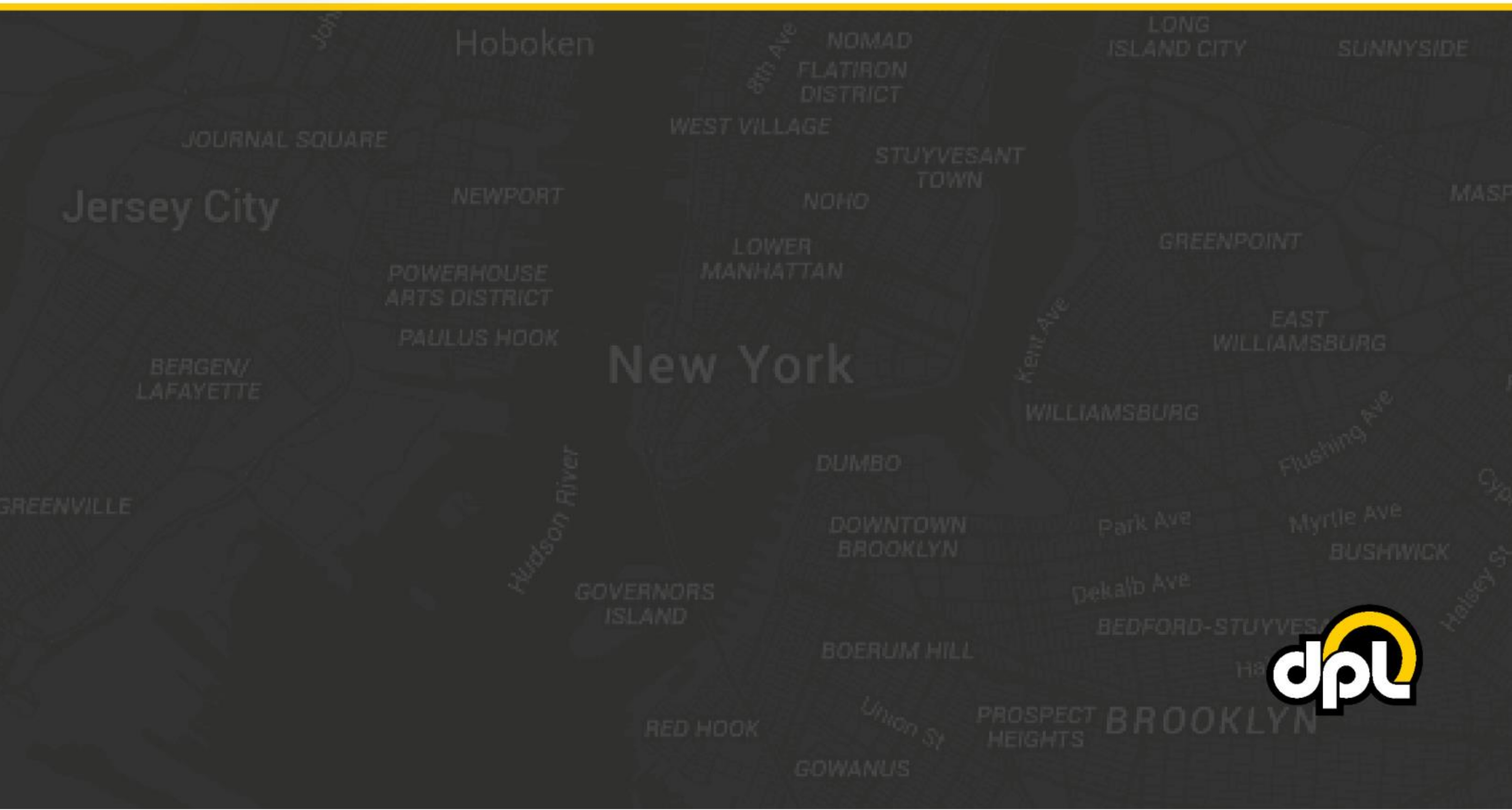
Triton SSL/TLS Configuration Guide

Proper SSL/TLS Setup for your Triton ATM



dpl

Table of Contents

Purpose

This guide will instruct you how to properly configure SSL/TLS on your Triton brand ATM. This guide is based on the Triton Argo RL2413 – the required steps for your model may vary. The document will take you through:

- Setting up address-based host setup
- Enabling SSL/TLS with certificate and hostname verification

By the end of the document you will have a securely connected ATM that should be resilient to Man-in-the-Middle (MITM) attacks involving external tampering of the Ethernet or modem.

Prerequisites

In order to successfully complete the steps that follow you will need:

- The hostname and port of your payment processor's SSL enabled ATM host application
- A working internet connection with which to test your ATM

Examples of the required information will be provided in the steps below.

Steps

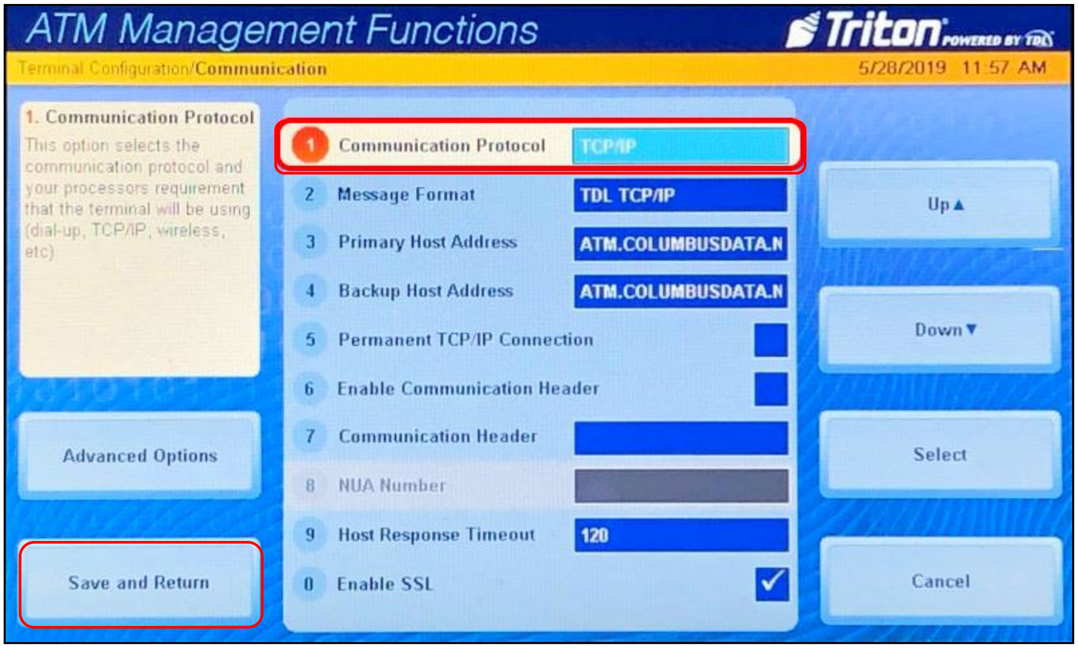
1. ATM TCP/IP Setup

Before we begin setting up SSL/TLS we will need to ensure that we are on a TCP/IP ATM with either a working DHCP or static IP setup for internet connectivity.

> **NOTE:** DHCP will enable dynamic allocation of the IP address from the Hercules modem that the ATM is plugged into. This is preferred as it means changes to the ATM are not required if changes are made to the settings of the Hercules modem. Static IP can be more stable for some older ATMs but requires manual ATM reconfiguration if the Hercules modem is updated to new addresses (or other network topology changes).

a) Open the communication menu and use the ATM Operator Menu to navigate to the **Communication** screen seen as below. From this screen, enable **TCP/IP** by pressing the **1 key** and choosing **TCP/IP**.

ATM Operator Menu > Terminal Configuration > Communication



1. Communication Protocol

This option selects the communication protocol and your processors requirement that the terminal will be using (dial-up, TCP/IP, wireless, etc)

1 Communication Protocol: TCP/IP

2 Message Format: TDL TCP/IP

3 Primary Host Address: ATM.COLUMBUSDATA.N

4 Backup Host Address: ATM.COLUMBUSDATA.N

5 Permanent TCP/IP Connection: □

6 Enable Communication Header: □

7 Communication Header:

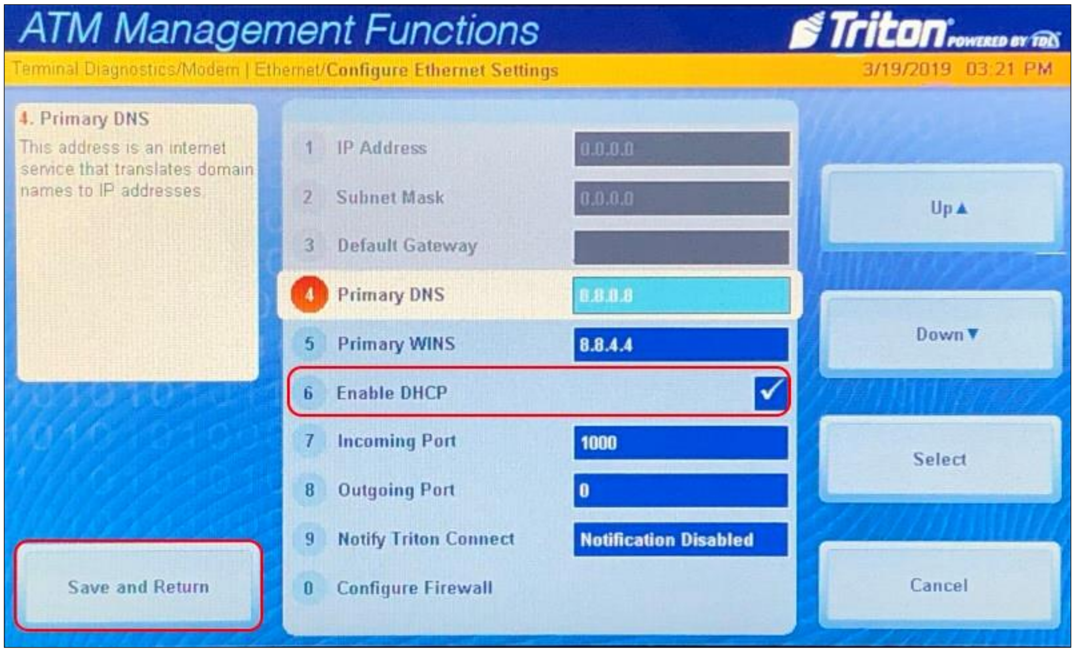
8 NUA Number:

9 Host Response Timeout: 120

0 Enable SSL: ☑

b) Now we will enable either DHCP (preferred for newer installations) or a static IP (using information provided by the installation site or the wireless modem being used) using the **6 key** on the keypad to toggle DHCP, then save using the **Save and Return** button on screen.

ATM Operator Menu > Diagnostics > Modem / Ethernet > Configure Ethernet Settings



Terminal Diagnostics/Modem | Ethernet/Configure Ethernet Settings 3/19/2019 03:21 PM

4. Primary DNS

This address is an internet service that translates domain names to IP addresses.

1 IP Address 0.0.0.0

2 Subnet Mask 0.0.0.0

3 Default Gateway

4 Primary DNS 8.8.8.8

5 Primary WINS 8.8.4.4

6 Enable DHCP ✓

7 Incoming Port 1000

8 Outgoing Port 0

9 Notify Triton Connect Notification Disabled

0 Configure Firewall

c) Once your information has been input you press the **Save and Return** on screen button to save the changes.

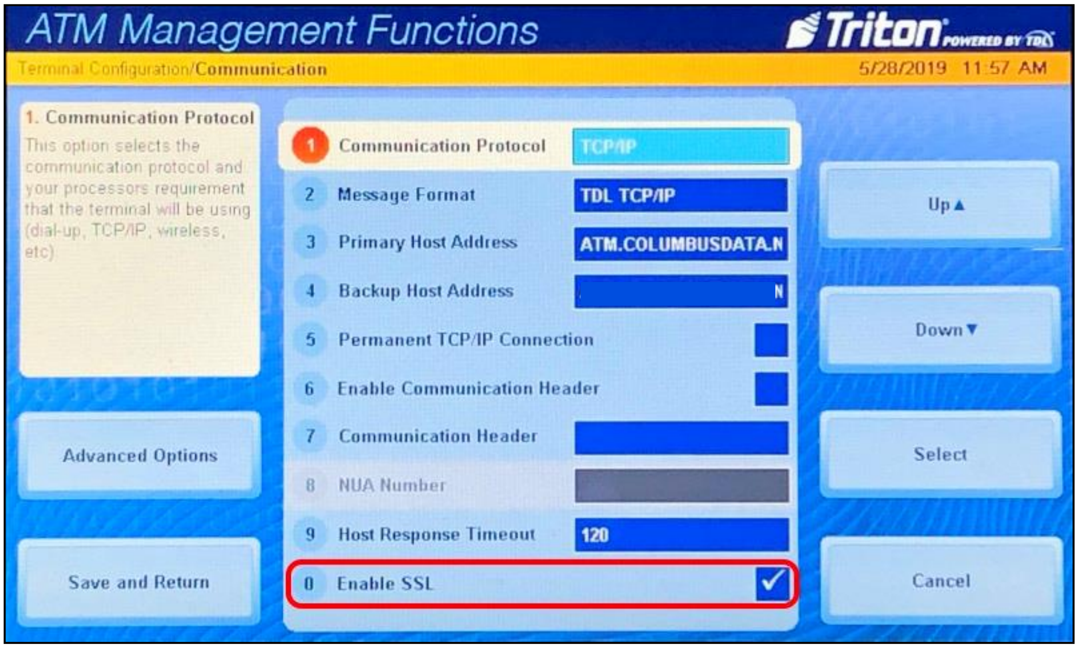
NOTE: If you have switched from Static to DHCP or vice versa, you may need to reboot the ATM now or after completing the remaining steps. See how to reboot your ATM under "**Testing SSL**" below.

2. Enabling SSL/TLS Properly

In this section we will enable TLS 1.2 to secure the ATM against man-in-the-middle attacks on the Ethernet line.

a) Navigate to the **Communication** screen using the path listed below, then check the **Enable SSL** box by pressing the **0 key** on the keypad.

ATM Operator Menu > Terminal Configuration > Communication



1. Communication Protocol
This option selects the communication protocol and your processors requirement that the terminal will be using (dial-up, TCP/IP, wireless, etc)

1	Communication Protocol	TCP/IP
2	Message Format	TDL TCP/IP
3	Primary Host Address	ATM.COLUMBUSDATA.N
4	Backup Host Address	N
5	Permanent TCP/IP Connection	□
6	Enable Communication Header	□
7	Communication Header	
8	NUA Number	
9	Host Response Timeout	120
0	Enable SSL	☑

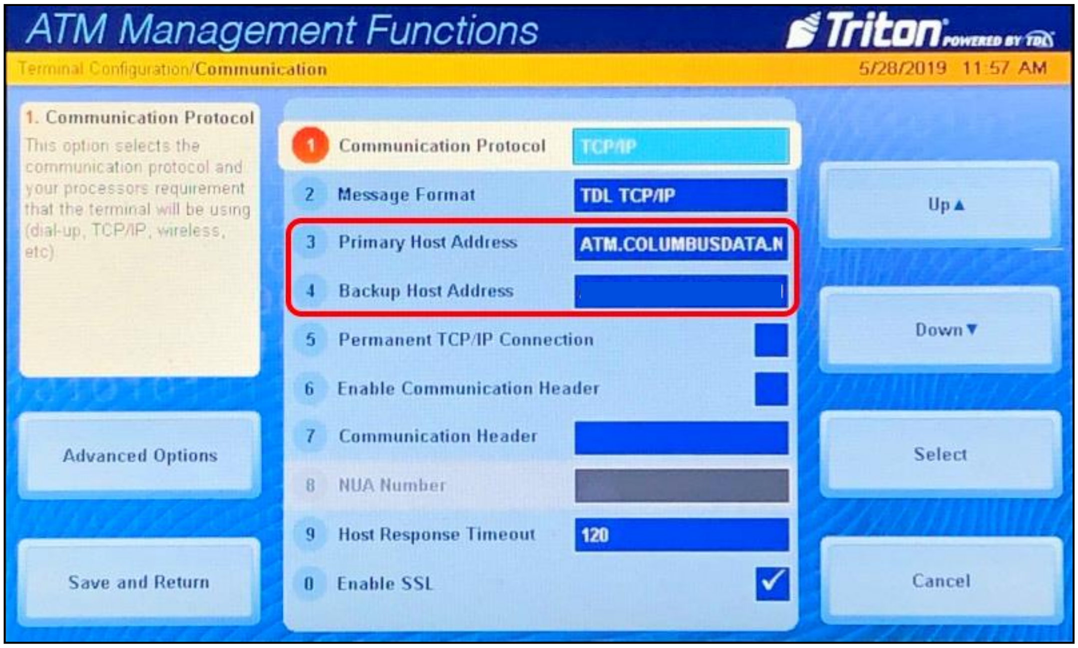
NOTE: The **Message Format** field will depend on your specific payment processor's requirements for no CRC or ETX, consult with them for the correct type.

3. SSL Host Configuration

In this section we will configure the host addresses for SSL/TLS. Configure the address fields to **atm.columbusdata.net** and the port fields to **6965** for example, use the information provided by your payment processor. Triton uses a URI instead of independent fields, for this reason, combine them to be **atm.columbusdata.net:6965** for example – this should be entered directly into the **Primary** and **Backup Host Addresses.**

a) Configure the information using the data listed above. Navigate to the **Communication** screen and enter the host information.

ATM Operator Menu > Terminal Configuration > Communication



1. Communication Protocol
This option selects the communication protocol and your processors requirement that the terminal will be using (dial-up, TCP/IP, wireless, etc)

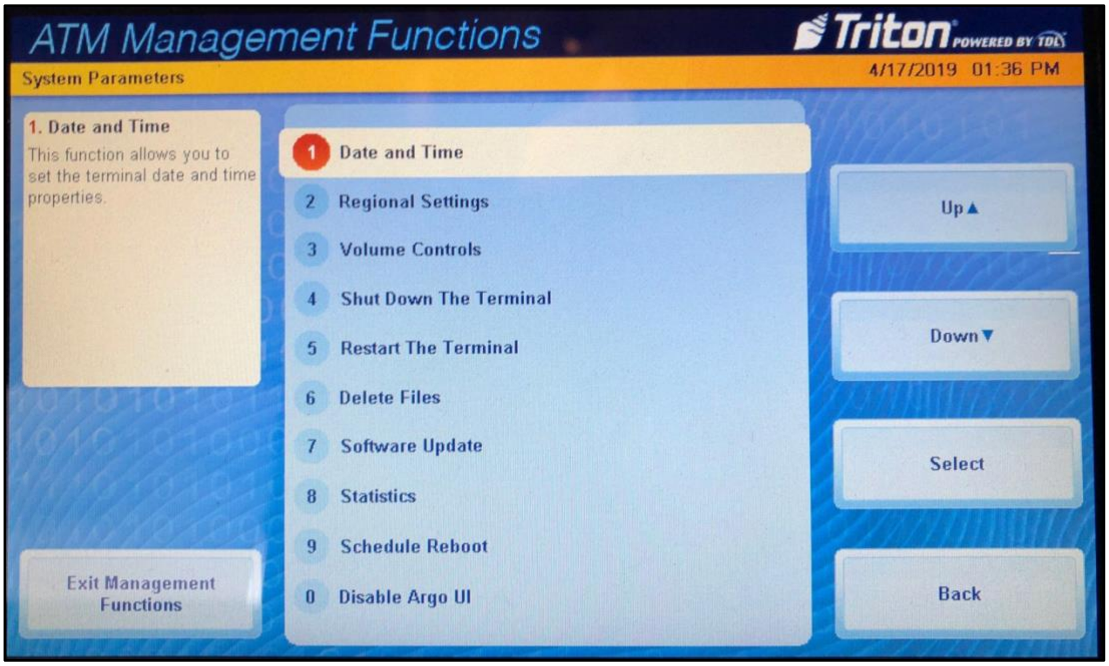
1 Communication Protocol: TCP/IP
2 Message Format: TDL TCP/IP
3 Primary Host Address: ATM.COLUMBUSDATA.N
4 Backup Host Address:
5 Permanent TCP/IP Connection
6 Enable Communication Header
7 Communication Header
8 NUA Number
9 Host Response Timeout: 120
0 Enable SSL ✓

4. Testing SSL

The easiest way to perform a test of your new SSL configuration for your is to do a dummy transaction on your Triton Argo RL2413.

NOTE: If you encounter any issues use the **5 key** to **Restart The Terminal** on the **System Parameters** screen as seen below as seen below to reboot the ATM to ensure the TCP/IP information has taken effect.

ATM Operator Menu > System Parameters > Restart The Terminal



This function allows you to set the terminal date and time properties.

If there is a failure at this point, go back and double check all the configuration options from the previous steps.

Conclusion

After completing all the above steps your Triton ATM will be set to use SSL (TLS 1.2) on all transactions with the payment processor. This ensures that no 3rd party can listen on the line and get any usable data, terminate the SSL connection and proxy it out (MITM attack), or any other nefarious logical attack against outgoing data from your ATMs.