GenMega SSL/TLS Configuration Guide

Proper SSL/TLS Setup for your GenMega ATM

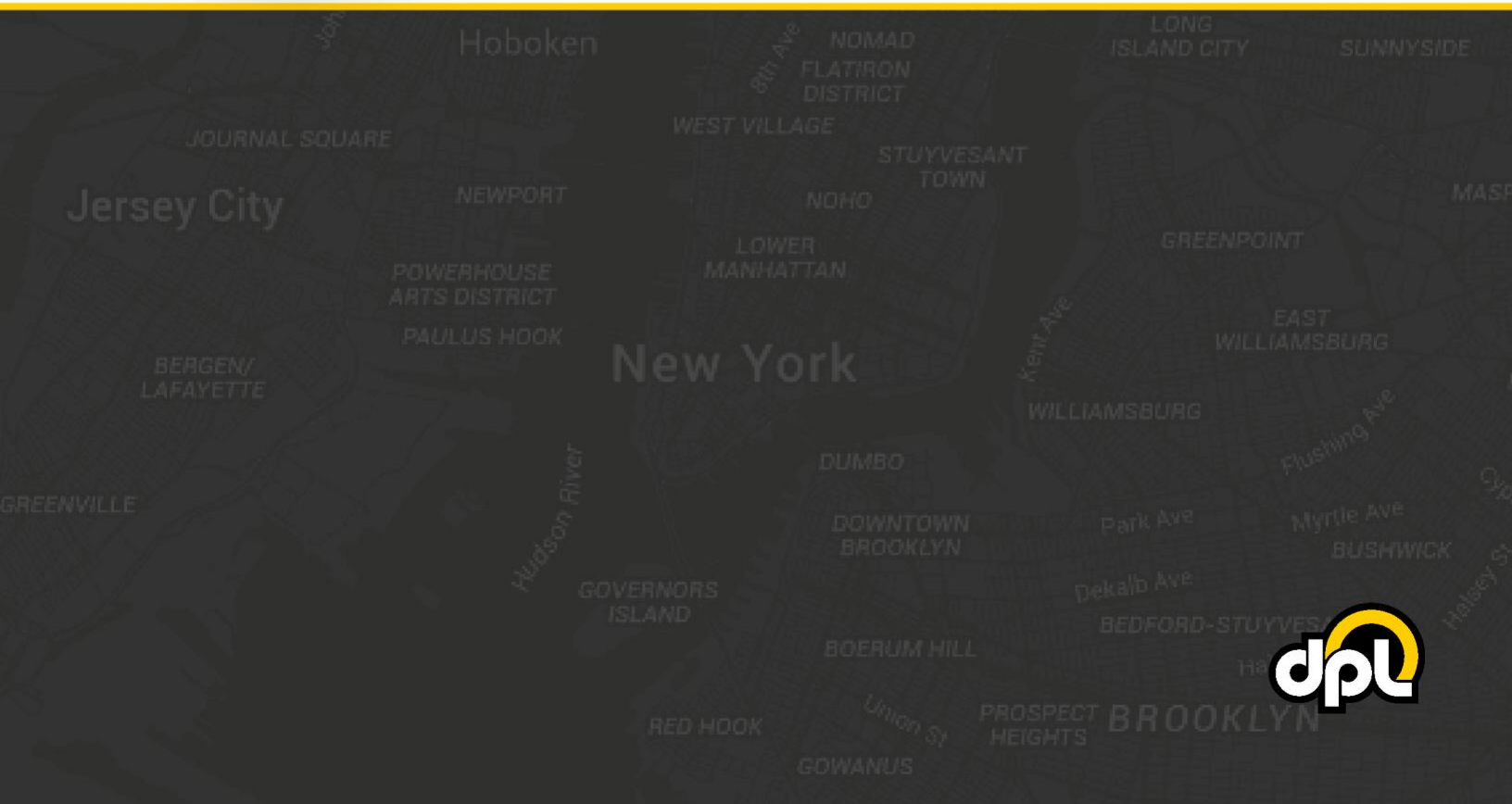


Table of Contents

Purpose

This guide will instruct you how to properly configure SSL/TLS on your GenMega brand ATM, this guide is based on the GenMega G2500 ATM – the required steps for your model may vary. The document will take you through:

- Installing the DPL **rootcert.pem** file
- Setting up address-based host setup
- Enabling certificate and hostname verification
- Enabling SSL/TLS

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

To successfully complete the following steps you will need:

- The DPL **rootcert.pem** or a **rootcert.pem** provided by your payment processor
- 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

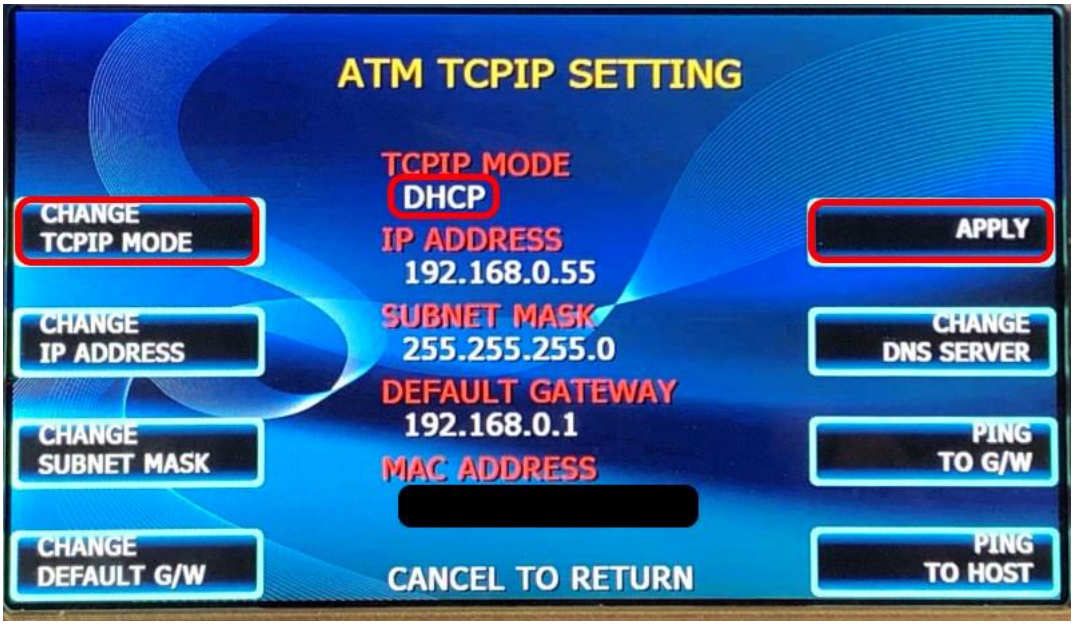
1. ATM TCP/IP Setup

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) Use the ATM Operator menu to navigate to the TCP/IP menu. Using the path listed below.

ATM Operator Menu > System Setup > Device Setup > ATM TCP/IP Settings



b) Enable either DHCP (preferred for newer installations) or a static IP (using information provided by the installation site or the modem being used) using the **Change TCP/IP Mode** button (and other buttons if using static).

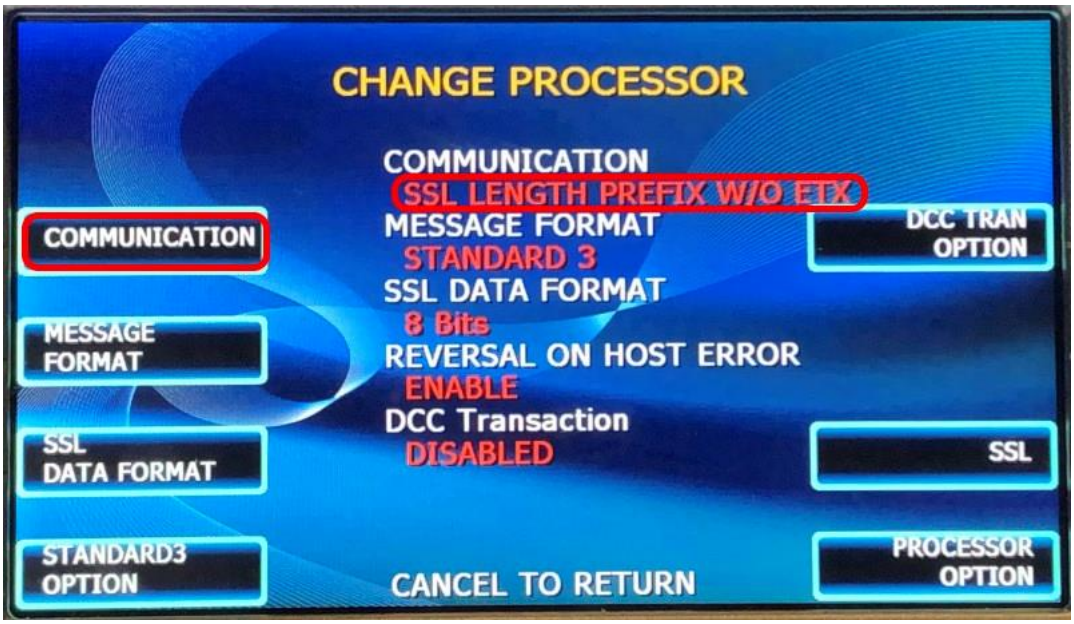
c) Once your information has been input you press the **Apply** button to save the changes.

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, enable hostname verification to block certificate spoofing, and finally enable certificate verification to make sure the ATM is verifying the certificate chain.

a) Navigate to the **Communication** screen using the path listed below. Configure the **Communication** field to **SSL Length Prefix w/o ETX** for example or check with your payment processor for the setup you require.

ATM Operator Menu > Customer Setup > Change Processor



NOTE: Match up the information (**Message Format, SSL Data Format,** etc.) as provided by your processor or modem manufacturer.

b) Navigate to the **SSL Configuration** screen using the path listed below. Configure the options for secure communication by pressing the **SSL** button on the **Change Processor** screen.

ATM Operator Menu > Customer Setup > Change Processor > SSL

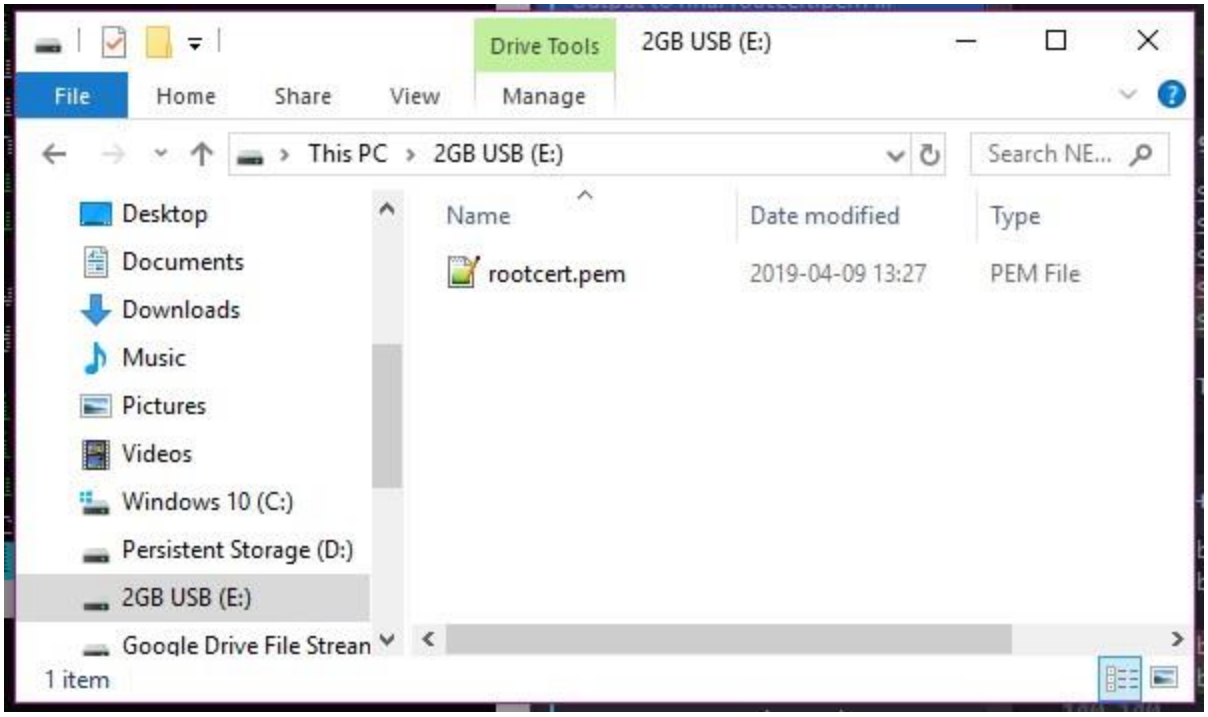
3. Installation of Root Certificate Files (rootcert.pem)

The **rootcert.pem** file is used to supplement the list of certificates already installed on your GenMega ATM. The supplemental certificates are trusted chains used by payment processors that are not always preinstalled on ATMs. These will allow validation to be enabled on the ATM for enhanced protection against logical attacks.

a) Download the DPL **rootcert.pem** file (or the certificate chain indicated by your payment processor) and install it on a USB drive or SD card that is 2GB or less in size. It should appear as depicted below.

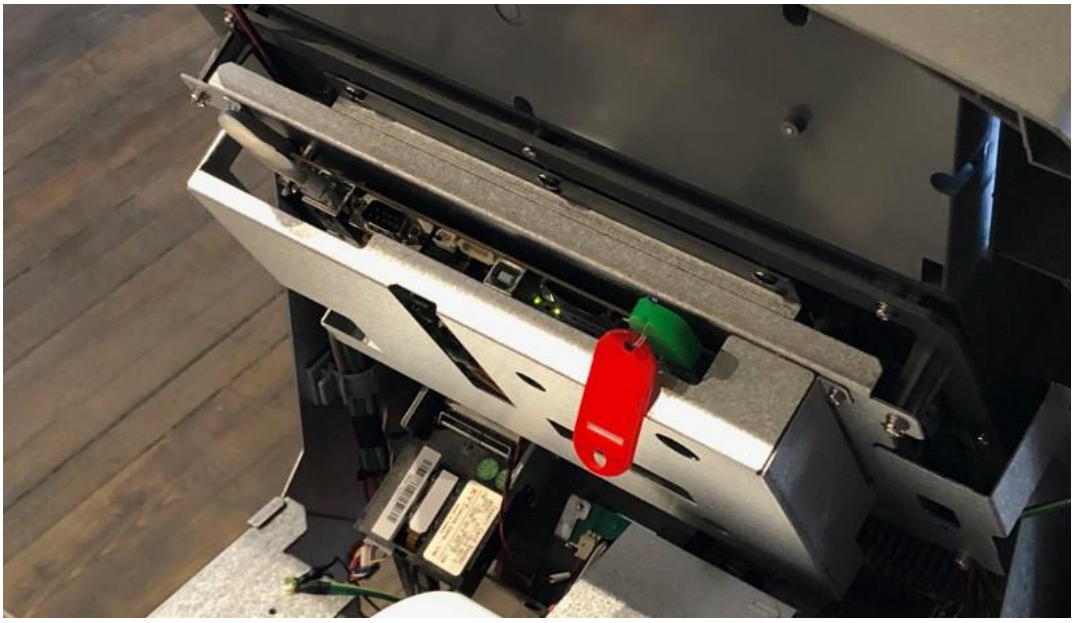
NOTE: The 2GB drive size is a requirement for GenMega ATMs. They can have trouble accessing drives larger than 2GB. **WARNING:** This is important. If you don't have one, purchase a 2GB drive.

Adding rootcert.pem to Root of USB Drive/SD Card



b) Plug the USB drive (or SD card) into the appropriate port on your GenMega's control board (the green USB drive in our example). The GenMega G2500 ports are as seen below. USB is on the right when viewing the ATM from behind.

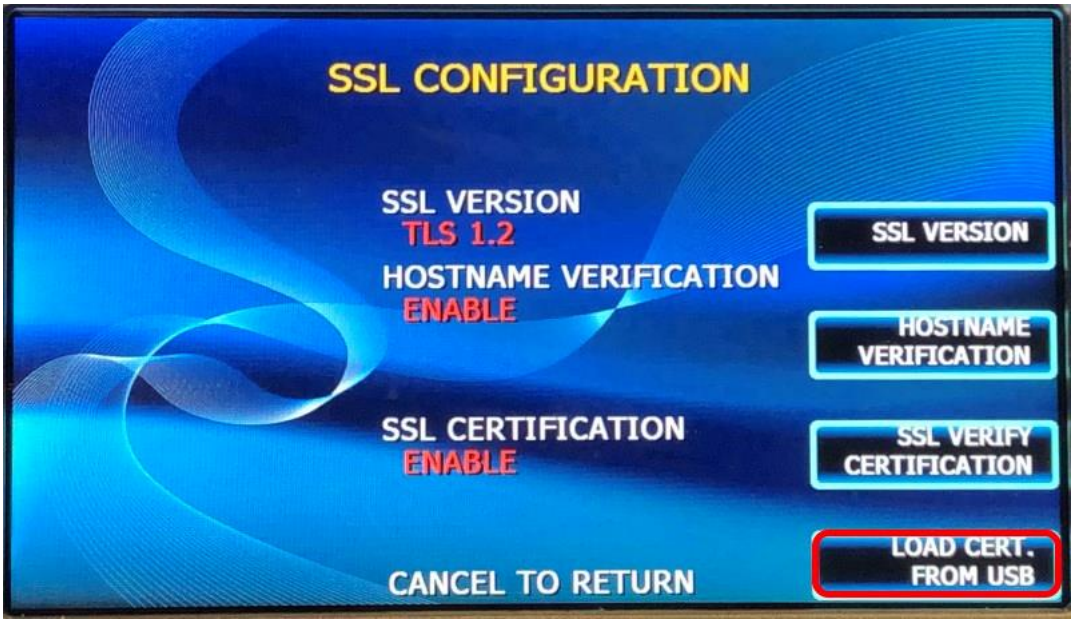
GenMega G2500 USB Port/SD Card Slot



c) To install the new **rootcert.pem,** navigate to the SSL Configuration screen using the path listed below and press **Load Cert. From USB.**

NOTE: If you encounter an error at this stage, you either misnamed the **rootcert.pem** file or your USB drive or SD card is not 2GB or less and FAT formatted (see previous steps).

ATM Operator Menu > Customer Setup > Change Processor > SSL



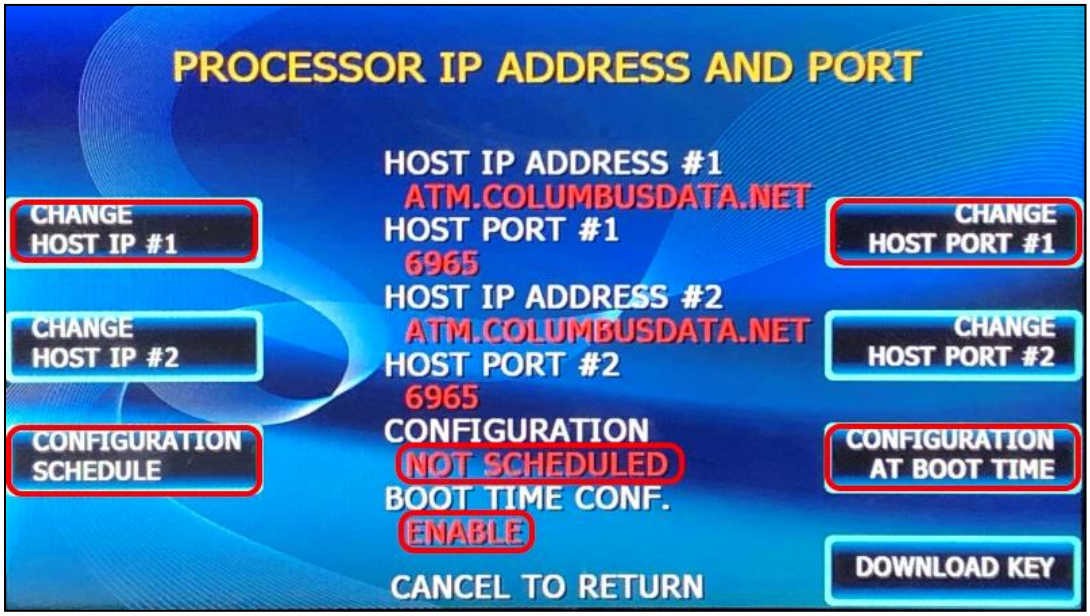
Once this is complete you should see an Operation Success displayed on screen.

4. SSL Host Configuration

Now we will configure the host addresses to point to the SSL enabled payment processor. Configure the address fields to match the information from your payment processor, we will use **atm.columbusdata.net** for our address field and **6965** for our port field.

a) First configure the information using the data from your processor or modem using the highlighted buttons.

ATM Operator Menu > Host Setup > Host IP Address



NOTE: For our example set the **Configuration Schedule** to **Not Scheduled** and enable **Configuration At Boot Time,** check with your payment processor for their preferred setup.

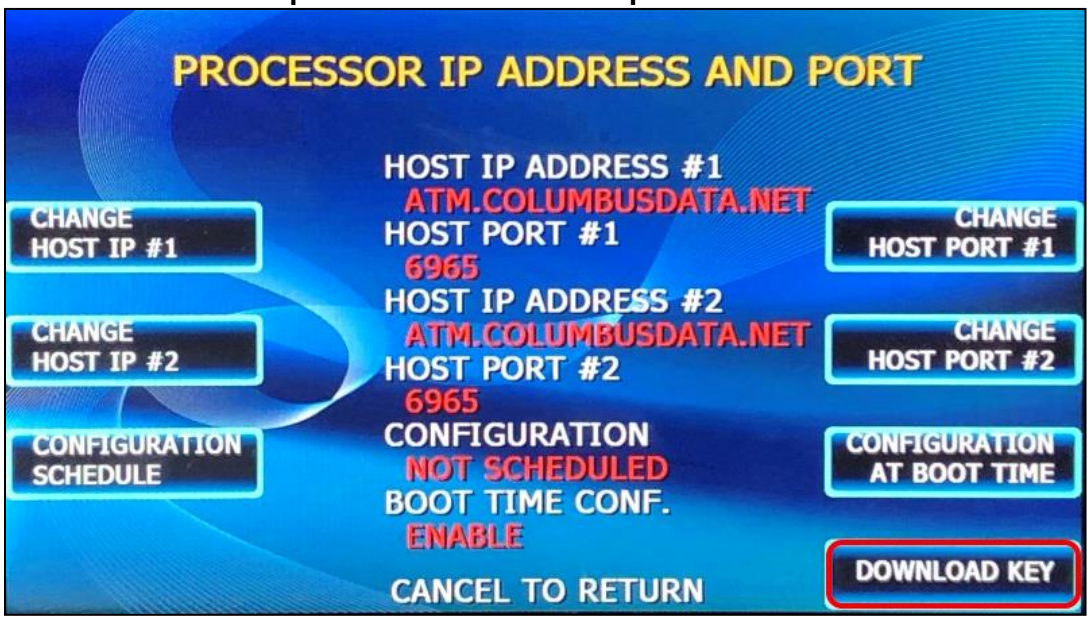
5. Testing SSL

In this final section there are a couple options we can use to test that SSL is configured properly on your ATM:

1. A dummy transaction could be completed on the ATM
2. Use the **Download Key** button on the **Host IP Address** screen will test the connection

For this document the **Download Key** options will be demonstrated.
Open the **Host IP Address** screen as seen below and press the **Download Key** button. It will give you a success message if everything is working correctly on your new setup.

ATM Operator Menu > Host Setup > Host IP Address



NOTE: If you encounter any issues use the **Reboot System** button on the **Set Reboot Time** screen as seen below to reboot the ATM to ensure the TCP/IP information has taken effect.

ATM Operator Menu > System Setup > Set Reboot > Reboot System

Once this is complete go back and attempt to test the SSL connection again. 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 GenMega 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.