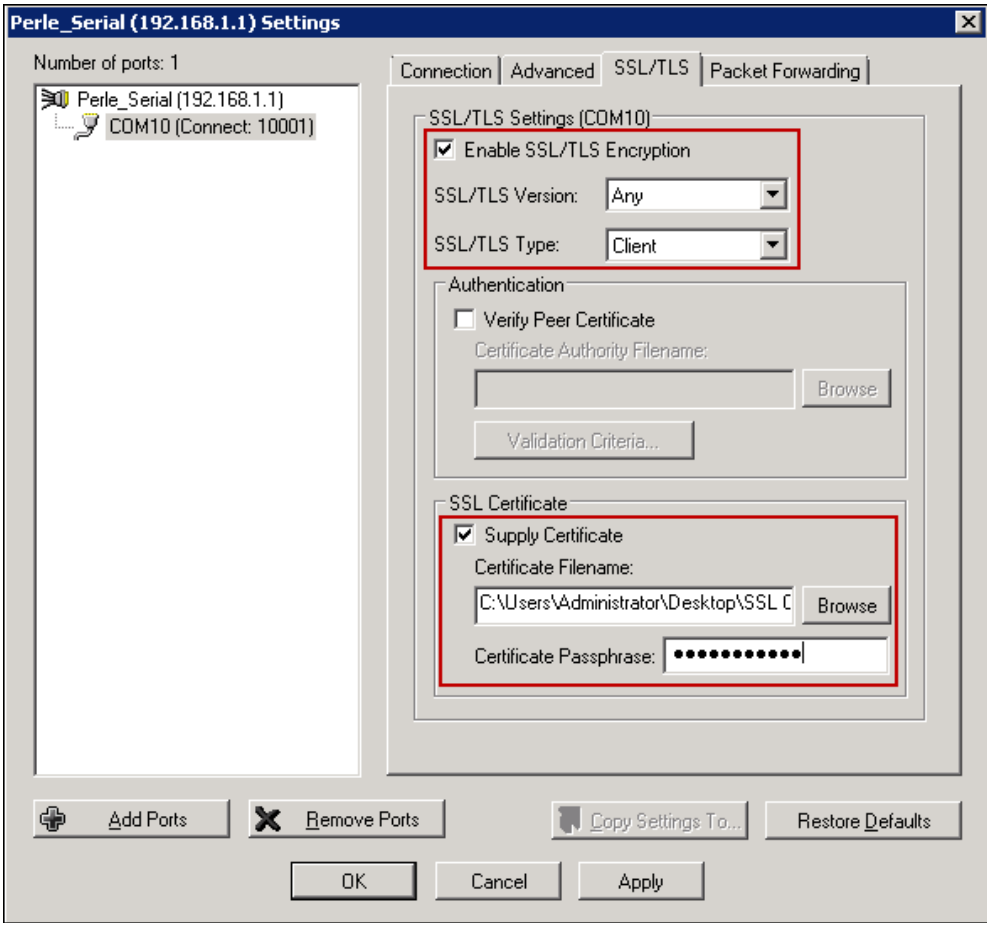
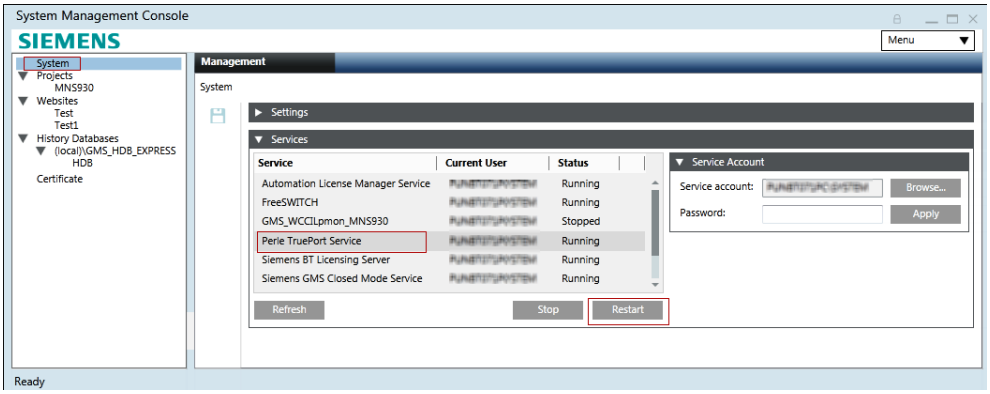


Fig. 52:

16. Select the **Enable SSL/TLS Encryption** check box.
17. Set the **SSL/TLS Version** field to **Any**.
18. Set the **SSL/TLS Type** field to **Client**.
19. Select the **Supply Certificate** check box.
20. Click the browse button and select the combined Root certificate. Refer to the Device Configuration section for more information on combining a Root certificate.
21. Enter the password in the **Certificate Passphrase** field.
22. Click **Apply** and then **OK**.
23. Restart the **Perle TruePort Service** from the SMC.



⇨ The TruePort driver is ready for I/O access.

Device Verification

I/O and Relays

A procedure for testing relays and I/O from the server without is yet to be determined.

Single Zone Audio Device Troubleshooting

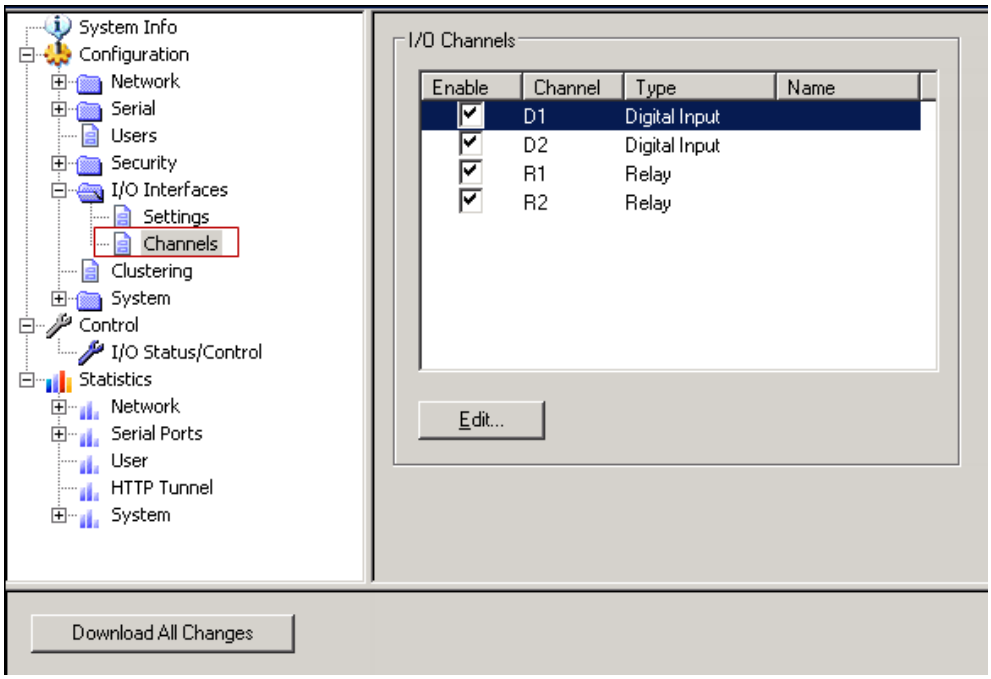
Problem: Once the device is created in the **Device Editor** section, the corresponding device gets in `Connected` state based on the **Check Status Rate** configured in the **Configuration Properties** of the driver. However, at times the device does not get connected after the **Check Status Rate**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

Problem: Messages not getting delivered to the Audio device.

Solution: Ensure that the corresponding I/O channels are selected. To select the I/O channels, select **I/O Interfaces > Channels** in the Device Manager of the Perle Device.

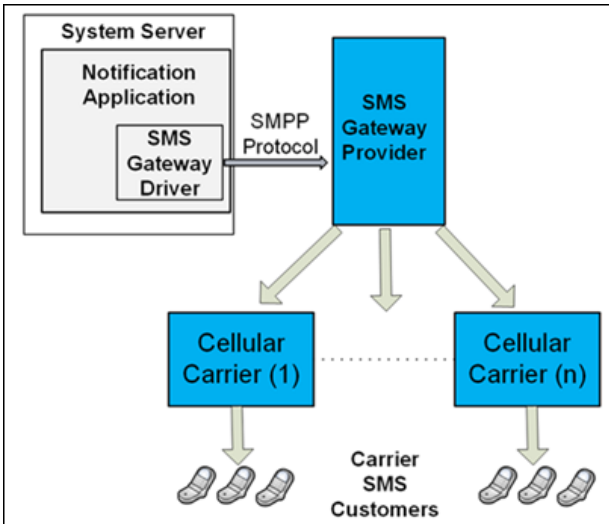


1.31 External SMS Gateway Provider

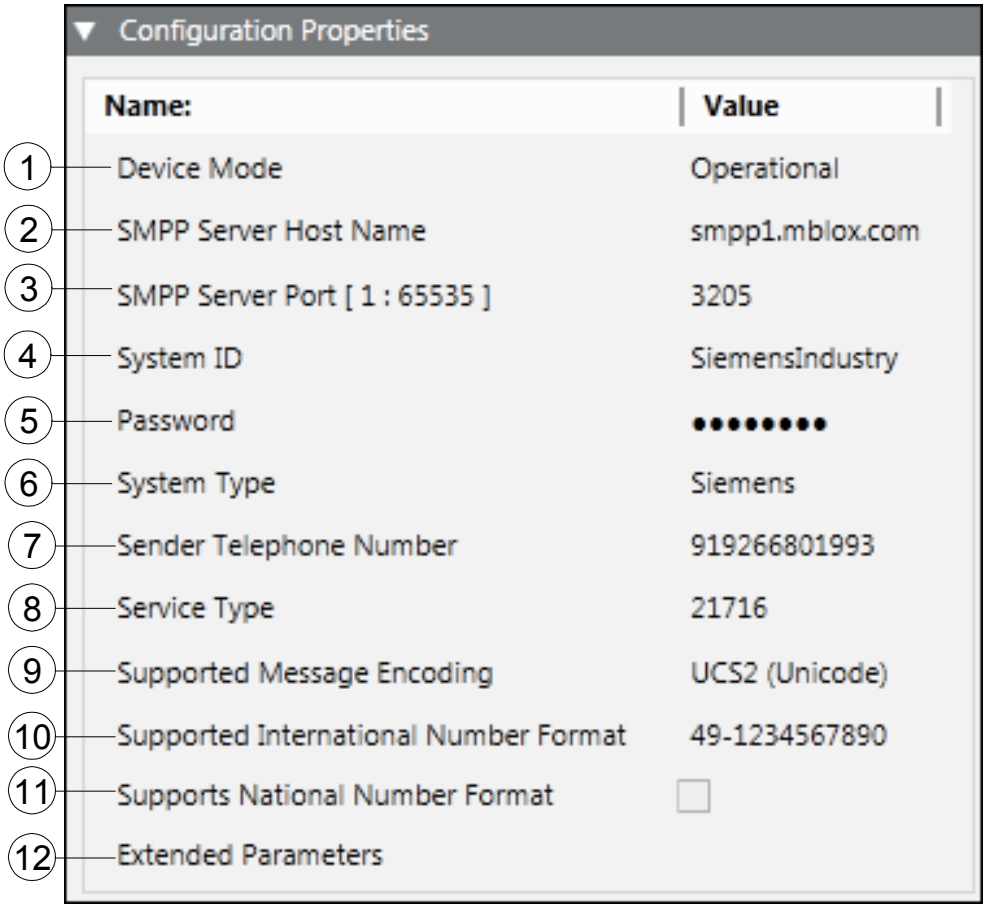
External SMS Gateway Provider

This section contains general reference information about Notification and how the External SMS Gateway provider device is integrated. For procedures and workflows, see the step-by-step section.

provides the capability to send messages to recipients through the Short Message Service (SMS) by way of an External SMS Gateway Provider using the Short Message Peer-to-Peer (SMPP) protocol. The following figure gives a conceptual overview of SMS messaging set up with External SMS Gateway Provider.



Configuration Properties for External SMS Gateway Provider Device



- **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.

- **SMPP Server Host Name**: Enter the External SMS Gateway Provider Server IP address or Host Name.
- **SMPP Server Port**: Enter the External SMS Gateway Provider Server Port number.
- **System ID**: Enter the user name (System ID) to enable to connect to External SMS Gateway Provider.
- **Password**: Enter the password for the corresponding user name (System ID). The Password parameter specifies the password to enable to connect to the External SMS Gateway Provider.
  NOTE: The Password is stored in encrypted format for security reasons.
- **System Type**: Enter a string that is used during login. It should be set only if required by the SMPP server. The SMPP system administrator will provide this value, when required. This value is usually a short text string.
- **Sender Telephone Number**: Enter the default sender telephone number to apply to outbound SMS messages.
- **Service Type**: Allows to set the SMPP parameter service type. The SMPP parameter is required by some service providers. This information is provided by the External SMS Gateway Provider.
- **Supported Message Encoding**: Select the message encoding that is supported by the External SMS Gateway Provider from the drop-down list.
- **Supported International Number Format**: Select the telephone number format for international dialing that is supported by the External SMS Gateway Provider.
  NOTE 1: If the External SMS Gateway Provider does not support any international formats, select Not supported.
  NOTE 2: If the External SMS Gateway Provider supports multiple formats, select any of them.
- **Supports National Number Format**: Select the check box if the External SMS Gateway Provider supports telephone numbers in national format (numbers without any country code).
- **Extended Parameters**: Allows passing additional parameters to the function call. This information is provided by the External SMS Gateway Provider.

If the format of telephone numbers configured for Recipient Users is not directly supported by an External SMS Gateway Provider, the driver performs one of the following conversions to a supported format:

- A national number is converted to an international number by optionally removing a leading zero and then adding the country code plus a supported prefix (none, +, or the international prefix for dialing).
- An international number is converted to a different format by changing the supported prefix (none, +, or the international prefix for dialing).
- The driver ignores all special characters in Recipient User telephone numbers, such as (,), -, /, and so on, except for a leading + sign that indicates an international number format

If a message contains more than 160 characters (under GSM-03.38 or ISO-88591 encodings) or 70 characters (under UCS2-UNICODE encoding), then the message gets split into smaller messages (each of length 153 characters under GSM-03.38 or ISO-88591 encodings and each of length 67 characters under UCS2-UNICODE encoding) by MNS and it gets concatenated at the receiving device (based on SMS concatenation capability of the network and receiving device). If the network or the receiving device does not support concatenation of the split messages into single SMS, then the split messages gets received as multiple SMS on the receiving device.

In order to receive SMS messages, ensure that the receiving device is not registered for Do Not Disturb (DND) service.

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.

In the case of GSM 03.38 encoding, certain special characters ("^", "{", "}", "\", "[", "~", "]", "|", "€") use 2 characters' space in an SMS. As a result, for each special character, the maximum length of the message decreases by 1.

If a message contains characters that are not supported by the configured encoding, then the respective characters are replaced with the ? symbol.

List of Operators

Operator	Description
Contains	Checks whether recipient user address string contains the assigned value or not. If yes, the corresponding message is routed through the device.
Does Not Contain	Checks whether recipient user address string contains the assigned value or not. If not, the corresponding message is routed through the device.
Starts with	Checks whether recipient user address string starts with the assigned value or not. 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 or not. If not, the corresponding message is routed through the device.
Ends With	Checks whether recipient user address string ends with the assigned value or not. 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 or not. If not, the corresponding message is routed through the device.
Equals	Checks whether recipient user address string is equal to the assigned value or not. If yes, 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 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 or not. If 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 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. You can 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.
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 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. You can 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 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 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.

Examples of Regular Expressions

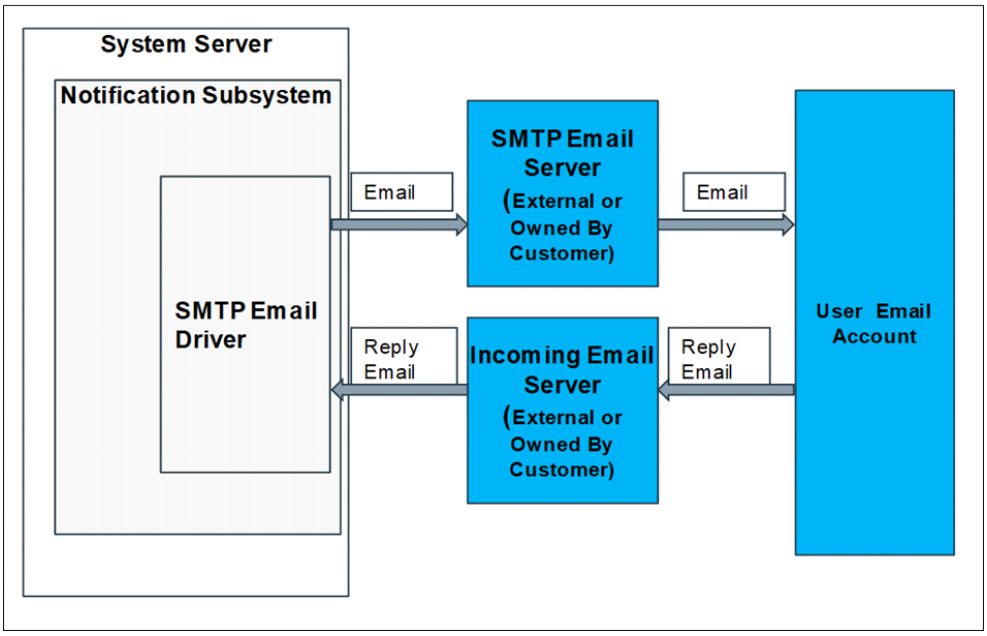
Regular Expressions	Description
^\d+	String starts with one or more digits only.
^[+](91)	String should start with +91.
^.+?\d$	String ending with digits only.
^[0-9]{10}(52|56|57)$	String is 12 digits long (numbers only) and ends with 52, 56, or 57.
^9881231231$	Matching exact mobile number.

1.32 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.

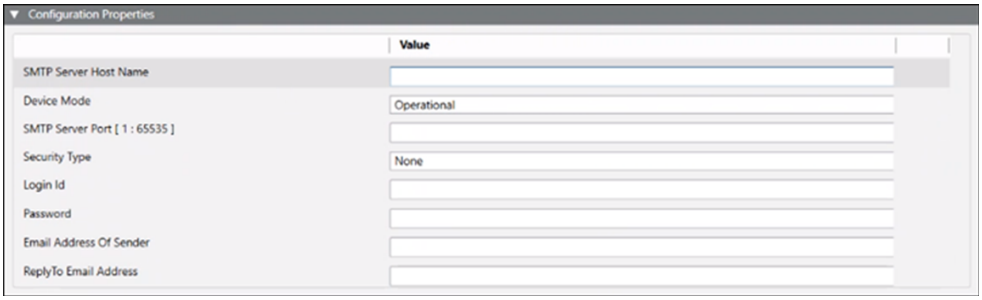
Though technically SMTP Email Server is not a device, generally uses the term device for entities participating in notification delivery, including intermediary services such as an SMTP Email Server.



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



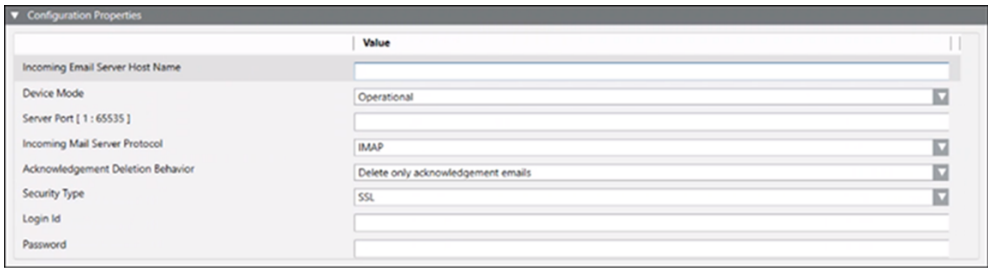
- **SMTP Server Host Name**: Enter the IP address or the server name of the SMTP Server.
- **Device Mode**: Select one of the following modes from the drop-down list:
  Disabled: In this mode, the driver does not process the messaging command, the device configuration change command, and perform status 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 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 .

Configuration Properties for Incoming Email Server



- **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 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 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.

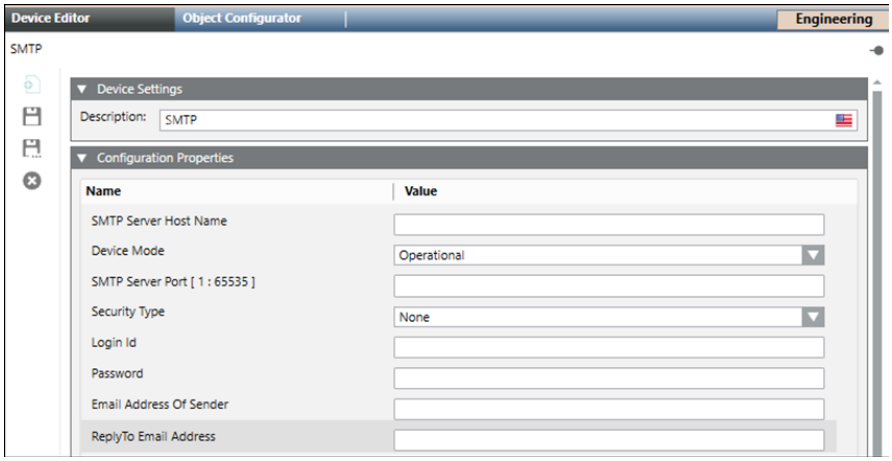
Configuring Message Identity

▷ 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.



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.

1.33 Telephony Device

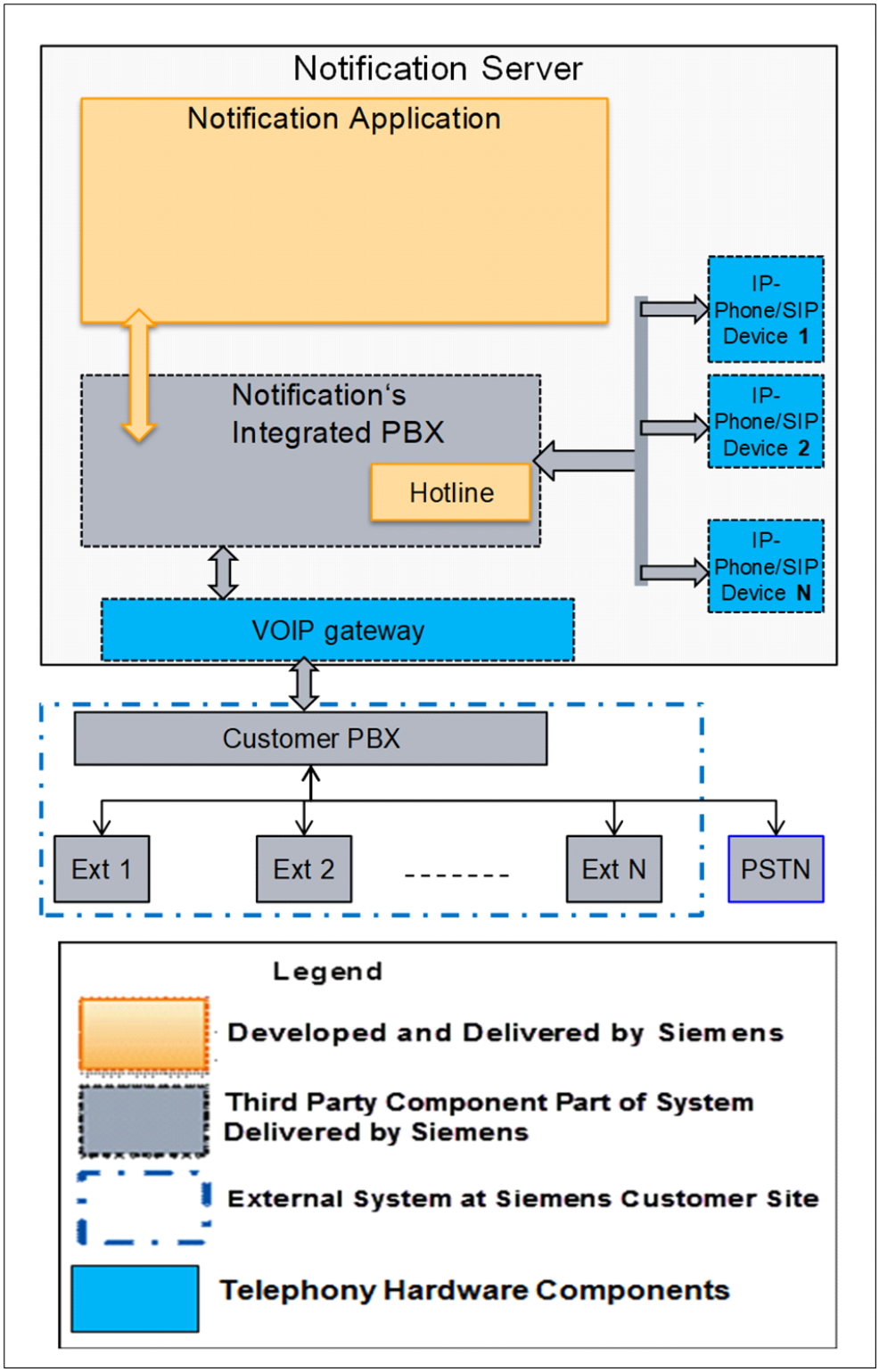
Telephony Configuration Device

This section provides reference and background information for integrating the Telephony device.

’s VoIP Switch is installed by the installer.

uses Voice over Internet Protocol (VoIP) technology to deliver audio content to recipient devices and users. The following voice features are available in using VoIP.

- Audio messaging to connected SIP capable devices
- Emergency Hotline
- Live Announcement
- Dial in
- Interface with on-site PBX for audio message delivery to landline or mobile phones



This is achieved using a VoIP PBX called FreeSWITCH (http://freeswitch.org/) hereafter referred to as 's VoIP Switch. This forms the basis for the various telephony based functionalities available in . The telephony functionalities require hardware and software components that need to be configured independently but work in unison to achieve various functionalities. The following image gives a pictorial overview of the different components involved.

Prerequisites

The following hardware and software components need to be installed and configured:

- 's VoIP Switch
- Polycom SoundPoint 331IP Phones

- Digital Acoustics IP7-ST, line level audio device
- For PBX integration: Sangoma Vega 200/400 VoIP gateway in case a traditional PBX is being used. If a VoIP switch is being used, details to access the server, like IP address and port numbers, would be needed.
  NOTE: The VoIP gateway supports redundant server deployment.

For installing the Telephony Configuration device, see Telephony Device section.

Overview of PBX Integration

can interface to a external PBX owned by the customer. This integration allows to call communicate with telephones outside the immediate network on a traditional telephone exchange system.

The table below summarizes the scenarios for which PBX integration is required.

Feature	Hotline	(Notification calling phone)
Access from IP Phone directly connected to FreeSwitch on Server	No	No
Landline	Yes	Yes
Mobile Phone	Yes	Yes
Extension on Customer's PBX	Yes	Yes

For more information on configuration and integration of PBX, see PBX Integration section.

Achieve PBX Integration

Depending on the type of PBX onsite, additional devices may be needed to integrate with that PBX.

Traditional PBX: A traditional PBX is a PBX which can only be interfaced to via a T1, E1, or J1 connection. Additional hardware, such as the a VoIP gateway, would be needed. The VoIP gateway supports redundant gateway.

VoIP-based PBX: In this case, no additional hardware is needed. can interface directly via SIP using the existing ethernet network. However, make sure that the server has network access to the VoIP switch.

For more information on configuration and integration of PBX, see PBX Integration.

NOTE:
The Telephony Configuration tool can be used to configure only the configurations on the side. It is up to the customer to do the necessary configurations on the PBX so that the system can establish connection with that PBX.

Telephony Device

This section contains additional procedures of Telephony Configuration device.

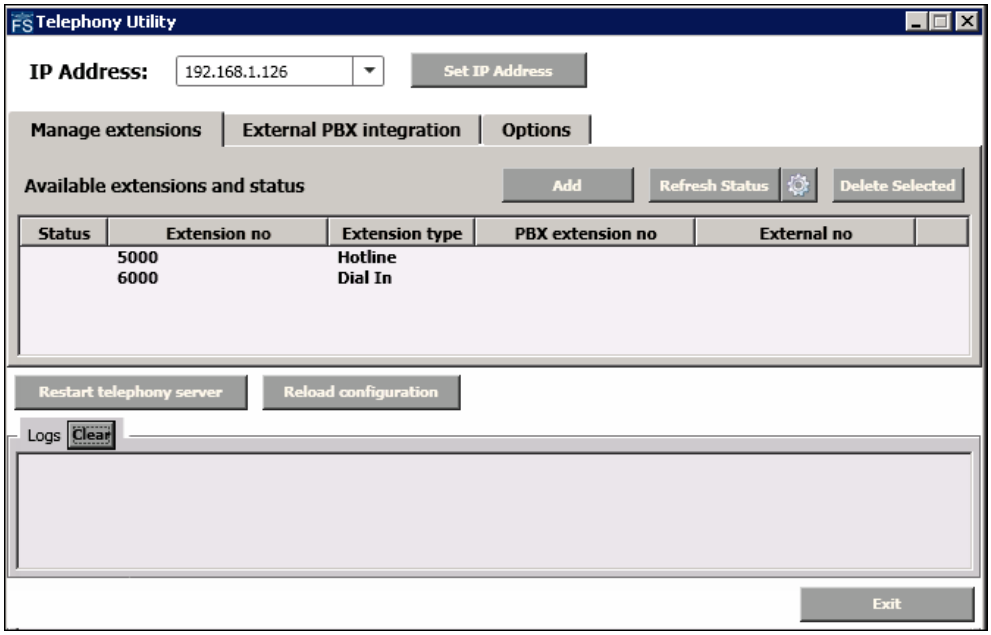
Overview of Telephony Device

All of the Notification's VoIP Switch related configuration and set up for is done through the 's VoIP Switch Configuration tool. From the Windows **Start** menu, select **Start > All Programs > [company name] > > Tools > MNSTools > Telephony Configuration Tool**.

System set up and configuration involves the following steps:

1. Setting the Network Interface Card (NIC) for 's VoIP Switch.
2. Creating new extensions: Every SIP device needs to have an extension. Hence, creating the extensions on 's VoIP Switch first is recommended.
3. Assign extensions to devices during the device configuration.
4. Configure PBX integration.

5. Start the Telephony Configuration tool.
6. The **Telephony Utility** window displays:



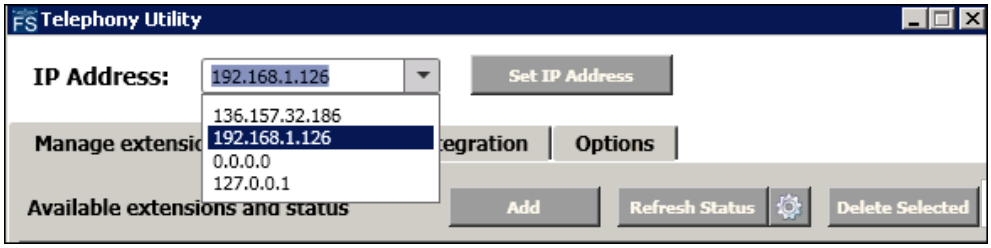
NOTE: Before starting the Telephony Configuration tool, ensure that the FreeSwitch service is running.

Set IP Address for Notification's VoIP Switch

▷ On servers which contain more than 1 Network Interface Card (NIC), the IP address to be used by 's VoIP Switch needs to be set explicitly. This would be the IP address of the network to which IP phones and other devices which need to connect to 's VoIP Switch are connected.
NOTE: Some of the devices, such as the line-level audio devices, need to be set with the IP address of the 's VoIP Switch server instead of the hostname. As a result, it is required that a static IP address be used for the server or that the IP address be reserved.

1. Select the IP address from the IP address drop-down list. In case the server has multiple network cards, multiple IP addresses are listed.
NOTE: Typically all devices including audio devices and IP phones are connected to the same network. Select the IP address that belongs to this network so that devices that need to connect with 's VoIP Switch on the server are able to do so.

   ⇨ The appropriate IP address is shown in the image below.



2. Enter the IP address from the previous step into the **IP Address** field.
3. Click **Set IP Address**.

⇨ The required configuration files are updated. The Server is now a SIP server and registrar on that IP address.
NOTE: The 's VoIP Switch service needs to be restarted for the changes to be effective. This can be done immediately by pressing the **Restart telephony server** button or can be done once all configuration steps are completed.

Creating and Managing Extensions

Extensions are added to the system by using the **Add** button which is used to bring up the **Add Extension(s)** dialog. The dialog can be used to create

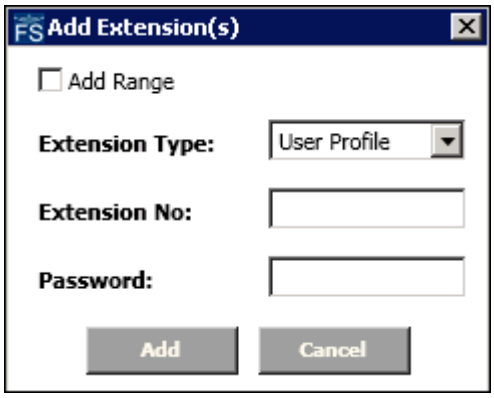
1. User Extensions
2. Dial In extensions
3. Hotline extensions

NOTE: 4 digit extension numbers are reserved for system usage and dial in and hotline functionalities. All user extension numbers need to be 5 digit numbers.

User Extension

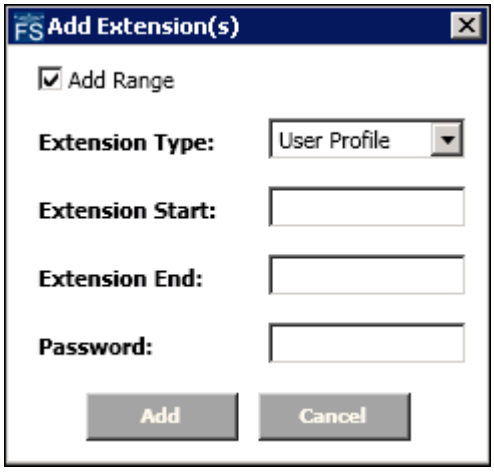
User extensions are assigned to end user devices like IP phones or line-level audio devices which need to connect to Notification's VoIP Switch to make or receive calls.

1. Click **Add** on the main user interface to bring up the **Add Extension(s)** dialog box.

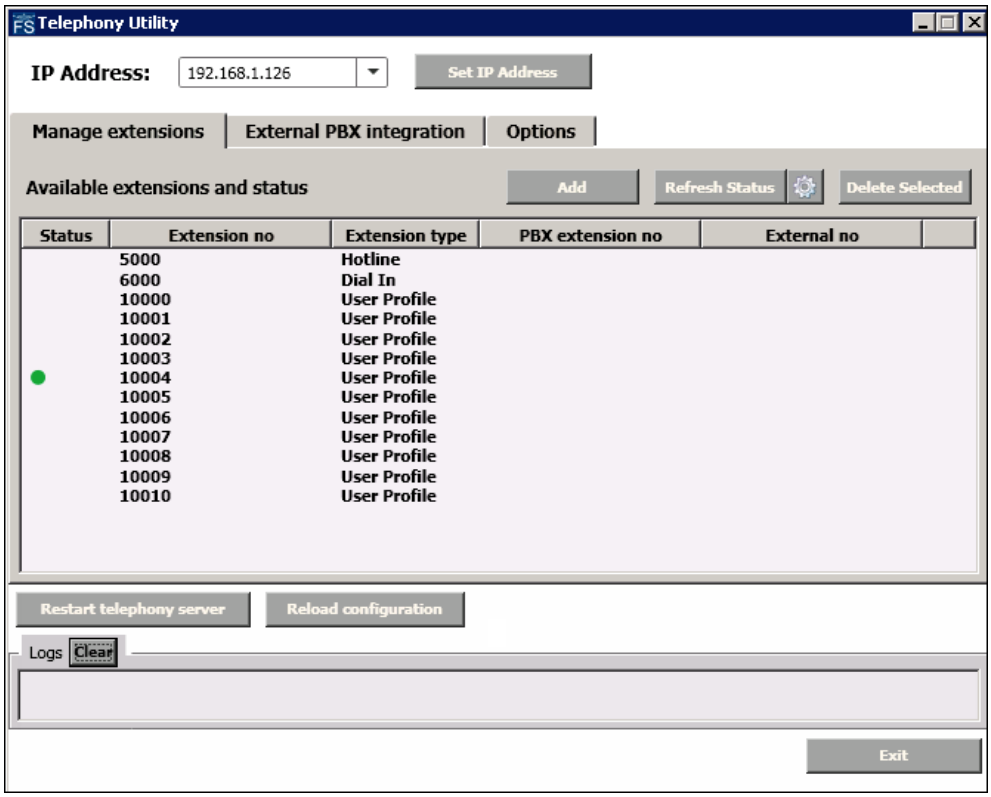


2. Select **User Profile** for the **Extension Type** field.
3. Enter the extension number and the password to be used for that extension. The extension numbers need to be five digits long.
   - When configuring the device (IP Phone or line-level audio device) with this extension, the same password is required to be entered at the device-side. Make sure extensions or passwords for specific devices are recorded for later use.
   - Passwords can only contain numbers 0 through 9. Alphabets and special characters are not allowed.
4. Click **Add**.
5. To create a multiple extensions at once, check the **Add Range** check box to create multiple extensions.
6. Enter the start and end extensions.

7. Enter a password to be used for these extensions.
   NOTE: The same password is applied to all the created extensions
8. Click **Add** to create multiple extensions.
   Example: To create 100 extension numbers from 11000 through 11099, enter **11000** into the **Extension Start** field and **11099** into the **Extension End** field.



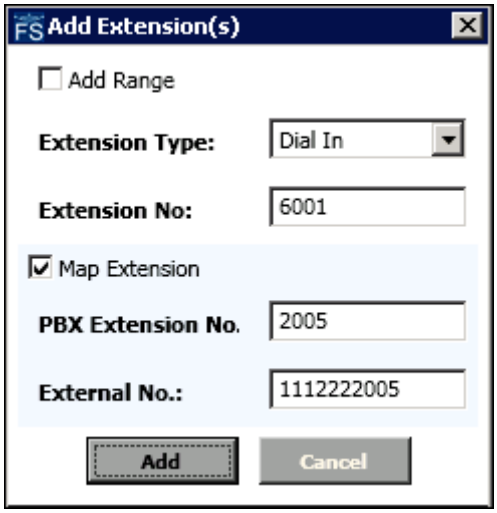
9. Repeat the previous steps to create all the required extensions.
10. Click **Restart telephony server** to restart 's VoIP Switch so that the configurations are loaded and the new extensions are available for use with devices.
    NOTE: The image below shows an example where extensions 10000 through 10010 have been created.



Dial-in Extension

Dial-in extensions are extensions used by to allow users the opportunity to call that extension via phone and initiate Notification incidents remotely.

1. Click **Add** to bring up the **Add Extension(s)** dialog box.
2. In the **Extension Type** field, select **Dial In**.
3. Enter the extension number to be created. Enter any number in the range of 6000 through 6099.



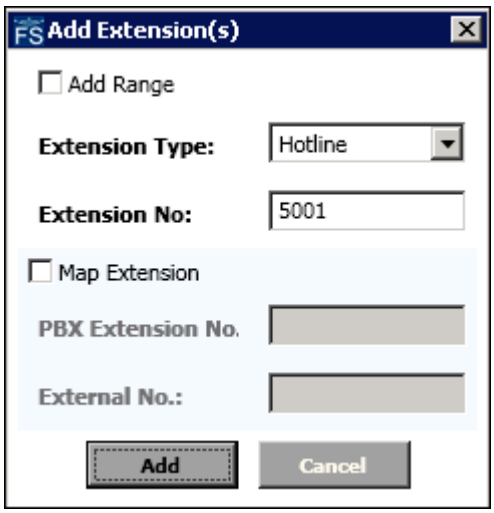
4. Click **Add** to create the dial-in extension.
5. Repeat the previous steps to create more dial-in extensions.
6. **Add Range** can be used to create multiple extensions in a single operation. But PBX mapping needs to be done in a separate step for each extension.
7. Click **Restart telephony server** to restart ’s VoIP Switch so that configurations are loaded and the new extensions are available in ’s VoIP Switch.

Hotline Extension

Hotline extensions are extensions used by to publish specific messages. User can then dial this hotline extension via a phone to listen to any active messages.

The procedure for creating hotline numbers is similar to that of a dial-in number. The only difference is selecting **Hotline** in the **Extension Type**.

1. For the extension enter any number in the range of 5000 through 5099. Extension 5000 is created by the system during installation.
2. Repeat steps to create more hotline extensions.
3. **Add Range** can be used to create multiple extensions in a single operation. But PBX mapping needs to be done in a separate step for each extension.
4. Click **Restart telephony server** to restart ’s VoIP Switch so that configurations are loaded and the new extensions are available in ’s VoIP Switch.

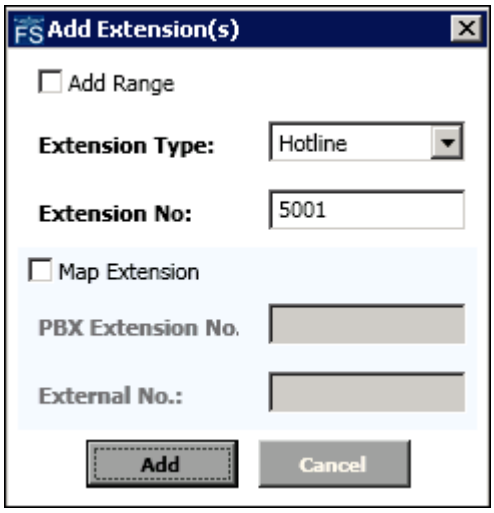


Hotline Extension

Hotline extensions are extensions used by to publish specific messages. User can then dial this hotline extension via a phone to listen to any active messages.

The only difference is selecting **Hotline** in the **Extension Type**.

1. For the extension enter any number in the range of 5000 through 5099. Extension 5000 is created by the system during installation.
2. Repeat steps to create more hotline extensions.
3. **Add Range** can be used to create multiple extensions in a single operation. But PBX mapping needs to be done in a separate step for each extension.
4. Click **Restart telephony server** to restart 's VoIP Switch so that configurations are loaded and the new extensions are available in 's VoIP Switch.



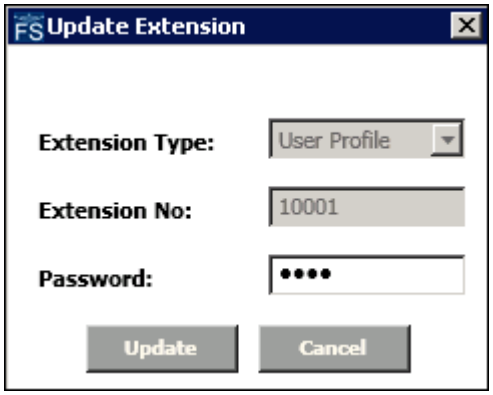
Managing Extensions

The same tool can be used to manage any extension after it has been created. Depending on the extension type following operations are possible:

1. User Extensions: Update the password or delete the extension.
2. Dial In and Hotline extensions: Update the PBX mapping settings or delete the extension.

Edit Password

1. Double-click an existing extension entry to bring up the **Update Extension** dialog box.



2. Enter a new password in the password field to update the extension's password.
3. Click **Update**.
4. Click **Reload Configuration** so that the updated extensions are loaded into 's VoIP Switch and are available for use by the devices.

Delete Extensions

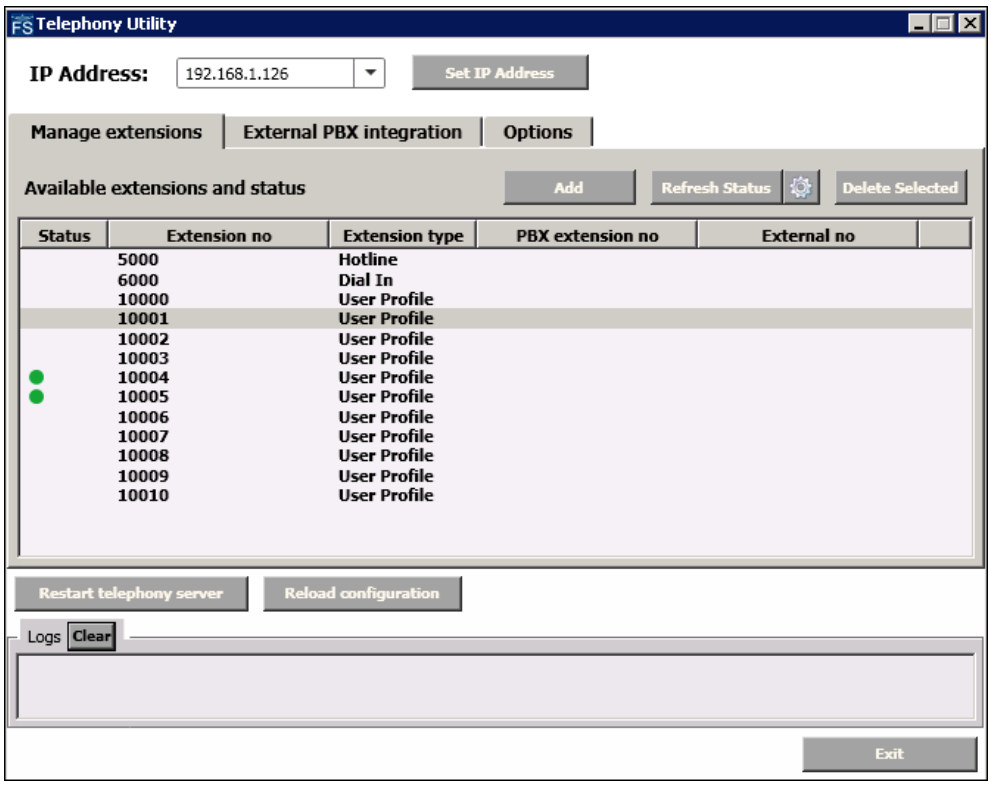
To delete one or more extensions, select one or more entries and click **Delete Selected**. Once deleted, click **Reload Configuration** to reload the updated XMLs into 's VoIP Switch.

View Connection status

The 's VoIP Switch tool can also be used to view the connection status of the devices that are configured to connect to 's VoIP Switch. Once you have configured such devices, click **Refresh Status**. A device which has successfully connected to and registered with 's VoIP Switch will have a GREEN dot to the left of the extension. An example is shown in the image below where extensions 10004 and 10005 have successfully registered with 's VoIP Switch.

The tool can also be configured to refresh the device connection automatically.

Click  next to the **Refresh Status** button to configure refresh settings.



Configuring Audio Devices and IP Phones

1. Assign the device an extension that is already available on ’s VoIP Switch and enter the password that was set when the extension was created.
2. Restart the device. For details on additional details on how to configure the device, refer to the appropriate device integration guide.
   NOTE: The UI on the device shows the status of the connection. This status is shown in the ’s VoIP Switch configuration UI for that particular extension.

PBX Integration

This section describes the steps for the integration of Notification to a external PBX owned by the customer.

Hardware Installation

Refer to the *VoIP Switch Configuration section* to set up and configure the device for use with . Perform the test steps (if any) detailed in the integration guide to ensure correct set up.

PBX Integration Configuration

The Telephony Configuration tool provides the necessary interface to configure the ‘s Integrated PBX to interface with the external PBX. Follow the instructions in the following sections to complete the configuration.

PBX Integration Workspace

The necessary interface for PBX configuration is available in the PBX Configuration tab as indicated in the image below:

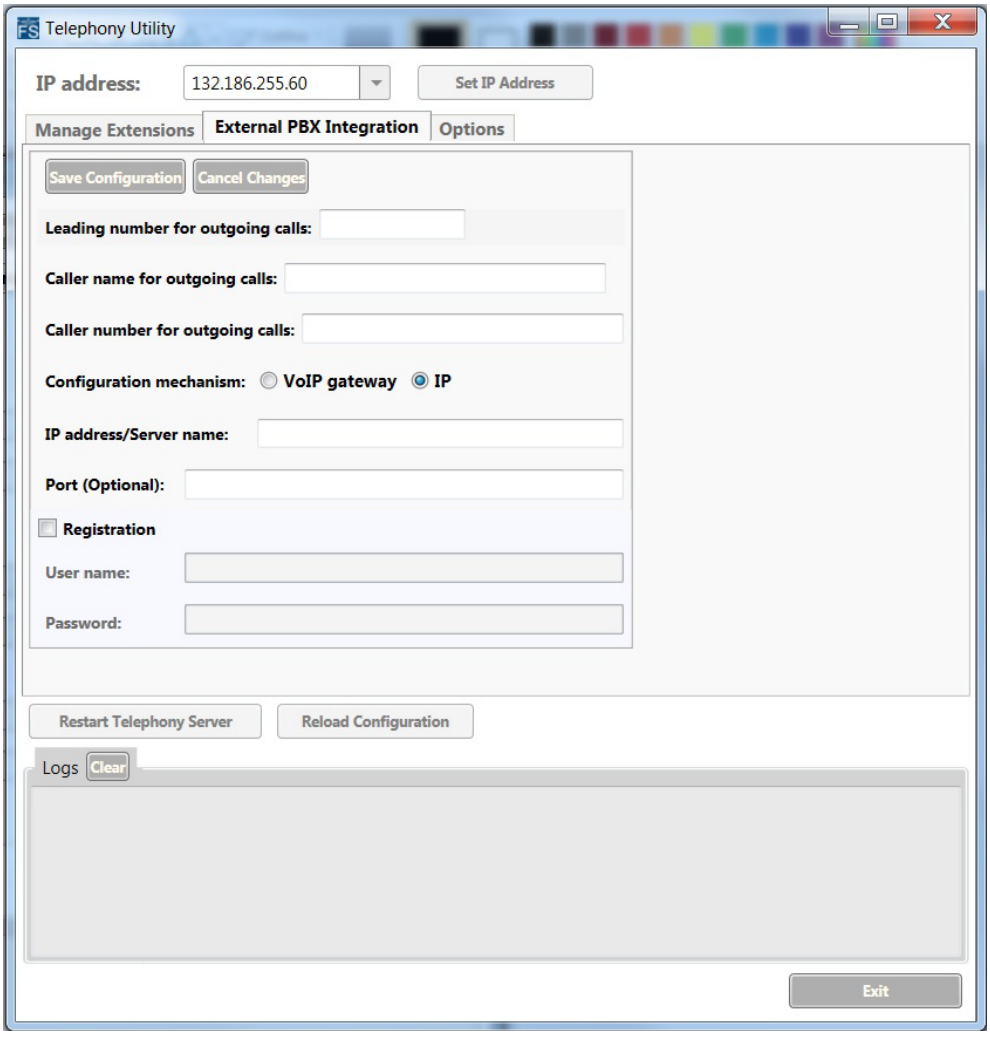
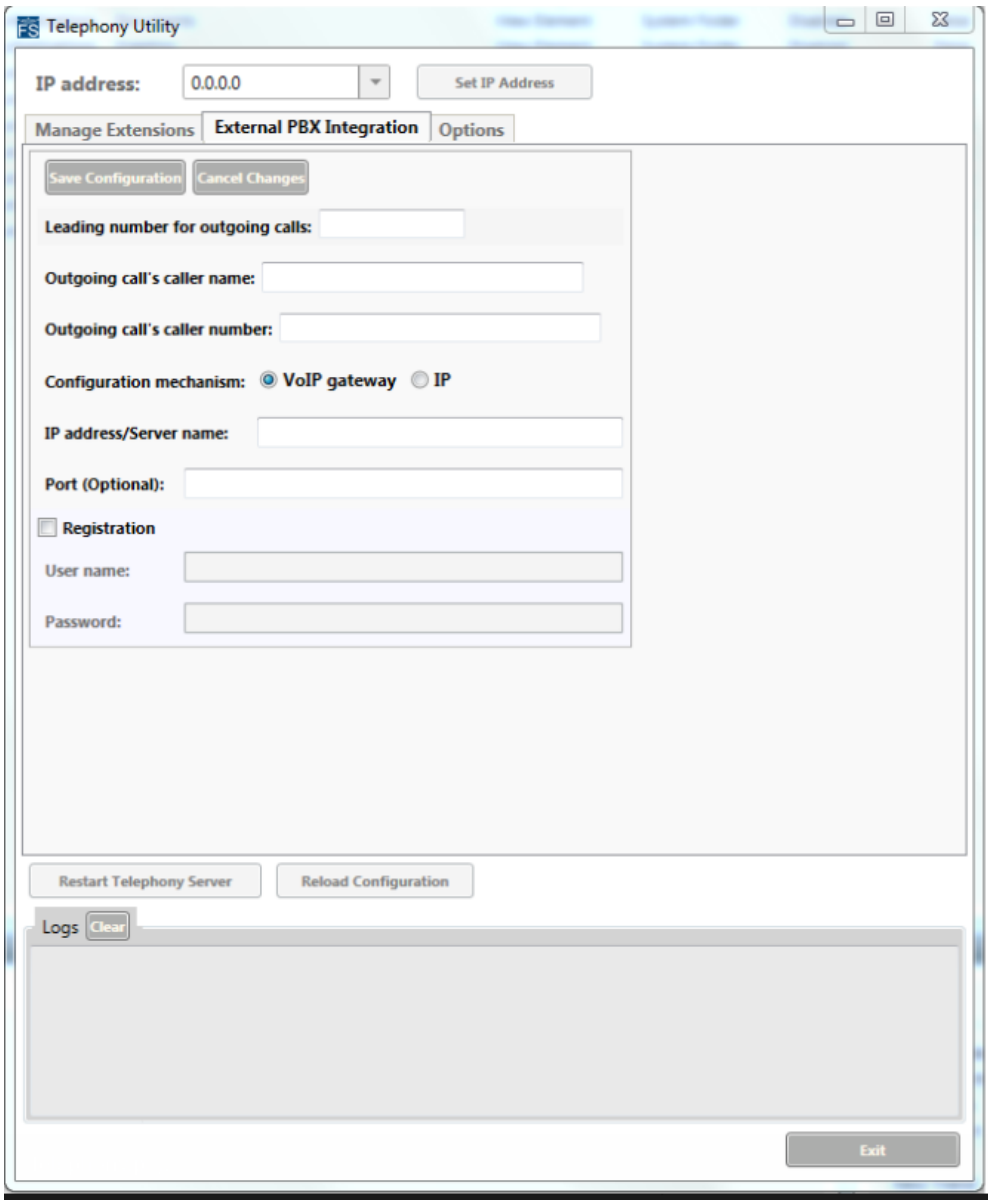


Fig. 53: Main User Interface – PBX Integration Tab

VoIP Gateway Configuration

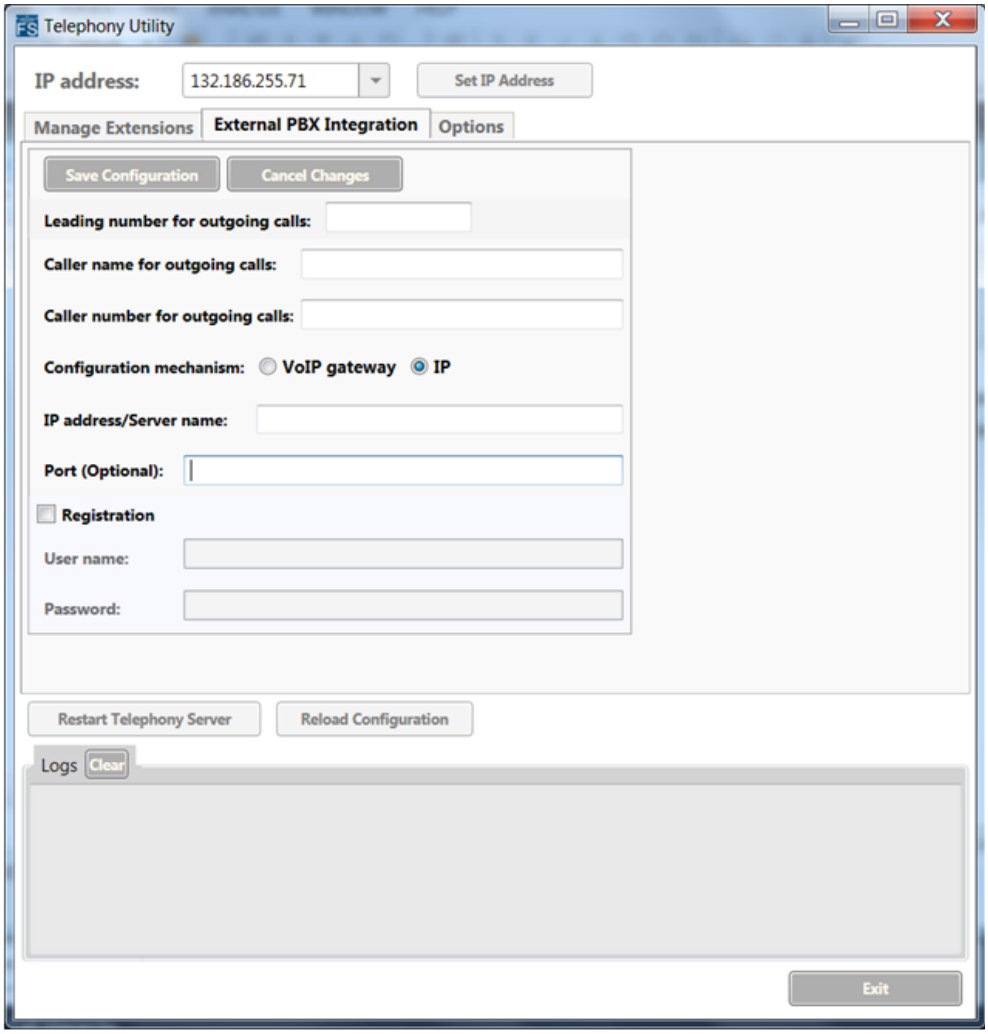
1. Launch the FreeSwitch Configuration UI.
2. Select the **PBX configuration** tab.
3. Click **Edit configuration**.
4. Select **VoIP gateway**.



5. **IP address/Server name:** Enter the IP address or the hostname for the VoIP gateway.
6. **Port:** Enter the port for the VoIP Gateway.
7. Click **Save**.
8. Click **Restart telephony server** to restart ‘s Integrated PBX service and make the changes effective.

Integration with VoIP PBX

1. Launch the Telephony Configuration UI.
2. Select the **PBX configuration** tab.
3. Click **Edit configuration**.
4. Select **IP**.



5. **IP address/Server name:** Enter the IP address or the hostname for the external VoIP-based PBX.
6. **Caller name for outgoing calls**: Enter the caller name for outgoing calls.
7. **Caller number for outgoing calls**: Enter the caller number for outgoing calls.
8. **Port:** Enter the port for the external VoIP-based PBX.
   NOTE: In external VoIP-based PBX configuration, provide Notification's VoIP Switch port number as 5080.
9. If the VoIP Switch requires credentials for accessing, check **Registration** and enter the user name and password to be used.
10. Click **Save**.
11. Click **Restart telephony server** to restart ‘s Integrated PBX service and make the changes effective.

Configuring Leading Number for Dial-Out

In some organizations, a leading number needs to be dialed for outgoing calls, such as **9** or **#4**. Enter this number in the **Leading number for outgoing calls** field. This is needed when needs to dial-out to landlines, mobile phones or extensions on the customer’s PBX to deliver messages.

Availability of Lines on Customer PBX for Notification

Depending on the customer’s needs and expected traffic to/from the system through the customer’s PBX, certain lines on the PBX need to be dedicated to dial-in, hotline and dial-out features. If a customer will be using all three features, each feature requires its own extension. A minimum of three extensions would be

required If all the 3 features need to be enabled. Few of these dedicated lines can be used for accessing the hotline feature and even less can be used for the dial-in feature. The remaining lines can be used for dialing out.

The number of simultaneous calls that can be made with the system depends on the hardware used for the PBX integration and the lines dedicated to the system. Once lines are dedicated to the system, the mapping of these lines to the extensions on the system is required.

NOTE:

supports the creation of 100 extensions each for hotline and dial-in features. These are four digit extensions and range from 5000 through 5099 for hotline and 6000 through 6099 for dial-in.

Availability of Lines on Customer PBX for Notification

Depending on the customer's needs and expected traffic to/from the system through the customer's PBX, certain lines on the PBX need to be dedicated to hotline features. If a customer will be using all three features, each feature requires its own extension. A minimum of three extensions would be required If all the 3 features need to be enabled. Few of these dedicated lines can be used for accessing the hotline feature.

The number of simultaneous calls that can be made with the system depends on the hardware used for the PBX integration and the lines dedicated to the system. Once lines are dedicated to the system, the mapping of these lines to the extensions on the system is required.

NOTE:

supports the creation of 100 extensions each for hotline feature. These are four digit extensions and range from 5000 through 5099 for hotline.

Mapping PBX Lines into Notification

Before creating and mapping PBX numbers, review the following example that details how the extensions and numbers of the customer's PBX are mapped with 's Integrated PBX on the server.

- The site has dedicated 10 lines for the system.
- These 10 lines have extensions 2000 through 2009 on the customer's PBX.
- The Direct Inward Dialing (DID) numbers or the landline numbers for these extensions are 1112222000 through 1112222009.
- The user wants to map extensions 2000 through 2003 for dial-in and 2004 through 2007 for hotline. Extensions 2008 and 2009 are left open.

The following table details the mapping of the different numbers.

FreeSWITCH Extension	PBX Extension	DID Number
5000	2000	1112222000
5001	2001	1112222001
5002	2002	1112222002
5003	2003	1112222003
6000	2004	1112222004
6001	2005	1112222005
6002	2006	1112222006
6003	2007	1112222007

Mapping PBX Lines into Notification

Before creating and mapping PBX numbers, review the following example that details how the extensions and numbers of the customer's PBX are mapped with 's Integrated PBX on the server.

- The site has dedicated 10 lines for the system.
- These 10 lines have extensions 2000 through 2009 on the customer's PBX.
- The Direct Inward Dialing (DID) numbers or the landline numbers for these extensions are 1112222000 through 1112222009.
- The user wants to map extensions 2004 through 2007 for hotline. Extensions 2008 and 2009 are left open.

The following table details the mapping of the different numbers.

FreeSWITCH Extension	PBX Extension	DID Number
5000	2000	1112222000
5001	2001	1112222001
5002	2002	1112222002
5003	2003	1112222003
6000	2004	1112222004
6001	2005	1112222005
6002	2006	1112222006
6003	2007	1112222007

Mapping Hotline and Dial-in Numbers to PBX

PBX Mapping while Creating Extension

1. For PBX integration, select the **Map Extension** check box.
2. Enter the **PBX Extension No.** and the external or DID number for that extension.
3. Click **Add** and proceed with further steps to complete the **Add** extension process as detailed in Dial-in Extension.

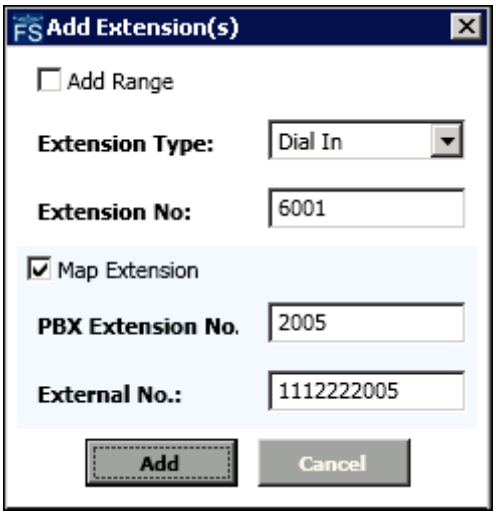
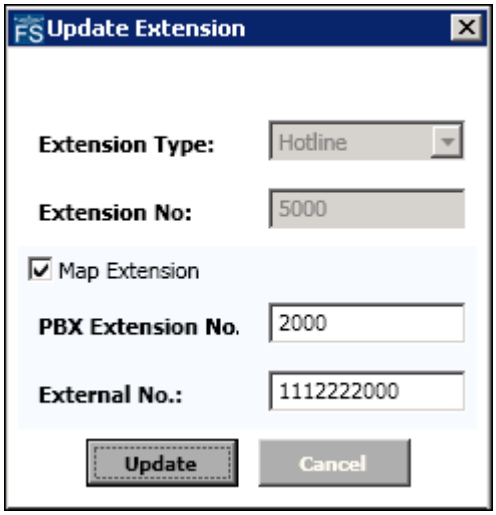


Fig. 54: Add Extensions - Dial In

Updating PBX Mapping for Extension

1. Double click on a dial in or hotline extension to bring up the **Update Extension** dialog.



2. For PBX integration, select **Map Extension** check box.
3. Enter the **PBX Extension No.** and the external or DID number for that extension.
4. Click **Update**.
5. Click **Restart telephony server** so that the updated configurations are loaded.

Voice Prompts for New Recipient Languages

By default, the system is deployed only with voice prompts in English language for the Hotline and Dial-In features. On systems that support additional recipient languages other than English, it is possible to configure Hotline and Dial-In features to support these additional recipient languages. If configured, the system provides the following, additional capabilities:

- Callers are greeted with a language selection prompt, like **Press One for English, Drücken Sie Zwei für Deutsch** and choose their preferred language using the phone's keypad.
- Hotline messages are played in the selected recipient language.
- All menu prompts of the Dial-In feature are played in the selected language.

If you would to configure your Hotline and Dial-In features with additional recipient languages, please contact your support team to perform this enhancement.

Voice Prompts for New Recipient Languages

By default, the system is deployed only with voice prompts in English language for the Hotline feature. On systems that support additional recipient languages other than English, it is possible to configure Hotline feature to support these additional recipient languages. If configured, the system provides the following, additional capabilities:

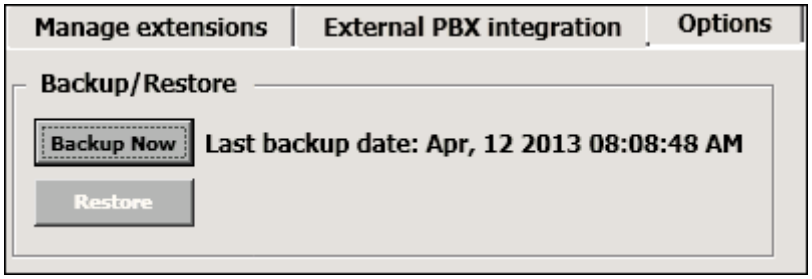
- Callers are greeted with a language selection prompt, like **Press One for English, Drücken Sie Zwei für Deutsch** and choose their preferred language using the phone's keypad.
- Hotline messages are played in the selected recipient language.

If you would to configure your Hotline feature with additional recipient languages, please contact your support team to perform this enhancement.

Backup and Restore of Telephony Configuration

Whenever user performs backup operation for a management station project, a similar operation needs to be performed to backup the telephony configurations. The backup options for the telephony configuration are available in the **Options** tab of the **TelephonyConfigurationTool**.

NOTE:
Backup-and Restore operation of telephony configurations is not integrated with the management station backup-restore functionality. Hence, both the operations need to be performed separately.

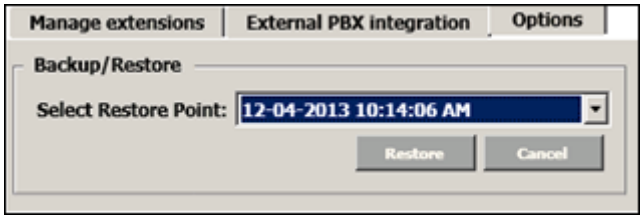


Backup Telephony Configuration

1. Click on **Backup Now**.
2. Backup operation is executed and the configurations are stored in a zip file under the folder **C:\ProgramData\[company name]\Notification Telephony Backup**. The file will be named with the current date and time.
   NOTE: If the backup taken needs to be restored on another freeswitch server system, then copy the backup file and place in the folder **C:\ProgramData\[company name]\\Notification Telephony Backup** on the target system.

Restore Telephony Configuration

1. Start the **Telephony Configuration Utility**.
2. Click **Restore**.



3. A drop-down list with the list of available restore points displays. Choose the appropriate restore point.

NOTE: The restore points gets populated with backup zip files at the following locations:
a. C:\ProgramData\[company name]\Notification Telephony Backup

b [System installation location]\GMSProjects\Notification Telephony Backup

In case of versions upto 2.1.57.900, FreeSwitch backup file used to go in location **b**. From version 2.1.57.960, FreeSwitch backup file goes to location **a**.

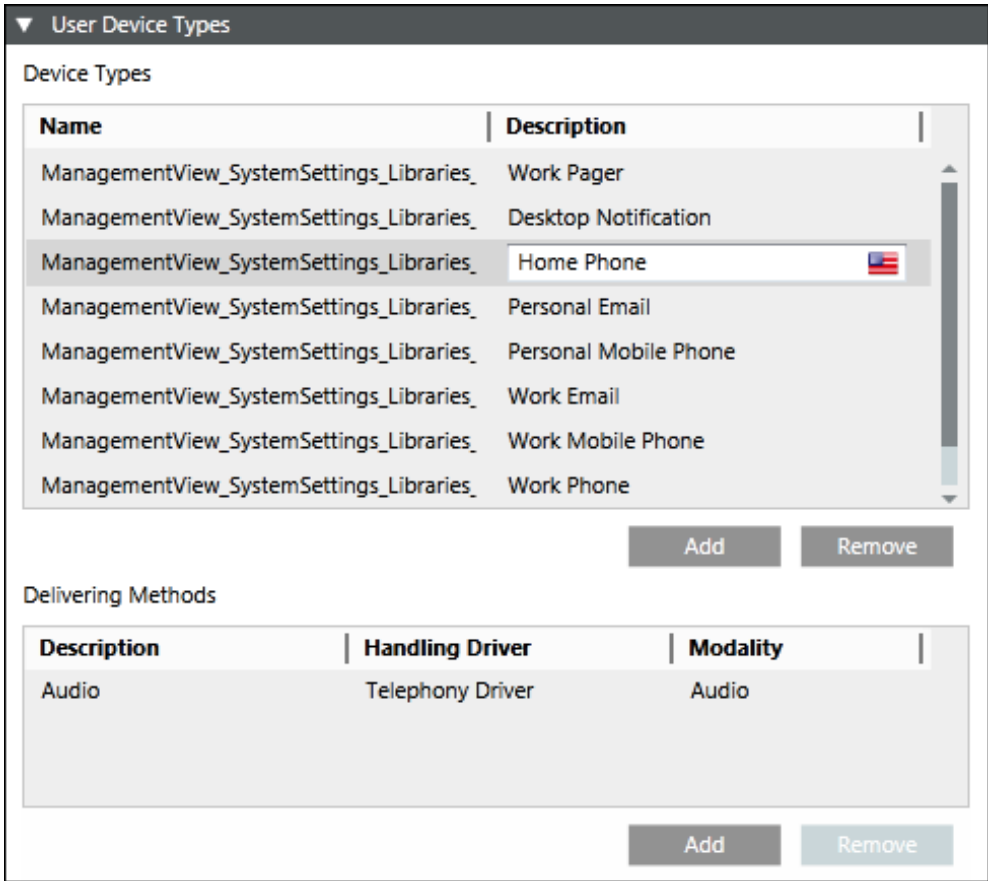
Telephony Configuration System Verification

To verify the added driver and device, perform the steps mentioned in the following sections.

Configuring User Device Types of Telephony Configuration

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

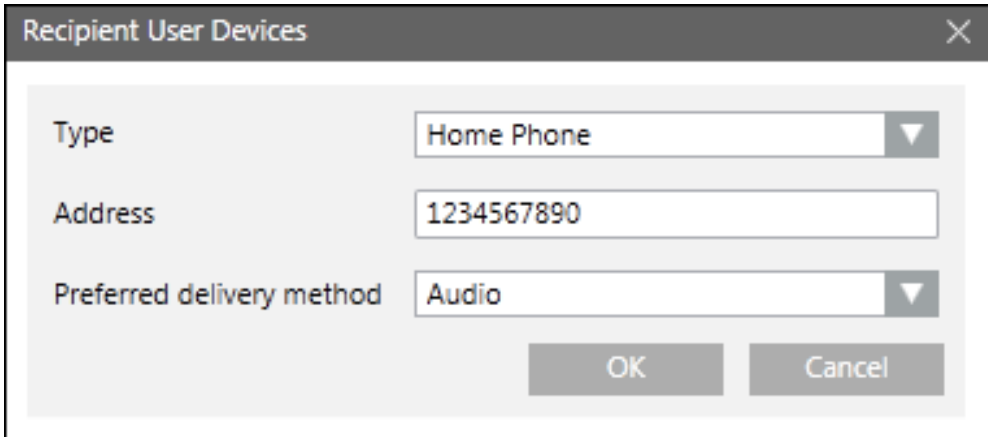
1. In System Browser, select **Application View**.
2. Select **Applications** > **Notification** > **Recipients**.
   ⇨ The **Recipients Editor** tab displays.
3. Click the **User Device Types** expander.
   ⇨ The list of default User Device Types displays under **Device Types**.
4. Select **Description**, select **Home Phone** or **Work Phone**.



   ⇨ The list of delivery methods associated with Home Phone or Work Phone displays under **Delivering Methods**.
   NOTE: If the user selects Home Phone, the delivery methods associated with Home Phone are displayed. If the user selects Work Phone, the delivery methods associated with Work Phone are displayed.
5. Edit the **Description** field.
6. In the **Handling Driver** drop-down list, select **Telephony Driver**.
7. In the **Modality** drop-down list, select **Audio**.
8. Click **Save** .

Configuring Recipient User Devices of Telephony Configuration

1. Add one or more users as recipients into that use home phone or work phone as a recipient device.
2. Select the **Recipient User Devices** expander.
3. Select **Home Phone** or **Work Phone** in the **Type** drop-down list for these recipient users.
4. Enter the phone number in the **Address** field. The **Preferred delivery method** field is automatically populated with Audio.



5. Set up Message and Incident Templates with these users as Recipients.
6. Once the incident is initiated, Recipients in the Message Template should receive a phone call with the content (text content converted into speech) as described in the corresponding Message Template.

Refer to the steps outlined in the following topics of the *Notification Engineering section*:

- Creating a Recipient User
- Creating an Incident Template

In addition to the above topics, refer to the following topic of the *Notification User section*:

- Initiating Incidents - Operating

1.34 Troubleshooting RENO migration

Troubleshooting RENO Migration

Once the device is created in the **Device Editor** tab, the corresponding device gets in **Connected** state based on the Check Status Rate configured in the Configuration Properties of the driver. If the device does not get connected after the Check Status Rate duration, then perform 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.

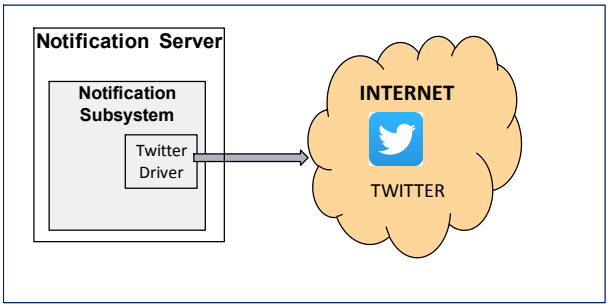
4. Disconnect the power cable of the Perle IOLAN device, wait for a few seconds and then reconnect the power cable.
5. Power off and on the devices connected to the Perle IOLAN device.

1.35 Twitter Account Device

Twitter Device

This section provides reference and background information for integrating the Twitter device. For procedures and workflows, see the step-by-step section.

has the capability to post messages on Twitter. Messages are posted on Twitter when incidents are initiated targeting a Twitter account. These messages are referred to as tweets in Twitter.



Other Twitter users who follow that Twitter account will then be able to read these tweets posted by . In the case of message delivery failure by Twitter due to network interruption, the system makes three attempts to successfully deliver a message to a Twitter account. If cannot successfully deliver a message to Twitter after three attempts, the message will be marked as failed in the user interface.

NOTE 1:
Twitter is a micro-blogging site and posts made on Twitter are termed as tweets.
NOTE 2:
Twitter only supports messages up to 140 characters. Any message that exceeds 140 characters will be truncated.

Prerequisites

A Twitter account needs to be created in order to receive *tweets* from . This should be followed by registering with that account so that can post *tweets* using the registered account.

Twitter Account Device Workspace

- **User Name**: Enter the user name of the Twitter account.
- **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 performs 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.

- **Access Token**: Value given at the Twitter Application Page. Refer to the Configuring Application Settings section.
- **Access Token Secret**: Value given at the Twitter Application Page. Refer to the Configuring Application Settings section.
- **Consumer Key**: Value given at the Twitter Application Page. Refer to the Configuring Application Settings section.
- **Consumer Secret**: Value given at the Twitter Application Page. Refer to the Configuring Application Settings section.
  NOTE: The Consumer Secret is stored in encrypted format for security reasons.

Twitter Account Device

This section provides the steps linked with the configuration and verification of the Twitter Account Device

Twitter Account Creation

Follow the steps below to create a new Twitter account.
NOTE: If a Twitter account already exists, go directly to the Notification Application Registration section.

▷ This document is tested with Twitter API Version **1.1** and OAuth Version **1.0a**.

1. Select the Twitter home page at https://twitter.com/
2. Click **Sign up for Twitter**.
3. Enter the necessary details in the form presented.
4. Before proceeding, post one or more *tweets* through the Twitter website interface of the account just created.
   NOTE: This is an optional step to ensure successful creation of the account and the account's usability.

NOTE 1:
Please go through Twitter's Terms of Use and follow the rules set forth by Twitter. The rules are still valid even when making posts through to the Twitter account.
NOTE 2:
If all Internet traffic is to be routed through an authenticating proxy, then the Twitter Driver needs to be deployed only on the main Server and not on the Front End Processor (FEP) since there can be authentication problems when those drivers attempt to access the Internet. Refer to the Installation Manual for more information on the Server and FEP.

Follow the steps below to create a new Twitter account.
NOTE: If a Twitter account already exists, go directly to the Notification Application Registration section.

▷ This document is tested with Twitter API Version **1.1** and OAuth Version **1.0a**.

1. Select the Twitter home page at https://twitter.com/
2. Click **Sign up for Twitter**.

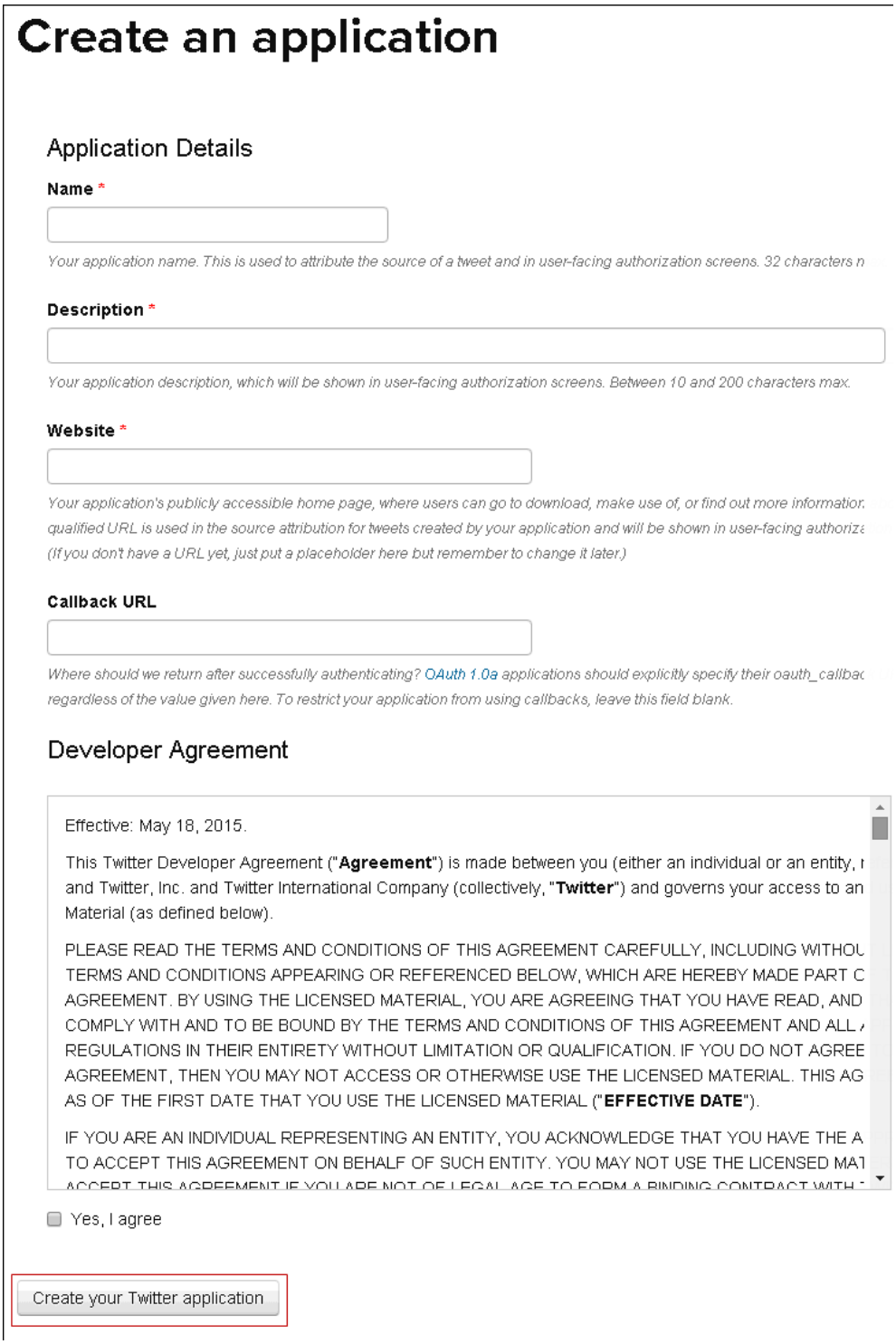
3. Enter the necessary details in the form presented.
4. Before proceeding, post one or more *tweets* through the Twitter website interface of the account just created.
   NOTE: This is an optional step to ensure successful creation of the account and the account's usability.

NOTE 1:
Please go through Twitter's Terms of Use and follow the rules set forth by Twitter. The rules are still valid even when making posts through to the Twitter account.
NOTE 2:
If all Internet traffic is to be routed through an authenticating proxy, then the Twitter Driver needs to be deployed only on the main Server and not on the Front End Processor (FEP) since there can be authentication problems when those drivers attempt to access the Internet.

Notification Application Registration

Follow the steps below to register with the Twitter account just created:

1. Select the Twitter Device home page at http://dev.twitter.com/apps/new. Log in with the credentials to the twitter account created earlier when prompted.



2. Enter a **Name**.
3. Enter a **Description** for the application.
4. In the **Website** field, enter a placeholder website URL if the URL is not known or unavailable.
   NOTE: This is necessary only when tweeting capability needs to be built into websites. For , any URL would work.
5. Leave the **Callback URL** field blank since will not post *tweets* from a website.

6. Select the **Yes, I agree** check box.
7. Click **Create your Twitter application**.

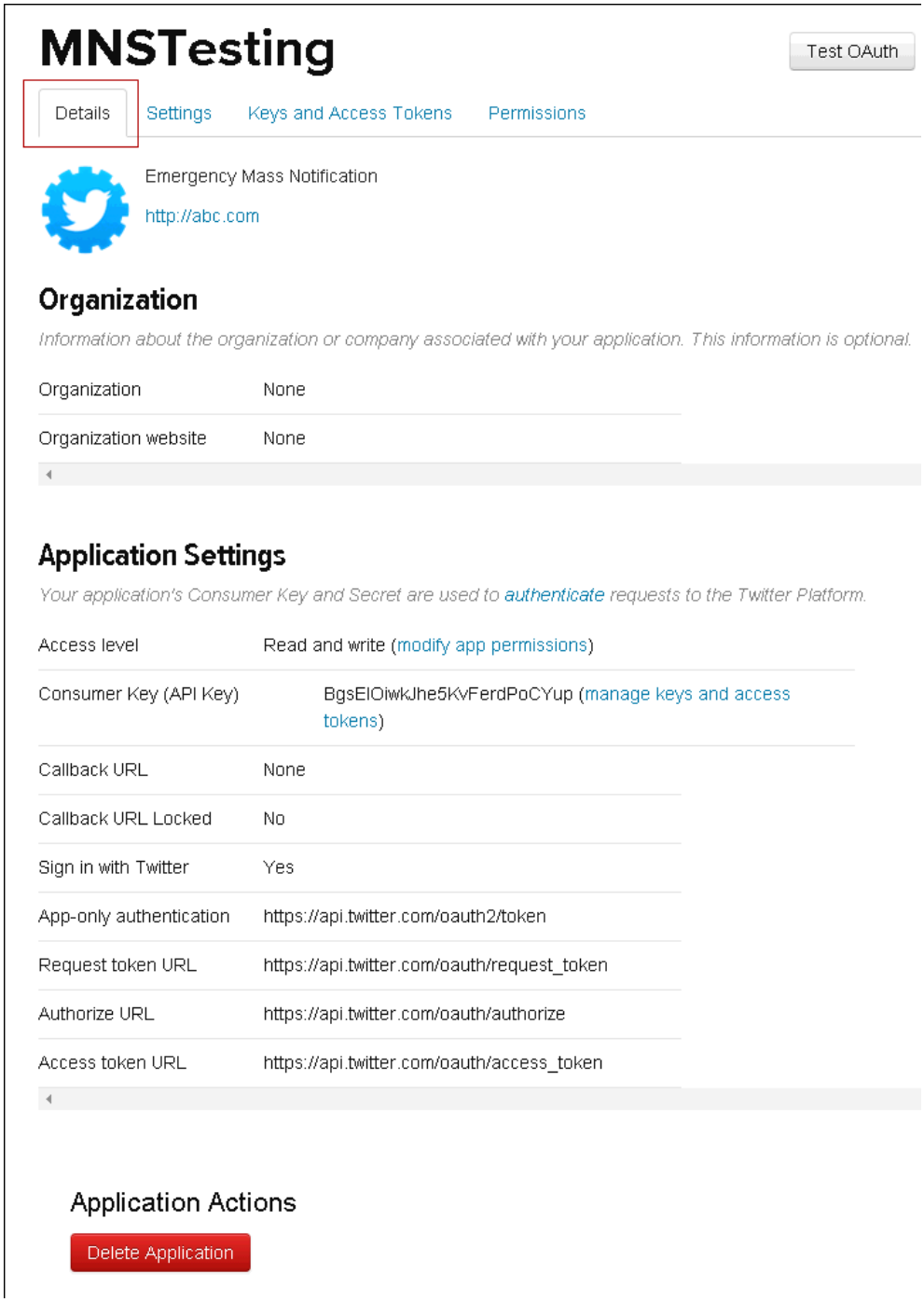
⇨ The Twitter application is now created.

Navigating to Application Page for Pre-existing Application

▷ If the Twitter application is already available with the Twitter account, follow the steps below to select the application page:

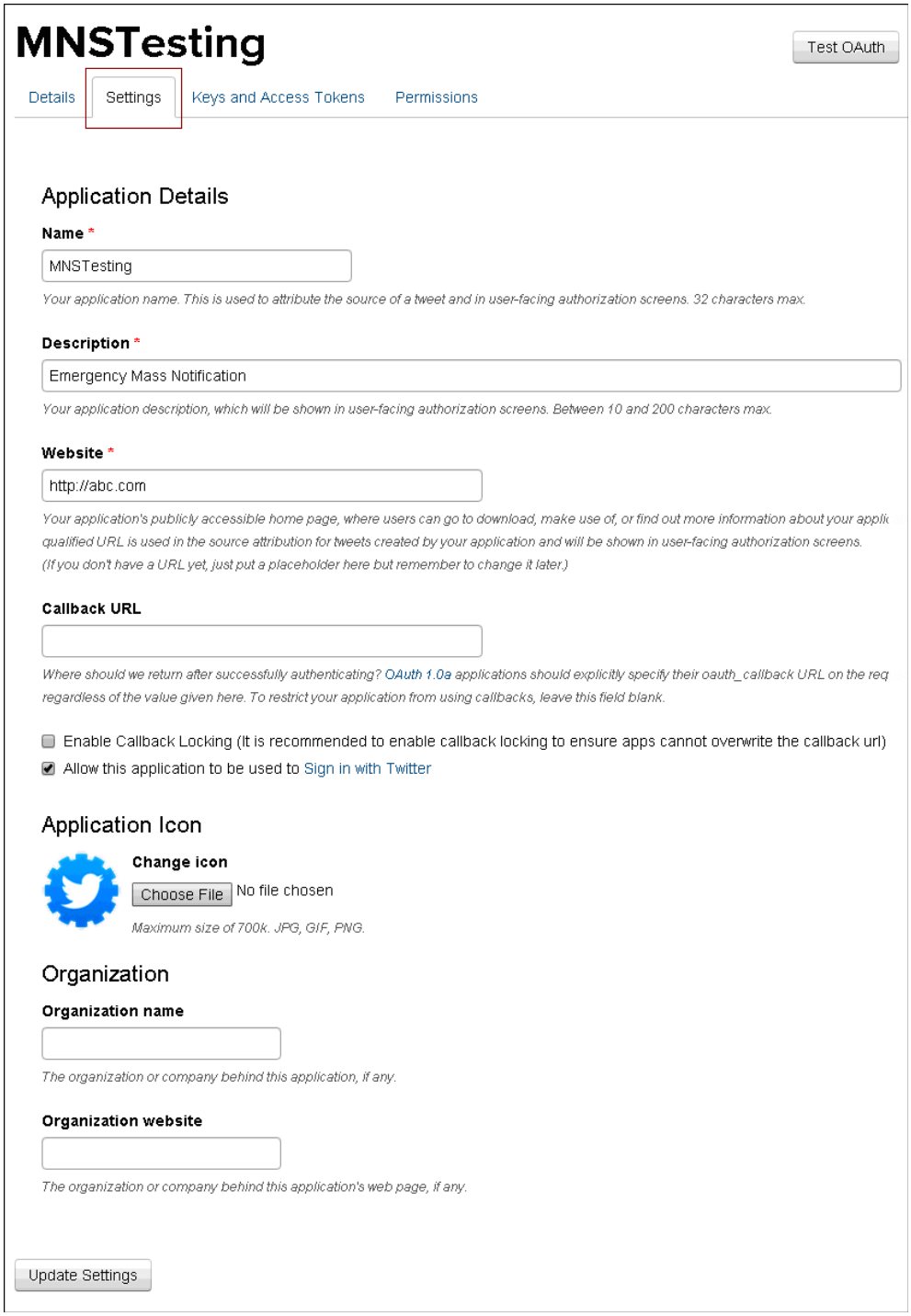
1. Select http://dev.twitter.com and log in using the credentials for that Twitter account.
2. Click **Application Management**.

3. Twitter applications created with that account are displayed. Click the appropriate Twitter application to select the application page as displayed below:

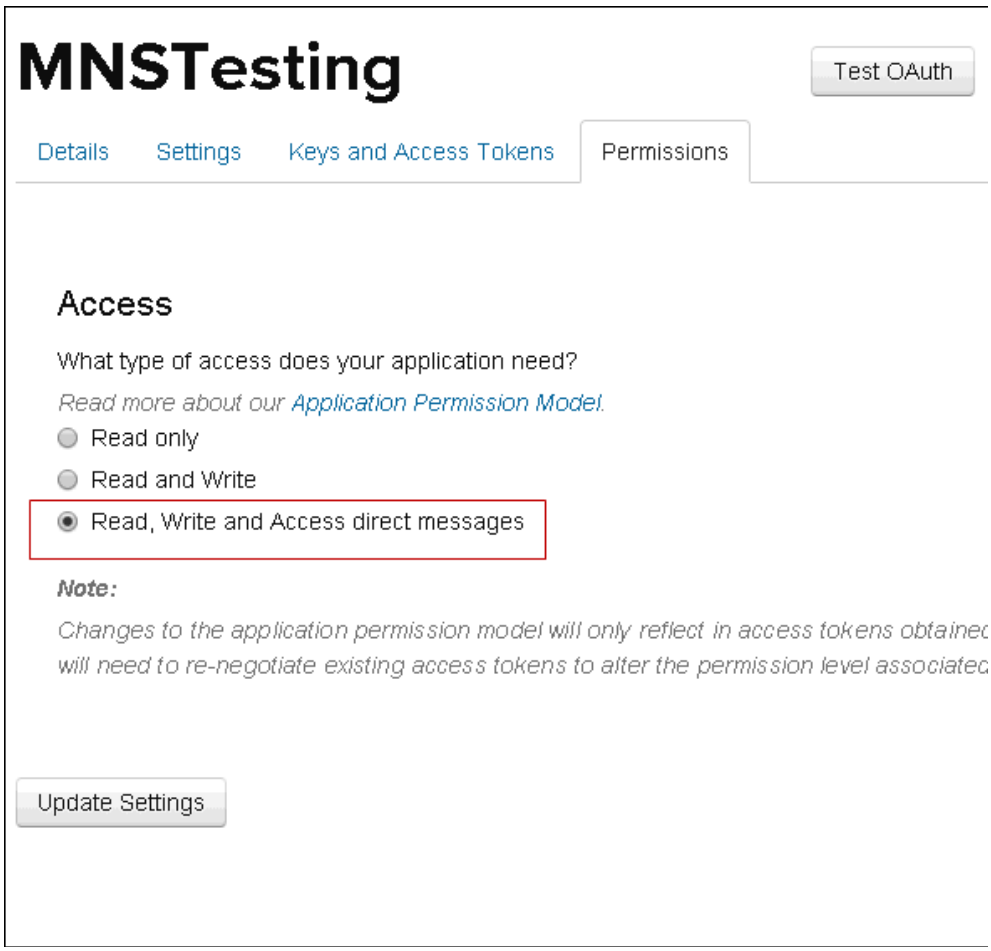


Configuring Application Settings

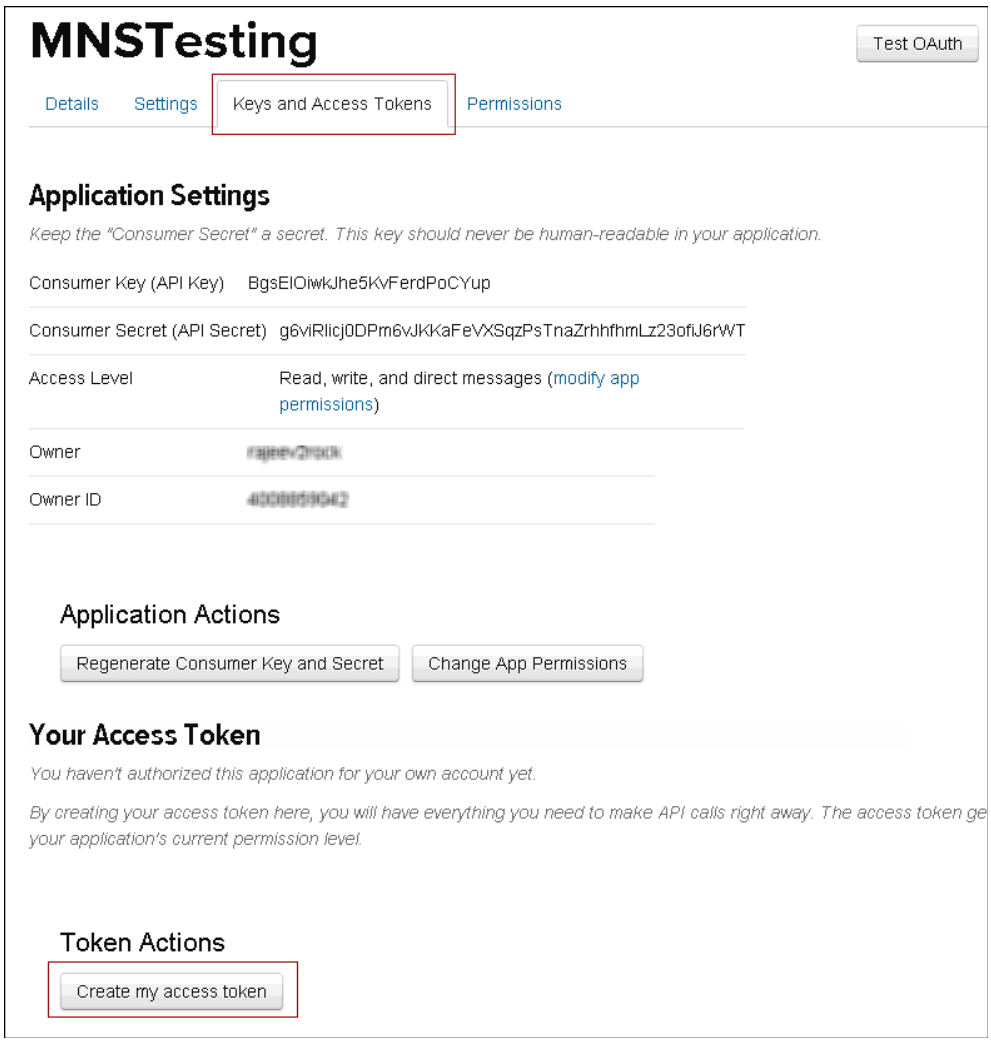
1. Click on the **Settings** tab.
   ⇨ The **Settings** page displays.



2. Set values for the different fields as indicated in the following steps:
   - **Name**: Enter a name for the application.
   - **Description**: Enter a description for the application.
   - **Website**: Enter the URL for the application's website if one exists. If not, enter a placeholder URL. See the notes on the Twitter page under the **Website** field for details on this field and its implications.
   - **Callback URL**: Enter a placeholder URL. See the note on the Twitter page under the **Callback URL** field for details on this field and its implications.
   - Select **Allow this application to be used to Sign in with Twitter**.
3. Enter organization details.
4. Click **Update Settings**.
5. Select the **Permissions** tab.

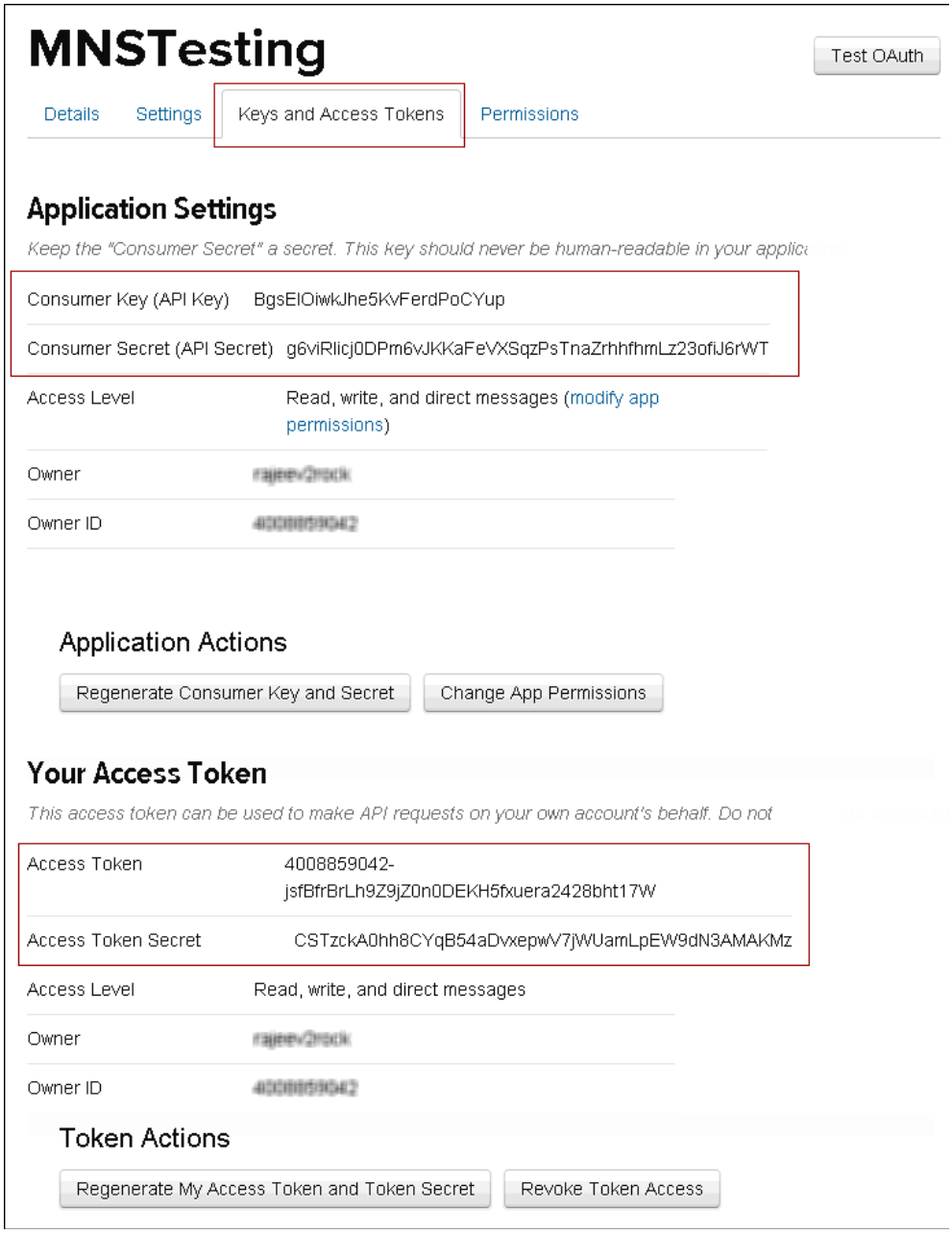


6. Change the access type to **Read, Write and Access direct messages**.
7. Click **Update Settings**.
8. Select the **Keys and Access Tokens** tab.
9. Click **Create my access token**.



10. Verify that value of **Access Level** under **Application Settings** is set to **Read, write, and direct messages**. If it is different, select the **Permissions** tab..
11. Verify that the value of **Access Level** under **Your Access Token** is set to **Read, write, and direct messages**. If it is set to Read-only, then click on **Recreate My Access Token and Token Secret** to create the tokens again.

    ⇨ Twitter application configurations are changed and required access keys and tokens are available.



12. Write down the values for the following properties as depicted in the image above and listed below. These values will need to be entered in the system while the Twitter Account device is being engineered into the system.
    - **Consumer Key (API Key)**
    - **Consumer Secret (API Secret)**
    - **Access Token**
    - **Access Token Secret**

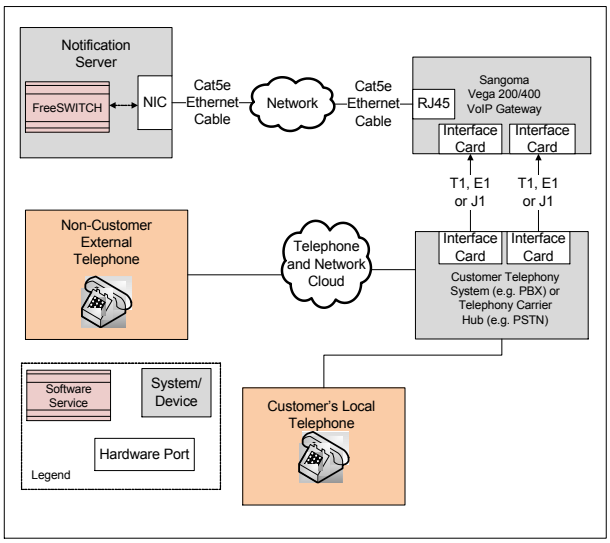
NOTE:
The above values need to be available only to those who are authorized and have engineering access to the system.

1.36 VoIP Switch Configuration

VoIP Switch Configuration

This section provides reference and background information for integrating the VoIP Switch. For procedures and workflows, see step-by-step section.

The Sangoma Vega Series VoIP Gateway provides the capability for the management station to interface to traditional external telephony systems. Using the VoIP Gateway, can expand beyond local area networked IP phones to include a customer's existing telephone system where analog or IP phones can be used to initiate incidents or receive notifications from .



The VoIP Gateway interfaces to the external PBX using a standard T1/E1 port. The server communicates with the VoIP Gateway through the SIP protocol over TCP/IP over a standard Ethernet-based network.

Unlike a telephony card, which is physically installed on the same workstation as , the VoIP Gateway can be separate from the system server with close proximity to the external PBX, all while providing the same functionality as the telephony card. Communication with the system server uses standard network topology via Ethernet. In addition, the use of the VoIP gateway is the default solution for redundant server deployments.

Prerequisites

Before proceeding, make sure that you have the following items in your possession:

- 1 - Sangoma Vega 400 or Vega 200 VoIP Gateway
- 2 – T1 cables (bundled with gateway)
- 1 – Cat5e Ethernet cable (bundled with gateway)
- 1 – Vega DSP expansion card, model VS0083 (bundled with gateway)
- 1 – Power line cord (bundled with gateway)
- 48-channel upgrade key (ordered through Sangoma; key is tied to the specific serial number of a gateway)

VoIP Switch Configuration

This section provides additional procedures for integrating the VoIP Switch Configuration.

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

Prerequisites

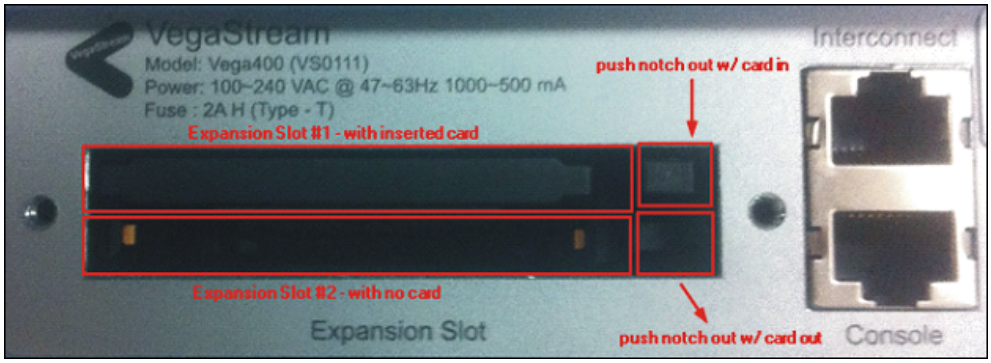
Before proceeding, make sure that you have the following items in your possession:

- 1 - Sangoma Vega 400 or Vega 200 VoIP Gateway
- 2 – T1 cables (bundled with gateway)
- 1 – Cat5e Ethernet cable (bundled with gateway)
- 1 – Vega DSP expansion card, model VS0083 (bundled with gateway)
- 1 – Power line cord (bundled with gateway)
- 48-channel upgrade key (ordered through Sangoma; key is tied to the specific serial number of a gateway)

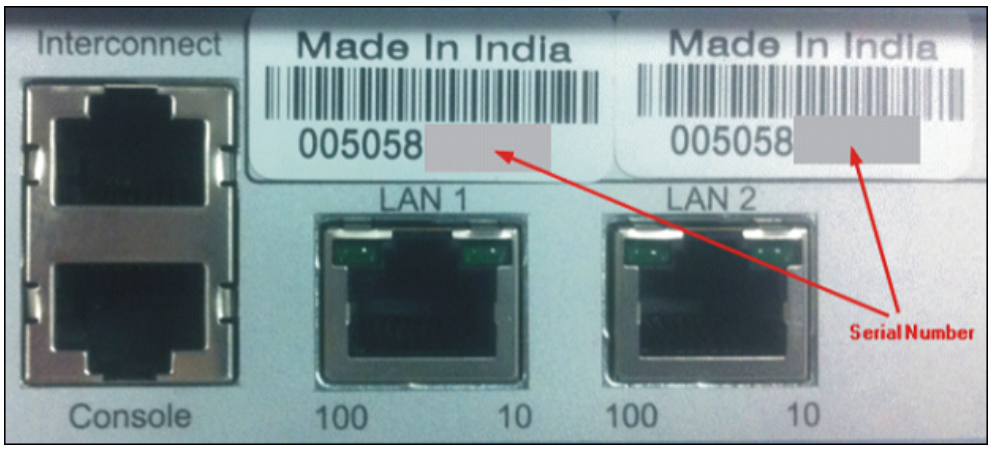
Mechanical Installation

1. Remove the protective plate from the expansion card slot.
   NOTE: There will be two slots where the cards can be placed.

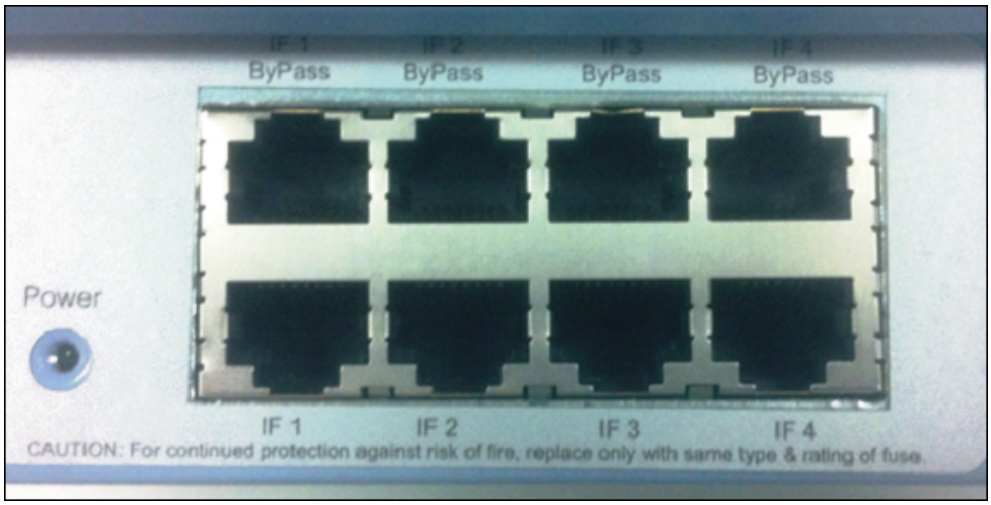
2. Insert the DSP card into the top slot (label face down).
   NOTE: Make sure to push the card all the way into the slot until the push notch comes all the way out.



3. Connect one end of the Ethernet cable to the port on the gateway marked **LAN 1**.
4. Connect the other cable end to the local switch/hub/router.



5. Connect one end of each T1 cable to the port on the gateway marked **IF 1** and **IF 2**. If one of the ends of the T1 cable is marked **GATEWAY END**, use that end to connect to the gateway.
6. Connect the other end of the T1 cable to the client's local PBX.



7. Connect the power line cord to the gateway and insert into a power outlet.
8. Flip the power switch (next to the power connector) to turn on the device.

⇨ The power LED (next to the T1 ports) should turn on and the lights on the front of the gateway should begin to flash. Wait approximately 60-90 seconds for the device to boot up and obtain an IP address. The device is automatically configured for DHCP.

Configuring IP Address

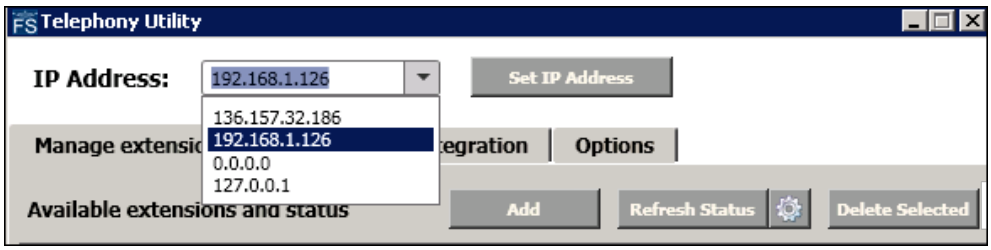
The device is automatically set for DHCP and is only configurable through a web interface. To determine the IP address, work with the site IT admin to determine the leased IP address based on the MAC address of the VoIP gateway. Alternatively, the IT admin can reserve an IP address based on the device's MAC address prior to installation.
NOTE: If there is no DHCP server on the LAN, the Vega's IP address will default to **136.254.x.y**, where **x** and **y** are the decimal versions of the last two bytes of the LAN interface MAC address.

Set IP Address for Notification's VoIP Switch

▷ On servers which contain more than 1 Network Interface Card (NIC), the IP address to be used by 's VoIP Switch needs to be set explicitly. This would be the IP address of the network to which IP phones and other devices which need to connect to 's VoIP Switch are connected.
NOTE: Some of the devices, such as the line-level audio devices, need to be set with the IP address of the 's VoIP Switch server instead of the hostname. As a result, it is required that a static IP address be used for the server or that the IP address be reserved.

1. Select the IP address from the IP address drop-down list. In case the server has multiple network cards, multiple IP addresses are listed.
NOTE: Typically all devices including audio devices and IP phones are connected to the same network. Select the IP address that belongs to this network so that devices that need to connect with 's VoIP Switch on the server are able to do so.

   ⇨ The appropriate IP address is shown in the image below.



2. Enter the IP address from the previous step into the **IP Address** field.
3. Click **Set IP Address**.

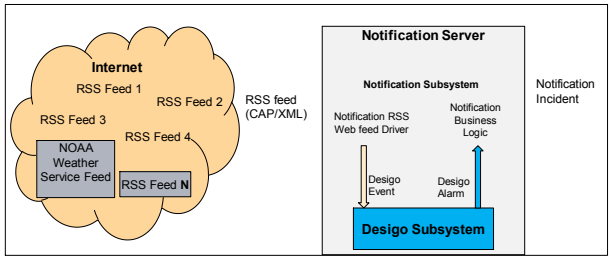
⇨ The required configuration files are updated. The Server is now a SIP server and registrar on that IP address.
NOTE: The 's VoIP Switch service needs to be restarted for the changes to be effective. This can be done immediately by pressing the **Restart telephony server** button or can be done once all configuration steps are completed.

1.37 Web Feed Input Device

RSS CAP

This section contains general reference information about Notification and how the RSS CAP device is integrated. For procedures and workflows, see step-by-step section.

has the capability to read and monitor RSS feeds. When an RSS feed is added to as a device, expressions and search patterns can be configured to analyze the incoming feeds, raise alarms, and initiate incidents automatically.



A typical use case would be to configure the system with a feed from the National Oceanic and Atmospheric Administration's (NOAA) weather service or the Homeland Security URL for a particular region, and then configure the system to take action when certain messages are received through the configured RSS feeds.

Listed below is a typical workflow that occurs in the background for this device.

- The user configures a feed into the system by entering a URL for the RSS feed.
- monitors the configured feed so that an action can be taken when new items are published.
- The Web Feed Input Driver analyzes the feed item against the message filter rules and raises the management station alarms if the filter rules are satisfied.
- The management station alarms raised show up in the system user interface and you can then take the necessary action.
- Configuring incident triggers is possible within Incident Templates so that incidents are initiated automatically when alarms occur in the system.
  NOTE 1:
  Really Simple Syndication (RSS) is used to publish frequently updated content like weather services, blog entries, videos, and so forth. The user can access a wide variety of applications (Web based applications, desktop applications or mobile device applications) to access the RSS feeds.
  NOTE 2:
  If all Internet traffic is to be routed through an authenticating proxy, then the Web Feed Input driver needs to be deployed only on the main server and not on the Front End Processor (FEP). If the Web Feed Input driver is deployed on the FEP, authentication problems can occur when those drivers attempt to access the Internet.

Prerequisite

The user of this document is required to be familiar with the following:

- RSS feeds
- XML
- HTML

References

- http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.html for the Common Alerting Protocol specifications.

Filters and Triggers for CAP/HTML/XML Feeds

RSS CAP is an input device which is capable of receiving inputs through RSS feeds. Before configuring event triggers, configure the system by adding one or more RSS feeds as detailed in 3 - Create Web Feed Input Field Network.

NOTE:
The event triggers can be configured both at the driver level and also when configuring the Web Feed Input device under the Field Network. In either case, rules are set to analyze different parts of the feed item.

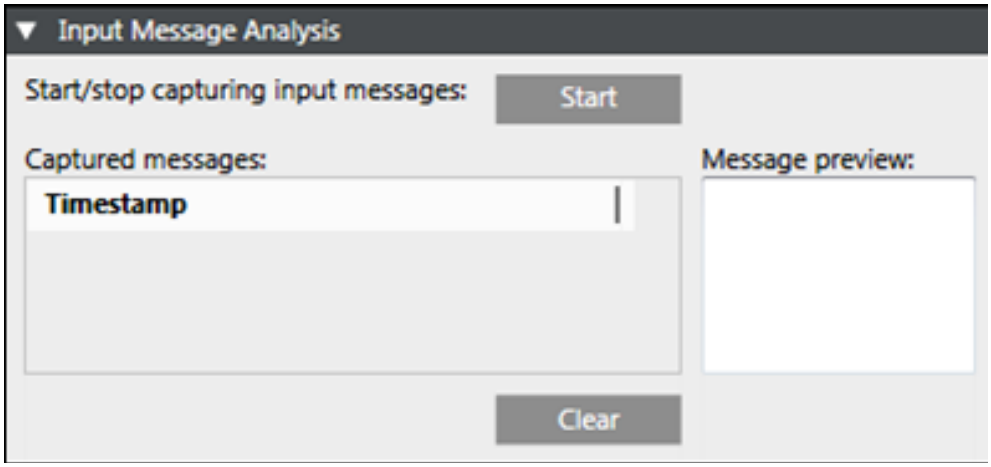
This section details how to configure message filters and trigger settings in the user interface so that the management station alarms can be raised. These management station alarms can then be used to trigger incidents thus achieving the goal of raising incidents based on data received from the RSS CAP feeds.

Refer to the --- MISSING LINK --- for some examples on real use-cases to gain some understanding on how to fill the different fields.

The event trigger rules for an input device are configured in, Input Message Analysis and Event Triggers.

Input Message Analysis: Input Message Analysis is used to analyze the data received by a device, separated into individual messages. This analysis is especially useful for reverse engineering if the input devices do not have a formally documented output. Input devices can be put into a message capturing mode where every received message displays for analysis. For each captured message, the raw textual data can be viewed.

The Input Message Analysis Workspace displays the content of the messages received from the different configured devices. The messages are displayed based on the timestamp. The received message can be previewed by clicking and selecting a particular timestamp. Note that the message displayed in the Message preview section contains the raw input as received from the feed. This can be used to analyze the input message and set the required filter and trigger rules.



- **Start/stop capturing input messages**: Allows for the start and stop of message capturing.
- **Message preview**: Displays the preview of the captured message.
- **Timestamp**: Displays the timestamp of the captured input message, or in absence of a timestamp, the time the input message was received.
- **Clear**: Deletes all captured input messages.

Event Triggers

An Event Trigger contains a number of Filter Rules and Event Field Mappings.

Filter Rules limit the input data that triggers the alarms. Filter Rules work on text data and optionally on XML data. During the filtering stage, for each Filter Rule, the device first applies an optional Xpath expression and then a mandatory regular expression.

Regular expressions are used for matching text to find characters, words, and patterns of characters in text. For XML input data, optional Xpath expressions are used to select sections (XML nodes) within XML documents and narrow down the text that needs to be searched with regular expressions.

Filter Rules can be negated, meaning that certain text patterns must not be present in input data for the Event Trigger to trigger an event.

Event field mappings are used to configure how event fields, such as the Event Category, shall be filled: Either with a default value, or with text extracted from the triggering event.

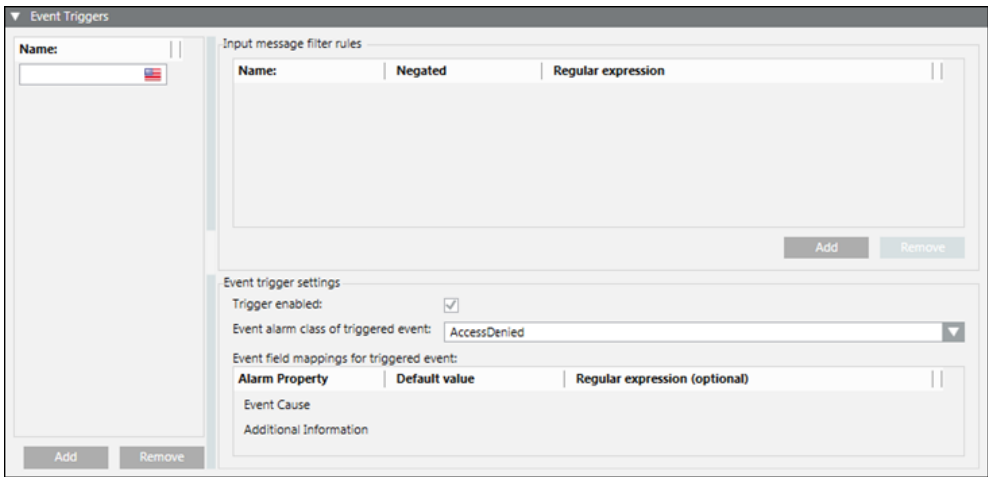
The three event fields that can be controlled are:

- Event category of triggered event
- Event Cause
- Additional Information

The triggered events can be classified into predefined event categories. For more information on events, refer to the *Alarm Management* section.

For Event Cause and Additional Information, either specify a static Default Value (mandatory), or extract text from the input data that triggered the event. Text extraction is accomplished using an optional Xpath expression followed by regular expressions (optional).

Event Triggers can individually be enabled or disabled.
NOTE: The explanation of XPath and regular expressions is beyond the scope of this document.



- **Name**: Displays the name of the event trigger configuration.
- **Add**: Adds an event trigger.
- **Remove**: Removes the event trigger.
- **Input message filter rules**:
  - **Name**: Displays the name of the input message filter rule.
  - **Negated**: Allows for negating the matching result of an input message filter rule.
  - **Xpath (optional)**: Displays the Xpath expression to extract specific XML node from input XML. The Xpath is an optional requirement in the Input message filter rules section.
  - **Regular expression**: Displays the regular expression to match a specific type of data from the received input.
  - **Add**: Adds an input message filter rule.
  - **Remove**: Removes the input message filter rule.
- **Event trigger settings**:
  - **Alarm Property**: Displays the event properties that can be dynamically filled in with content from input messages.
  - **Default Value**: Displays the default values that should be used to assign to properties of triggered events if no further content extraction settings (Xpath and Regular expression) are provided.
  - **Trigger enabled**: Select this check box if a rule configuration is required to be used for analyzing and filtering data.
  - **Xpath (optional)**: Displays the optional Xpaths expressions that are applied to XML-based input messages to extract information and assign it to the properties of triggered events.
    NOTE: Configuration of an XPath must not be done if the Web Feed item is in HTML format. This will not result in the alarms and automatic incident triggering.
  - **Event alarm class of triggered event**: Displays the event category for the triggered event.
  - **Regular expression (optional)**: Displays the optional Regular expressions that are applied to textual input messages. The Regular expressions are used to extract information and assign it to the properties of triggered events.

NOTE: As a limitation, in the current version of only alarm classes ending in **Ack/ Reset** and **No Reset** must be chosen, or else the operator will not be able to acknowledge and reset the generated events.

Additional Samples

This section displays the CAP feed XML sample, XML and HTML examples.

CAP feed XML Sample

```
<?xml version = '1.0' encoding = 'UTF-8' standalone = 'yes'?>
<?xml-stylesheet href='http://alerts.weather.gov/cap/capatomproduct.xsl'
type='text/xsl'?>

<!--
This atom/xml feed is an index to active advisories, watches and warnings
issued by the National Weather Service.  This index file is not the complete
Common Alerting Protocol (CAP) alert message.  To obtain the complete CAP
alert, please follow the links for each entry in this index.  Also note the
CAP message uses a style sheet to convey the information in a human readable
format.  Please view the source of the CAP message to see the complete data
set.  Not all information in the CAP message is contained in this index of
active alerts.
-->

<alert xmlns = 'urn:oasis:names:tc:emergency:cap:1.1'>

  <!-- http-date = Thu, 07 Mar 2013 02:34:00 GMT -->
  <identifier>NOAA-NWS-ALERTS-
NJ124EF3CCA228.WinterWeatherAdvisory.124EF3CDF470NJ.PHIWSWPHI.5f086e703ef796f4ec8
688b16e3313af</identifier>
  <sender>w-nws.webmaster@noaa.gov</sender>
  <sent>2013-03-06T21:34:00-05:00</sent>
  <status>Actual</status>
  <msgType>Alert</msgType>
  <scope>Public</scope>
  <note>Alert for Coastal Ocean; Northwestern Burlington; Ocean; Southeastern
Burlington (New Jersey) Issued by the National Weather Service</note>
  <info>
    <category>Met</category>
    <event>Winter Weather Advisory</event>
    <urgency>Expected</urgency>
    <severity>Minor</severity>
    <certainty>Likely</certainty>
    <eventCode>
      <valueName>SAME</valueName>
      <value></value>
    </eventCode>
    <effective>2013-03-06T21:34:00-05:00</effective>
    <expires>2013-03-07T06:00:00-05:00</expires>
    <senderName>NWS Philadelphia - Mount Holly (New Jersey, Delaware,
Southeastern Pennsylvania)</senderName>
    <headline>Winter Weather Advisory issued March 06 at 9:34PM EST until March
07 at 6:00AM EST by NWS Philadelphia - Mount Holly</headline>
    <description>
      ...WINTER WEATHER ADVISORY REMAINS IN EFFECT UNTIL 6 AM EST
      THURSDAY...
      * SNOW ACCUMULATION...1 TO 2 INCHES, GREATEST ON UNTREATED
      SURFACES.
      * TIMING...RAIN IS EXPECTED TO MIX WITH THEN CHANGE TO A PERIOD OF
      SNOW OVERNIGHT. TEMPERATURES ARE FORECAST TO BE ABOVE FREEZING
      AND THIS WILL ASSIST WITH MELTING ON TREATED SURFACES.
      * IMPACTS...SLIPPERY CONDITIONS SHOULD DEVELOP OVERNIGHT AS THE
      WET SNOW BEGINS TO ACCUMULATE ON UNTREATED ROAD SURFACES.
      * WINDS...NORTH 20 TO 30 MPH WITH GUSTS UP TO 45 MPH.
      * TEMPERATURES...DROPPING TO THE MID 30S.
    </description>
```

```
    <instruction>
      A WINTER WEATHER ADVISORY MEANS THAT PERIODS OF SNOW COULD CAUSE
      TRAVEL DIFFICULTIES. BE PREPARED FOR SLIPPERY ROADS AND LIMITED
      VISIBILITIES, AND USE CAUTION WHILE DRIVING.
    </instruction>
    <parameter>
      <valueName>WMOHEADER</valueName>
      <value></value>
    </parameter>
    <parameter>
      <valueName>UGC</valueName>
      <value>NJZ019-020-026-027</value>
    </parameter>
    <parameter>
      <valueName>VTEC</valueName>
      <value>/O.CON.KPHI.WW.Y.0014.000000T0000Z-130307T1100Z/</value>
    </parameter>
    <parameter>
      <valueName>TIME...MOT...LOC</valueName>
      <value></value>
    </parameter>
    <area>
      <areaDesc>Coastal Ocean; Northwestern Burlington; Ocean; Southeastern
Burlington</areaDesc>
      <polygon></polygon>
      <geocode>
        <valueName>FIPS6</valueName>
        <value>034005</value>
      </geocode>
      <geocode>
        <valueName>FIPS6</valueName>
        <value>034029</value>
      </geocode>
      <geocode>
        <valueName>UGC</valueName>
        <value>NJZ019</value>
      </geocode>
      <geocode>
        <valueName>UGC</valueName>
        <value>NJZ020</value>
      </geocode>
      <geocode>
        <valueName>UGC</valueName>
        <value>NJZ026</value>
      </geocode>
      <geocode>
        <valueName>UGC</valueName>
        <value>NJZ027</value>
      </geocode>
    </area>
  </info>
</alert>
```

Practical Examples of XML

The XML below is used as a basis for the different solutions detailed in the following sections.

```
<alert xmlns = 'urn:oasis:names:tc:emergency:cap:1.1'>
  <!-- http-date = Mon, 18 Mar 2013 12:41:00 GMT -->
  <identifier>NOAA-NWS-ALERTS-
KY124EF4760444.FlashFloodWarning.3791d05556b7c4ce96aa8c6b4cd6411c</identifier>
  <sender>w-nws.webmaster@noaa.gov</sender>
  <sent>2013-03-18T08:41:00-04:00</sent>
  <status>Actual</status>
  <msgType>Alert</msgType>
  <scope>Public</scope>
  <note>Alert for Lewis; Mason (Kentucky) Issued by the National Weather Service</note>
  <info>
    <category>Met</category>
    <event>Flash Flood Warning</event>
    <urgency>Immediate</urgency>
    <severity>Severe</severity>
    <certainty>Likely</certainty>
    <eventCode>
      <valueName>SAME</valueName>
      <value>FFW</value>
    </eventCode>
    <effective>2013-03-18T08:41:00-04:00</effective>
    <expires>2013-03-18T11:45:00-04:00</expires>
    <senderName>NWS Wilmington (Southwestern Ohio)</senderName>
    <headline>Flash Flood Warning issued March 18 at 8:41AM EDT until March 18 at 11:45AM EDT
by NWS Wilmington</headline>
    <description>
      THE NATIONAL WEATHER SERVICE IN WILMINGTON HAS ISSUED A
      * FLASH FLOOD WARNING FOR...
      LEWIS COUNTY IN NORTHEAST KENTUCKY...
      MASON COUNTY IN NORTHERN KENTUCKY...
      SOUTHERN ADAMS COUNTY IN SOUTHWEST OHIO...
      SCIOTO COUNTY IN SOUTHWEST OHIO...
    </description>
    <instruction>
      ACT QUICKLY TO PROTECT YOUR LIFE IF YOU ARE IN A LOW LYING AREA...
      ALONG A CREEK...STREAM OR IN AN AREA EXPERIENCING FLOODING. MOVE TO
      HIGHER GROUND IMMEDIATELY.
      NEVER DRIVE INTO AREAS WHERE WATER COVERS THE ROAD. ONLY A FEW INCHES
      OF RAPIDLY FLOWING WATER CAN QUICKLY CARRY AWAY YOUR VEHICLE. FIND AN
      ALTERNATE ROUTE OR WAIT UNTIL THE WATER RECEDES.
    </instruction>
    <parameter>
      <valueName>WMOHEADER</valueName>
      <value></value>
    </parameter>
    <parameter>
      <valueName>UGC</valueName>
      <value>KYC135-161-OHC001-145</value>
    </parameter>
    <parameter>
      <valueName>VTEC</valueName>
      <value>
        /O.NEW.KILN.FF.W.0001.130318T1241Z-130318T1545Z/
        /00000.0.ER.000000T0000Z.000000T0000Z.000000T0000Z.OO/
      </value>
    </parameter>
    <parameter>
      <valueName>TIME...MOT...LOC</valueName>
      <value></value>
    </parameter>
    <area>
      <areaDesc>Lewis; Mason</areaDesc>
      <polygon>38.39,-83.41 38.43,-83.58 38.52,-83.64 38.47,-83.81 38.49,-83.89 38.60,-83.99
38.65,-83.95 38.64,-83.71 38.78,-83.68 38.90,-82.76 38.72,-82.69 38.67,-82.76 38.60,-82.74
38.59,-82.75 38.59,-82.85 38.75,-82.88 38.72,-83.02 38.43,-83.23 38.36,-83.23 38.32,-83.33
38.39,-83.41</polygon>
      <geocode>
        <valueName>FIPS6</valueName>
        <value>021135</value>
      </geocode>
      <geocode>
        <valueName>FIPS6</valueName>
        <value>021161</value>
      </geocode>
      <geocode>
        <valueName>UGC</valueName>
        <value>KYC135</value>
      </geocode>
      <geocode>
        <valueName>UGC</valueName>
        <value>KYC161</value>
      </geocode>
    </area>
  </info>
</alert>
```

Example 1

Objective

1. Check if the input feed is set with the Severity of type **Severe**.
2. If yes, then trigger an alarm that contains the following information:

- **Event Cause**: Include the text from the **event** tag.
- **Additional Information**: Include the text from the **headline**.

Solution

Set the following rules for the Input message filter:

Name	Negated	Xpath	Regular Expression
User defined name	Leave deselected	/alert/info/severity/ text()	(?<ValueToExtract>Severe)

Set the following for the Event Trigger Settings:

Alarm Property	Default Value	Xpath	Regular Expression
Event Cause		/alert/info/event/text()	
Additional Information		/alert/info/headline/ text()	

Example 2

Objective – Adding Multiple Trigger Rules

1. Check if the **event** filed contains the text **Warning** .
2. If yes, then trigger an alarm that contains the following information:
   - **Event Cause**: Include the text from the **event** tag.
   - **Additional Information**: Extract the county names from the **description** field.

Solution

Set the following for the Input message filter rules:

Name	Negated	Xpath	Regular Expression
User defined name	Leave deselected	/alert/info/event/text()	(?<ValueToExtract>.*Warning)

Set the following for the Event Trigger Settings:

Alarm Property	Default Value	Xpath	Regular Expression
Event Cause		/alert/info/event/text()	
Additional Information		/alert/info/ description /text()	(?<ValueToExtract>[A-Z].*[A-Z]*.COUNTY)

Practical Example of HTML

The following is an extract from a feed item's HTML source:

<title>Wal-Mart to stop selling AR-15, other semi-automatic rifles| Reuters</title>

<p><span class="articleLocation">Wal-Mart Stores Inc (WMT.N), the United States' top seller of guns and ammunition, said on Wednesday it would stop selling the AR-15 and other semi-automatic rifles because of sluggish demand and focus instead on "hunting and sportsman firearms."</p><p>Wal-Mart said the decision was unrelated to high-profile incidents involving the rifles,

including the killing of 26 students and adults at Sandy Hook Elementary School in Connecticut in 2012. "This is done solely on what customer demand was," said company spokesman Kory Lundberg. "We are instead focusing on hunting and sportsman firearms." Lundberg said Wal-Mart would stop selling a class of rifle called the modern sporting rifle (MSR), which includes the semi-automatic AR-15. He said that class of rifle was sold in fewer than a third of its roughly 4,500 U.S. stores.

Objective

1. Check if the input feed is regarding **Wal-Mart**.
2. If yes, then trigger an alarm that contains the following information:
   - **Event Cause**: Include the title of the feed item.
   - **Additional Information**: Include the focus paragraph of the feed item.

Solution

Set the following for the Input message filter rules:

Name	Negated	Xpath	Regular Expression
User defined name	Leave deselected		(?<ValueToExtract>Wal-Mart|Walmart)

NOTE: Even though **Walmart** is the official name of the company, sometimes news articles use the name **Wal-Mart**. This input rule will match all web feed articles that contain either **Walmart** or **Wal-Mart** and therefore this rule is more robust.

Set the **following** for the Event Trigger Settings:

Alarm Property	Default Value	Xpath	Regular Expression
Event Cause			\<title\>(?<ValueToExtract>.*)\</title\>
Additional Information			\<span class="focusParagraph"\>\<p\>(?<ValueToExtract>.*)\</p\>

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