SecureTable

By PayFacto

Setup & Use

For Maitre'D

Maitre'D

Software that serves you better

October 2021

Table of Contents

Introduction **3**
- Overview 3
- Requirements 5

STPI Secure Installation **6**
- Installation process overview 6
- Install Microsoft .NET Framework 3.5 SP1 7
- Install Java for Windows 11
- Install the STPI Client Software 12
- Activate the STPI Secure License 18
- Start the STPI Secure Client 20
- Configure the STPIClient as a Service 26

Maitre'D Configuration **31**
- Electronic Funds Transfer Setup 31
- Media Type Mappings for SecureTable 36
- Generic Media Type Mapping for SecureTable 43

SecureTable Application **49**
- SecureTable Installation on Android Terminals 49
- SecureTable Application - Basic Navigation 53
- SecureTable Application Configuration 56
- SecureTable Functions 63

Payment Process **66**
- SecureTable Full Transaction Workflow 66
- Working with Tips 81
- Voids 92

Tasks - How To's **96**
- Task : Add an APN to Your Payment Terminal 96
- Task : Configure Port Forwarding 102
- Task : Switch between WiFi and LTE 106

Troubleshooting **111**
- .NET Framework 3.5 missing 111
- Java is missing 113

Overview

Purpose of this document

This document will cover the configuration required to operate SecureTable using the Maitre'DVeloce direct integration to the STPI client.

SecureTable

securetable

SecureTable is a universal middleware platform that provides an EMV-Compliant, Pay at the Table (PATT) processing solution that can be connected to a POS (Point of Sale) system. The solution can work in standalone mode as well as integrated to a Point of Sale (POS) system such as Maitre'D, Veloce, Squirrel, Aloha and Micros among other.

"Pull" architecture

SecureTable uses a "Pull" architecture. This means that a payment terminal using SecureTable can initiate the transaction process by ***Pulling*** check data from the POS system. In other words, after the guest checks are printed and handed to customers, there is no need for the server to walk back to the POS workstation to apply payments and close guest checks. All payments, including credit, debit and cash, can be applied at the table side, and checks are closed automatically.

By comparison, a traditional "Push" architecture is a system where the transaction would be initiated from the POS system, and check data pushed to the payment terminal. In a table-service restaurant, this process often required the customers to get up and walk to the POS workstation to insert their payment card and enter their PIN using a tethered payment terminal.

Accurate payment reporting

The integration of SecureTable with various POS systems allows the payment terminal to retrieve guest check data from the POS System. Once a payment has been processed by the payment terminal, SecureTable sends the payment data back to the POS System for reporting purposes. Payment amounts, tip amounts and card brand used are all automatically transmitted to the POS system to allow for accurate reporting.

Compatible with SecurePay

SecureTable and SecurePay can both be used on the same POS system. This allows merchants to use any combination of stationary Pay-at-the-Counter terminals and wireless Pay-at-the-Table terminals. SecureTable and SecurePay share a similar user interface which provides a consistent user experience for customers and employees.

Compatibility with third-party payment terminals

If a third-party solution with tethered (wired) payment terminals is already in place and integrated to the POS system, SecureTable can still be used without worry. A configurable table-locking or invoice-locking mechanism prevents accidentally accessing guest checks that are being processed by a payment terminal through SecureTable. This means that establishments can, for example, use wireless payment terminals with SecureTable in the dining room while using tethered payment terminals for the cashier station, bar, pickup counter and drive-through windows.

Full-featured solution through direct integration

With a direct integration, Maitre’D communicates directly with SecureTable’s STPI client through a secure socket connection without using drop-files. This allows Maitre’D to take advantage of all the features offered by SecureTable, without the limitations imposed by using the former TPI client middleware.

Requirements

Maitre’D Software Version Requirements

- Maitre’D version 7.08.000.280 or later.

Maitre’D License Requirements

- Maitre’D Electronic Funds Transfer Interface.
- Maitre’D Enhanced EFT option.

Software Requirements

- Any supported Windows operating system with all latest updates.
- Java SE Runtime Environment.
- Microsoft .NET Framework 3.5.
- STPI Client software (included with the STPISecure Installer)

NOTE: The TPI client is NOT required, thanks to the direct integration of SecureTable within the Maitre’D software.

Hardware Requirements

- SecureTable-Compatible Payment terminal(s)
- 1 Gbps (Gigabit) Ethernet (wired) network or better.
- WiFi network (802.11 ac or better)
- High-Speed Internet connection.

Installation Process Overview

Here is a quick overview of the entire installation and setup process:

1. Install/enable Microsoft .NET Framework 3.5 SP1.
2. Install the latest version of Oracle's Java for Windows.
3. Use the STPISecure to installer to install the STPIClient software.
4. Install the STPIClient license.
5. Start the STPIClient application for the first time.
6. Configure the STPIClient to start as a service (Optional).
7. Configure your POS System.
8. Connect, power up and configure payment terminals.

Before you begin

By default, the payment terminals using SecureTable will communicate with the POS system over TCP port 9999.

- Open TCP port 9999 on the corporate firewall.
- Open TCP port 9999 on the Windows Defender Firewall on the POS system's Back-Office as well as on all POS workstations.
- The wireless network (for wireless payment terminals) needs to be able to communicate with the POS System.
- Each payment terminal needs access to the Internet.

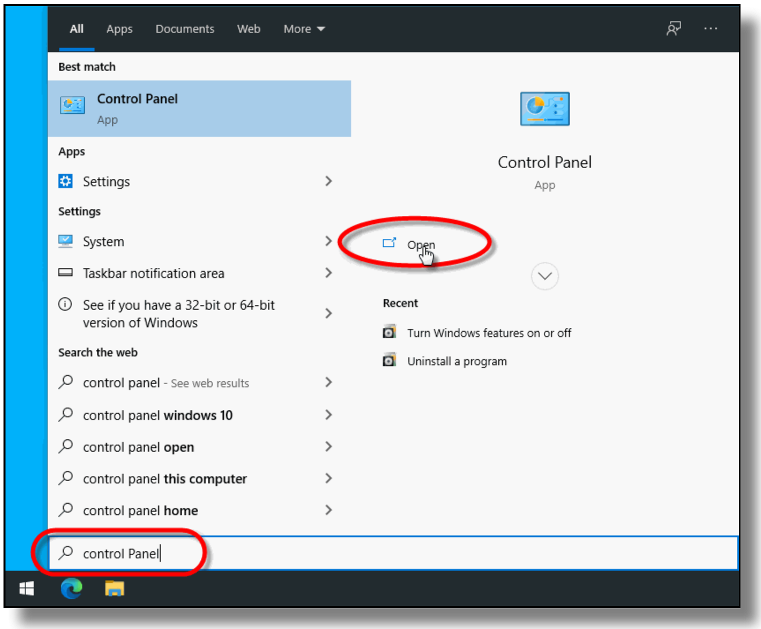
Install Microsoft .NET Framework 3.5 SP1

The .NET Framework (pronounced as "dot net") is a software framework developed by Microsoft that runs primarily on Microsoft Windows. Microsoft .NET Framework version 3.5 Service Pack 1 is required before the STPISecure installer can be used to install the STPISecure client or other components, such as the RTI-SIPA plugin.

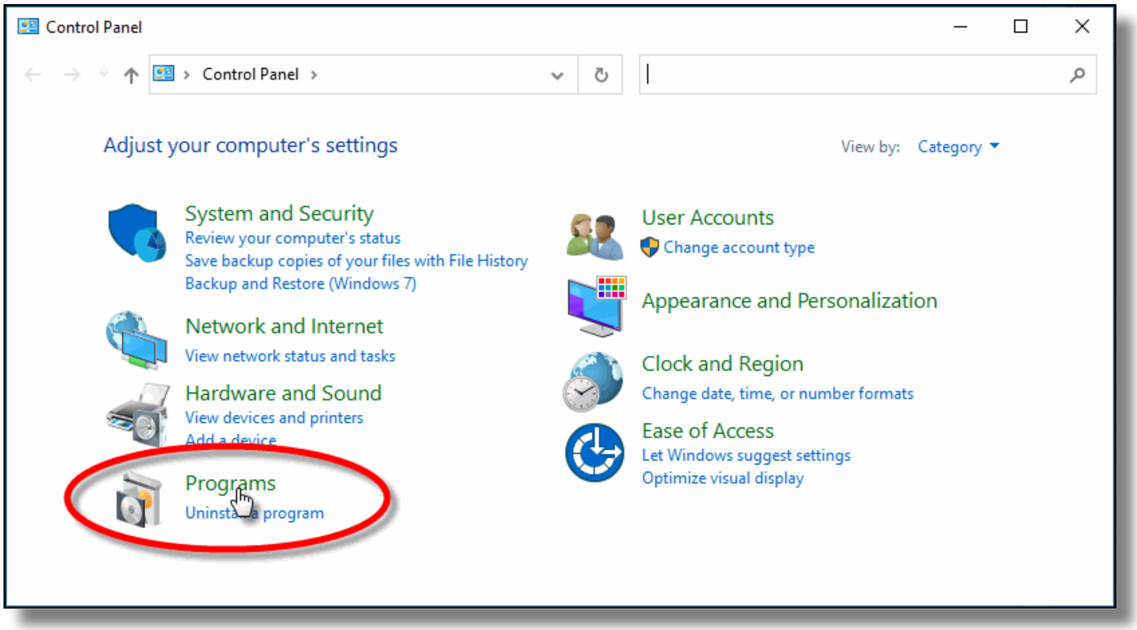
Enabling Microsoft .NET Framework 3.5 SP1 for Windows 10

On Windows 10, starting with version 1809, Microsoft .NET Framework 3.5 SP1 is included as a standard Windows feature and enabled by default. However, older versions of Windows 10, Enterprise or IoT editions, could be missing this essential component. Here is the procedure to check whether .NET Framework 3.5 SP1 is installed and how to enable it on Windows 10:

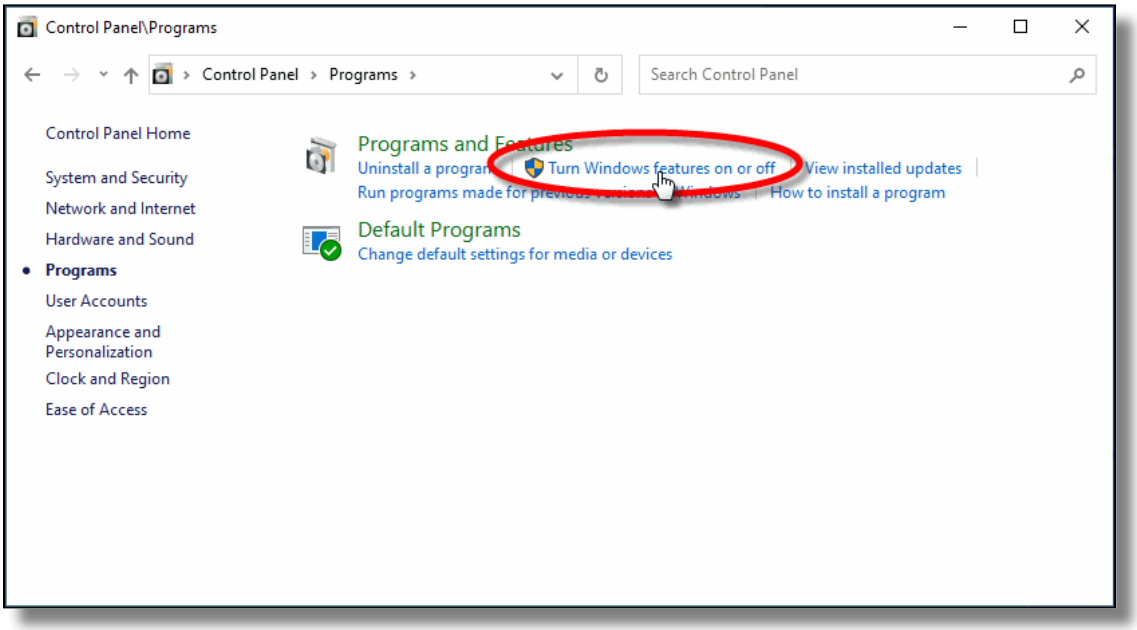
1. Click on the Windows 10 Start button and type ***Control Panel***.
2. The ***Control Panel app*** should appear as a search result. Click on ***Open***.



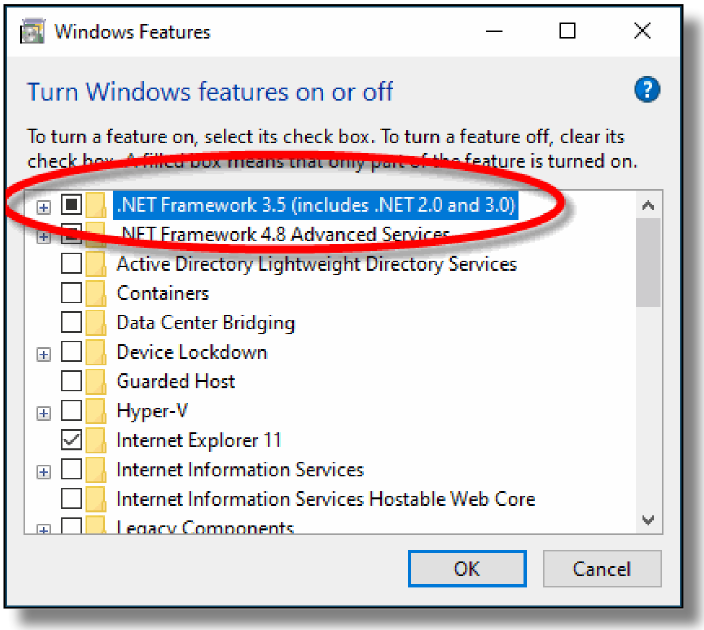
3. Within the Control Panel app, click on ***Programs***.


Control Panel
Control Panel ›
Adjust your computer's settings
View by: Category ▾
System and Security
Review your computer's status
Save backup copies of your files with File History
Backup and Restore (Windows 7)
Network and Internet
View network status and tasks
Hardware and Sound
View devices and printers
Add a device
Programs
Uninstall a program
User Accounts
Change account type
Appearance and Personalization
Clock and Region
Change date, time, or number formats
Ease of Access
Let Windows suggest settings
Optimize visual display

4. Under ***Programs and Features***, select ***Turn Windows features on or off***.



5. The ***Windows Features*** list will appear.



Windows Features

Turn Windows features on or off

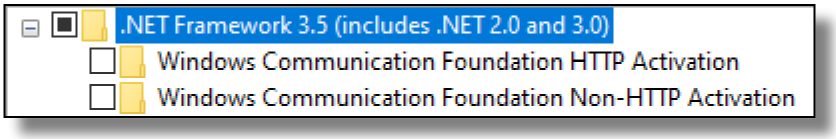
To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- ⊞ ■ .NET Framework 3.5 (includes .NET 2.0 and 3.0)
- ⊞ ■ .NET Framework 4.8 Advanced Services
- □ Active Directory Lightweight Directory Services
- □ Containers
- □ Data Center Bridging
- ⊞ □ Device Lockdown
- □ Guarded Host
- ⊞ □ Hyper-V
- ☑ Internet Explorer 11
- ⊞ □ Internet Information Services
- □ Internet Information Services Hostable Web Core
- ⊞ □ Legacy Components

6. Look for the feature called ***.NET Framework 3.5 (includes .NET 2.0 and 3.0)***.

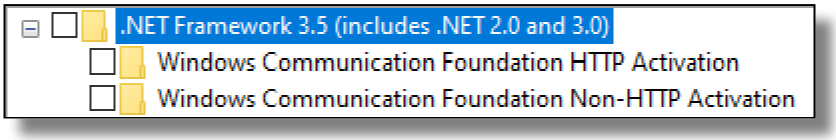
   a. If this feature is not listed, install .NET Framework manually. (See below)

   b. If you see a black square in this checkbox, .NET Framework 3.5 is already enabled and no further action is required.



- ⊟ ■ .NET Framework 3.5 (includes .NET 2.0 and 3.0)
  - □ Windows Communication Foundation HTTP Activation
  - □ Windows Communication Foundation Non-HTTP Activation

   c. If the checkbox is blank, enable it.



- ⊟ □ .NET Framework 3.5 (includes .NET 2.0 and 3.0)
  - □ Windows Communication Foundation HTTP Activation
  - □ Windows Communication Foundation Non-HTTP Activation

> **NOTE:** The black square in the check box means that the feature itself is enabled, but that some optional components are disabled. The optional components are not required for STPISecure or RTI-SIPA, so leave them disabled.

7. Click ***OK*** on the Windows Features list. This will close the list and apply any changes.

8. Files may be copied and you may be required to restart the PC.

Installing Microsoft .NET Framework 3.5 SP1 manually

For versions of Windows prior to Windows 10 1809, or for some older Enterprise or IoT editions, Microsoft .NET Framework 3.5 SP1 may need to be downloaded and installed manually.

The full installer can be obtained from the official Microsoft download site here:

Microsoft .NET Framework 3.5 SP1

Download the file and double-click it to start the installation process. Follow the on-screen instructions and restart your PC as required.

> ! **IMPORTANT!** If the link provided here does not work, please use your preferred search engine and look for "Microsoft .NET Framework 3.5". Be sure to download the files from the official Microsoft download site. For security reasons, please avoid non-Microsoft sources.

Install Java for Windows

The STPISecure Installer, the STPISecure client software for SecureTable and the RTI-SIPA plugin for SecurePay requires the installation of ***Java for Windows*** software. This can be downloaded and installed for free from Oracle’s Java website, Here.

Please download and install the latest version of ***Java for Windows*** for your specific Windows edition (32-bit or 64-bit).

NOTE: Please consult Oracle's Java website for detailed licensing conditions and support.

Install the STPISecure Client software

The following instructions describes the installation and configuration process for the Maitre'D POS System.

STPI Secure installation

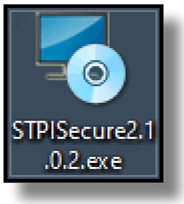
Note for Maitre'D POS users

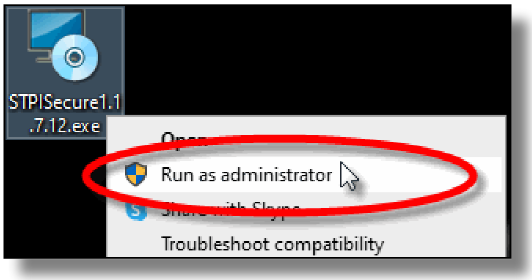
On a Maitre'D POS system, the latest version of the STPISecure Installer is bundled with each service pack update. To obtain the latest compatible version of the STPI Secure Installer and ensure optimal compatibility, please install the latest service pack update for your Maitre'D POS system.

Once the Maitre'D service pack update is installed, the STPISecure installer will be located here:

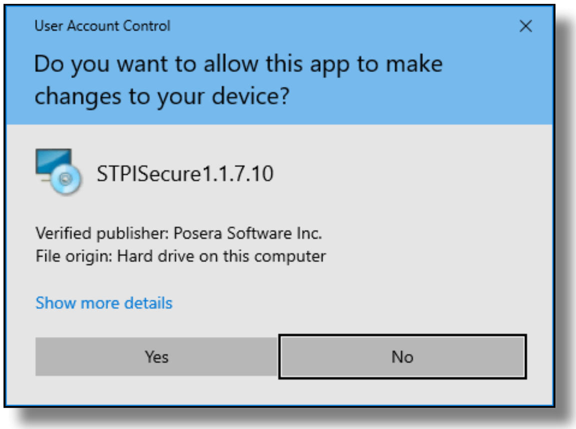
C:\POSERA\MaitreD\PRG\Setup

1. Locate the ***STPISecureX.X.X.X.exe*** file, then right-click the file and select ***Run as administrator***.





2. You may see a UAC prompt. Click ***Yes***.



User Account Control

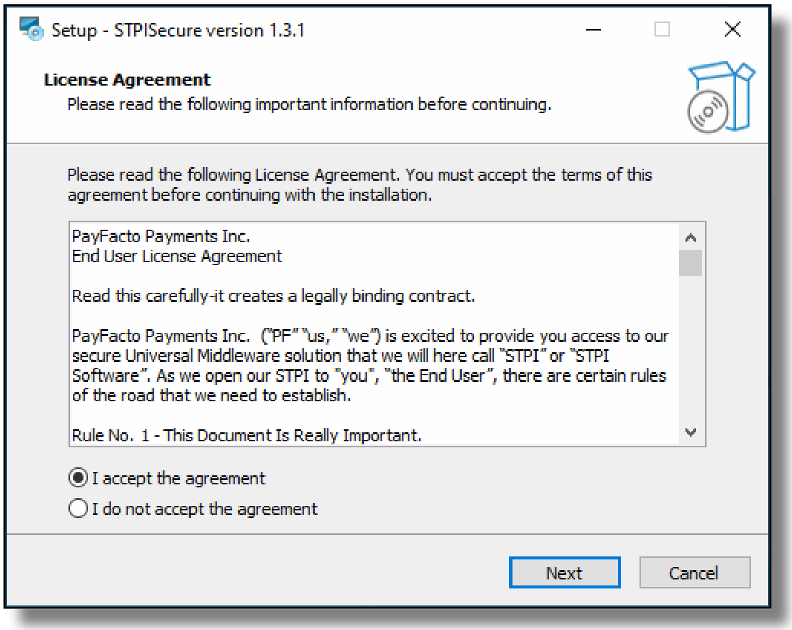
Do you want to allow this app to make changes to your device?

STPISecure1.1.7.10

Verified publisher: Posera Software Inc.
File origin: Hard drive on this computer

Show more details

3. Please read the End-User Licence Agreement. If you agree with the terms, select ***I accept the agreement*** and click ***Next>***.



Setup - STPISecure version 1.3.1

License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

PayFacto Payments Inc.
End User License Agreement

Read this carefully-it creates a legally binding contract.

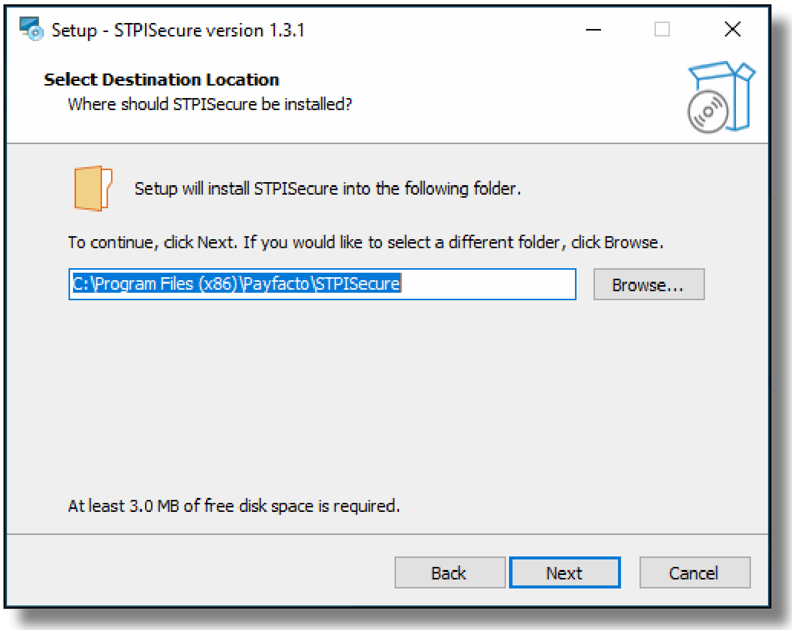
PayFacto Payments Inc. ("PF" "us," "we") is excited to provide you access to our secure Universal Middleware solution that we will here call "STPI" or "STPI Software". As we open our STPI to "you", "the End User", there are certain rules of the road that we need to establish.

Rule No. 1 - This Document Is Really Important.

● I accept the agreement

○ I do not accept the agreement

4. Select the installation destination for STPISecure files. Accept the default path by clicking ***Next>***.



Setup - STPISecure version 1.3.1

Select Destination Location

Where should STPISecure be installed?

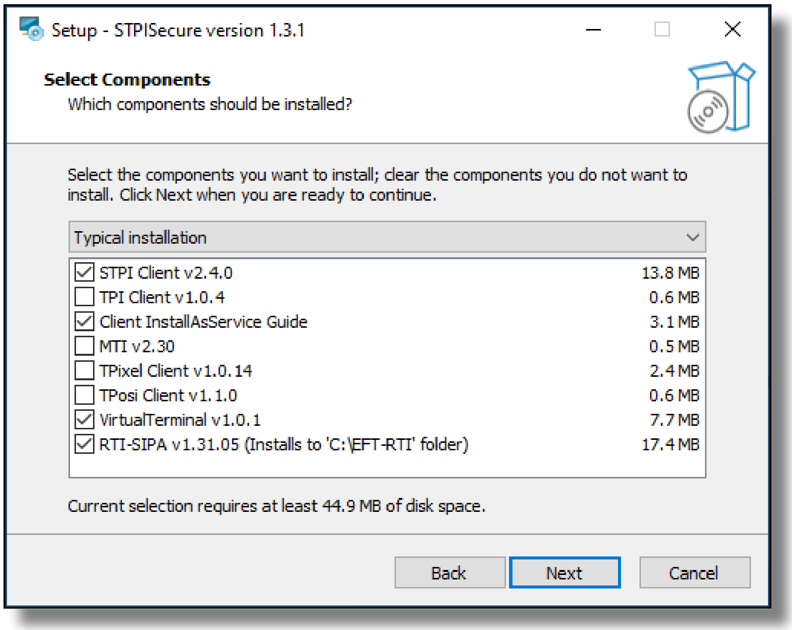
Setup will install STPISecure into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

C:\Program Files (x86)\Payfacto\STPISecure

At least 3.0 MB of free disk space is required.

5. Select the components you wish to install and click ***Next>***. A brief description of each available component is provided below. Install only what you need.



Select Components

Which components should be installed?

Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.

Typical installation

☑ STPI Client v2.4.0	13.8 MB
□ TPI Client v1.0.4	0.6 MB
☑ Client InstallAsService Guide	3.1 MB
□ MTI v2.30	0.5 MB
□ TPixel Client v1.0.14	2.4 MB
□ TPosi Client v1.1.0	0.6 MB
☑ VirtualTerminal v1.0.1	7.7 MB
☑ RTI-SIPA v1.31.05 (Installs to 'C:\EFT-RTI' folder)	17.4 MB

Current selection requires at least 44.9 MB of disk space.

STPI Client v2.x.x.x

This component is required to use the SecureTable application with wireless payment terminals in a table service environment, with a POS system like Maitre'D, Veloce and others. It can be installed alone or alongside RTI-SIPA v1.xx.x.x if a combination of Wireless PATT terminals and fixed terminals are used.

TPI Client v1.x.x

This component is only required with older versions of Maitre'D, such as 7.05.x.x. ***Do NOT*** install this component with newer versions of Maitre'D.

Client InstallAsService Guide

This component is optional and copies documents to the install folder with instructions on how to setup various clients as services.

MTI v2.30

This component is required for the Micros POS system only.

TPixel Client v1.0.12

This component is required for the Pixel Point POS system only.

TPosi Client v1.1.0

This component is required for the Positouch POS system only.

VirtualTerminal v1.0.1

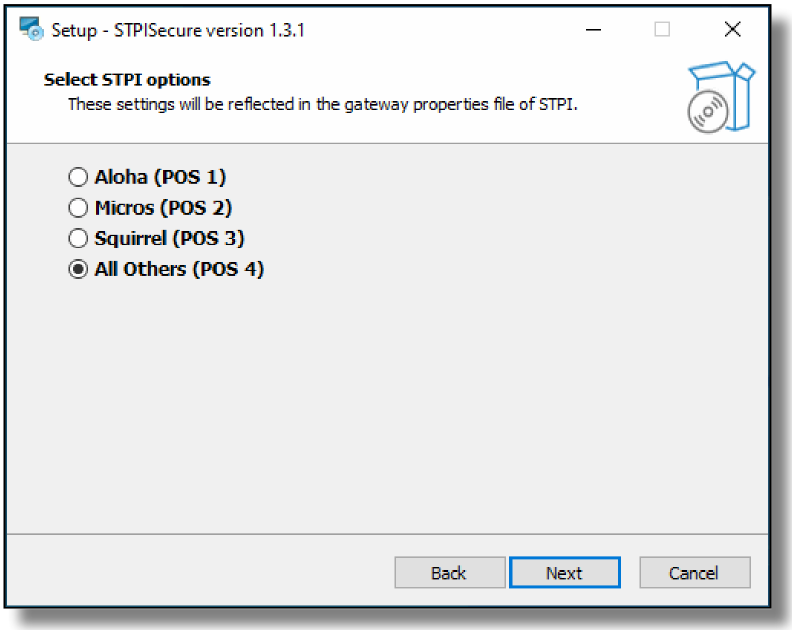
This is an optional component that allows for the software to be tested and demonstrated.

RTI-SIPA v1.xx.x.x

This component installs the Retail Terminal Interface for Semi-Integrated Payment Application (RTI-SIPA) plugin files for use with the SecurePay application. This component needs to be installed on the POS system's main Back-Office PC as well as on all POS workstations that will manage a payment terminal. It can be installed alone or alongside STPI Client v2.x.x.x if a combination of Wireless PATT terminals and fixed terminals are used.

NOTE: If you don't use fixed payments terminals with SecurePay, you don't need to install this component

6. Select the ***All Others (POS 4)*** option and click ***Next>***.



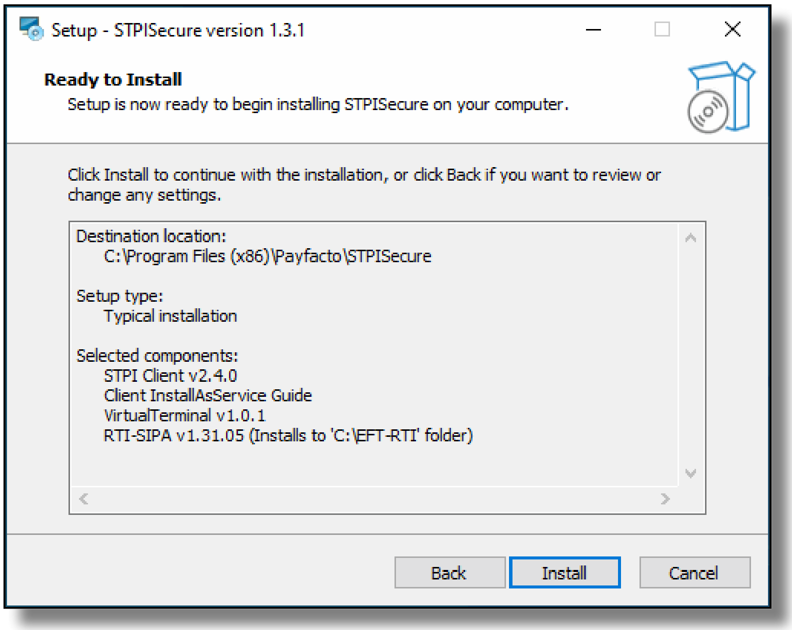
Setup - STPISecure version 1.3.1

Select STPI options

These settings will be reflected in the gateway properties file of STPI.

○ Aloha (POS 1)
○ Micros (POS 2)
○ Squirrel (POS 3)
● All Others (POS 4)

7. The setup wizard is now ready to begin the automated installation process. Review your settings and click the ***Install*** button.



Setup - STPISecure version 1.3.1

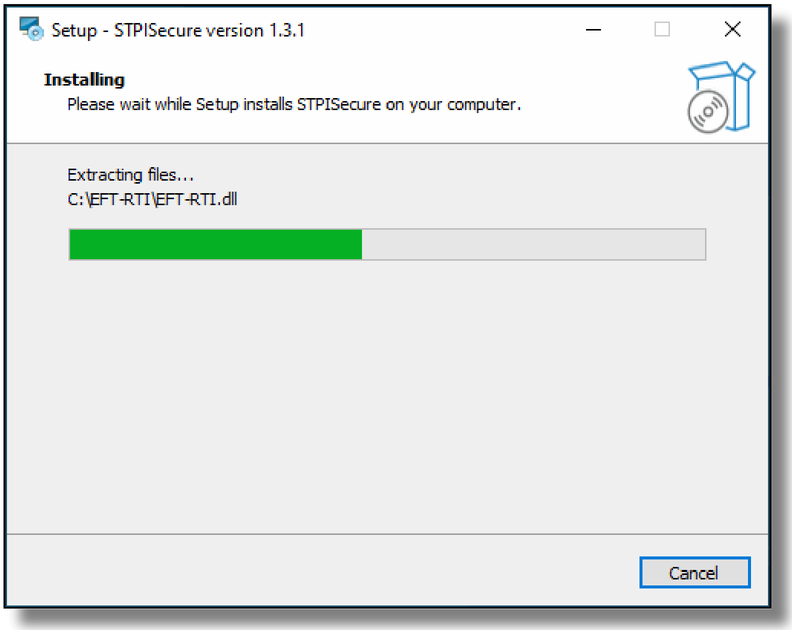
Ready to Install

Setup is now ready to begin installing STPISecure on your computer.

Click Install to continue with the installation, or click Back if you want to review or change any settings.

```
Destination location:
    C:\Program Files (x86)\Payfacto\STPISecure

Setup type:
    Typical installation

Selected components:
    STPI Client v2.4.0
    Client InstallAsService Guide
    VirtualTerminal v1.0.1
    RTI-SIPA v1.31.05 (Installs to 'C:\EFT-RTI' folder)
```

8. You will see various progress bars during the installation process. This could take a few minutes.



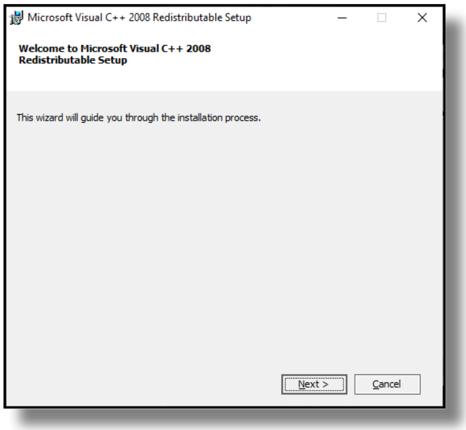
Setup - STPISecure version 1.3.1

Installing

Please wait while Setup installs STPISecure on your computer.

Extracting files...
C:\EFT-RTI\EFT-RTI.dll

a. During the installation, you could see the installation of required components like Microsoft C++ 2008 Redistributables. This will only appear if the component is missing from your system. Otherwise, you will not see this.

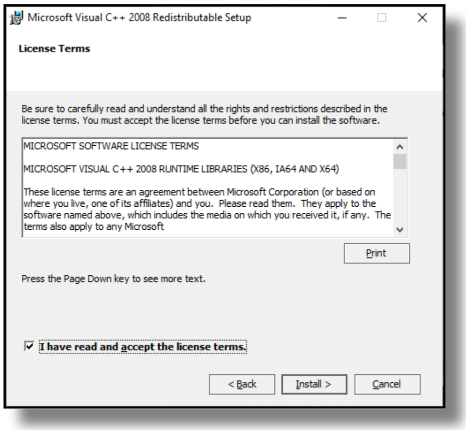


Microsoft Visual C++ 2008 Redistributable Setup

Welcome to Microsoft Visual C++ 2008 Redistributable Setup

This wizard will guide you through the installation process.

b. Select I have read and accept the license terms and click ***Install***.



Microsoft Visual C++ 2008 Redistributable Setup

License Terms

Be sure to carefully read and understand all the rights and restrictions described in the license terms. You must accept the license terms before you can install the software.

MICROSOFT SOFTWARE LICENSE TERMS

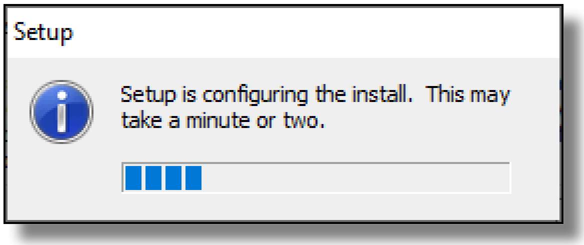
MICROSOFT VISUAL C++ 2008 RUNTIME LIBRARIES (X86, IA64 AND X64)

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft

Press the Page Down key to see more text.

☑ **I have read and accept the license terms.**

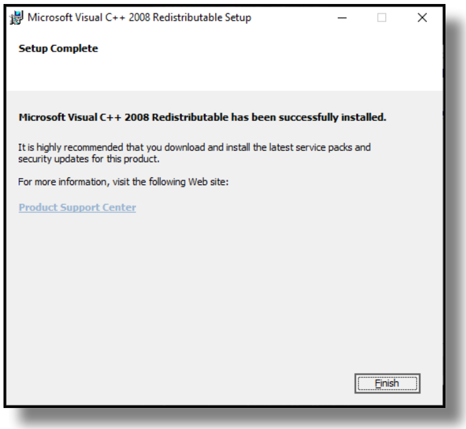
c. A progress bar will be displayed during the installation process.



Setup

Setup is configuring the install. This may take a minute or two.

d. When the process completes, a confirmation will appear. Click ***Finish***.



Microsoft Visual C++ 2008 Redistributable Setup

Setup Complete

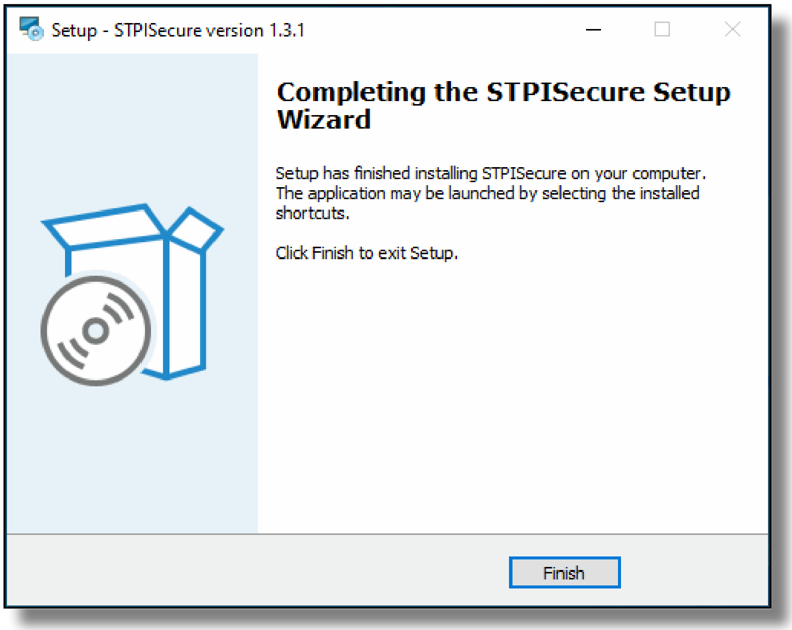
Microsoft Visual C++ 2008 Redistributable has been successfully installed.

It is highly recommended that you download and install the latest service packs and security updates for this product.

For more information, visit the following Web site:

Product Support Center

9. Once the installation completes, you will see the screen pictured below. Click the ***Finish*** button.



Setup - STPISecure version 1.3.1

Completing the STPISecure Setup Wizard

Setup has finished installing STPISecure on your computer. The application may be launched by selecting the installed shortcuts.

Click Finish to exit Setup.

This completes the installation process for the STPISecure Client software.

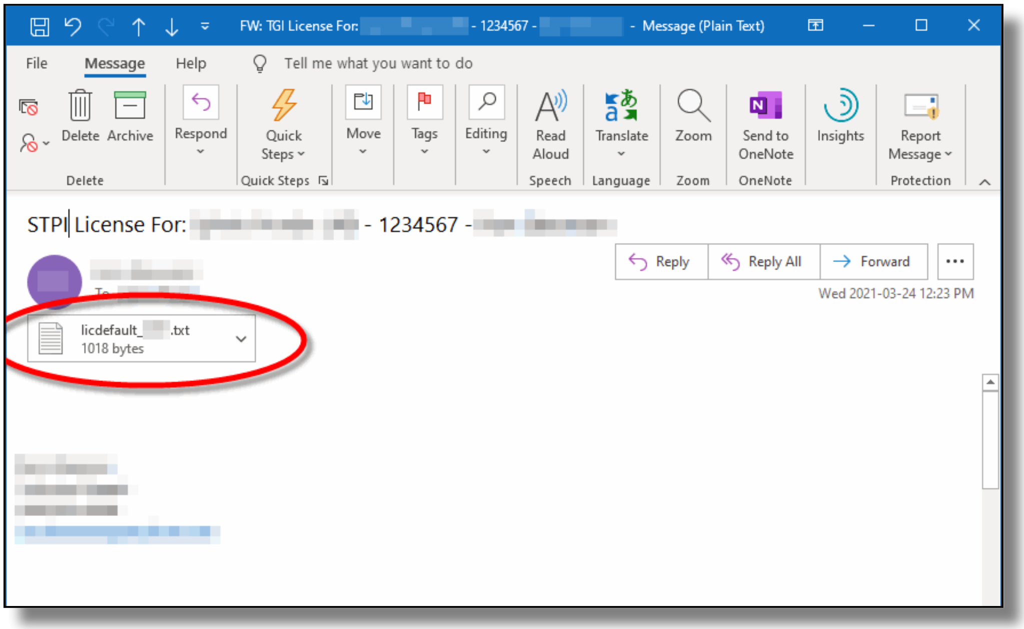
Activate the STPI Secure License

Purchasing a License

Before a license can be activated, it needs to be purchased and created for you. Please contact the PayFacto Boarding team or your local Sales Representative to purchase a STPISecure license.

STPISecure License File

After you have purchased a STPISecure license, the license file will be sent to you as a text file attachment via e-mail. The e-mail will come from the PayFacto Boarding Team or your local Sales Representative.



FW: TGI License For: [redacted] - 1234567 - [redacted] - Message (Plain Text)

STPI License For: [redacted] - 1234567 - [redacted]

[redacted]

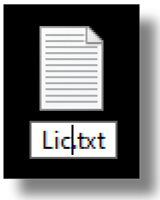
Wed 2021-03-24 12:23 PM

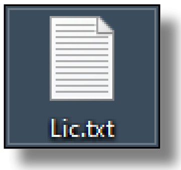
licdefault_[redacted].txt
1018 bytes

[redacted]

Install the License File

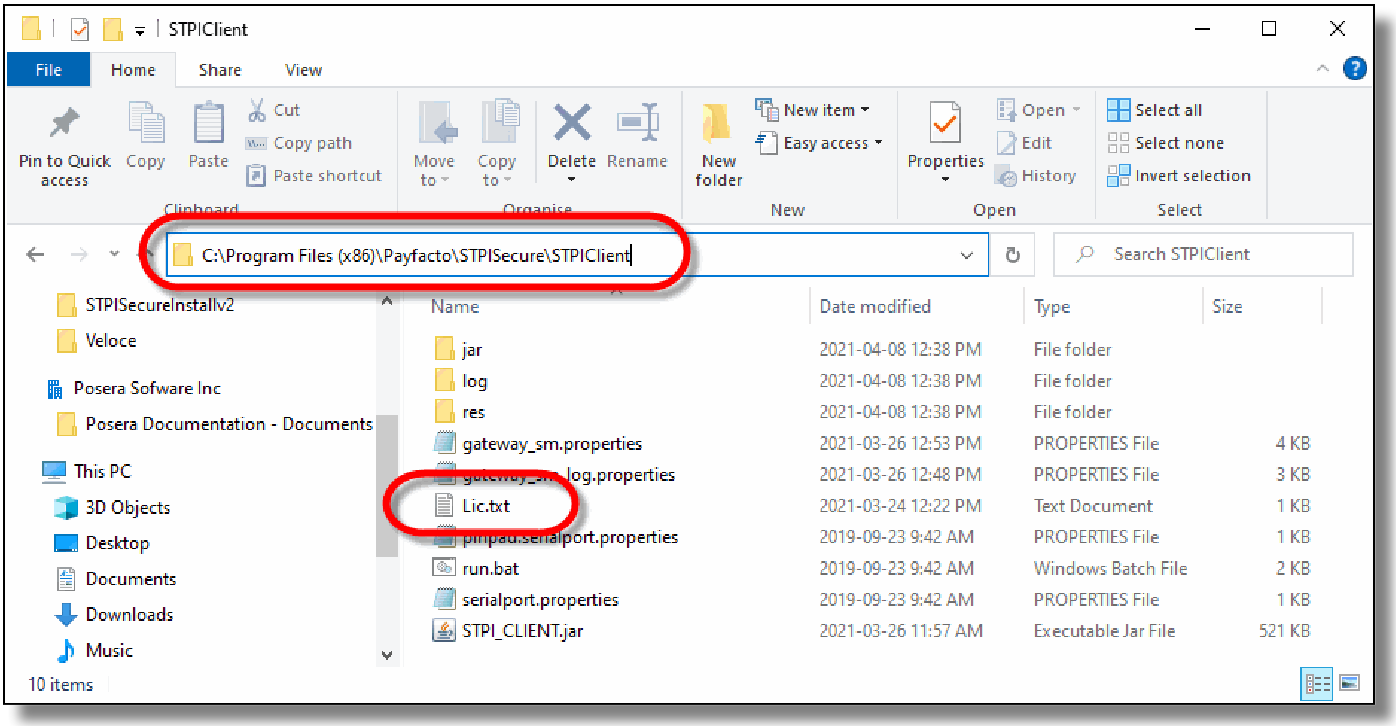
1. Save the file from the e-mail to your Windows Desktop. Typically, the file is named something like "***Licdefault_12345.txt***".
2. Rename the file to "***Lic.txt***". To achieve this, you can right-click the file and select the ***Rename*** option, or select the file and press the ***F2*** key on your keyboard.





3. Move the file to the following folder:

C:\Program Files (x86)\PayFacto\STPISecure\STPIClient\



C:\Program Files (x86)\Payfacto\STPISecure\STPIClient

Name	Date modified	Type	Size
jar	2021-04-08 12:38 PM	File folder	
log	2021-04-08 12:38 PM	File folder	
res	2021-04-08 12:38 PM	File folder	
gateway_sm.properties	2021-03-26 12:53 PM	PROPERTIES File	4 KB
gateway_sm_log.properties	2021-03-26 12:48 PM	PROPERTIES File	3 KB
Lic.txt	2021-03-24 12:22 PM	Text Document	1 KB
pinpad.serialport.properties	2019-09-23 9:42 AM	PROPERTIES File	1 KB
run.bat	2019-09-23 9:42 AM	Windows Batch File	2 KB
serialport.properties	2019-09-23 9:42 AM	PROPERTIES File	1 KB
STPI_CLIENT.jar	2021-03-26 11:57 AM	Executable Jar File	521 KB

The license activation process is now complete.

Start the STPI Client for the first time

> ! **IMPORTANT!** Before attempting to start the STPI Secure client, a license needs to be installed. Otherwise, the STPI Secure Client will attempt to start and immediately shutdown.

STPI Secure Shortcuts

After the STPISecure installation process, a folder called ***STPI Shortcuts*** was created on your Windows Desktop. This folder contains the shortcut that will be used to start the STPI Client software.

Setup the shortcut to run with Administrative privileges

To run correctly, the STPI Secure Client needs to run with Windows Administrative privileges. To achieve this:

1. From the Windows desktop, open the folder called ***STPI Shortcuts*** by double-clicking on it.

2. Two shortcuts allow you to start the STPI Client. You can use either ***STPIClient (Hidden***) or ***STPIClient***. Select the shortcut which better meets your desired use case:

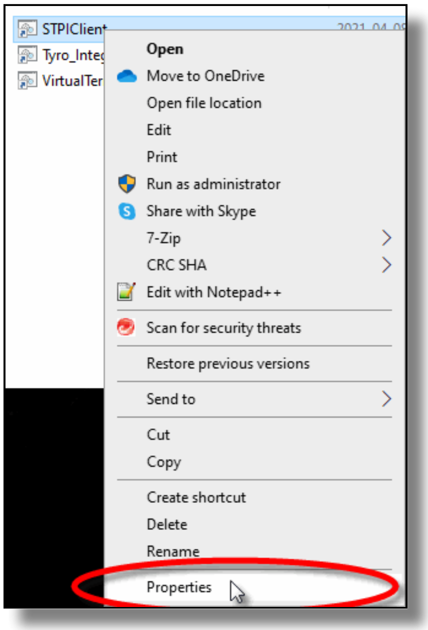
STPIClient

This shortcut makes the STPI Client run with the command prompt window visible on the screen. This takes up space on the screen and on the Windows taskbar, but allows you to see all the operations going through the STPI Client in real-time.

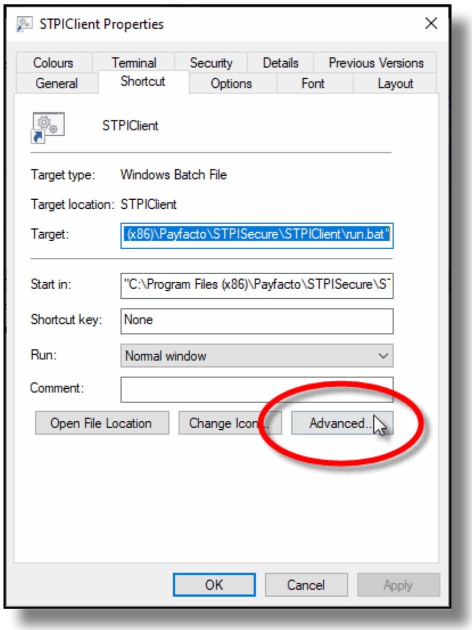
STPIClient (Hidden)

This shortcut allows the STPI Client to run with the command prompt window hidden from view. This frees up space on the screen and Windows taskbar, but the operations going through the STPI Client are not visible.

3. Right-click the shortcut called ***STPIClient*** or ***STPIClient (Hidden)***, and select the ***Properties*** option.



4. The STPIClient or STPIClient (Hidden) shortcut's properties page opens to the ***Shortcut*** tab. Click the ***Advanced...*** button.



Target type: Windows Batch File

Target location: STPIClient

Target: (x86)\Payfacto\STPISecure\STPIClient\run.bat"

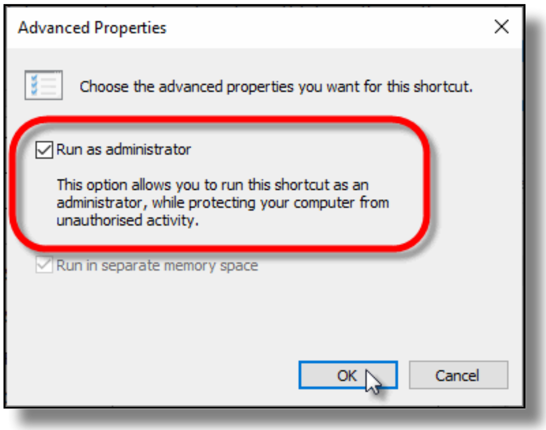
Start in: "C:\Program Files (x86)\Payfacto\STPISecure\S

Shortcut key: None

Run: Normal window

Comment:

5. Activate the ***Run as administrator*** checkbox and click ***OK***.



Advanced Properties

Choose the advanced properties you want for this shortcut.

☑ Run as administrator

This option allows you to run this shortcut as an administrator, while protecting your computer from unauthorised activity.

☑ Run in separate memory space

6. You will be back to the STPIClient (or STPIClient (Hidden)) shortcut's properties page. Click ***OK*** to close it.

With this setup, the STPI Secure client will always start with administrative privileges whenever you use this shortcut.

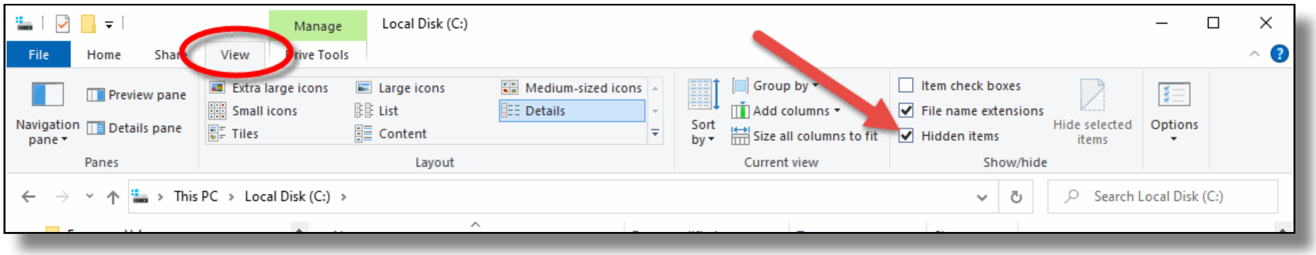
Make the STPIClient start automatically as Windows starts

IMPORTANT! If you intend to use the STPIClient as a service instead of running it as an application, please skip the rest of the instructions on this page and go directly to the Configure the STPIClient as a Service guide.

You can add a copy of the STPIClient or STPIClient (Hidden) shortcut to the Windows startup folder to force the STPI client to start automatically as Windows starts. Here is the procedure to follow with Windows 10:

1. Make sure that hidden files and folders are visible:

   a. From Windows explorer, click on the ***View*** menu and make sure that the ***Hidden Items*** option is selected from the ***Show/Hide*** section.



□ Item check boxes
☑ File name extensions
☑ Hidden items

2. Browse to the following folder:

   C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp

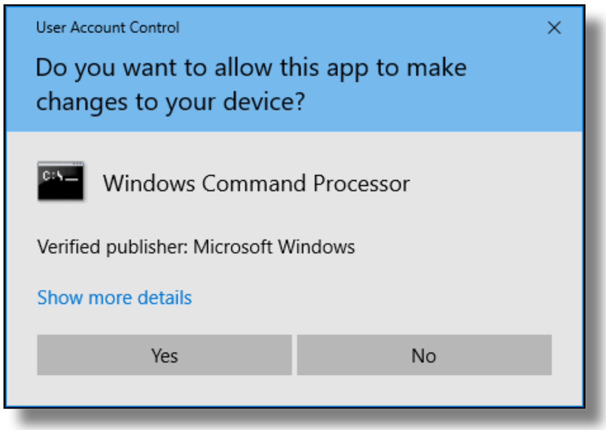
3. Copy the ***STPISecure*** or ***STPISecure (Hidden)*** shortcut to the ***StartUp*** folder.

NOTE: Be sure to apply the ***Run as administrator*** option as explained above, before copying the shortcut.

With this setup, the STPI Client application with automatically start itself if Windows is restarted.

Start the STPI Client application manually

1. Double-click the ***STPIClient*** or ***STPISecure (Hidden)*** shortcut.
2. you will see a UAC warning. Click ***Yes***.



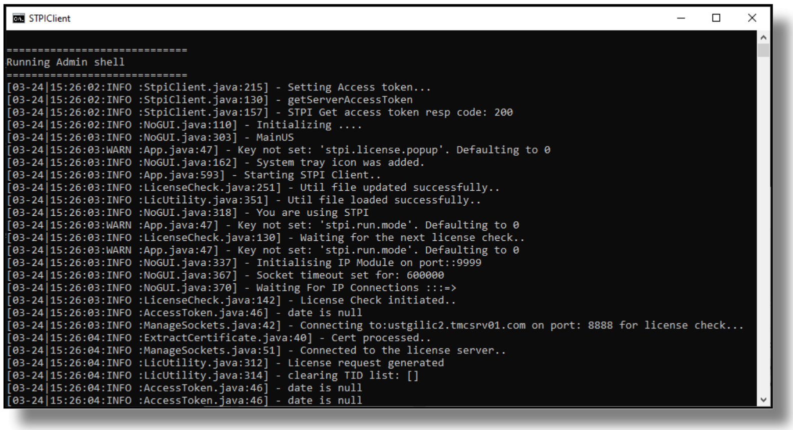
User Account Control

Do you want to allow this app to make changes to your device?

Windows Command Processor

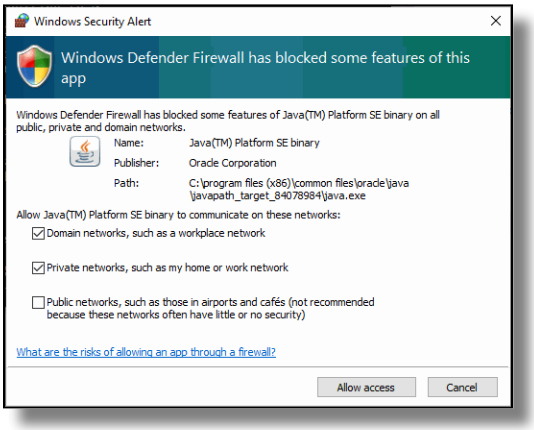
Verified publisher: Microsoft Windows

3. If you selected the regular ***STPISecure*** shortcut, a command prompt window will appear, with the ***Running Admin shell*** header. You will see text scrolling on the window. If you used the ***STPISecure (Hidden)*** instead, you will not see this window and skip directly to the next step.



```
=============================
Running Admin shell
=============================
[03-24|15:26:02:INFO :StpiClient.java:215] - Setting Access token...
[03-24|15:26:02:INFO :StpiClient.java:130] - getServerAccessToken
[03-24|15:26:02:INFO :StpiClient.java:157] - STPI Get access token resp code: 200
[03-24|15:26:02:INFO :NoGUI.java:110] - Initializing ....
[03-24|15:26:03:INFO :NoGUI.java:303] - MainUS
[03-24|15:26:03:WARN :App.java:47] - Key not set: 'stpi.license.popup'. Defaulting to 0
[03-24|15:26:03:INFO :NoGUI.java:162] - System tray icon was added.
[03-24|15:26:03:INFO :App.java:593] - Starting STPI Client..
[03-24|15:26:03:INFO :LicenseCheck.java:251] - Util file updated successfully..
[03-24|15:26:03:INFO :LicUtility.java:351] - Util file loaded successfully..
[03-24|15:26:03:INFO :NoGUI.java:318] - You are using STPI
[03-24|15:26:03:WARN :App.java:47] - Key not set: 'stpi.run.mode'. Defaulting to 0
[03-24|15:26:03:INFO :LicenseCheck.java:130] - Waiting for the next license check..
[03-24|15:26:03:WARN :App.java:47] - Key not set: 'stpi.run.mode'. Defaulting to 0
[03-24|15:26:03:INFO :NoGUI.java:337] - Initialising IP Module on port::9999
[03-24|15:26:03:INFO :NoGUI.java:367] - Socket timeout set for: 600000
[03-24|15:26:03:INFO :NoGUI.java:370] - Waiting For IP Connections :::=>
[03-24|15:26:03:INFO :LicenseCheck.java:142] - License Check initiated..
[03-24|15:26:03:INFO :AccessToken.java:46] - date is null
[03-24|15:26:03:INFO :ManageSockets.java:42] - Connecting to:ustgilic2.tmcsrv01.com on port: 8888 for license check...
[03-24|15:26:04:INFO :ExtractCertificate.java:40] - Cert processed..
[03-24|15:26:04:INFO :ManageSockets.java:51] - Connected to the license server..
[03-24|15:26:04:INFO :LicUtility.java:312] - License request generated
[03-24|15:26:04:INFO :LicUtility.java:314] - clearing TID list: []
[03-24|15:26:04:INFO :AccessToken.java:46] - date is null
[03-24|15:26:04:INFO :AccessToken.java:46] - date is null
```

4. The very first time the STPIClient starts, you will see a ***Windows Security Alert*** from the ***Windows Defender Firewall***.



Windows Security Alert

Windows Defender Firewall has blocked some features of this app

Windows Defender Firewall has blocked some features of Java(TM) Platform SE binary on all public, private and domain networks.

Name: Java(TM) Platform SE binary

Publisher: Oracle Corporation

Path: C:\program files (x86)\common files\oracle\java\javapath_target_84078984\java.exe

Allow Java(TM) Platform SE binary to communicate on these networks:

☑ Domain networks, such as a workplace network

☑ Private networks, such as my home or work network

□ Public networks, such as those in airports and cafés (not recommended because these networks often have little or no security)

What are the risks of allowing an app through a firewall?

   a. Enable the ***Domain networks, such as a workplace network*** option (available only if your PC is part of an Active Directory domain).

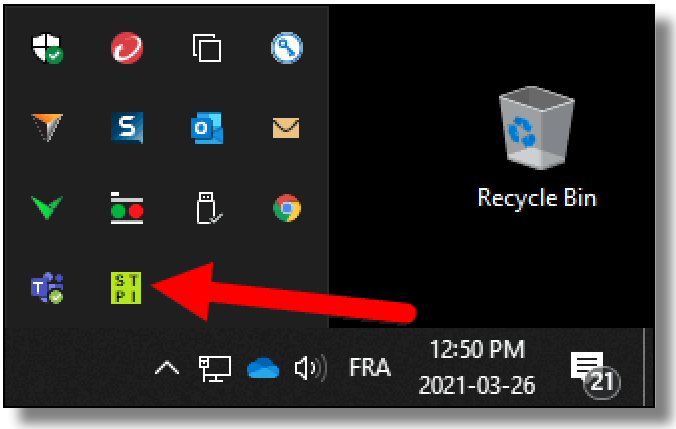
   b. Enable the ***Private networks, such as my home or work network*** option.

   c. Disable the ***Public networks*** option.

   d. Click ***Allow access***.

5. If you selected the ***STPISecure*** shortcut, the command prompt window will remain on the screen. You may minimize it, but do not close it.

6. An icon will also be added to the Windows system tray.

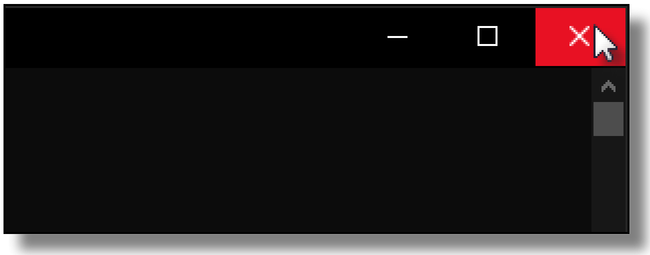


Stopping the STPI Client application

> **IMPORTANT!** Stopping the STPI Client application will prevent payment terminals using SecureTable from processing transactions. Only stop the STPI Client for troubleshooting purposes.

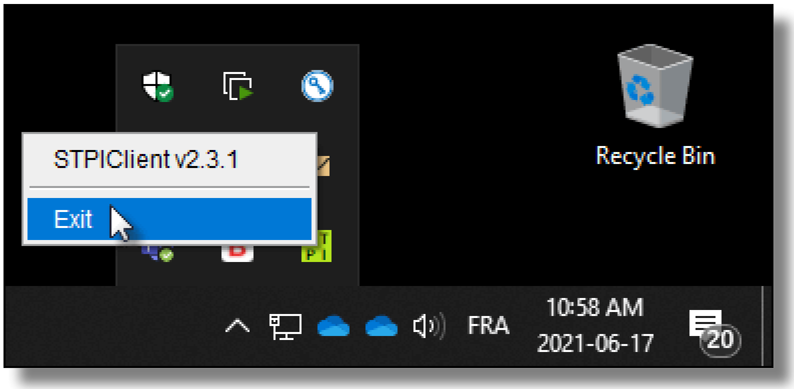
Closing the command prompt window

If you are using the ***STPISecure*** shortcut, simply close the command prompt window by clicking the "X" in the upper-right corner.



Using the system tray icon

You can also right-click the STPI icon in the system tray and select the ***Exit*** option.



Congratulations!

The STPI Client software is now up-and-running on your system.

Configure the STPI Client as a Service

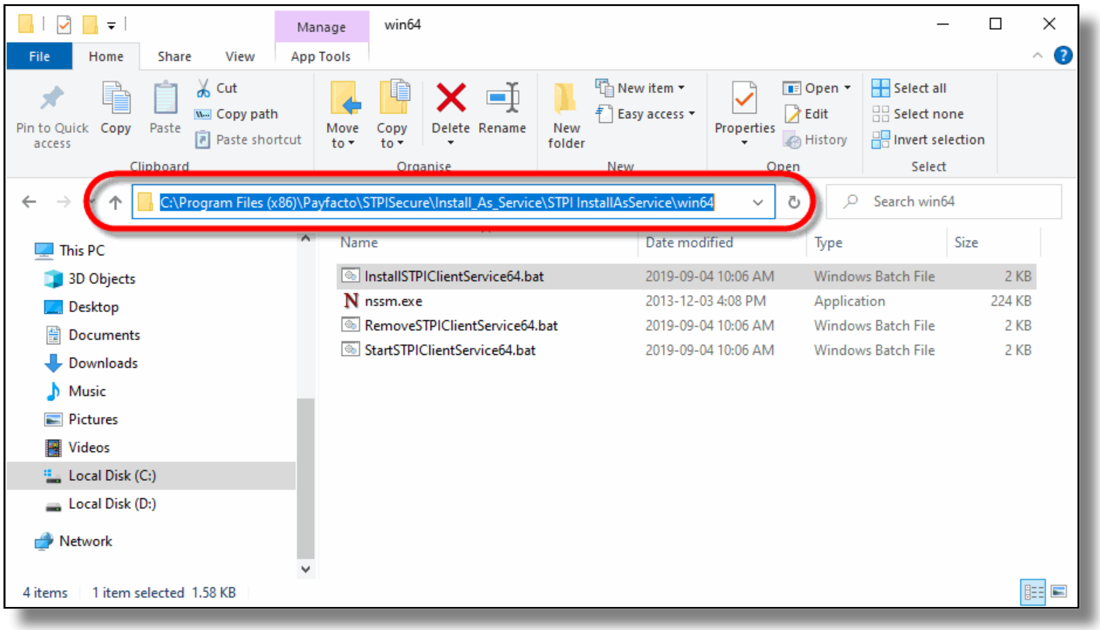
This step is required to have the STPISecure client start automatically when Windows starts, and have it run silently in the background.

IMPORTANT! If you have already configured the STPIClient application shortcut to start automatically with Windows by copying its shortcut to the Windows StartUp folder, be sure to un-do this configuration before proceeding further.

1. Using Windows Explorer, browse to:

   C:\Program Files (x86)\PayFacto\STPISecure\Install_As_Service\STPI InstallAsService

   Depending on your operating system, select the ***Win64*** folder for 64-bit versions of Windows or ***Win32*** for 32-bit versions of Windows.

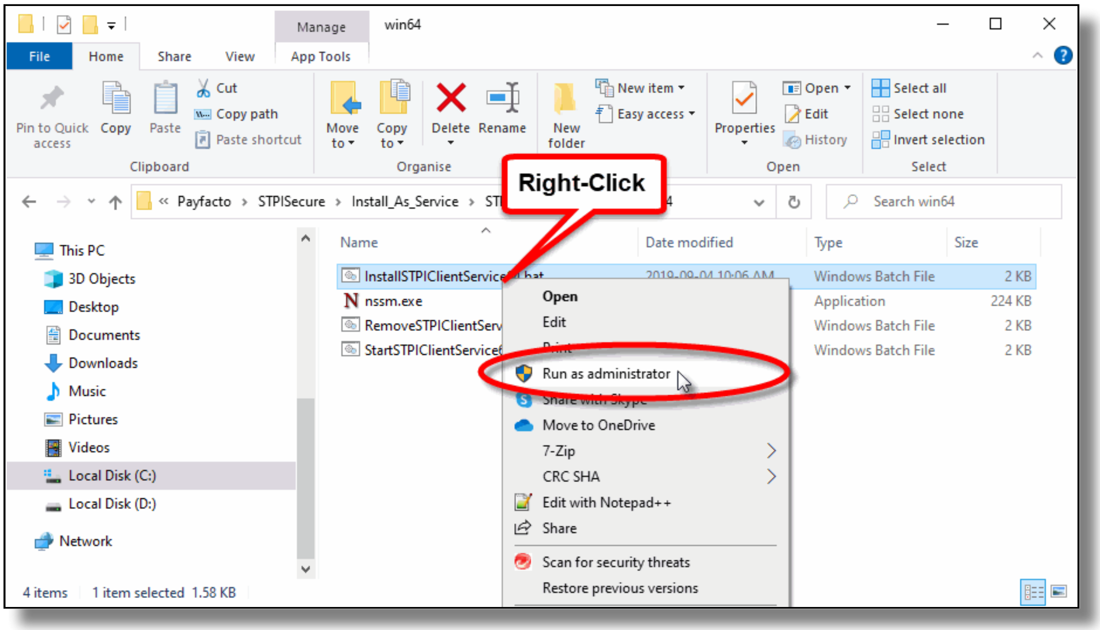


C:\Program Files (x86)\Payfacto\STPISecure\Install_As_Service\STPI InstallAsService\win64

Name	Date modified	Type	Size
InstallSTPIClientService64.bat	2019-09-04 10:06 AM	Windows Batch File	2 KB
nssm.exe	2013-12-03 4:08 PM	Application	224 KB
RemoveSTPIClientService64.bat	2019-09-04 10:06 AM	Windows Batch File	2 KB
StartSTPIClientService64.bat	2019-09-04 10:06 AM	Windows Batch File	2 KB

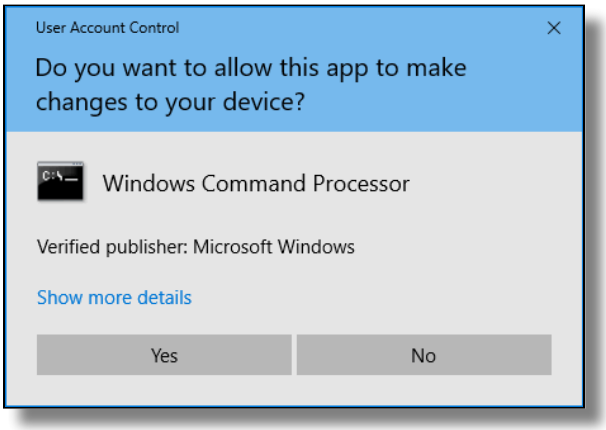
4 items 1 item selected 1.58 KB

2. Locate the file called ***InstallTGIClientService64.bat*** (for 64-bit Windows) or ***InstallTGIClientService32.bat*** (for 32-bit Windows). Right-click the file and select ***Run as administrator***.



Name	Date modified	Type	Size
InstallSTPIClientService...bat	2019-09-04 10:06 AM	Windows Batch File	2 KB
nssm.exe		Application	224 KB
RemoveSTPIClientServ...		Windows Batch File	2 KB
StartSTPIClientService...		Windows Batch File	2 KB

3. You may see a UAC prompt. Click ***Yes***.

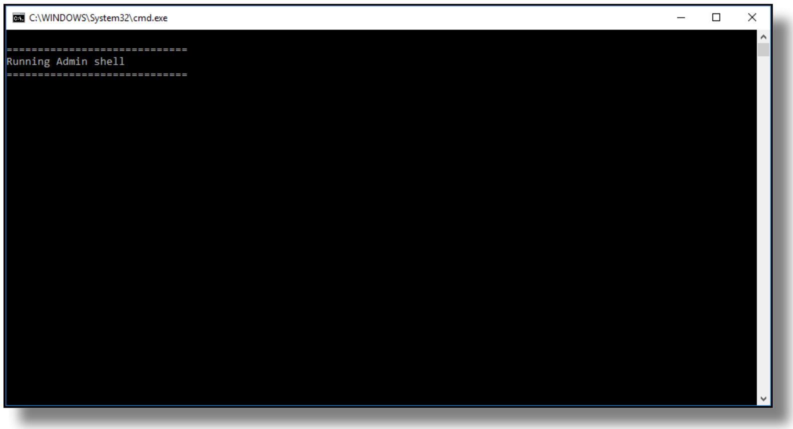

User Account Control

Do you want to allow this app to make changes to your device?

Windows Command Processor

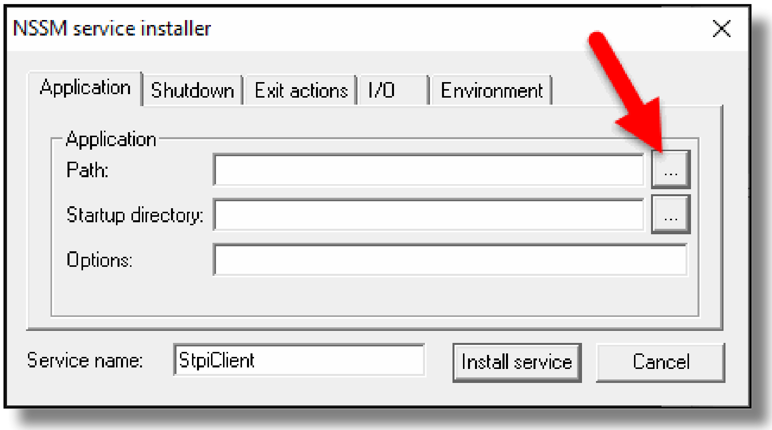
Verified publisher: Microsoft Windows

4. A command prompt window saying ***Running admin shell*** will appear. Leave it there. Do not close it.



```
===========================
Running Admin shell
===========================
```

5. The ***MSSM*** service installer window will open. Click the browse button (3 dots) next to the ***Path*** field:

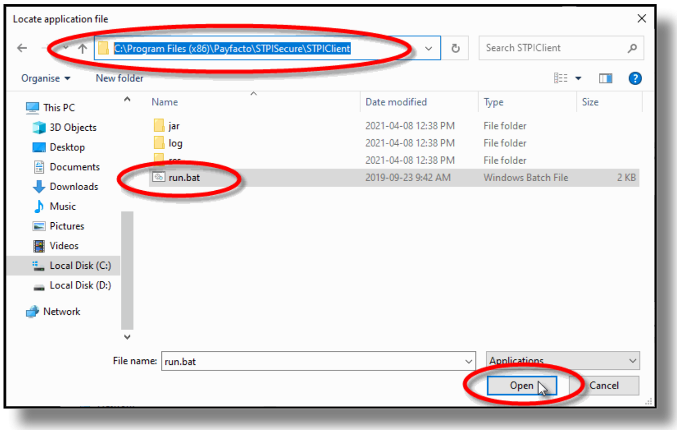


Service name: StpiClient

6. In the ***Locate Application File*** window, browse to:

   C:\Program Files (x86)\PayFacto\STPISecure\STPIClient\

   Select the ***Run.bat*** file and click ***Open***.

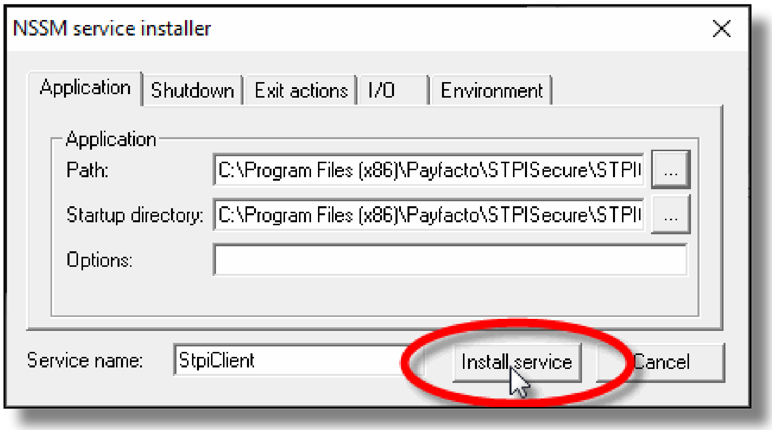


C:\Program Files (x86)\Payfacto\STPISecure\STPIClient

Name	Date modified	Type	Size
jar	2021-04-08 12:38 PM	File folder	
log	2021-04-08 12:38 PM	File folder	
res	2021-04-08 12:38 PM	File folder	
run.bat	2019-09-23 9:42 AM	Windows Batch File	2 KB

File name: run.bat

7. You will be taken back to the MSSN service Installer window. Click the ***Install Service*** button.

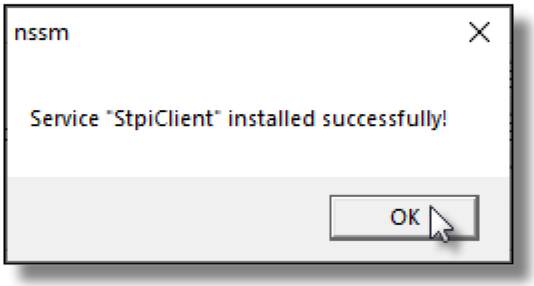


Path: C:\Program Files (x86)\Payfacto\STPISecure\STPI(

Startup directory: C:\Program Files (x86)\Payfacto\STPISecure\STPI(

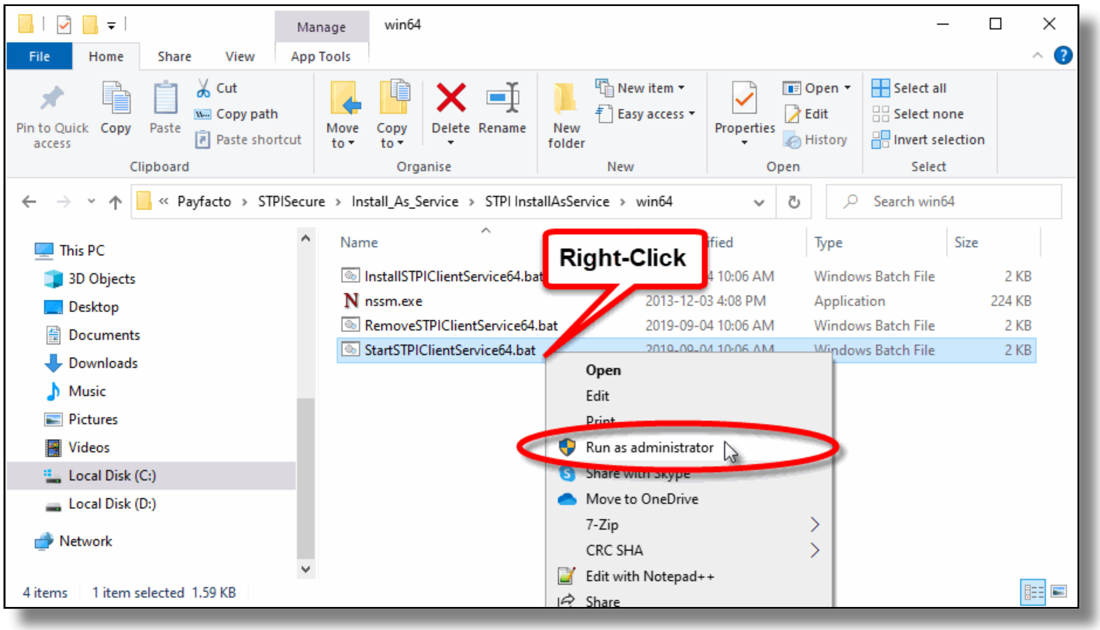
Service name: StpiClient

8. A confirmation message will appear. Click ***OK***.



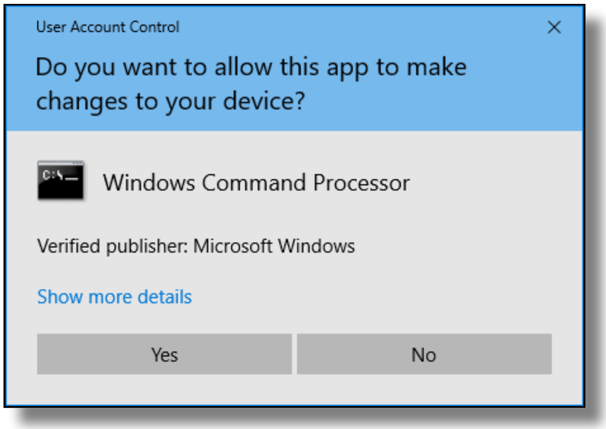
Service "StpiClient" installed successfully!

9. Locate the file called ***StartSTPIClientService64.bat*** (for 64-bit Windows) or ***StartSTPIClientService32.bat*** (for 32-bit Windows). Right-click the file and select ***Run as administrator***.



Name	Date modified	Type	Size
InstallSTPIClientService64.bat	4 10:06 AM	Windows Batch File	2 KB
nssm.exe	2013-12-03 4:08 PM	Application	224 KB
RemoveSTPIClientService64.bat	2019-09-04 10:06 AM	Windows Batch File	2 KB
StartSTPIClientService64.bat	2019-09-04 10:06 AM	Windows Batch File	2 KB

10. You may see a UAC prompt. Click ***Yes***.



User Account Control

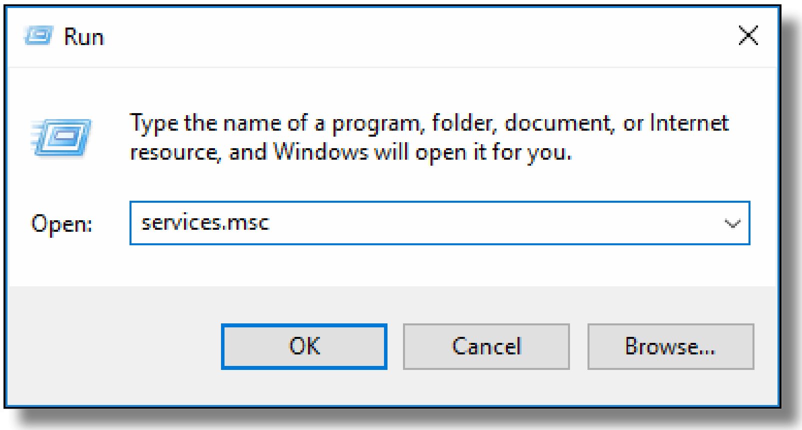
Do you want to allow this app to make changes to your device?

Windows Command Processor

Verified publisher: Microsoft Windows

Verify that the service is running properly

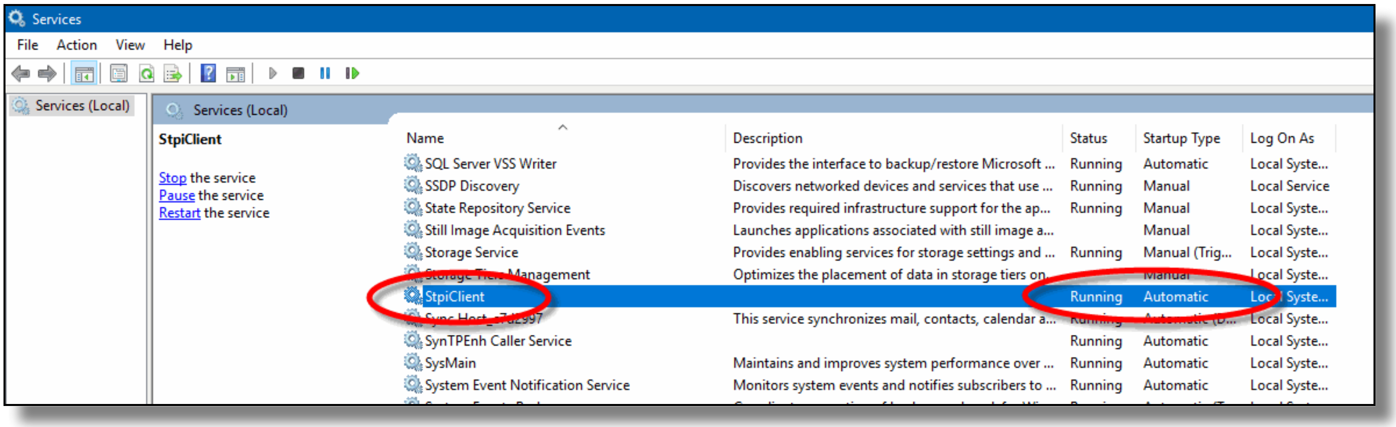
1. To verify that the service is started properly, right-click the Windows start button and select the ***Run...*** option. You can also press the ***Windows key + R*** on your keyboard. In the ***Open:*** box, type ***services.msc*** and click ***OK***.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: services.msc

2. In the services list, look for the ***StpiClient*** service. The Status should be ***Running*** and the Startup Type should be ***Automatic***.



StpiClient

Stop the service
Pause the service
Restart the service

Name	Description	Status	Startup Type	Log On As
SQL Server VSS Writer	Provides the interface to backup/restore Microsoft ...	Running	Automatic	Local Syste...
SSDP Discovery	Discovers networked devices and services that use ...	Running	Manual	Local Service
State Repository Service	Provides required infrastructure support for the ap...	Running	Manual	Local Syste...
Still Image Acquisition Events	Launches applications associated with still image a...		Manual	Local Syste...
Storage Service	Provides enabling services for storage settings and ...	Running	Manual (Trig...	Local Syste...
Storage Tiers Management	Optimizes the placement of data in storage tiers on...		Manual	Local Syste...
StpiClient		Running	Automatic	Local Syste...
Sync Host_e7d2997	This service synchronizes mail, contacts, calendar a...	Running	Automatic (D...	Local Syste...
SynTPEnh Caller Service		Running	Automatic	Local Syste...
SysMain	Maintains and improves system performance over ...	Running	Automatic	Local Syste...
System Event Notification Service	Monitors system events and notifies subscribers to ...	Running	Automatic	Local Syste...

Test automatic startup

At this point, it is good practice to test your system to make sure it will recover properly in case of an unexpected restart. To do this, simply restart the PC and log back on.

From there, make sure that the STPIClient service is running by looking at the Windows services as described above.

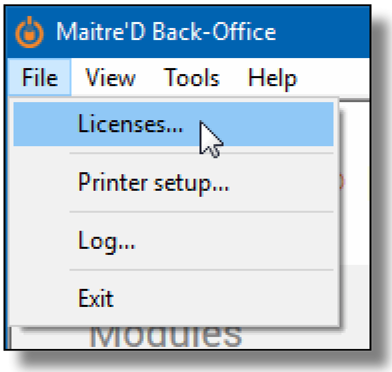
Congratulations!

The STPI Client is now up-and-running. It is also properly configured as a service and will start automatically in the background whenever Windows restarts.

Maitre'D Electronic Funds Transfer Module Setup

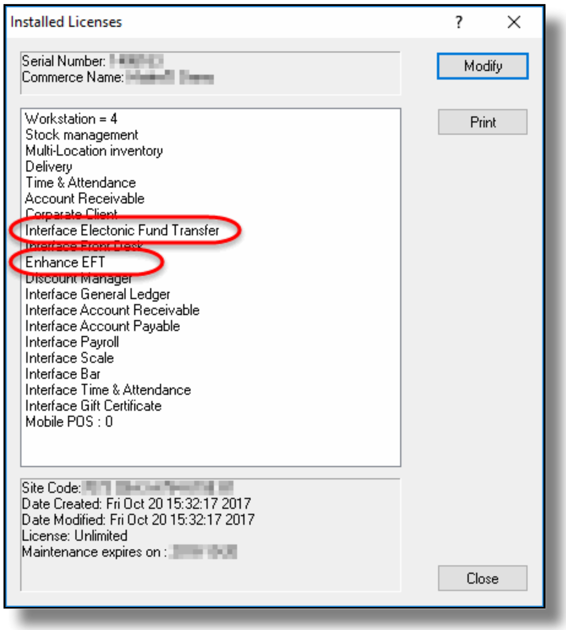
Verify the Maitre’D license

Make sure that the Maitre’D ***Electronic Funds Transfer Interface*** and ***Enhanced EFT*** options are included on the Maitre’D license. To confirm this, simply logon to the Maitre’D Back-Office using appropriate credentials, click on the ***File*** menu and select the ***Licenses*** option.



This will bring up the license’s properties. Two options are required for SecureTable to operate properly:

- ***Interface Electronic Fund Transfer.***
- ***Enhanced EFT.***



Serial Number: [redacted]
Commerce Name: [redacted]

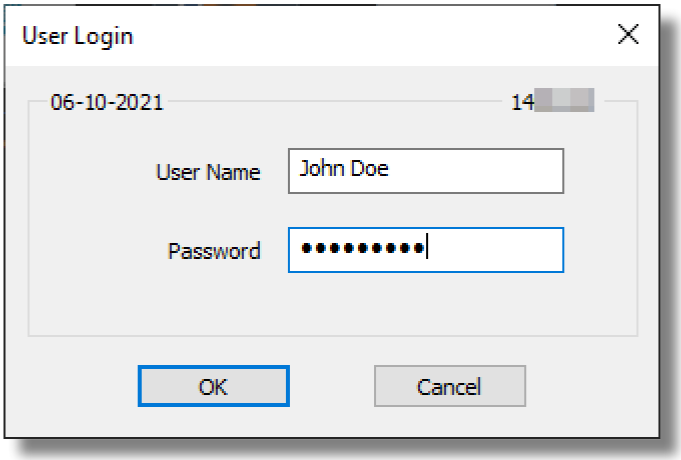
Workstation = 4
Stock management
Multi-Location inventory
Delivery
Time & Attendance
Account Receivable
Corporate Client
Interface Electonic Fund Transfer
Interface Front Desk
Enhance EFT
Discount Manager
Interface General Ledger
Interface Account Receivable
Interface Account Payable
Interface Payroll
Interface Scale
Interface Bar
Interface Time & Attendance
Interface Gift Certificate
Mobile POS : 0

Site Code: [redacted]
Date Created: Fri Oct 20 15:32:17 2017
Date Modified: Fri Oct 20 15:32:17 2017
License: Unlimited
Maintenance expires on : [redacted]

If any of these two options are missing, they will need to be purchased before you can use SecureTable. Please contact your local sales representative.

Electronic Funds Transfer (EFT) Interface setup

1. Logon to the Maitre'D Back-Office with appropriate credentials. (Distributor or System Owner)

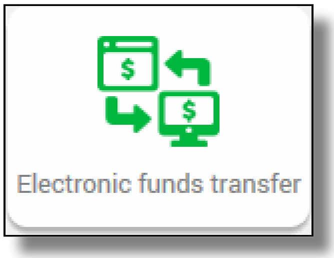

User Login

06-10-2021 14[redacted]

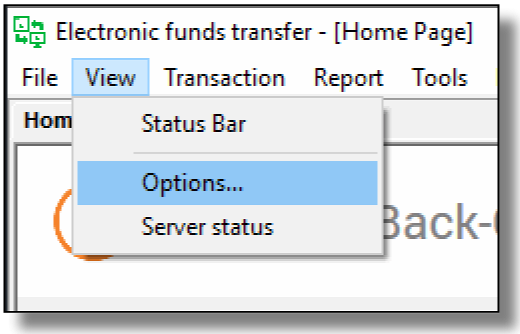
User Name: John Doe

Password: ••••••••••

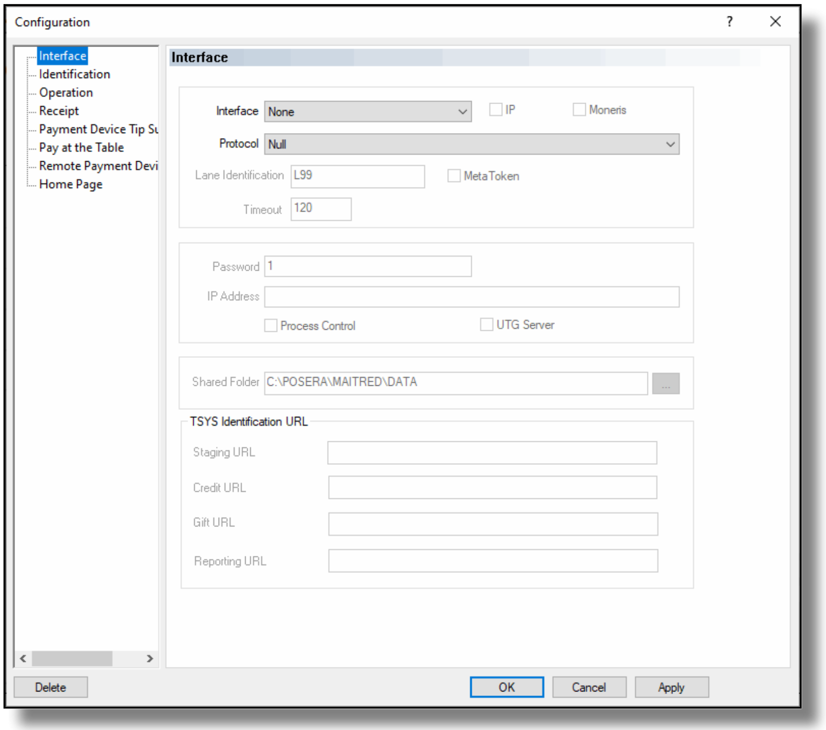
2. Start the ***Electronic Funds Transfer*** Module.



3. Click the ***View*** menu, and select ***Options…***


Electronic funds transfer - [Home Page]

4. The Configuration screen opens on the ***Interface*** branch.



Interface

Interface: None
□ IP
□ Moneris
Protocol: Null
Lane Identification: L99
□ Meta Token
Timeout: 120

Password: 1
IP Address:
□ Process Control
□ UTG Server

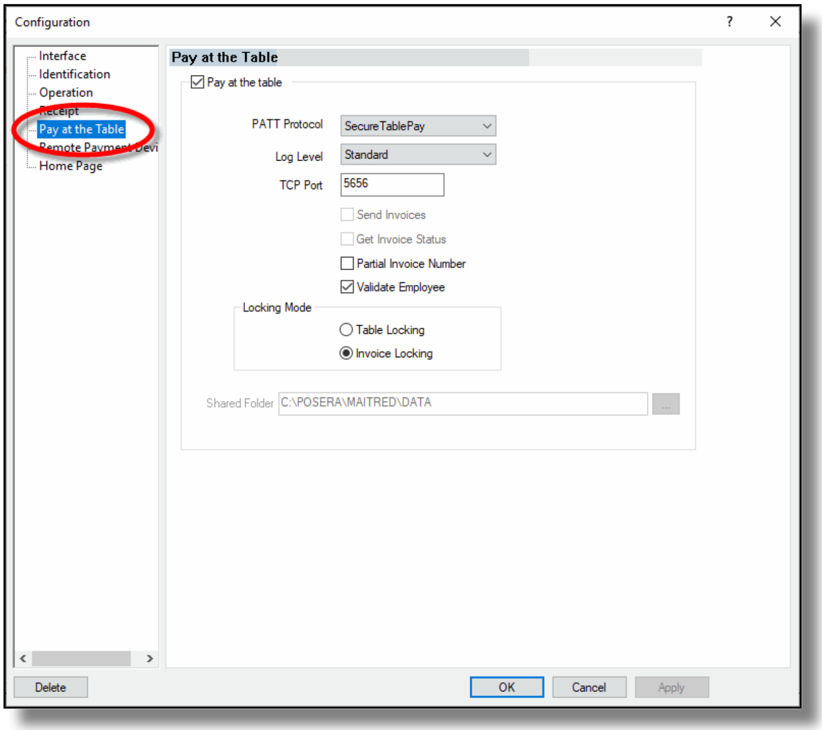
Shared Folder: C:\POSERA\MAITRED\DATA

TSYS Identification URL
Staging URL:
Credit URL:
Gift URL:
Reporting URL:

5. The settings from the ***Interface***, ***Identification***, ***Operation, Receipt***, ***Payment Device Tip Suggestion***, ***Remote Payment Device*** and ***Home Page*** branches don't have any effect on the operation of SecureTable. Please make sure not to change or remove any settings found in these pages, as these could affect the operation of tethered payment terminals.

NOTE: It is possible to use tethered payment terminals from a third-party processor along with SecureTable. The settings in these windows would then be setup per your processor's requirements.

6. Click on the ***Pay at the Table*** branch.



Pay at the Table

☑ Pay at the table

PATT Protocol: SecureTablePay

Log Level: Standard

TCP Port: 5656

□ Send Invoices

□ Get Invoice Status

□ Partial Invoice Number

☑ Validate Employee

Locking Mode

○ Table Locking

● Invoice Locking

Shared Folder: C:\POSERA\MAITRED\DATA

Pay at the table

Enable this option to activate Pay at the Table (PATT) functionality.

PATT Protocol

Select the ***SecureTablePay*** protocol.

Log Level

Select the desired log level for the Pay at the Table interface. Available choices are:

- ***None***: No log file is created.
- ***Standard***: Standard log level. All operations are logged in a summary format.
- ***Detailed***: Detailed log level. All operations are logged with detailed information.
- ***Debug***: Detailed log level with extra information for troubleshooting and investigation purposes.

TCP Port

Type in the TCP Port number used by the STPI Secure client.

Send Invoices

Disabled. This option is not available because it is not compatible with the SecureTablePay protocol.

Get Invoice Status

Disabled. This option is not available because it is not compatible with the SecureTablePay protocol.

Partial Invoice Number

Enable this option to allow the payment terminal to retrieve checks by entering only the last 4 digits of the check number. If this option is disabled, the full check number will be required to retrieve checks.

Validate Employee

Enable this option to force the validation of the employee number entered at the payment terminal. With this option enabled, only the employee who owns the table associated with the printed check will be able to access that check from the payment terminal. If this option is disabled, any employee will be able to access any checks from the payment terminal.

Locking mode

Select the locking mode that will be used when accessing checks from the payment terminal. Two locking modes are available:

Table Locking

Select the table locking mode to lock the entire table as soon as a check is accessed by a payment terminal with SecureTable. For example, if you have 4 printed checks on Table #99, accessing any check from table #99 from a payment terminal with SecureTable will lock all checks from table #99. This prevents any of these checks from being accessed by other payment terminals or POS workstations.

Invoice Locking

Select the invoice locking option to lock only the check being accessed, without locking the entire table. This allows other checks on a given table to be closed simultaneously with other payment terminals or from POS workstations.

Shared Folder

This option is not available because it is not compatible with the SecureTablePay protocol.

7. Click ***OK*** to save changes and close the options window.

Note on locking (Table locking or invoice locking)

As soon as a table or invoice is accessed from a payment terminal with SecureTable, it is locked. This is done to prevent accidental double payment or double processing of invoices. While it is possible to override table or invoice locking, it is not recommended to do so. Unlocking a table or invoice in the middle of it being processed can cause invoices to remain open after being paid and discrepancies in reporting.

Media Type mappings for SecureTable or SecurePay

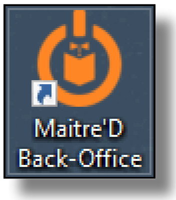
Before you begin

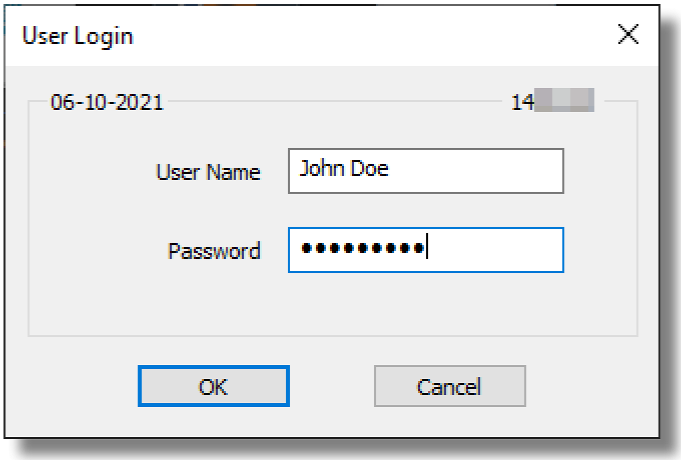
In order to get accurate reporting data with SecureTable or SecurePay, media types known as mappings need to be created for each card brand that will be accepted by the merchant. Before beginning, gather information on all the card brands and payment types that are accepted at the restaurant. Obtain this information from the restaurant owner and managers, and from the restaurant's credit card processor.

> **NOTE:** SecureTable and SecurePay can be used at the same time on the same POS system. Therefore, the merchant can have any combination of stationary terminals using SecurePay and mobile terminals using SecureTable. Both types of terminals will share the same media type mappings.

Creating mappings for each card brand

1. Logon to the Maitre'D Back-Office with appropriate credentials. (Distributor or System Owner)



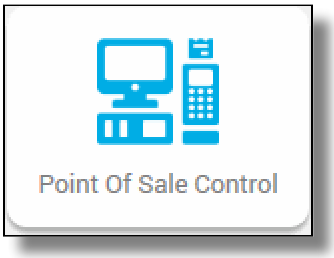

User Login

06-10-2021 14[redacted]

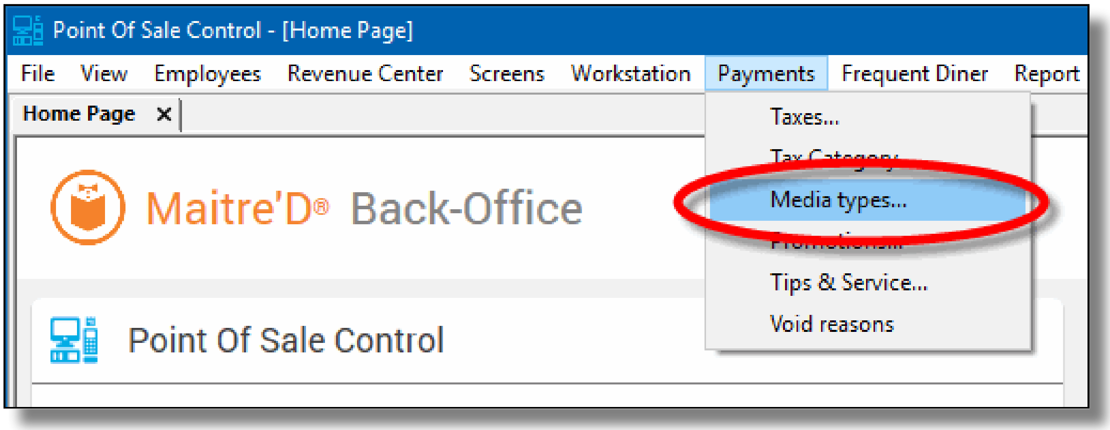
User Name: John Doe

Password: ••••••••••

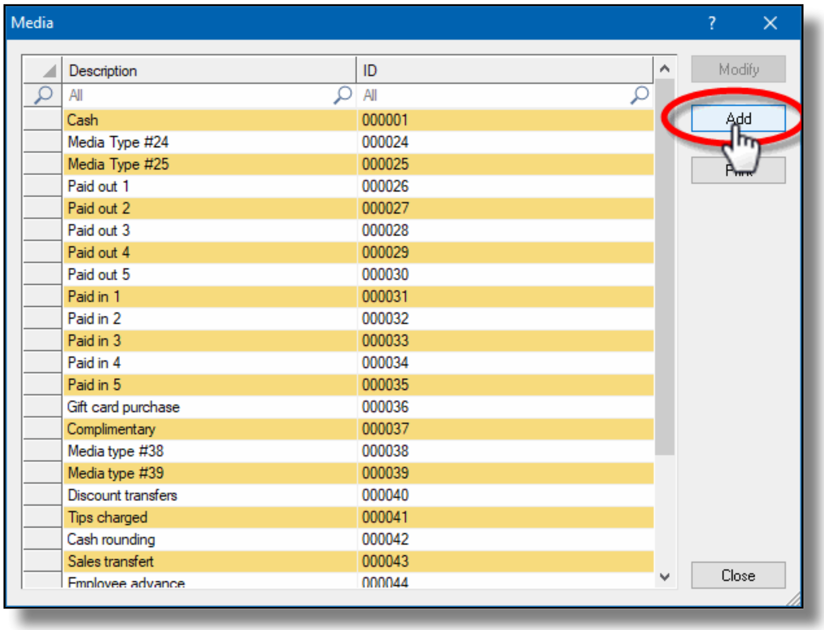
2. Start the ***Point of Sale Control*** Module.



3. Click the ***Payments*** menu, and select the ***Media Types...*** option.

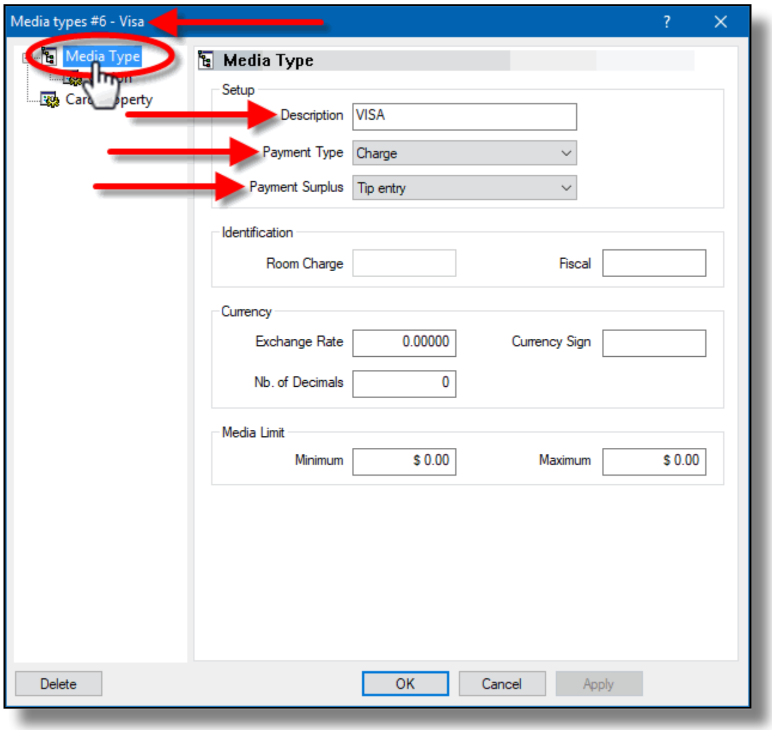


4. The list of all current media types will be displayed. Click the ***Add*** button.



Description	ID
All	All
Cash	000001
Media Type #24	000024
Media Type #25	000025
Paid out 1	000026
Paid out 2	000027
Paid out 3	000028
Paid out 4	000029
Paid out 5	000030
Paid in 1	000031
Paid in 2	000032
Paid in 3	000033
Paid in 4	000034
Paid in 5	000035
Gift card purchase	000036
Complimentary	000037
Media type #38	000038
Media type #39	000039
Discount transfers	000040
Tips charged	000041
Cash rounding	000042
Sales transfert	000043
Employee advance	000044

5. A blank Media Type window will open directly on the ***Media Type*** branch. Configure according to the information below:



Media types #6 - Visa

Media Type

Setup

Description: VISA

Payment Type: Charge

Payment Surplus: Tip entry

Identification

Room Charge:

Fiscal:

Currency

Exchange Rate: 0.00000

Currency Sign:

Nb. of Decimals: 0

Media Limit

Minimum: $ 0.00

Maximum: $ 0.00

Media Type ID

The Media Type ID number is automatically determined by Maitre'D when the Media Type is created. Maitre'D will always use the lowest available number between #2 and #23 inclusively.

Description

Enter a meaningful description for this media type. This should generally be a card brand name such as Visa, MasterCard, AMEX, etc. This description will be shown on customer receipts and media reports.

Payment Type

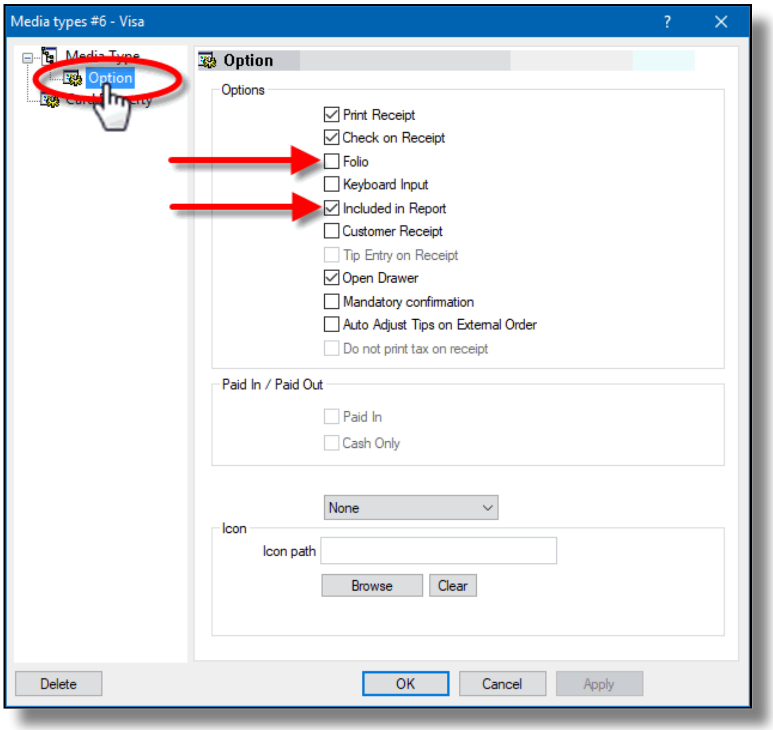
Select the ***Charge*** option from the drop-down list.

Payment Surplus

- Select ***Tip Entry*** if the merchant accepts tips for servers.
- Select ***NULL*** if the merchant does not accept tips.

Configure remaining options per the merchant's needs and preferences.

6. Click on the ***Option*** branch.



Option

Options

☑ Print Receipt
☑ Check on Receipt
☐ Folio
☐ Keyboard Input
☑ Included in Report
☐ Customer Receipt
☐ Tip Entry on Receipt
☑ Open Drawer
☐ Mandatory confirmation
☐ Auto Adjust Tips on External Order
☐ Do not print tax on receipt

Paid In / Paid Out

☐ Paid In
☐ Cash Only

None

Icon

Icon path

Print Receipt (Optional)

Enable this option to allow for a receipt to be printed after the transaction has been processed.

Check on Receipt (Optional)

Enable this option to have the detailed check print on the receipt.

Folio

Disabled. This option needs to be disabled for cards to be read properly.

Keyboard Input

Disabled. This option cannot be used since the ***Folio*** option above also needs to be disabled.

Included in Report

Enable this option so that this media type is shown in Back-Office reports (Recommended). Disabling this option will cause this media type to be hidden in the reports (NOT recommended).

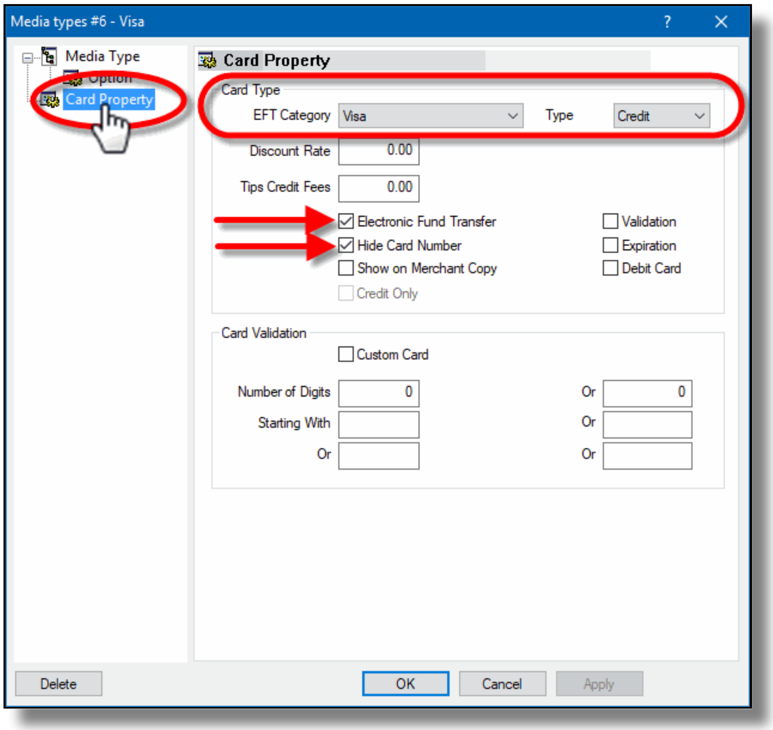
Open Drawer (Optional)

Enable this option to make the cash drawer open when this media type is used.

NOTE: ***Print Receipt***, ***Check on Receipt*** and ***Open Drawer*** options have no effect on wireless payment terminals using SecureTable. However, payment terminals with SecurePay will be affected.

Configure remaining options per the merchant's needs and preferences.

7. Click on the ***Card Property*** branch.



Card Property

Card Type

EFT Category: Visa

Type: Credit

Discount Rate: 0.00

Tips Credit Fees: 0.00

☑ Electronic Fund Transfer
☑ Hide Card Number
□ Show on Merchant Copy
□ Credit Only
□ Validation
□ Expiration
□ Debit Card

Card Validation

□ Custom Card

Number of Digits: 0 Or: 0

Starting With: Or:

Or: Or:

EFT Category

Set this drop-down list to whichever card brand that needs to be mapped to this media type.

Type

This drop-down list is used to determine the type of payment for the purpose of Sales Recording Modules and fiscal printers. The available settings are described below.

Cash

Select the Cash option for the default cash payment and any other payment involving cash, such as foreign currencies.

Credit

Select this option for all credit card payments.

Debit

Select this option for U.S. Debit and Canadian debit (Interac) payments.

Other

Select this option for all payments which do not fall in any of the above categories. Gift card purchases and Gift Card redeem are common examples of media types where ***Other*** needs to be selected.

Discount Rate

This option is not supported with EMV protocols and semi-integrated protocols like SecureTable or SecurePay. Leave this value at 0.00.

Tips Credit Fees

Enter the percentage of tips paid to the waiters that will be withheld to cover for fees charged by payment processors. If you do not wish to use this feature, leave it at 0.00.

NOTE: Some jurisdictions don't allow transaction or credit card processing fees to be passed down to employees. Please verify your local regulations before using this feature.

Electronic Funds Transfer

Enable this option. This option needs to be enabled to block operations that are not compatible with EMV payments, such as Cancel/Reopen Check.

Hide Card Number

This option automatically becomes enabled when Electronic Funds Transfer is enabled. Leave it enabled.

Show on Merchant Copy

Disable this option. This option was used by older, non-integrated protocols and caused the credit card number to be printed on the merchant copy of EFT transaction records. This option has no effect with any Electronic Funds Transfer protocol, semi-integrated protocols, SecureTable or SecurePay.

Credit Only

This option is not usable (grayed-out) with most EFT protocols. It is only used with the Datacap - DSIEMVUS semi-integrated protocols to allow Pre-Authorization and PreAuth Capture with select processors that support this feature.

Validation

Disable this option. Validation is only used with fully integrated EFT protocols and has no effect with semi-integrated protocols such as SecureTable or SecurePay.

Expiration

Disable this option. This option automatically becomes enabled when Electronic Funds Transfer is enabled. Make sure to ***DISABLE*** it. Otherwise, the POS will request the credit card's expiration date, which will slow down your operations. This information is already checked by the payment terminal and does not need to be re-validated by the POS.

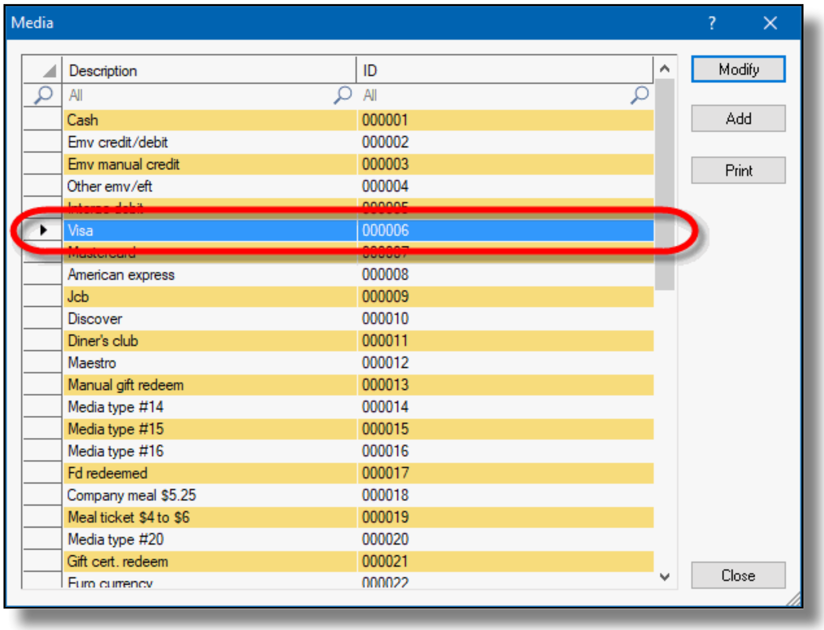
Debit Card

- ***Enable*** this option if you are creating a mapping for U.S. Debit or Canadian Debit (Interac).
- ***Disable*** this option for credit card brand mappings (Visa, Mastercard, American Express, Discover, etc.).

Card Validation

All the options in this section must be cleared. Make sure to clear the ***Custom Card*** checkbox as well as all the fields in the ***Card Validation*** section.

8. Click ***OK*** to save changes. The new media type will appear in the list.



Description	ID
All	All
Cash	000001
Emv credit/debit	000002
Emv manual credit	000003
Other emv/eft	000004
Interac debit	000005
Visa	000006
Mastercard	000007
American express	000008
Jcb	000009
Discover	000010
Diner's club	000011
Maestro	000012
Manual gift redeem	000013
Media type #14	000014
Media type #15	000015
Media type #16	000016
Fd redeemed	000017
Company meal $5.25	000018
Meal ticket $4 to $6	000019
Media type #20	000020
Gift cert. redeem	000021
Euro currency	000022

9. Repeat the previous steps until all required mappings are created. At the end of the process, you should have one mapping for each card brand that is accepted by the merchant.

Generic Media Type mapping for SecureTable or SecurePay

Before you begin

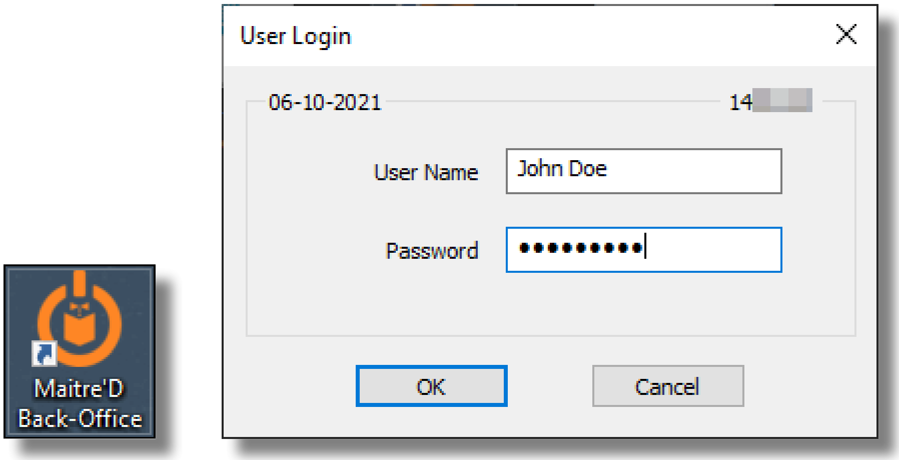
This configuration is optional for most merchants. Before proceeding, make sure that individual media type mappings are created for each accepted card brand.

A generic media type mapping may be required to cover the rare cases where a customer may pay with a card that is accepted by the merchant, but not already configured as a mapping in Maitre'D media types. If a dedicated media type mapping does not already exist, the payment would be recorded against the main media type, generally called "CREDIT/DEBIT". The goal of the generic mapping is to have such payments recorded against a media type with a more meaningful name, something like "Other Card Payment" for instance.

NOTE: SecureTable and SecurePay can be used at the same time on the same POS system. Therefore, the merchant can have any combination of stationary terminals using SecurePay and mobile terminals using SecureTable. Both types of terminals will share the same generic media type mapping.

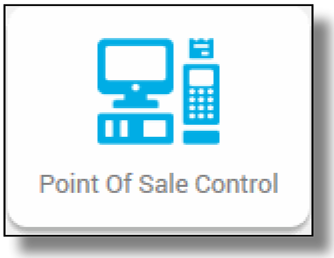
Creating the Generic mapping

1. Logon to the Maitre'D Back-Office with appropriate credentials. (Distributor or System Owner)

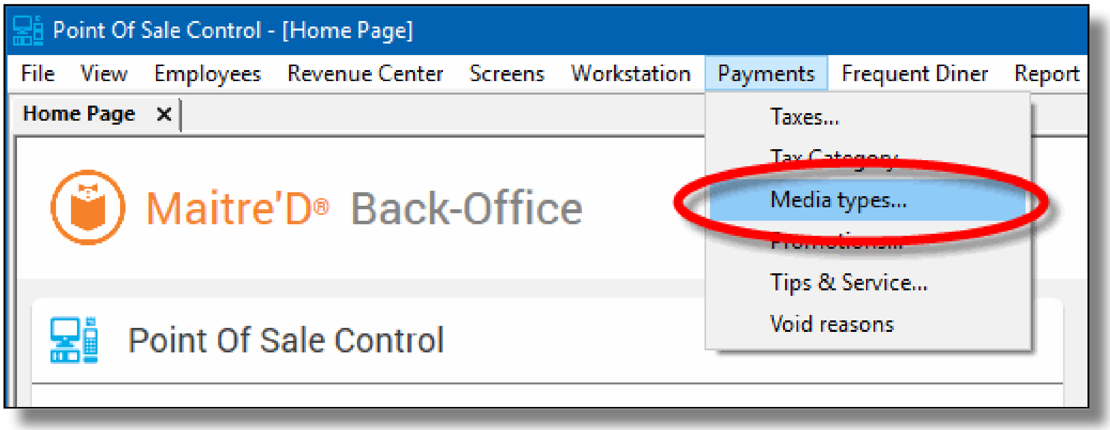


06-10-2021 14[redacted]
User Name: John Doe
Password: ••••••••••

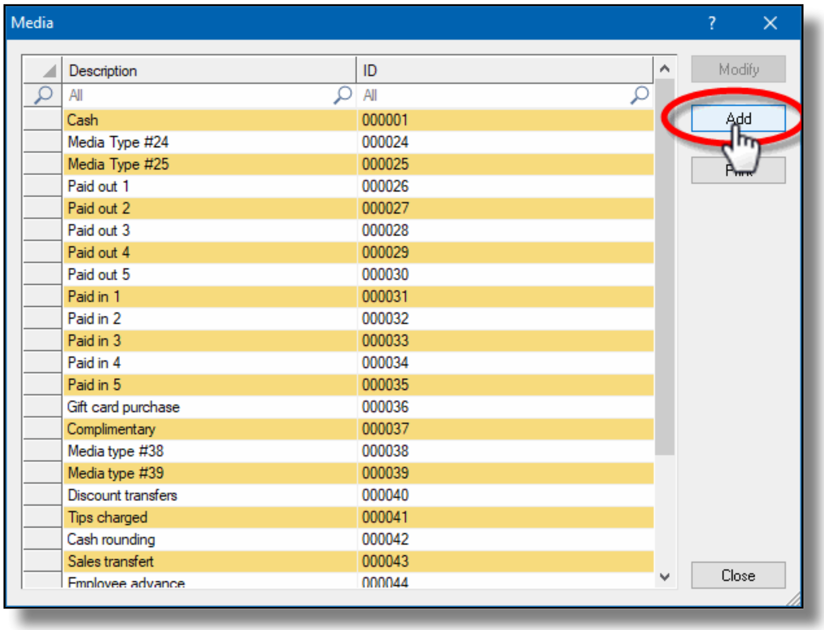
2. Start the ***Point of Sale Control*** Module.



3. Click the ***Payments*** menu, and select the ***Media Types...*** option.

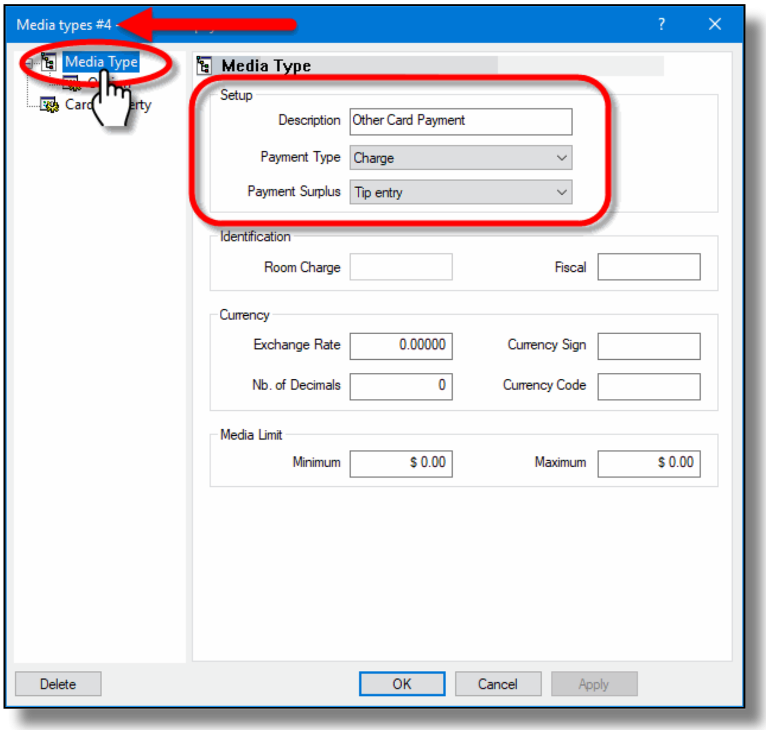


4. The list of all current media types will be displayed. Click the ***Add*** button.



Description	ID
All	All
Cash	000001
Media Type #24	000024
Media Type #25	000025
Paid out 1	000026
Paid out 2	000027
Paid out 3	000028
Paid out 4	000029
Paid out 5	000030
Paid in 1	000031
Paid in 2	000032
Paid in 3	000033
Paid in 4	000034
Paid in 5	000035
Gift card purchase	000036
Complimentary	000037
Media type #38	000038
Media type #39	000039
Discount transfers	000040
Tips charged	000041
Cash rounding	000042
Sales transfert	000043
Employee advance	000044

5. A blank Media Type window will open directly on the ***Media Type*** branch. Configure according to the information below:



Media Type

Setup
Description: Other Card Payment
Payment Type: Charge
Payment Surplus: Tip entry

Identification
Room Charge:
Fiscal:

Currency
Exchange Rate: 0.00000
Currency Sign:
Nb. of Decimals: 0
Currency Code:

Media Limit
Minimum: $ 0.00
Maximum: $ 0.00

Media Type ID

The Media Type ID number is automatically determined by Maitre'D when the Media Type is created. Maitre'D will always use the lowest available number between #2 and #23 inclusively.

Description

Enter a meaningful description for this media type. For the Generic mapping, this could be ***Other Card Payments*** or something similar. This description will be shown on customer receipts and media reports.

Payment Type

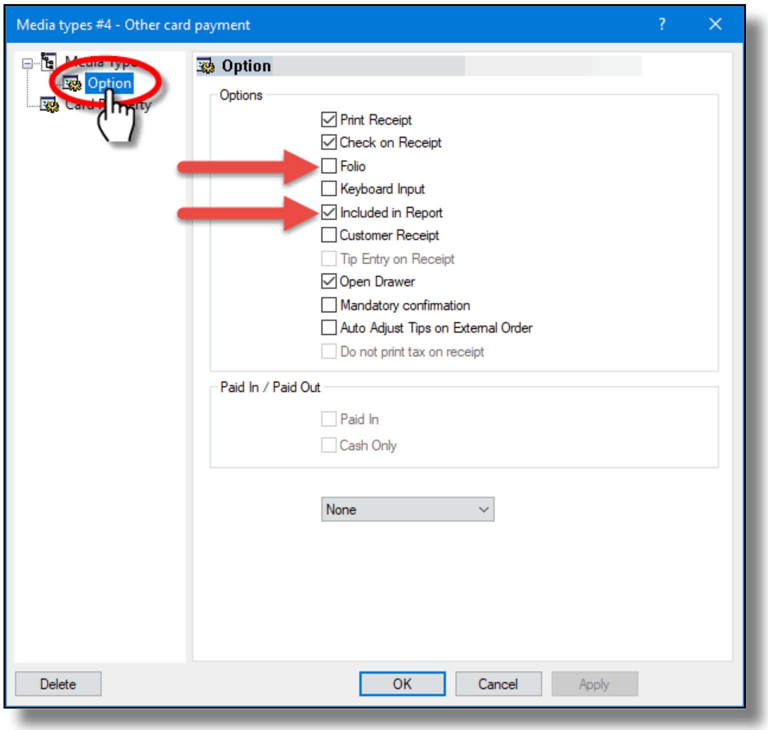
Select the ***Charge*** option from the drop-down list.

Payment Surplus

- Select ***Tip Entry*** if the merchant accepts tips for servers.
- Select ***NULL*** if the merchant does not accept tips.

Configure remaining options per the merchant's needs and preferences.

6. Click on the ***Option*** branch.



Print Receipt (Optional)

Enable this option to allow for a receipt to be printed after the transaction has been processed.

Check on Receipt (Optional)

Enable this option to have the detailed check print on the receipt.

Folio

Disabled. This option needs to be disabled.

Keyboard Input

Disabled. This option cannot be used since the ***Folio*** option above also needs to be disabled.

Included in Report

Enable this option so that this media type is shown in Back-Office reports (Recommended). Disabling this option will cause this media type to be hidden in the reports (NOT recommended).

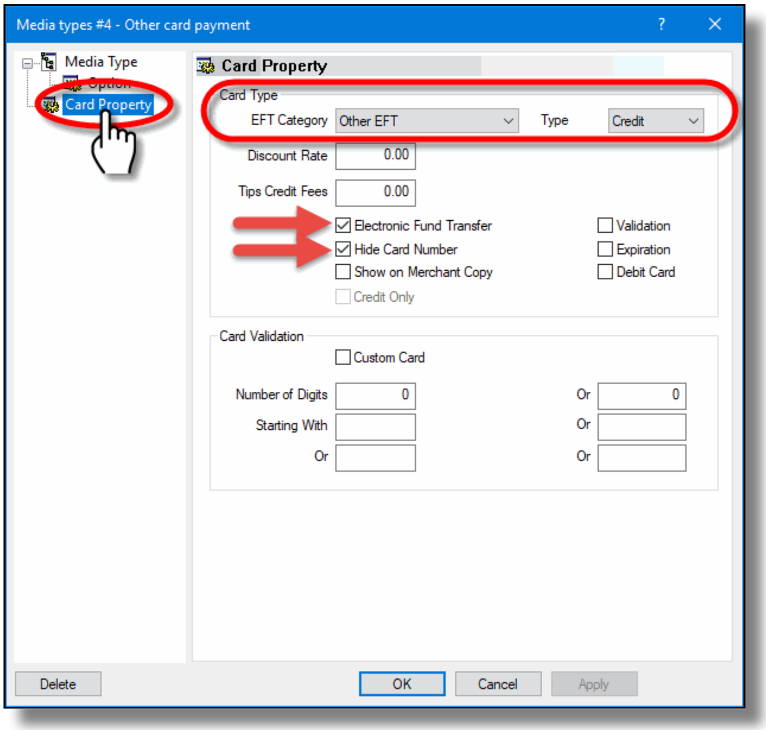
Open Drawer (Optional)

Enable this option to make the cash drawer open when this media type is used.

NOTE: ***Print Receipt***, ***Check on Receipt*** and ***Open Drawer*** options have no effect on wireless payment terminals using SecureTable. However, payment terminals with SecurePay will be affected.

Configure remaining options per the merchant's needs and preferences.

7. Click on the ***Card Property*** branch.



Card Property

Card Type

EFT Category: Other EFT

Type: Credit

Discount Rate: 0.00

Tips Credit Fees: 0.00

☑ Electronic Fund Transfer
☑ Hide Card Number
□ Show on Merchant Copy
□ Credit Only
□ Validation
□ Expiration
□ Debit Card

Card Validation

□ Custom Card

Number of Digits: 0 Or: 0

Starting With: Or:

Or: Or:

EFT Category

Set this drop-down list to ***Other EFT***.

Type

Set this drop-down list to ***Credit***.

Discount Rate

This option is not supported with EMV protocols and semi-integrated protocols like SecureTable or SecurePay. Leave this value at 0.00.

Tips Credit Fees

Enter the percentage of tips paid to the waiters that will be withheld to cover for fees charged by payment processors. If you do not wish to use this feature, leave it at 0.00.

> **NOTE:** Some jurisdictions don't allow transaction or credit card processing fees to be passed down to employees. Please verify your local regulations before using this feature.

Electronic Funds Transfer

Enable this option. This option needs to be enabled to block operations that are not compatible with EMV payments, such as Cancel/Reopen Check.

Hide Card Number

Enable this option. It automatically becomes enabled when Electronic Funds Transfer is enabled, so leave it enabled.

Show on Merchant Copy

Disable this option. This option was used by older, non-integrated protocols and caused the credit card number to be printed on the merchant copy of EFT transaction records. This option has no effect with any Electronic Funds Transfer protocol, semi-integrated protocols, SecureTable or SecurePay.

Credit Only

This option is not usable (grayed-out) with most EFT protocols. It is only used with the Datacap - DSIEMVUS semi-integrated protocols to allow Pre-Authorization and PreAuth Capture with select processors that support this feature.

Validation

Disable this option. Validation is only used with fully integrated EFT protocols and has no effect with semi-integrated protocols such as SecureTable or SecurePay.

Expiration

Disable this option. This option automatically becomes enabled when Electronic Funds Transfer is enabled. Make sure to ***DISABLE*** it. Otherwise, the POS will request the credit card's expiration date, which will slow down your operations. This information is already checked by the payment terminal and does not need to be re-validated by the POS.

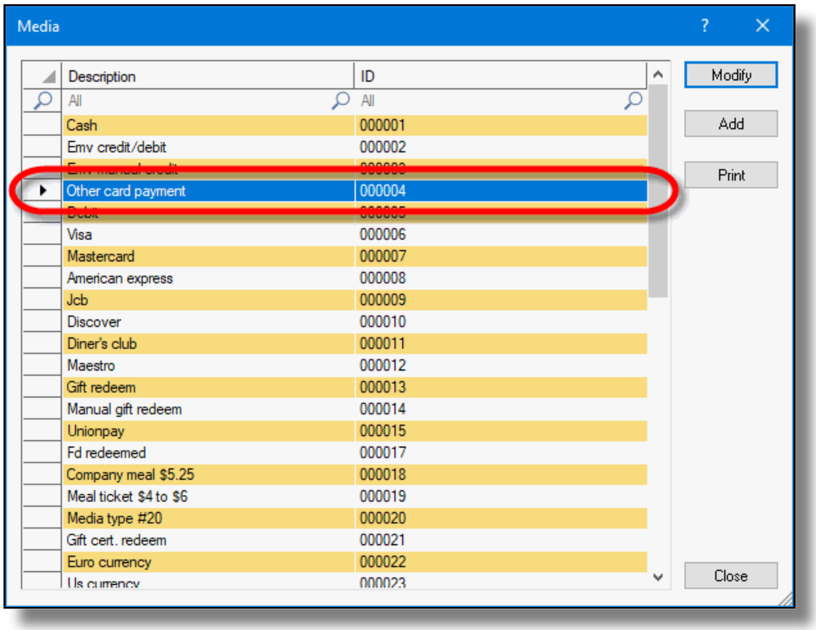
Debit Card

Disable this option for the generic media type mapping.

Card Validation

All the options in this section must be cleared. Make sure to clear the ***Custom Card*** checkbox as well as all the fields in the ***Card Validation*** section.

8. Click ***OK*** to save changes. The new media type will appear in the list.



Description	ID
All	All
Cash	000001
Emv credit/debit	000002
Emv manual credit	000003
Other card payment	000004
Debit	000005
Visa	000006
Mastercard	000007
American express	000008
Jcb	000009
Discover	000010
Diner's club	000011
Maestro	000012
Gift redeem	000013
Manual gift redeem	000014
Unionpay	000015
Fd redeemed	000017
Company meal $5.25	000018
Meal ticket $4 to $6	000019
Media type #20	000020
Gift cert. redeem	000021
Euro currency	000022
Us currency	000023

The configuration of the generic media type mapping is now completed.

SecureTable Installation on Android Payment Terminals

After the STPISecure client is installed, configured and running properly on the POS system, make sure that all payment terminals are properly configured so they can communicate with the POS system. Android payment terminals are generally shipped with all the necessary applications pre-installed by PayFacto, including the latest versions of SecureTable and of the latest version of the Payment application. If the SecureTable application appears to be missing, install it using the instructions below.

PAX A920 Android Terminal

The instructions below were created using the PAX A920 Android-based Payment terminal and the PAX store. However, the instructions are the same for all Android-based payment terminals, such as other models offered by PAX, AMP terminals or Clover Flex. For brands other than PAX, the mechanism they use to install apps may look different but the general principle should remain the same.

Before you begin

Before installing SecureTable on your payment terminal, please make sure that the appropriate payment application is installed and configured properly. You may also want to check out our documentation on the PAX A920, A920Pro or A80 terminals or any other Android-based terminal you may be using with SecureTable.

PayFacto Payment Application (For the Canadian market):

Android PayFacto Application - Manual setup of application

PayFacto - Clerk Management

PayFacto Quick Reference Guide

BroadPOS Payment application (For the US market):

Link

PAX A920 Payment Terminal:

PAX A920 - Introduction

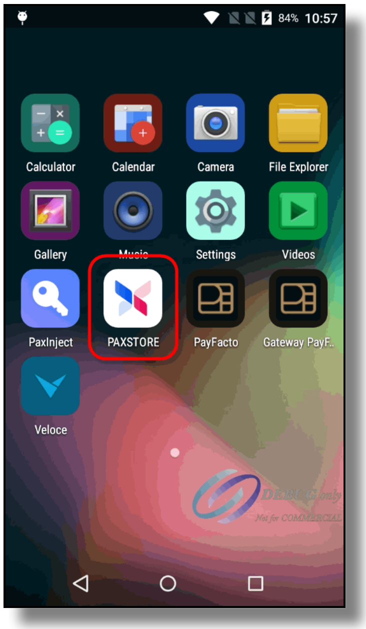
PAX A920 - Quick Setup Guide

Getting to know the PAX A920 Terminal

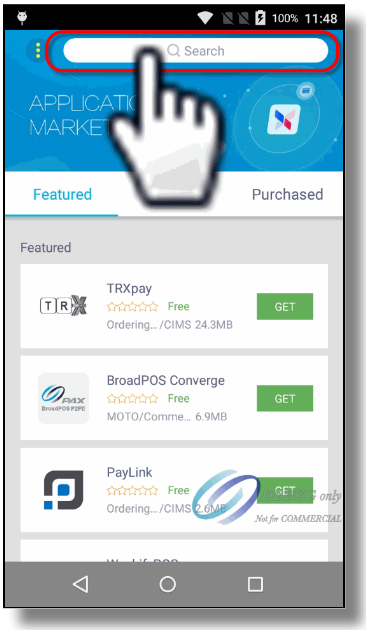
Installing the SecureTable Android application

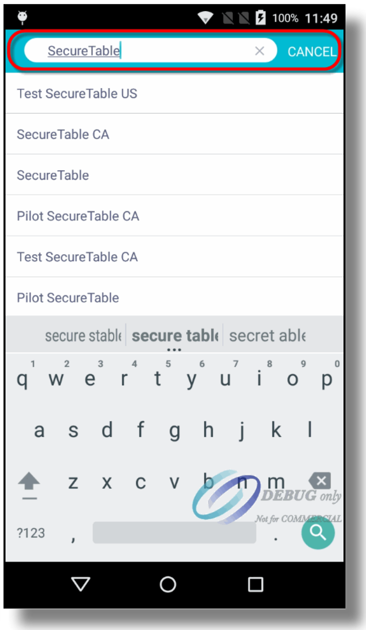
NOTE: The SecureTable application can be installed on certified payment terminals only. It cannot be used on regular phones or tablets.

1. Power-up your terminal, and make sure it is connected to the Internet.
2. If any application start automatically, shut them down to reach the Android home screen.
3. From the Android home screen, start the ***PAXSTORE*** by touching the appropriate icon.

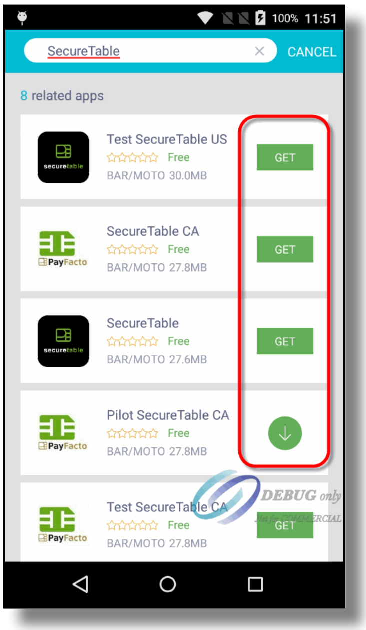


4. In the PAXSTORE (Application Marketplace), search for ***SecureTable***.

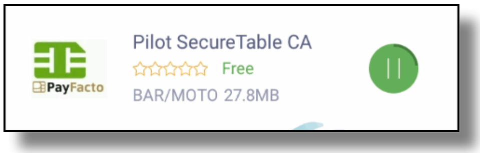


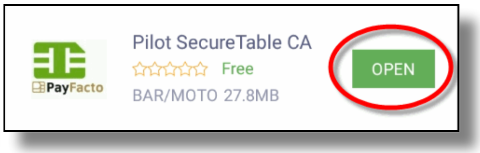


5. Locate the version which is appropriate for your region, and touch the ***GET*** button to download and install it.

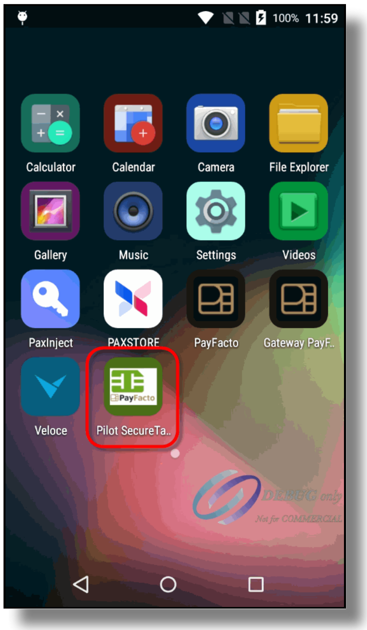


6. During the installation, the GET button will turn to a circle with the Pause symbol inside. Once installation is complete, the GET button will change to OPEN.





7. An icon will also be created on the Android home screen.

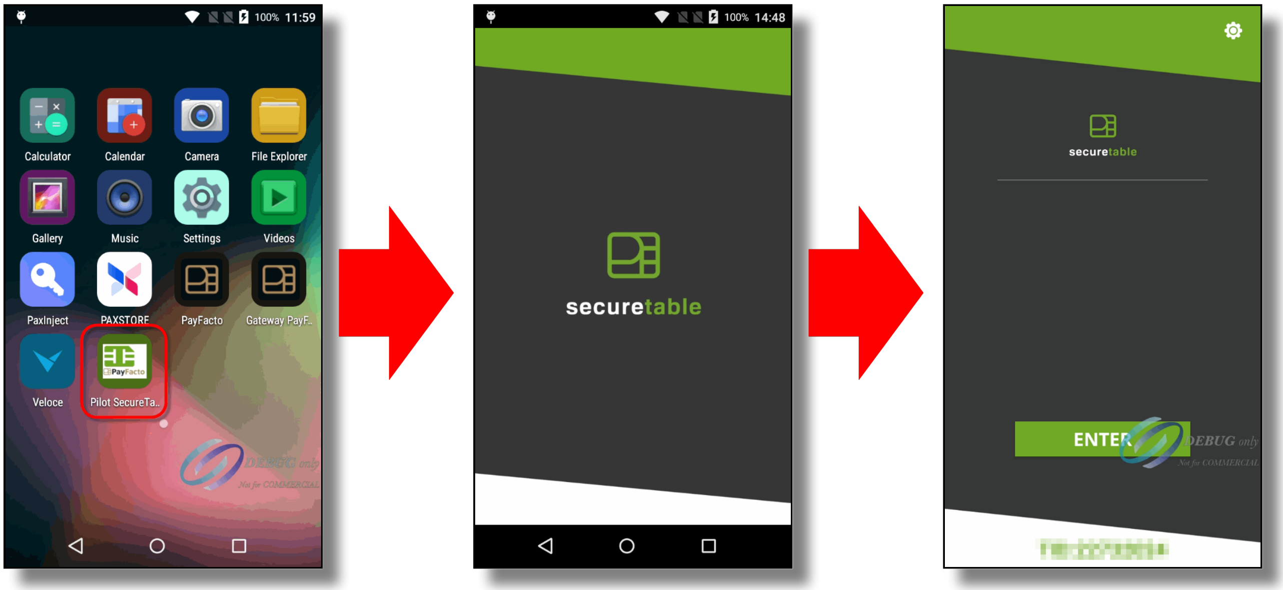


Installation of the SecureTable application is now complete.

SecureTable Application - Basic Navigation

Starting the SecureTable Application

If the SecureTable application does not start automatically, simply touch the appropriate icon on the Android home screen. A splash screen will briefly be displayed, followed by the SecureTable home screen.



Basic Navigation

Enter Button

ENTER

Use the ***ENTER*** button to start a transaction with SecureTable.

Settings

⚙

The ***Settings*** button is used to access SecureTable's configuration options. This icon appears in the top-right corner of the SecureTable home screen.

Home

⌂

When available, the ***Home*** button will appear in the top-right corner of the screen. Use it to jump directly to the SecureTable home screen without saving changes.

Back

When available, the ***Back*** button will appear in the top-left corner of the screen. Use it to go back to the previous screen without saving changes.

WiFi / 4G LTE

When available, the Wifi or 4G/LTE icon will appear in the top-left corner of the screen. The icon indicates which network is currently being used. Touching the icon allows the user to switch from WiFi to LTE or vice-versa.

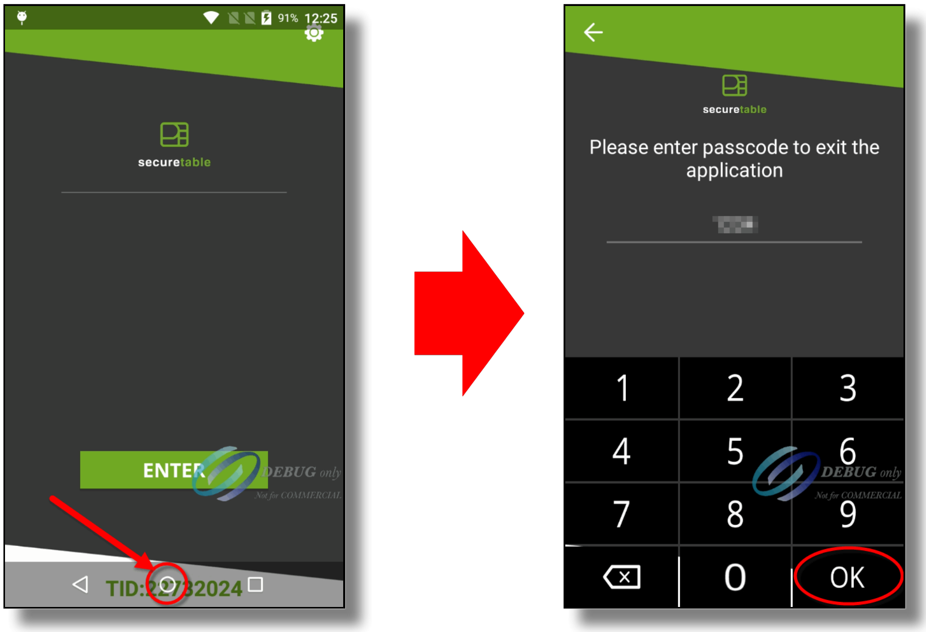
Default Password

The SecureTable application settings are protected by a password. The default password on a new installation is ***1234***.

> **NOTE:** It is highly recommended to change the default password as soon as possible. See SecureTable Application Configuration for the detailed procedure.

Exit the SecureTable Application

1. To exit the SecureTable application, swipe the terminal's screen either from the top edge going down, or the bottom edge going up, then touch the Android ***Home (circle)*** button.
2. You will be prompted to enter a ***passcode*** to exit the application. Enter the ***passcode*** and touch the ***OK*** button.



Please enter passcode to exit the application

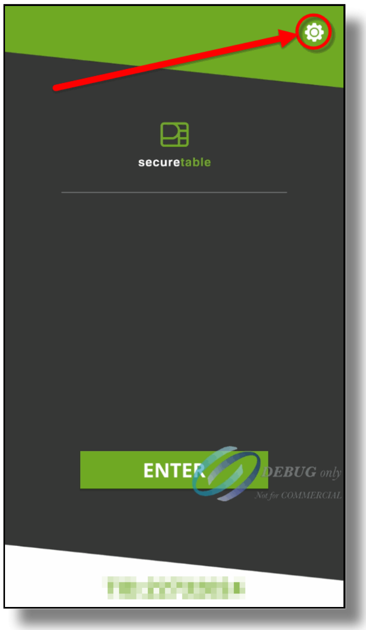
NOTE: The default passcode after a new installation is ***1234***. It is the same as the settings password.

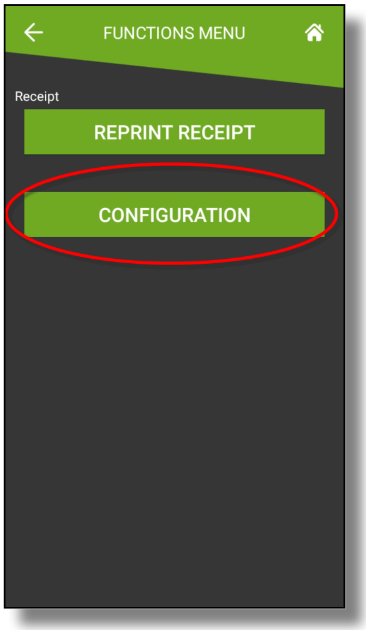
1. SecureTable Application Configuration
2. SecureTable Installation on Android Terminals

SecureTable Application Configuration

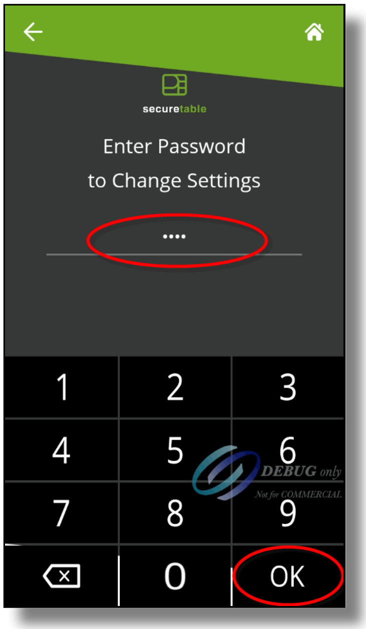
Access SecureTable App Settings

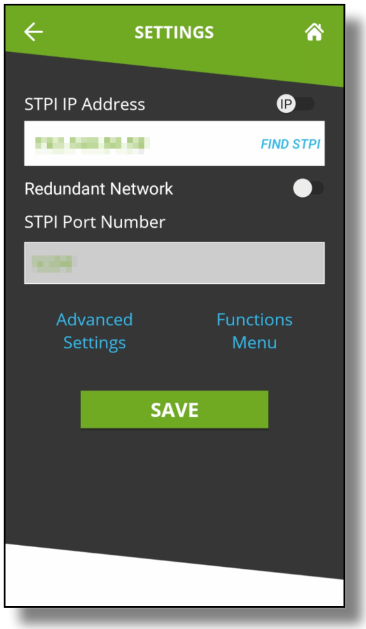
1. From the SecureTable home screen, touch the cog wheel icon (⚙) at the top-right of the screen.
2. The ***FUNCTIONS*** menu will be displayed. Touch the ***CONFIGURATION*** button.





3. You will be prompted to enter a password before you can access settings. Enter the password and press the ***OK*** key.
4. The ***SETTINGS*** screen will be displayed.

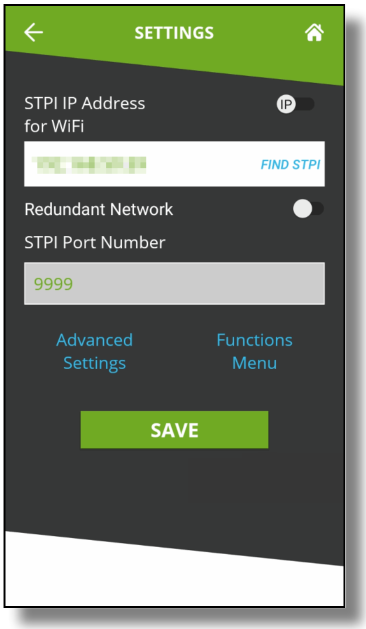




NOTE: The default password after a new installation is ***1234***.

Configure Basic Settings

NOTE: Before configuring the IP address or URL, it is strongly recommended to start the STPI Client on the PC where it was installed, and make sure it is running properly. This will allow you to test the communication using the ***FIND STPI*** links found with some settings.



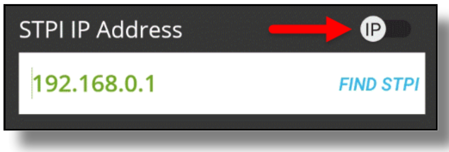
STPI IP Address for WiFi: [redacted]

STPI Port Number: 9999

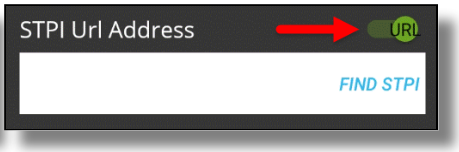
IP / URL toggle switch

By default, the toggle switch is set to IP, and the field is labeled ***STPI IP Address.*** By touching the toggle switch, the field will change to ***STPI URL Address***.

- The IP option is used to locate the STPISecure Client using an IP address, such as 192.168.xxx.xxx.
- The URL option is used to locate the STPISecure Client using a Uniform Rersource Locator (URL), such as https://payfacto.com/.



STPI IP Address: 192.168.0.1



STPI Url Address

STPI IP/URL Address for WiFi

Enter the IP address or URL of the PC or resource where the STPI Client is installed and running, when accessing it through the local WiFi network.

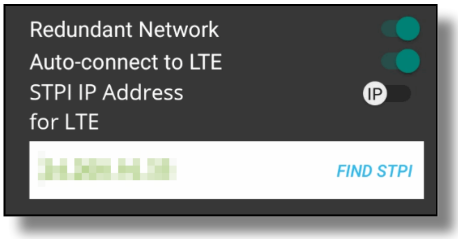
Find STPI

After entering the IP address or URL, touch this link to verify the communication between your payment terminal and the STPI Client.

Redundant Network

Enable this option to allow the SecureTable application to communicate over both WiFi and 4G/LTE mobile networks. By default, SecureTable will always try to use WiFi networks first, to avoid extra costs from using data over mobile networks. If the terminal is out of range of any known WiFi networks, SecureTable will automatically switch to 4G/LTE mobile network. Enabling this option will also unlock additional settings.

NOTE: A SIM card needs to be installed in the payment terminal to get access to 4G/LTE mobile networks. Also, this option will be hidden if no SIM card is detected.



Redundant Network ●
Auto-connect to LTE ●
STPI IP Address for LTE (IP) ○
[redacted] FIND STPI

Auto-connect to LTE

** This settings is only visible if ***Redundant Network*** is also enabled.

With this option enabled, SecureTable will offer the option to automatically switch from WiFi to 4G/LTE if unable to reach the POS system during a transaction. This switch will only happen if the application is actively trying to connect to the POS system. It will not happen while the application is idle.

If this option is disabled and there is a WiFi communication issue during a transaction, you will get a generic error message and you will need to manually switch to 4G/LTE and re-attempt the transaction.

STPI IP/URL Address for LTE

** This settings is only visible if ***Redundant Network*** is also enabled.

Enter the Public IP address or URL to access the STPI Client is installed and running, when accessing it through the 4G/LTE mobile network.

Find STPI

After entering the IP address or URL, touch this link to verify the communication between your payment terminal and the STPI Client.

NOTE: The STPI Client needs to be up-and-running. If you are using ***FIND STPI*** for 4G/LTE, Port Forwarding also needs to be configured on the router/firewall controlling the access to the local area network.

STPI Port Number

This field displays the current TCP port number used for communication with the STPI Client.

NOTE: This setting can only be modified from the ***Advanced Settings*** screen and is displayed here for information purposes only.

Advanced Settings

Touch this link to access the ***Advanced Settings*** screen.

Functions Menu

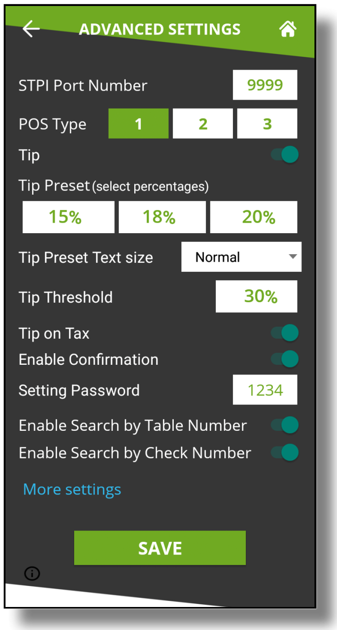
Touch this link to access the ***Functions Menu*** screen.

SAVE

Touch this button to save your changes and return to the home screen.

> **NOTE:** On a brand-new installation, the application will not let you save your settings with an empty (blank) STPI Port Number. To prevent this issue, go to the ***Advanced Settings*** screen, configure the STPI Port Number, Save, and then go back to the basic settings screen to set the IP address or URL.

Configure Advanced Settings



STPI Port Number: 9999

POS Type: 1 | 2 | 3

Tip

Tip Preset (select percentages): 15% | 18% | 20%

Tip Preset Text size: Normal

Tip Threshold: 30%

Tip on Tax

Enable Confirmation

Setting Password: 1234

Enable Search by Table Number

Enable Search by Check Number

STPI Port Number

Default: 9999

This is the TCP port number used by STPI. Be sure that this TCP port is unblocked by your network administrator.

POS Type

- Select 1 for Maitre’D, Veloce or any POS other than Micros or Squirrel.
- Select 2 for Micros.
- Select 3 for Squirrel.

Tip

Enable this option to have the SecureTable application prompt for tip entry. Disable this option to prevent tip entry. Disabling this option will also hide all the tip-related options below.

Tip Preset (Select percentages)

Configure preset tip percentages that the customer will see when prompted for tip. Up to 3 presets can be configured. If you do not wish to use all of them, presets that are set to 0% will not be displayed to the customer.

Tip Preset Text Size

Select the text size used to display preset tip percentages. Available choices are Normal, Medium and Large.

Tip Threshold

Enter the maximum allowed tip percentage. Any tip amount that exceeds this percentage will require the settings password to be entered. Setting the percentage to 0% disables the tip threshold validation.

Tip on Tax

Enable this option to calculate the tip percentage from the total check amount, including taxes. If this option is disabled, the tip amount will be calculated on the sub-total instead, which does not include taxes.

NOTE: For the ***Tip on Tax*** feature to have an effect, the POS system needs to send both the sub-total and check total as separate values to the STPIClient. If the POS system only sends the check total without the sub-total, this setting will have no effect. The percentage will be calculated on the check total sent by the POS, regardless of the status of this option.

Enable Confirmation

Enable this option to present a dedicated tip confirmation screen for the customer. If this option is disabled, the tip confirmation screen will be skipped when selecting a tip preset or the NO TIP option. If using custom $ or custom % with this option disabled, the tip amount, percentages and resulting totals will be updated in real-time as the customer types the numbers in, but no additional confirmation screen will be presented before the actual payment.

Setting Password

Configure the password used to access settings. This is also the password that will be requested if the customer enters a tip amount that exceeds the Tip Threshold.

Enable Search by Table Number

Enable this option to have the terminal prompt the server for a table number. This allows the SecureTable application to search for all available checks for a given table number.

Enable Search by Check Number

Enable this option to have the terminal prompt for a check number. This allows servers to enter a check number in order to directly access a check, instead of selecting the check from a list.

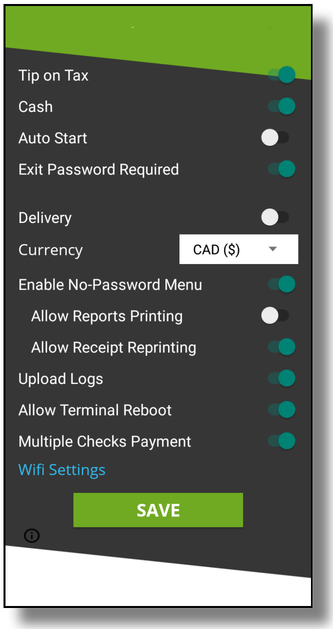
More Settings

Touch this link to view more advanced settings.

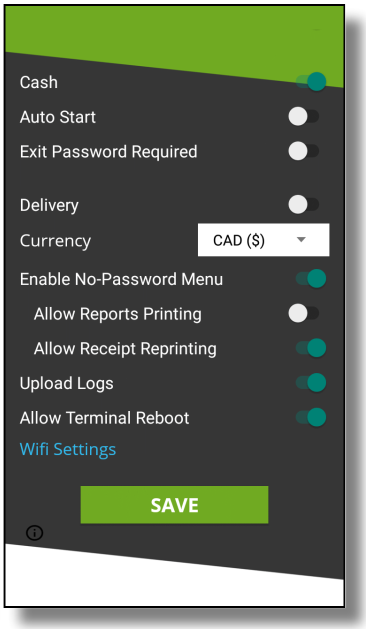
SAVE

Touch this button to save your changes and return to the home screen.

Configure More Advanced Settings



Tip on Tax ☑
Cash ☑
Auto Start ☐
Exit Password Required ☑
Delivery ☐
Currency CAD ($)
Enable No-Password Menu ☑
Allow Reports Printing ☐
Allow Receipt Reprinting ☑
Upload Logs ☑
Allow Terminal Reboot ☑
Multiple Checks Payment ☑
Wifi Settings
SAVE



Cash ☑
Auto Start ☐
Exit Password Required ☐
Delivery ☐
Currency CAD ($)
Enable No-Password Menu ☑
Allow Reports Printing ☐
Allow Receipt Reprinting ☑
Upload Logs ☑
Allow Terminal Reboot ☑
Wifi Settings
SAVE

Cash

Enable this option to allow cash payments to be applied on checks from the SecureTable application.

Auto Start

Enable this option to have the SecureTable application start automatically when powering on the payment terminal.

Exit Password Required

With this option enabled, the SecureTable application will request the settings password before closing.

Delivery

Enable this option to use the SecureTable application in Delivery mode. With this option enabled, the payment terminal will display the delivery order numbers instead of table numbers.

Currency

Select the default currency for your region. Supported currencies are:

- Canadian Dollar (CAD ($))
- United States Dollar (USD ($))
- United Kingdom Pound (GBP (£))
- European Union Euro (EUR (€))
- Australian Dollar (AUD ($))

Enable No-Password Menu

Enable this option to allow users to access a simplified version of the ***Functions*** menu without entering a password. This menu is accessed by touching the cog wheel icon (⚙) at the top-right of the home screen. Enabling this option will also unlock access to the ***Allow Reports Printing*** and ***Allow Receipt Reprinting*** options below.

Allow Reports Printing

Enable this option to allow users to access and print the ***Detailed Report*** and ***Summary Report*** from the No-password menu. If this option is disabled, the reports can still be printed from the FUNCTIONS menu, which requires the settings password.

Allow Receipt Reprinting

Enable this option to activate the ***Reprint Receipt*** option in the No-password menu. If this option is disabled, the receipts can still be reprinted from the FUNCTIONS menu, which requires the settings password.

Upload Logs

Enable this option to upload the SecureTable application logs to the PayFacto Cloud services. It is recommended to leave this option enabled.

Allow Terminal Reboot

Enable this option to allow the terminal to reboot after an automatic batch settlement. It is recommended to leave this option enabled.

WiFi Settings

Use this shortcut to configure the payment terminal's WiFi settings.

SAVE

Touch this button to save your changes and return to the home screen.

NOTE: The payment terminal ***MUST*** be connected to your WiFi or Ethernet network and have internet access. Otherwise, payments cannot be processed and payment information cannot be transmitted to the POS system.

IMPORTANT! Be sure to touch the ***SAVE*** button to save your changes. Using any other button to exit from the settings screen will discard all changes.

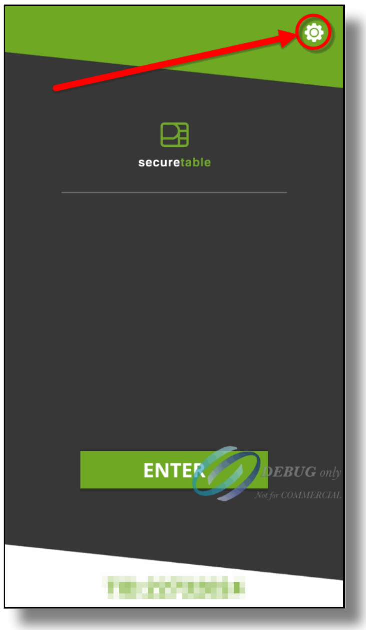
SecureTable Functions

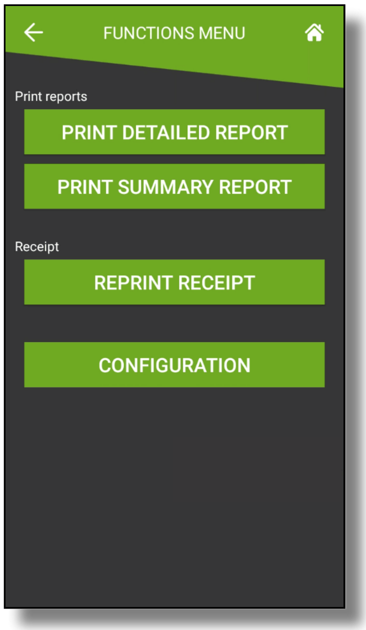
No Password Menu

The ***No Password Menu*** is a simplified version of the ***Functions*** menu. It contains basic functions that are useful to employees, while manager functions remain hidden.

> **NOTE:** Before the ***No Password menu*** can be used, the corresponding option needs to be enabled in the SecureTable application settings. Please consult the Enable No Password Menu option in the SecureTable application settings for more details.

1. From the SecureTable home screen, touch the cog wheel icon (⚙) at the top-right of the screen.
2. The ***FUNCTIONS*** menu will be displayed. The options available from this menu will vary based on your SecureTable application settings.





Print Reports

The ***Print Reports*** section will be displayed if the Allow Reports Printing option is enabled in the SecureTable Application Settings.

PRINT DETAILED REPORT

This option prints a report with the details of every card payment processed at the terminal since the last batch closing.

> **NOTE:** Cash payments processed through the SecureTable application are not included in this report. Please use your POS system's reports for this purpose.

PRINT SUMMARY REPORT

This option prints a report that shows a summary of sales, refunds, tips and grand total for each card brand.

Receipt

The ***Receipt*** section will be displayed if the AllowReceiptReprinting option is enabled in the SecureTable Application Settings.

REPRINT RECEIPT

This option allows receipts to to be reprinted based on invoice number, sequence number or the last transaction processed at the terminal.

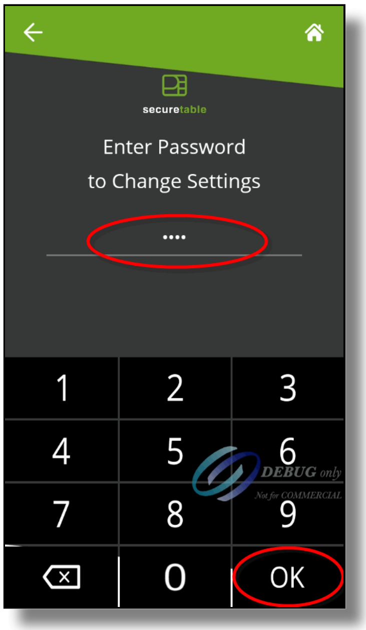
CONFIGURATION

This option brings up the SecureTable application settings.

Full functions menu

The full functions menu contains all the options from the No Password Menu, plus a few more administrative options. To access the full functions menu:

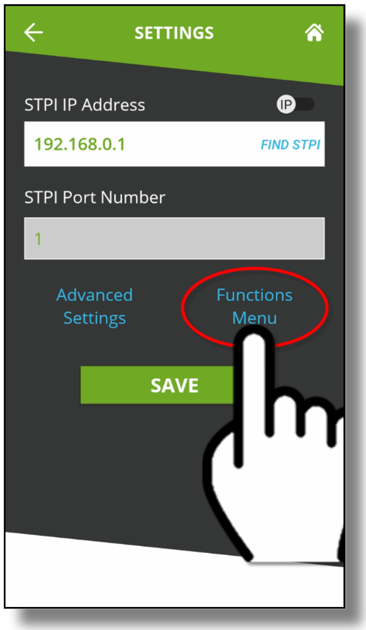
1. From the SecureTable home screen, touch the cog wheel icon (⚙) at the top-right of the screen.
2. The ***FUNCTIONS*** menu (no password menu) will be displayed. Touch the ***CONFIGURATION*** option.
3. You will be prompted to enter a password before you can access settings. Enter the password and press the ***OK*** key.
4. The ***SETTINGS*** screen will be displayed. Touch the blue ***Functions Menu*** link.



securetable

Enter Password to Change Settings

••••



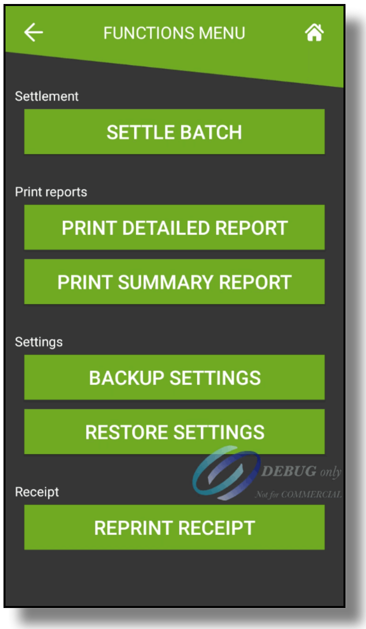
SETTINGS

STPI IP Address: 192.168.0.1

STPI Port Number: 1

<u>NOTE:</u> The default password after a new installation is ***1234***.

The ***Functions menu*** will be displayed. Contrary to the ***No Password Menu*** discussed above, all the options shown below are always available, regardless of the status of the advanced settings.



SETTLE BATCH

This option will manually close the current batch.

IMPORTANT! Transactions that are part of a batch that is closed can no longer be voided, reprinted or otherwise modified.

PRINT DETAILED REPORT

This option prints a report with the details of every card payment processed at the terminal since the last batch closing.

PRINT SUMMARY REPORT

This option prints a report that shows a summary of sales, refunds, tips and grand total for each card brand.

BACKUP SETTINGS

This option will save all of the current settings to an S3 Bucket cloud location. Backing up the settings allows for quick recovery of the configuration in case the settings get reset to default after a major application update or Android update.

RESTORE SETTINGS

Use this option to restore saved settings. Using this option will override all settings with the ones found in the backup, except for the terminal ID.

REPRINT RECEIPT

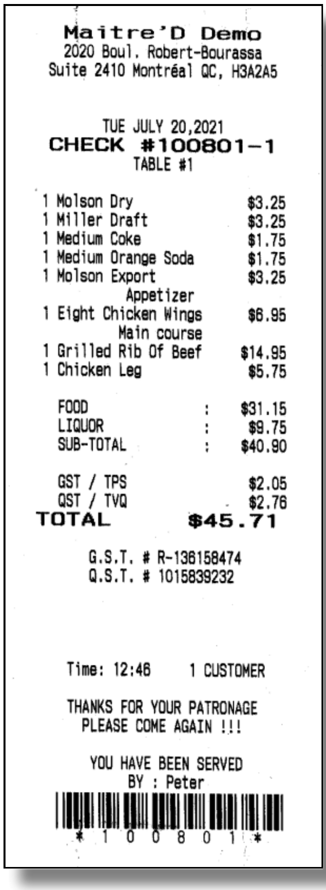
This option allows receipts to to be reprinted based on invoice number, sequence number or the last transaction processed at the terminal.

General use of SecureTable to apply payments

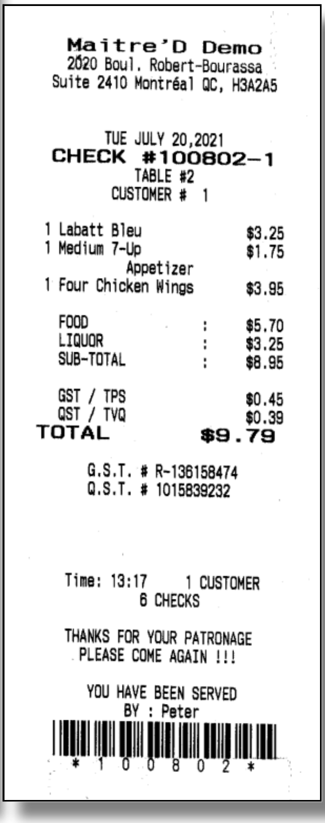
This section will cover the general workflow that users and customers will see when using SecureTable. The workflow will vary slightly based on the SecureTable application's configuration. The workflow steps that are user-configurable are also optional and can be skipped during the transaction process. Those will be indicated as such below.

Before starting a transaction

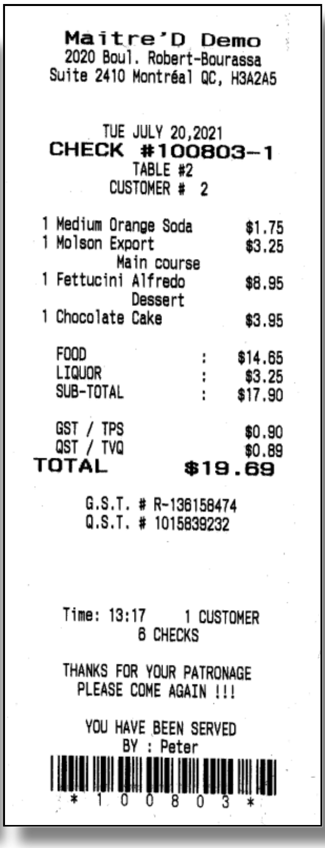
Before starting a transaction using a payment terminal with SecureTable, at least one check must be printed from the POS system. SecureTable can also work with split checks as well a tables with multiple checks. Open tables without printed checks cannot be accessed by SecureTable.



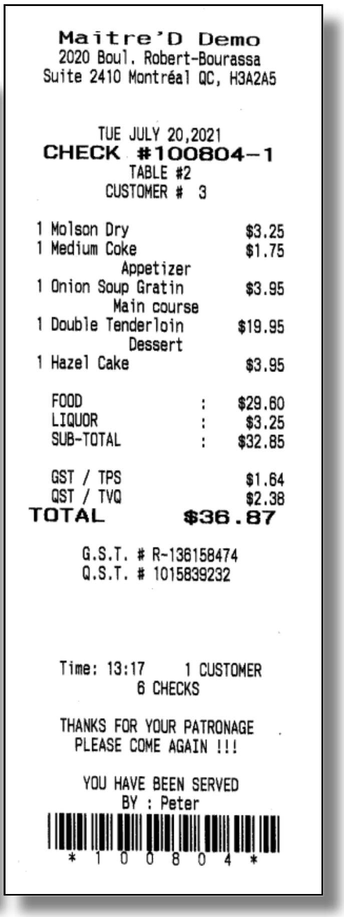
```
       Maitre'D Demo
  2020 Boul. Robert-Bourassa
Suite 2410 Montréal QC, H3A2A5

      TUE JULY 20,2021
   CHECK  #100801-1
          TABLE #1

1 Molson Dry               $3.25
1 Miller Draft             $3.25
1 Medium Coke              $1.75
1 Medium Orange Soda       $1.75
1 Molson Export            $3.25
         Appetizer
1 Eight Chicken Wings      $6.95
         Main course
1 Grilled Rib Of Beef     $14.95
1 Chicken Leg              $5.75

  FOOD               :    $31.15
  LIQUOR             :     $9.75
  SUB-TOTAL          :    $40.90

  GST / TPS                $2.05
  QST / TVQ                $2.76
TOTAL                  $45.71

   G.S.T. # R-136158474
   Q.S.T. # 1015839232


 Time: 12:46     1 CUSTOMER

 THANKS FOR YOUR PATRONAGE
   PLEASE COME AGAIN !!!

    YOU HAVE BEEN SERVED
         BY : Peter
     * 1 0 0 8 0 1 *
```



```
       Maitre'D Demo
  2020 Boul. Robert-Bourassa
Suite 2410 Montréal QC, H3A2A5

      TUE JULY 20,2021
   CHECK  #100802-1
          TABLE #2
       CUSTOMER #  1

1 Labatt Bleu              $3.25
1 Medium 7-Up              $1.75
         Appetizer
1 Four Chicken Wings       $3.95

  FOOD               :     $5.70
  LIQUOR             :     $3.25
  SUB-TOTAL          :     $8.95

  GST / TPS                $0.45
  QST / TVQ                $0.39
TOTAL                   $9.79

   G.S.T. # R-136158474
   Q.S.T. # 1015839232


 Time: 13:17     1 CUSTOMER
          6 CHECKS

 THANKS FOR YOUR PATRONAGE
   PLEASE COME AGAIN !!!

    YOU HAVE BEEN SERVED
         BY : Peter
     * 1 0 0 8 0 2 *
```



```
       Maitre'D Demo
  2020 Boul. Robert-Bourassa
Suite 2410 Montréal QC, H3A2A5

      TUE JULY 20,2021
   CHECK  #100803-1
          TABLE #2
       CUSTOMER #  2

1 Medium Orange Soda       $1.75
1 Molson Export            $3.25
         Main course
1 Fettucini Alfredo        $8.95
         Dessert
1 Chocolate Cake           $3.95

  FOOD               :    $14.65
  LIQUOR             :     $3.25
  SUB-TOTAL          :    $17.90

  GST / TPS                $0.90
  QST / TVQ                $0.89
TOTAL                  $19.69

   G.S.T. # R-136158474
   Q.S.T. # 1015839232


 Time: 13:17     1 CUSTOMER
          6 CHECKS

 THANKS FOR YOUR PATRONAGE
   PLEASE COME AGAIN !!!

    YOU HAVE BEEN SERVED
         BY : Peter
     * 1 0 0 8 0 3 *
```



```
       Maitre'D Demo
  2020 Boul. Robert-Bourassa
Suite 2410 Montréal QC, H3A2A5

      TUE JULY 20,2021
   CHECK  #100804-1
          TABLE #2
       CUSTOMER #  3

1 Molson Dry               $3.25
1 Medium Coke              $1.75
         Appetizer
1 Onion Soup Gratin        $3.95
         Main course
1 Double Tenderloin       $19.95
         Dessert
1 Hazel Cake               $3.95

  FOOD               :    $29.60
  LIQUOR             :     $3.25
  SUB-TOTAL          :    $32.85

  GST / TPS                $1.64
  QST / TVQ                $2.38
TOTAL                  $36.87

   G.S.T. # R-136158474
   Q.S.T. # 1015839232


 Time: 13:17     1 CUSTOMER
          6 CHECKS

 THANKS FOR YOUR PATRONAGE
   PLEASE COME AGAIN !!!

    YOU HAVE BEEN SERVED
         BY : Peter
     * 1 0 0 8 0 4 *
```

Transaction workflow

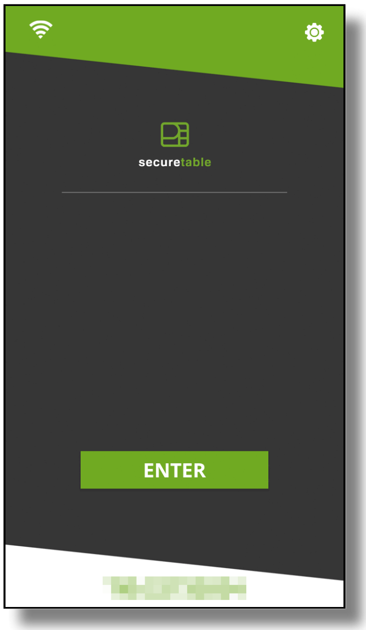
The workflow will vary based on SecureTable's application settings. This section covers all possible configurations. Here are quick links to each step of the workflow:

1. Home Screen (Start)
2. Enter Server Number
   a. Enter Table Number (Optional)
   b. Enter Check Number (Optional)

3. Select Table
4. Select from multiple checks
5. Split Calculator
   a. Equal Split
   b. Unequal Split
6. Tip Calculation (with tip presets)
   a. Custom tip amount
   b. Custom tip percentage
7. Tip Confirmation
8. Payment (Card processing)
9. Payment posting to the POS

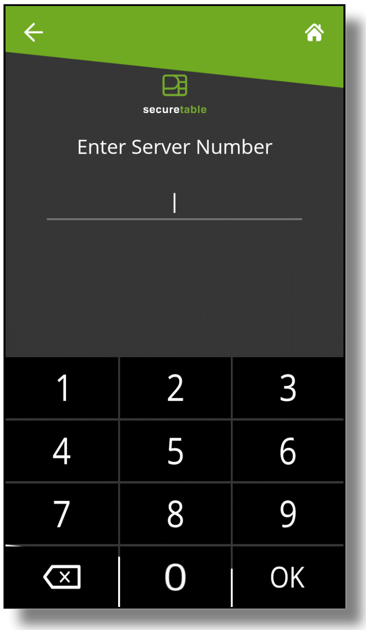
Home Screen

The transaction workflow always starts from the SecureTable home screen. To start, simply press the ***ENTER*** button.



Enter Server Number (mandatory)

Enter the Server, Clerk or employee number and press the ***OK*** button in the lower-right corner of the screen. The server number is mandatory to start a transaction. It will be used to filter the tables and checks, and only the tables or checks that are related to the server number entered will be available.



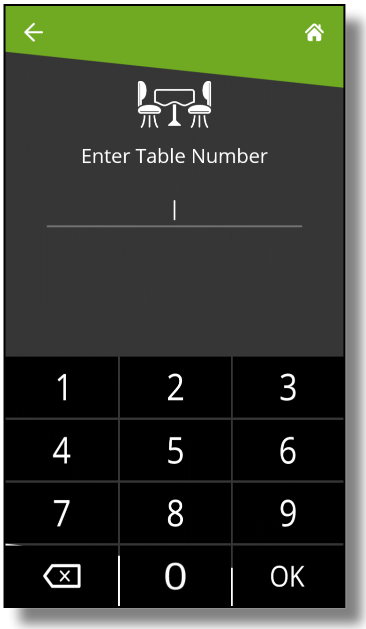
NOTE: On devices equipped with a physical keypad, the on-screen keypad will not be displayed. The physical keypad buttons will be used instead.

Enter Table Number (optional)

This screen will only be displayed if the Enable Search by Table Number option is enabled in the SecureTable application's settings.

The table number is used to further filter the checks that will be displayed. This is useful to display the full list of checks associated with a specific table.

To use it, enter the table number and press the ***OK*** button in the lower-right corner of the screen. To skip this step, simply press ***OK*** without entering a table number.



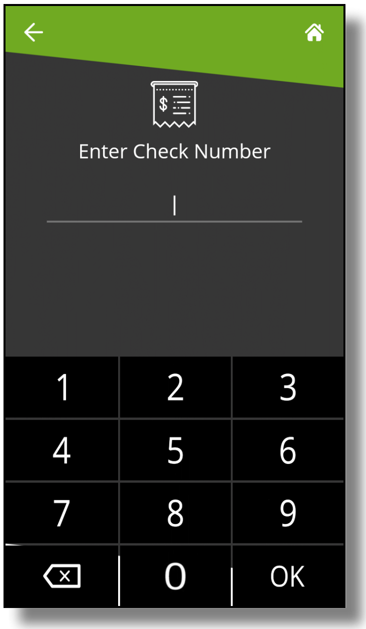
NOTE: On devices equipped with a physical keypad, the on-screen keypad will not be displayed. The physical keypad buttons will be used instead.

Enter Check Number (optional)

This screen will only be displayed if the Enable Search by Check Number option is enabled in the SecureTable application's settings.

The check number is used to search for a specific check. This is useful when you have the check in hand and you just want to bring it up immediately on the SecureTable application.

To use it, enter the check number and press the ***OK*** button in the lower-right corner of the screen. To skip this step, simply press ***OK*** without entering a check number.



NOTE: On devices equipped with a physical keypad, the on-screen keypad will not be displayed. The physical keypad buttons will be used instead.

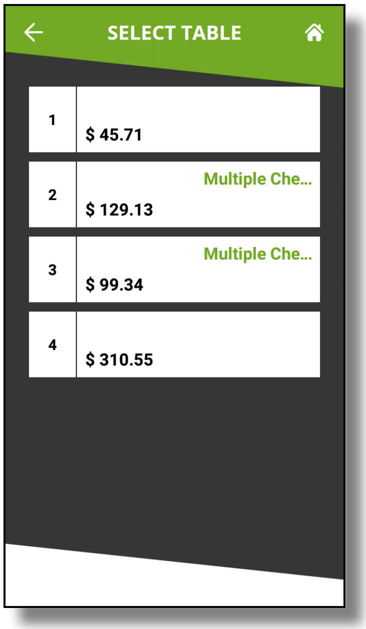
Select Table

This screen may look different or may not be displayed altogether, based on settings and previous choices made:

- A list of all tables containing printed checks will be displayed if both the ***Table Number*** and ***Check Number*** screens were skipped.
- A single table will be displayed if a valid table number was entered at the ***Table Number*** screen and the check number was skipped.
- This screen will be skipped altogether if a check number was entered at the ***Check Number*** screen. In this case, SecureTable will skip directly to the ***Split Calculator*** screen, further below.

The table number is indicated to the left of each white box. Each box displays the total amount due for the entire table, and the green ***Multiple Checks*** text indicates that this table has more than one printed checks.

To select a table, simply touch the desired box.



SELECT TABLE

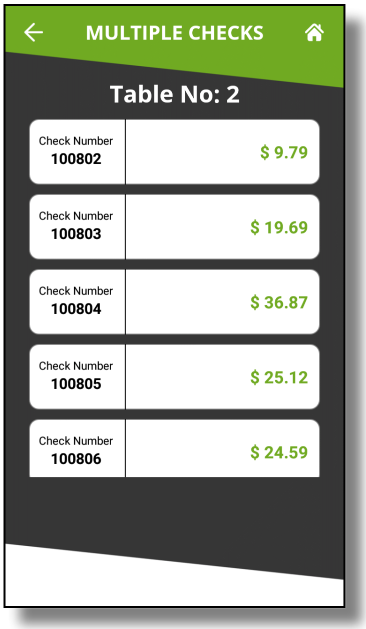
1	$ 45.71
2	Multiple Che... $ 129.13
3	Multiple Che... $ 99.34
4	$ 310.55

Multiple Checks

When a table containing multiple printed checks is selected, the list of available checks is displayed. On a typical payment terminal screen, up to 5 checks can be displayed at once. If there are more than 5 checks, the list can be scrolled by swiping up and down the screen.

This screen will not be displayed if a table with a single check was selected, or if a check number was entered at the Check Number screen.

To select a check to be paid, simply touch the corresponding box on the screen.



MULTIPLE CHECKS

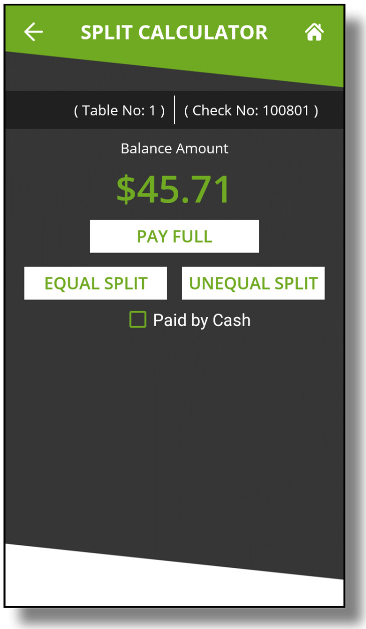
Table No: 2

Check Number 100802	$ 9.79
Check Number 100803	$ 19.69
Check Number 100804	$ 36.87
Check Number 100805	$ 25.12
Check Number 100806	$ 24.59

Split Calculator

The split calculator is the step where the server discusses with the customer about how the check will be paid. The following needs to be determined:

- Will the check be paid by cash or by card?
- Will the check be paid in full in one payment, or in multiple payments (split)?
- If the payment is to be split, will it be in equal or unequal amounts?



Paid by Cash

Enable this checkbox if the customer pays with cash. If the customer pays by card, leave this box unchecked.

PAY FULL

Touch this button to pay the check in full.

EQUAL SPLIT

Touch this button to split the check amount in up to 10 equal parts.

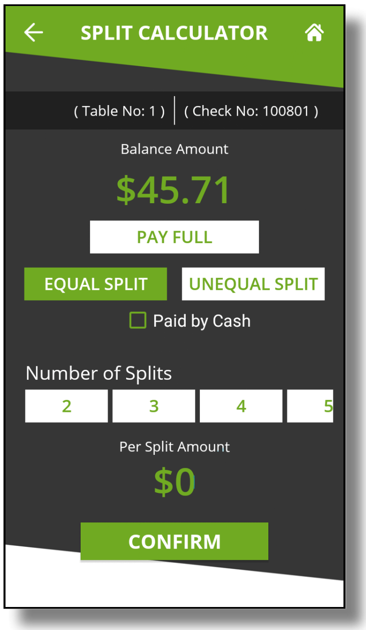
UNEQUAL SPLIT

Touch this button to split the check in unequal parts.

Split Calculator - Equal Split

Equal split is used to divide the total check amount in up to 10 equal parts. This is useful when there is a single printed check for 2 or more customers, and they want to split the expense among themselves.

After touching the ***EQUAL SPLIT*** button, select the ***Number of Splits***. The ***Per Split Amount*** will be updated automatically.



(Table No: 1) | (Check No: 100801)

Balance Amount

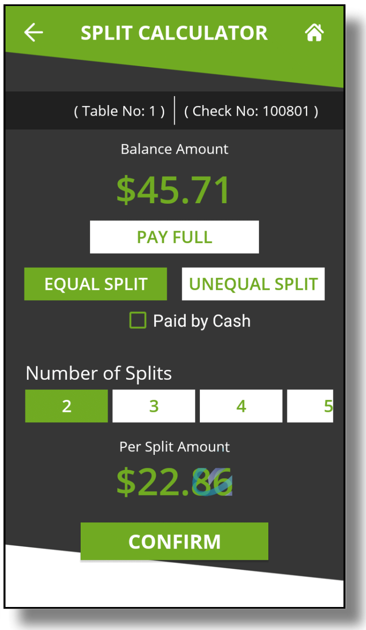
$45.71

□ Paid by Cash

Number of Splits

Per Split Amount

$0



(Table No: 1) | (Check No: 100801)

Balance Amount

$45.71

□ Paid by Cash

Number of Splits

Per Split Amount

$22.86

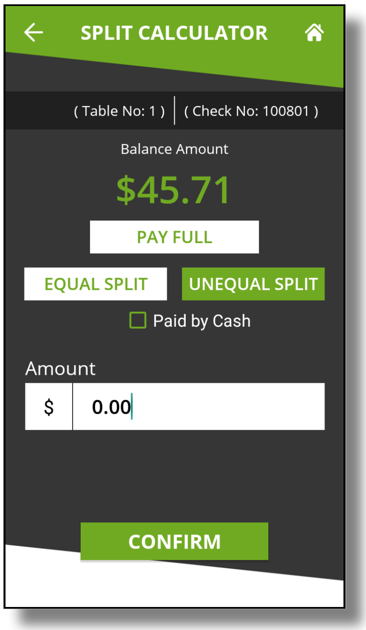
Touch the ***CONFIRM*** button to proceed with the first payment.

> **NOTE:** If the amount is not equally divisible by the number of splits selected, there will be a difference of $0.01 between split amounts. In the screenshot above, dividing $45.71 by 2 creates the first split at $22.86 and the second one at $22.85.

Split Calculator - Unequal Split

The UNEQUAL SPLIT function is used to divide the check amount in unequal parts. This is useful if the in a single printed check which multiple customers wish to pay with various amounts.

After touching the ***UNEQUAL SPLIT*** button, touch the ***Amount*** field and enter the amount that the customer wishes to pay.

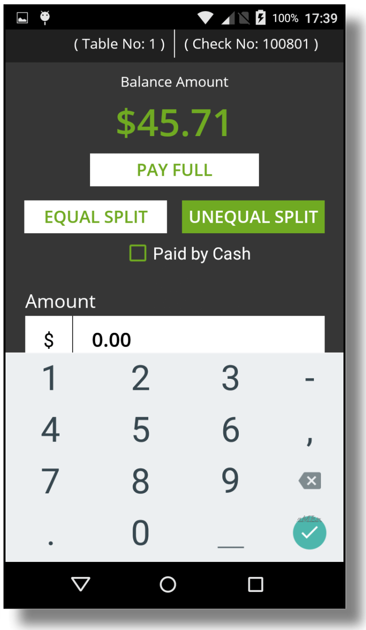


(Table No: 1) (Check No: 100801)

Balance Amount $45.71

□ Paid by Cash

Amount $ 0.00

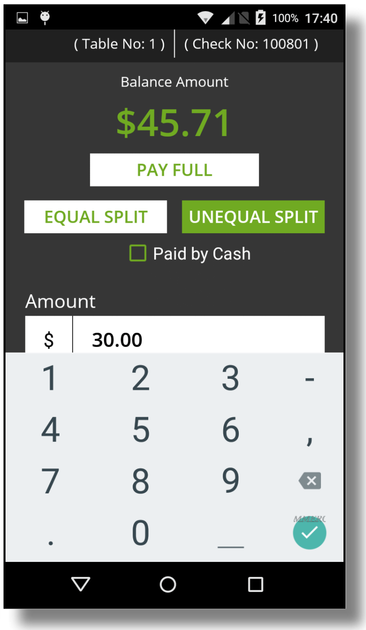


(Table No: 1) (Check No: 100801)

Balance Amount $45.71

□ Paid by Cash

Amount $ 0.00

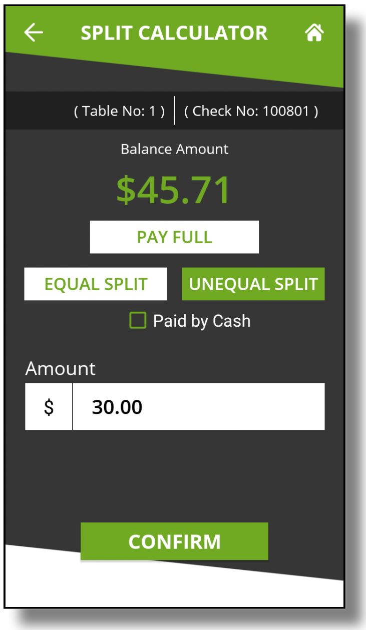


(Table No: 1) (Check No: 100801)

Balance Amount $45.71

□ Paid by Cash

Amount $ 30.00



(Table No: 1) (Check No: 100801)

Balance Amount $45.71

□ Paid by Cash

Amount $ 30.00

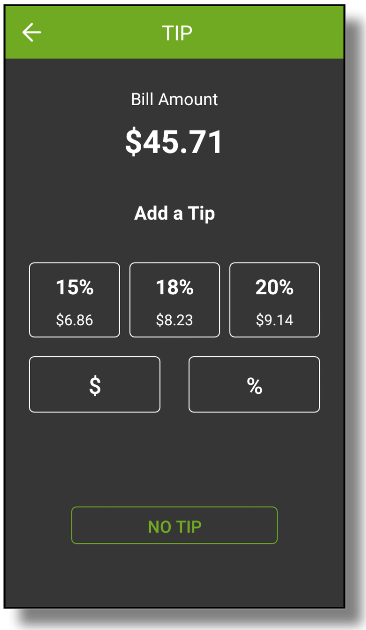
Touch the ***CONFIRM*** button to proceed with the first payment.

Tip Calculation

If the ***Tip*** option is enabled in the SecureTable application settings, the tip calculation screen will be displayed.

When the Tip calculation screen appears, the payment terminal needs to be handed to the customer. The customer has the following options:

- Select one of the pre-set percentages;
- Enter a custom dollar amount;
- Enter a custom percentage;
- Leave no tip at all.



Bill Amount
$45.71

Bill Amount

This section shows the total amount to be paid.

Add a Tip

In this section, the tip presets configured in the Tip Preset Percentages in SecureTable's advanced settings are displayed. Each percentage box also indicates the corresponding dollar amount.

Touching a preset automatically adds the stated tip amount to the transaction.

$

Touch the ***$*** button to enter a custom dollar amount as tip instead of using a preset.

%

Touch the ***%*** button to enter a custom percentage of tip instead of using a preset.

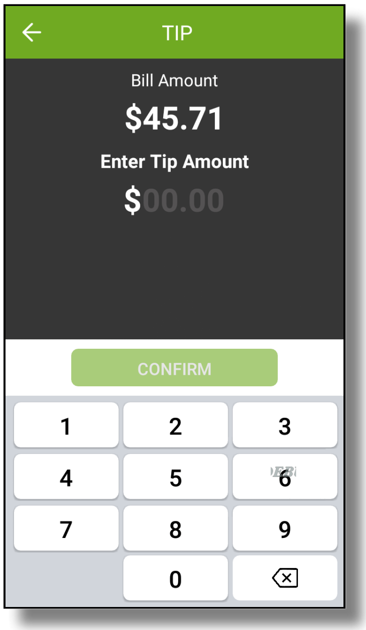
NO TIP

Touch this button to skip the tip entry process altogether and leave no tip.

Custom tip amount

The screen below only appears if the customer touches the ***$*** button to enter a custom tip amount.

The customer uses the provided keypad to enter a tip amount, which will make the green ***CONFIRM*** button available.



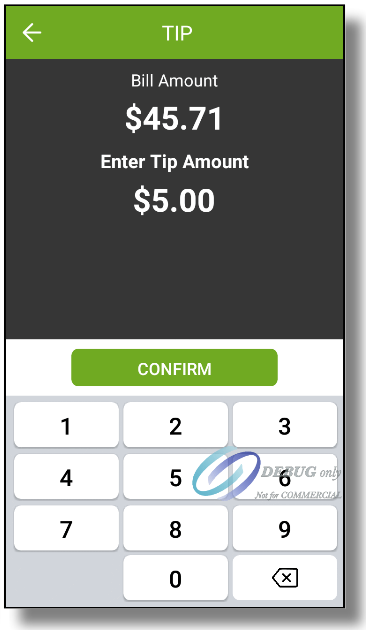
TIP

Bill Amount

$45.71

Enter Tip Amount

$00.00



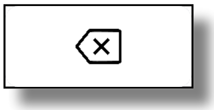
TIP

Bill Amount

$45.71

Enter Tip Amount

$5.00



The customer can use the backspace key to correct typing mistakes.

When ready, the customer presses the green ***CONFIRM*** button.

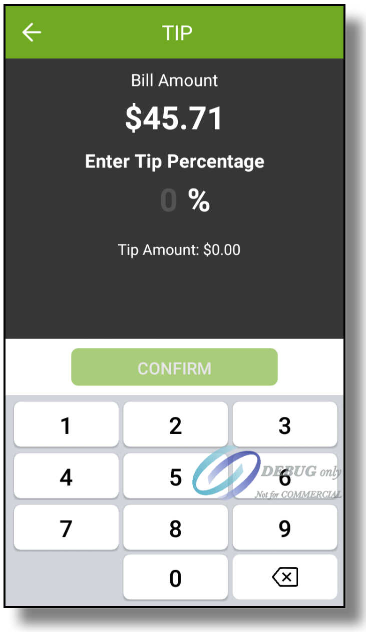
> **<u>NOTE:</u>** On devices equipped with a physical keypad, the on-screen keypad will not be displayed. The physical keypad buttons will be used instead.

Custom tip percentage

The screen below only appears if the customer touches the ***%*** button to enter a custom tip percentage.

The customer uses the provided keypad to enter a tip percentage, which will make the green ***CONFIRM*** button available.

Also note the Tip Amount value is updated in real-time as the customer types the percentage. This is provided so that the customer will immediately know exactly how much will be added to the check as tips, based on the percentage entered.



TIP

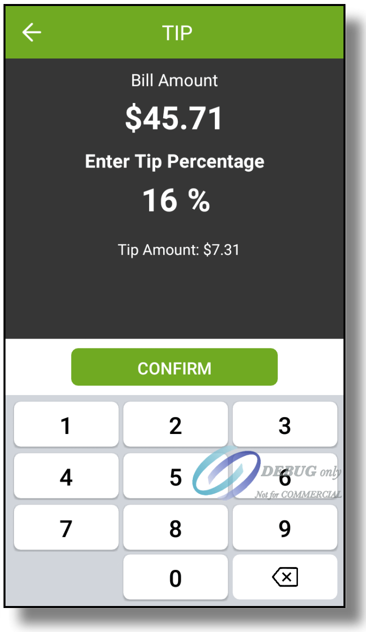
Bill Amount

$45.71

Enter Tip Percentage

0 %

Tip Amount: $0.00



TIP

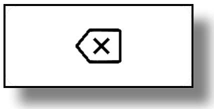
Bill Amount

$45.71

Enter Tip Percentage

16 %

Tip Amount: $7.31



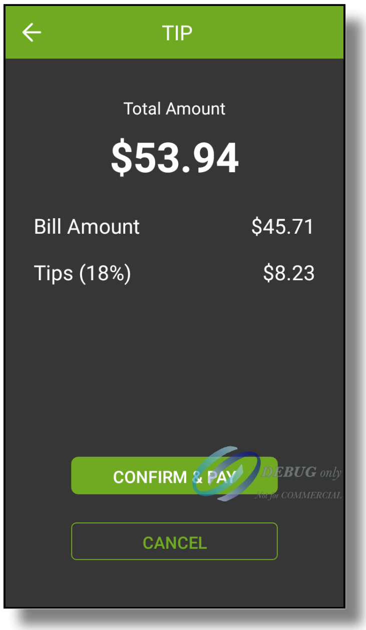
The customer can use the backspace key to correct typing mistakes.

When ready, the customer presses the green ***CONFIRM*** button.

NOTE: On devices equipped with a physical keypad, the on-screen keypad will not be displayed. The physical keypad buttons will be used instead.

Tip Confirmation

If the ***Enable Confirmation*** option is enabled in the SecureTable application settings, the tip confirmation screen will appear. This is the last confirmation before the actual payment.



Total Amount

$53.94

Bill Amount $45.71

Tips (18%) $8.23

Total amount

This is the total amount to be paid, which is calculated from the check amount plus tip amount.

Bill Amount

This is the amount that was passed from the POS system. It is also known as the Check amount or Invoice amount, depending on the terminology used by the POS system.

Tips (__%)

This field displays the tip amount added. The percentage between parenthesis is calculated from the Bill amount vs. tip amount, and is always rounded to the nearest percentage point.

CONFIRM & PAY

Touch this button to proceed with the actual payment.

CANCEL

Touch this button to cancel the transaction and return to the home screen to start over. A confirmation screen will be displayed before actually cancelling the operation.

Payment

At this point, SecureTable will call the payment application installed on the payment terminal. The prompts that the customer will see will depend on the payment application used and the card type used. For more information on this specific part of the workflow, please consult your payment application's documentation.

PayFacto Payment Process

PayFacto User Guide
PayFacto Quick Reference Guide

BroadPOS Payment Process

BroadPOS Quick Reference Guide

Payment posting to POS

After the payment has been authorized by the payment application, the payment data will be sent to the POS system. Note that only non-sensitive data is exchanged between SecureTable and the POS system.

The message ***Payment applied successfully!*** will be briefly displayed on the screen.

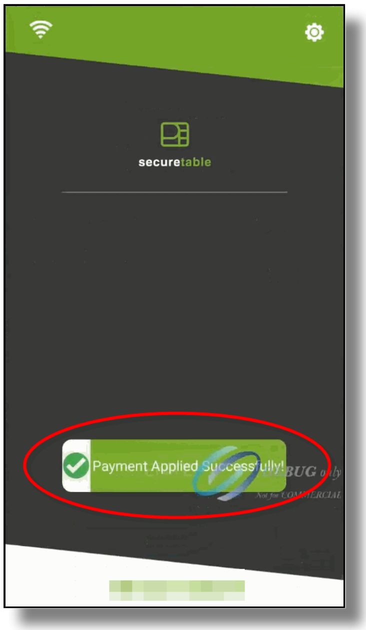
Then, one of two things can happen:

Splits

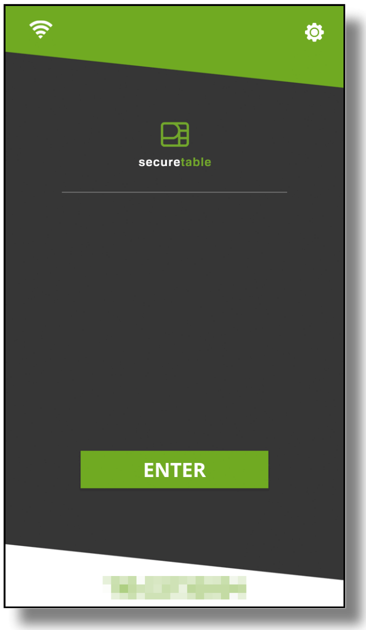
If this was a payment resulting from a split, SecureTable will return to the Split Calculator to process the next payment.

Full payment / Last payment

If this was a full payment or the last payment of a series of splits, SecureTable will return to the home screen.



Payment Applied Successfully!

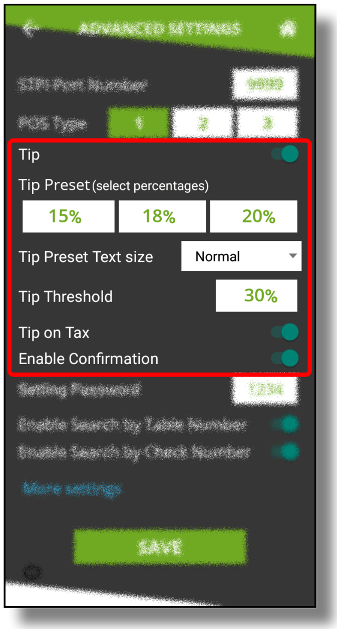


The payment workflow with SecureTable is now complete, and the application is ready to process the next payment.

Working with Tips

Being specifically designed for fine dining and delivery transactions, tip management is an integral part of SecureTable. This section focuses on the various options available in SecureTable to facilitate tip management.

Tip options are found in SecureTable's advanced settings. Here is a summary of available tip options:



ADVANCED SETTINGS

STPI Port Number: 9999

POS Type: 1 | 2 | 3

Tip: ●

Tip Preset (select percentages): 15% | 18% | 20%

Tip Preset Text size: Normal

Tip Threshold: 30%

Tip on Tax: ●

Enable Confirmation: ●

Setting Password: 1234

Enable Search by Table Number: ●

Enable Search by Check Number: ●

More settings

SAVE

Tip

Enable this option to have the SecureTable application prompt for tip entry. Disable this option to prevent tip entry. Disabling this option will also hide all the tip-related options below.

Tip Preset (Select percentages)

Configure preset tip percentages that the customer will see when prompted for tip. Up to 3 presets can be configured. If you do not wish to use all of them, presets that are set to 0% will not be displayed to the customer.

Tip Preset Text Size

Select the text size used to display preset tip percentages. Available choices are Normal, Medium and Large.

Tip Threshold

Enter the maximum allowed tip percentage. Any tip amount that exceeds this percentage will require the settings password to be entered. Setting the percentage to 0% disables the tip threshold validation.

Tip on Tax

Enable this option to calculate the tip percentage from the total check amount, including taxes. If this option is disabled, the tip amount will be calculated on the sub-total instead, which does not include taxes.

NOTE: For the ***Tip on Tax*** feature to have an effect, the POS system needs to send both the sub-total and check total as separate values to the STPIClient. If the POS system only sends the check total without the sub-total, this setting will have no effect. The percentage will be calculated on the check total sent by the POS, regardless of the status of this option.

Enable Confirmation

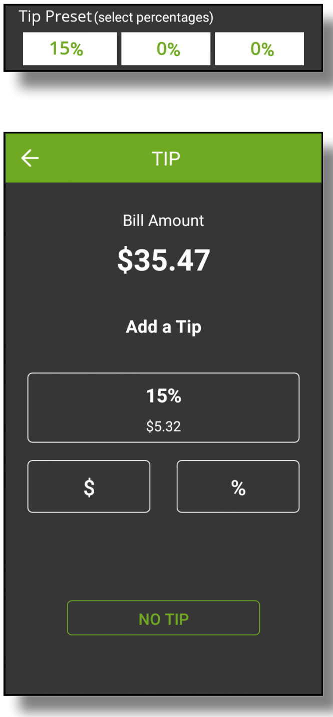
Enable this option to present a dedicated tip confirmation screen for the customer. If this option is disabled, the tip confirmation screen will be skipped when selecting a tip preset or the NO TIP option. If using custom $ or custom % with this option disabled, the tip amount, percentages and resulting totals will be updated in real-time as the customer types the numbers in, but no additional confirmation screen will be presented before the actual payment.

Tip Presets

Tip presets are used to simplify and speed up the tipping process by allowing customers to select between pre-calculated tip percentages that are commonly used. Any percentage can be configured, but they need to be realistic for the market in which the terminal is used.

- Up to 3 tip presets can be configured.
- Presets configured at 0% are not displayed.
- The space used by each preset button is automatically adjusted to fit the width of the screen, as demonstrated in screenshots below.

One tip preset



Tip Preset (select percentages) 15% | 0% | 0%

TIP

Bill Amount
$35.47

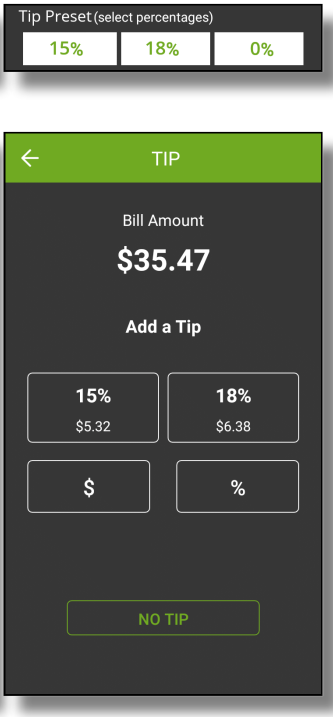
Add a Tip

15% $5.32

$ | %

NO TIP

Two tip presets



Tip Preset (select percentages) 15% | 18% | 0%

TIP

Bill Amount
$35.47

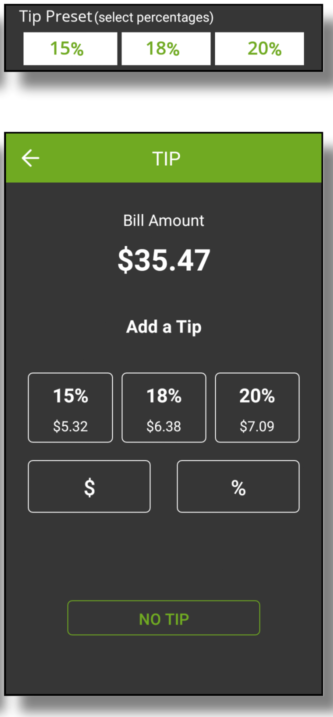
Add a Tip

15% $5.32 | 18% $6.38

$ | %

NO TIP

Three tip presets



Tip Preset (select percentages) 15% | 18% | 20%

TIP

Bill Amount
$35.47

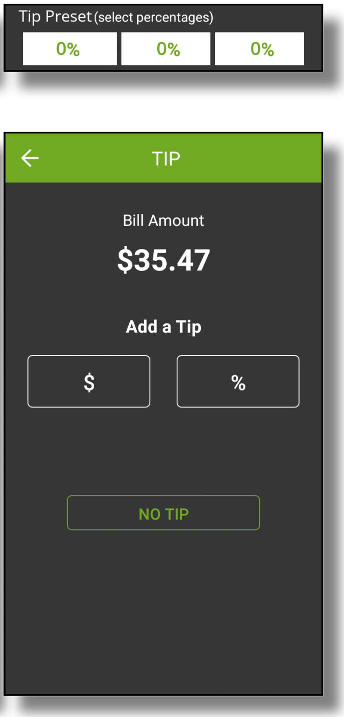
Add a Tip

15% $5.32 | 18% $6.38 | 20% $7.09

$ | %

NO TIP

No tip presets



Tip Preset (select percentages) 0% | 0% | 0%

TIP

Bill Amount
$35.47

Add a Tip

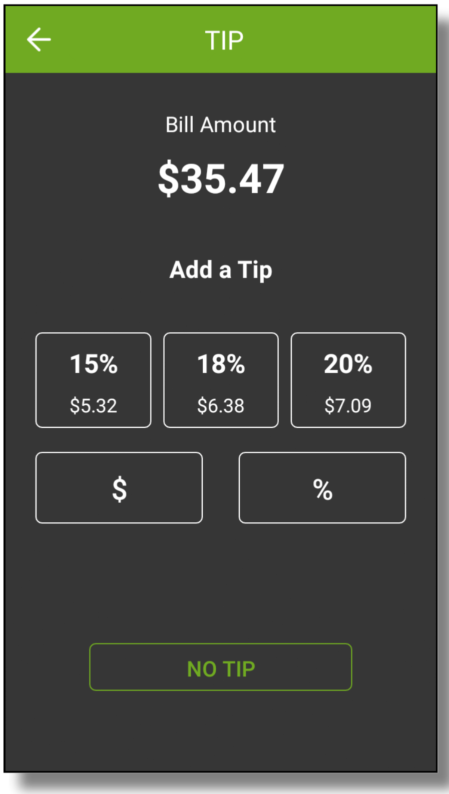
$ | %

NO TIP

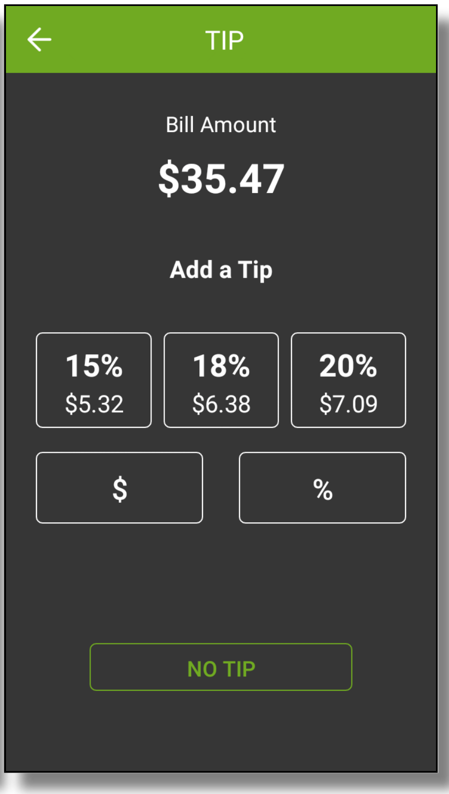
Tip Preset Text Size

The Tip Preset Text Size drop-down allows you to change the font size used to display percentages and amounts in each tip preset. The screenshots below illustrate each available size.

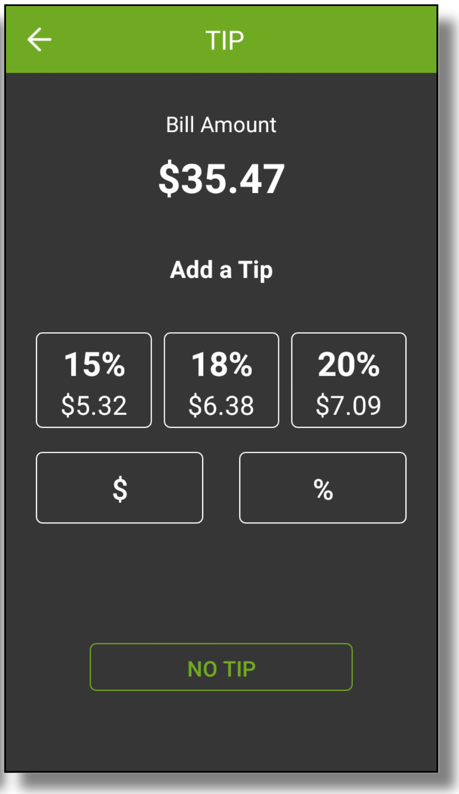
Normal



Medium



Large

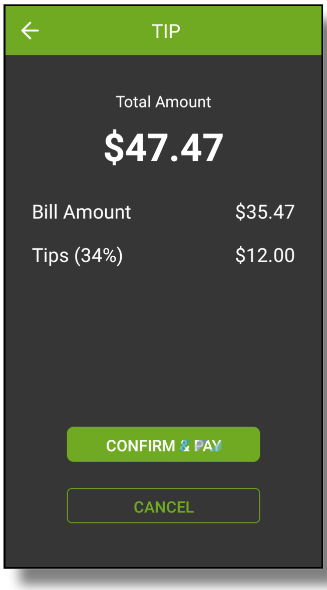


Tip Threshold

The Tip Threshold is a control measure to prevent accidental over-tipping. If the tip amount exceeds the set threshold, SecureTable will request the administrator password before applying the tip.

> **IMPORTANT!** Be sure to carefully evaluate how tips work in the establishment before setting this value. With low value items, the threshold percentage can be exceeded very quickly. For example, buying a water bottle for $2.00 and leaving $1.00 as a tip is already 50% in tip value.

Tip amount is higher than 30% threshold



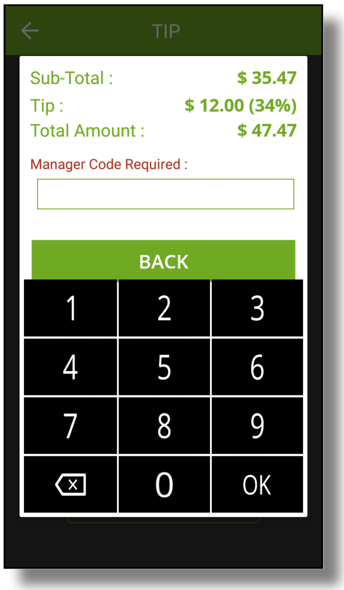
TIP

Total Amount

$47.47

Bill Amount	$35.47
Tips (34%)	$12.00

Manager code is requested after touching the CONFIRM button



TIP

Sub-Total :	$ 35.47
Tip :	$ 12.00 (34%)
Total Amount :	$ 47.47

Manager Code Required :

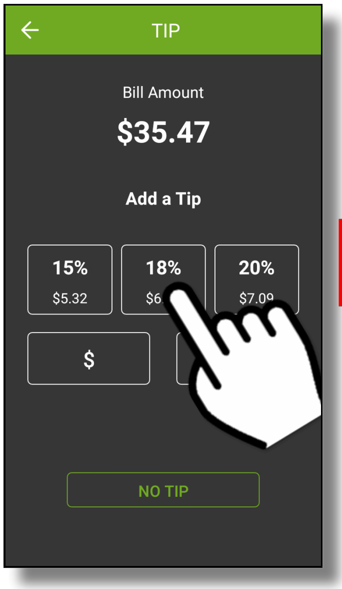
Tip Confirmation

The tip confirmation screen is an extra step which allows the customer to review the details of the payment in a clear, minimalist display, without any other distractions on the terminal screen.

Tip confirmation enabled

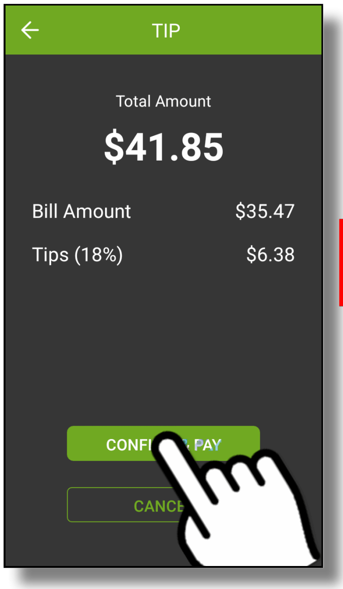
With the tip confirmation option enabled, the customer is presented with the detailed calculation of the tip. This screen also allows the customer to quickly back track and make corrections using the Back (←) button.

Add tip



Bill Amount $35.47

Confirmation screen

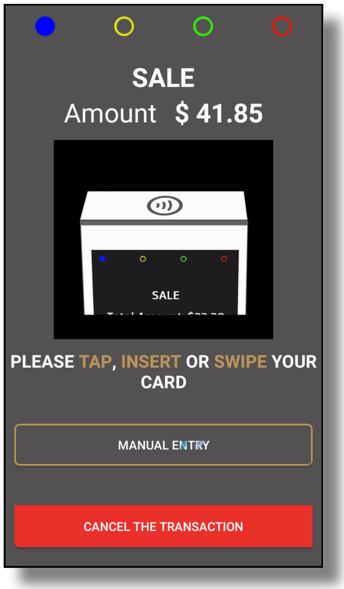


Total Amount $41.85

Bill Amount $35.47

Tips (18%) $6.38

Payment



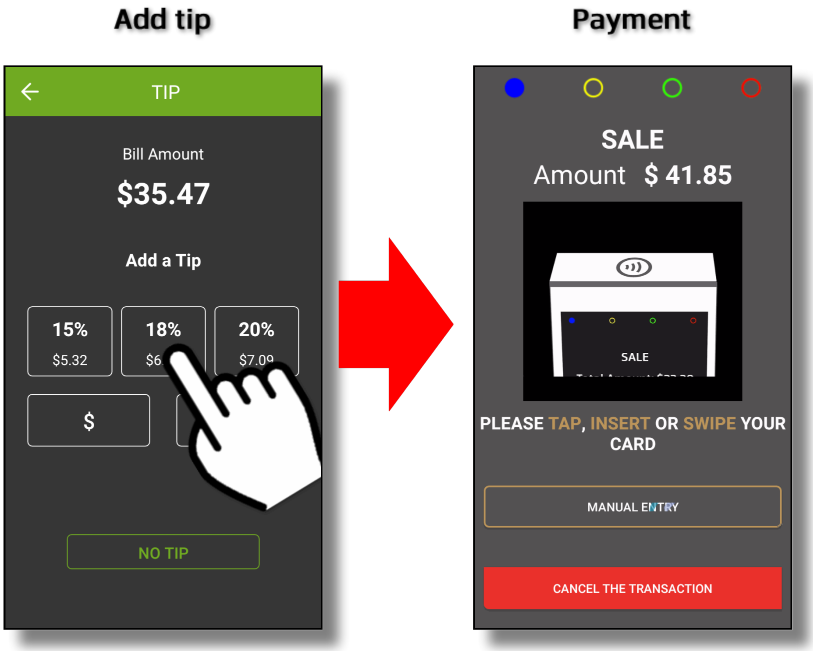
SALE

Amount $ 41.85

PLEASE TAP, INSERT OR SWIPE YOUR CARD

Tip confirmation disabled

If tip confirmation is disabled, the confirmation screen is skipped and the terminal proceeds directly to the payment. If the customer notices a mistake once the payment process is started, the transaction needs to be canceled at the payment application which will bring the customer back to the tip calculation screen.

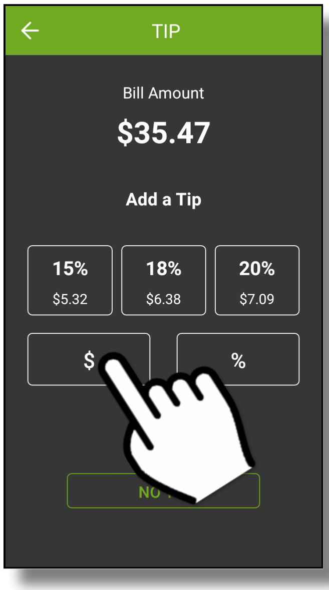


For more details and to quickly see the difference between various configurations, consult the workflows below:

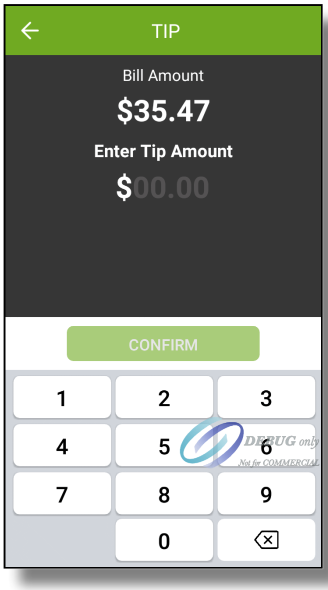
Using custom tip amount with tip confirmation enabled

This workflow shows the screens that the customer will go through while applying a tip using a custom amount and with tip confirmation enabled.

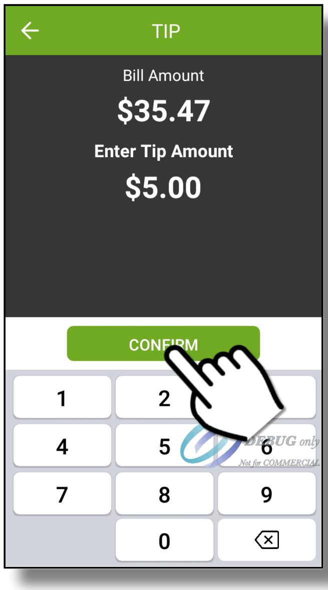
Select custom $



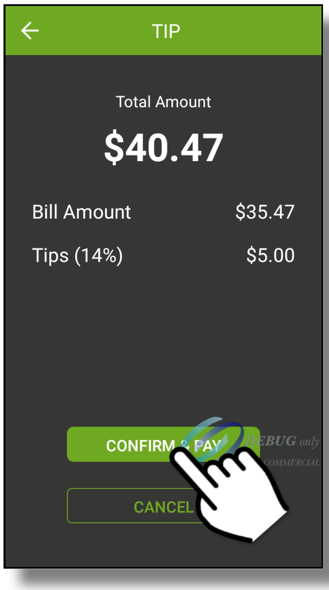
Enter amount



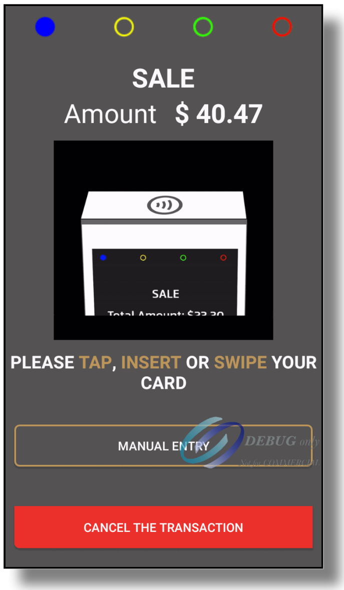
Confirm



Confirmation screen



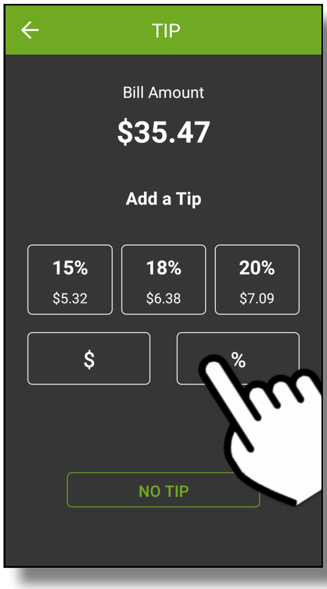
Payment



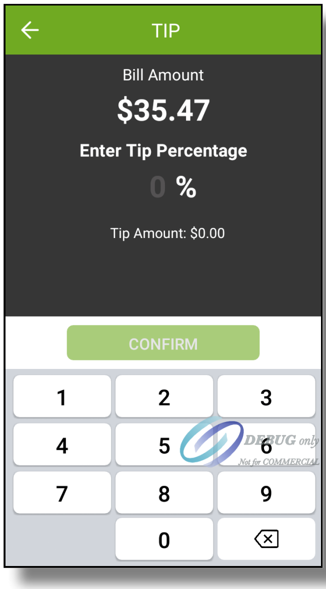
Using custom tip percentage with tip confirmation enabled

This workflow shows the screens that the customer will go through while applying a tip using a custom percentage and with tip confirmation enabled.

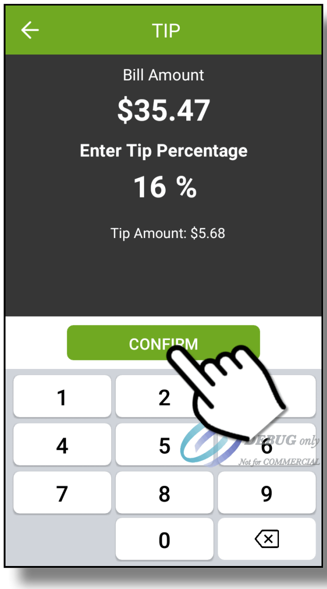
Select custom %



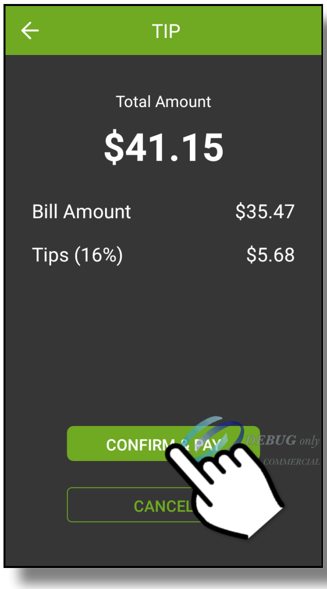
Enter percentage



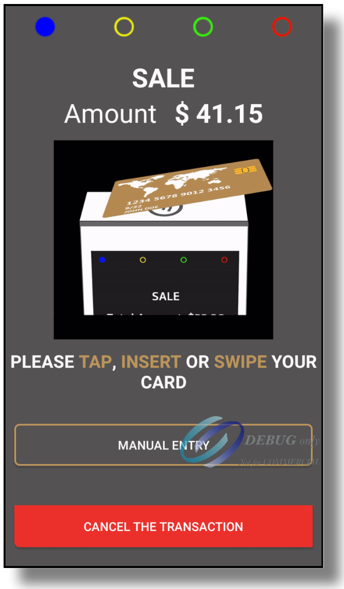
Confirm



Confirmation screen



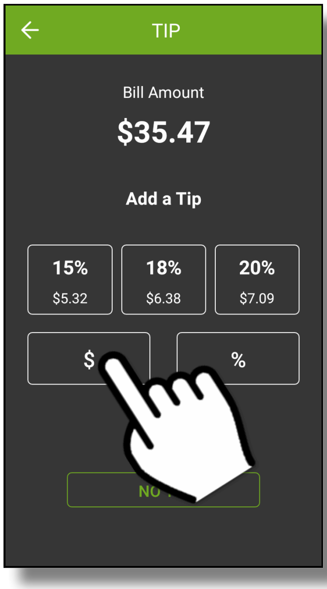
Payment



Using custom tip amount with tip confirmation disabled

This workflow shows the screens that the customer will go through while applying a tip using a custom tip amount and with tip confirmation disabled.

Select custom $

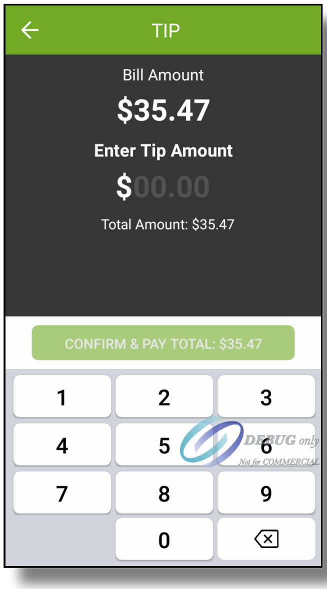

TIP

Bill Amount

$35.47

Add a Tip

Enter amount


TIP

Bill Amount

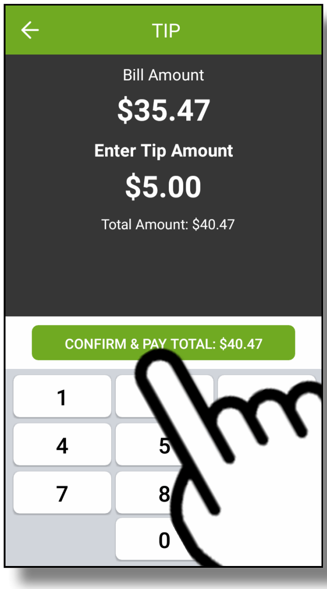
$35.47

Enter Tip Amount

$00.00

Total Amount: $35.47

Confirm


TIP

Bill Amount

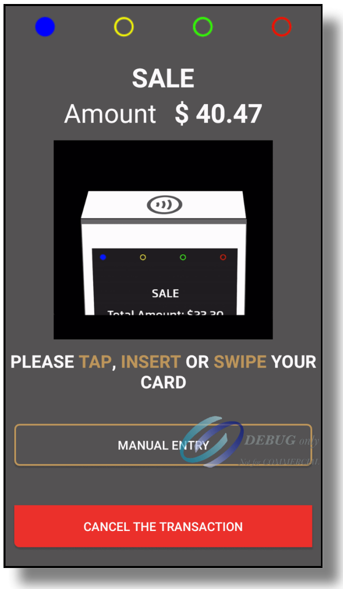
$35.47

Enter Tip Amount

$5.00

Total Amount: $40.47

Payment


SALE

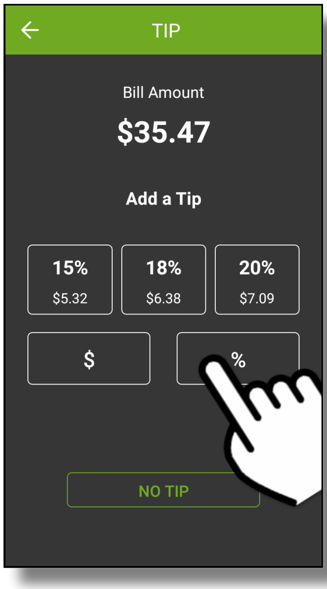
Amount $ 40.47

PLEASE TAP, INSERT OR SWIPE YOUR CARD

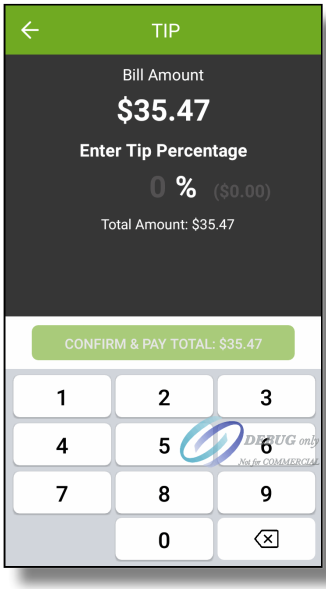
Using custom tip percentage with tip confirmation disabled

This workflow shows the screens that the customer will go through while applying a tip using a custom tip percentage and with tip confirmation disabled.

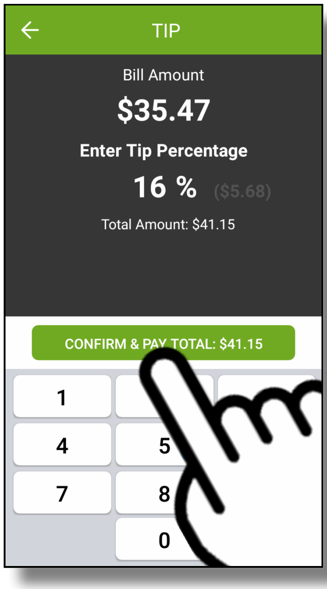
Select custom %



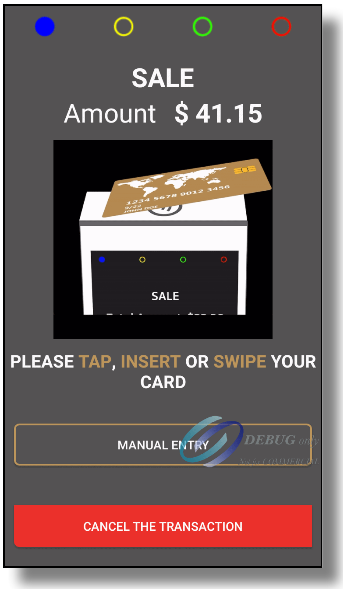
Enter percentage



Confirm



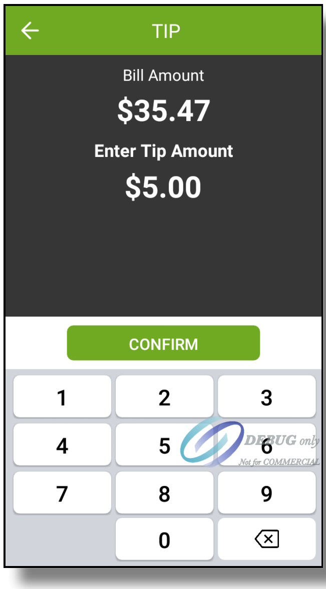
Payment



Comparison: Custom Tip Amount with confirmation enabled/disabled

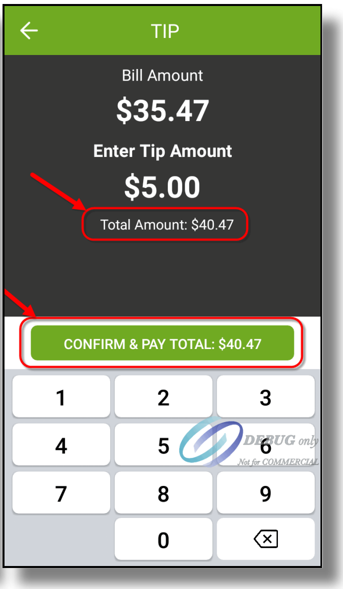
The screenshots below illustrate the differences in the custom tip amount screen when tip confirmation is enabled or disabled. Notice how the screen with confirmation disabled shows more information. This is to compensate for the absence of the dedicated confirmation screen.

Confirmation Enabled **Confirmation Disabled**


TIP

Bill Amount
$35.47

Enter Tip Amount
$5.00


TIP

Bill Amount
$35.47

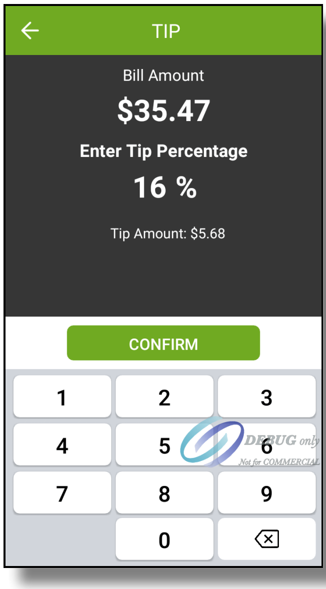
Enter Tip Amount
$5.00

Total Amount: $40.47

Comparison: Custom Tip Percentage with confirmation enabled/disabled

The screenshots below illustrate the differences in the custom tip percentage screen when tip confirmation is enabled or disabled. Notice how the screen with confirmation disabled shows more information. This is to compensate for the absence of the dedicated confirmation screen.

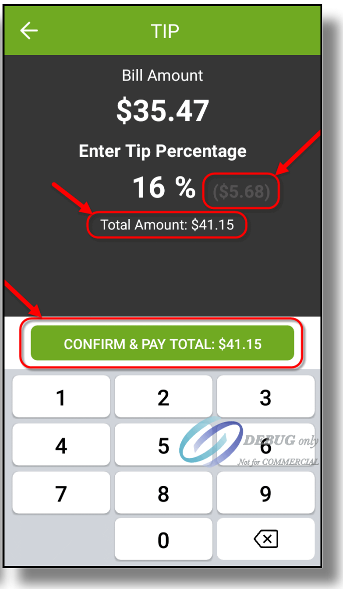
Confirmation Enabled **Confirmation Disabled**


TIP

Bill Amount
$35.47

Enter Tip Percentage
16 %

Tip Amount: $5.68


TIP

Bill Amount
$35.47

Enter Tip Percentage
16 % ($5.68)

Total Amount: $41.15

Voids

SecureTable supports voids initiated by the POS system. To be able to use this feature, the POS system must support it as well.

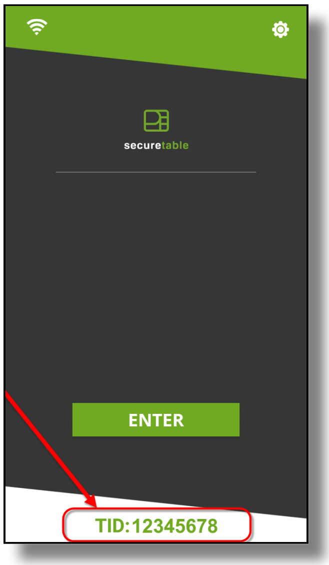
Void Sale

The Void Sale operation consists in cancelling a sale transaction that was carried out in the current transaction batch. With this operation, the funds are returned to the customer.

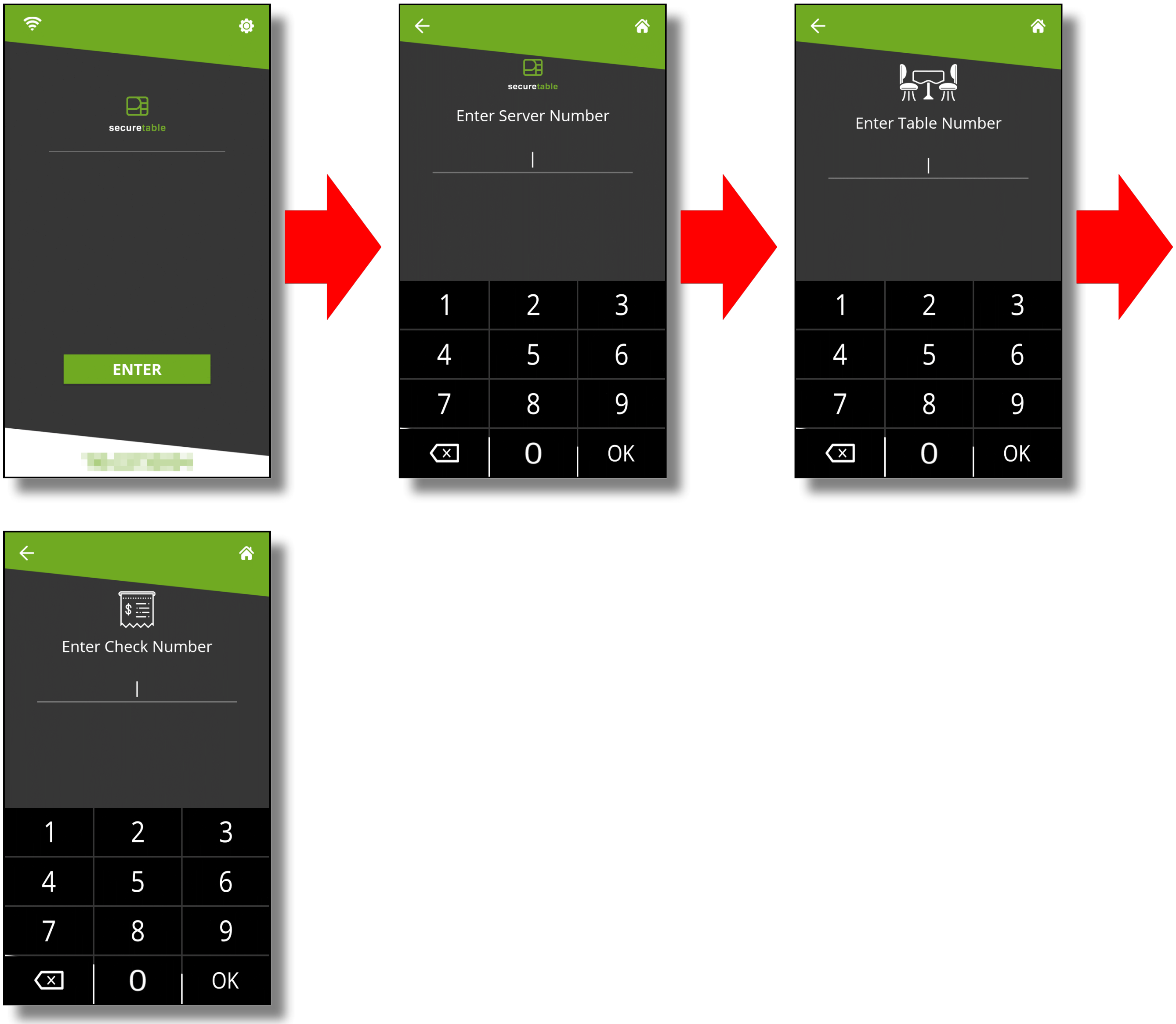
> **IMPORTANT!** Only transactions from the Current Batch can be voided. Transactions that belong to a closed batch cannot be voided. To refund a transaction belonging to a closed batch, see Refunds.

1. Initiate the void from the POS system. The POS system should tell you which Terminal ID was used in the original transaction, as well as the original check or invoice number. The information should be available either on-screen or on a printed coupon.

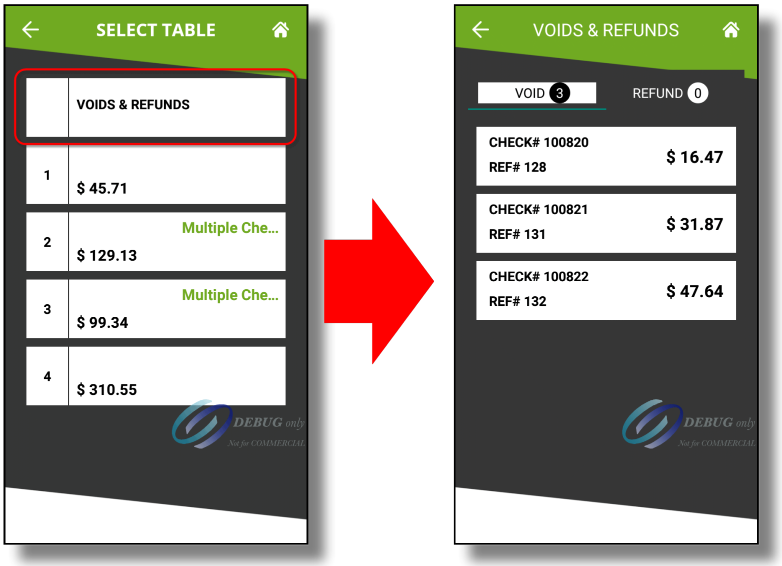
2. Locate the payment terminal with the appropriate Terminal ID (TID). On the SecureTable application, the terminal ID (TID) is displayed in green at the bottom of the home screen and consists of 8 digits.



3. Logon to SecureTable with your employee number. There is no need to enter a table or check number, so simply touch OK without entering anything if prompted for those.



4. If there are voids to be treated, you will see a section for Voids at the top of the list of tables and checks. Touch the Voids box, which will display the list of pending voids.

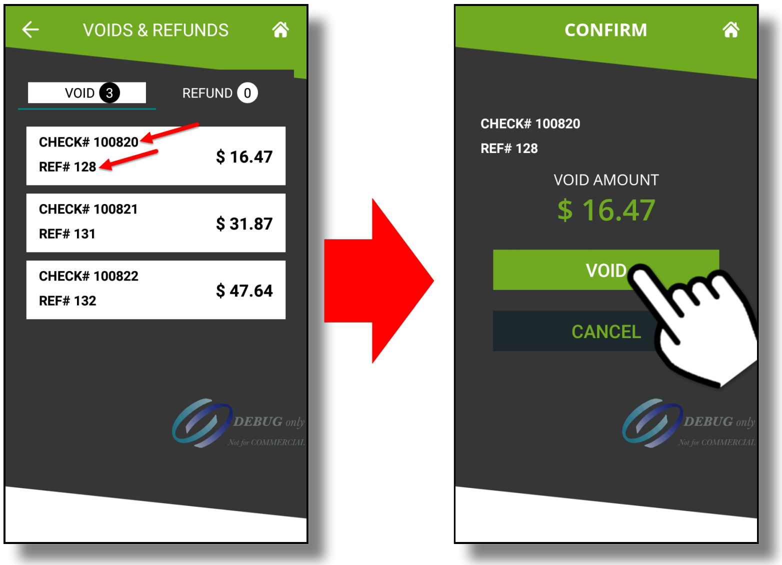


1	$ 45.71
2	Multiple Che... $ 129.13
3	Multiple Che... $ 99.34
4	$ 310.55

CHECK# 100820 REF# 128	$ 16.47
CHECK# 100821 REF# 131	$ 31.87
CHECK# 100822 REF# 132	$ 47.64

NOTE: If you don't see the Voids section, it means that no voids were initiated from the POS system, or your POS system does not support this feature with SecureTable

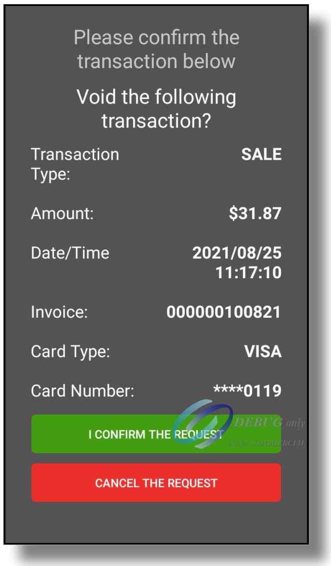
5. Locate the box that represents the transaction you wish to void and touch it. If multiple pending voids are listed, use the invoice (check) number or reference number to locate the one you wish to process. Touch the VOID button to initiate the process.



CHECK# 100820 REF# 128	$ 16.47
CHECK# 100821 REF# 131	$ 31.87
CHECK# 100822 REF# 132	$ 47.64

CHECK# 100820
REF# 128
VOID AMOUNT
$ 16.47

6. The payment application will display the transaction details. Verify that this is indeed the transaction you wish to void, then:



Please confirm the transaction below

Void the following transaction?

Transaction Type: **SALE**

Amount: **$31.87**

Date/Time **2021/08/25 11:17:10**

Invoice: **000000100821**

Card Type: **VISA**

Card Number: ******0119**

   a. touch the green "***I CONFIRM THE REQUEST***" button to proceed, or;

   b. Touch the red "***CANCEL THE REQUEST***" button to return to SecureTable. (This will return to the SecureTable Home Screen.)

7. At this point, whether the customer will need to manipulate the payment terminal depends on the type of card used for the original payment.

   a. For credit cards, no further manipulation is required and the void will be processed automatically.

   b. For debit cards, hand the payment terminal to the customer. The customer will insert the original payment card and follow the prompts to process the void.

8. Once the process is completed, the terminal will return to the SecureTable home screen.

Task: Add an APN to your Android Payment Terminal

What is an APN?

An Access Point Name (APN) is the name of a gateway between a GSM, GPRS, 3G or 4G/LTE mobile network and another computer network, frequently the public Internet. In simple terms, an APN is required for your mobile device to be able to access the Internet through the carrier's mobile network.

Most mobile devices (phones, tablets, etc.) supplied by common carriers come with the carrier's APN pre-configured, so most users don't need to worry about manually configuring an APN.

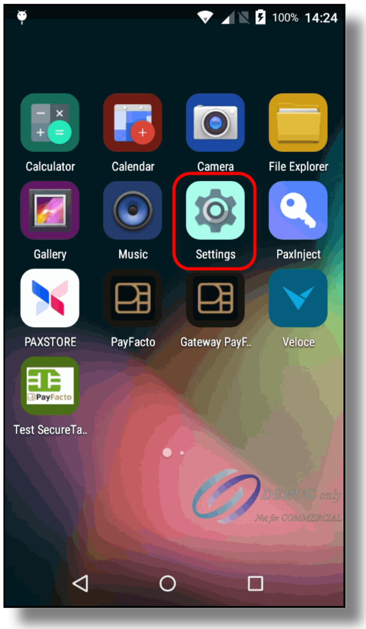
However, mobile devices provided by PayFacto are carrier-agnostic, so they can connect to your carrier of choice to access GSM, GPRS, 3G or 4G/LTE mobile networks for mobile payment processing. For this reason, the APN can't be configured in advance and therefore needs to be configured manually.

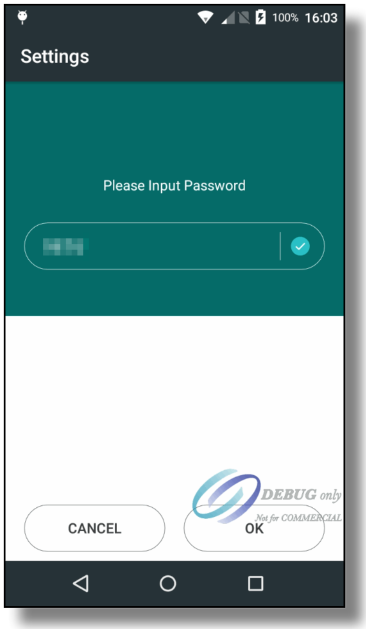
Before you begin

Before configuring an APN on your Android terminal, be sure to have a SIM card installed in your terminal. Please review the documentation specific to your terminal model to learn how to install a SIM card.

Access Android APN Settings

1. Exit any payment application that may be running on the terminal. You should now see the home screen of your terminal.
2. Touch the ***settings*** app icon to access the device's settings.
3. A password prompt will appear. Enter the device's password and touch the ***OK*** button.

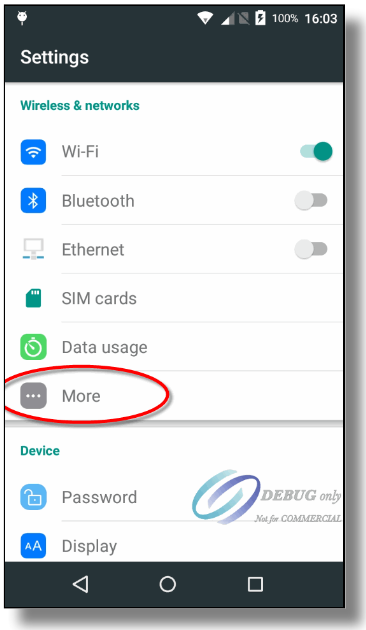


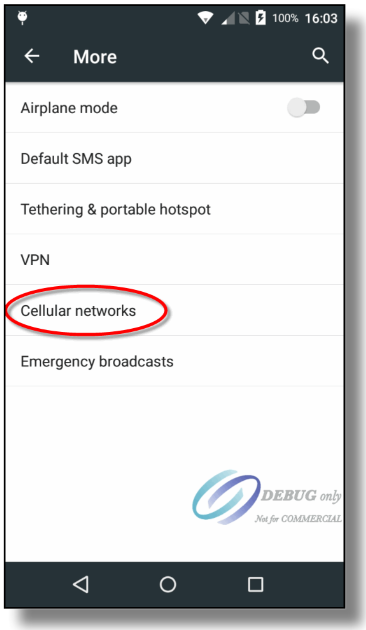


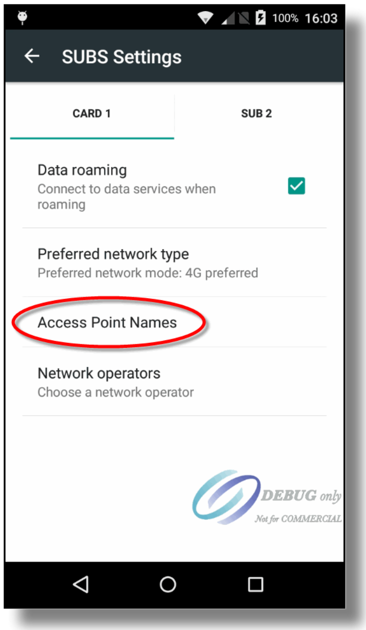
> **NOTE:** Settings passwords are changed before shipping to end-users. Passwords are unique to each terminal. Please review the documentation that came with your terminal to find your settings password.

4. In the ***Wireless & Networks*** section, touch the ***More...*** option.

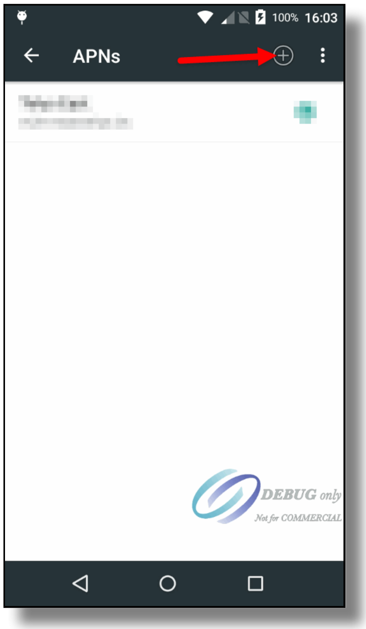
5. Touch ***Cellular Networks***.
6. Touch ***Access Point Names***.







7. The first time you access this setting, the list of APN's should be empty. Touch the "**+**" sign at the very top of the list to add a new entry.



8. Configure the following settings:

   Name

   Give a meaningful name to this APN. This generally corresponds to your mobile network carrier name.

   APN

   This is the actual name of the gateway. **This is provided by your mobile service carrier.**

   MCC

   The default value for this setting is ***302***. Leave it to the default value **unless otherwise specified by your mobile service carrier.**

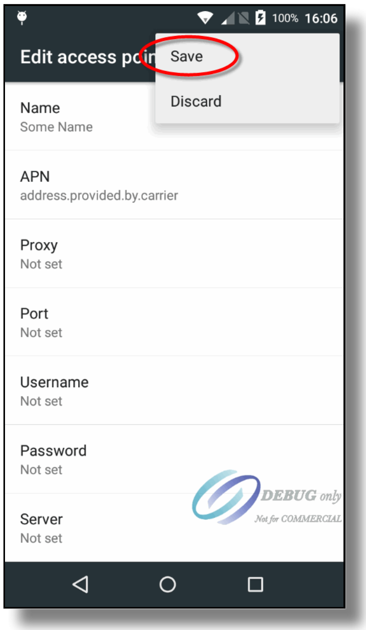
   MNC

   The default value for this setting is ***760***. Leave it to the default value **unless otherwise specified by your mobile service carrier.**

   Other settings

   The settings listed above are the minimal settings required to get an APN to work properly. Different carriers may require additional settings to be configured. Please inquire with your mobile service carrier.

9. Touch the 3 dots at the top-right of the screen and select ***Save***.



Name
Some Name

APN
address.provided.by.carrier

Proxy
Not set

Port
Not set

Username
Not set

Password
Not set

Server
Not set

10. The new APN will appear in the list.

11. Use the ***Back*** button to exit all the way back to the home screen.

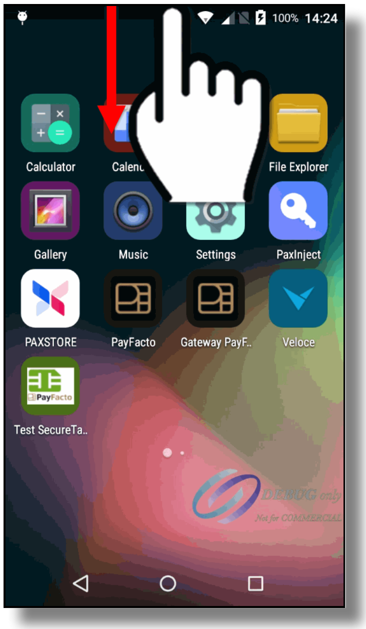
Test your APN

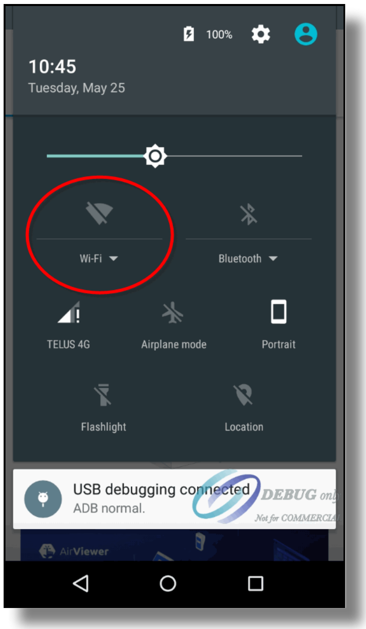
To make sure that your APN and SIM card work properly, they need to be tested. Unfortunately, payment terminals don't have browsers which would allow for a quick and easy test, but here's a workaround:

Disable WiFi

Disabling WiFi will ensure that you are testing Internet connectivity through the mobile network only.

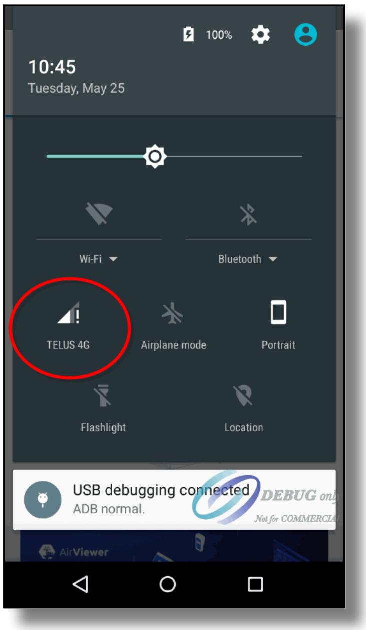
From the Home screen, swipe twice from the very top of the screen. This will show some quick settings for the terminal. Touch the Wi-Fi icon to disable your Wi-Fi connection.

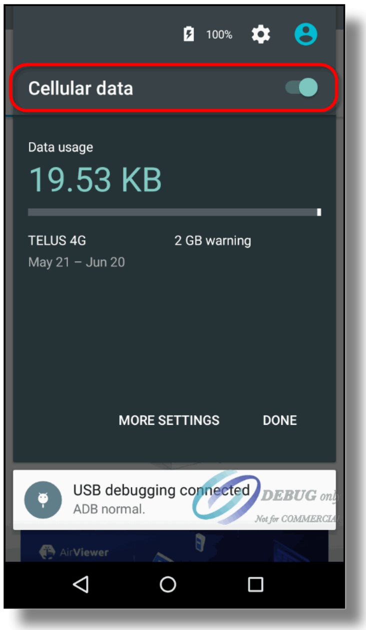




Enable cellular data

While still in the settings screen, touch the Cellular Data icon. Then, make sure that the ***Cellular Data*** option is enabled.

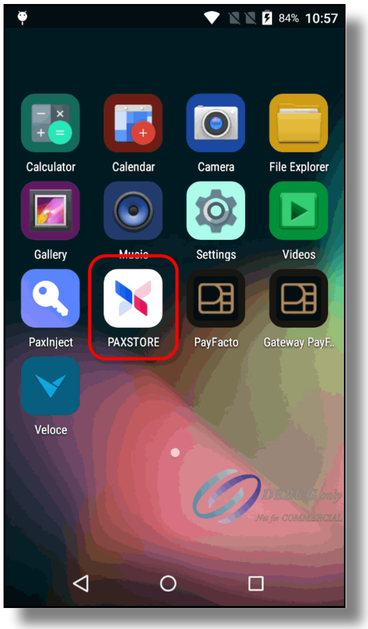




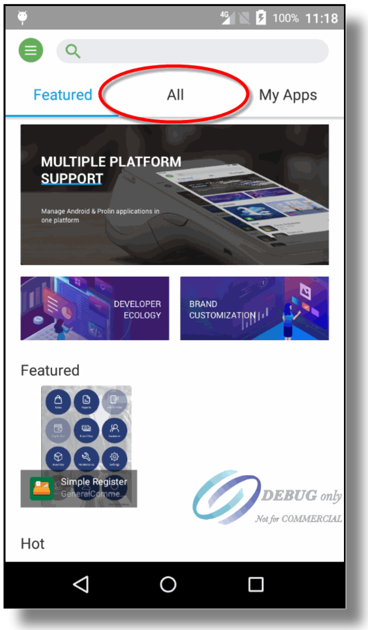
Start the PAX Store

Since the PAX Store requires Internet connectivity to allow you to download applications, you can use it to tell if your APN and SIM card are working properly.

Start the ***PAXSTORE*** by touching its icon on the home screen.

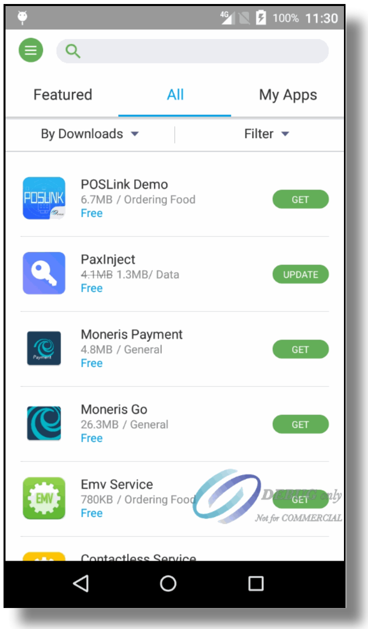


Once in the PAXSTORE, touch ***"All"*** near the top of the screen.



APN and cellular data working correctly

If the APN is correctly configured and that Internet access is working properly through the mobile network, you will see a list of applications that can be downloaded and installed:



100% 11:30

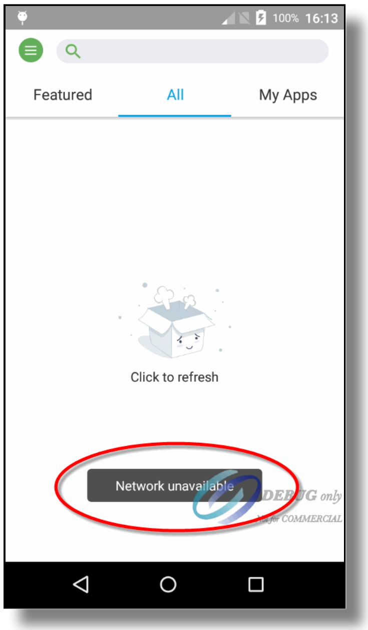
Featured | All | My Apps

By Downloads ▾ | Filter ▾

- POSLink Demo — 6.7MB / Ordering Food — Free — GET
- PaxInject — ~~4.1MB~~ 1.3MB/ Data — Free — UPDATE
- Moneris Payment — 4.8MB / General — Free — GET
- Moneris Go — 26.3MB / General — Free — GET
- Emv Service — 780KB / Ordering Food — Free — GET
- Contactless Service

Internet access not working

If the APN is not configured correctly or if there is an issue with Internet connectivity through the mobile network, you will see a message saying ***"Network Unavailable"*** briefly displayed on the screen. Instead of the applications list, you will see a ***"Click to refresh"*** message and an empty box icon.



100% 16:13

Featured | All | My Apps

Click to refresh

Network unavailable

If Internet access is not working, please review your APN settings and try restarting your terminal. If Internet access through mobile networks still doesn't work, please call the PayFacto help desk or your mobile network carrier for assistance.

Re-enable WiFi

Now that Internet access through the mobile network is tested, don't forget to re-enable WiFi to keep data usage from the mobile network at a minimum.

Task: Configure Port Forwarding

In this task, we will configure Port Forwarding on a router/firewall device to allow SecureTable to communicate with the POS system through the STPI Client while delivery drivers are on their delivery routes. The device used in this tutorial is an Asus RT-AC66U B1 wireless router and firewall. While the exact settings and menus will differ between models and manufacturers, the general principles are the same.

Corporate Networks

If your restaurant's network is managed by a larger entity, such as a franchise head office or a network administrator, please communicate with them to inquire about setting up port forwarding. you can also provide your network administrator with the instructions below. They should be able to adapt them to your needs.

Do I need Port Forwarding and if so, why?

Port Forwarding is generally required when using SecureTable over mobile networks. If you don't use SecureTable over mobile networks, there is no need to configure port forwarding and you can skip this tutorial altogether. Also, some mobile carriers may offer special VPN access to your local network, which is a more secure alternative to port forwarding. Please inquire with your mobile carrier to see if they offer this option. If they do, Port Forwarding will not be required.

SecureTable is used over mobile networks mostly by delivery drivers. However, mobile network connectivity is also useful to cover gaps in a restaurant's WiFi coverage.

When SecureTable is used locally in the restaurant, payment terminals are able to communicate with the POS system through the STPI client directly over the local WiFi network. However, when drivers are out on the road, the payment terminals need to use mobile networks to access the Internet to authorize payments. Being on the "public" Internet, the payment terminal will not be able to communicate directly with the POS system to close the delivery orders. This is where Port Forwarding comes in. To connect to the POS system, the payment terminal needs to connect to the restaurant's router, which will then redirect the communication to the STPI Client via port forwarding.

An analogy often used to describe this is finding the bathroom inside your house. For anyone currently inside the house, finding the bathroom should be quite easy. However, for someone currently outside of the house, they first need to know your home address, then someone from inside the house needs to let them in and show them the way to the bathroom. This is essentially what happens when a payment terminal running SecureTable is being used on the road.

Information needed

Before you begin the actual configuration, you need the following information:

- Your router's ***public*** IP address.
- Your router's ***private*** IP address.
- Your router's username and password to access its configuration utility.
- IP address and TCP port used by the STPI Secure Client.

Here are short instructions to find each piece of information:

Your router's public IP address

This is the IP address that is given to your router by your Internet Service Provider (ISP). It is called a "public" address because it is facing the public Internet. You can easily find what is your public IP address by visiting the following site:

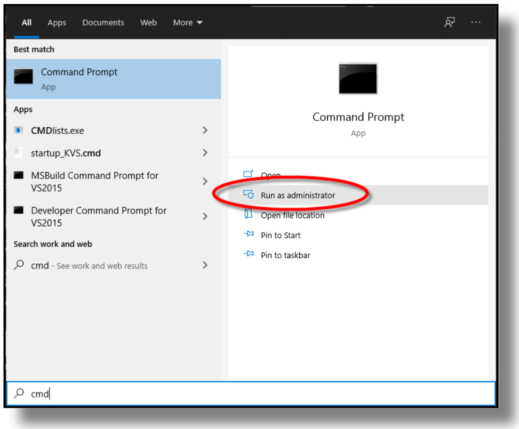
ip4.me

IP4.me is a simple site that will display your public IP address without any ads or unneeded information.

Your router's private IP address

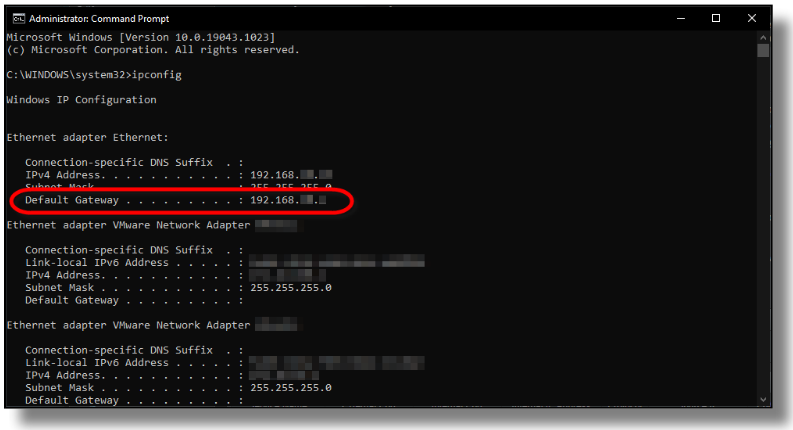
As its name suggests, the router's private IP address is invisible to the outside world. To find it, you need to be connected to your local network and follow these simple instructions:

1. Open a command prompt with administrative privileges. Do so by clicking the Windows Start menu and typing ***CMD***. Then, select ***Run as Administrator*** under the ***Command Prompt*** app.



2. In the command prompt window, type ***ipconfig*** and press the ***ENTER*** key.

3. Look for the line that starts with ***Default Gateway***, and take note of the IP address listed there. This is the private IP address of your router.


Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.19043.1023]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.[redacted].[redacted]
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.[redacted].[redacted]
Ethernet adapter VMware Network Adapter [redacted]

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : [redacted]
   IPv4 Address. . . . . . . . . . . : [redacted]
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter [redacted]

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : [redacted]
   IPv4 Address. . . . . . . . . . . : [redacted]
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```

Your router's username and password

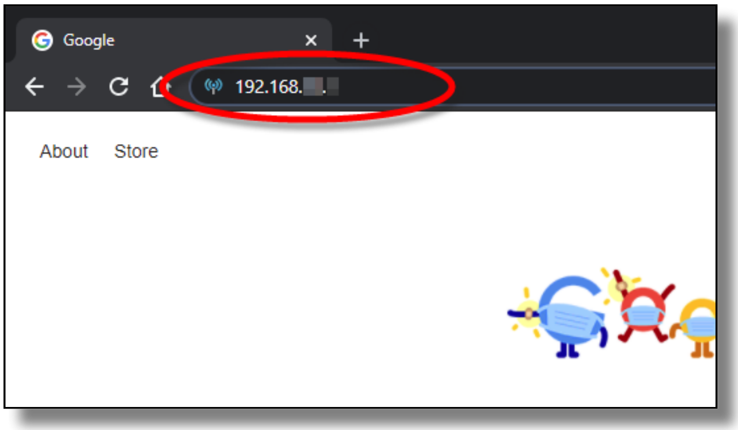
Every modern router has a configuration utility that is protected by a username and password. If you don't know what it is, either contact your network administrator or look for the default username and password in your device's documentation.

STPI Secure's IP address and TCP port number

This is the IP address of the PC where STPI Secure has been installed. The TCP port number is normally configured during the installation. The default recommended value for the TCP port is 9999, but it could be configured differently during the installation process.

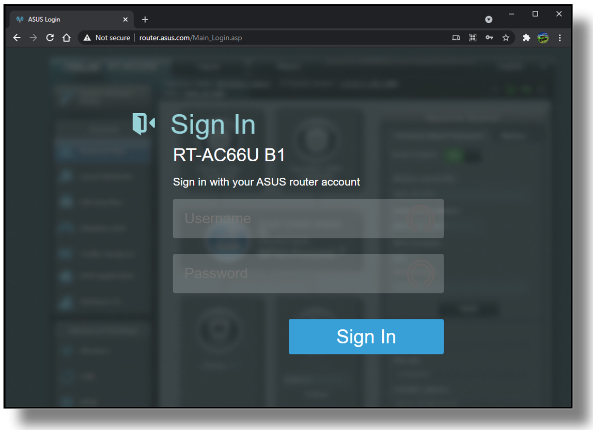
Access your router's configuration page

1. From a PC connected to the local network, open your favorite browser (Google Chrome, Microsoft Edge, Firefox, etc.) and type your router's ***private IP address*** in the address bar. Press ***ENTER*** on your keyboard.



192.168.[redacted]

2. The login screen for your router's configuration utility should be displayed. Type the username and password that will allow you to login to your device. This screen will differ depending on your device's manufacturer and model.



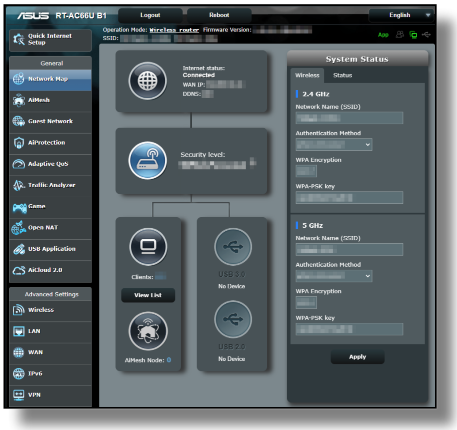
Not secure | router.asus.com/Main_Login.asp

Sign In

RT-AC66U B1

Sign in with your ASUS router account

3. Your router's main configuration screen should be displayed.



Operation Mode: Wireless router Firmware Version: [redacted]
SSID: [redacted]

Internet status:
Connected
WAN IP: [redacted]
DDNS: [redacted]

Security level: [redacted]

Clients: [redacted]

AiMesh Node: 0

USB 3.0
No Device

USB 2.0
No Device

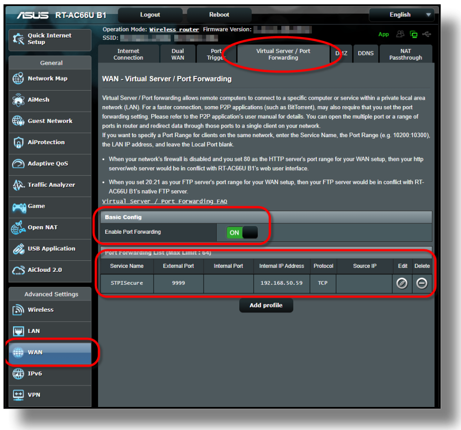
System Status

2.4 GHz
Network Name (SSID) [redacted]
Authentication Method [redacted]
WPA Encryption [redacted]
WPA-PSK key [redacted]

5 GHz
Network Name (SSID) [redacted]
Authentication Method [redacted]
WPA Encryption [redacted]
WPA-PSK key [redacted]

Enable and Configure Port Forwarding

1. Look for ***Port Forwarding*** settings. This is typically found in ***WAN settings***, under ***Advanced settings***. Again, this will be different based on your device's manufacturer and model. Please consult your device's documentation if you can't find the appropriate settings.



Operation Mode: Wireless router Firmware Version: [redacted]
SSID: [redacted]

WAN - Virtual Server / Port Forwarding

Virtual Server / Port forwarding allows remote computers to connect to a specific computer or service within a private local area network (LAN). For a faster connection, some P2P applications (such as BitTorrent), may also require that you set the port forwarding setting. Please refer to the P2P application's user manual for details. You can open the multiple port or a range of ports in router and redirect data through those ports to a single client on your network.
If you want to specify a Port Range for clients on the same network, enter the Service Name, the Port Range (e.g. 10200:10300), the LAN IP address, and leave the Local Port blank.

- When your network's firewall is disabled and you set 80 as the HTTP server's port range for your WAN setup, then your http server/web server would be in conflict with RT-AC66U B1's web user interface.
- When you set 20:21 as your FTP server's port range for your WAN setup, then your FTP server would be in conflict with RT-AC66U B1's native FTP server.

Virtual Server / Port Forwarding FAQ

Basic Config

Enable Port Forwarding: ON

Port Forwarding List (Max Limit : 64)

Service Name	External Port	Internal Port	Internal IP Address	Protocol	Source IP	Edit	Delete
STPISecure	9999		192.168.50.59	TCP			

2. Enable ***Port Forwarding***.
3. Add a port forwarding entry with the following parameters:

Service Name

STPISecure

External Port

TCP Port number used by STPISecure. Default: 9999

Internal Port

Leave blank.

Internal IP Address

IP address of the PC where STPI Secure was installed.

Protocol

TCP

Source IP

Leave blank.

4. Save your settings.
5. Some router models may need to be rebooted. Please refer to your device's documentation to learn how to do this.

The task of configuring port forwarding on your router is now complete.

Task: Switch between Wifi and 4G/LTE

The SecureTable application has the ability to use Wifi and mobile networks to communicate with your POS system. Switching from one network to the other generally occurs automatically and transparently, but there are situations where users may want to control how and when the application switches networks.

One such example is if you have areas at the limit of the Wifi range. In such an area, the terminal may repeatedly switch between Wifi and mobile networks, causing connectivity issues. In this case, the user may want to force the application to use the mobile network all the time while in that area.

Prerequisites

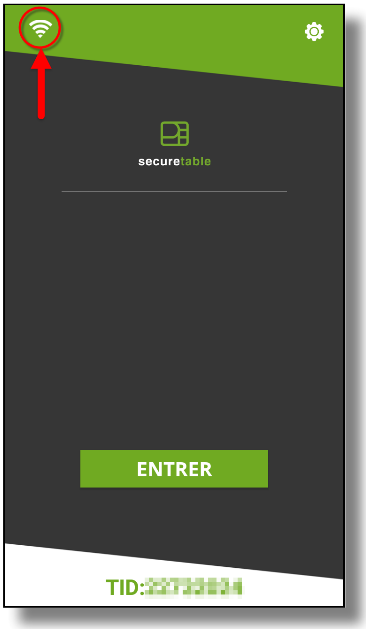
Before using mobile networks with SecureTable, the following requirements need to be met:

- Use SecureTable ***version 4.67.6 or later***.
- Use an Android payment terminal ***equipped with a SIM card***. (The SIM card is provided by your preferred mobile network carrier.)
- ***Configure an APN*** on your Android terminal to allow Internet connectivity through mobile networks. You can learn how to configure an APN here: Task : Add an APN to Your Payment Terminal.
- ***Setup Port Forwarding*** on your router/firewall. A generic walkthrough is provided here: Task : Configure Port Forwarding
- Configure ***Redundant Network*** as described here: Configure Redundant Network options

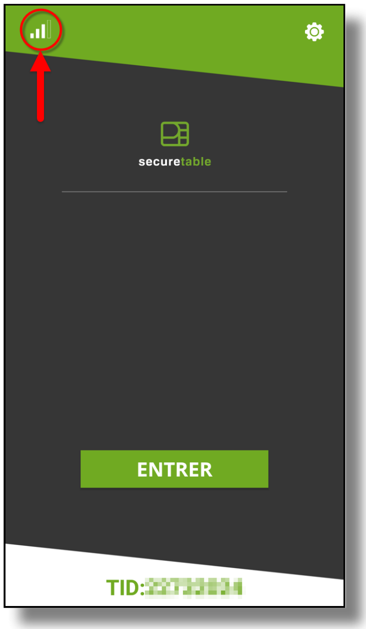
Knowing Current Network Status

You can always tell which network SecureTable is currently using by looking at the icon in the upper-left corner of the home screen:

SecureTable operating on Wifi

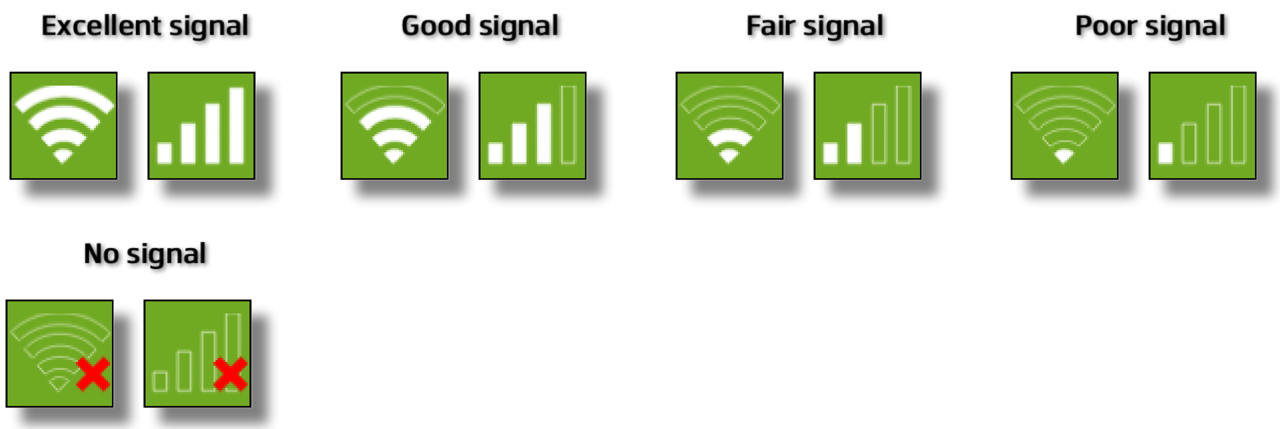


SecureTable operating on Mobile



Signal Strength

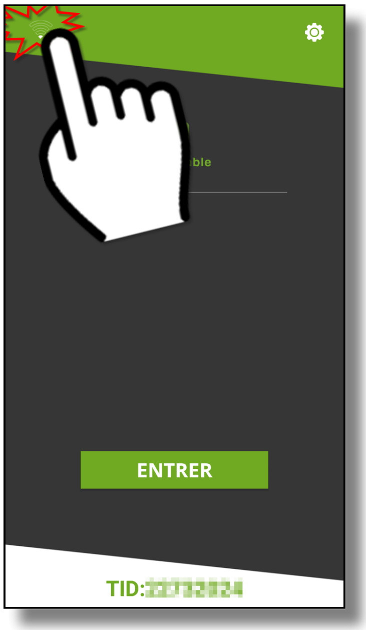
The icon also informs the user of the signal strength.



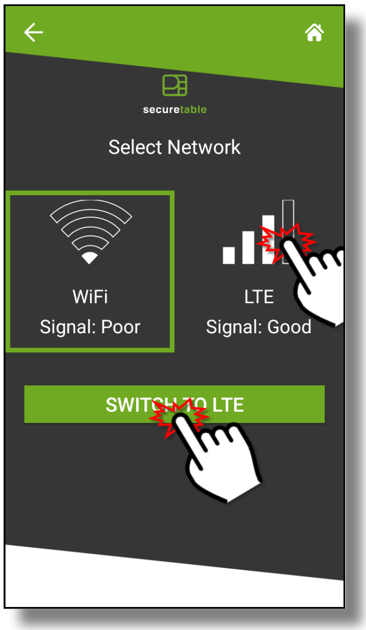
Manual Network Switching from Wifi to LTE

By default, SecureTable will always try to connect to known Wifi networks to reduce fees related to data usage over mobile networks. However, it is possible to force SecureTable to use mobile networks. This is useful to cover blind spots in Wifi coverage or in areas at the limit of Wifi range, where the signal can be unstable.

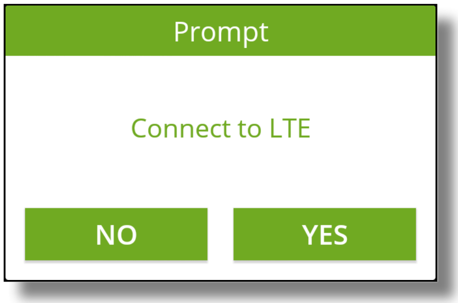
1. Touch the Wifi icon in the upper-left corner of the screen.



2. Touch the LTE signal icon or the SWITCH TO LTE button.



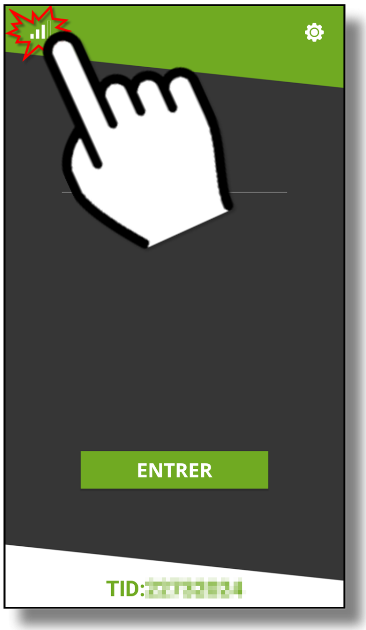
3. A confirmation dialog will appear. Touch YES to switch to LTE.



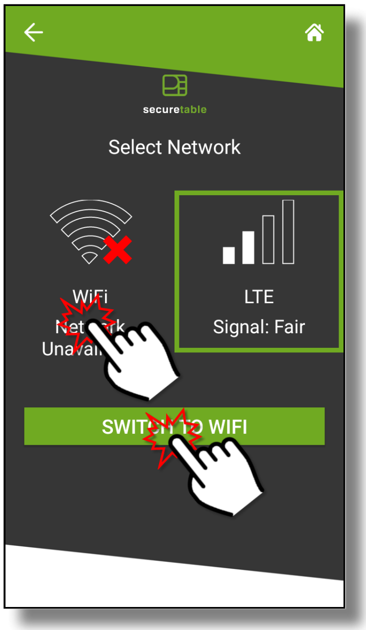
IMPORTANT! After manually switching to LTE, SecureTable will not try to switch back to Wifi on its own. If you wish to use Wifi again, you will need to switch to Wifi manually.

Manual Network Switching from LTE to Wifi

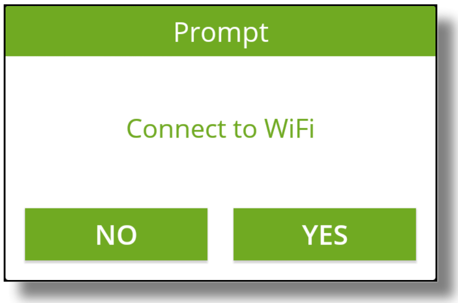
1. Touch the 4G/LTE icon in the upper-left corner of the screen.



2. Touch the Wifi signal icon or the SWITCH TO WIFI button.



3. A confirmation dialog will appear. Touch YES to switch to Wifi.



Prompt

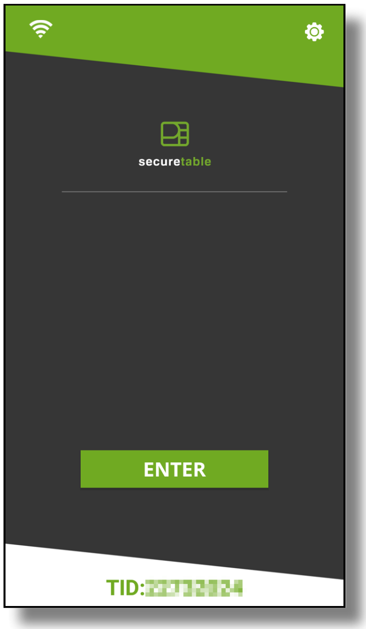
Connect to WiFi

> **IMPORTANT!** In the Select Network screen, the Wifi network appears as if it is unavailable. This is normal. This is because the Wifi antenna of the terminal was disabled during the manual switch to LTE. If the terminal is within Wifi range, switching back to Wifi will reactivate the antenna and reconnect to the network.

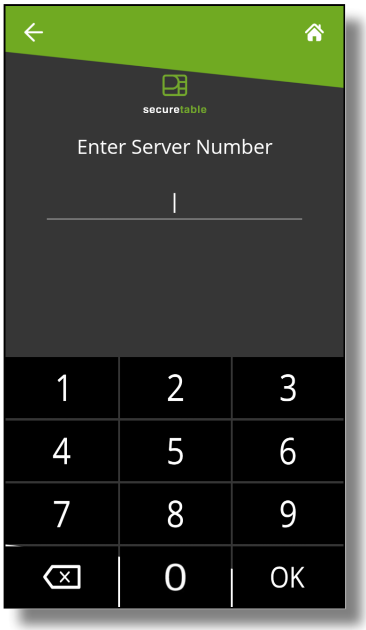
Automatic Network Switching during a transaction

When the option Auto-connect to LTE is enabled, SecureTable can attempt to connect to LTE in the event that the connection fails over Wifi. This failover feature will only occur during a transaction process. It will never happen when the SecureTable application is idle.

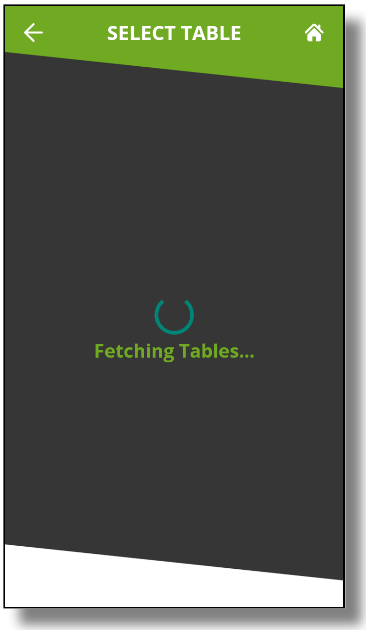
1. Start a transaction as you normally would, by touching the ENTER button.



2. Input your server number and touch OK.

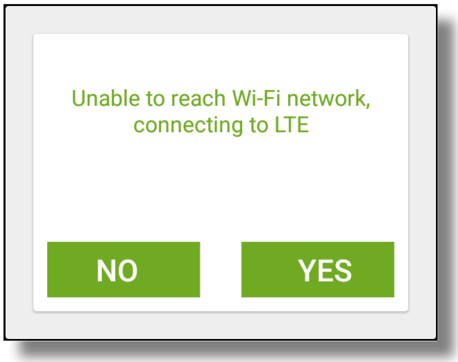


3. If there is an issue with the Wifi connectivity, the terminal will remain on "Fetching tables" longer than usual.



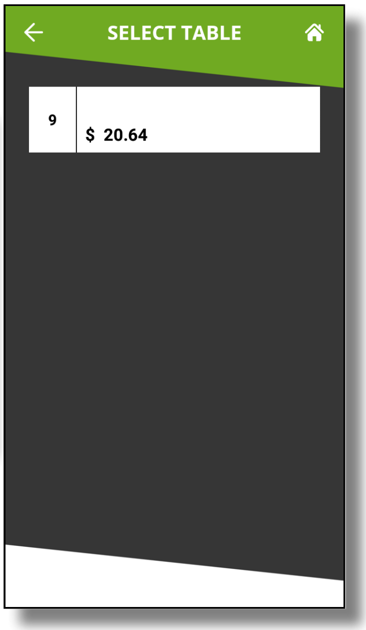
Fetching Tables...

4. After a few seconds, an error message will appear: *Unable to reach Wi-Fi network, connecting to LTE*. Touch YES to connect to LTE.



Unable to reach Wi-Fi network, connecting to LTE

5. The transaction process will resume over LTE.



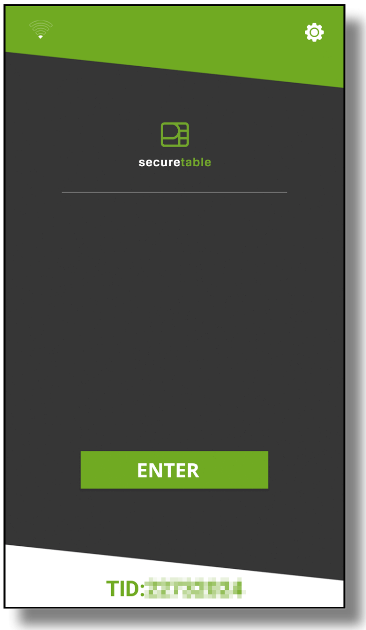
9	$ 20.64

IMPORTANT! After this type automatic switch to LTE, SecureTable will not try to switch back to Wifi on its own. If you wish to use Wifi again, you will need to switch to Wifi manually.

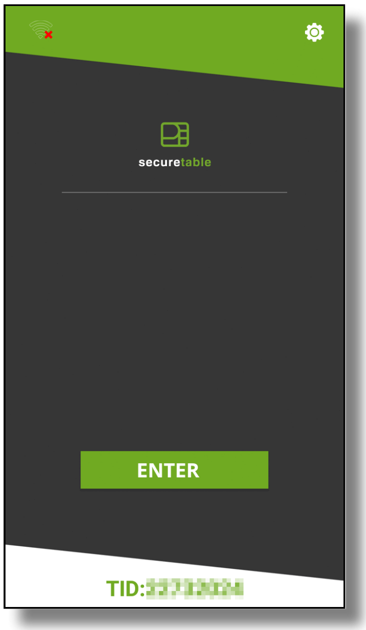
Automatic Network Switching due to lost WiFi signal

When WiFi signal is lost, SecureTable will automatically switch to Mobile networks, regardless of the status of the Auto-connect to LTE option. This happens without user intervention, as soon as the WiFi signal is lost. When the terminal is brought back within WiFi range, SecureTable will automatically switch back to the WiFi network.

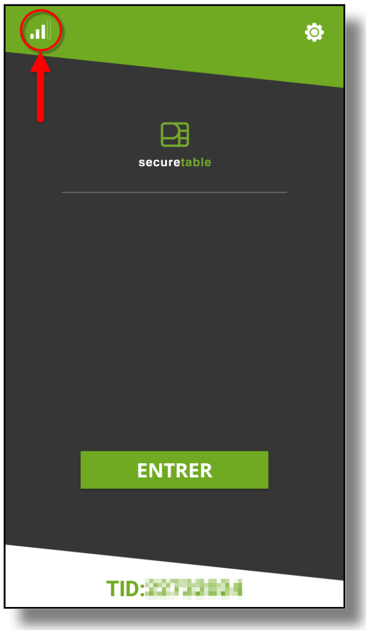
1. The terminal is brought to the limit of Wifi coverage.



2. WiFi signal is lost.



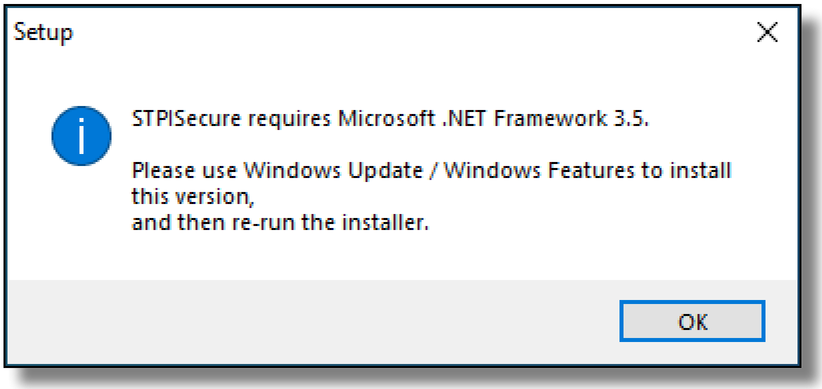
3. SecureTable automatically switches to 4G/LTE mobile network.



Microsoft .NET Framework 3.5 is missing

Issue Description:

While attempting to install STPISecure, an error message is displayed:



Setup

STPISecure requires Microsoft .NET Framework 3.5.

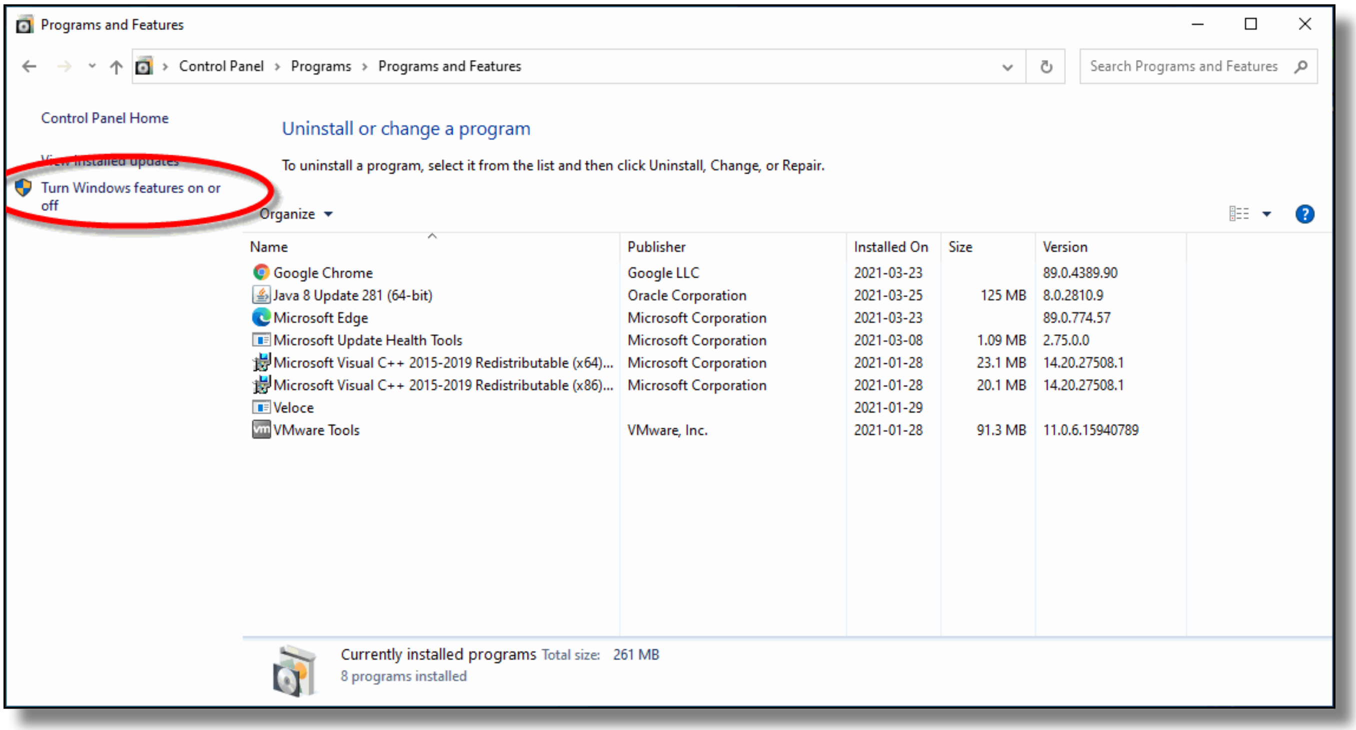
Please use Windows Update / Windows Features to install this version,
and then re-run the installer.

STPISecure requires Microsoft .NET Framework 3.5.

Please use Windows Update / Windows Features to install this version, and then re-run the installer.

Solution:

Install Microsoft .NET Framework 3.5 through Windows Update or use the "Turn Windows features on or off" option from Add/Remove programs to enable .NET Framework 3.5.



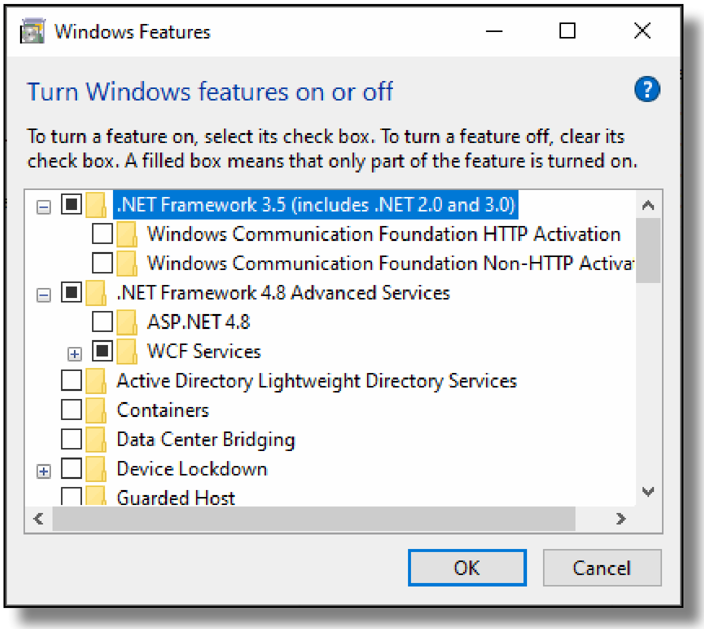
Programs and Features
Control Panel > Programs > Programs and Features
Search Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Organize

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher	Installed On	Size	Version
Google Chrome	Google LLC	2021-03-23		89.0.4389.90
Java 8 Update 281 (64-bit)	Oracle Corporation	2021-03-25	125 MB	8.0.2810.9
Microsoft Edge	Microsoft Corporation	2021-03-23		89.0.774.57
Microsoft Update Health Tools	Microsoft Corporation	2021-03-08	1.09 MB	2.75.0.0
Microsoft Visual C++ 2015-2019 Redistributable (x64)...	Microsoft Corporation	2021-01-28	23.1 MB	14.20.27508.1
Microsoft Visual C++ 2015-2019 Redistributable (x86)...	Microsoft Corporation	2021-01-28	20.1 MB	14.20.27508.1
Veloce		2021-01-29		
VMware Tools	VMware, Inc.	2021-01-28	91.3 MB	11.0.6.15940789

Currently installed programs Total size: 261 MB
8 programs installed



Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

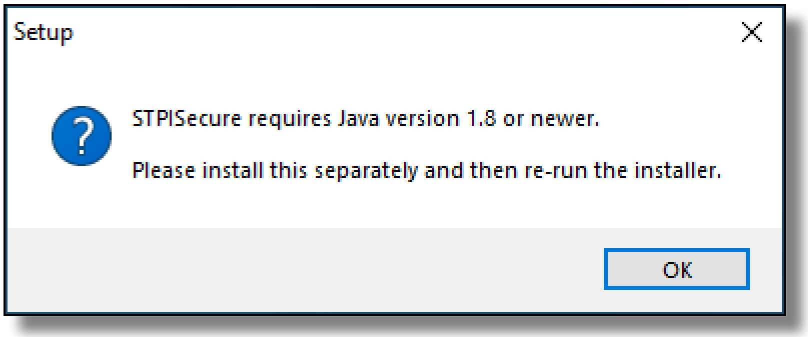
- ■ .NET Framework 3.5 (includes .NET 2.0 and 3.0)
  - □ Windows Communication Foundation HTTP Activation
  - □ Windows Communication Foundation Non-HTTP Activa
- ■ .NET Framework 4.8 Advanced Services
  - □ ASP.NET 4.8
  - ■ WCF Services
- □ Active Directory Lightweight Directory Services
- □ Containers
- □ Data Center Bridging
- □ Device Lockdown
- □ Guarded Host

Once Microsoft .NET Framework 3.5 is installed, retry installing STPISecure.

Java is missing

Issue Description:

While attempting to install STPISecure, an error message is displayed:



Setup

STPISecure requires Java version 1.8 or newer.

Please install this separately and then re-run the installer.

STPISecure requires Java version 1.8 or newer.
Please install this separately and then re-run the installer.

Solution:

Download and install Java from the Oracle website:

https://www.java.com/en/

Once Java is installed on your system, retry installing STPISecure.