Code and Go for unattended Application User Manual

Version: 1.1.5 | April 15, 2021

USER MANUAL - ALL TERMINAL PRODUCTS

WARNING

Information in this document is subject to change without prior notice.

REVISION HISTORY

Version	Changes	Author	Date
1.0	Creation	Judy Zhu	June 30, 2020
1.0.1	Modify document format	Judy Zhu	July 2, 2020
1.0.2	1) Add the section "Installation Instructions"; 2) Update the "APPENDIX A" to v1.7; 3) Add the instructions of Castles new terminal model - VEGA3000P; 4) Add the section "Code_N_Go_unatt (Kiosk) Transactions - PreAuth & AuthComplete"; 5) Add the instructions of new command communication type - BT & Ethernet; 6) Update the "APPENDIX B"; Update the section "Slide Show Update"; 7) Add the section "Modify Terminal" of CTMS Configuration	Judy Zhu	July 21, 2020
1.0.3	1) Add the instructions of "Ethernet Setting" button in Service Menu; 2) Update the "Telemetry Menu"; 3) Update the "APPENDIX A v1.7" - delete the tag "Payment Type" and add three examples; 4) Add the instructions of "Details of Check List"; 5) Add the instructions of "USB Update Slide Show"	Judy Zhu	August 4, 2020
1.0.4	Add the instructions of how to configure on the Kiosk machine	Judy Zhu	August 18, 2020
1.0.5	Change to only for "Code_N_Go_unatt" application	Judy Zhu	September 18, 2020
1.0.6	Add the supported transaction host "Apriva"	Judy Zhu	October 12, 2020
1.0.7	1) Add the Token transaction and related content; 2) Add the parameter "HLVoltageFlag"; 3) Modify the parameters "DHCP/ Ethernet Command Port/ CTMS Port"	Judy Zhu	November 3, 2020
1.0.8	1) Update the APPENDEX A: Castles Semi-Integrated Command to ver1.9 2) Add the Swipe UI only for MSR transaction	Judy Zhu	December 4, 2020

1.0.9	1) Delete the note of parameter "HLVoltageFlag"; 2) Modify the UI for account type for Interac 3) Update the APPENDEX A: Castles Semi-Integrated Command to ver2.0	Judy Zhu	December 24, 2020
1.1.0	1) Update the APPENDEX A: Castles Semi-Integrated Command to ver2.1 2) Add the parameter "IsAmountZeroSupport" and the related UI "Amount Invalid" 3) Update the default value of "CTMS UAT Address"	Judy Zhu	February 3, 2021
1.1.1	1) Update the APPENDEX A: Castles Semi-Integrated Command to ver2.2 2) Add the section "Adjust Transaction"	Judy Zhu	February 20, 2021
1.1.2	1) Update the APPENDEX A: Castles Semi-Integrated Command to ver2.3 2) Add the parameter "Transaction Environment"	Judy Zhu	March 9, 2021
1.1.3	1) Add the parameters about Card Type and Entry Mode for Apriva host 2) Add the different payment screens and different select card type screens for Apriva transaction flow 3) Add the parameter "CheckList TimeOut"	Judy Zhu	March 15, 2021
1.1.4	1) Update the APPENDEX A: Castles Semi-Integrated Command to ver2.4 2) Add the parameters "Is Close Receipt Tips", "CTMS Host" and "Speaker" 3) Add the parameter "Is Show French First" and related screens 4) Change the mode of parameters "Page Numbers" and "Page Switching Interval" to Group Part	Judy Zhu	April 12, 2021

1.1.5	1) Add the parameters “AprivaVoidURL”, “AprivaCashSaleURL” and “AprivaAdjustURL” 2) Add the section “Parameter List” for parameters quick check, and update the section “Configuration Parameters” to “Parameters Detail” 3) Update transaction host info for Apriva – support quick chip 4) Add the sections “Update CAPK for Apriva” in CTMS Function and USB Function	JudyZhu	April 15, 2021

TABLE OF CONTENTS

3. GLOSSARY

Term	Description
GPRS	General Packet Radio Service (GPRS) is a mobile data service available to users of GSM mobile phones.
SIM	A Subscriber Identity Module securely stores the key identifying a mobile phone service subscriber, as well as subscription information, saved telephone numbers, preferences, text messages and other information. Each SIM is uniquely identified by its ICCID (International Circuit Card ID).
NTP	Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.
CTMS	Castles Terminal Management System (CTMS) is a system designed for administrators or managers to manage the electronic funds transfers at point of sale (terminals) produced by Castles.
EMV	Euro card, MasterCard and Visa consortium that manages new chip and pin requirements including contactless ...

4. ABOUT THIS MANUAL

This manual provides basic instructions for user of Code and Go for unattended application terminal products. It is suggested that you read through this document to assist you in getting the full value of using the features provided by the Code and Go for unattended application.

4.1. Document Conventions

The following symbols are used throughout this manual allowing the reader to easily identify instructions, explanations and examples of the features found in the unattended application.

- ❖ When you see this symbol, it represents an explanation or a definition of the feature or option you are reading about. Information is provided to assist the user when using the many features and options provided by unattended application.
- ➢ When you see this symbol, it represents important additional information such as an example of how the feature can be used, an important tip for using the feature or an important note to be brought to your attention.

5. ABOUT THIS APP

5.1. Application Instruction - Code_N_Go_unatt

❖ The Code and Go for unattended (Code_N_Go_unatt) application sets the transaction process according to the upper system, and the display examples in this manual will reflect that of the application specifically. Please see the definition of this application below:

Code_N_Go_unatt	The terminal with Code_N_Go_unatt application will communicate with the upper computer through command messages based on the Castles Semi-Integrated Command Protocol. It will do sale (or pre-auth, auth-complete) and reversal transactions to complete purchase. For detailed instructions of command protocol, please refer to the section "APPENDIX A: Castles Semi-Integrated Command".

5.2. Identifying which Castles Product you have

❖ In this manual you will see instructions and step/action guides for both the Castles UPT1000F terminal product and Castles VEGA3000P terminal product. Use the chart below to identify which of the instructions to follow for the terminal you are working with.

UPT1000F	You can identify if your terminal model is UPT1000F by the following: ● Turn your terminal over; the label will identify UPT and the model of that specific terminal. Ie: UPT1000F ● There is no keypad under the display
VEGA3000P	You can identify if your terminal model is VEGA3000P by the following: ● Turn your terminal over; the label will identify VEGA and the model of that specific terminal. Ie: VEGA3000P ● There is a keypad under the display

➢ There are some differences in supported features between Castles UPT1000F terminal and VEGA3000P terminal. Use the chart below to confirm the specific features supported by the terminal you are working with.

UPT1000F	● Supported Host Communication Type: GPRS, Ethernet ● Supported Command Communication Type: RS232, USB, Bluetooth, Ethernet

VEGA3000P	● Supported Update Configuration Method: CTMS, USB ● Is Speaker Supported: YES
	● Supported Host Communication Type: Only Ethernet ● Supported Command Communication Type: RS232, USB, Ethernet ● Supported Update Configuration Method: Only CTMS ● Is Speaker Supported: NO

5.3. Castles Keypad Layouts

❖ Castles VEGA3000P terminal has a keypad under the display. These keys are the same and perform the same function regardless of the Castles model.

Key	Function
1-0 Number Keys	● Enter password, PIN, parameter value and such. ● Alphanumeric entry - multitap to access the alpha characters.
Green OK	● Functions as the OK key.
Red X	● Cancels a transaction. ● Exits the enter options to return to previous menu.
Yellow ←	● Back space to clear data fields
↑ Arrow	● Special characters entry
↓ Arrow	● Special characters entry

5.4. Service Mode Menu

❖ There is one menu that resides in the Code_N_Go_unatt application, which is for user to quickly know the basic information and perform the basic functions. Please see the definition of Service Mode Menu below:

Service Mode Menu	In this menu you will find the configuration settings that are used by this application and the basic functions that can be performed by user. Some examples of Service Mode Menu items are: Basic Information, Version Information, CTMS, NTP, Connect Test, Switch TXN Host, Terminal Setting, etc. For detailed instructions of Service Mode Menu options, please refer to the section "TERMINAL FEATURES – SERVICE MODE MENU".

6. TRANSACTION HOST

6.1. Supported Transaction Host

❖ At present, the Code_N_Go_unatt application supports three transaction hosts: Heartland Portico USA, GP Canada and Apriva. Which host the application supports will determine the specific card types supported, whether EMV Quick Chip is supported, and other transaction details of the application. Use the chart below to check out the differences for that three hosts:

Heartland Portico USA	● Supported Card Brand: VISA/ MasterCard/ AMEX/ Discover/ JCB ● Supported POS Entry Mode: Tap/ Insert/ Swipe ● Is EMV Quick Chip Supported: YES
GP Canada	● Supported Card Brand: VISA/ MasterCard/ AMEX/ Discover/ JCB/ Interac ● Supported POS Entry Mode: Tap/ Insert/ Swipe ● Is EMV Quick Chip Supported: NO
Apriva	● Supported Card Brand: VISA/ MasterCard/ AMEX/ Discover/ Maestro/ Military Star ● Supported POS Entry Mode: Tap/Insert/Swipe (Note: Apriva Host is working on the certifications of EMV and EMVCL) ● Is EMV Quick Chip Supported: YES

7. TRANSACTIONS

❖ This chapter describes the steps necessary to complete a Credit or Debit card transaction on the Code_N_Go_unatt application. Please note that if additional transaction prompts are required of that card they will present themselves in the flow of the transaction, for example: If AID Select is required of your card then you will be prompted to select the AID during the transaction.

7.1. Sale Transactions

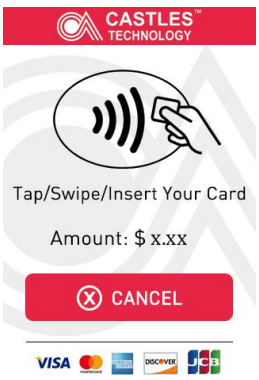
❖ Transactions demonstrated in this section are the following:

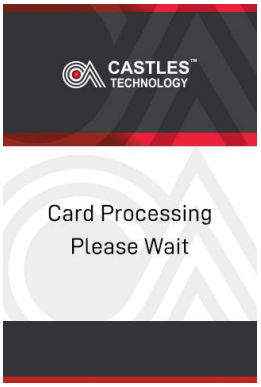
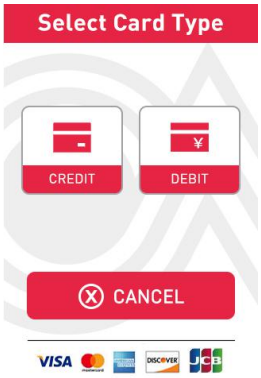
- EMV Transaction- Quick Chip
- EMV Transaction- Not Quick Chip
- MSR Transaction
- EMVCL Transaction
- Interac Transaction- Contact
- Interac Transaction- Contactless
- Re-Sale Transaction
- Kiosk Cancel Transaction
- MSR Transaction for Apriva
- Token Transaction
- Adjust Transaction

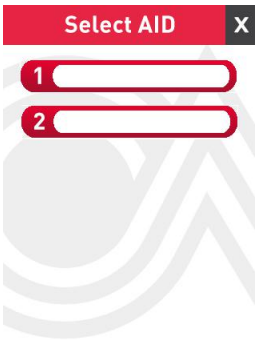
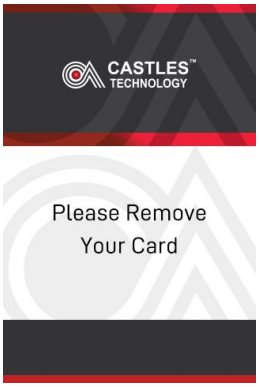
➢ During the transaction, if you see an error message, please consult the Transaction Error Messages chart. The terminal will return to idle mode after any error message shown.

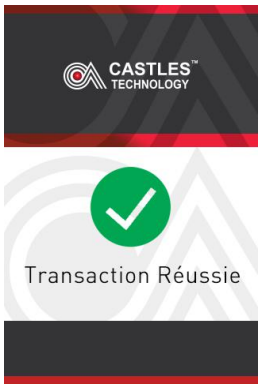
7.1.1. EMV TRANSACTION - QUICK CHIP

❖ Use the chart below to process a EMV chip card transaction when the card is inserted at the point of transaction. This flow is available when the application supports Quick Chip.

Step	Action	Display	
		US	Canada (French)
1.	On Kiosk - Select products and plan to pay (Kiosk sends a sale command request to terminal) If the sending process or request content has problems, the terminal may have the following behavior: ● Terminal no response ● Terminal shows "CMD Format Err" ● Terminal shows "Selection Over Limit" If the operation times out or user presses cancel, you may see the following error:	 (x refers to digit)	 (x refers to digit) Or

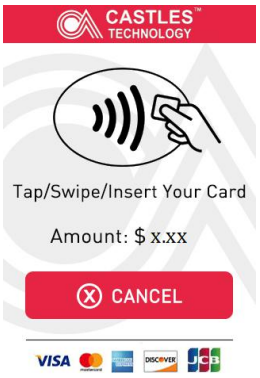
	● Transaction Canceled ● Operation Time Out		 (If French first)
2.	Insert EMV Chip Card If the card process fails, you may see the following error: ● Tap or Swipe This Card or Try Another Card ● Transaction Declined by Local		 Or  (If French first)
3.	Select card type if prompted If the selection times out or user presses cancel, you may see the following error: ● Transaction Canceled ● Operation Time Out		Card type selection is not required for Canada

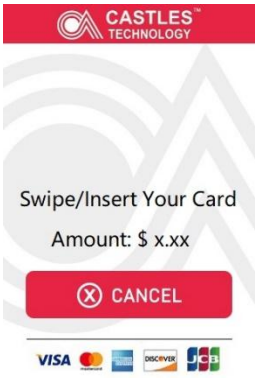
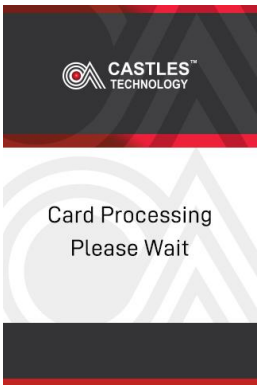
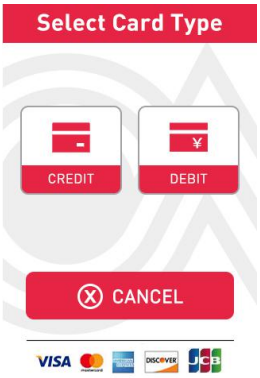
4.	Select the AID if prompted If the selection times out or user presses cancel, you may see the following error: ● Transaction Canceled ● Operation Time Out		
5.	Input the PIN if prompted and press OK If PIN is incorrect, you may see the following error: ● Incorrect PIN ● PIN Blocked ● PIN Failblocked If the entry times out or user presses cancel, you may see the following error: ● Transaction Canceled ● Operation Time Out		
6.	Remove the card if prompted		
7.	Terminal communicates to the host for sale transaction		

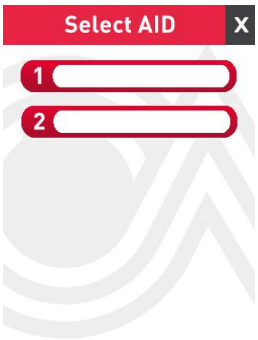
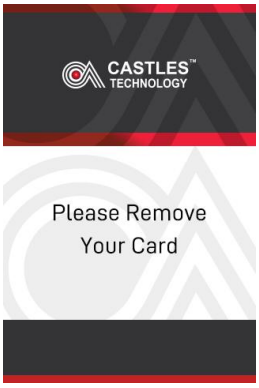
8.	Terminal displays the result of sale transaction If sale transaction fails, you may see the following error: ● Transaction Failed ● Transaction Declined		
9.	Terminal flashes "Thank You" and returns to the idle mode		

7.1.2. EMV TRANSACTION- NOT QUICK CHIP

❖ Use the chart below to process a EMV chip card transaction when the card is inserted at the point of transaction. This flow is available when the Quick Chip is disabled.

Step	Action	Display US	Display Canada (French)
1.	On Kiosk - Select products and plan to pay (Kiosk sends a sale command request to terminal) If the sending process or request content has problems, the terminal may have the following behavior: ● Terminal no response ● Terminal shows "CMD Format Err" ● Terminal shows "Selection Over Limit" If the operation times out or user presses cancel, you may see the following error: ● Transaction Canceled	 (x refers to digit) Or	 (x refers to digit) Or

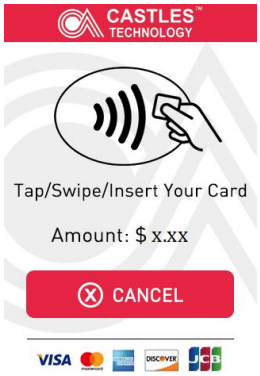
	● Operation Time Out Note: For the application with Apriva transaction host, the payment screen will be displayed based on the supported Entry Modes.	 (If not support Contactless Card)	 (If French first)
2.	Insert EMV Chip Card If the card process fails, you may see the following error: ● Tap or Swipe This Card or Try Another Card ● Transaction Declined by Local		 Or  (If French first)
3.	Select card type if prompted If the selection times out or user presses cancel, you may see the following error: ● Transaction Canceled ● Operation Time Out		Card type selection is not required for Canada

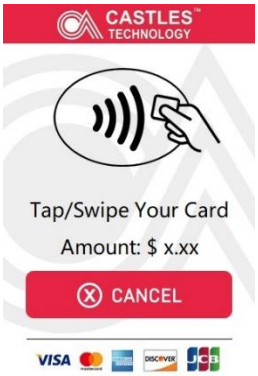
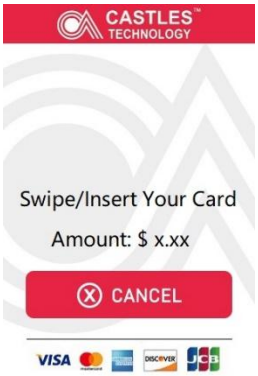
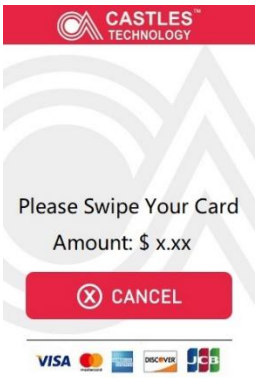
4.	Select the AID if prompted If the selection times out or user presses cancel, you may see the following error: ● Transaction Canceled ● Operation Time Out		
5.	Input the PIN if prompted and press OK If PIN is incorrect, you may see the following error: ● Incorrect PIN ● PIN Blocked ● PIN Failblocked If the entry times out or user presses cancel, you may see the following error: ● Transaction Canceled ● Operation Time Out		
6.	Terminal communicates to the host for sale transaction		
7.	Remove the card if prompted		

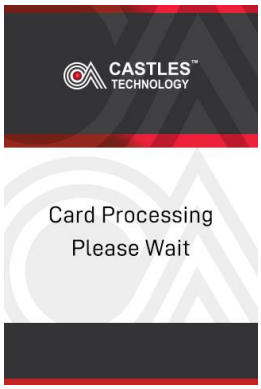
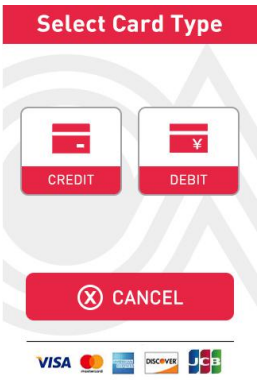
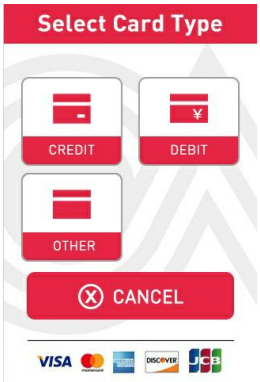
8.	Terminal displays the result of sale transaction If sale transaction fails, you may see the following error: ● Transaction Failed ● Transaction Declined		
9.	Terminal flashes "Thank You" and returns to the idle mode		

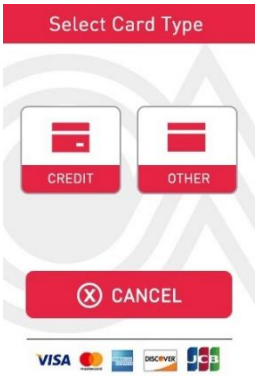
7.1.3. MSR TRANSACTION

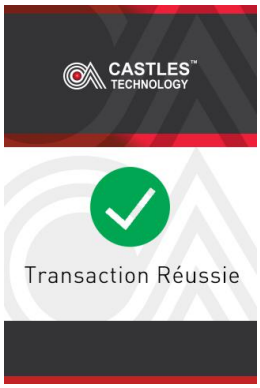
❖ Use the chart below to process a MSR card transaction when the card is swiped at the point of transaction.

Step	Action	Display US	Display Canada (French)
1.	On Kiosk - Select products and plan to pay (Kiosk sends a sale command request to terminal) If the sending process or request content has problems, the terminal may have the following behavior: ● Terminal no response ● Terminal shows "CMD Format Err" ● Terminal shows "Selection Over Limit" If the operation times out or user presses cancel, you may see the following error: ● Transaction Canceled ● Operation Time Out	 (x refers to digit) Or	 (x refers to digit) Or

	Note: For the application with Apriva transaction host, the payment screen will be displayed based on the supported Entry Modes.	 (If not support Contact Card) Or  (If not support Contactless Card) Or  (If not support Contact and Contactless Card)	 (If French first)

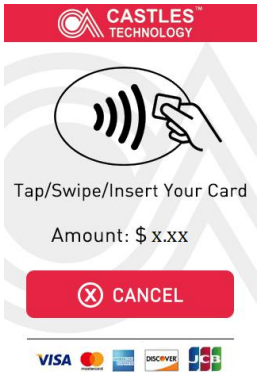
2.	Swipe Card If the card process fails, you may see the following error: ● Polling Card Failed ● Card Not Support ● Transaction Declined by Local ● Please Insert Your Card (MSR with chip)		 Or  (If French first)
3.	Select card type if prompted. If the selection times out or user presses cancel, you may see the following error: ● Transaction Canceled ● Operation Time Out Note: For the application with Apriva transaction host, the select card type screen will be displayed based on the supported Card Types, and the "OTHER" type mainly refers to campus card.	 Or  (If Closed Loop Card	Card type selection is not required for Canada

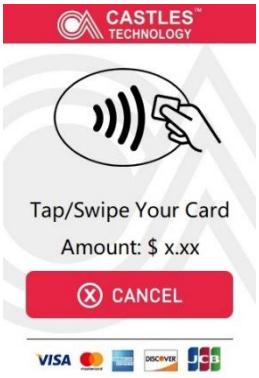
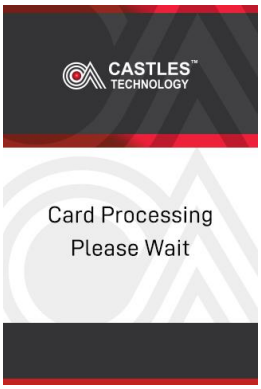
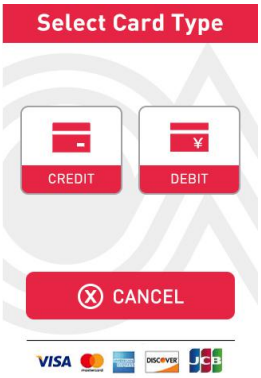
		supported) Or  (If Closed Loop Card supported but Debit Card not supported)	
4.	Input the PIN if prompted and press OK If PIN is incorrect, you may see the following error: ● Incorrect PIN ● PIN Blocked ● PIN Failblocked If the entry times out or user presses cancel, you may see the following error: ● Transaction Canceled ● Operation Time Out	 	Canada does not support Online PIN
5.	Terminal communicates to the host for sale transaction	 	

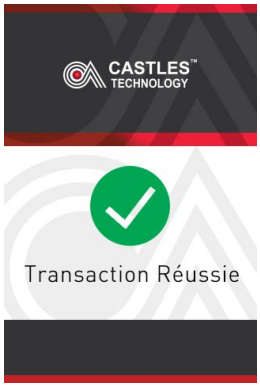
6.	Terminal displays the result of sale transaction If sale transaction fails, you may see the following error: ● Transaction Failed ● Transaction Declined		
7.	Terminal flashes "Thank You" and returns to the idle mode		

7.1.4. EMVCL TRANSACTION

❖ Use the chart below to process a EMVCL card transaction when the card is tapped at the point of transaction.

Step	Action	Display US	Display Canada (French)
1.	On Kiosk - Select products and plan to pay (Kiosk sends a sale command request to terminal) If the sending process or request content has problems, the terminal may have the following behavior: ● Terminal no response ● Terminal shows "CMD Format Err" ● Terminal shows "Selection Over Limit" If the operation times out or user presses cancel, you may see the following error: ● Transaction Canceled ● Operation Time Out	 (x refers to digit) Or	 (x refers to digit) Or

	Note: For the application with Apriva transaction host, the payment screen will be displayed based on the supported Entry Modes.	 (If not support Contact Card)	 (If French first)
2.	Tap Card If the card process fails, you may see the following error: ● Polling Card Failed ● Card Not Support ● Transaction Declined by Local ● Insert or Swipe This Card		 Or  (If French first)
3.	Select card type if prompted If the selection times out or user presses cancel, you may see the following error: ● Transaction Canceled ● Operation Time Out		Card type selection is not required for Canada

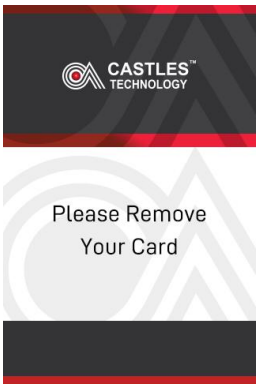
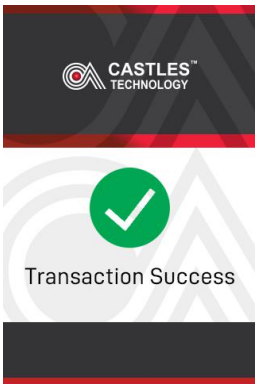
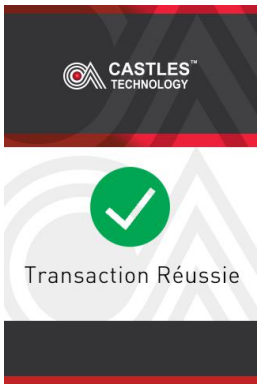
4.	Input the PIN if prompted and press OK If PIN is incorrect, you may see the following error: ● Incorrect PIN ● PIN Blocked ● PIN Failblocked If the entry times out or user presses cancel, you may see the following error: ● Transaction Canceled ● Operation Time Out		Canada does not support Online PIN
5.	Terminal communicates out to the host for sale transaction		
6.	Terminal displays the result of sale transaction If sale transaction fails, you may see the following error: ● Transaction Failed ● Transaction Declined		
7.	Terminal flashes “Thank You” and returns to the idle mode		

7.1.5. INTERAC TRANSACTION- CONTACT

❖ Use the chart below to process an Interac Debit card transaction when the card is inserted at the point of transaction. Please ignore this section if the host which you used does not support the interact contact card.

Step	Action	Display	
		Canada (English)	Canada (French)
1.	On Kiosk - Select products and plan to pay (Kiosk sends a sale command request to terminal) If the sending process or request content has problems, the terminal may have the following behavior: ● Terminal no response ● Terminal shows "CMD Format Err" ● Terminal shows "Selection Over Limit" If the operation times out or user presses cancel, you may see the following error: ● Transaction Canceled ● Operation Time Out	 (x refers to digit) Or  (If French first)	 (x refers to digit) Or  (If French first)
2.	Insert Interac Card If the card process fails, you may see the following error: ● Polling Card Failed ● Transaction Declined by Local	 Or	 Or

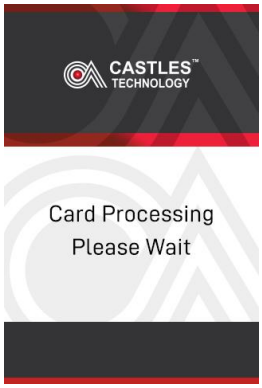
		 (If French first)	 (If French first)
3.	Select YES to continue transaction if prompted If the selection times out or user presses NO, you may see the following error: ● Operation Time Out ● Transaction Canceled		
4.	Select Account Type if prompted If the selection times out or user presses EXIT, you may see the following error: ● Operation Time Out ● Transaction Canceled		
5.	Terminal communicates out to the host for sale transaction		

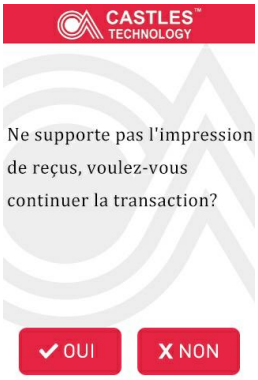
6.	Remove the card if prompted		
7.	Terminal displays the result of sale transaction If sale transaction fails, you may see the following error: ● Transaction Failed ● Transaction Declined		
8.	Terminal flashes “Thank You” and returns to the idle mode		

7.1.6. INTERAC TRANSACTION- CONTACTLESS

❖ Use the chart below to process an Interac Debit card transaction when the card is tapped at the point of transaction. Please ignore this section if the host which you used does not support the interact contactless card.

Step	Action	Display	
		Canada (English)	Canada (French)

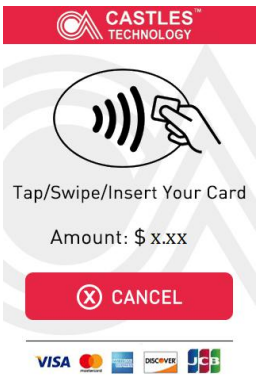
1.	On Kiosk - Select products and plan to pay (Kiosk sends a sale command request to terminal) If the sending process or request content has problems, the terminal may have the following behavior: ● Terminal no response ● Terminal shows “CMD Format Err” ● Terminal shows “Selection Over Limit” If the operation times out or user presses cancel, you may see the following error: ● Transaction Canceled ● Operation Time Out	 (x refers to digit) Or  (If French first)	 (x refers to digit) Or  (If French first)
2.	Tap Interac Card If the card process fails, you may see the following error: ● Polling Card Failed ● Transaction Declined by Local		 Or 

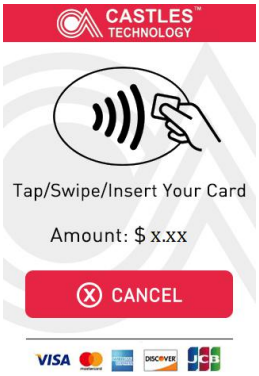
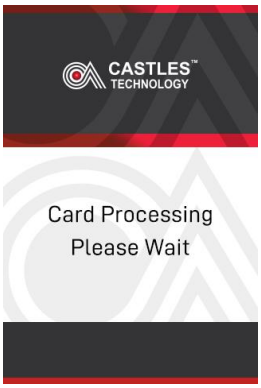
			(If French first)
3.	Select YES to continue transaction if prompted If the selection times out or user presses NO, you may see the following error: ● Operation Time Out ● Transaction Canceled		
4.	Select Account Type if prompted If the selection times out or user presses EXIT, you may see the following error: ● Operation Time Out ● Transaction Canceled		
5.	Terminal communicates out to the host for sale transaction		
6.	Terminal displays the result of sale transaction If sale transaction fails, you may see the following error: ● Transaction Failed ● Transaction Declined		

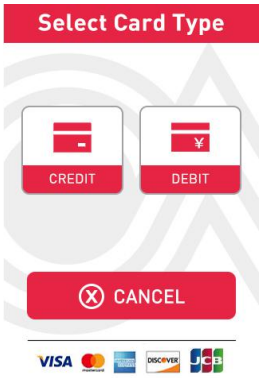
7.	Terminal flashes “Thank You” and returns to the idle mode		

7.1.7. RE-SALE TRANSACTION

- ❖ This transaction is used when the user has not paid for the existing products, but re-selects products and want to pay for.
- ➢ This function can be disabled through parameter “Resale Support”, please see in the annex configuration “External Command”. For detailed instructions of parameter update, please refer to the section “TERMINAL FEATURES - CONFIGURATION UPDATE”.
- ➢ The transaction process below takes MSR card as an example.

Step	Action	Display US	Canada (French)
1.	On Kiosk - Select products and plan to pay (Kiosk sends a sale command request to terminal) If the sending process or request content has problems, the terminal may have the following behavior: ● Terminal no response ● Terminal shows “CMD Format Err” ● Terminal shows “Selection Over Limit” If the operation times out or user presses cancel, you may see the following error: ● Transaction Canceled ● Operation Time Out	 (x refers to digit)	 (x refers to digit) Or

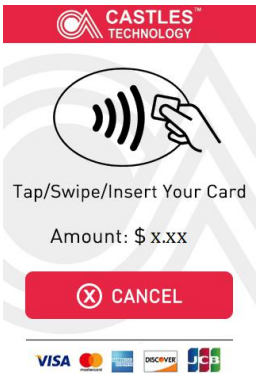
			 (If French first)
2.	Before the card be detected. On Kiosk - Select products and plan to pay again (Kiosk sends a new sale command request to terminal) If the sending process or request content has problems, the terminal may have the following behavior: ● Terminal no response ● Terminal shows "CMD Format Err" ● Terminal shows "Selection Over Limit" If the operation times out or user presses cancel, you may see the following error: ● Transaction Canceled ● Operation Time Out		 Or  (If French first)
3.	Swipe Card If the card process fails, you may see the following error: ● Polling Card Failed ● Card Not Support ● Transaction Declined by Local ● Please Insert Your Card (MSR with chip)		 Or

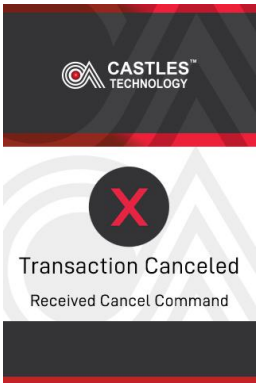
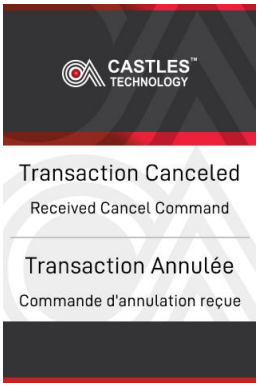
			 (If French first)
4.	Select card type if prompted If the selection times out or user presses cancel, you may see the following error: ● Transaction Canceled ● Operation Time Out		Card type selection is not required for Canada
5.	Input the PIN if prompted and press OK If PIN is incorrect, you may see the following error: ● Incorrect PIN ● PIN Blocked ● PIN Failblocked If the entry times out or user presses cancel, you may see the following error: ● Transaction Canceled ● Operation Time Out		Canada does not support Online PIN
6.	Terminal communicates to the host for sale transaction		

7.	Terminal displays the result of sale transaction If sale transaction fails, you may see the following error: ● Transaction Failed ● Transaction Declined		
8.	Terminal flashes "Thank You" and returns to the idle mode		

7.1.8. KIOSK CANCEL TRANSACTION

❖ This transaction is used to cancel the transaction on the kiosk before the card be detected.

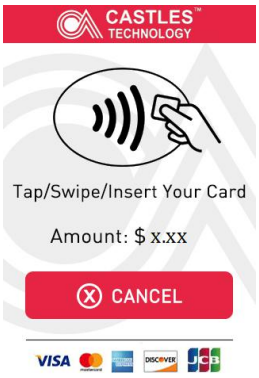
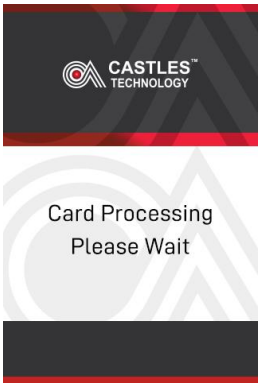
Step	Action	Display US	Display Canada (French)
1.	On Kiosk - Select products and plan to pay (Kiosk sends a sale command request to terminal) If the sending process or request content has problems, the terminal may have the following behavior: ● Terminal no response ● Terminal shows "CMD Format Err" ● Terminal shows "Selection Over Limit" If the operation times out or user presses cancel, you may see the following error: ● Transaction Canceled ● Operation Time Out	 (x refers to digit)	 (x refers to digit) Or

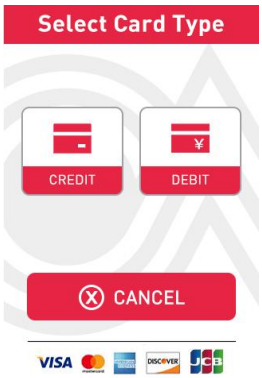
			 (If French first)
2.	On Kiosk - Press cancel (Kiosk sends a cancel command request to terminal)		 Or  (If French first)
3.	Terminal returns to the idle mode		

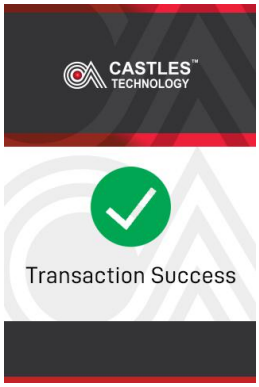
7.1.9. TOKEN TRANSACTION

- This transaction is used when the user does not want to use the physical card. When the user completes the payment by using a physical card for the first time, then the user can directly use the unique token value of the card to complete the next payments without using the physical card. Please note that only Heartland Portico USA and GP Canada support this transaction.

➢ The transaction process below takes MSR card as an example. If the token value of the card is already gotten by the Kiosk, the user can turn to step 8 to perform the transaction directly.

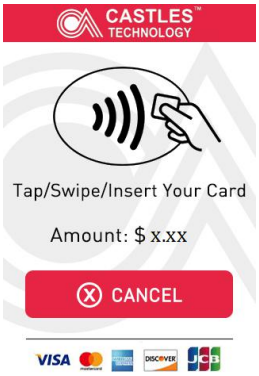
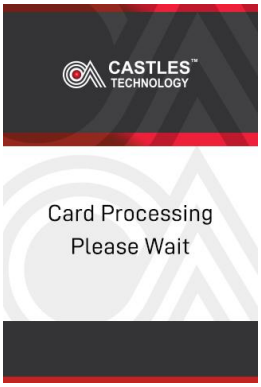
Step	Action	Display US	Canada (French)
1.	On Kiosk - Select products and plan to pay (Kiosk sends a sale command request with the tag "RequestToken" to terminal, it's value is TRUE) If the sending process or request content has problems, the terminal may have the following behavior: ● Terminal no response ● Terminal shows "CMD Format Err" ● Terminal shows "Selection Over Limit" ● Terminal shows "Amount Not Support" If the operation times out or user presses cancel, you may see the following error: ● Transaction Canceled ● Operation Time Out	 (x refers to digit)	 (x refers to digit) Or  (If French first)
2.	Swipe Card If the card process fails, you may see the following error: ● Polling Card Failed ● Card Not Support ● Transaction Declined by Local ● Please Insert Your Card (MSR with chip)		

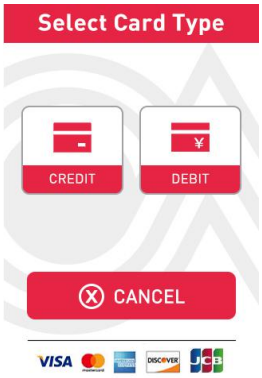
3.	Select card type if prompted If the selection times out or user presses cancel, you may see the following error: ● Transaction Canceled ● Operation Time Out		Card type selection is not required for Canada
4.	Input the PIN if prompted and press OK If PIN is incorrect, you may see the following error: ● Incorrect PIN ● PIN Blocked ● PIN Failblocked If the entry times out or user presses cancel, you may see the following error: ● Transaction Canceled ● Operation Time Out		Canada does not support Online PIN
5.	Terminal communicates to the host for sale transaction		
6.	Terminal displays the result of sale transaction If sale transaction fails, you may see the following error: ● Transaction Failed ● Transaction Declined		

7.	Terminal flashes “Thank You” and returns to the idle mode Terminal responses the Token Value of the card to Kiosk, and Kiosk should save this value to local for the user to do the next transaction		
8.	On Kiosk - Select products and plan to pay (Kiosk sends a sale command request with the tag “TokenValue” to terminal, it’s value should be the token value of the card) Terminal communicates to the host for sale transaction		
9.	Terminal displays the result of sale transaction If sale transaction fails, you may see the following error: ● Transaction Failed ● Transaction Declined		
10.	Terminal flashes “Thank You” and returns to the idle mode		

7.1.10. ADJUST TRANSACTION

- ❖ This transaction is used when the user wants to adjust the amount of the last sale transaction. When the user completes the payment by using a physical card for the first time, then the user can use the unique TXN ID value to adjust the amount of this transaction without using the physical card.
- ➢ The transaction process below takes MSR card as an example.

Step	Action	Display US	Display Canada (French)
1.	On Kiosk - Select products and plan to pay (Kiosk sends a sale command request to terminal) If the sending process or request content has problems, the terminal may have the following behavior: ● Terminal no response ● Terminal shows "CMD Format Err" ● Terminal shows "Selection Over Limit" ● Terminal shows "Amount Not Support" If the operation times out or user presses cancel, you may see the following error: ● Transaction Canceled ● Operation Time Out	 (x refers to digit)	 (x refers to digit) Or  (If French first)
2.	Swipe Card If the card process fails, you may see the following error: ● Polling Card Failed ● Card Not Support ● Transaction Declined by Local ● Please Insert Your Card (MSR with chip)		 Or

			 (If French first)
3.	Select card type if prompted If the selection times out or user presses cancel, you may see the following error: ● Transaction Canceled ● Operation Time Out		Card type selection is not required for Canada
4.	Input the PIN if prompted and press OK If PIN is incorrect, you may see the following error: ● Incorrect PIN ● PIN Blocked ● PIN Failblocked If the entry times out or user presses cancel, you may see the following error: ● Transaction Canceled ● Operation Time Out		Canada does not support Online PIN
5.	Terminal communicates to the host for sale transaction		

6.	Terminal displays the result of sale transaction If sale transaction fails, you may see the following error: ● Transaction Failed ● Transaction Declined		
7.	Terminal flashes “Thank You” and returns to the idle mode Terminal responses the Token Value of the card to Kiosk, and Kiosk should save this value to local for the user to do the next transaction		
8.	On Kiosk - Select products and plan to pay (Kiosk sends an adjust command request with the tag “HostTXNID” to terminal, it’s value should be that of the last transaction) Terminal communicates to the host for adjust transaction		
9.	Terminal displays the result of adjust transaction If adjust transaction fails, you may see the following error: ● Transaction Failed ● Transaction Declined		

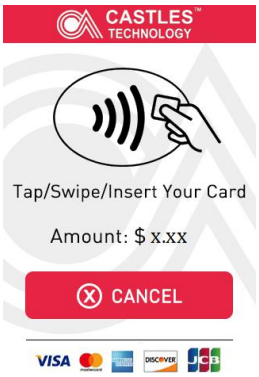
10.	Terminal flashes “Thank You” and returns to the idle mode		

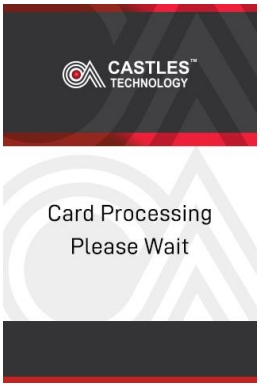
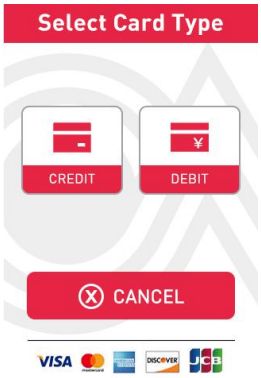
7.2. PreAuth & AuthComplete Transactions

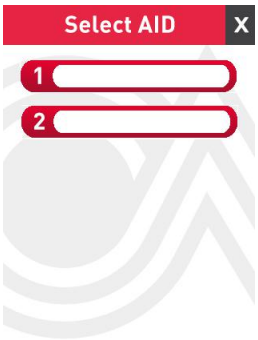
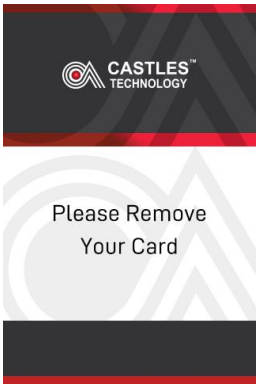
- ❖ Transactions demonstrated in this section are the following:
  - EMV Transaction- Quick Chip
  - EMV Transaction- Not Quick Chip
  - MSR Transaction
  - EMVCL Transaction
  - Interac Transaction- Contact
  - Interac Transaction- Contactless
  - Kiosk Cancel Transaction
  - Kiosk Cancel Pre-Auth
  - MSR Transaction for Apriva
  - Token Transaction
- ➢ During the transaction, if you see an error message, please consult the Transaction Error Messages chart. The terminal will return to idle mode after any error message shown.

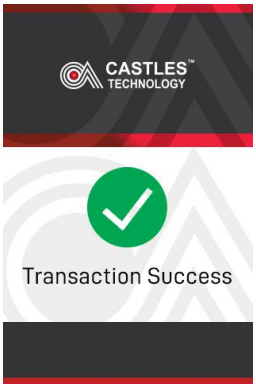
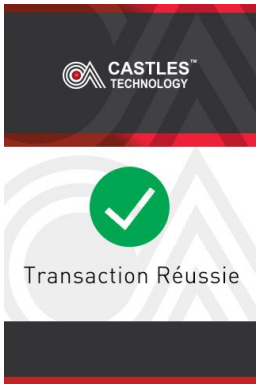
7.2.1. EMV TRANSACTION- QUICK CHIP

- ❖ Use the chart below to process a EMV chip card transaction when the card is inserted at the point of transaction. This flow is available when the application supports Quick Chip.

Step	Action	Display US	Display Canada (French)
1.	On Kiosk - Plan to pay (Kiosk sends a pre-auth command request to terminal) If the sending process or request content has problems, the terminal may have the following behavior: ● Terminal no response ● Terminal shows “CMD Format Err” ● Terminal shows “Selection Over Limit” If the operation times out or user	 (x refers to digit)	 (x refers to digit) Or

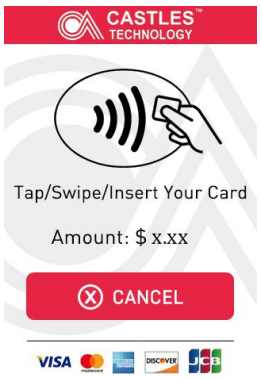
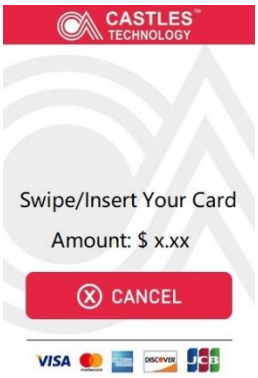
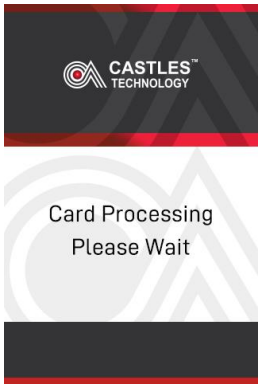
	presses cancel, you may see the following error: ● Transaction Canceled ● Operation Time Out		 (If French first)
2.	Insert EMV Chip Card If the card process fails, you may see the following error: ● Tap or Swipe This Card or Try Another Card ● Transaction Declined by Local		 Or  (If French first)
3.	Select card type if prompted If the selection times out or user presses cancel, you may see the following error: ● Transaction Canceled ● Operation Time Out		Card type selection is not required for Canada

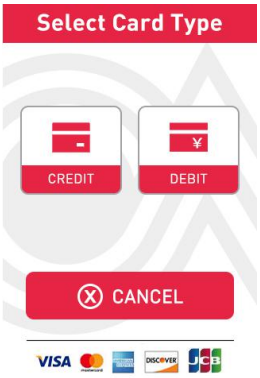
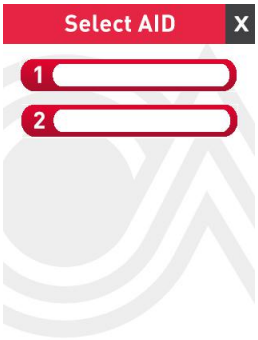
4.	Select the AID if prompted If the selection times out or user presses cancel, you may see the following error: ● Transaction Canceled ● Operation Time Out		
5.	Input the PIN if prompted and press OK (you have three times to enter the PIN) If PIN is incorrect, you may see the following error: ● Incorrect PIN ● PIN Blocked ● PIN Failblocked If the entry times out or user presses cancel, you may see the following error: ● Transaction Canceled ● Operation Time Out		
6.	Remove the card if prompted		
7.	Terminal communicates to the host for pre-auth transaction		

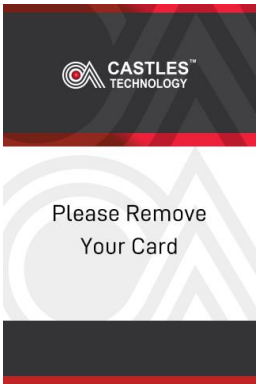
8.	Terminal displays the result of pre-auth transaction If pre-auth transaction fails, you may see the following error: ● Transaction Failed ● Transaction Declined		
9.	Terminal flashes “Thank You” and returns to the idle mode		
10.	On Kiosk - Plan to settle accounts (Kiosk sends a auth-complete command request to terminal) If the sending process or request content has problems, you may see the following error: ● (Terminal No Response) ● CMD Format Err		
11.	Terminal displays the result of auth-complete transaction and returns to idle mode If auth-complete transaction fails, you may see the following error: ● Transaction Failed ● Transaction Declined		

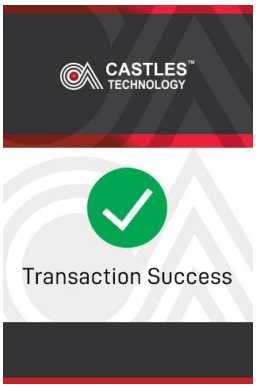
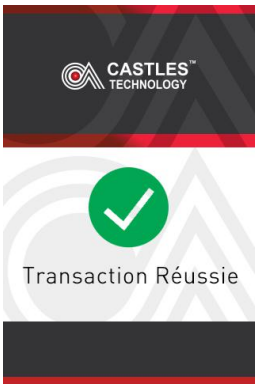
7.2.2. EMV TRANSACTION- NOT QUICK CHIP

❖ Use the chart below to process a EMV chip card transaction when the card is inserted at the point of transaction. This flow is available when the application does not support Quick Chip.

Step	Action	Display US	Canada (French)
1.	On Kiosk - Plan to pay (Kiosk sends a pre-auth command request to terminal) If the sending process or request content has problems, the terminal may have the following behavior: ● Terminal no response ● Terminal shows "CMD Format Err" ● Terminal shows "Selection Over Limit" If the operation times out or user presses cancel, you may see the following error: ● Transaction Canceled ● Operation Time Out Note: For the application with Apriva transaction host, the payment screen will be displayed based on the supported Entry Modes.	 (x refers to digit) Or  (If not support Contactless Card)	 (x refers to digit) Or  (If French first)
2.	Insert EMV Chip Card If the card process fails, you may see the following error: ● Tap or Swipe This Card or Try Another Card ● Transaction Declined by Local		 Or

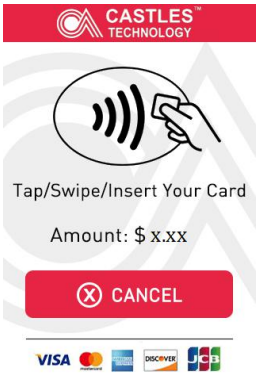
			 (If French first)
3.	Select card type if prompted If the selection times out or user presses cancel, you may see the following error: ● Transaction Canceled ● Operation Time Out		Card type selection is not required for Canada
3.	Select the AID if prompted If the selection times out or user presses cancel, you may see the following error: ● Transaction Canceled ● Operation Time Out		
4.	Input the PIN if prompted and press OK (you have three times to enter the PIN) If PIN is incorrect, you may see the following error: ● Incorrect PIN ● PIN Blocked ● PIN Failblocked If the entry times out or user presses cancel, you may see the following error: ● Transaction Canceled		

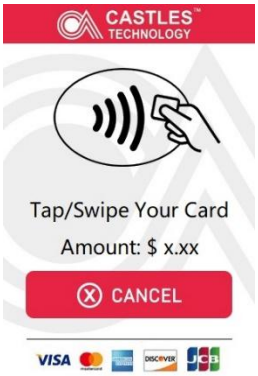
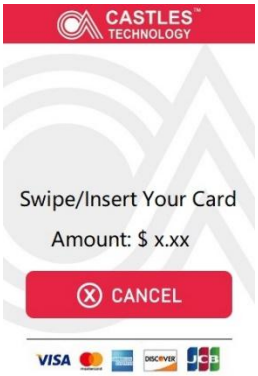
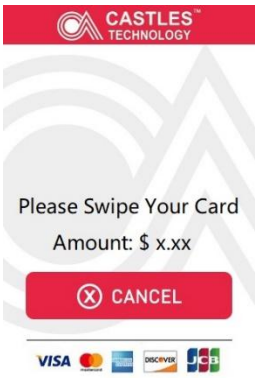
	● Operation Time Out		
5.	Terminal communicates out to the host for pre-auth transaction		
6.	Remove the card if prompted		
7.	Terminal displays the result of pre-auth transaction If pre-auth transaction fails, you may see the following error: ● Transaction Failed ● Transaction Declined		
8.	Terminal flashes “Thank You” and returns to the idle mode		

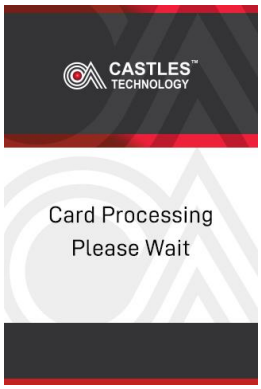
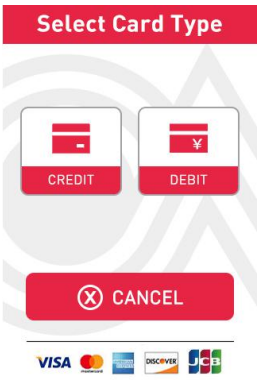
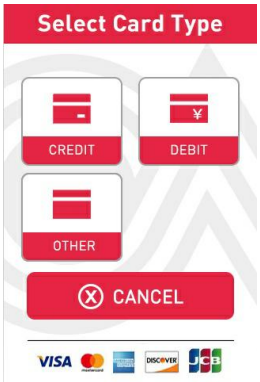
9.	On Kiosk - Plan to settle accounts (Kiosk sends a auth-complete command request to terminal) If the sending process or request content has problems, you may see the following error: ● (Terminal No Response) ● CMD Format Err		
10.	Terminal displays the result of auth-complete transaction and returns to idle mode If auth-complete transaction fails, you may see the following error: ● Transaction Failed ● Transaction Declined		

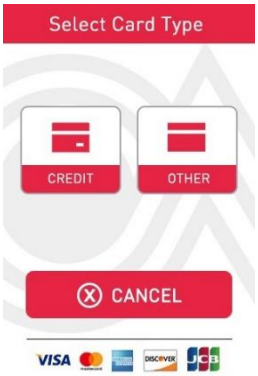
7.2.3. MSR TRANSACTION

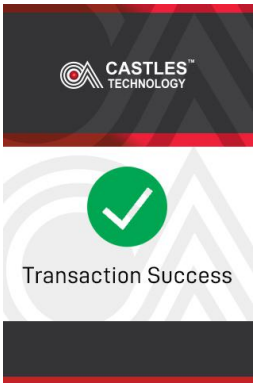
❖ Use the chart below to process a MSR card transaction when the card is swiped at the point of transaction.

Step	Action	Display US	Canada (French)
1.	On Kiosk - Plan to pay (Kiosk sends a pre-auth command request to terminal) If the sending process or request content has problems, the terminal may have the following behavior: ● Terminal no response ● Terminal shows "CMD Format Err" ● Terminal shows "Selection Over Limit" If the operation times out or user presses cancel, you may see the following error: ● Transaction Canceled ● Operation Time Out	 (x refers to digit) Or	 (x refers to digit) Or

	Note: For the application with Apriva transaction host, the payment screen will be displayed based on the supported Entry Modes.	 (If not support Contact Card) Or  (If not support Contactless Card) Or  (If not support Contact and Contactless Card)	 (If French first)

2.	Swipe Card If the card process fails, you may see the following error: ● Polling Card Failed ● Card Not Support ● Transaction Declined by Local ● Please Insert Your Card (MSR with chip)		 Or  (If French first)
3.	Select card type if prompted. If the selection times out or user presses cancel, you may see the following error: ● Transaction Canceled ● Operation Time Out Note: For the application with Apriva transaction host, the select card type screen will be displayed based on the supported Card Types, and the "OTHER" type mainly refers to campus card.	 Or  (If Closed Loop Card	Card type selection is not required for Canada

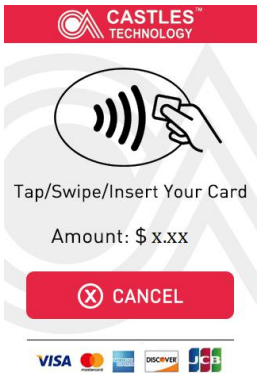
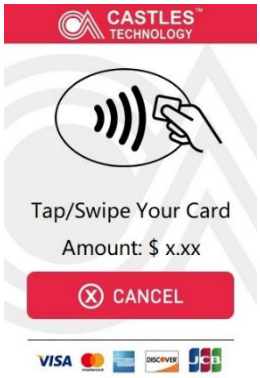
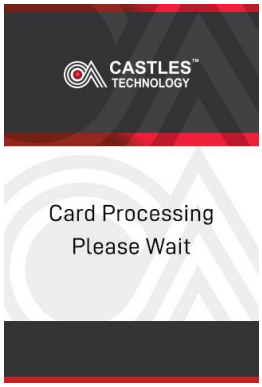
		supported) Or  (If Closed Loop Card supported but Debit Card not supported)	
4.	Terminal communicates out to the host for pre-auth transaction	 	
5.	Terminal displays the result of pre-auth transaction If pre-auth transaction fails, you may see the following error: ● Transaction Failed ● Transaction Declined	 	

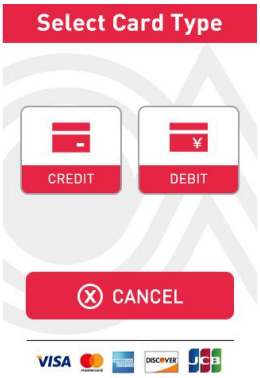
6.	Terminal flashes “Thank You” and returns to the idle mode		
7.	On Kiosk - Plan to settle accounts (Kiosk sends a auth-complete command request to terminal) If the sending process or request content has problems, you may see the following error: ● (Terminal No Response) ● CMD Format Err		
8.	Terminal displays the result of auth-complete transaction and returns to idle mode If auth-complete transaction fails, you may see the following error: ● Transaction Failed ● Transaction Declined		

7.2.4. EMVCL TRANSACTION

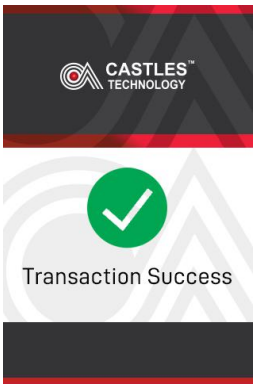
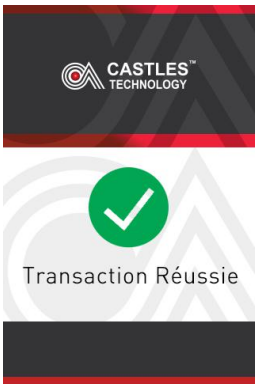
❖ Use the chart below to process a EMVCL card transaction when the card is tapped at the point of transaction.

Step	Action	Display	
		US	Canada (French)

1.	On Kiosk - Plan to pay (Kiosk sends a pre-auth command request to terminal) If the sending process or request content has problems, the terminal may have the following behavior: ● Terminal no response ● Terminal shows “CMD Format Err” ● Terminal shows “Selection Over Limit” If the operation times out or user presses cancel, you may see the following error: ● Transaction Canceled ● Operation Time Out Note: For the application with Apriva transaction host, the payment screen will be displayed based on the supported Entry Modes.	 (x refers to digit) Or  (If not support Contact Card)	 (x refers to digit) Or  (If French first)
2.	Tap Card If the card process fails, you may see the following error: ● Polling Card Failed ● Card Not Support ● Transaction Declined by Local ● Insert or Swipe This Card		 Or

			 (If French first)
3.	Select card type if prompted. If the selection times out or user presses cancel, you may see the following error: ● Transaction Canceled ● Operation Time Out		Card type selection is not required for Canada
4.	Input the PIN if prompted and press OK (you have three times to enter the PIN) If PIN is incorrect, you may see the following error: ● Incorrect PIN ● PIN Blocked ● PIN Failblocked If the entry times out or user presses cancel, you may see the following error: ● Transaction Canceled ● Operation Time Out		Canada does not support Online PIN

5.	Terminal communicates out to the host for pre-auth transaction		
6.	Terminal displays the result of pre-auth transaction If sale transaction fails, you may see the following error: ● Transaction Failed ● Transaction Declined		
7.	Terminal flashes “Thank You” and returns to the idle mode		
8.	On Kiosk - Plan to settle accounts (Kiosk sends a auth-complete command request to terminal) If the sending process or request content has problems, you may see the following error: ● (Terminal No Response) ● CMD Format Err		

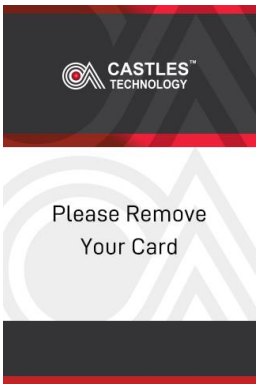
9.	Terminal displays the result of auth-complete transaction and returns to idle mode If auth-complete transaction fails, you may see the following error: ● Transaction Failed ● Transaction Declined		

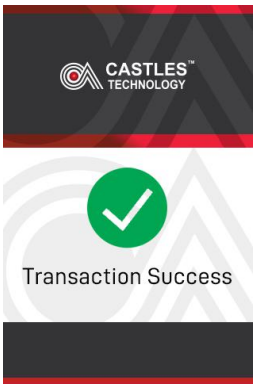
7.2.5. INTERAC TRANSACTION- CONTACT

❖ Use the chart below to process an Interac Debit card transaction when the card is inserted at the point of transaction. Interac card type is only supported with GP Canada transaction host.

Step	Action	Display Canada (English)	Canada (French)
1.	On Kiosk - Plan to pay (Kiosk sends a pre-auth command request to terminal) If the sending process or request content has problems, the terminal may have the following behavior: ● Terminal no response ● Terminal shows "CMD Format Err" ● Terminal shows "Selection Over Limit" If the operation times out or user presses cancel, you may see the following error: ● Transaction Canceled ● Operation Time Out	 (x refers to digit) Or  (If French first)	 (x refers to digit) Or  (If French first)

2.	Insert Interac Card If the card process fails, you may see the following error: ● Polling Card Failed ● Transaction Declined by Local	 Or  (If French first)	 Or  (If French first)
3.	Select YES to continue transaction if prompted If the selection times out or user presses NO, you may see the following error: ● Operation Time Out ● Transaction Canceled		
4.	Select Account Type if prompted If the selection times out or user presses EXIT, you may see the following error: ● Operation Time Out ● Transaction Canceled		

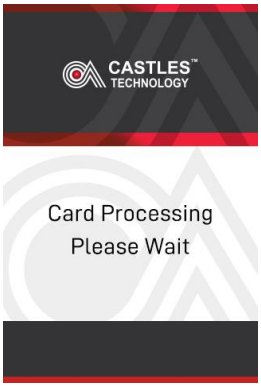
5.	Terminal communicates out to the host for pre-auth transaction		
6.	Remove the card if prompted		
7.	Terminal displays the result of pre-auth transaction If sale transaction fails, you may see the following error: ● Transaction Failed ● Transaction Declined		
8.	Terminal flashes “Thank You” and returns to the idle mode		

9.	On Kiosk - Plan to settle accounts (Kiosk sends a auth-complete command request to terminal) If the sending process or request content has problems, you may see the following error: ● (Terminal No Response) ● CMD Format Err		
10.	Terminal displays the result of auth-complete transaction and returns to idle mode If auth-complete transaction fails, you may see the following error: ● Transaction Failed ● Transaction Declined		

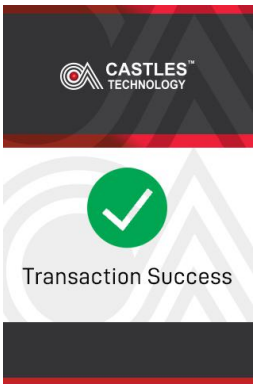
7.2.6. INTERAC TRANSACTION- CONTACTLESS

❖ Use the chart below to process an Interac Debit card transaction when the card is tapped at the point of transaction. Interac card type is only supported with GP Canada transaction host.

Step	Action	Display Canada (English)	Canada (French)
1.	On Kiosk - Plan to pay (Kiosk sends a pre-auth command request to terminal) If the sending process or request content has problems, the terminal may have the following behavior: ● Terminal no response ● Terminal shows "CMD Format Err" ● Terminal shows "Selection Over Limit" If the operation times out or user presses cancel, you may see the following error: ● Transaction Canceled	 (x refers to digit) Or	 (x refers to digit) Or

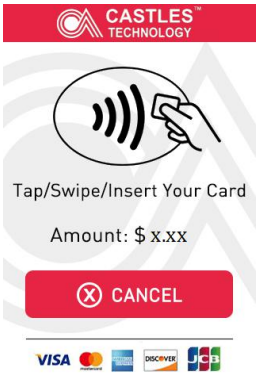
	● Operation Time Out	 (If French first)	 (If French first)
2.	Tap Interac Card If the card process fails, you may see the following error: ● Polling Card Failed ● Transaction Declined by Local		 Or  (If French first)
3.	Select YES to continue transaction if prompted If the selection times out or user presses NO, you may see the following error: ● Operation Time Out ● Transaction Canceled		

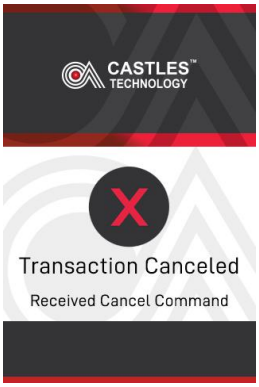
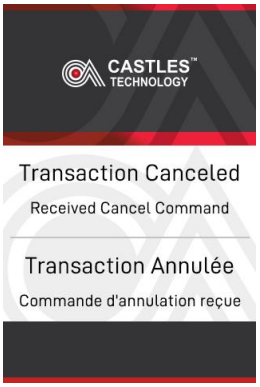
4.	Select Account Type if prompted If the selection times out or user presses EXIT, you may see the following error: ● Operation Time Out ● Transaction Canceled		
5.	Terminal communicates out to the host for pre-auth transaction		
6.	Terminal displays the result of pre-auth transaction If sale transaction fails, you may see the following error: ● Transaction Failed ● Transaction Declined		
7.	Terminal flashes “Thank You” and returns to the idle mode		

8.	On Kiosk - Plan to settle accounts (Kiosk sends a auth-complete command request to terminal) If the sending process or request content has problems, you may see the following error: ● (Terminal No Response) ● CMD Format Err		
9.	Terminal displays the result of auth-complete transaction and returns to idle mode If auth-complete transaction fails, you may see the following error: ● Transaction Failed ● Transaction Declined		

7.2.7. KIOSK CANCEL TRANSACTION

❖ This transaction is used when the user has not paid for the existing products; but wants to cancel. This cancellation could be done before the terminal communicates with the host for pre-auth transaction.

Step	Action	Display US	Canada (French)
1.	On Kiosk - Plan to pay (Kiosk sends a pre-auth command request to terminal) If the sending process or request content has problems, the terminal may have the following behavior: ● Terminal no response ● Terminal shows "CMD Format Err" Terminal shows "Selection Over Limit" If the operation times out or user presses cancel, you may see the following error: ● Transaction Canceled	 (x refers to digit)	 (x refers to digit) Or

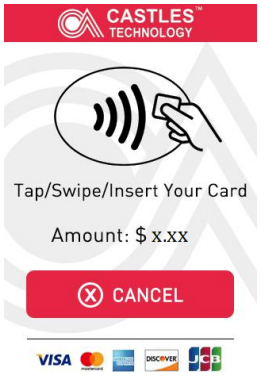
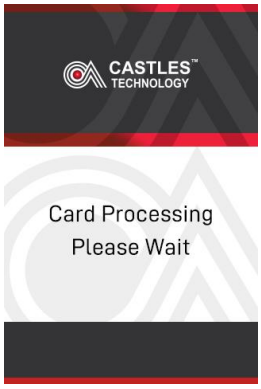
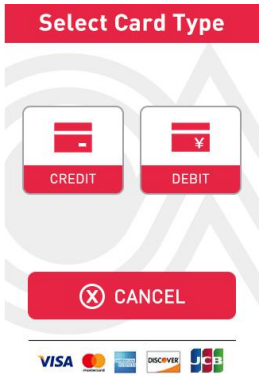
	● Operation Time Out		 (If French first)
2.	On Kiosk - Press cancel (Kiosk sends a cancel command request to terminal)		 Or  (If French first)
3.	Terminal returns to the idle mode		

7.2.8. KIOSK CANCEL PRE-AUTH

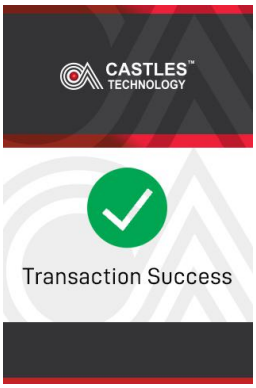
❖ This transaction is used when the user has pre-paid for the existing products; but wants to cancel. The terminal will communicate with the host to do reversal transaction. This cancellation could be done after the terminal communicates with the host for pre-auth transaction, but before auth-complete transaction.

➢ The transaction process below takes MSR card as an example.

Step	Action	Display

		US	Canada (French)
1.	On Kiosk - Plan to pay (Kiosk sends a pre-auth command request to terminal) If the sending process or request content has problems, the terminal may have the following behavior: ● Terminal no response ● Terminal shows “CMD Format Err” ● Terminal shows “Selection Over Limit” If the operation times out or user presses cancel, you may see the following error: ● Transaction Canceled ● Operation Time Out	 (x refers to digit)	 (x refers to digit) Or  (If French first)
2.	Swipe Card If the card process fails, you may see the following error: ● Polling Card Failed ● Card Not Support ● Transaction Declined by Local ● Please Insert Your Card (MSR with chip)		
3.	Select card type if prompted. If the selection times out or user presses cancel, you may see the following error: ● Transaction Canceled ● Operation Time Out		Card type selection is not required for Canada

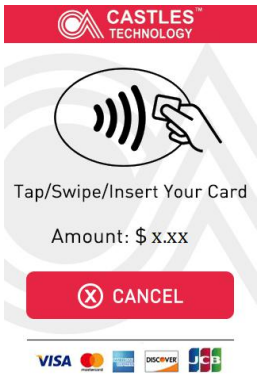
4.	Terminal communicates out to the host for pre-auth transaction		
5.	Terminal displays the result of pre-auth transaction If pre-auth transaction fails, you may see the following error: ● Transaction Failed ● Transaction Declined		
6.	Terminal flashes “Thank You” and returns to the idle mode		
7.	On Kiosk - Plan to cancel transaction (Kiosk sends a cancel pre-auth command request to terminal) If the sending process or request content has problems, you may see the following error: ● (Terminal No Response) ● CMD Format Err		

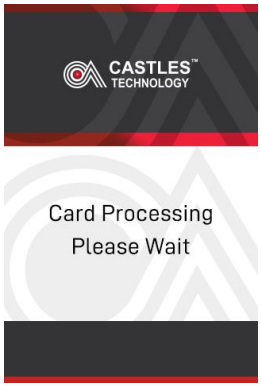
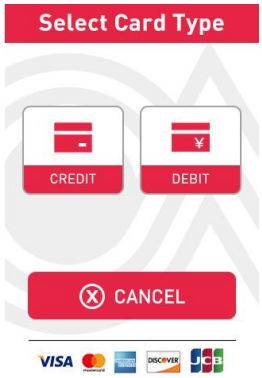
8.	Terminal displays the result of cancel pre-auth transaction and returns to idle mode If cancel pre-auth transaction fails, you may see the following error: ● Transaction Failed ● Transaction Declined		

7.2.9. TOKEN TRANSACTION

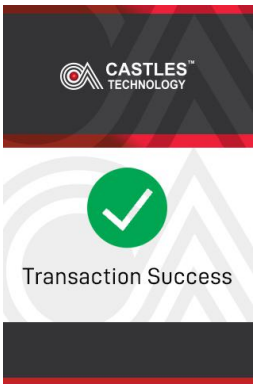
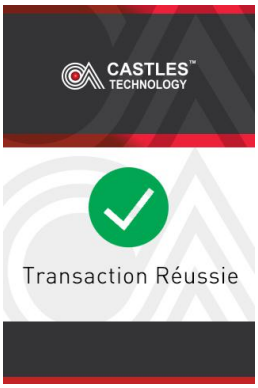
❖ This transaction is used when the user does not want to use the physical card. When the user completes the payment by using a physical card for the first time, then the user can directly use the unique token value of the card to complete the next payments without using the physical card. Please note that only Heartland Portico USA and GP Canada support this transaction.

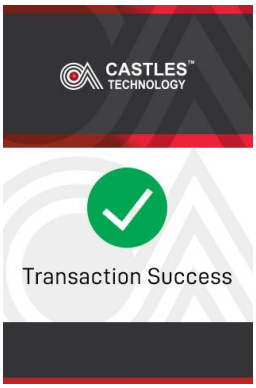
➢ The transaction process below takes MSR card as an example. If the token value of the card is already gotten by the Kiosk, the user can turn to step 9 to perform the transaction directly.

Step	Action	Display	
		US	Canada (French)
1.	On Kiosk - Plan to pay (Kiosk sends a pre-auth command request with the tag "RequestToken" to terminal, it's value is TRUE) If the sending process or request content has problems, the terminal may have the following behavior: ● Terminal no response ● Terminal shows "CMD Format Err" ● Terminal shows "Selection Over Limit" If the operation times out or user presses cancel, you may see the following error: ● Transaction Canceled ● Operation Time Out	 (x refers to digit)	 (x refers to digit) Or

			 (If French first)
2.	Swipe Card If the card process fails, you may see the following error: ● Polling Card Failed ● Card Not Support ● Transaction Declined by Local ● Please Insert Your Card (MSR with chip)		 Or  (If French first)
3.	Select card type if prompted. If the selection times out or user presses cancel, you may see the following error: ● Transaction Canceled ● Operation Time Out		Card type selection is not required for Canada

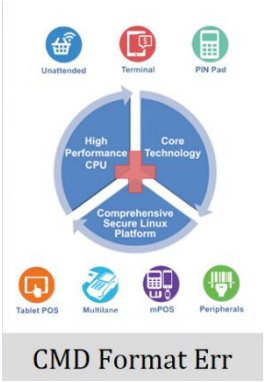
4.	Terminal communicates out to the host for pre-auth transaction		
5.	Terminal displays the result of pre-auth transaction If pre-auth transaction fails, you may see the following error: ● Transaction Failed ● Transaction Declined		
6.	Terminal flashes “Thank You” and returns to the idle mode Terminal responses the Token Value of the card to Kiosk, and Kiosk should save this value to local for the user to do the next transaction		
7.	On Kiosk - Plan to settle accounts (Kiosk sends a auth-complete command request to terminal) If the sending process or request content has problems, you may see the following error: ● (Terminal No Response) ● CMD Format Err		

8.	Terminal displays the result of auth-complete transaction and returns to idle mode If auth-complete transaction fails, you may see the following error: ● Transaction Failed ● Transaction Declined		
9.	On Kiosk - Select products and plan to pay (Kiosk sends a pre-auth command request with the tag "TokenValue" to terminal, it's value should be the token value of the card) Terminal communicates to the host for pre-auth transaction		
10.	Terminal displays the result of pre-auth transaction If pre-auth transaction fails, you may see the following error: ● Transaction Failed ● Transaction Declined		
11.	Terminal flashes "Thank You" and returns to the idle mode		

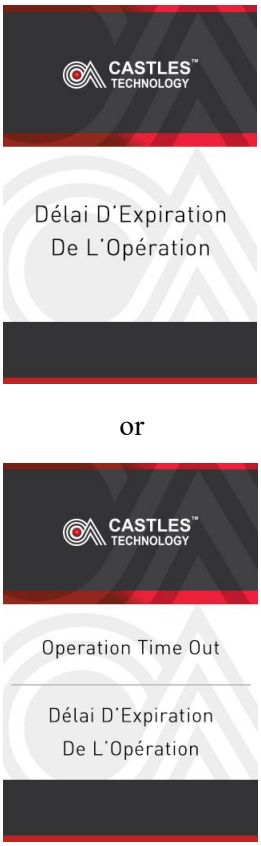
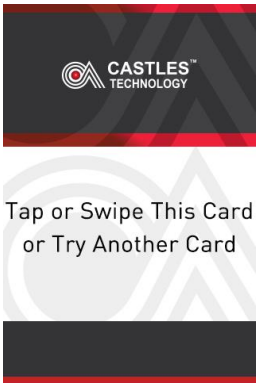
12.	On Kiosk - Plan to settle accounts (Kiosk sends a auth-complete command request to terminal) If the sending process or request content has problems, you may see the following error: ● (Terminal No Response) ● CMD Format Err		
13.	Terminal displays the result of auth-complete transaction and returns to idle mode If auth-complete transaction fails, you may see the following error: ● Transaction Failed ● Transaction Declined		

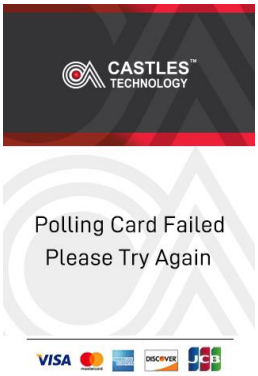
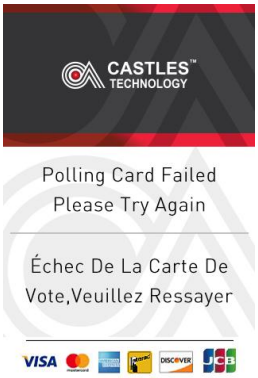
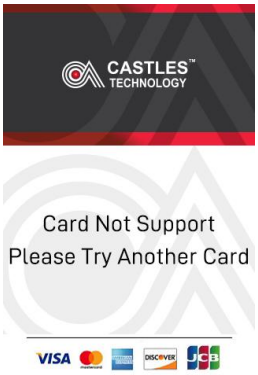
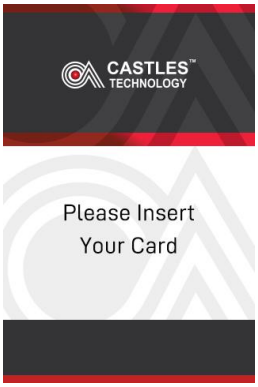
7.3. Transaction Error Messages

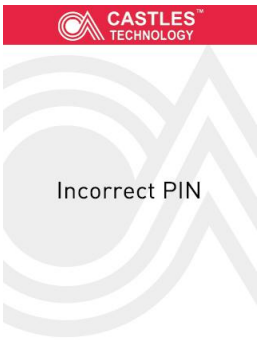
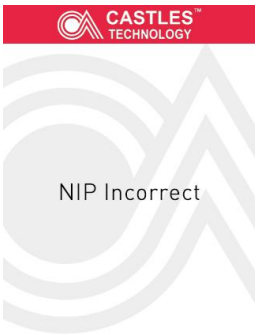
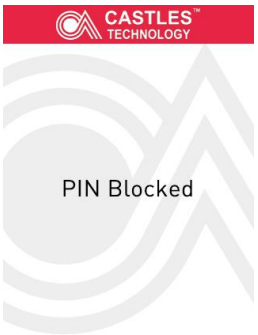
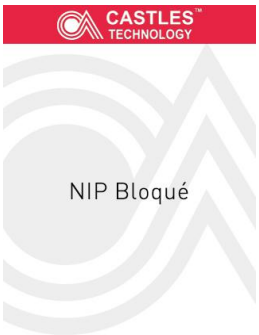
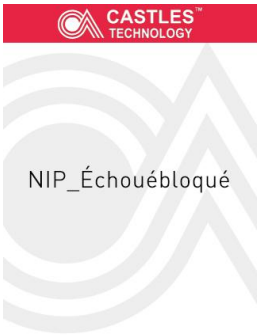
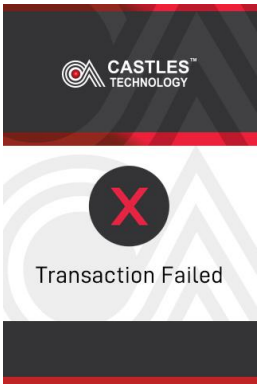
❖ Use the chart below to check the display and cause of the error messages that may appear in Code_N_Go_unatt transactions.

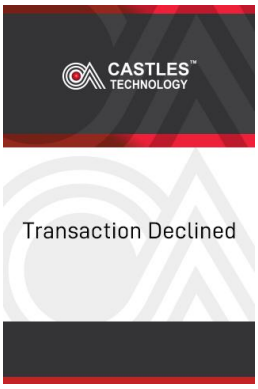
Error Message Kisok	Cause	Display	
		US	Canada (French)
CMD Format Err	Fails to parse command because there's something wrong with the command		

Selection Over Limit	The price of selected product exceeds the amount limit	CASTLES TECHNOLOGY Selection Over Limit Charge Canceled No Charge	CASTLES TECHNOLOGY Selection Over Limit Charge Canceled No Charge Sélection Hors Limite Frais Annulée Sans Frais
Amount Not Support	The amount of sale or pre-auth request equals to zero, but it is not supported (The request with an amount equal to zero is for Token transaction)	CASTLES TECHNOLOGY Amount Invalid Charge Canceled No Charge	CASTLES TECHNOLOGY Amount Invalid Charge Canceled No Charge Montant invalide Frais Annulée Sans Frais
Transaction Canceled	User cancels the transaction during card processing	CASTLES TECHNOLOGY Transaction Canceled	CASTLES TECHNOLOGY Transaction Annulée or CASTLES TECHNOLOGY Transaction Canceled Transaction Annulée

Operation Time Out	User's operation times out during card processing		
Tap or Swipe This Card or Try Another Card	Fails to read EMV card data, EMV Fallback		
Insert or Swipe This Card or Try Another Card	Fails to read EMVCL card data, EMVCL Fallback		

Transaction Declined by Local	Offline Declined Something went wrong while your card is being processed		
Polling Card Failed Please Try Again	Fails to read MSR or EMVCL card data		
Card Not Support Please Try Another Card	The Card Bin of MSR card may is not supported The Pre-auth Amount may exceed the CVM Limit		
Please Insert Your Card	This MSR card supports chip		

Incorrect PIN	The entered PIN incorrect		
PIN Blocked	Card is locked due to the last PIN entered is incorrect		
PIN Failblocked	Card is locked due to the last PIN entered for Online PIN is incorrect		
Transaction Failed	Fails to finish the sale transaction		

Transaction Declined	The host decline the transaction		
Transaction Declined Need Key Injection	The PIN key is required when processing transaction with online PIN		

8. INSTALLATION INSTRUCTIONS

- The terminal should be installed correctly on Kiosk Machine before using. This section describes the accessories required and installation instructions of Castles UPT1000F terminal and VEGA3000P terminal respectively.

8.1. UPT1000F Installation

- The unattended application in Castles UPT1000F terminal supports two host communication types with transaction server (GPRS and Ethernet), four command communication types (RS232, USB, Bluetooth and Ethernet). Please confirm the specific communication types for the terminal which you are working with before using.

8.1.1. Accessories Required

- Use the chart below to describes the accessories which may be required for Castles Supported Kiosk.

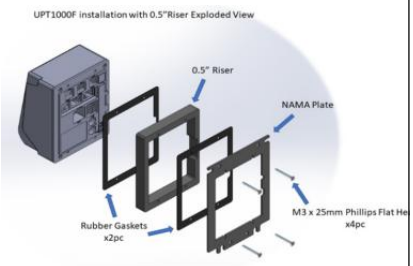
ID	Item	Apply	Accessory
1	UPT1000F	Castles Terminal Model: UPT1000F	
2	Antenna	Used with SIM card when communication type with transaction server is GPRS.	
3	Ethernet Cable	Used when communication type with transaction server is Ethernet.	

4	MDB Power Cable	Used for power supply.	
5	Nama Plate/ Screws	Used when installation if needed.	
6	RS232 Cable	Used when command communication type is RS232.	
7	USB Cable	Used when command communication type is USB.	

8.1.2. Installation Steps

❖ This section describes the steps necessary to install a UPT1000F terminal on a Castles Supported Kiosk.

Step	Action	Detail	Illustration

1	Check SIM Installation (if GPRS)	Verify that the SIM for wireless access is properly installed in the correct slot of the terminal. The SIM should be in the upper left slot behind the rubber card port door, with the cut corner facing out and up, and the SIM contacts facing to the right.	
2	Antenna installation (if GPRS)	Verify that the Antenna is properly installed in the correct port of the terminal tightly. The Antenna should be tightened and not be shielded.	
3	Ethernet Installation (if Ethernet)	Verify that the Ethernet for wire access is properly installed in the correct port of the terminal.	
4	Install Risers on Terminal (if needed)	Install the risers required for the specific machine correctly.	
5	RS232 Cable Connection (if RS232)	Plug the RS232 Cable into the COM1 port of UPT1000F, then plug the other end into the Kiosk Controller RS232 port.	

6	USB Cable Connection (if USB)	Plug the USB Cable into the USB1 port of UPT1000F, then plug the other end into Kiosk Controller USB port.	
7	Power Supply Connection (if needed)	Locate the MDB power cable and plug it into MDB Connection slot of UPT1000F, then connect to the Kiosk Controller or other power supply terminal.	

8.2. VEGA3000P Installation

- The unattended application in Castles VEGA3000P terminal supports one host communication type with transaction server (Ethernet), three command communication types (RS232, USB and Ethernet). Please confirm the specific communication types for the terminal which you are working with before using.

8.2.1. Accessories Required

- Use the chart below to describes the accessories which may be required for Castles Supported Kiosk.

ID	Item	Apply	Accessory
1	VEGA3000P with USB cable	Castles Terminal Model: VEGA3000P Used when command communication type is USB	
2	VEGA3000P with RS232 cable	Castles Terminal Model: VEGA3000P Used when command communication type is RS232	

3	Ethernet Cable	Used for host communication	
4	USB Power Supply	Used for power supply	

8.2.2. Installation Steps

❖ This section describes the steps necessary to install a VEGA3000P terminal on a Castles Supported Kiosk.

Step	Action	Detail	Illustration
1	USB Cable Connection (if USB)	Verify that the cable connect with terminal is USB cable, then plug the other end into Kiosk Controller USB Port	
2	RS232 Cable Connection (if RS232)	Verify that the cable connect with terminal is RS232 cable, then plug the other end into Kiosk Controller RS232 Port	

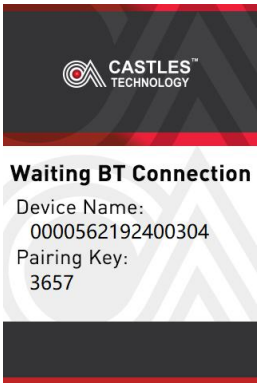
3	Ethernet Installation	Verify that the Ethernet for wire access is properly installed in the correct port of the terminal.	
4	Power Supply Connection	Locate the USB Power Supply cable and plug it into the correct port of the terminal, then connect to the Kiosk Controller or other power supply terminal.	

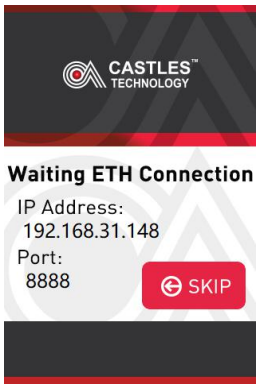
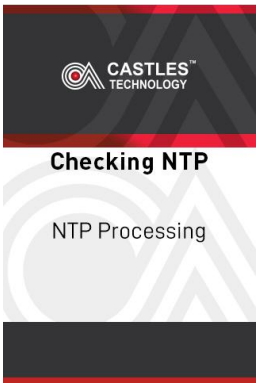
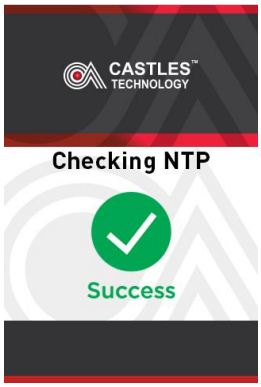
9. TERMINAL INITIALIZATION

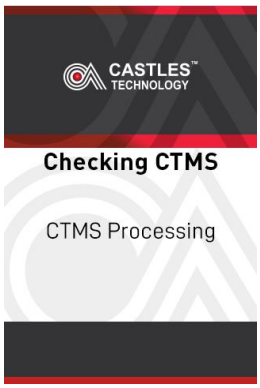
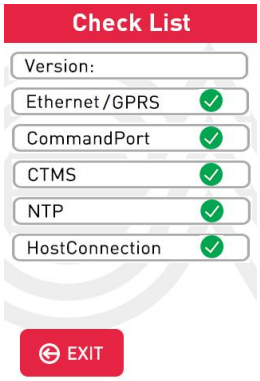
9.1. Initialization Process

- ❖ Power up the terminal, there will be an initialization process before entering slide show. A series of messages similar in appearance to the one in the chart below will appear on the terminal display. If you see an error message, consult the Init Error Messages table in the next section.
- ➢ For the Code_N_Go_unatt application, you need to configure on the kiosk machine and to connect the command communication between the terminal and the kiosk machine successfully, otherwise transactions cannot be executed. Please refer to the section "How to configure on Kiosk machine" for details.

Step	Action	Display
1.	Start to run the application and load the configuration If GPRS, you may see the following error: ● SIM Card Not Ready	
2.	Trying to update the configuration file Note: This process will only be performed after USB Configuration Update	
3.	Terminal is successfully updates the configuration file If something goes wrong, you may see the following error: ● Update CFG File Failed	

4.	Trying to connect to the wireless network	
5.	Successfully connected to the wireless network. If connect failed, you may see the following error: ● Checking Network Failed	
6.	Terminal is waiting the Bluetooth connection. You need to find that Bluetooth terminal on the kiosk machine and pair it successfully, and open the command port Note: This process will only be performed when the used command communication type is Bluetooth	 (The terminal name of every terminal is unique, and the pairing key is generated randomly)
7.	Successfully connected to Kiosk through Bluetooth If command port open failed, you may see the following error: ● Open BT CMD Port Failed	

8.	Terminal is waiting the Ethernet connection. You need to fill the correct IP and Port on the kiosk machine, and open the command port Note: This process will only be performed when the used command communication type is Ethernet	 (The IP Address of every terminal is unique and configurable)
9.	Successfully connected to the Kiosk through Ethernet	
10.	Terminal is completing the Network Time Protocol (NTP); comparing the time registered by the network with the time on the internal clock of the terminal	
11.	NTP is completed and terminal clock is set to the time on the network If something goes wrong, you may see the following error: ● Checking NTP Failed	

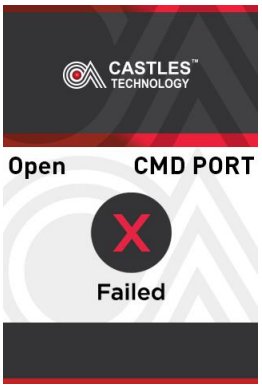
12.	The terminal is attempting to communicate with the CTMS system, confirm it is correctly registered with the system and get the trigger time.	
13.	Validates correct communication timing between CTMS and the terminal If the terminal is not correctly set up in CTMS or something goes wrong, you may see the following error: ● Checking CTMS Failed ● CTMS Trigger Time receive failed ● Terminal Not Set Up in CTMS ● Terminal Not Set Up in Group ● CTMS Trigger Time Not Exist	
14.	Check List: Will display after initialization. It is for user to check the initialization result, and press any one of the items to view details.	
15.	Application Home page (slide show): Will display after check list. The status bar at the bottom has characters that scroll from left to right. Status bar will display one of the messages below, depending on state of the terminal. ● Welcome ● Reader Disabled	

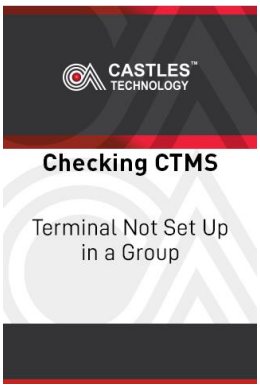
		

9.2. Init Error Messages

❖ Use the chart below to check the display and cause of the error messages that may appear in the initialization process

Error Message	Cause	Display
SIM Card Not Ready	This notification indicates SIM card is not installed properly; or, has not been properly set up with the wireless carrier.	
Update CFG File Failed	Terminal is unable to update the latest configuration file value	
Checking Network Failed	Terminal is unable to connect the network	

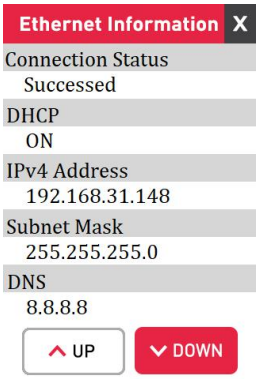
Open CMD Port Failed	Terminal is unable to open the command port	
Checking NTP Failed	Can occur when the website used for the time check is unavailable, or for other reasons.	
Checking CTMS Failed	This message is displayed when the terminal fails to connect to the CTMS	
Terminal Not Set Up in CTMS	This message is displayed when the serial number of the terminal is not set up in CTMS.	

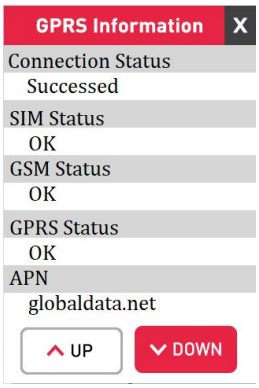
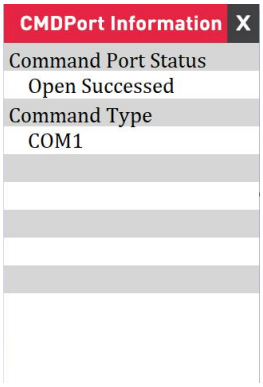
Terminal Not Set Up in a Group	This message is displayed when the terminal belongs to Terminal Pool in CTMS	
CTMS Trigger Time Not Exist	This message is displayed when the trigger time is not set in your group	

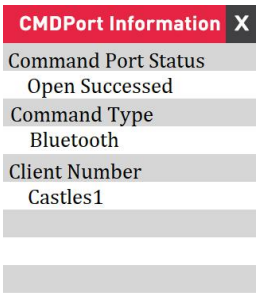
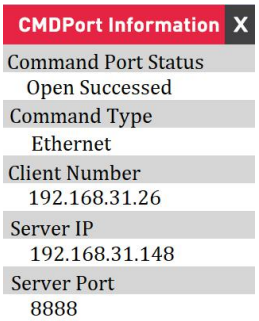
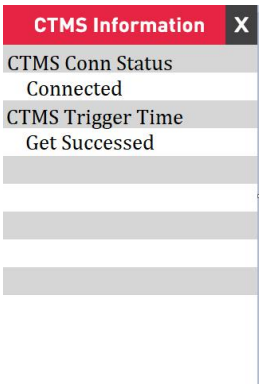
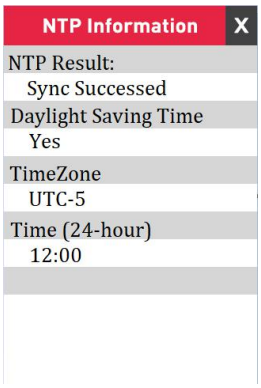
9.3. Details of Check List

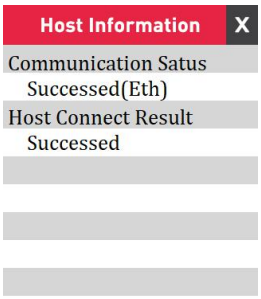
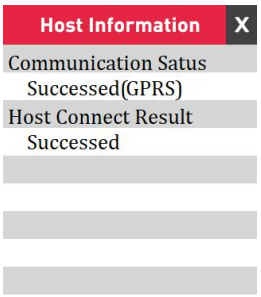
❖ Use the chart below to check the details of check list. Initialization items listed in this section are the following:

- Ethernet
- GPRS
- CommandPort
- CTMS
- NTP
- HostConnction

Items	Details	Display
Ethernet (Displayed when the used communication method with transaction host is Ethernet)	Connection Status: ● Successed ● Not Open ● Not Support ● IP Invalid ● Open Failed ● Get Info Failed ● Unknown Error (When the connection status is not successed, the values of following information would be "NA".) DHCP: ● ON ● OFF	

	IPv4 Address: (actual value) Subnet Mask: (actual value) DNS: (actual value) Default Gateway: (actual value)	
GPRS (Displayed when the used communication method with transaction host is GPRS)	Connection Status: ● Successed ● Failed SIM Status: ● OK ● SIM Not Ready ● SIM Slot Invalid GSM Status: ● OK ● GSM Mode Invalid ● GSM Open Failed ● PIN Verify Failed GPRS Status: ● OK ● GPRS Not Support ● GPRS Not Open ● GPRS Open Failed ● GPRS Info Get Failed ● GPRS DNS Set Failed ● Unknown Error APN: (actual value) UserName: (actual value) Password: (actual value)	
CommandPort	(When the command type is neither Bluetooth nor Ethernet) Command Port Status: ● Open Successed ● Open Failed Command Type: ● COM1 ● COM3 ● USB1	

	(When the command type is Bluetooth) Command Port Status: ● Open Successed ● Open Failed Command Type: ● Bluetooth Client Number: (actual value)	
	(When the command type is Ethernet) Command Port Status: ● Open Successed ● Open Failed Command Type: ● Ethernet Client Number: (actual value) Server IP: (actual value) Server Port: (actual value)	
CTMS	CTMS Conn Status: ● Connected ● Not Connected CTMS Trigger Time: ● Get Successed ● Physical Link Error ● Terminal Not Set Up ● Not Add to Group ● Not Set Up (indicates the trigger time is not set) ● Trigger Time Failed	
NTP	NTP Result: ● Sync Successed ● Invalid Param ● Invalid IP ● Get RTC Failed ● Set Url Failed ● Set DNS IP Failed ● Sync Time Out ● Sync Time Failed ● Set Time Failed ● TimeZone Over Limit ● Set TimeZone Failed ● Unknown Error	

	Daylight Saving Time: ● Yes ● No TimeZone: (actual value) Time (24-hour): (actual value)	
HostConnection	(When the communication method is Ethernet) Communication Status: ● Successed(Eth) ● Failed(Eth) Host Connect Result: ● Successed ● Failed	
	(When the communication method is GPRS) Communication Status: ● Successed(GPRS) ● Failed(GPRS) Host Connect Result: ● Successed ● Failed	

9.4. How to configure on Kiosk machine

❖ This section describes the steps and instructions necessary to configure on the PC side to simulate the kiosk machine for command communication. With the Code_N_Go_unatt application, UPT1000F terminals support four methods to communication with the Kiosk: RS232, USB, Bluetooth and Ethernet; and VEGA3000P terminals only support three of them: RS232, USB and Ethernet. Configuration methods demonstrated in this section are the following:

- Configure RS232
- Configure USB
- Configure Bluetooth
- Configure Ethernet

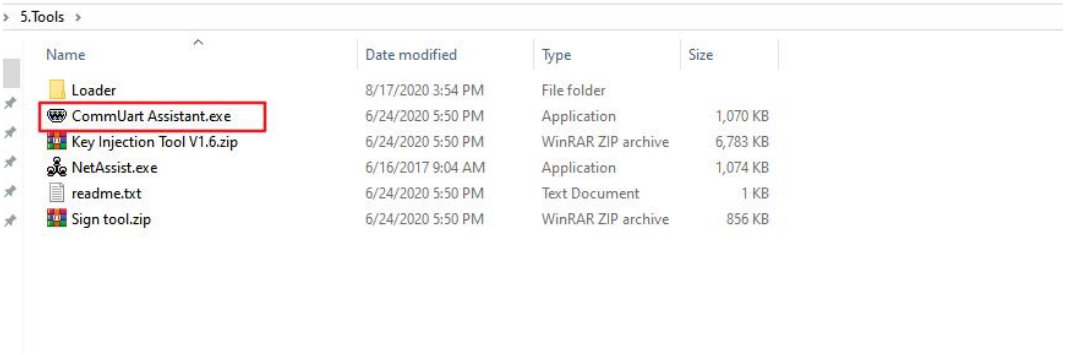
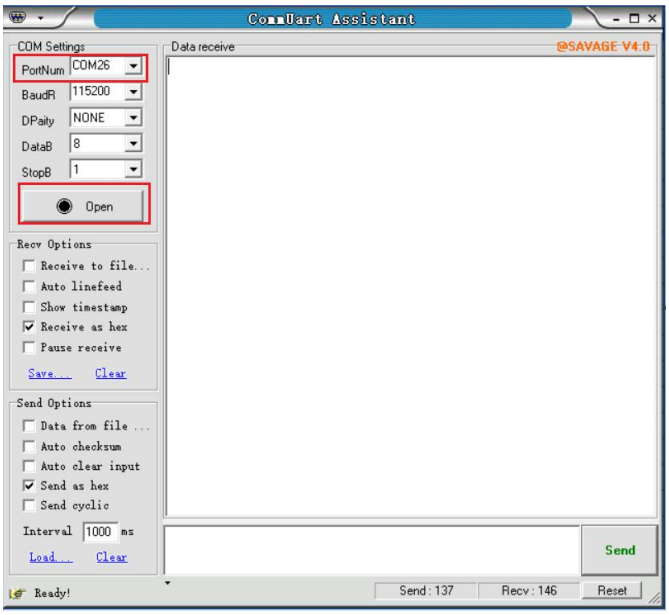
➢ The command communication method can be switched through CTMS or USB parameter update, there is a parameter named "Command Communication" for you to change, please see in the annex configuration "COMM Config" to check the parameter definition.

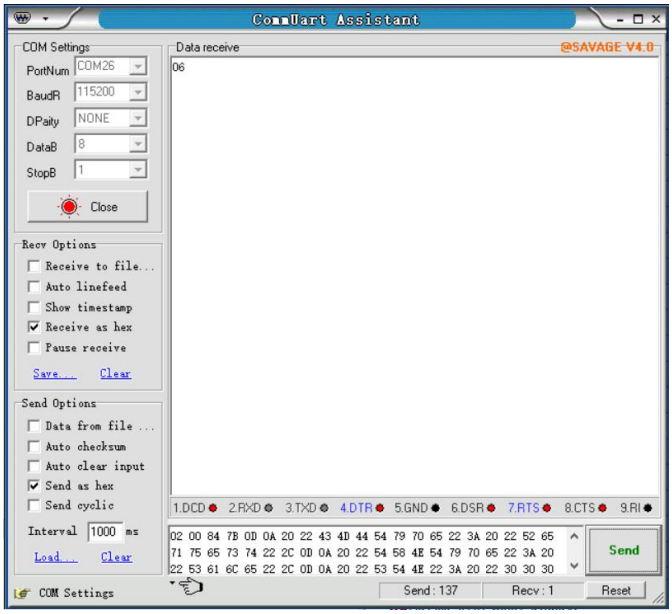
9.4.1. Configure RS232

❖ Use the chart below to configure related RS232 settings on the PC side. Please

refer to your own kiosk specification for the specific steps may be based on kiosk machine.

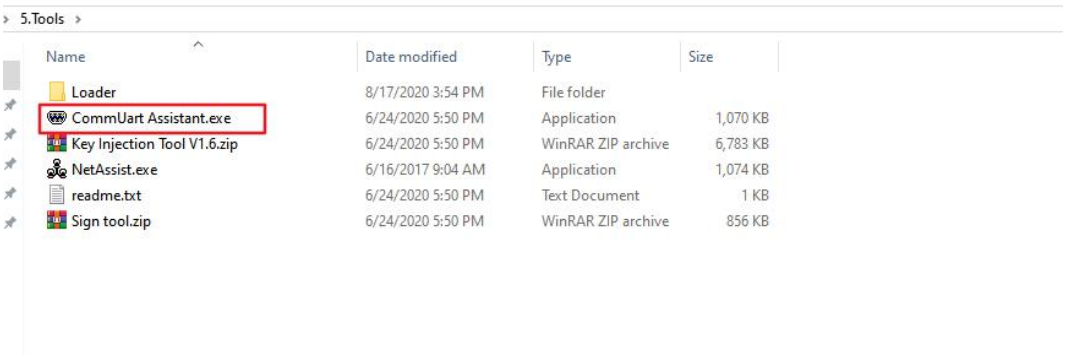
- On the PC side, you need to use one debugging tool to simulate the kiosk machine. We use the "CommUart Assistant" tool, which can be found in the "5.Tools" folder of the release package.

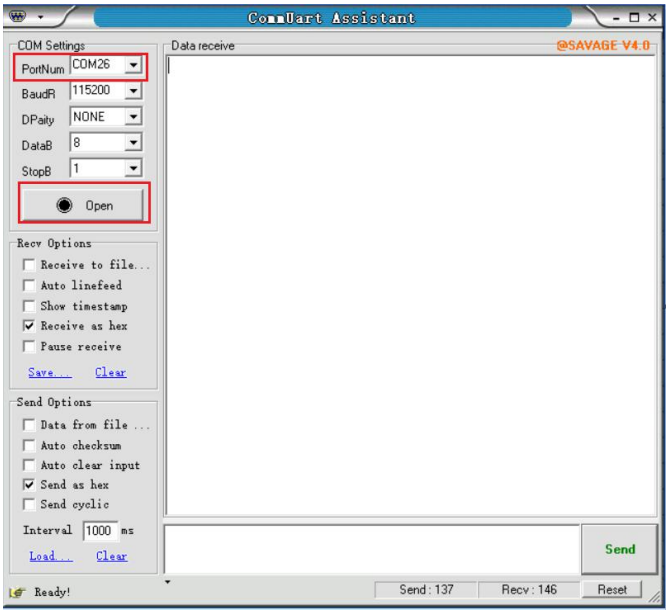
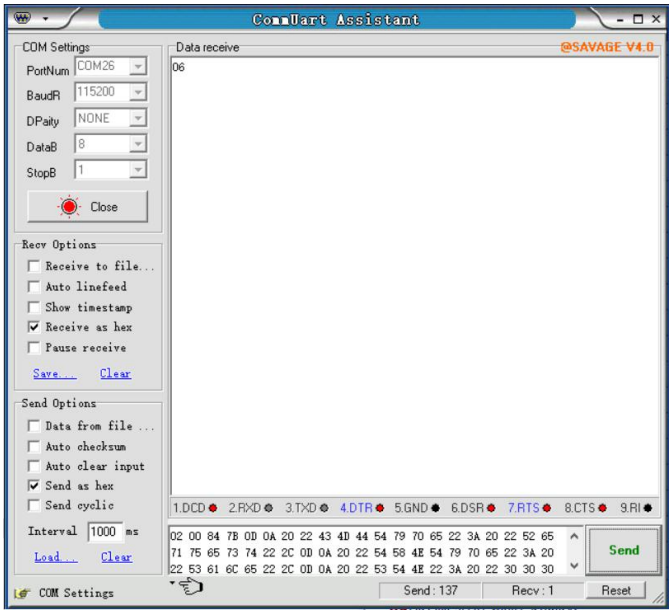
Step	Action & Display
1.	Make sure that the command communication type of the terminal you are working with is RS232. If not, please follow the steps in "Communication Switch" to switch it. Note: Only when your UPT1000F terminal does not support MDB, the COM3 port could be used for command communication
2.	Connect the RS232 cable between the terminal and your PC correctly, please refer to the section "INSTALLTION INSTRUCTIONS" for details
3.	On the PC side, open the "CommUart Assistant" tool 
4.	Select the correct COM Port in the PortNum drop-down box, and then click the Open button 
5.	In the idle state of the terminal, tick the Send as hex box, input the command, click the Send button, and then the command will be sent to your terminal through this debugging tool

9.4.2. Configure USB

- ❖ Use the chart below to configure related USB settings on the PC side. Please refer to your own kiosk specification for the specific steps may be based on kiosk machine.
- ➢ On the PC side, you need to use one debugging tool to simulate the kiosk machine. We use the "CommUart Assistant" tool, which can be found in the "5.Tools" folder of the release package.

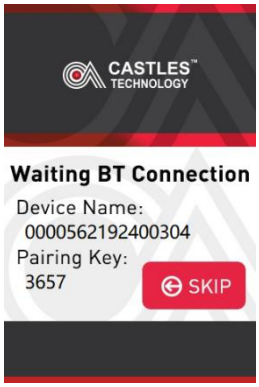
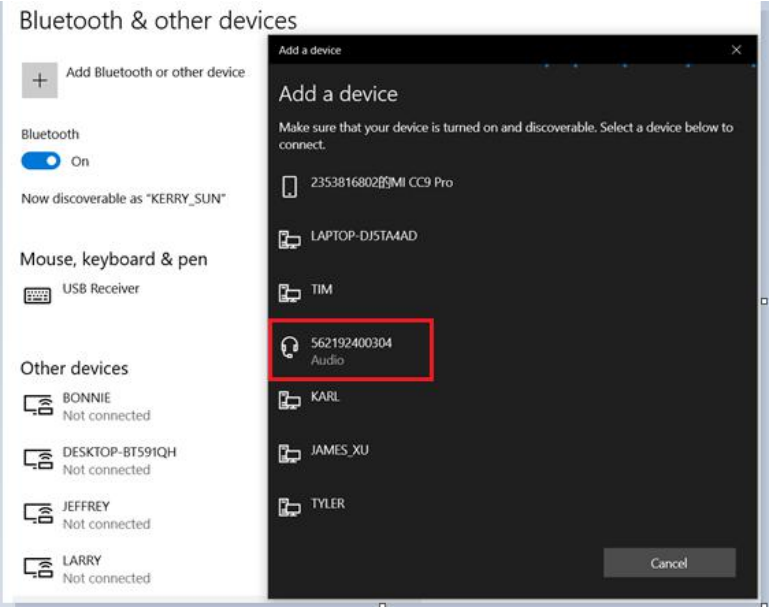
Step	Action & Display
1.	Make sure that the command communication type of the terminal you are working with is USB. If not, please follow the steps in "Communication Switch" to switch it.
2.	Connect the USB cable between the terminal and your PC correctly, please refer to the section "INSTALLTION INSTRUCTIONS" for details
3.	On the PC side, open the "CommUart Assistant" tool 
4.	Select the correct COM Port in the PortNum drop-down box, and then click the Open button

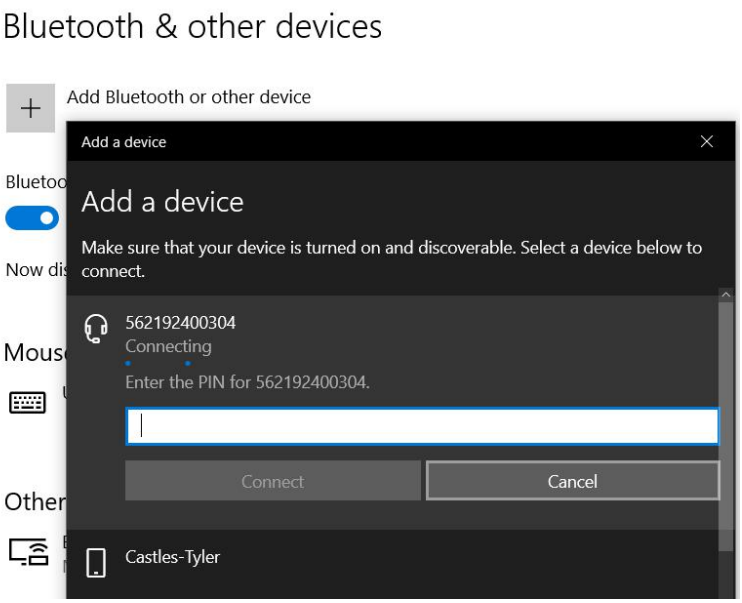
	
5.	In the idle state of the terminal, tick the Send as hex box, input the command, click the Send button, and then the command will be sent to your terminal through this debugging tool 

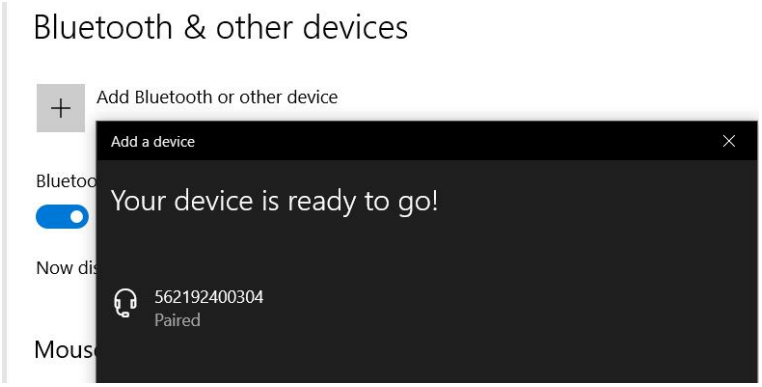
9.4.3. Configure Bluetooth

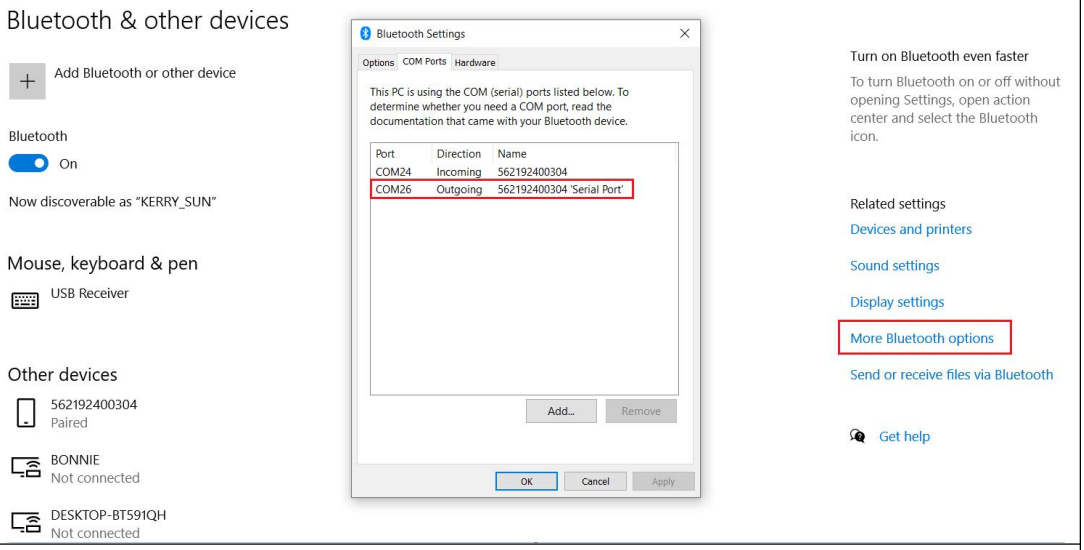
- ❖ Use the chart below to configure related Bluetooth settings on the PC side. Please refer to your own kiosk specification for the specific steps may be based on kiosk machine.
- ➢ On the PC side, you need to use one debugging tool to simulate the kiosk machine. We use the "CommUart Assistant" tool, which can be found in the "5.Tools" folder of the release package.

Step	Action & Display

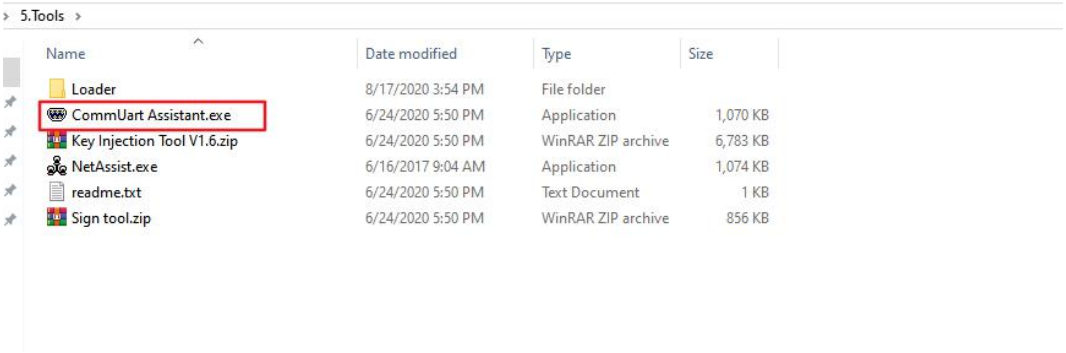
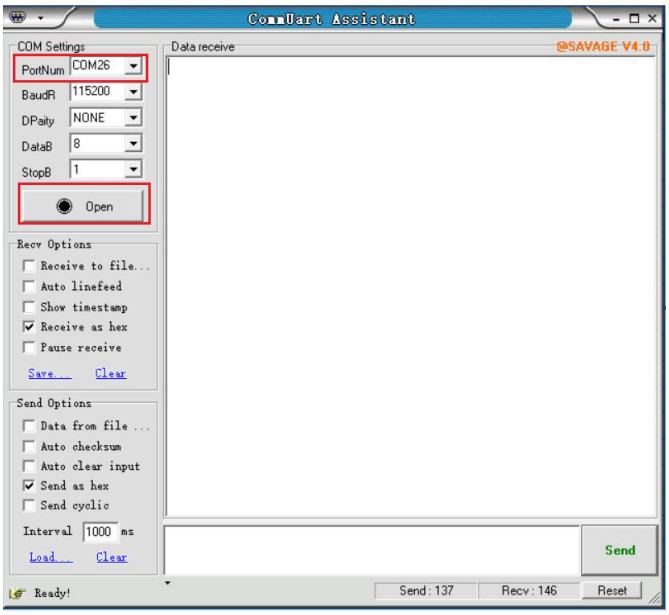
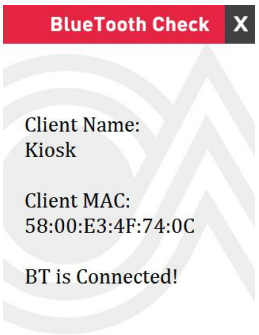
1.	Make sure that the command communication type of the terminal you are working with is Bluetooth. If not, please follow the steps in "Communication Switch" to switch it.
2.	Confirm the configuration of Bluetooth on the terminal：Device Name and Pairing Key ■ Do not restart the terminal, you can check the Bluetooth information in Service Mode menu. For detailed instructions of how to check the information, please refer to the section "Bluetooth" ■ Restart the terminal, you can check the Bluetooth information during the initialization **Check in Bluetooth Menu** / **Check in initialization**  
3.	On the PC side: ■ Open Bluetooth & other devices settings ■ Confirm that the Bluetooth of your PC is on; if not, turn on it ■ Select to add Bluetooth device ■ Wait the scanning of Bluetooth devices until the device name which indicated in step3 is displayed 
4.	■ Select to add that device ■ Fill in the Pairing Key which indicated in step3 in the PIN field ■ Click "Connect" button, it will display paired after the successful connection

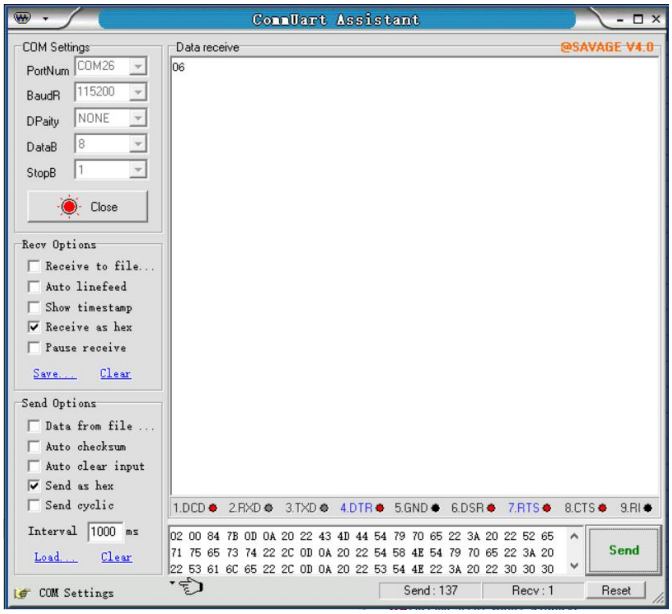
<table>
<tr><td></td><td>




</td></tr>
<tr><td>5.</td><td>After paired, confirm the COM(serial) Port for your Bluetooth device through viewing the Bluetooth Settings


</td></tr>
<tr><td>6.</td><td>Open the "CommUart Assistant" tool</td></tr>
</table>

<table>
<tr><td></td><td> 
</td></tr>
<tr><td>7.</td><td>Select the correct COM Port which indicated in step6 in the PortNum drop-down box, and then click the Open button
 
</td></tr>
<tr><td>8.</td><td>After the Bluetooth is connected successfully, you can check the connection result or status on the terminal
■ Do not restart the terminal, the information shown in Bluetooth menu will be updated with “BT is Connected”
■ During the initialization, the connection result will be displayed automatically after the connected
<table>
<tr><th>Check in Bluetooth Menu</th><th>Check in initialization</th></tr>
<tr><td> 
</td><td> 
</td></tr>
</table></td></tr>
<tr><td>9.</td><td>In the idle state of the terminal, tick the Send as hex box, input the command, click the</td></tr>
</table>

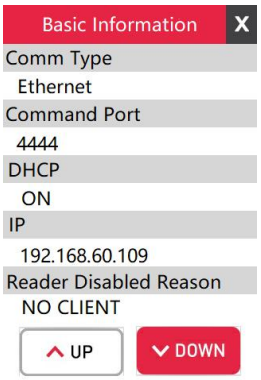
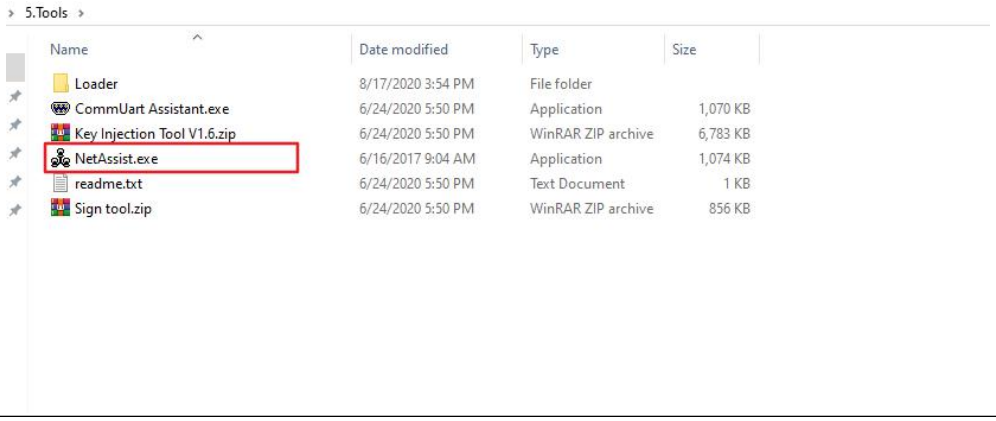
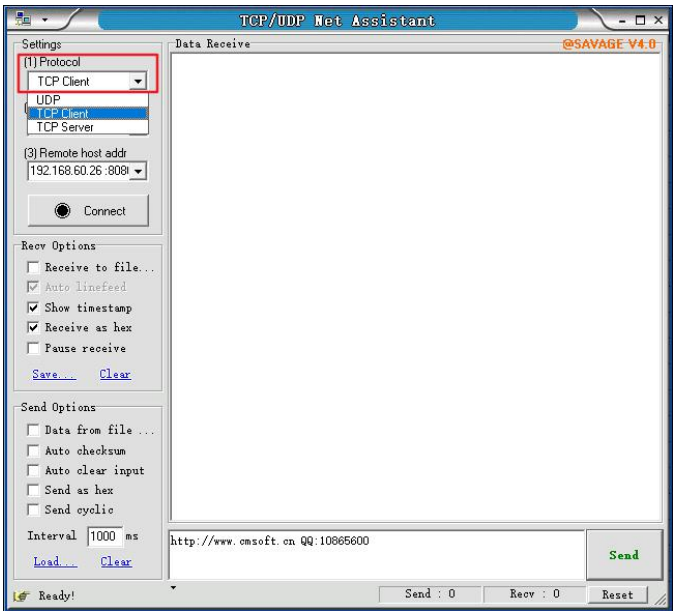
	Send button, and then the command will be sent to your terminal through this debugging tool 

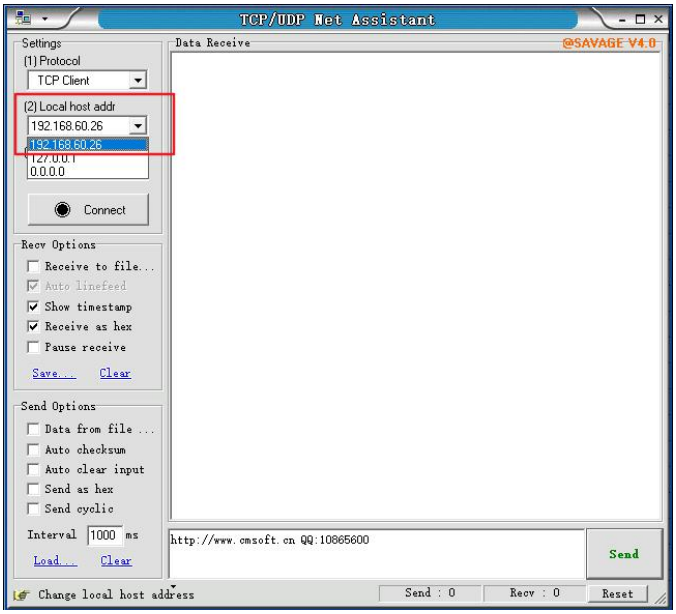
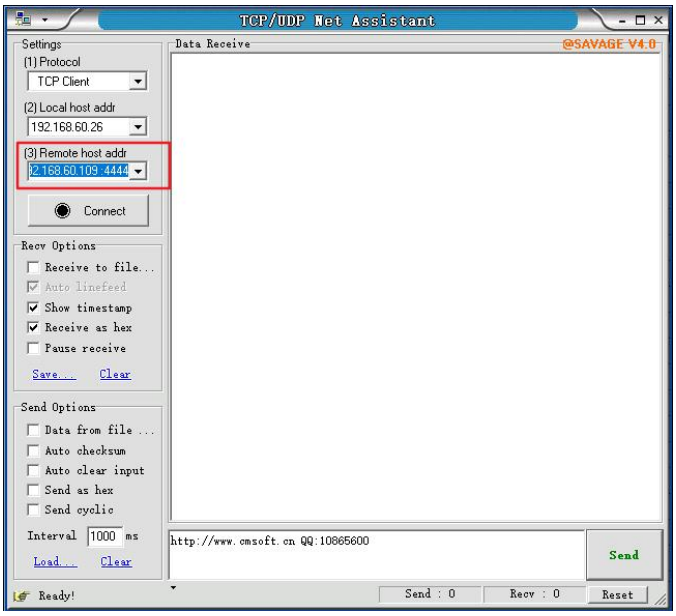
9.4.4. Configure Ethernet

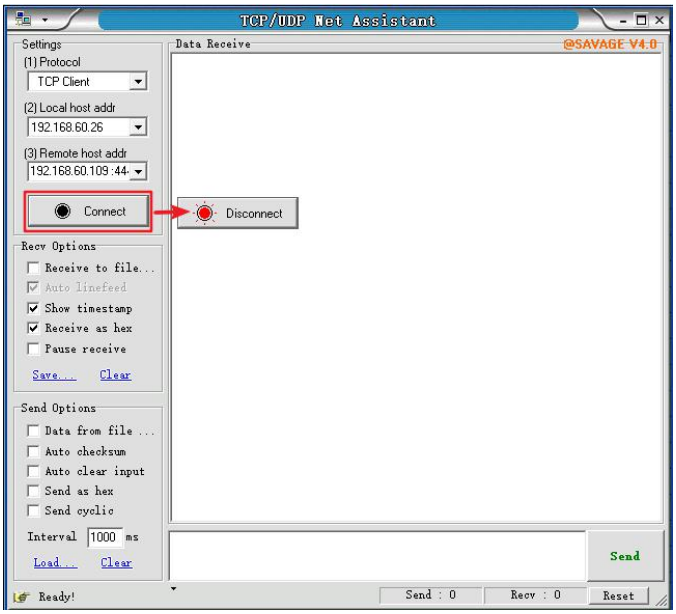
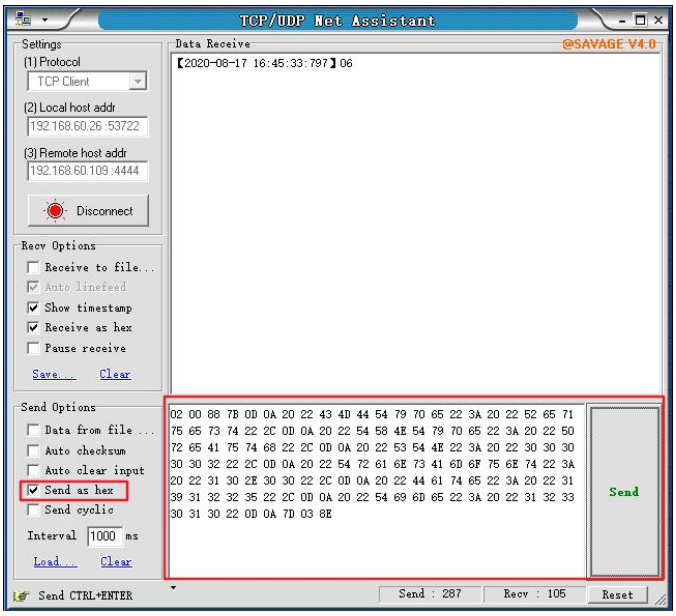
- ❖ Use the chart below to configure related Ethernet settings on the PC side. Please refer to your own kiosk specification for the specific steps may be based on kiosk machine.

- ➢ On the PC side, you need to use one debugging tool to simulate the kiosk machine. We use the "TCP/UDP Net Assistant" tool, which can be found in the "5.Tools" folder of the release package.

Step	Action & Display
1.	Make sure that the command communication type of the terminal you are working with is Ethernet. If not, please follow the steps in "Communication Switch" to switch it.
2.	Confirm that the Ethernet for wire access is properly installed in the correct port of the terminal, please refer to the section "INSTALLATION INSTRUCTIONS" for details
3.	Confirm that the Ethernet for wire access is properly installed in the correct port of the PC side (kiosk machine) Note: Make sure the terminal and PC are in the same network.
4.	Confirm the configuration of Ethernet on the terminal：IP and Command Port ■ Do not restart the terminal, you can check the Ethernet information in Service Mode menu. For detailed instructions of how to check Basic Information, please refer to the section "Basic Information" ■ Restart the terminal, you can check the Ethernet information during the initialization Check in Basic Information　　Check in initialization

<table>
<tr><td></td><td> 
</td><td> 
</td></tr>
<tr><td>5.</td><td>On the PC side, open the “TCP/UDP Net Assistant” tool

</td></tr>
<tr><td>6.</td><td>Select “TCP Client” in the Protocol drop-down box

</td></tr>
<tr><td>7.</td><td>Select the correct IP address in the Local host addr drop-down box
Note: If you do not confirm the Local IP address, please open the Network & Internet settings to view your network properties on your personal computer.</td></tr>
</table>

	
8.	Fill in the Remote host addr according to the information shown in Step6 Note: The format of remote host address should be “IP:Port” 
9.	Click the Connect button

	
10.	Tick the Send as hex box, input the command, click the Send button, and then the command will be sent to your terminal through this debugging tool 

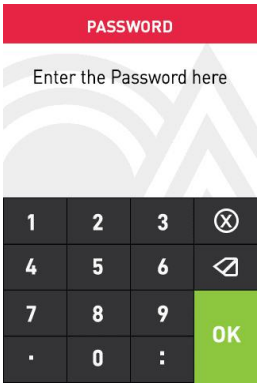
10. TERMINAL FEATURES - SERVICE MODE MENU

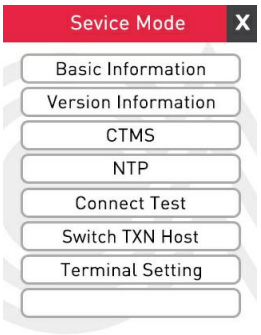
❖ The terminal offers the Service Mode menu for the installation personnel to view the basic information, update basic settings and perform basic diagnosis of the terminal. The following section provides feature explanations and steps for that. And the basic terminal features outlined in this section are the following:

- Basic Information
- Version Information
- CTMS Menu
- NTP Check
- Connect Test
- Switch TXN Host
- Terminal Setting
- GPRS APN Setting
- Ethernet Setting
- Bluetooth

10.1. How to trigger Service Mode menu

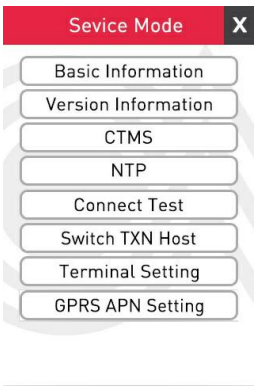
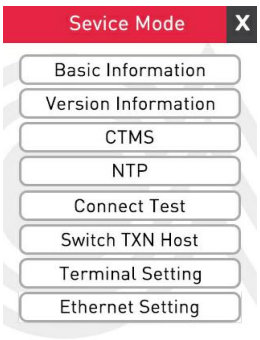
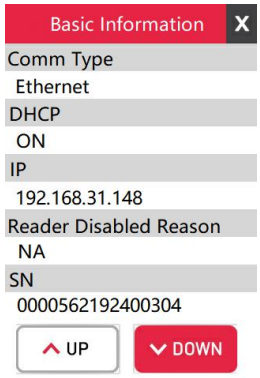
❖ Use the chart below to process trigger the Service Mode menu, the default password is 1 2 3 4.

Step	Action	Display
1.	Touch the status bar on the screen 5 times or more to access the Service Mode menu Note: Touching the positions in the yellow box of the display picture is effective.	
2.	Input the password if prompted and press OK (you have three times to enter the password)	

3.	Terminal displays the Service Mode menu	

10.2. Basic Information

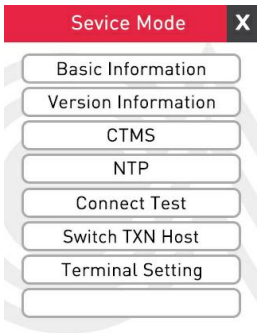
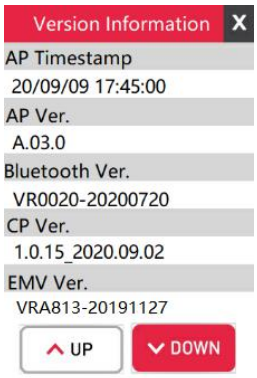
- ❖ Use the chart below to view the basic information of the terminal with unattended application: Comm Type, SN, Time, Time Zone, Reader Disabled Reason, etc.
- ➢ The Comm Type displayed in the basic information is the current communication method used by the terminal. The Reader Disabled Reason displayed is the reason why the terminal is in reader disabled state currently, it is for check quickly.

Step	Action	Display	
		GPRS Comm	Ethernet Comm
1.	Access the Service Mode menu from idle mode		
2.	Using your fingertip tap the word “Basic Information”		
3.	Press X icon or wait until timeout to exit this page		

	Terminal returns to the Service Mode menu

10.3. Version Information

- ❖ Use the chart below to view the version information of the terminal with unattended application: AP Version, CP Version, EMV Version, EMVCL Version, FW Version, KNL Version, SoundPlayer Version, etc.
- ➢ The version information will be displayed according to whether the terminal supports and the application supports. For example, Bluetooth version will be displayed on the UPT1000F terminal but not on the VEGA3000P terminal.

Step	Action	Display
1.	Access the Service Mode menu from idle mode	
2.	Using your fingertip tap the word “Version Information”	
3.	Press DOWN button to the next page of Version Information	
4.	Press X icon or wait until timeout to exit this page	

	Terminal returns to the Service Mode menu

10.4. CTMS Menu

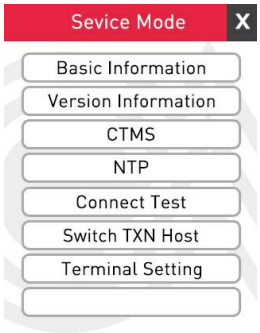
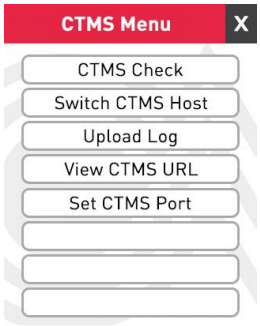
❖ In this menu, the terminal provides the basic settings and functions about CTMS. The CTMS features in this section are as follows:

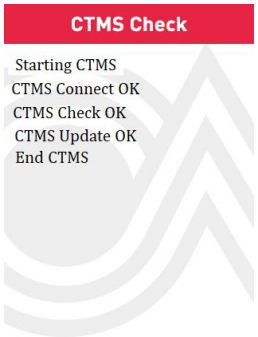
- CTMS Check
- Switch CTMS Host
- Set CTMS Port
- Upload Log
- View CTMS URL

10.4.1. CTMS Check

❖ Use the chart below to perform the function "CTMS Check", the terminal will connect to the CTMS server, attempt to get the trigger time, check for updates of application, firmware, patches, parameters, etc., and update locally if there is an update.

➢ If any update other than parameters is detected during the CTMS check process, the terminal will enter the Program Manager interface to download and update, and restart automatically after the update.

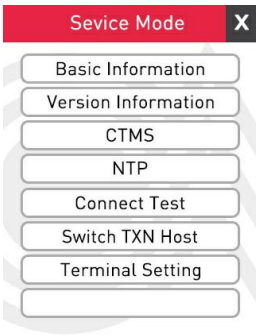
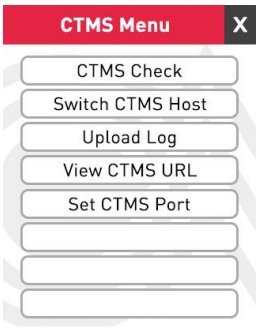
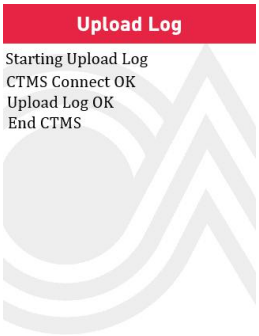
Step	Action	Display
1.	Access the Service Mode menu from idle mode	
2.	Using your fingertip tap the word "CTMS"	

3.	Press “CTMS Check” button, the terminal will prompt the user to confirm the operation If the operation times out or user presses NO button, the terminal will return to CTMS Menu	
4.	Press YES button, the terminal will perform CTMS Check If parameter updates are detected, the terminal will display “CTMS Update OK” after this process	**No Parameter Update**  **Parameter Update** 
5.	If any update other than parameters is detected, the terminal will display the prompt and start update. If no other updates are detected, the terminal will return to CTMS Menu	

10.4.2. Upload Log

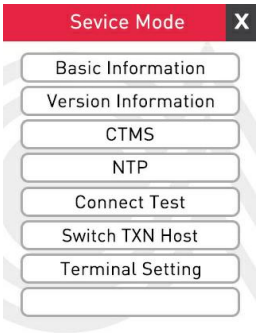
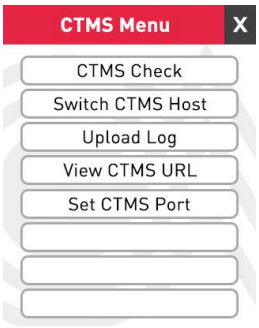
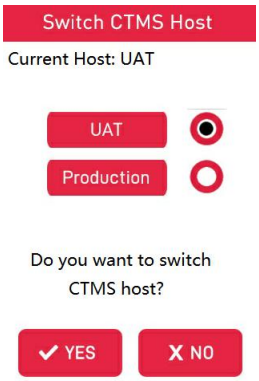
- ❖ Use the chart below to perform the function “Upload Log”, the terminal will connect to the CTMS server, and attempt to upload the log file to CTMS website.
- ➢ Press the button “Upload Log” is to upload the log file of that day. For detailed instructions of viewing log files on the CTMS website, please refer to the section “View Log File”.

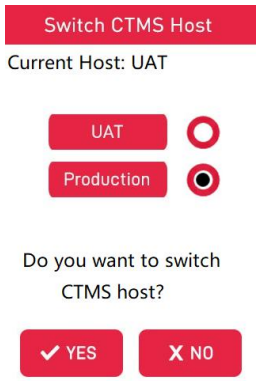
Step	Action	Display

1.	Access the Service Mode menu from idle mode	
2.	Using your fingertip tap the word “CTMS”	
3.	Press “Upload Log” button, the terminal will prompt the user to confirm the operation If the operation times out or user presses NO button, the terminal will return to CTMS Menu	
4.	Press YES button, the terminal will perform Upload Log If something goes wrong during this process, you may see the following messages: ● CTMS Connect Failed ● Upload Log Failed	
5.	Terminal returns to CTMS Menu	

10.4.3. Switch CTMS Host

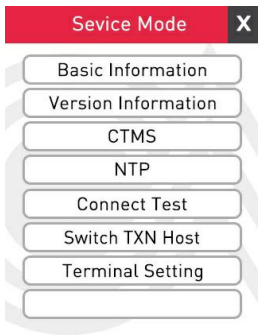
- ❖ Use the chart below to switch the CTMS host, the terminal will attempt to switch it according to your selection. In general, the terminal will provide two selections: UAT and PRD.
- ➢ UAT refers to the user acceptance test environment of CTMS, which is generally used in the developing, testing and trial operation; PRD refers to the production environment of CTMS, which will be used by the terminals put into the market.

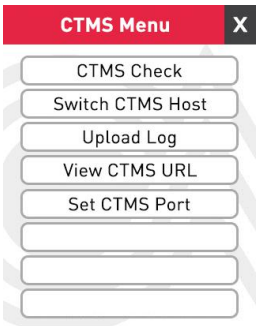
Step	Action	Display
1.	Access the Service Mode menu from idle mode	
2.	Using your fingertip tap the word “CTMS”	
3.	Press “Switch CTMS Host” button, terminal will display the current host and provide the options for switching: ● UAT ● Production	

4.	Press the option you want to switch to, the terminal will refresh the screen If the operation times out or user presses NO button, the terminal will do not change the CTMS Host and return to CTMS Menu	
5.	Press YES button, the terminal will flash the switching result If something goes wrong during the switch, you may see the message: ● Switch Host Failed	
6.	Terminal returns to CTMS Menu	

10.4.4. View CTMS URL

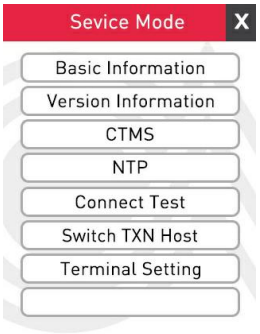
❖ Use the chart below to view CTMS URL, the terminal will display the details of CTMS Host Address.

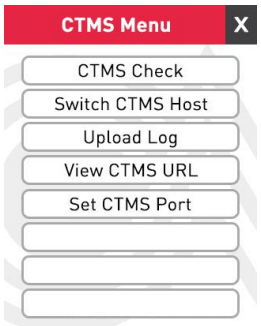
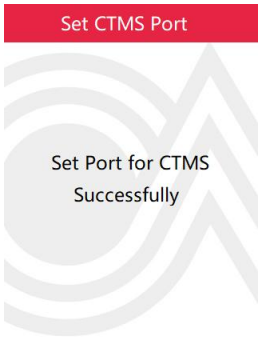
Step	Action	Display
1.	Access the Service Mode menu from idle mode	

2.	Using your fingertip tap the word “CTMS”	
3.	Press “View CTMS URL” button, the terminal will display the details of CTMS host address	
4.	Press EXIT button or wait until timeout to exit this page Terminal returns to CTMS Menu	

10.4.5. Set CTMS Port

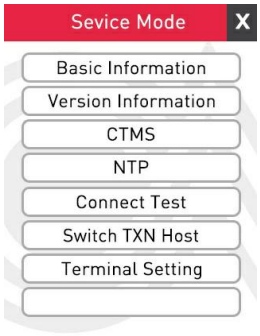
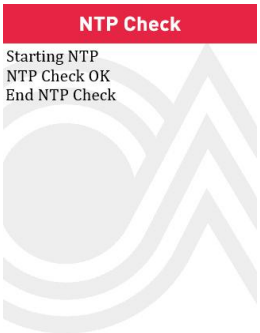
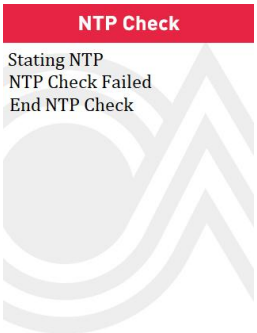
❖ Use the chart below to set the CTMS port, the terminal will display the current CTMS port and provide the keyboard for changing the port value.

Step	Action	Display
1.	Access the Service Mode menu from idle mode	

2.	Using your fingertip tap the word “CTMS”	
3.	Press “Set CTMS Port” button, the terminal will display the current CTMS port and provide the keyboard for changing the port value If the operation times out or user presses X key, the terminal will return to CTMS Menu	
4.	Input the port and press OK to set it Note: The maximum number of digits for the port value is 5	
5.	Terminal flashes the result of setting	
6.	Terminal returns to CTMS Menu	

10.5. NTP Check

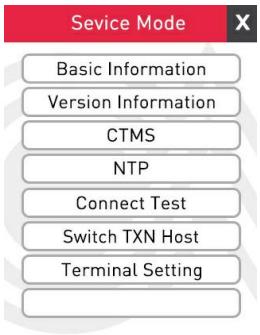
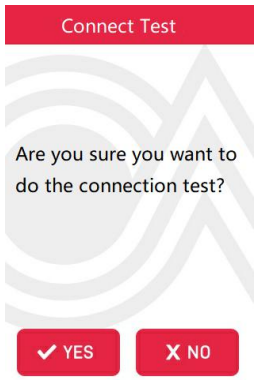
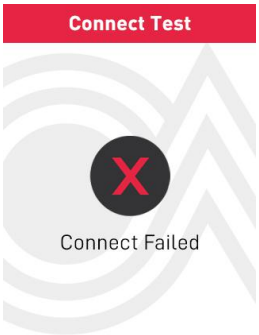
❖ Use the chart below to check NTP, the terminal will accurately calibrate the RTC (Real Time Clock) according to the current NTP URL and Time Zone.

Step	Action	Display
1.	Access the Service Mode menu from idle mode	
2.	Using your fingertip tap the word "NTP", the terminal will display the current NTP URL and provide the selection for checking NTP If the operation times out or user presses NO button, the terminal will return to Service Mode menu	
3.	Press YES button, the terminal will perform NTP Check	Check OK:  Check Failed: 
4.	Terminal returns to CTMS Menu	

10.6. Connect Test

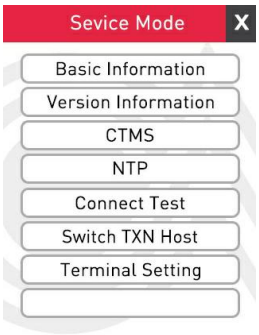
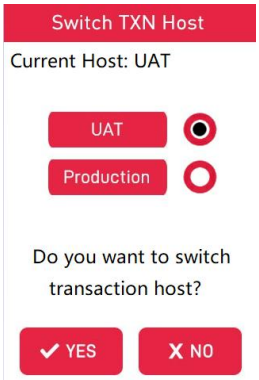
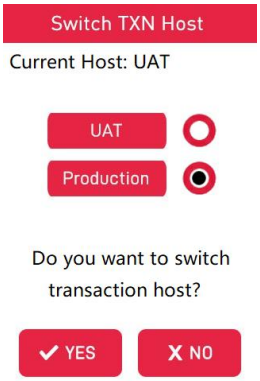
❖ Use the chart below to perform the function "Connect Test", the terminal will attempt communications with the payment gateway, and indicate success or failure on the screen.

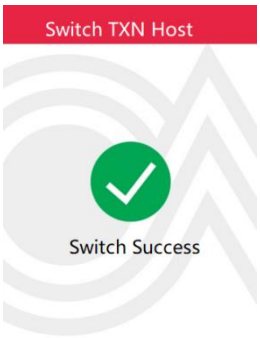
Step	Action	Display

1.	Access the Service Mode menu from idle mode	
2.	Using your fingertip tap the word "Connect Test", the terminal will prompt the user to confirm the operation If the operation times out or user presses NO button, the terminal will return to Service Mode menu	
3.	Press YES button, the terminal will perform Connect Test	
4.	Terminal flashes the result of connection testing	Success:  Failure: 
5.	Terminal returns to Service Mode menu	

10.7. Switch TXN Host

- Use the chart below to set the host address of payment gateway, the terminal will attempt to switch it according to your selection. In general, the terminal will provide two selections: UAT and Production.
- UAT refers to the test host of payment gateway, which is generally used in the developing, testing and trial operation; Production refers to the production host of payment gateway, which will be used by the terminals put into the market.

Step	Action	Display
1.	Access the Service Mode menu from idle mode	
2.	Using your fingertip tap the word "Switch TXN Host", the terminal will display the current host and provide the options for switching: ● UAT ● Production	
3.	Press the option you want to switch to, the terminal will refresh the screen If the operation times out or user presses NO button, the terminal will do not change the TXN Host and return to Service Mode menu	

4.	Press YES button, the terminal will flash the switching result If something goes wrong during the switch, you may see the message: ● Switch Failed	
5.	Terminal returns to Service Mode menu	

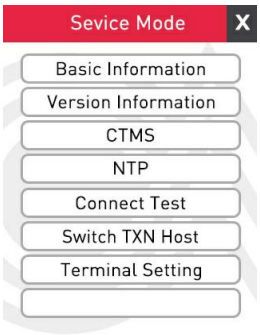
10.8. Terminal Setting

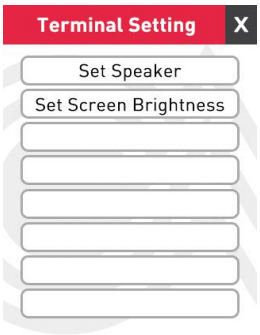
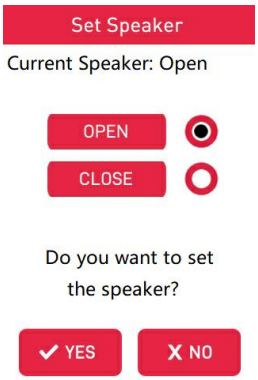
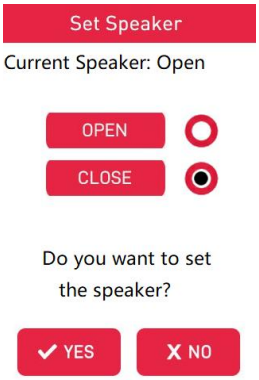
❖ In this menu, the terminal provides the two local settings of the terminal: Set Speaker and Set Screen Brightness.

10.8.1. Set Speaker

❖ Use the chart below to turn on or off the speaker of terminal.

➢ The speaker setting is on by default and the terminal will say something to indicate the user during the transaction, such as "Please remove your card" to indicate user to remove the card. This setting is permanent to the terminal and will not be changed after restart, application update, firmware update, or any other updates.

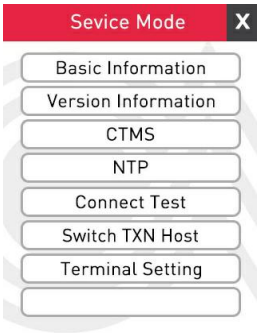
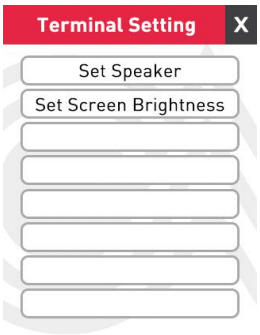
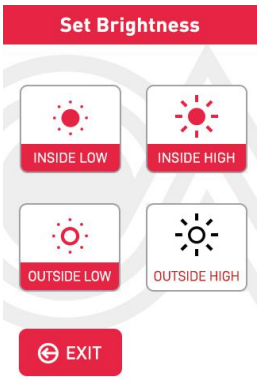
Step	Action	Display
1.	Access the Service Mode menu from idle mode	

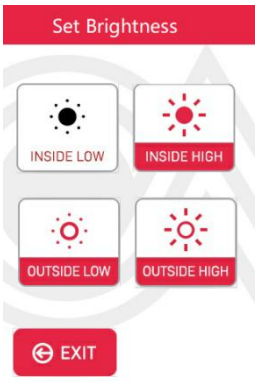
2.	Using your fingertip tap the word “Terminal Setting” If the operation times out or user presses X icon, the terminal will return to Service Mode menu	
3.	Press “Set Speaker” button, the terminal will display the current speaker status and provide the options for setting: ● OPEN ● CLOSE	
4.	Press the option you want to set to, the terminal will refresh the screen If the operation times out or user presses NO button, the terminal will do not change the speaker and return to Terminal Setting menu	
5.	Press YES button, the terminal will flash the setting result	
6.	Terminal returns to Terminal Setting menu	

10.8.2. Set Screen Brightness

❖ Use the chart below to set the screen brightness of terminal. The terminal will provide four selections according to different installation environments: Inside Low, Inside High, Outside Low, Outside High.

➢ The screen brightness setting is “Outside High” by default and the terminal will update the screen brightness in time when you change the option. Same as the speaker, this setting also is permanent to the terminal and will not be changed after restart, application update, firmware update, or any other updates.

Step	Action	Display
1.	Access the Service Mode menu from idle mode	
2.	Using your fingertip tap the word “Terminal Setting” If the operation times out or user presses X icon, the terminal will return to Service Mode menu	
3.	Press “Set Screen Brightness” button, the terminal will display the current brightness status and provide the options for setting: ● INSIDE LOW ● INSIDE HIGH ● OUTSIDE LOW ● OUTSIDE HIGH	

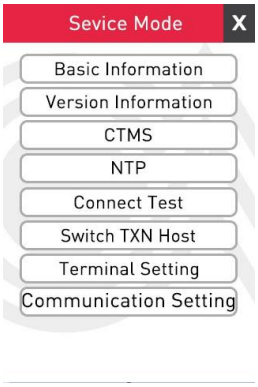
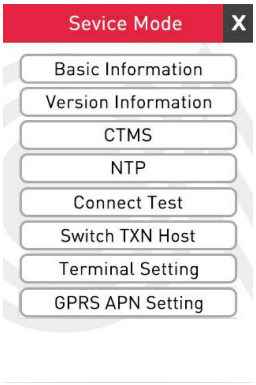
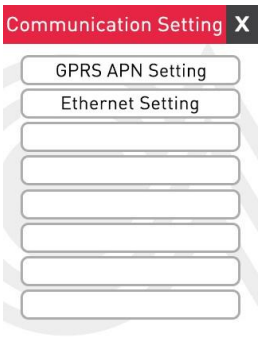
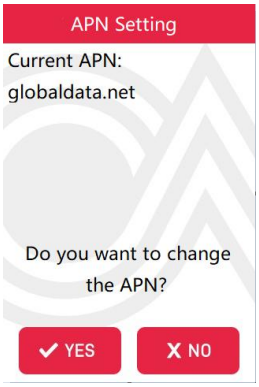
4.	Press the option you want to set to, the terminal will refresh the screen and change the brightness in real time	
5.	Press EXIT button or wait until timeout to exit, the terminal will save the current setting	
6.	Terminal flashes the result of saving and returns to Terminal Setting menu	

10.9. GPRS APN Setting

- ❖ When the host communication type of the terminal is GPRS, the button "GPRS APN Setting" will appear on Service Mode menu. In this menu, you can change the GPRS settings:
  - ■ Set APN (GPRS)
  - ■ Set APN UserName
  - ■ Set APN Password
- ➢ As long as the APN setting is changed, the terminal will perform communication check when returning to idle mode. Please refer to the section "COMM Check - AUTO" for detailed instructions.

10.9.1. Set APN (GPRS)

❖ Use the chart below to set the APN value of terminal.

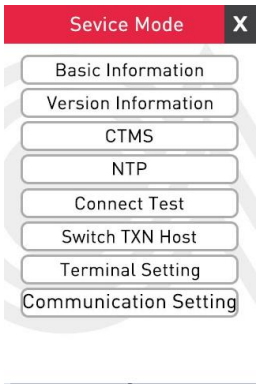
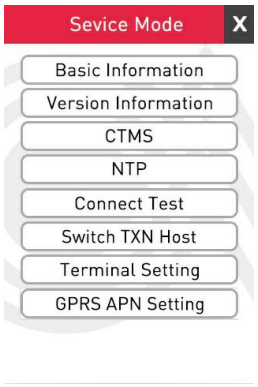
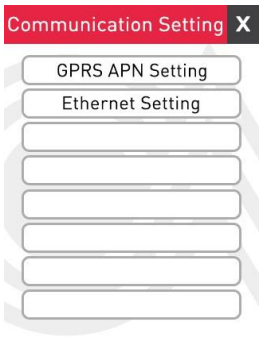
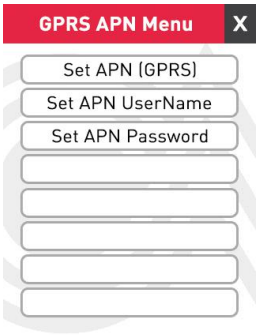
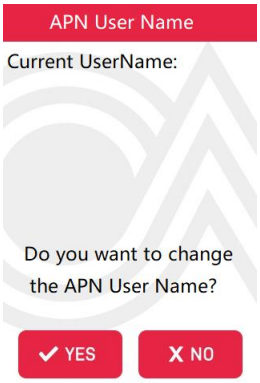
Step	Action	Display	
		CMD communication method is Ethernet	CMD communication method is not Ethernet
1.	Access the Service Mode menu from idle mode		
2.	Using your fingertip tap the word "Communication Setting"		/
3.	Using your fingertip tap the word "GPRS APN Setting" If the operation times out or user presses X icon, the terminal will return to the previous menu		
4.	Press "Set APN (GPRS)" button, the terminal will display the current APN and provide the selection for changing the APN. If the operation times out or user presses NO button, the terminal will return to GPRS APN Menu		

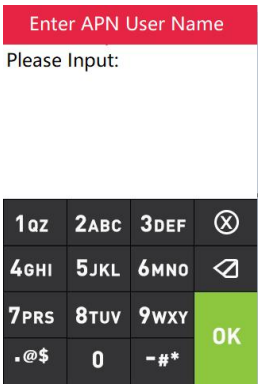
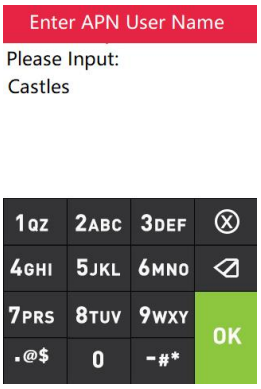
5.	Press YES button, the terminal will provide the keyboard for changing the APN value If the operation times out or user presses X key, the terminal will return to GPRS APN Menu	
6.	Input the APN and press OK to set it Note: This keyboard supports the input of (upper and lower case) letters, numbers, and related special characters. You can click the same key to change the input when the underlined of this has not disappeared.	 (the value in picture is an example)
7.	Terminal flashes the result of setting	
8.	Terminal returns to GPRS APN Menu	

10.9.2. Set APN UserName

❖ Use the chart below to set the APN UserName value of terminal.

Step	Action	Display	
1.	Access the Service Mode menu from idle mode	CMD communication method is Ethernet	CMD communication method is not Ethernet

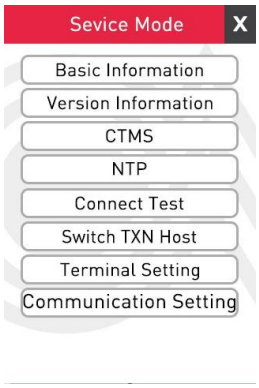
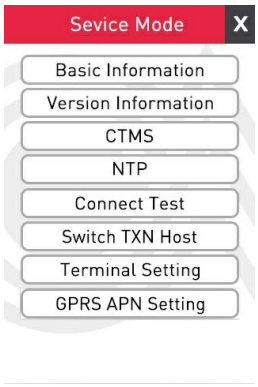
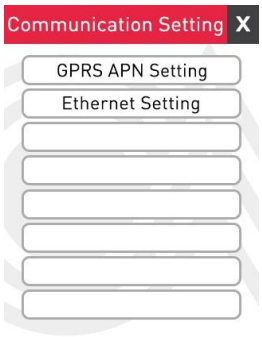
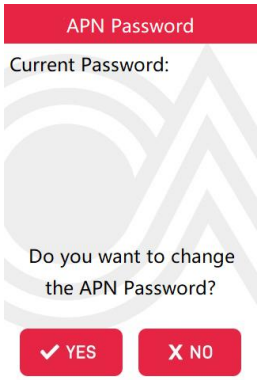
			
2.	Using your fingertip tap the word "Communication Setting"		/
3.	Using your fingertip tap the word "GPRS APN Setting" If the operation times out or user presses X icon, the terminal will return to the previous menu		
4.	Press "Set APN UserName" button, the terminal will display the current APN UserName and provide the selection for changing it If the operation times out or user presses NO button, the terminal will return to GPRS APN Menu		

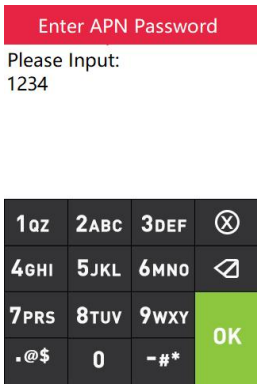
5.	Press YES button, the terminal will provide the keyboard for changing the APN UserName value If the operation times out or user presses X key, the terminal will return to GPRS APN Menu	
6.	Input the APN UserName and press OK to set it	 (the value in picture is an example)
7.	Terminal flashes the result of setting	
8.	Terminal returns to GPRS APN Menu	

10.9.3. Set APN Password

❖ Use the chart below to set the APN Password value of terminal.

Step	Action	Display	
1.	Access the Service Mode menu from idle mode	CMD communication method is Ethernet	CMD communication method is not Ethernet

			
2.	Using your fingertip tap the word “Communication Setting”		/
3.	Using your fingertip tap the word “GPRS APN Setting” If the operation times out or user presses X icon, the terminal will return to the previous menu		
4.	Press “Set APN Password” button, the terminal will display the current APN Password and provide the selection for changing it If the operation times out or user presses NO button, the terminal will return to GPRS APN Menu		

5.	Press YES button, the terminal will provide the keyboard for changing the APN Password value If the operation times out or user presses X key, the terminal will return to GPRS APN Menu	
6.	Input the APN Password and press OK to set it	 (the value in picture is an example)
7.	Terminal flashes the result of setting	
8.	Terminal returns to GPRS APN Menu	

10.10. Ethernet Setting

❖ When the host communication type or the command communication type of the terminal is Ethernet, the button "Ethernet Setting" will appear on Service Mode menu. In this menu, you can change the Ethernet settings:

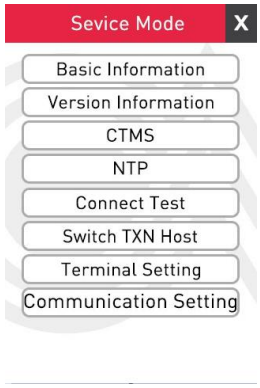
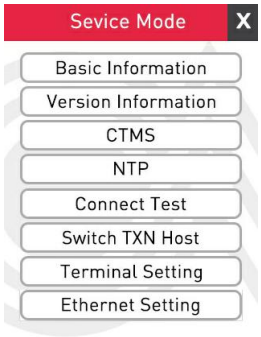
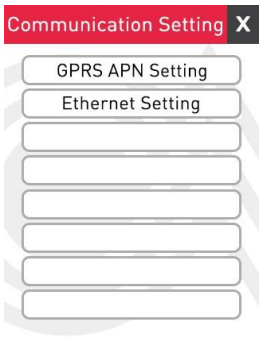
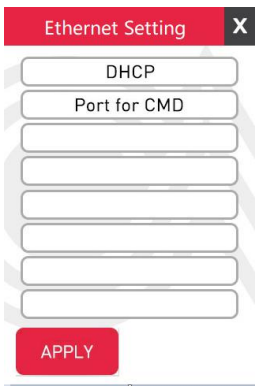
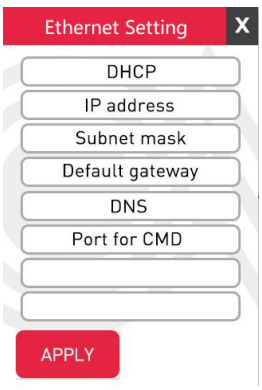
- DHCP
- IP address
- Subnet mask
- Default gateway
- DNS
- Port for CMD

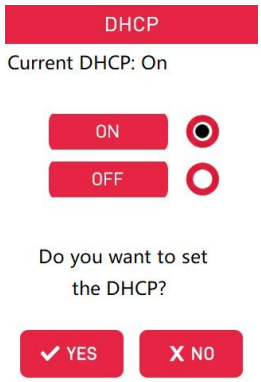
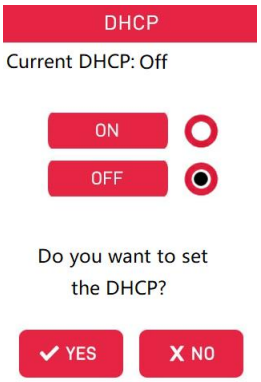
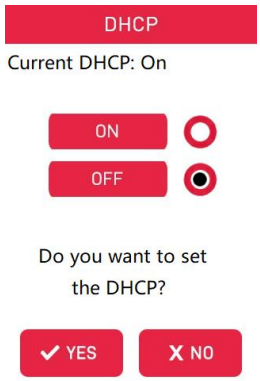
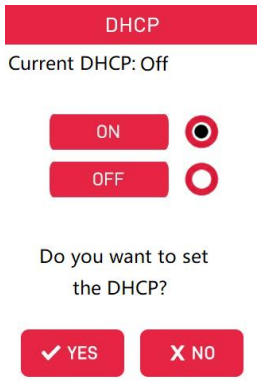
➢ The options "IP address", "Subnet mask", "Default gateway" and "DNS" will only appear when the setting "DHCP" of the terminal is turned off. And the option "Port for CMD" will only appear when the command type is Ethernet.

No matter what settings are changed, you need to confirm again and apply them, otherwise the changes will be invalid. See the section “Apply Settings” for the details.

10.10.1.DHCP

❖ Use the chart below to enable or disable a DHCP server to automatically assign an IP address and other information to the terminal.

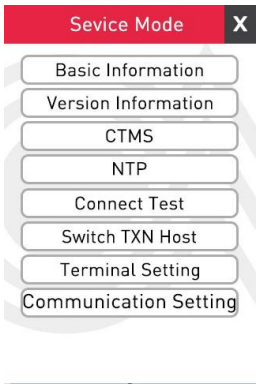
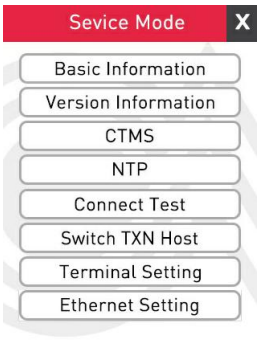
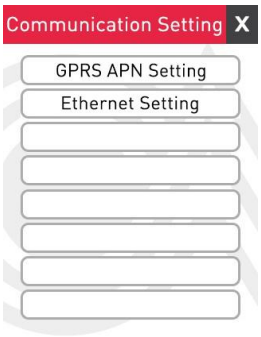
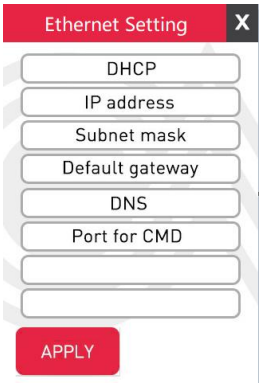
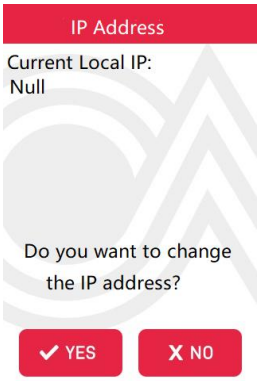
Step	Action	Display	
		Host communication method is GPRS	Host communication method is not GPRS
1.	Access the Service Mode menu from idle mode		
2	Using your fingertip tap the word “Communication Setting”		/
3.	Using your fingertip tap the word “Ethernet Setting” If the operation times out or user presses X icon, the terminal will return to the previous menu	DHCP ON	DHCP OFF
			

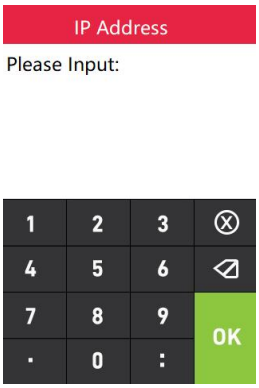
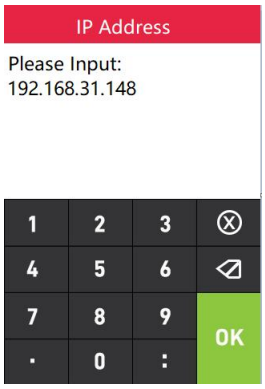
4.	Press “DHCP” button, the terminal will display the current DHCP status and provide the options for setting		
5.	Press the option you want to set to, the terminal will refresh the screen If the operation times out or user presses NO button, the terminal will do not change the DHCP and return to Ethernet Setting menu		
6.	Press YES button, the terminal will flash the setting result		
7.	Terminal returns to Ethernet Setting menu		

10.10.2.IP Address

❖ Use the chart below to set the IP address of Ethernet for the terminal.

Step	Action	Display	
1.	Access the Service Mode menu from idle mode	Host communication method is GPRS	Host communication method is not GPRS

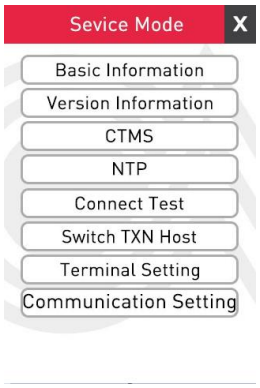
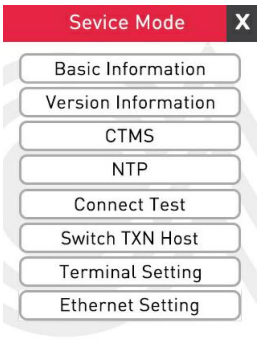
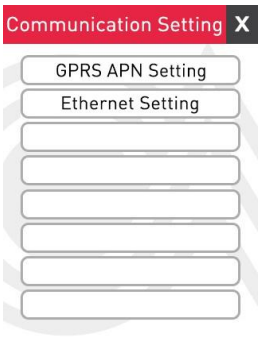
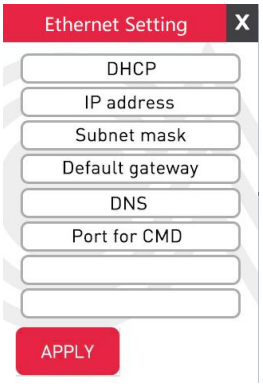
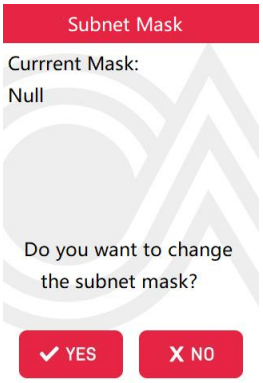
			
2.	Using your fingertip tap the word "Communication Setting"		/
3.	Using your fingertip tap the word "Ethernet Setting" If the operation times out or user presses X icon, the terminal will return to the previous menu	 (The menu appears when DHCP OFF)	
3.	Press "IP address" button, the terminal will display the current IP address value and provide the selection for changing the IP address If the operation times out or user presses NO button, the terminal will return to Ethernet Setting menu		

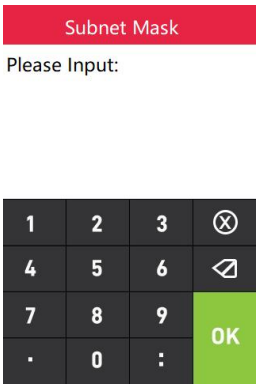
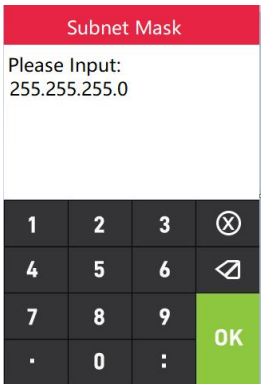
4.	Press YES button, the terminal will provide the keyboard for changing the IP address If the operation times out or user presses X key, the terminal will return to Ethernet Setting menu	
5.	Input the IP address and press OK to set it If something goes wrong during the setting, you may see the message: ● Input format error	 (the value in picture is an example)
6.	Terminal flashes the result of setting	
7.	Terminal returns to Ethernet Setting Menu	

10.10.3.Subnet Mask

❖ Use the chart below to set the Subnet mask of Ethernet for the terminal.

Step	Action	Display	
1.	Access the Service Mode menu from idle mode	Host communication method is GPRS	Host communication method is not GPRS

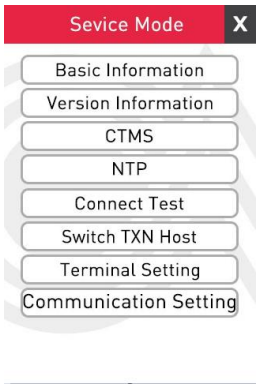
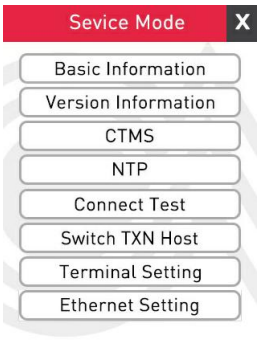
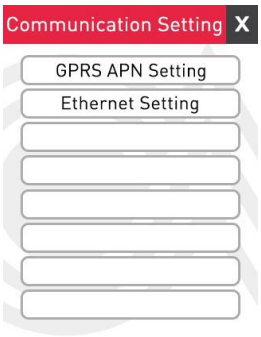
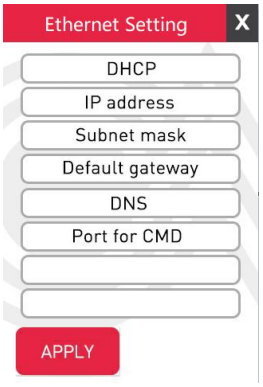
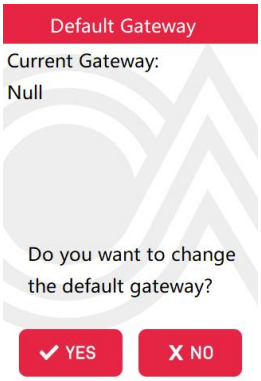
			
2.	Using your fingertip tap the word "Communication Setting"		/
3.	Using your fingertip tap the word "Ethernet Setting" If the operation times out or user presses X icon, the terminal will return to the previous menu	 (The menu appears when DHCP OFF)	
4.	Press "Subnet mask" button, the terminal will display the current subnet mask value and provide the selection for changing the subnet mask If the operation times out or user presses NO button, the terminal will return to Ethernet Setting menu		

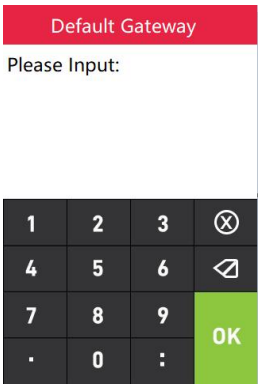
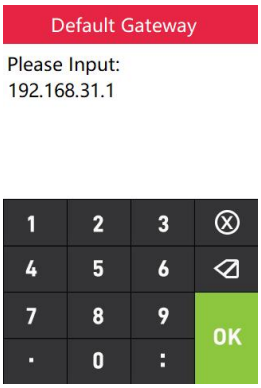
5.	Press YES button, the terminal will provide the keyboard for changing the subnet mask If the operation times out or user presses X key, the terminal will return to Ethernet Setting menu	
6.	Input the subnet mask and press OK to set it If something goes wrong during the setting, you may see the message: ● Input format error	 (the value in picture is an example)
7.	Terminal flashes the result of setting	
8.	Terminal returns to Ethernet Setting Menu	

10.10.4.Default Gateway

❖ Use the chart below to set the default gateway of Ethernet for the terminal.

Step	Action	Display	
1.	Access the Service Mode menu from idle mode	Host communication method is GPRS	Host communication method is not GPRS

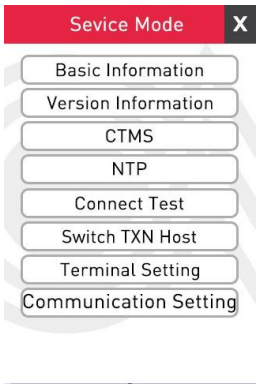
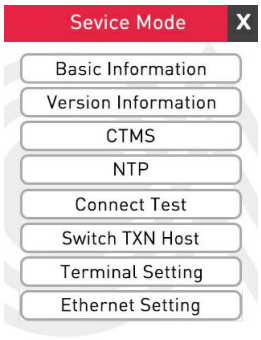
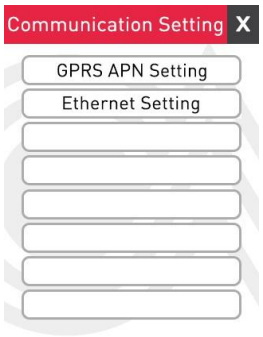
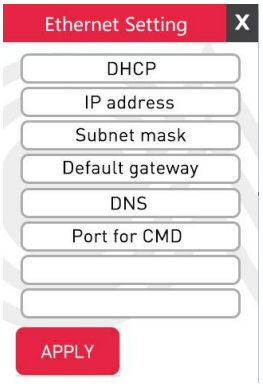
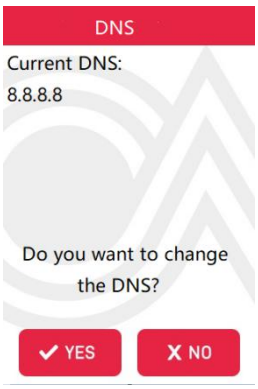
			
2.	Using your fingertip tap the word "Communication Setting"		/
3.	Using your fingertip tap the word "Ethernet Setting" If the operation times out or user presses X icon, the terminal will return to the previous menu	 (The menu appears when DHCP OFF)	
4.	Press "Default gateway" button, the terminal will display the current default gateway value and provide the selection for changing the default gateway If the operation times out or user presses NO button, the terminal will return to Ethernet Setting menu		

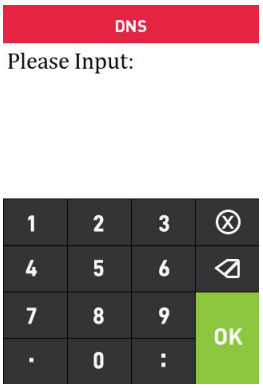
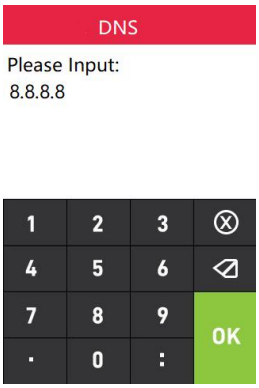
5.	Press YES button, the terminal will provide the keyboard for changing the default gateway If the operation times out or user presses X key, the terminal will return to Ethernet Setting menu	
6.	Input the default gateway and press OK to set it If something goes wrong during the setting, you may see the message: ● Input format error	 (the value in picture is an example)
7.	Terminal flashes the result of setting	
8.	Terminal returns to Ethernet Setting Menu	

10.10.5.DNS

❖ Use the chart below to set the DNS value of Ethernet for the terminal.

Step	Action	Display	
1.	Access the Service Mode menu from idle mode	Host communication method is GPRS	Host communication method is not GPRS

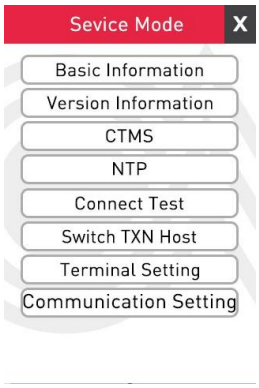
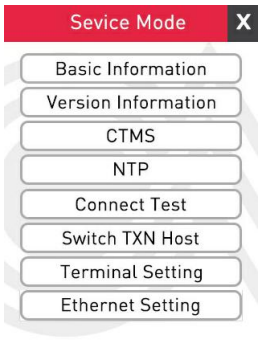
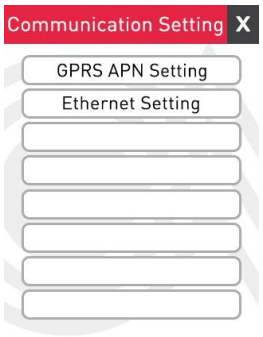
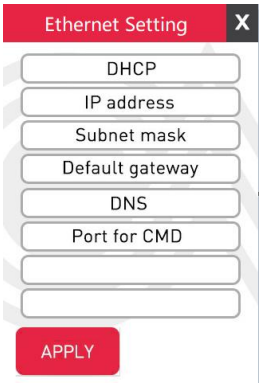
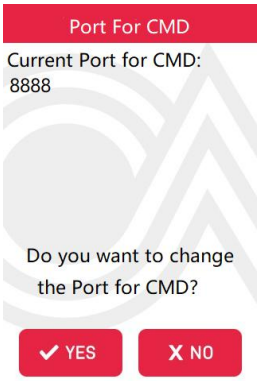
			
2.	Using your fingertip tap the word "Communication Setting"		/
3.	Using your fingertip tap the word "Ethernet Setting" If the operation times out or user presses X icon, the terminal will return to the previous menu	 (The menu appears when DHCP OFF)	
4.	Press "DNS" button, the terminal will display the current DNS value and provide the selection for changing the DNS If the operation times out or user presses NO button, the terminal will return to Ethernet Setting menu		

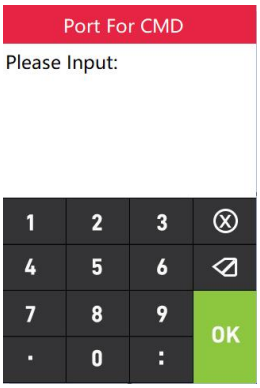
5.	Press YES button, the terminal will provide the keyboard for changing the DNS If the operation times out or user presses X key, the terminal will return to Ethernet Setting menu	
6.	Input the DNS and press OK to set it If something goes wrong during the setting, you may see the message: ● Input format error	 (the value in picture is an example)
7.	Terminal flashes the result of setting	
8.	Terminal returns to Ethernet Setting Menu	

10.10.6.Port for CMD

❖ Use the chart below to set the command port of Ethernet for the terminal.

Step	Action	Display	
1.	Access the Service Mode menu from idle mode	Host communication method is GPRS	Host communication method is not GPRS

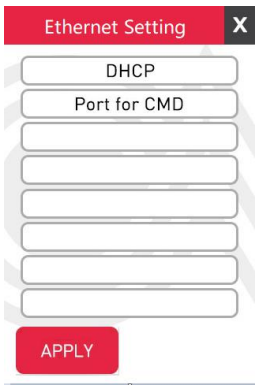
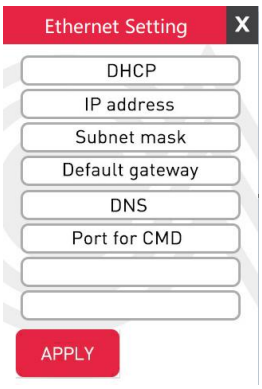
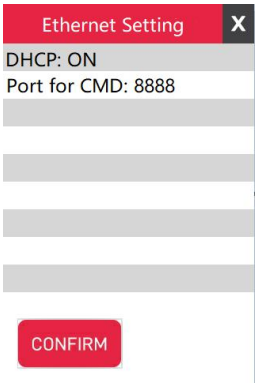
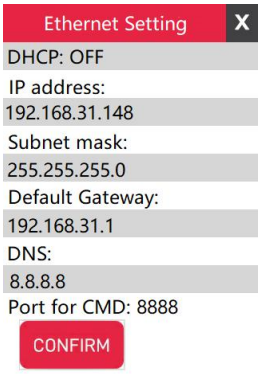
			
2.	Using your fingertip tap the word "Communication Setting"		/
3.	Using your fingertip tap the word "Ethernet Setting" If the operation times out or user presses X icon, the terminal will return to the previous menu	 (The menu appears when DHCP OFF)	
4.	Press "Port for CMD" button, the terminal will display the current command port value and provide the selection for changing the command port If the operation times out or user presses NO button, the terminal will return to Ethernet Setting menu		

5.	Press YES button, the terminal will provide the keyboard for changing the command port If the operation times out or user presses X key, the terminal will return to Ethernet Setting menu	
6.	Input the command port and press OK to set it If something goes wrong during the setting, you may see the message: ● Port for CMD 1024-65535	 (the value in picture is an example)
7.	Terminal flashes the result of setting	
8.	Terminal returns to Ethernet Setting Menu	

10.10.7.Apply Settings

❖ After finishing the above Ethernet settings, you need to confirm again and apply them. Use the chart below to apply Ethernet settings for the terminal.

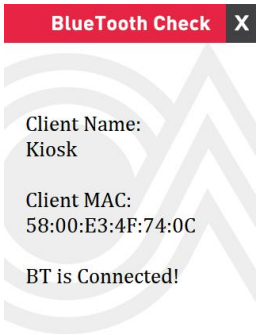
Step	Action	Display	
1.	Finish the all settings, terminal	DHCP ON	DHCP OFF

	returns to Ethernet Setting menu If the operation times out or user presses X icon, the terminal will return to previous menu and the settings changed by the user will not be applied		
2.	Press “APPLY” button, the terminal will display the current Ethernet settings changed by the user If the operation times out or user presses X icon, the terminal will return to Ethernet Setting menu and user can change the settings again		
3.	Press “CONFIRM” button, the settings will be applied		
4.	Terminal returns to the previous menu		

10.11. Bluetooth

- ❖ Use the chart below to check the current connection status of Bluetooth. If it is connected, it will display the connected device and mac address; if it is disconnected, it will display the device name and pairing key.
- ➢ When the command communication type of the terminal is Bluetooth, the button “Bluetooth” will appear on Service Mode menu. Otherwise, this button will not be shown.

Step	Action	Display

1.	Access the Service Mode menu from idle mode	
2.	Using your fingertip tap the word “Bluetooth”, the terminal will display the connection status of Bluetooth	Connected:  Disconnected: 
3.	Press X icon or wait until timeout to exit this page Terminal returns to the Service Mode menu	

11. TERMINAL FEATURES - AUTO TRIGGER

❖ The terminal automatically triggers some functions to remotely check the basic information, complete basic updates and perform basic diagnosis of the terminal. The basic terminal features explained in this section are the following:

- Comm Check - AUTO
- CTMS Check - AUTO
- Upload Log - AUTO
- NTP Check - AUTO

11.1. Comm Check - AUTO

❖ Communication check means the terminal will regularly check the communication status, attempt to communicate with the payment gateway, and indicate the result on the status bar. If it is unable to communicate with the payment gateway, the terminal will display "Reader Disabled" on the status bar, indicating that the transaction may fail at this time. Use the chart below to confirm the indication of this process.

Step	Action	Display
1.	Terminal is checking the connection	 (Cycle display)
2.	Terminal displays the result of	Comm Check Success Comm Check Failed

	communication check		

- Parameters: The interval of each communication check is 5 minutes by default and this value can be set through the parameter "Comm Check Interval". For the parameter definition, see in the annex configuration "Timer Config". And for detailed instructions of parameter update, please refer to the section "TERMINAL FEATURES – CONFIGURATION UPDATE".

11.2. CTMS Check - AUTO

- The automatic check of CTMS means that at the trigger time, the terminal will connect to the CTMS server, attempt to get the next trigger time, check for updates and update locally if there is an update. During the check process, you may see the following messages in the status bar:
  - CTMS IN SESSION
  - CTMS CHECK OK
  - CTMS CHECK FAILED
- Retry Logic: The terminal will attempt to get the first trigger time during the initialization. If it is not obtained, the terminal will attempt to get the trigger time after one hour, two hours and three hours, respectively. If it is still not obtained, the terminal will retry once a day until it is obtained. This logic is for each attempt when the trigger time is not obtained.

11.3. Upload Log - AUTO

- The automatic upload log means that at the trigger time, the terminal will connect to the CTMS server, and attempt to upload the log file of the previous day to CTMS website. During the upload process, you may see the message "UPLOAD LOG" in the status bar.
- Parameters: The trigger time of upload log is 2 o'clock every day by default. And the function can be disabled through the parameter "Is Upload Log Enable", the trigger time also can be set through the parameter "Upload log Time". For the parameter definitions, see in the annex configuration "CTMS

Config". And for detailed instructions of parameter update, please refer to the section "TERMINAL FEATURES - CONFIGURATION UPDATE".

11.4. NTP Check - AUTO

- ❖ The automatic check of NTP means that at the trigger time, the terminal will accurately calibrate the RTC according to the current NTP URL and Time Zone. During the check process, you may see the message "UPDATE NTP" in the status bar.
- ➢ Parameters: The trigger time of NTP check is 6 o'clock every day by default. And the function can be disabled through the parameter "Is NTP Enable", also the trigger time, check frequency, Time Zone, NTP URL can be set through other related parameters, please see in the annex configuration "NTP Server". For detailed instructions of parameter update, please refer to the section "TERMINAL FEATURES - CONFIGURATION UPDATE".

12. TERMINAL FEATURES - CONFIGURATION UPDATE

- The terminal supports some specific functions through CTMS and USB configuration. The following section provides feature explanations and steps for that.

12.1. CTMS Function

- CTMS is an easy and convenient tool for customers(users) to manage terminals. The content of management includes the role, user, terminals, groups, data file (e.g. parameter, private file, application, firmware), log and so on. The terminal with unattended application supports to get the log files, update applications, patches and firmware, update parameters and slide show through CTMS. The CTMS functions outlined in this section are the following:

  - Preparation on CTMS website
  - Update Parameters
  - Update Slide Show
  - Update AP, FW and Patches
  - View Log File

12.1.1. Preparation on CTMS website

- Before using the CTMS function, it is required to make some preparations on the CTMS website: import data files, import terminal, create group, etc. The data files related to the unattended application includes Configuration, Parameters, Private File, which could be usually found in the release package. Take the UAT CTMS website as an example, the preparation outlined in this section are the following:

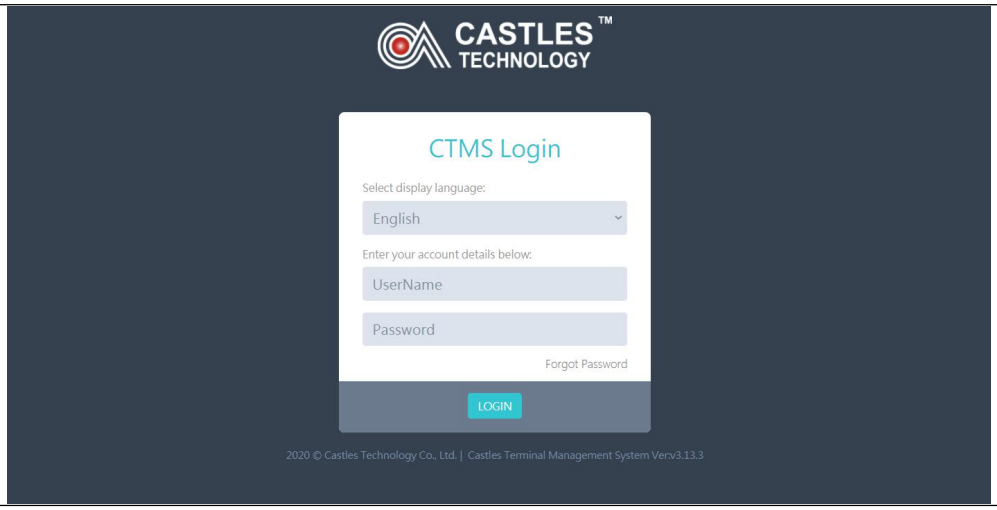
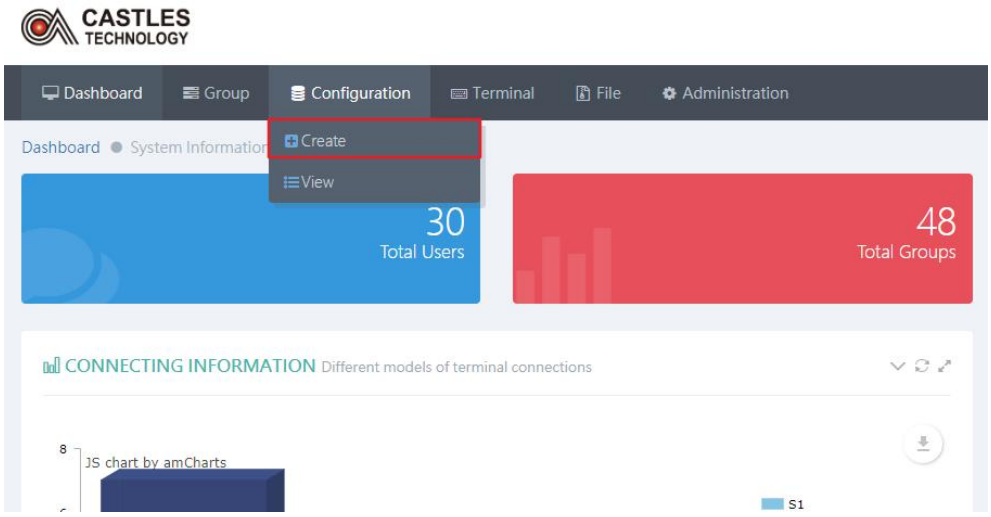
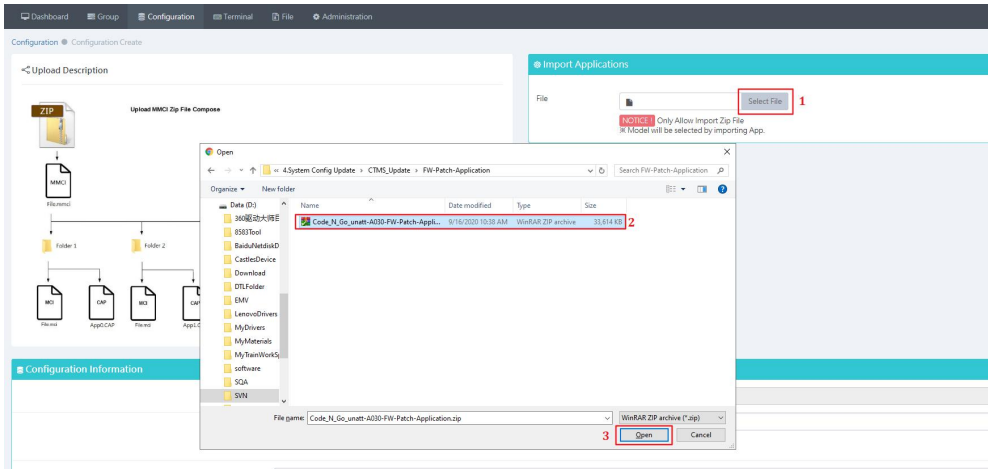
  - Import Configuration
  - Import Terminal
  - Import Parameter File
  - Create Group

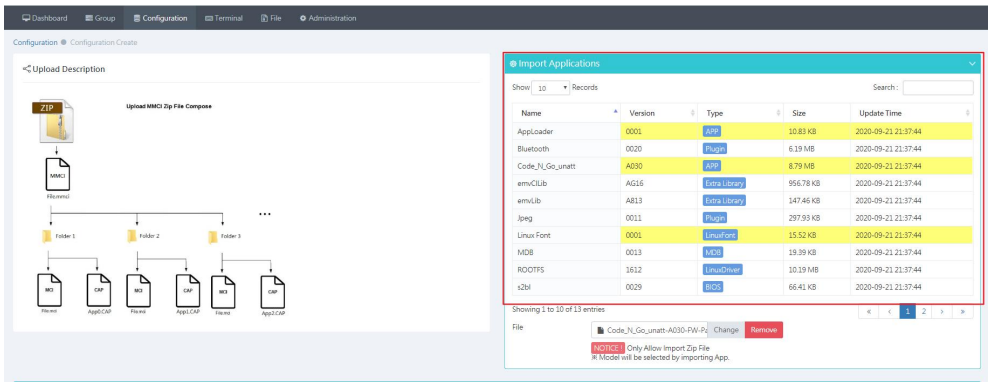
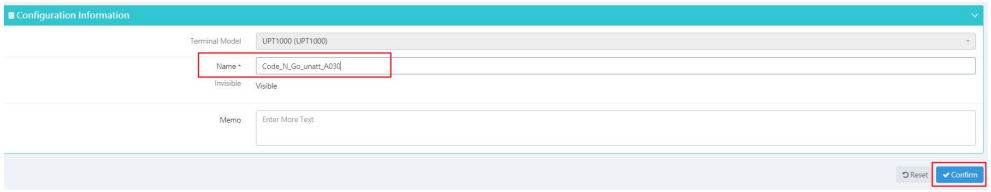
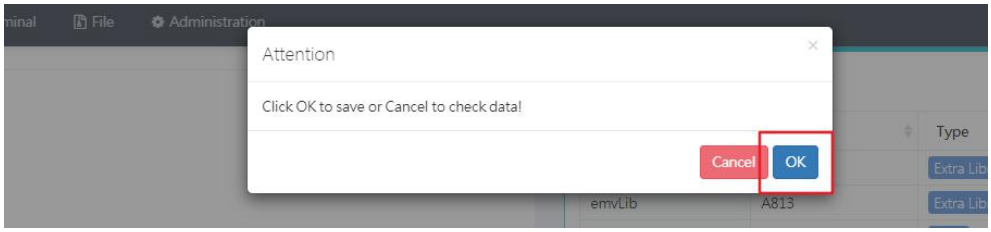
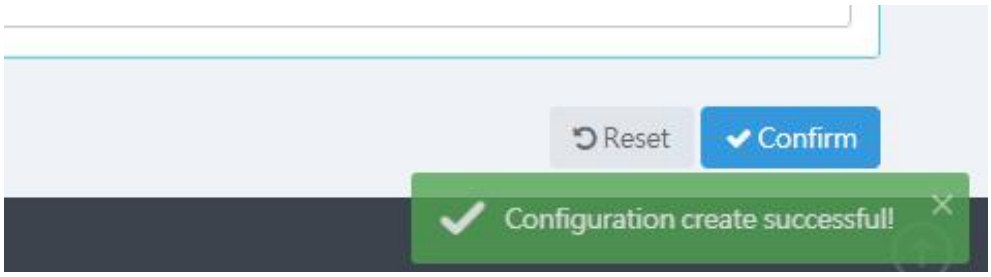
12.1.1.1. Import Configuration

- Configurations are the sets of firmware and applications. A configuration can be assigned to multiple groups, and a group can only hold one configuration. In general, configurations are used when the application, firmware or patches on the terminal need to be updated. Use the chart below to import configuration.

- For the unattended application, some configuration packages already are prepared in the release package which path is “package\4.System Config Update\CTMS_Update”. Typically, it is recommended to use the configuration package contains all files, which is placed in the folder “FW-Patch-Application”.

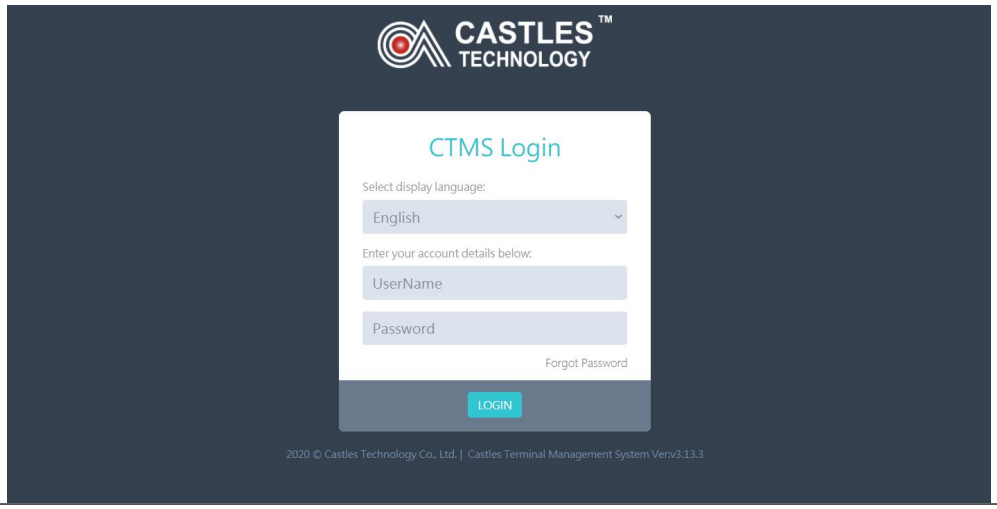
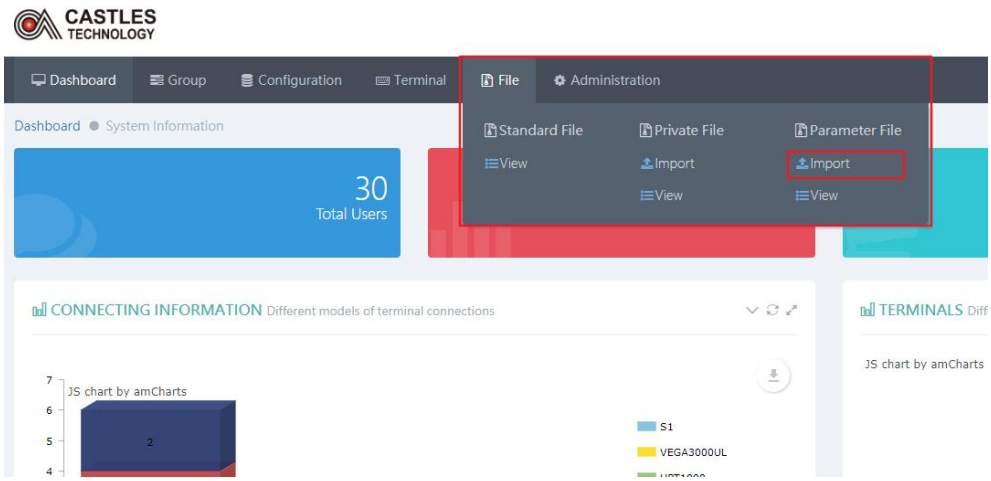
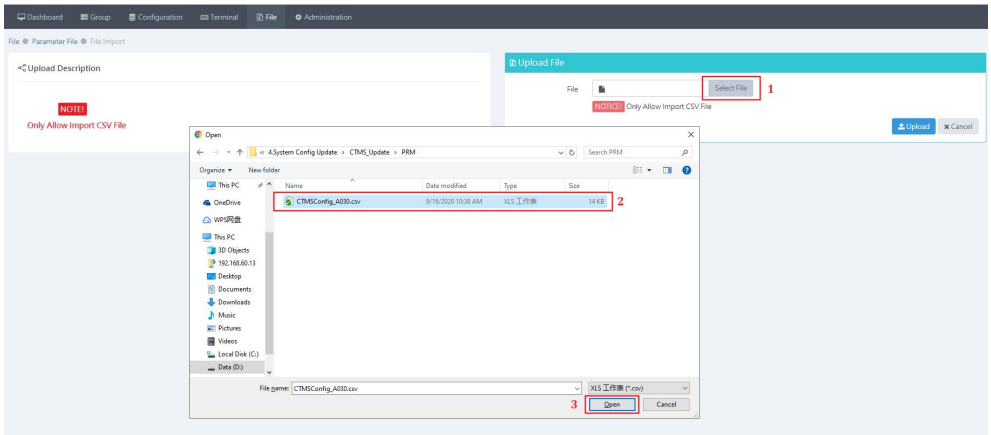
Step	Action & Display
1.	Login CTMS management system

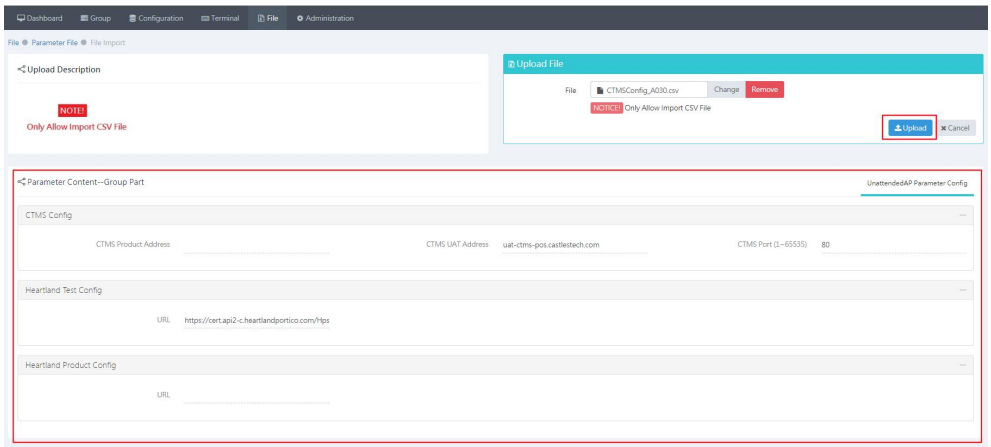
	
2.	Point to Configuration and click Create 
3.	Click Select File and select the ZIP file which you want to import 
4.	The file information will be displayed after imported, check whether the content is correct

	
5.	■ Scroll down to Configuration Info section and input information: Name, Memo ■ Click Confirm button 
6.	Click OK button when prompted for attention 
7.	After the import is completed, it will prompt “Configuration create successful” or other similar message in the lower right corner of the page 

12.1.1.2. Import Parameter File

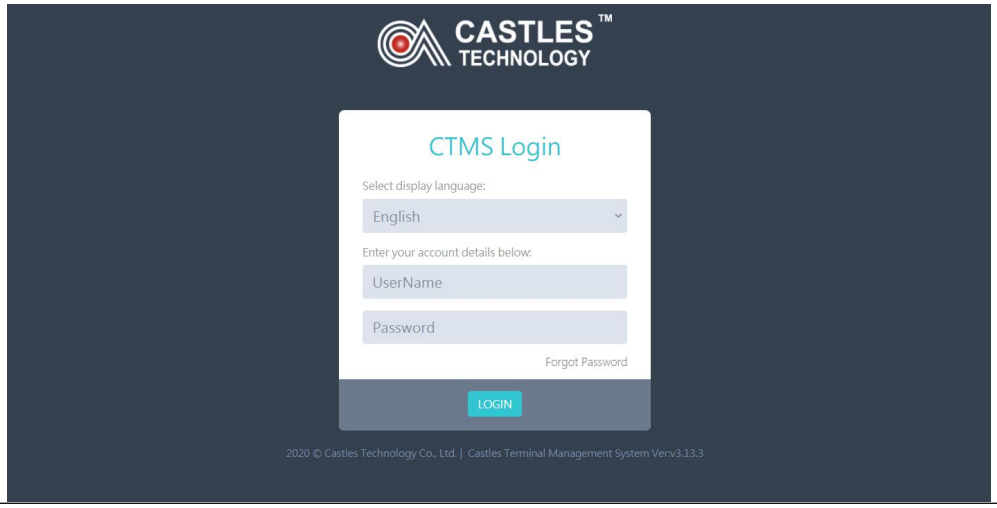
- ❖ Parameters are used to import into applications, the parameter file is attached for with the specific application. Putting the parameter mechanism into the design of the program could let the program become more flexible. Use the chart below to import parameter file.
- ❖ For the unattended application, the parameter file already is prepared in the release package which path is “package\4.System Config Update\CTMS_Update\PRM”.

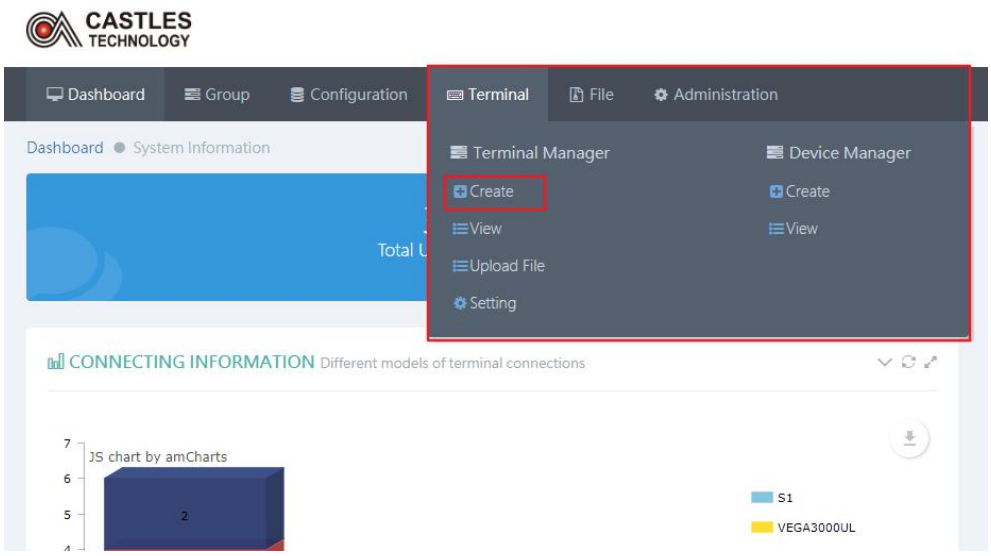
Step	Action & Display
1.	Login CTMS management system 
2.	Point to Parameter File and click File Import 
3.	Click Select File and select the CSV file which you want to import 
4.	■ The parameter content will be displayed after imported, check whether it is correct ■ Click Upload button

	
5.	After the import is completed, it will prompt "Parameter template file create successful" or other similar message in the lower right corner of the page 

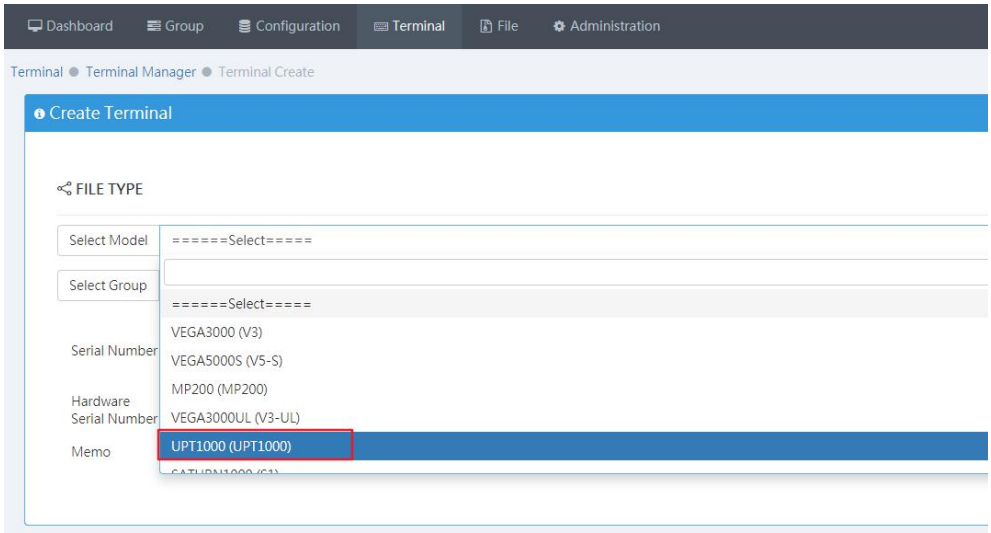
12.1.1.3. Import Terminal

❖ Using the CTMS function requires adding the terminal to CTMS website. Use the chart below to import terminals for unattended application.

Step	Action & Display
1.	Login CTMS management system 
2.	Point to Terminal and then click Create

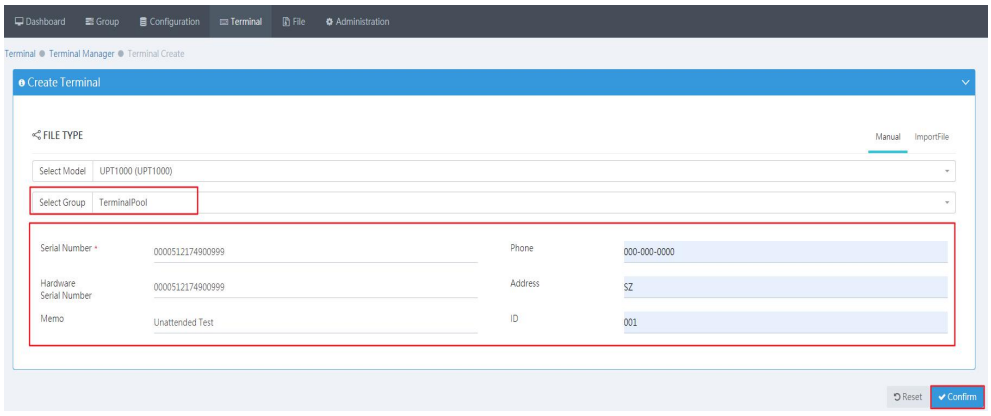


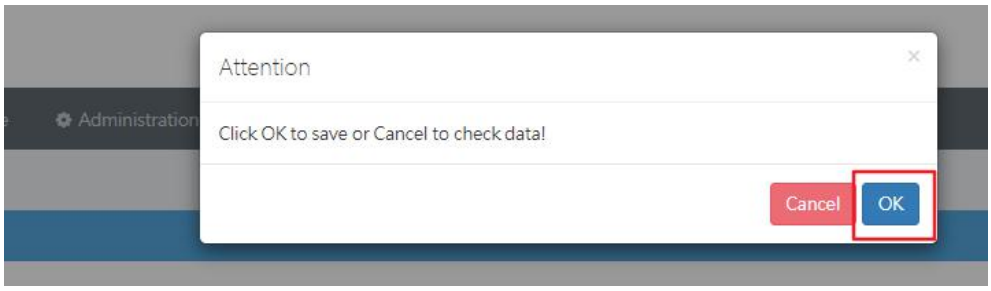
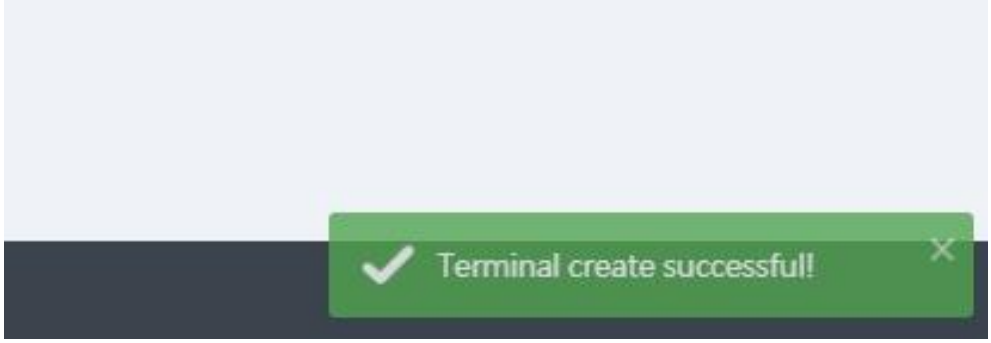
3. Select the Model according to the model of your terminal: UPT1000(UPT1000) or VEGA3000 (V3)



4.

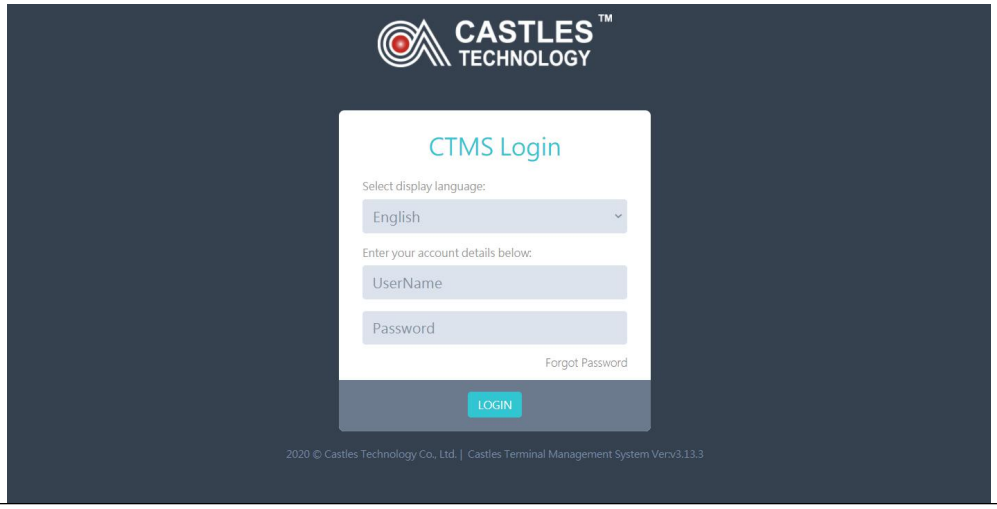
- Select Terminal Pool as the Group. If the group you want to add the terminal into has been created, select that group name
- Input terminal information: Serial Number, Hardware Serial Number, Memo, Phone, Address, ID
- Click Confirm button

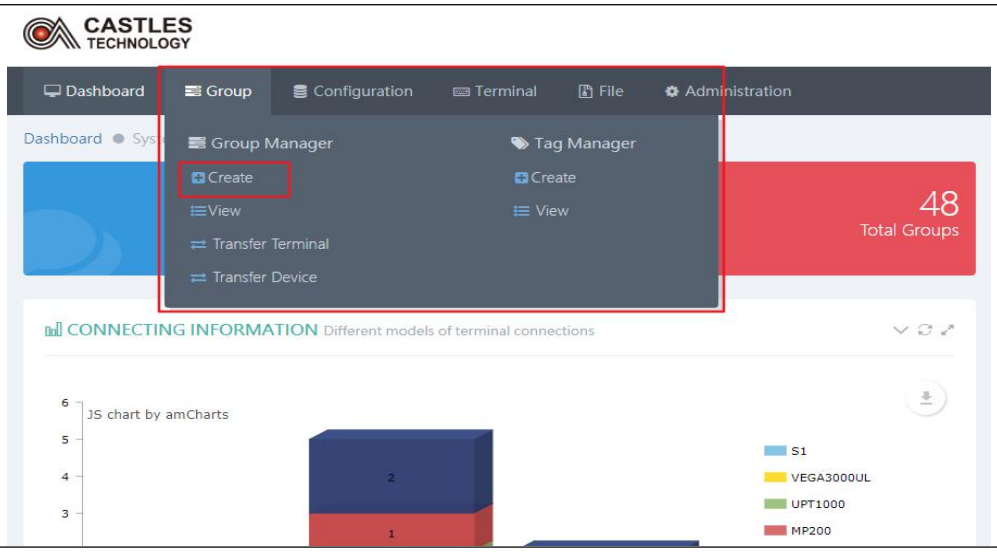
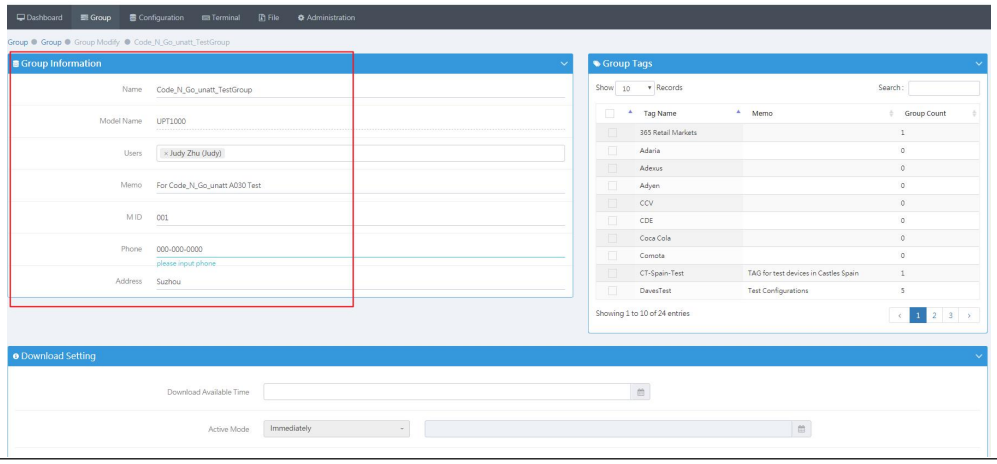
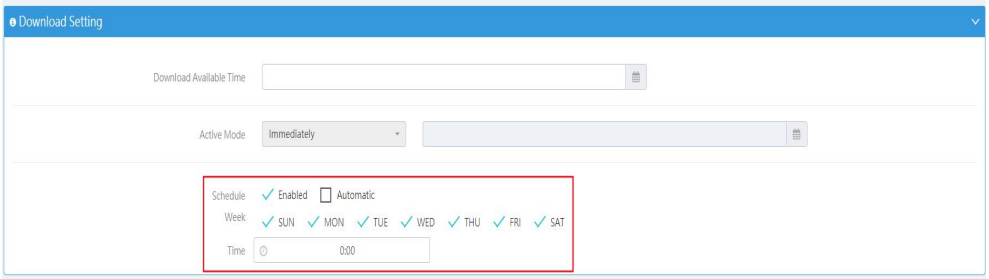


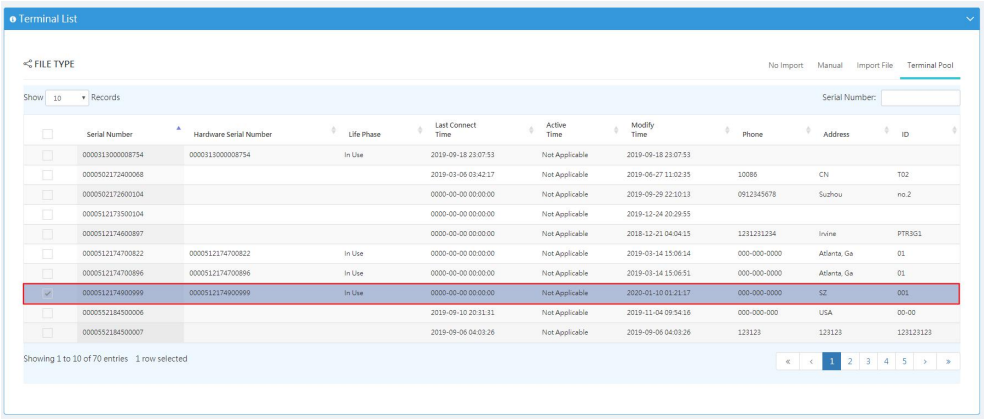
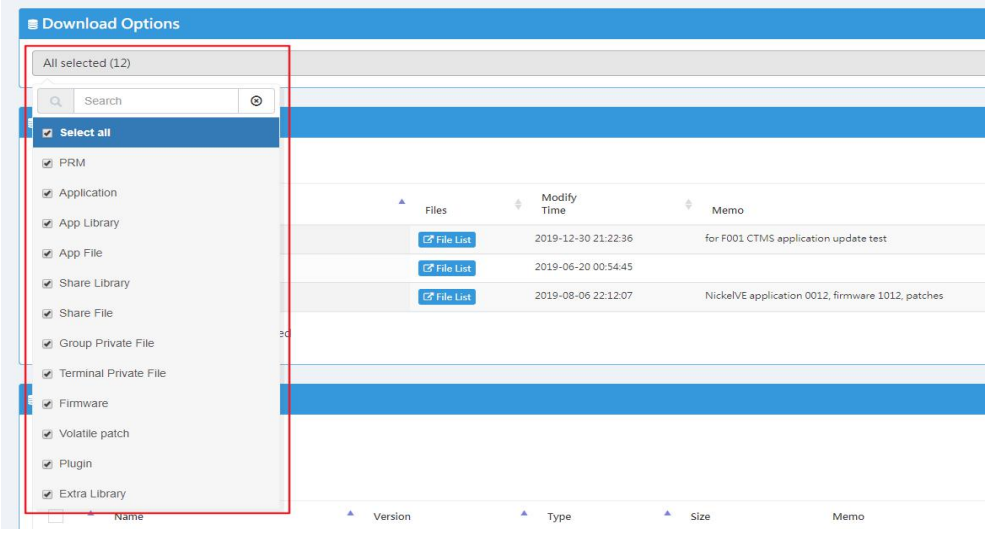
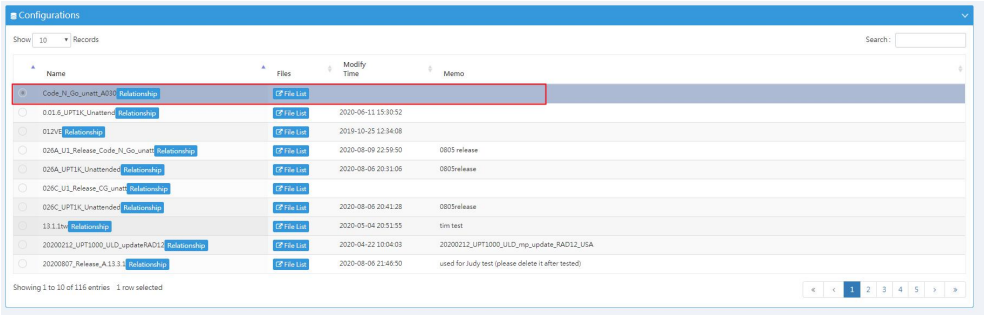
5.	Click OK button when prompted for attention 
6.	After the import is completed, it will prompt “Terminal create successful” or other similar message in the lower right corner of the page 

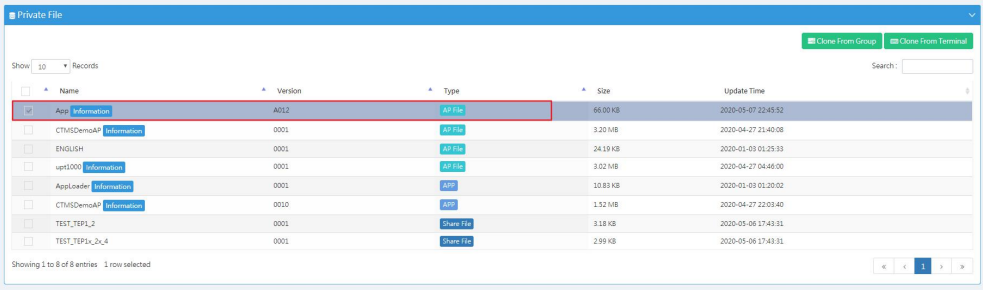
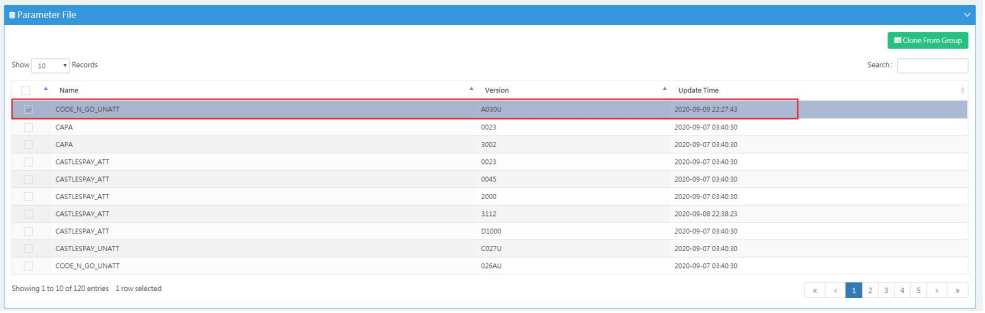
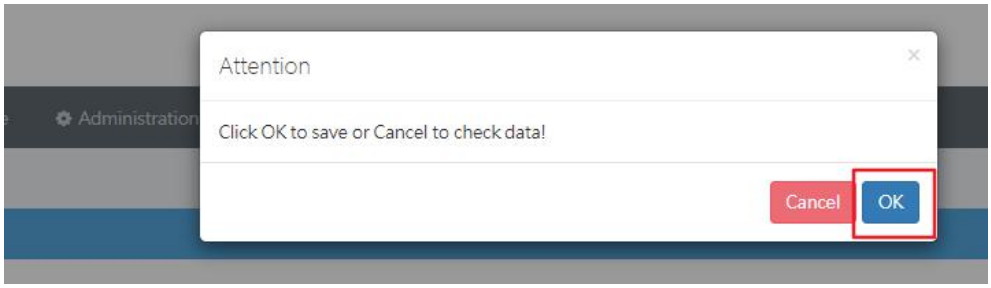
12.1.1.4. Create Group

❖ Using the CTMS function also requires adding the terminal to one group. Use the chart below to create a group for the terminals with unattended application.

Step	Action & Display
1.	Login CTMS management system 
2.	Point to Group and then click Group Create

	
3.	Input the Group Info: Name, Model Name, User, Memo, M ID, Phone and Address 
4.	Scroll to the Download Setting section, set the Trigger Time for this group 
5.	Scroll to the Terminal List section, click the Terminal Pool and select the terminals to join this Group

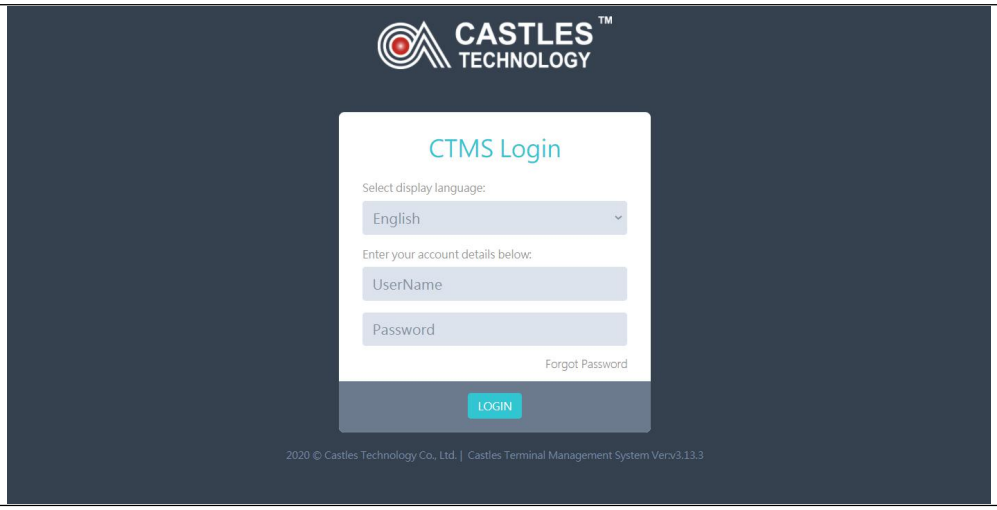
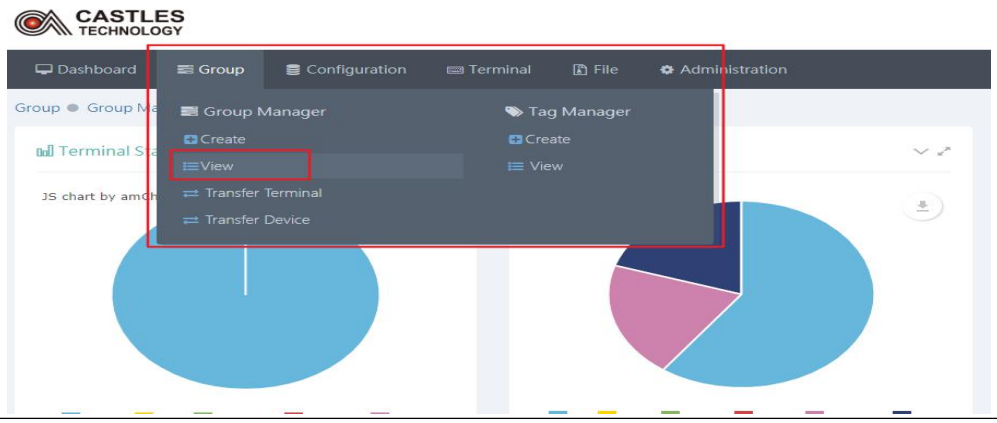
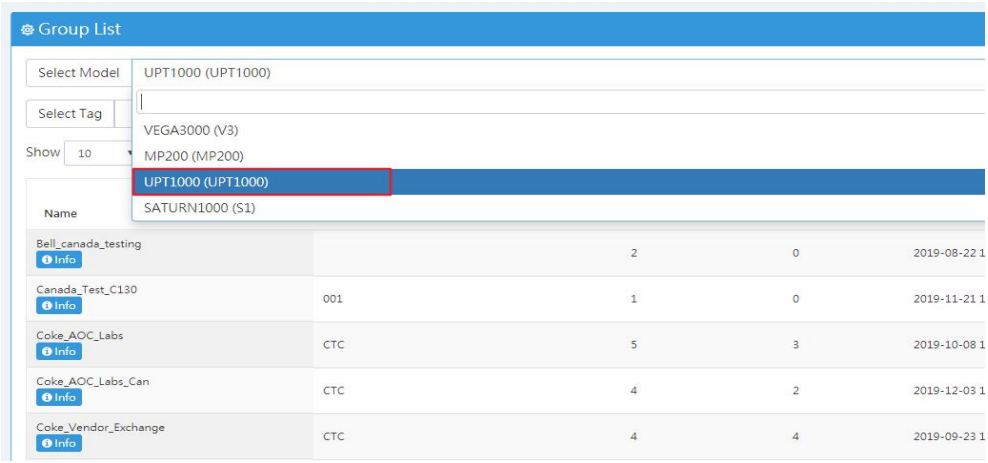
	
6.	Scroll to the Download Options section, select the options which you want to update 
7.	Scroll to the Configurations section, select the one you want the terminals to update to 
8.	Scroll to the Private File section, select the one you want the terminals to update or none

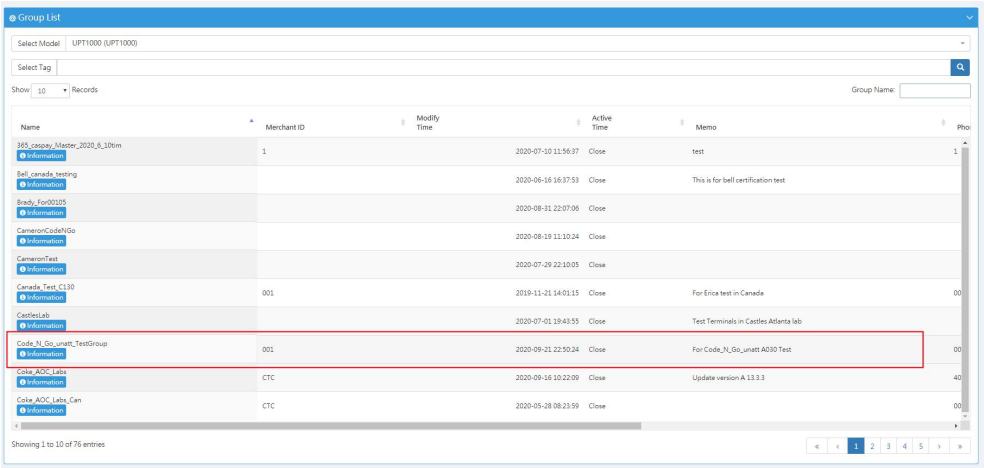
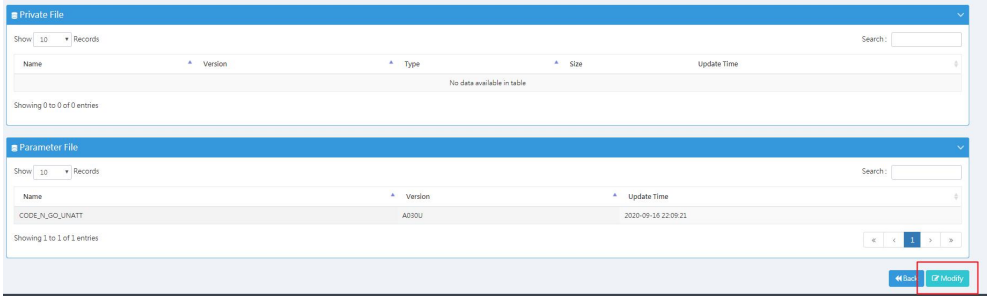
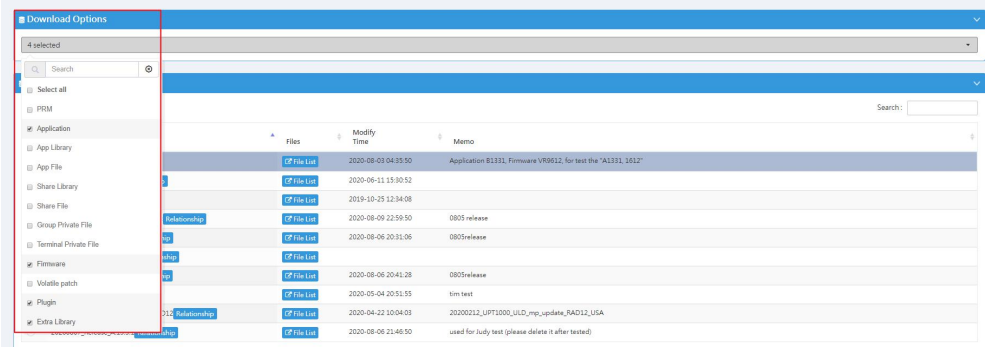
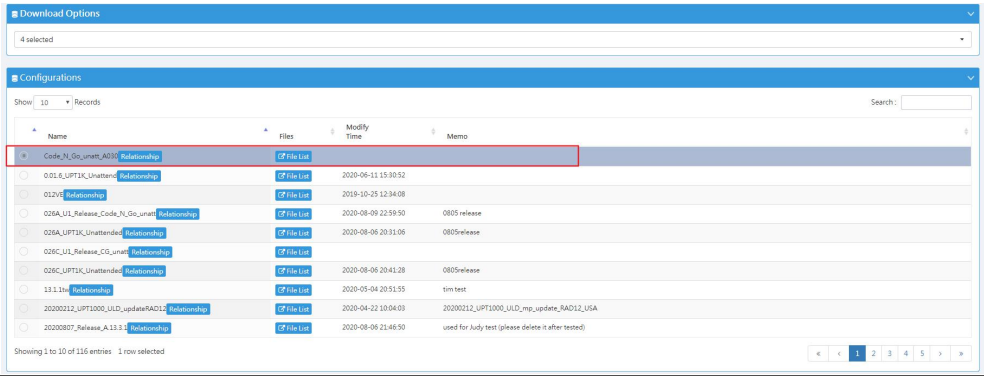
	
9.	Scroll to the Parameter File section, select the parameter files for this Group. You can double click the parameter file which you selected and edit the parameter values 
10.	■ Click Confirm button ■ Click OK button when prompted for attention 
11.	After the creation is completed, it will prompt “[Group: XXXX] create successful” or other similar message in the lower right corner of the page 

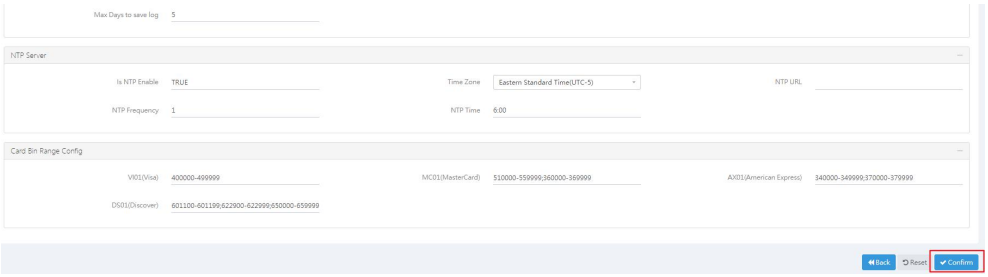
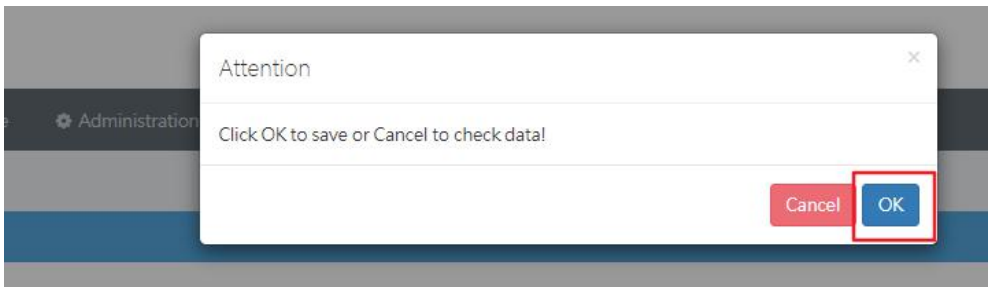
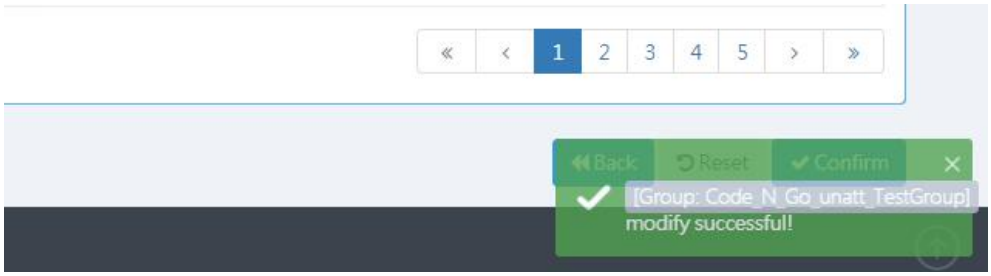
12.1.2. Update AP, FW and Patches

❖ Use the chart below to update applications, patches and firmware through CTMS.

Step	Action & Display
1.	Login CTMS management system

	
2.	Make sure that the configuration files used to update applications, patches and firmware have been imported into CTMS website, and that the terminal you are working with is correctly added to CTMS website; if not, follow the steps in section "Preparation on CTMS website" to complete.
3.	Point to Group and click View 
4.	Scroll down to Group List, select the Model according to the model of your terminal: UPT1000(UPT1000) or VEGA3000(V3) 
5.	Find the group which your terminal belongs to and double click it

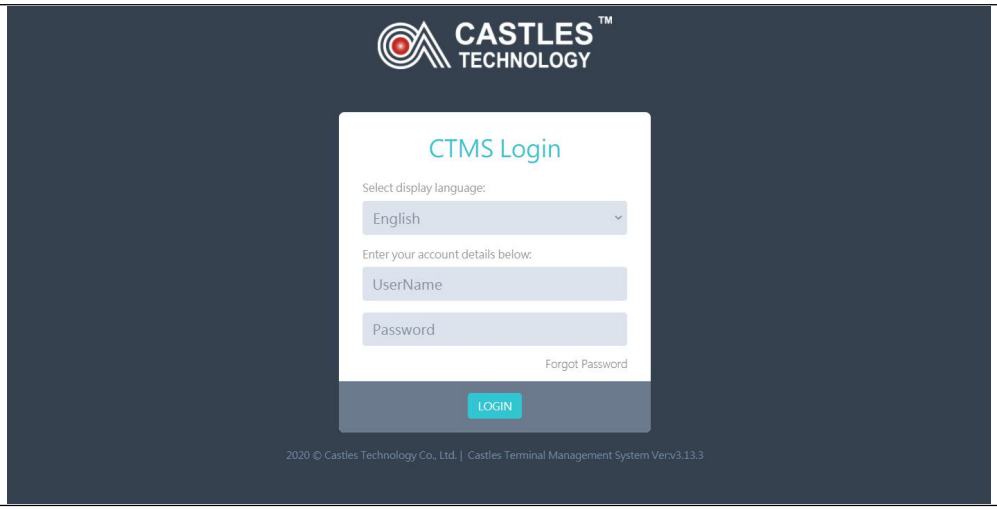
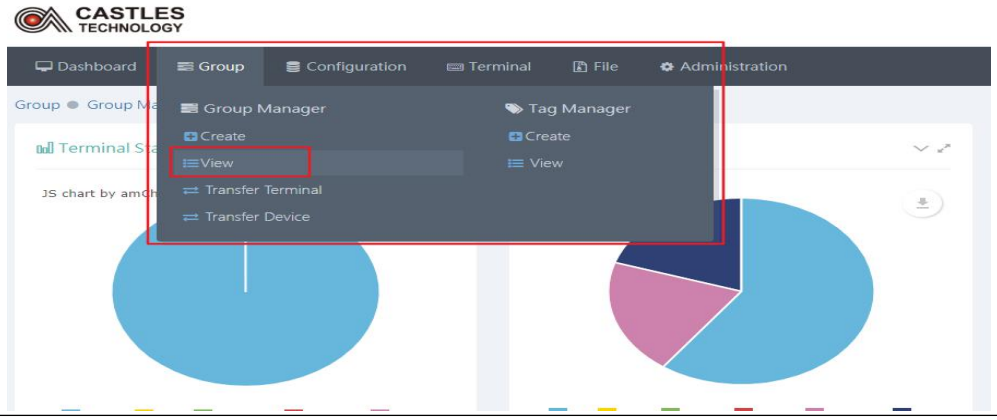
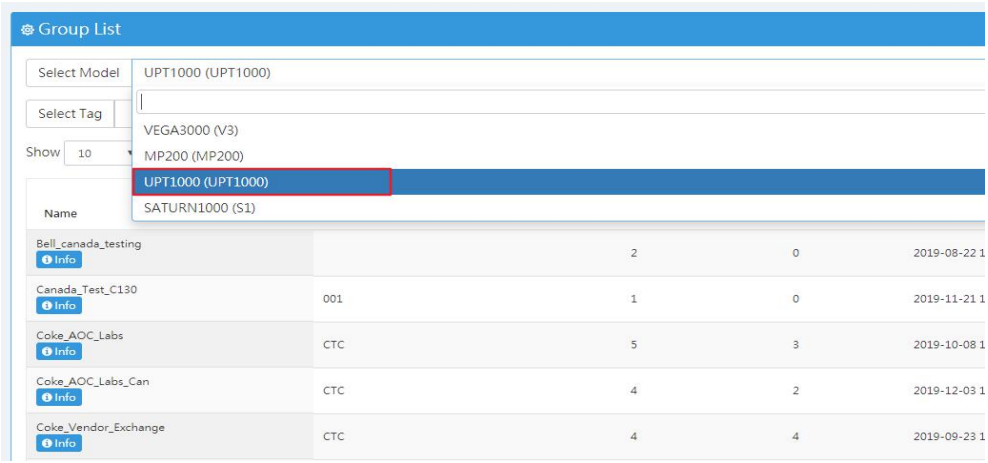
	
6.	After turning to the Group Detail page, scroll down to the bottom of the page and click the button Modify 
7.	After turning to the Group Modify page, scroll down to Download Options and select “Application, Firmware, Plugin, Extra Library” 
8.	Scroll down to Configuration, select the one used to update applications, patches and firmware, which should be the configuration file imported in step 2 

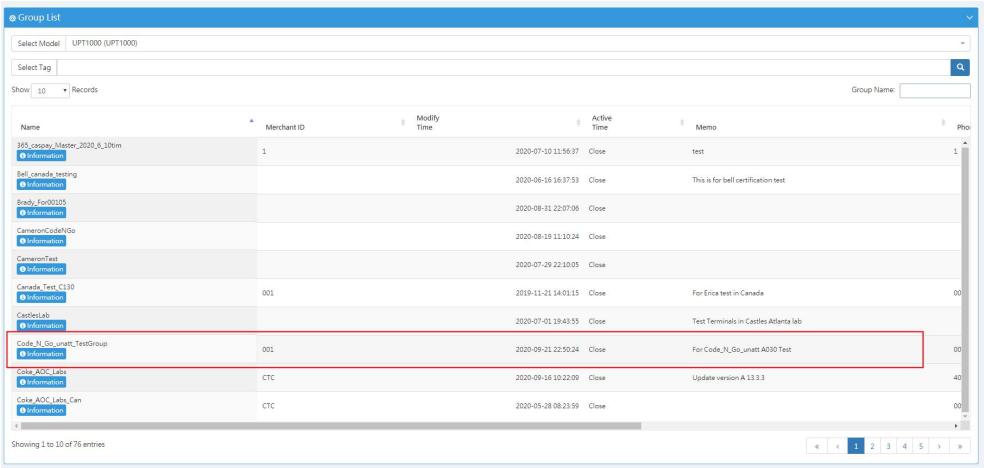
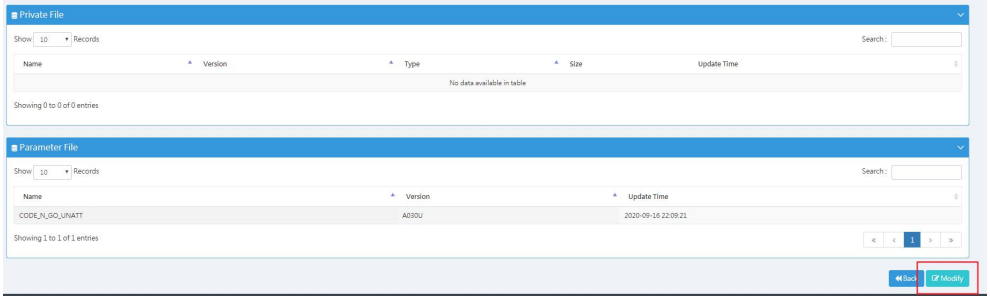
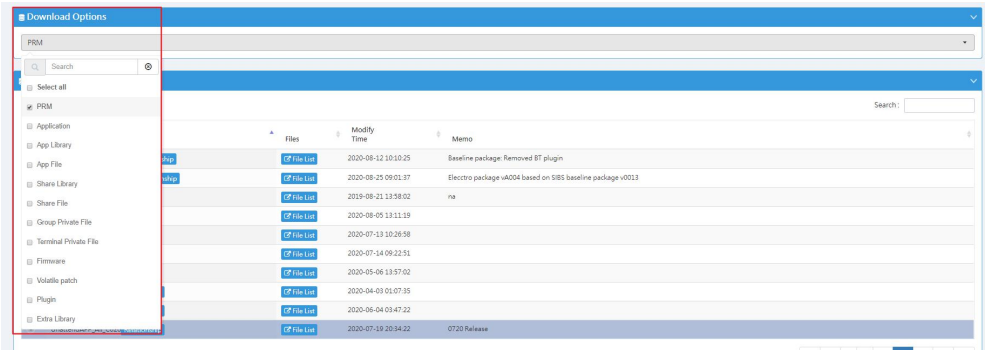
9.	After the modification, scroll down to the bottom of the page and click Confirm button 
10.	Click OK button when prompted for attention 
11.	After the modification is completed, it will prompt "[Group: XXXX] modify successful" or other similar message in the lower right corner of the page 
12.	Follow the steps in section "CTMS Check" or wait until the CTMS trigger time, perform CTMS check to complete the updates.

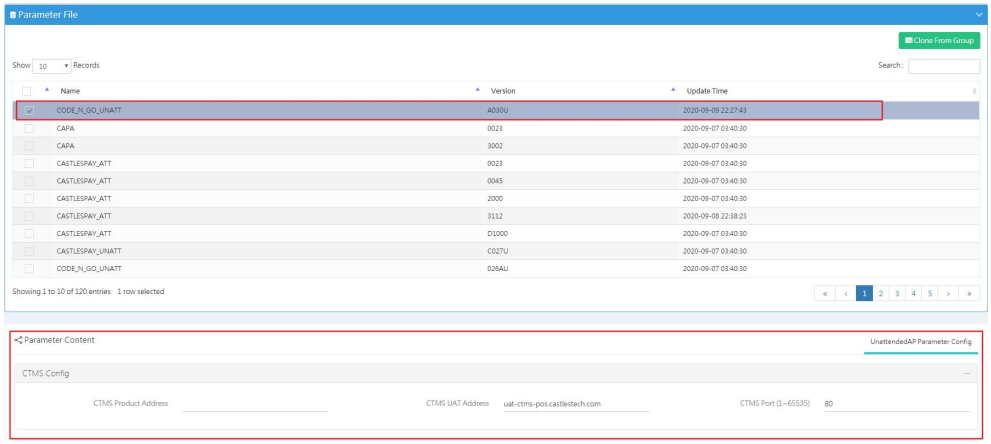
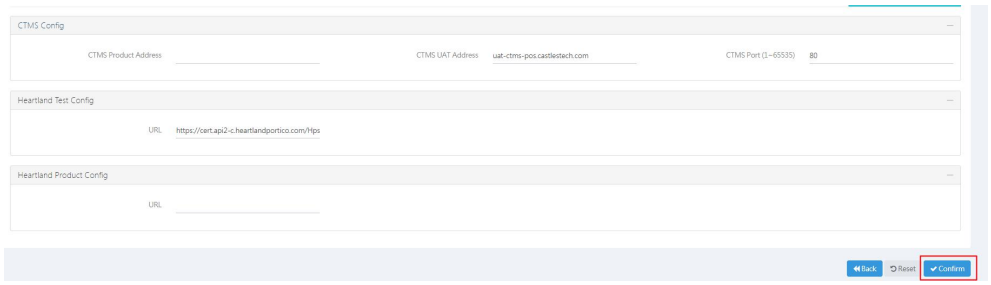
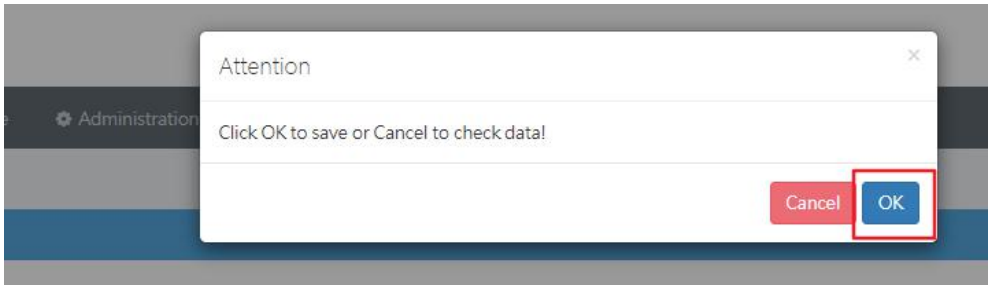
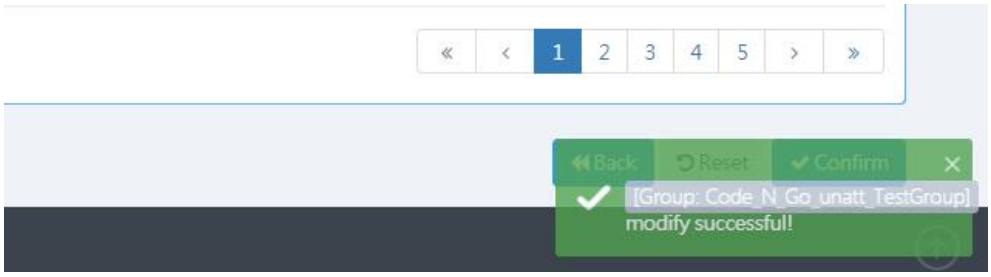
12.1.3. Update Parameters

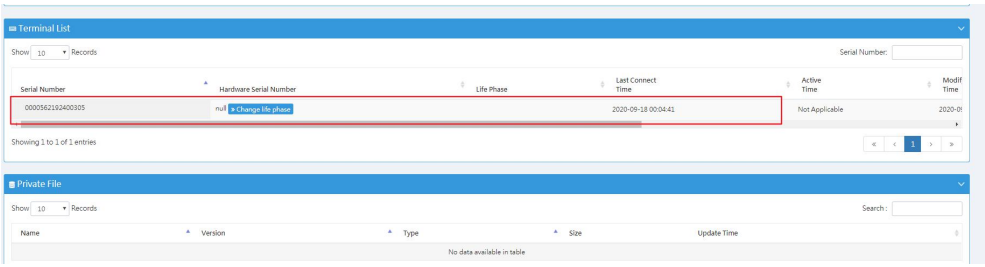
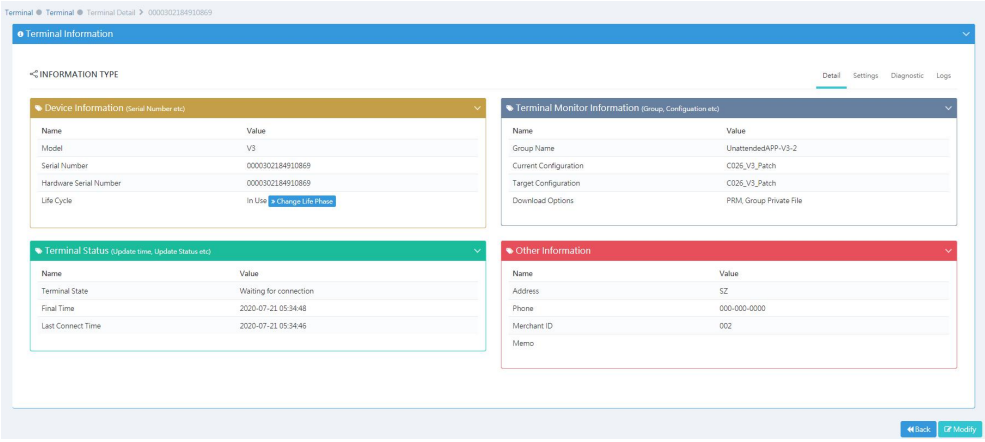
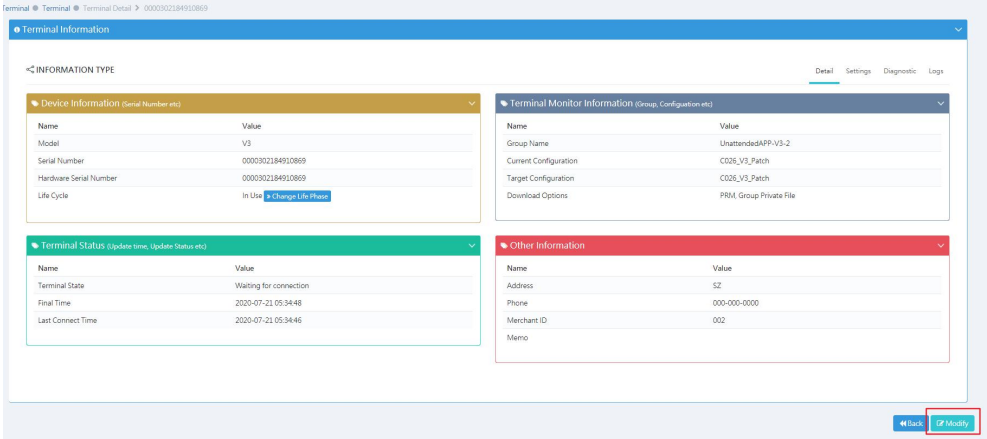
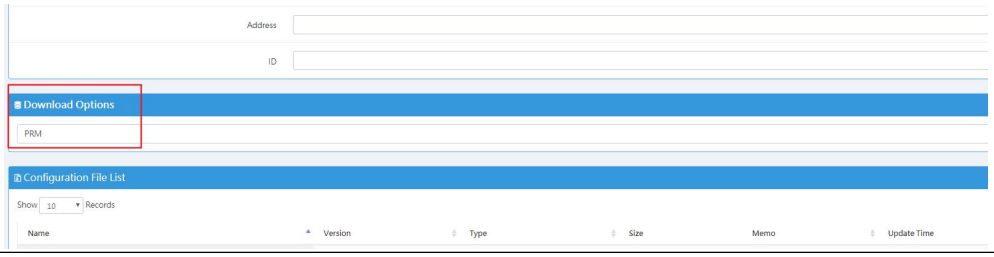
- ❖ At present, the parameters in the parameter file specific for unattended application are divided into group part and terminal part. The parameters in the group part are shared by the terminals in the same group, and the terminal part could be modified to match the different requirements of the terminals. Use the chart below to update parameters through CTMS.
- ➢ Update parameters through CTMS will update all parameters in the CTMS website, so make sure that all parameters in the website have the values you expect. For the definition and description of parameters, please refer to "APPENDIX B: Unattended Project Configuration Parameters".

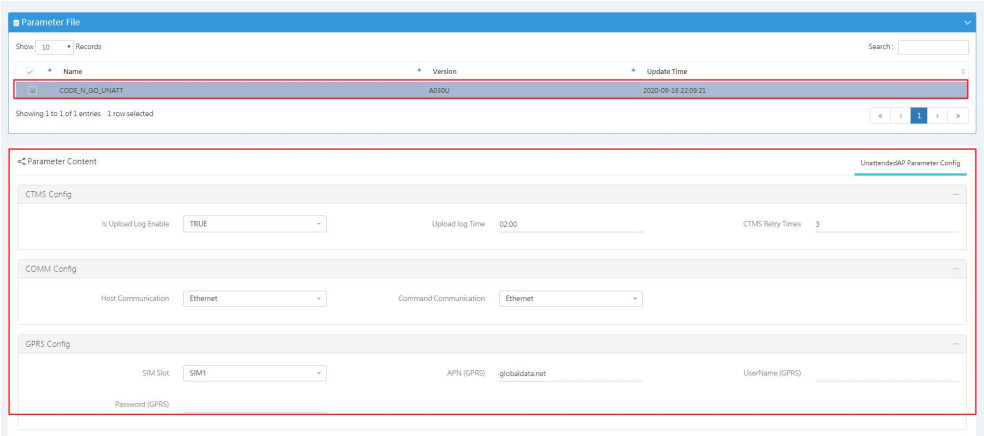
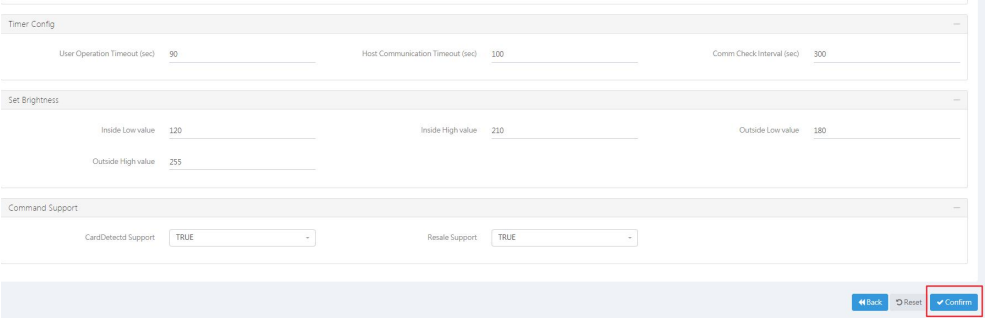
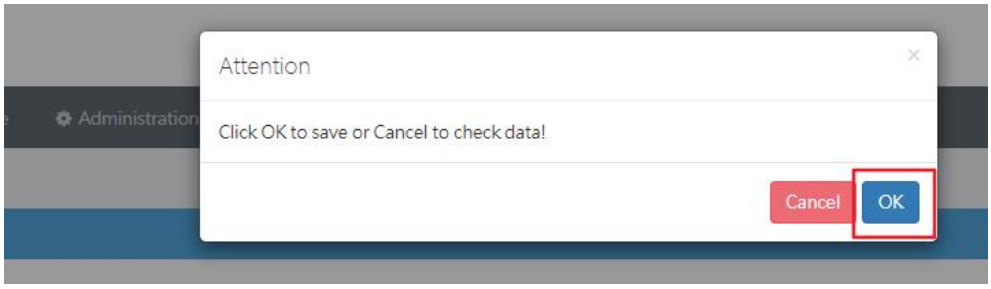
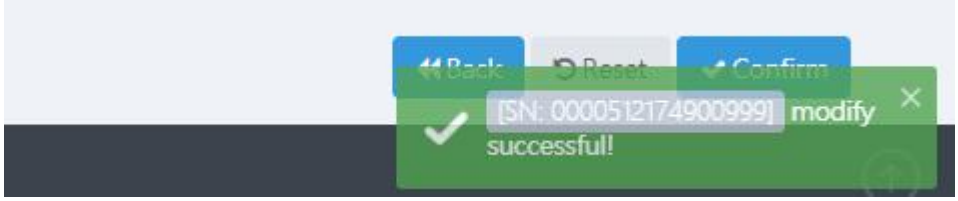
Step	Action & Display
1.	Login CTMS management system

	
2.	Make sure that the parameter file specific for unattended application has been imported into CTMS website, and that the terminal you are working with is correctly added to CTMS website; if not, follow the steps in section "Preparation on CTMS website" to complete.
3.	Group Part - Point to Group and click View 
4.	Scroll down to Group List, select the Model according to the model of your terminal: UPT1000(UPT1000) or VEGA3000(V3) 
5.	Find the group which your terminal belongs to and double click it

	
6.	After turning to the Group Detail page, scroll down to the bottom of the page and click the button Modify 
7.	After turning to the Group Modify page, scroll down to Download Options and select “PRM” 
8.	Scroll down to Parameter File, double click the parameter file to modify the parameters which is in the group part

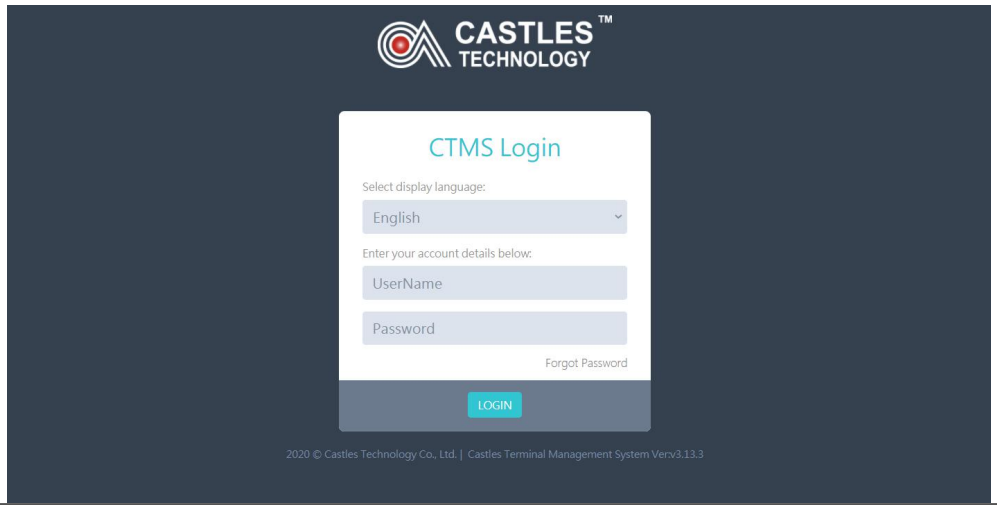
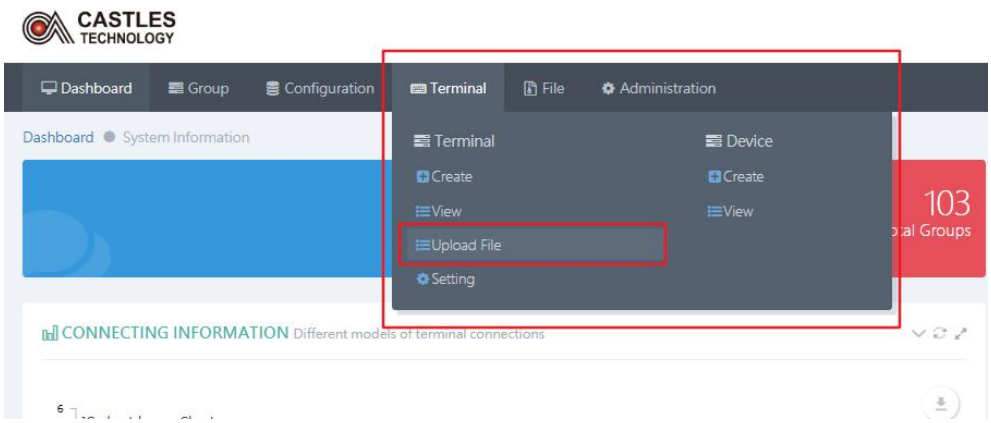
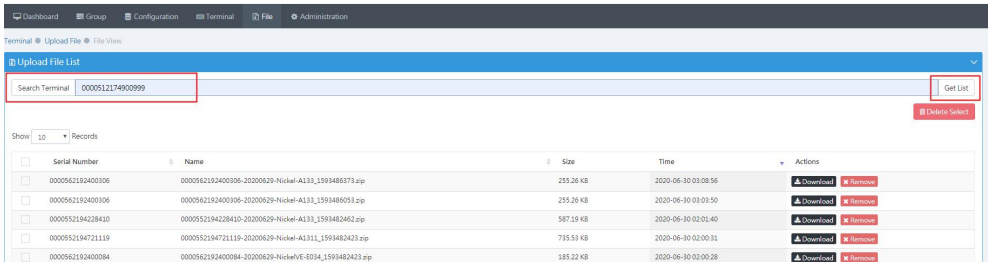
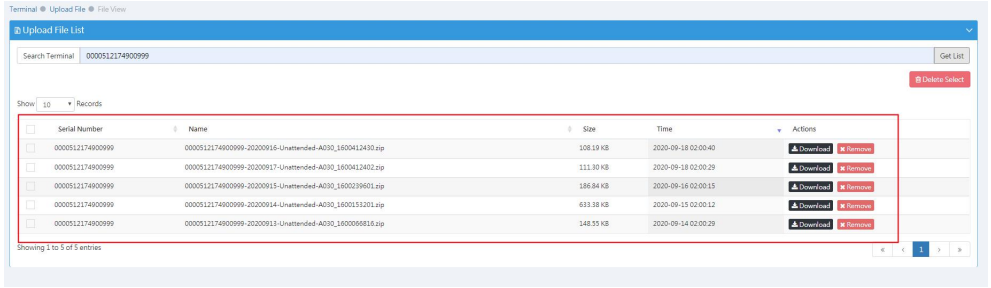
	
9.	After the modification, scroll down to the bottom of the page and click Confirm button 
10.	Click OK button when prompted for attention 
11.	After the modification is completed, it will prompt "[Group: XXXX] modify successful" or other similar message in the lower right corner of the page. And it will turn to the Group Detail page 
12.	Terminal Part – In the Group Detail page, scroll to Terminal List and you're your terminal's record

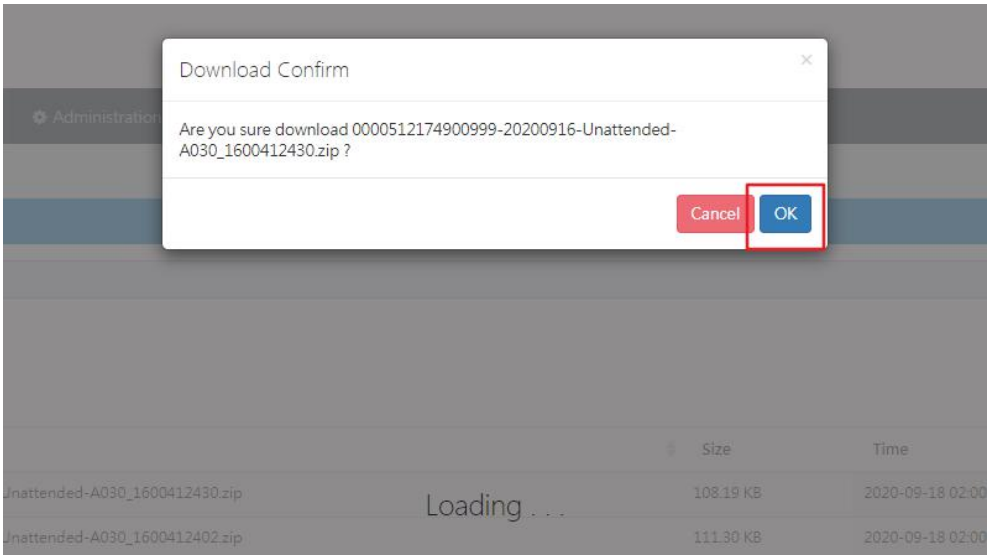
	
13.	Double click the terminal record, it will turn to the Terminal Detail page of that terminal 
14.	After turning to the Terminal Detail page, scroll down to the bottom of the page and click the button Modify 
15.	After turning to the Terminal Modify page, scroll down to Download Options and make sure that “PRM” option is selected 
16.	Scroll down to Parameter File, double click the parameter file to modify the parameters which is in the terminal part

	
17.	After the modification, scroll down to the bottom of the page and click Confirm button 
18.	Click OK button when prompted for attention 
19.	After the modification is completed, it will prompt “[SN: XXXX] modify successful” or other similar message in the lower right corner of the page 
20.	Follow the steps in section “CTMS Check” or wait until the CTMS trigger time, perform CTMS check to complete the updates.

12.1.4. View Log File

❖ Use the chart below to view log files of the terminals with unattended application, you also can download the files to check.

Step	Action & Display
1.	Login CTMS management system 
2.	Point to Terminal and click Upload File 
3.	In the Upload File List, input the serial number of the terminal and then press Enter or click the Get List button 
4.	The log files of this terminal will be shown in the list, click the Download button to download the specific file 

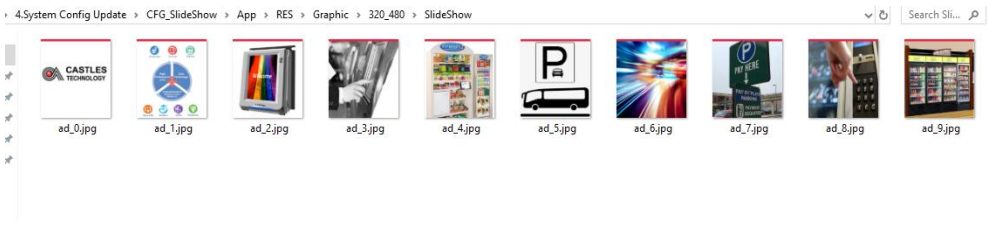
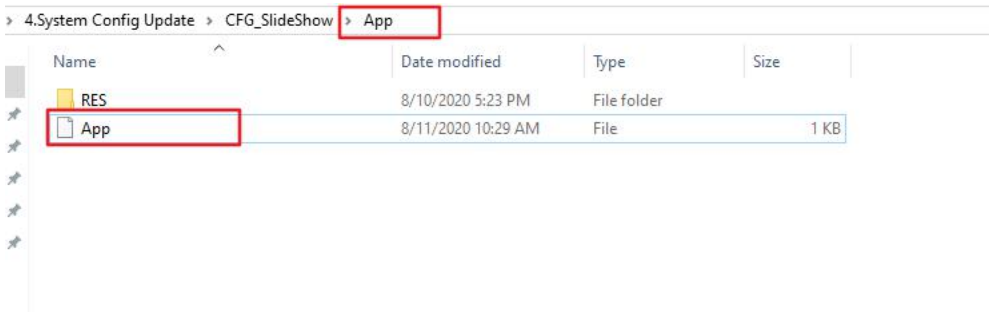
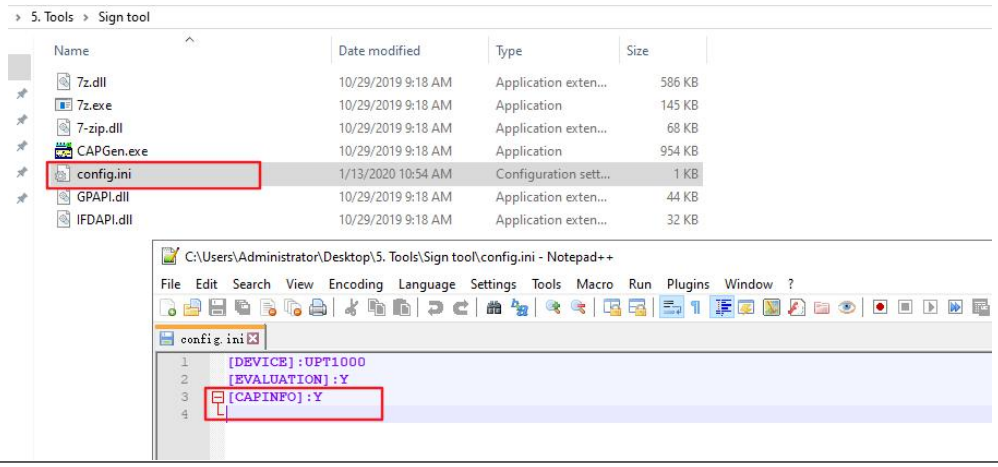
5.	Click OK button when prompted for Download Confirm 
6.	The download content and download process will be displayed in the lower left corner of the page, and you can view the log file locally after completion 

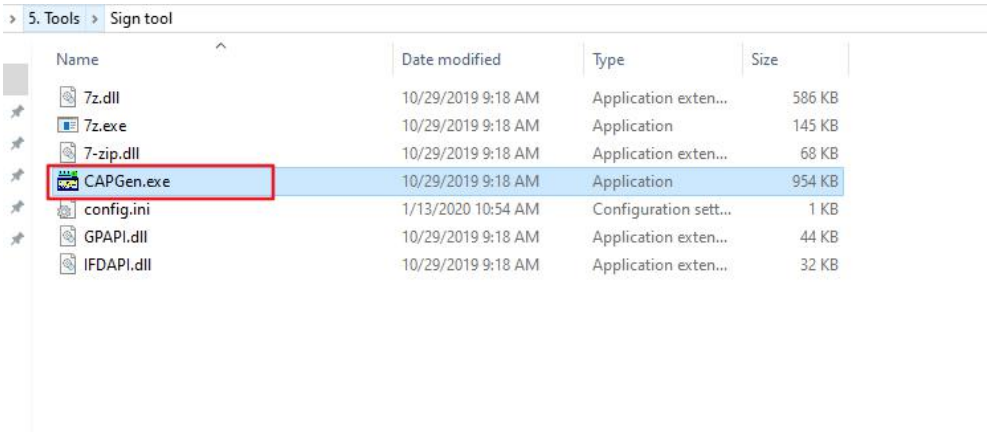
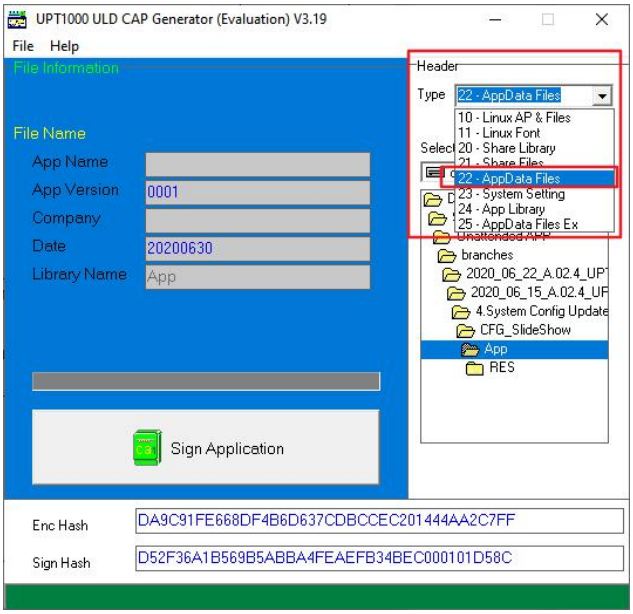
12.1.5. Update Slide Show

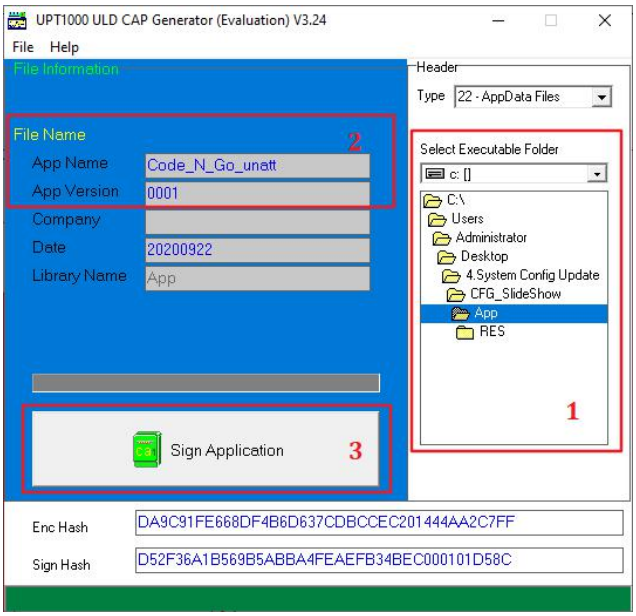
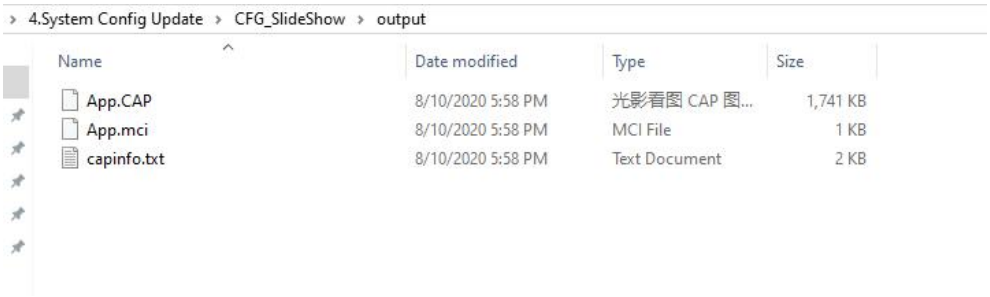
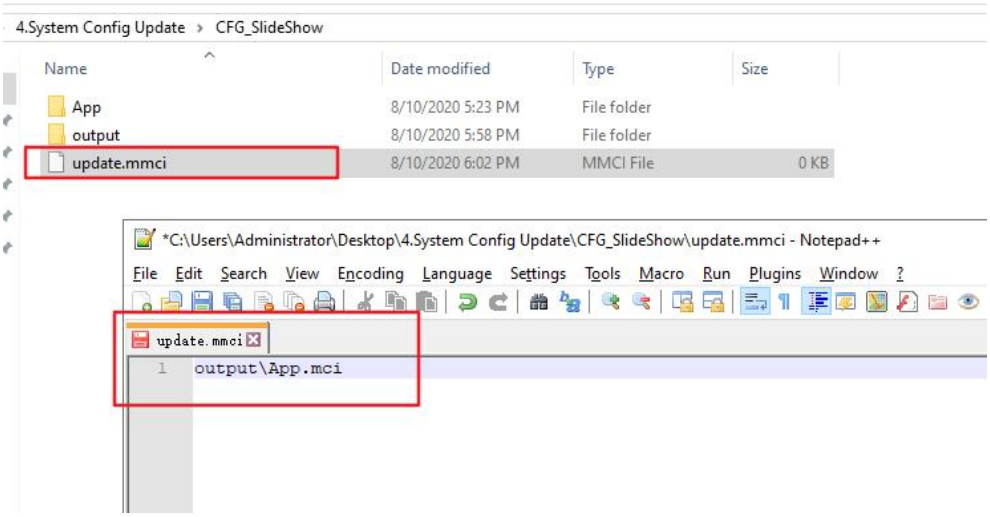
- Private files are the files used by the applications. A private file can be regarded as the parameter which is not a string or a number but a file. As a result, a private file can be assigned to more than one groups and terminals; but can't be modified. In general, private files are used when the pictures, voice files, xml files and other files on the terminal need to be updated.

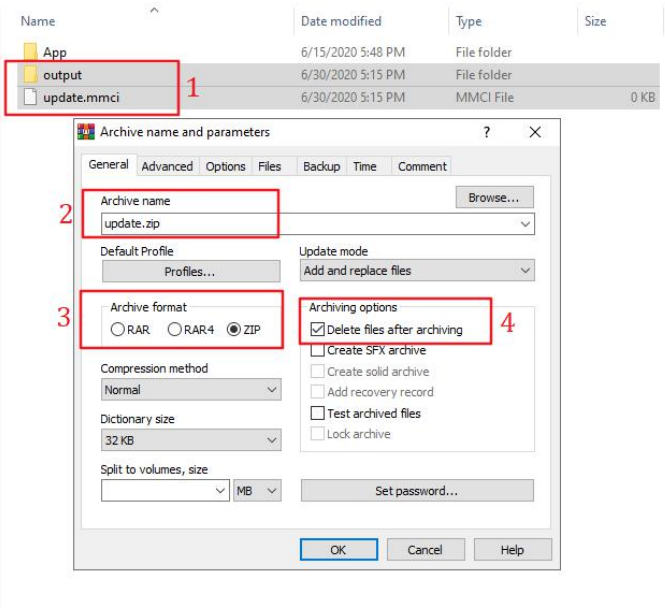
- For the unattended application, it is supported to update the slide show picture through CTMS private file update. Use the chart below to change the pictures of slide show for the terminal with unattended application.

Step	Action & Display
1.	Prepare the zip file for updating - Prepare the pictures you want to play on the terminal Note: The picture format has special requirements, otherwise the Castles terminal may not be able to display pictures or happen to other problems. Here are the requirements: ● Picture Type: JPG ● Dimensions: 320*360
2.	Copy the file named "App" to local which is for updating the slide show Note: The file "App" can be found in the release package (typically, the path is package\4.System Config Update\CFG_SlideShow)
3.	Find the previous pictures in the path "App\RES\Graphic\320_480\SlideShow"

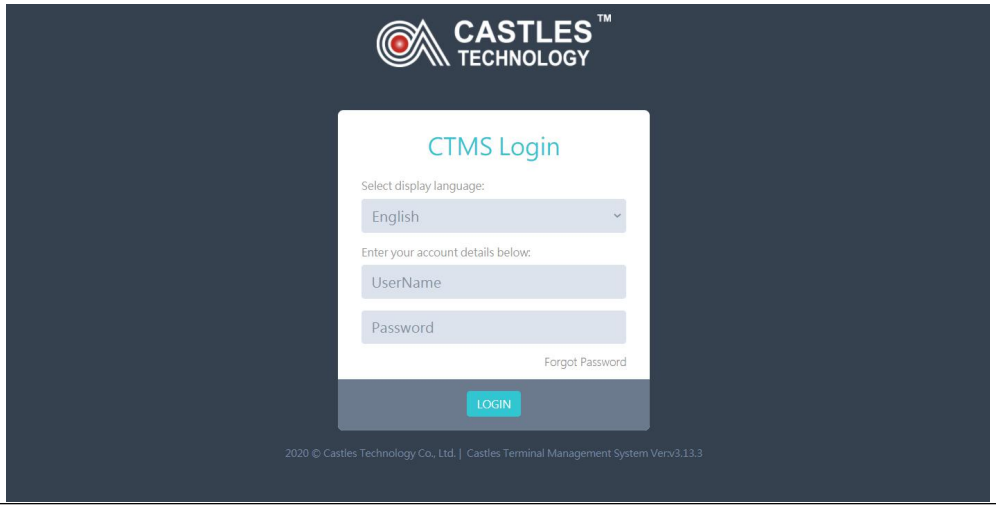
	
4.	Replace the previous pictures with your pictures Note: ● The picture names should not be changed ● The order in the name of the picture is also the order in which the picture is played ● If the number of pictures exceeds 10, the picture should be named like "ad_10.jpg", "ad_11.jpg", "ad_12.jpg", etc ● The default number of pictures is 10, you can change it through updating the parameter "Page Numbers".
5.	"Folder name" must have to same with a "file name", you can create a new file if no same file name Note: File content can't be null. If it is null, it will error. 
6.	Find the sign tool and confirm that the CAPINFO of the tool is enabled (Y means enabled, N means disabled) Note: The sign tool of UPT1000F and VEGA3000P terminals is different (the corresponding tool will be placed in the folder "5.Tools" of the release package, here takes the sign tool of UPT1000F as an example) 
7.	Double click "CAPGen.exe" to open the sign tool

	
8.	Select “22 - AppData Files” as the Type of Header 
9.	■ Select the executable according to the path where you create it locally； ■ Input the App Name (the APP Name should be Code_N_Go_unatt) ■ Input the App Version (Updates can be detected when the versions are different, so it is better to manage the versions regularly, such as 0001, 0002, 0003, etc); ■ Click the button “Sign Application”

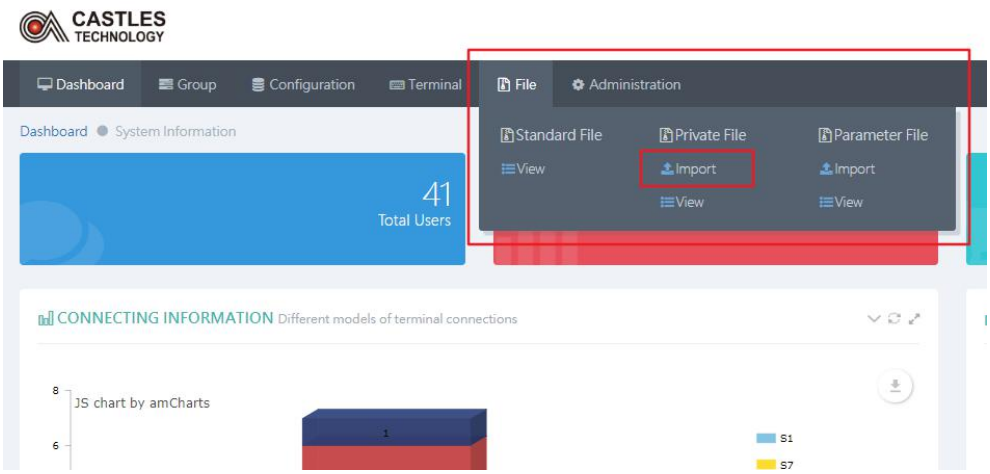
	
10.	When the signature is completed, a folder named “output” will be generated with three files in 
11.	Create a mmci file with the content “output\App.mci” 
12.	Compress the “output” folder and “update.mmci” file into a zip file. The filename can be “update.zip” and you can delete the source files after compression



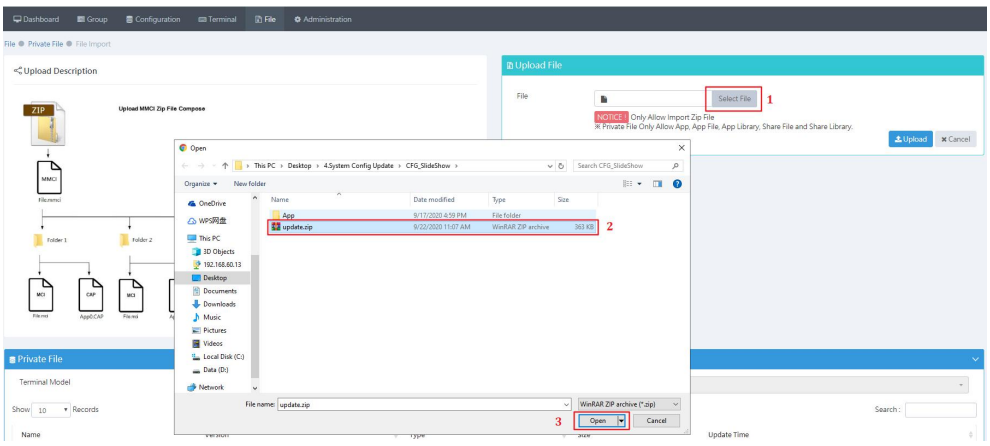
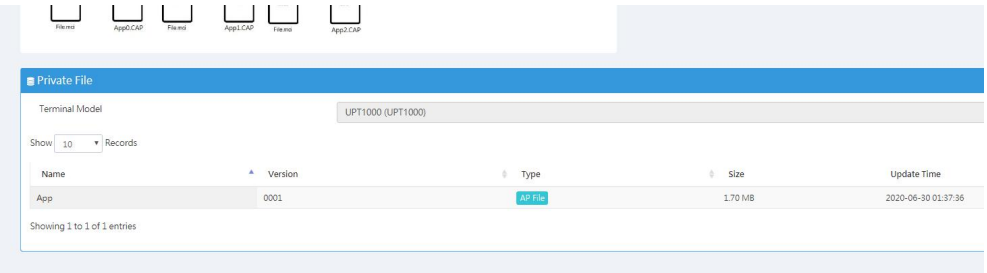
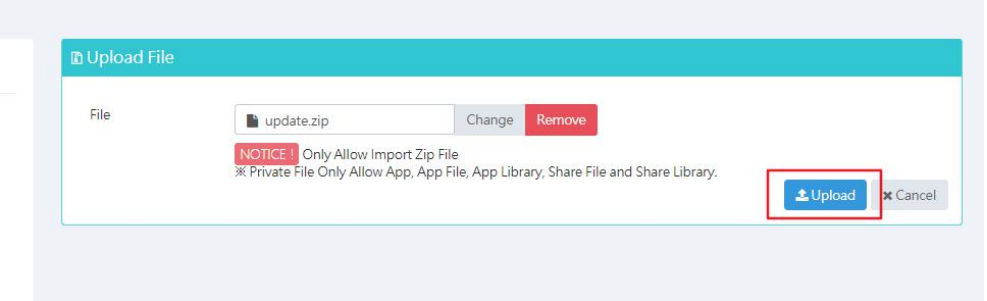
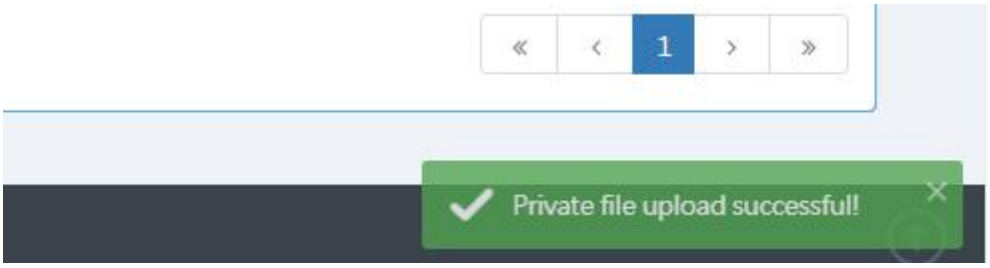
13. Import the zip file to CTMS website - Login CTMS management system

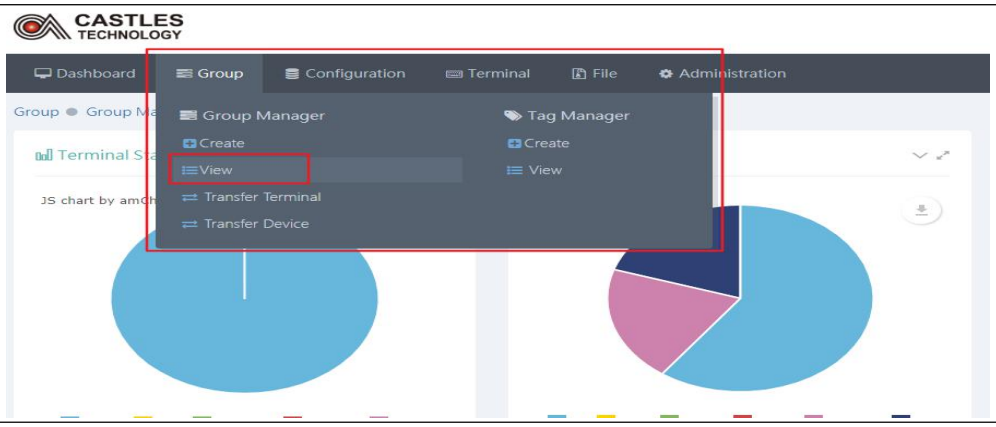
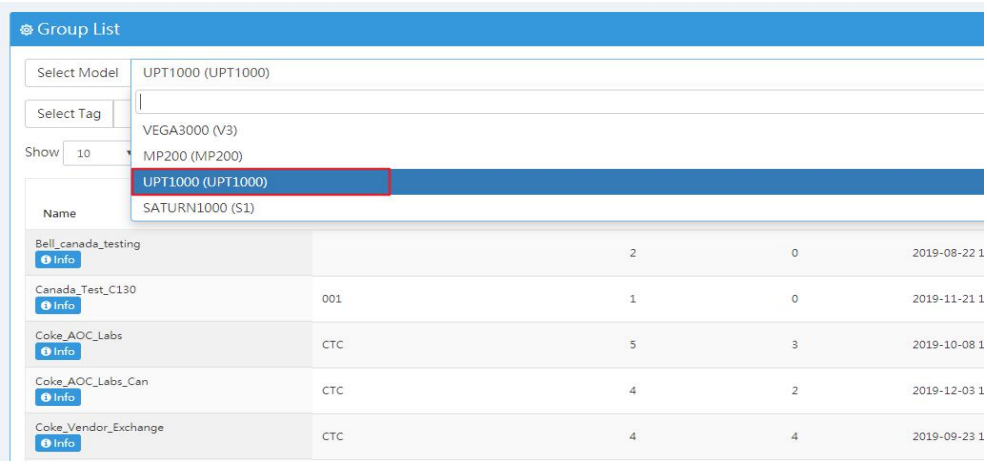
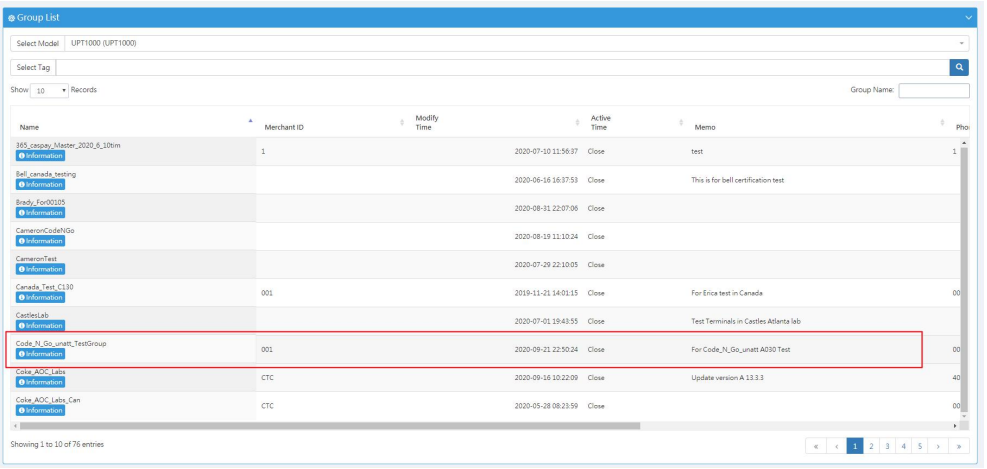


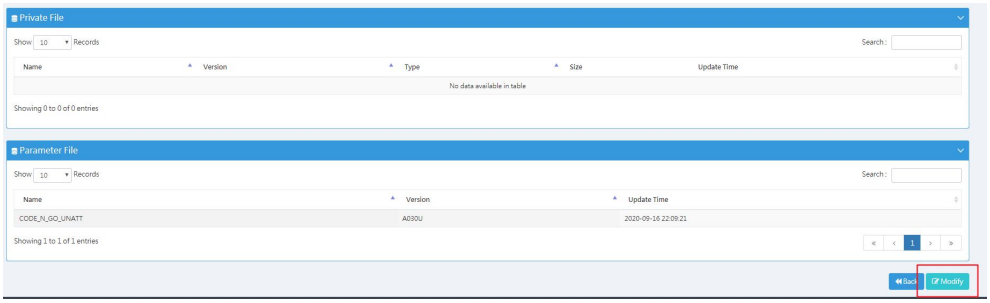
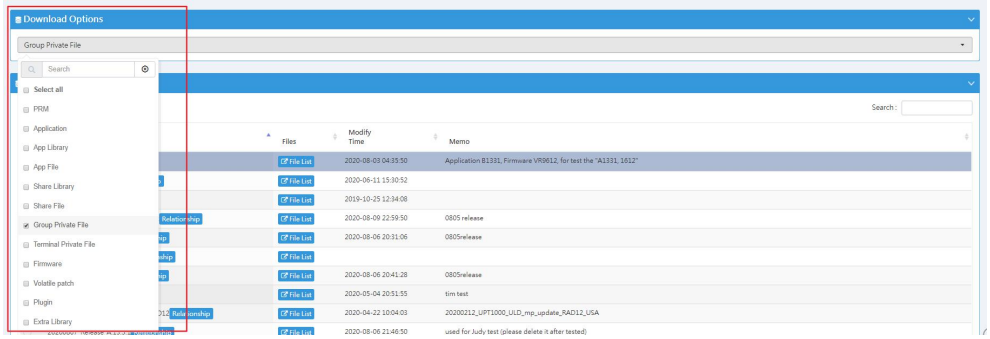
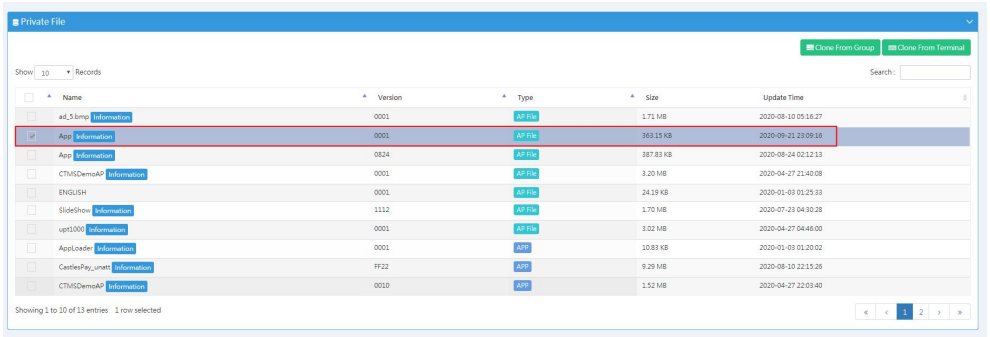
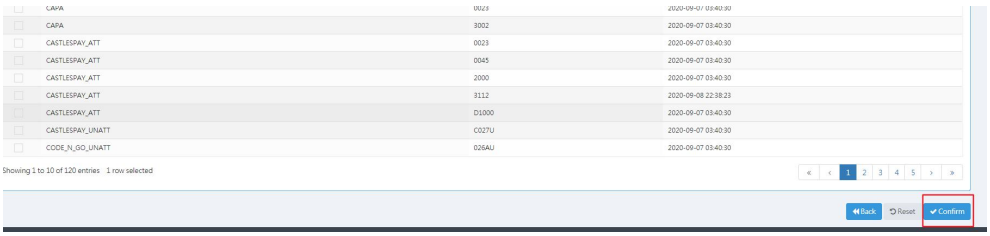
14. Point to Private File and click File Import

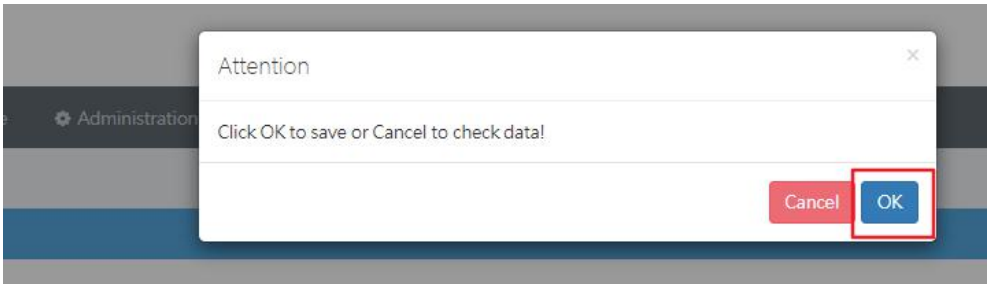
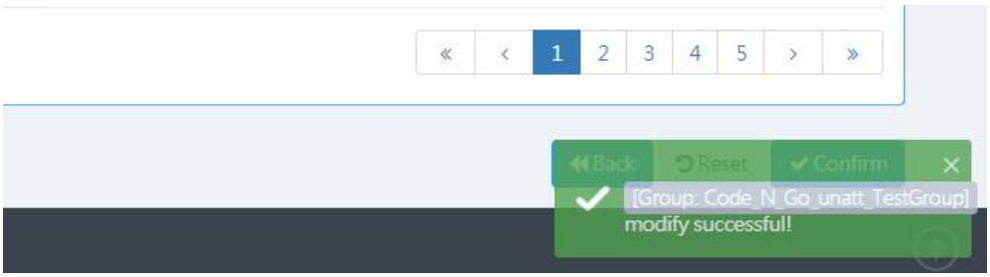


15. Click Select File and select the ZIP file which should be the file compressed in step 12

	
16.	The file information will be displayed after imported, check whether it is correct 
17.	Click Upload button 
18.	After the import is completed, it will prompt “Private file upload successful” or other similar message in the lower right corner of the page 
19.	Make sure that the terminal you are working with is correctly added to CTMS website; if not, follow the steps in section “Preparation on CTMS website” to complete.
20.	Modify the group - Point to Group and click View

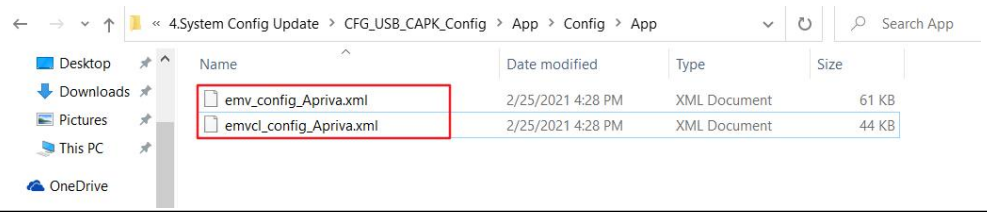
	
21.	Scroll down to Group List, select the Model according to the model of your terminal: UPT1000(UPT1000) or VEGA3000(V3) 
22.	Find the group which your terminal belongs to and double click it 
23.	After turning to the Group Detail page, scroll down to the bottom of the page and click the button Modify

	
24.	After turning to the Group Modify page, scroll down to Download Options and select "Group Private File" 
25.	Scroll down to Private File, select the private file which should be the file uploaded in step 18 
26.	After the modification, scroll down to the bottom of the page and click Confirm button 
27.	Click OK button when prompted for attention

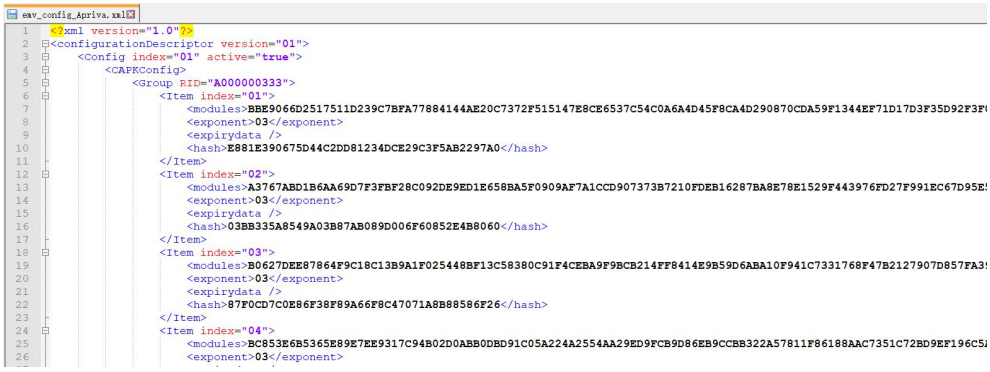
	
28.	After the modification is completed, it will prompt "[Group: XXXX] modify successful" or other similar message in the lower right corner of the page. And it will turn to the Group Detail page 
29.	Follow the steps in section "CTMS Check" or wait until the CTMS trigger time, perform CTMS check to complete the updates.

12.1.6. Update CAPK for Apriva

- ❖ One-off Delivery file is designed for customers to download file types which CTMS doesn't support, such as AppData, Ex, KeyCAP, etc. One thing that noted is that One-off Delivery will not compare the version number. In other words, it doesn't support version control function.
- ❖ For the unattended application, it is supported to update the CAPK through CTMS One-off Delivery file update. Use the chart below to update CAPK for the terminal with unattended application.

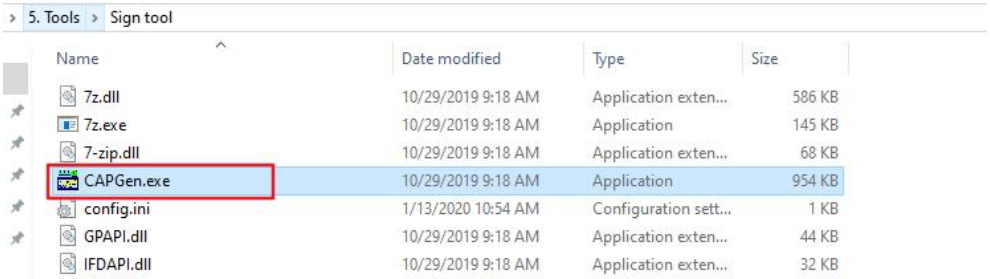
Step	Action & Display
1.	Copy the file named "App" to local which is for updating the configuration Note: The file "App" can be found in the release package (typically, the path is package\4.System Config Update\CFG_USB_CAPK_Config)
2.	Find the files "emv_config_Apriva.xml" and "emvcl_config_Apriva.xml" in the path "App\Config\App" 
3.	Edit the content of the files and save them Note: Blank (no set any values) means that it will not change the original value in the terminal after update; Empty (fill in "Empty") means that it will clear the value in the

terminal after Update.

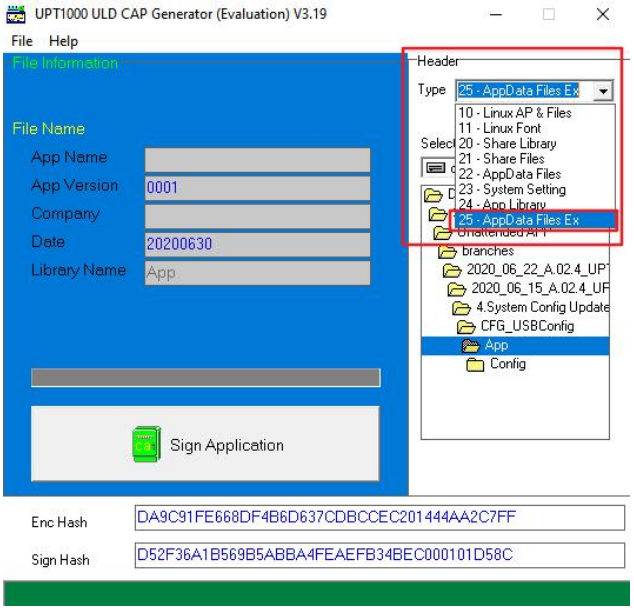


4. Double click “CAPGen.exe” to open the sign tool

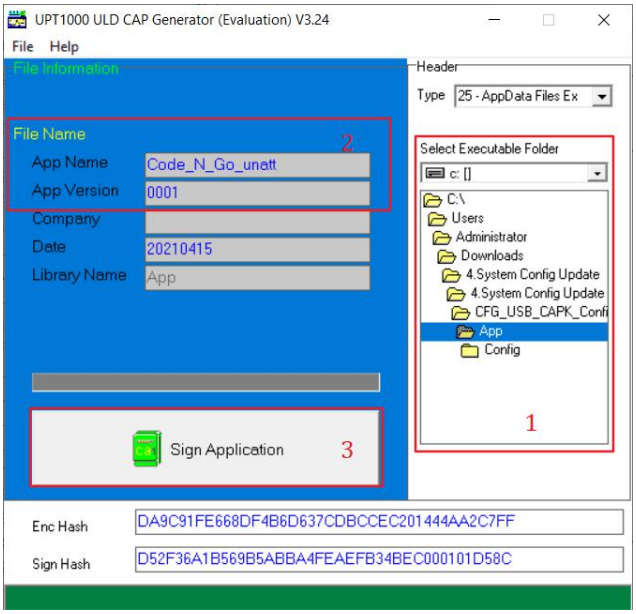
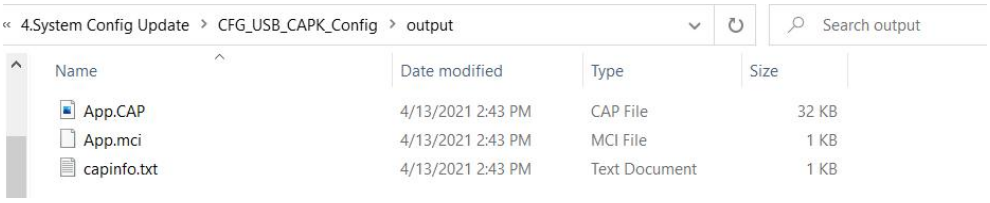
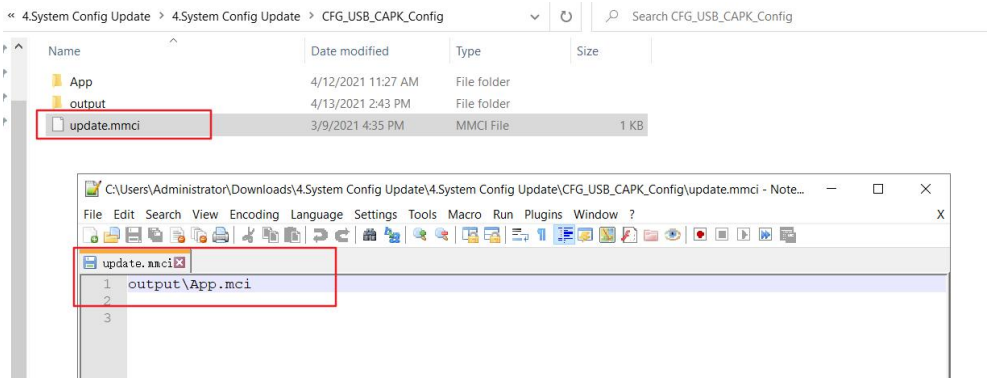
Note: The corresponding tool will be placed in the folder “5.Tools” of the release package

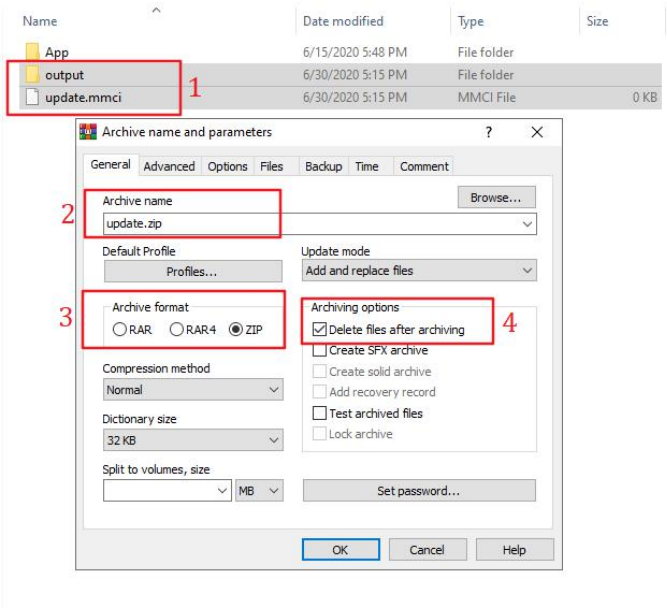
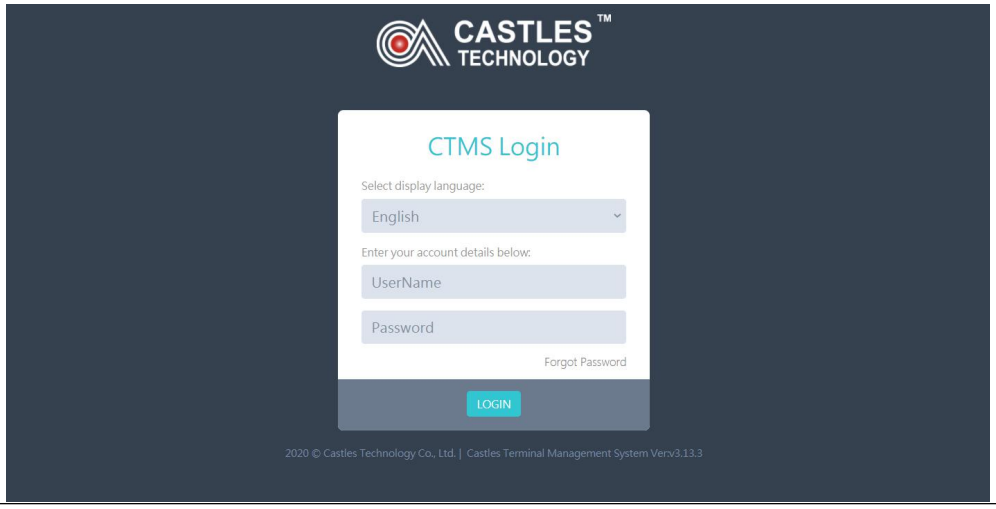
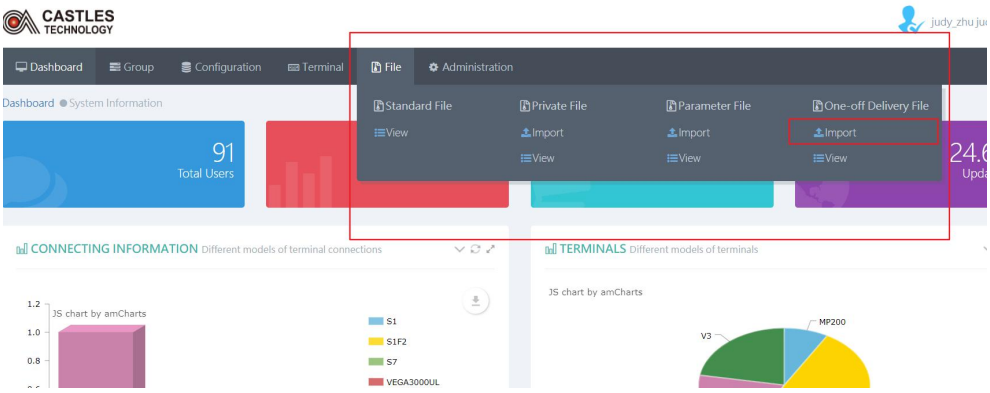


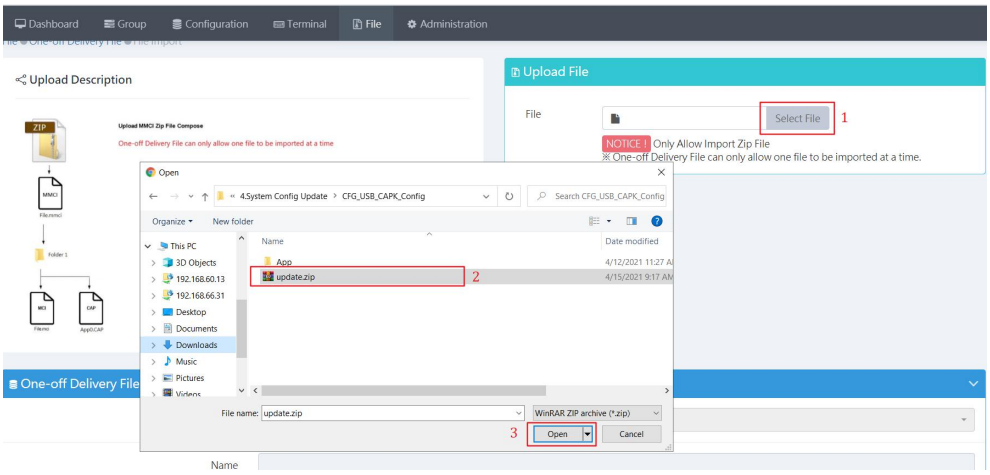
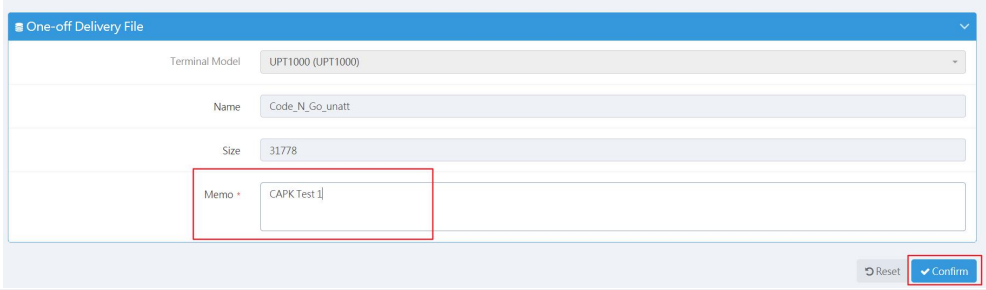
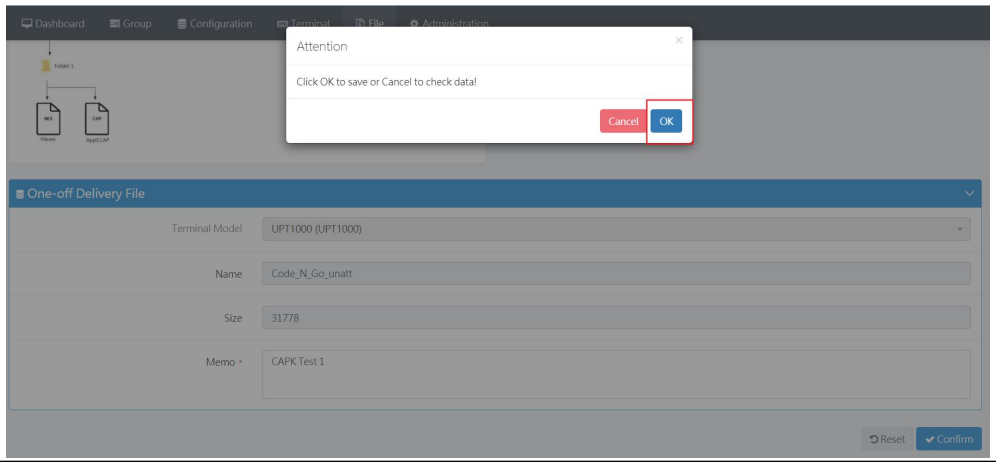
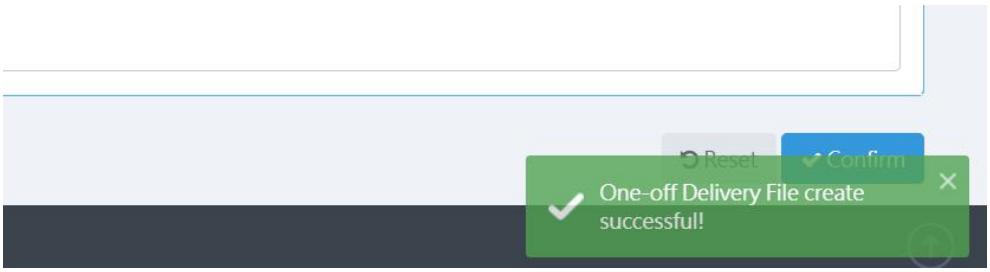
5. Select “25 – AppData Files” as the Type of Header

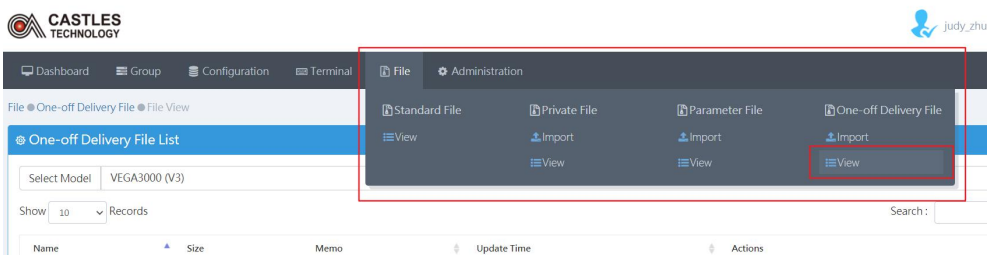
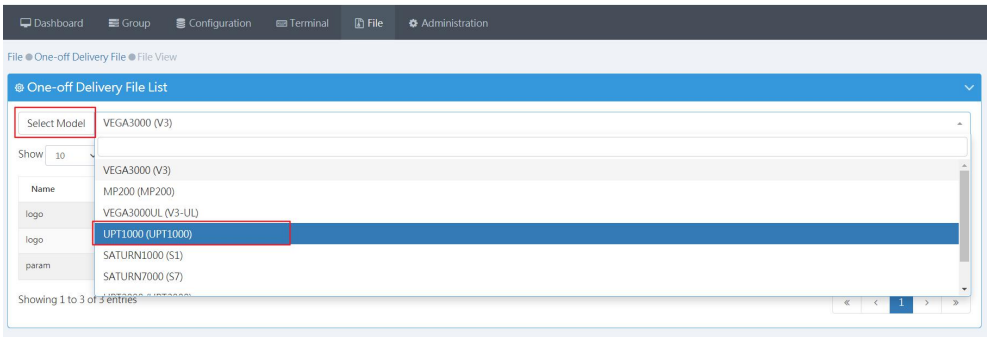
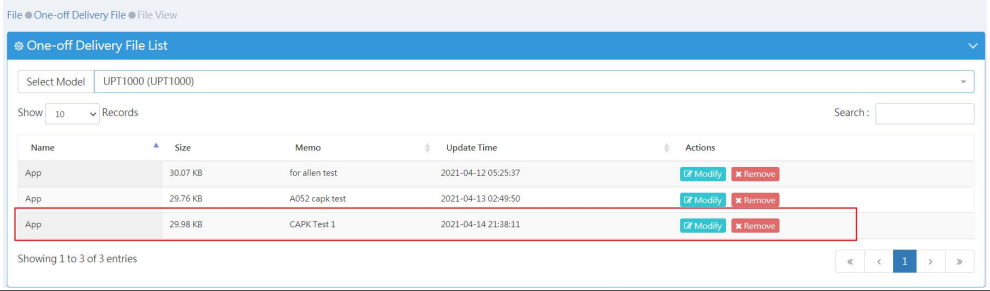
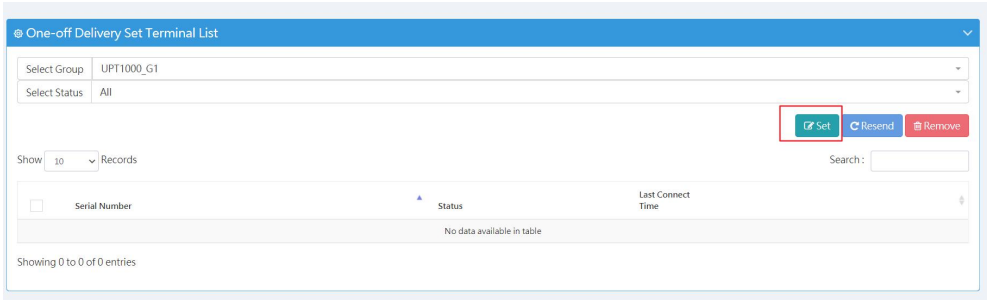


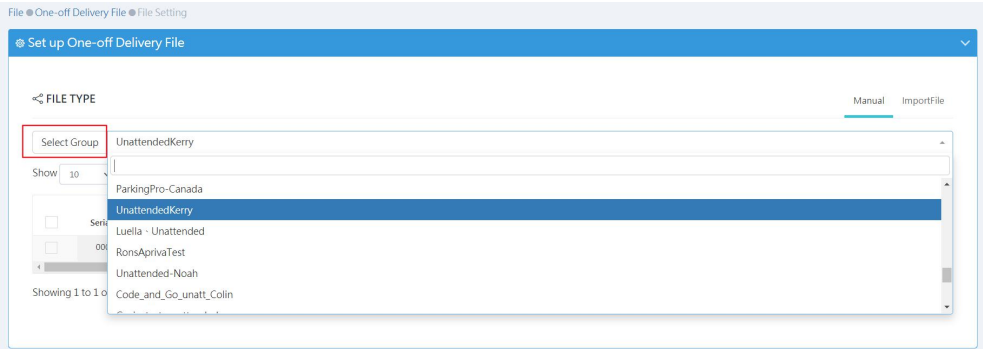
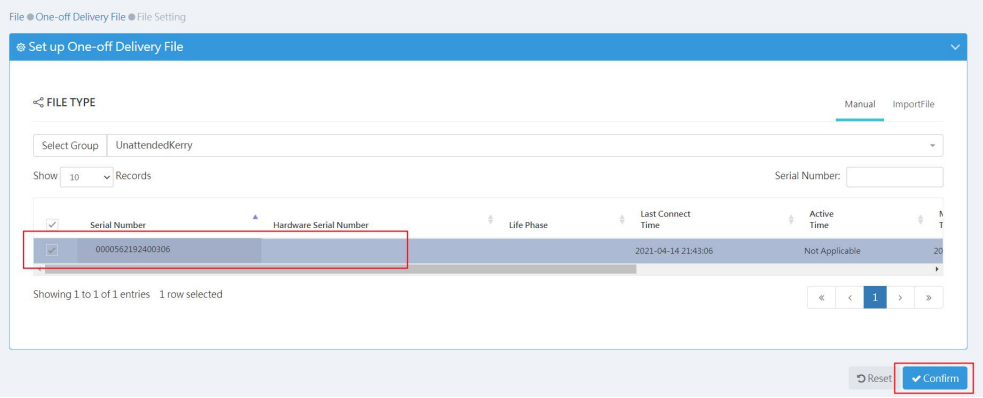
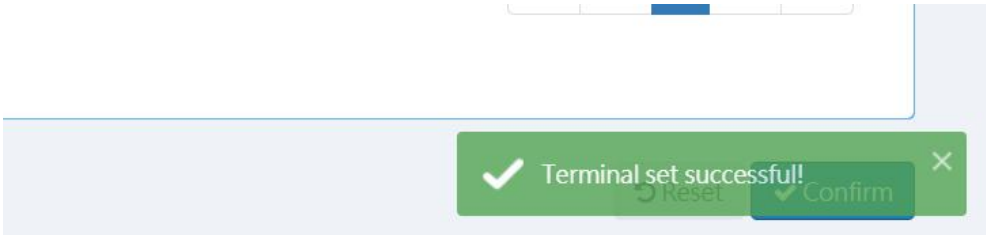
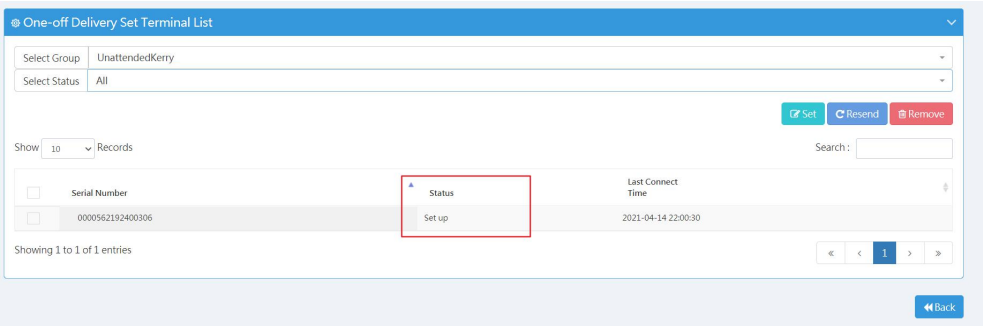
6.
- Select the executable folder “App” according to the path where you save it locally;
- Input the App Name and the App Version (The APP Name should be Code_N_Go_unatt);

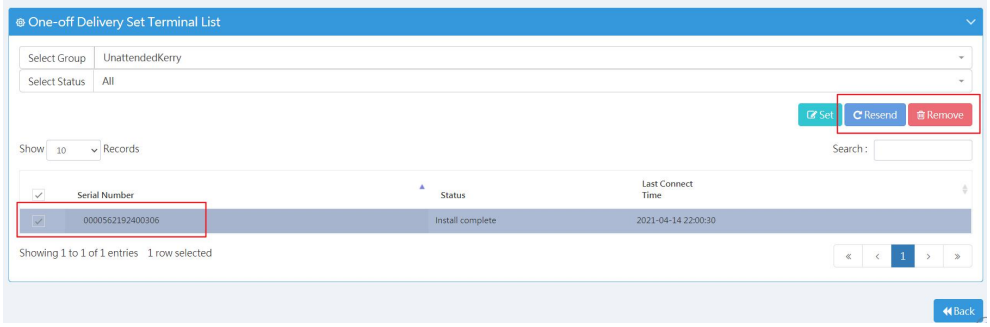
	■ Click the button “Sign Application” 
7.	When the signature is completed, a folder named “output” will be generated with three files in 
8.	Create a mmci file with the content “output\App.mci” 
9.	Compress the “ouput” folder and “update.mmci” file into a zip file. The filename can be “update.zip” and you can delete the source files after compression

	
10.	Import the zip file to CTMS website - Login CTMS management system 
11.	Point to One-off Delivery File and click File Import 
12.	Click Select File and select the ZIP file which should be the file compressed in step 9

	
13.	The file information will be displayed after imported, input the required information. Note: One-off Delivery supports different file types, but the file type will not be displayed in the information column. So Memo should be input to identify different file, as shown in the following figure. 
14.	Click Confirm button and then click OK 
15.	After the import is completed, it will prompt “One-off Delivery file create successful” or other similar message in the lower right corner of the page 

16.	Make sure that the terminal you are working with is correctly added to CTMS website; if not, follow the steps in section "Preparation on CTMS website" to complete.
17.	View the One-off Delivery file - Point to One-off Delivery File and click View 
18.	Select the Model according to the model of your terminal: UPT1000(UPT1000) or VEGA3000(V3) to filter the list 
19.	Find the file which you want to view and double click it 
20.	After turning to the File Detail page, scroll down to One-off Delivery Set Terminal List and click Set 
21.	After turning to the File Setting page, select the Group which your terminal belongs to

	
22.	Click the terminal that you want to download the One-off Delivery File, then click Confirm button 
23.	After confirmed, it will prompt “Terminal set successful” or other similar message in the lower right corner of the page 
24.	Follow the steps in section “CTMS Check” or wait until the CTMS trigger time, perform CTMS check to complete the updates.
25.	After the setting is completed, you can view the One-off Delivery File status. If the update is completed and successful, it will show “Install Complete” 
26.	If you want to Resend or Remove the One-off Delivery File from the terminal, click the terminal and click Resend or Remove. Note: Resend will reset the status of the One-off Delivery File for this terminal.



12.2. USB Function

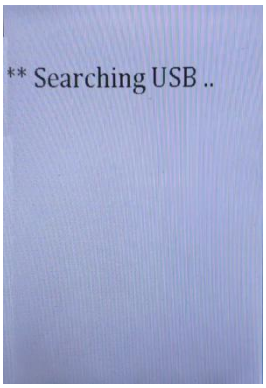
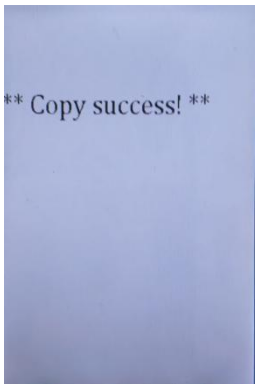
❖ For unattended application on UPT1000F terminal, the terminal supports to get the log file, update application and firmware, update parameters and update slide show through U-Disk; For that on VEGA3000P terminal, it does not support USB function.

- ■ USB Log
- ■ Update Files
- ■ Update Parameters
- ■ Update Slide Show

12.2.1. USB Log

❖ Use the chart below to get the log file through U-Disk. The terminal will copy the log files from the terminal to the U-Disk, and there will be a zip file named "logDir" in the U-Disk after copied.

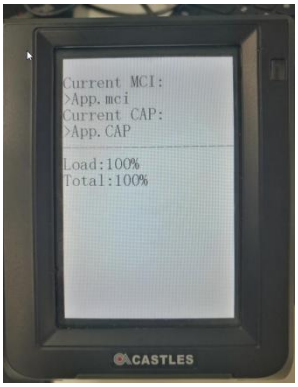
Step	Action	Display
1.	Prepare a U-Disk and copy the folder named "update" in it Note: The "update" folder can be found in the release package (typically, the path is package\4.System Config Update\USB_Update)	
2.	Insert the U-Disk to the USB Port 2 of the terminal with a USB adapter	
3.	Terminal displays USB Menu after about 10 seconds If the operation times out or user presses EXIT button, the terminal will return to idle mode	

4.	Press the button “USB Log”, terminal will search the USB and copy the file, you may see the following messages on the screen: ● Searching USB ● Found U Disk ● Copying ● Copy Success!	 
5.	Terminal returns to USB Menu	

12.2.2. Update AP, FW and Patches

❖ Use the chart below to update applications, patches and firmware through U-Disk.

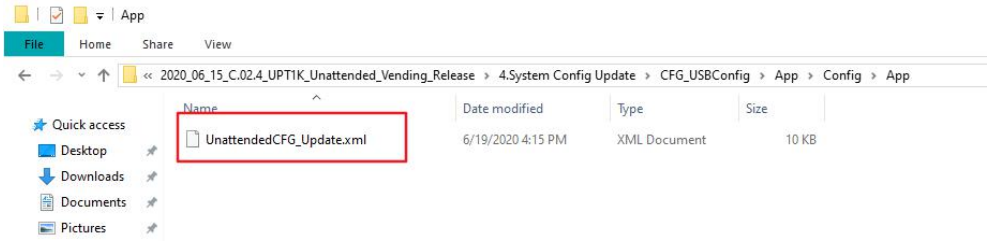
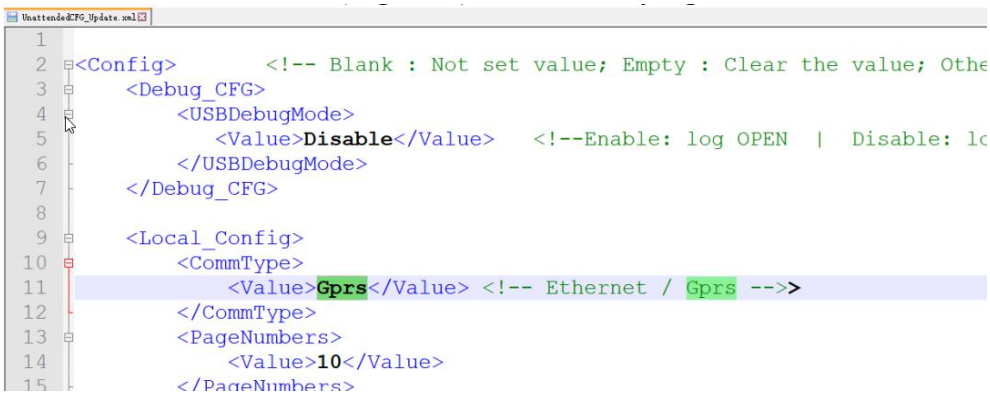
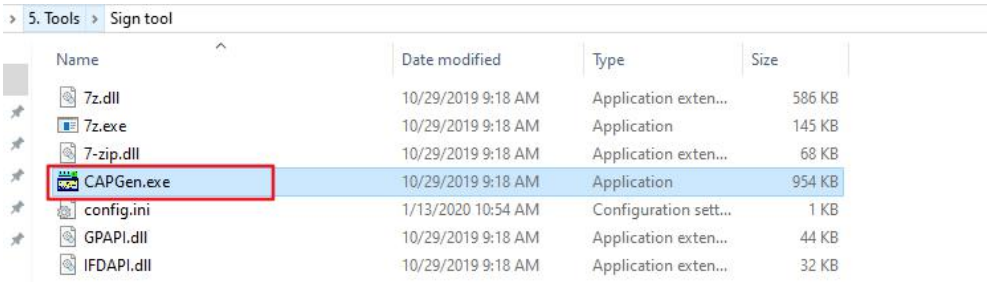
Step	Action	Display
1.	Prepare a U-Disk and copy the folder named “update” in it Note: The “update” folder can be found in the release package (typically, the path is package\4.System Config Update\USB_Update)	
2.	Insert the U-Disk to the USB Port 2 of the terminal with a USB adapter	
3.	Terminal displays the USB Menu after about 10 seconds If the operation times out or user presses EXIT button, the terminal will return to idle mode	

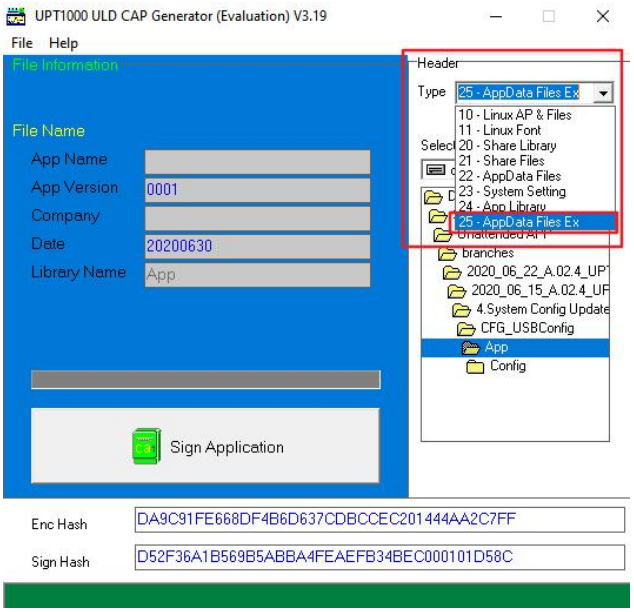
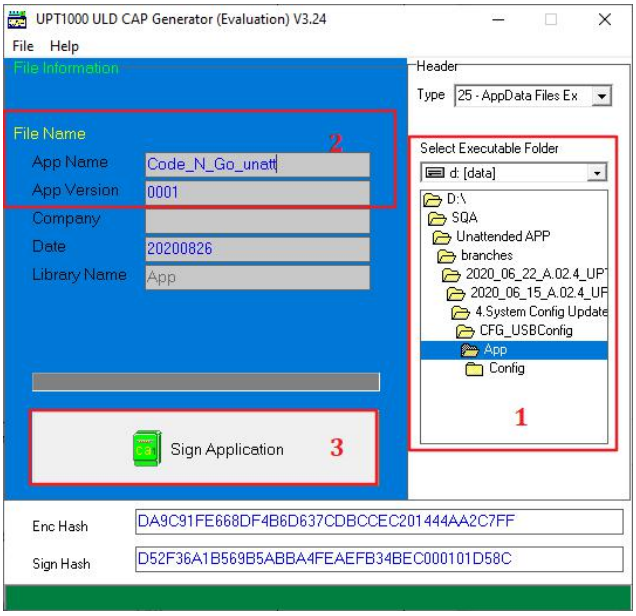
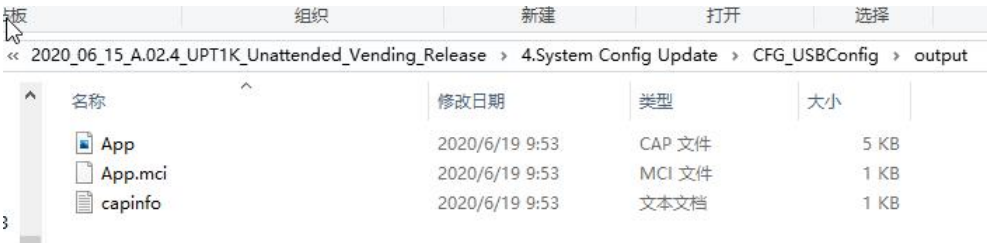
4.	Press the button “USB Update”, the terminal will prompt the user to confirm the update If the operation times out or user presses NO button, the terminal will return to USB Menu	
5.	Press YES button, the terminal will start update	
6.	Terminal enters PM interface to download the file and update it, then reboot automatically	

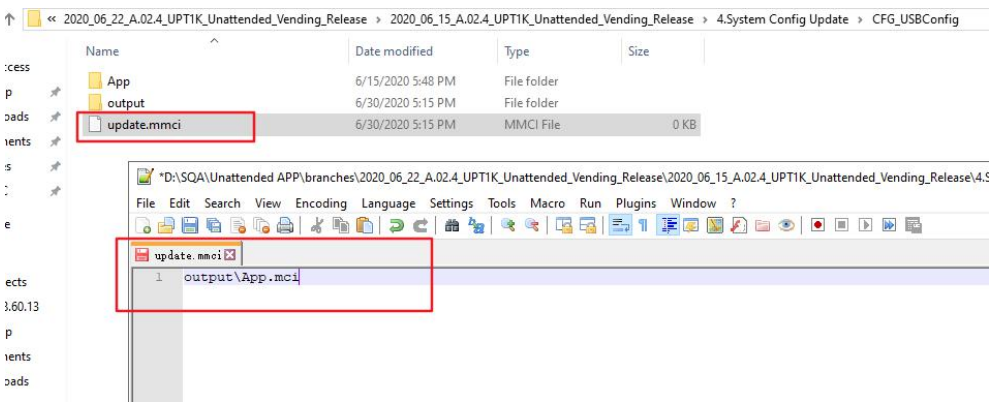
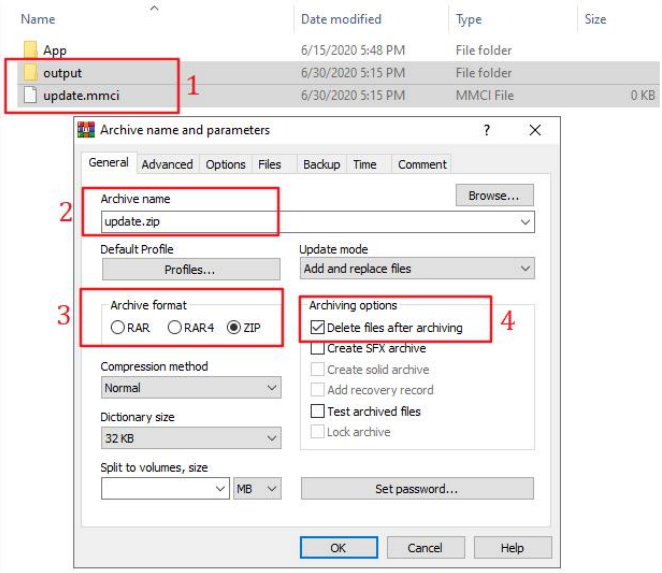
12.2.3. Update Parameters

- ❖ Use the chart below to update parameters through U-Disk. The effect of this function is same as updating the parameter file through CTMS. If you do not want to use CTMS, you can use this function.
- ➢ Update parameters through USB will update all parameters in the XML file, so make sure that all parameters in the file have the values you expect. For the definition and description of parameters, please refer to “APPENDIX B: Unattended Project Configuration Parameters”.

Step	Action & Display
1.	Copy the file named “App” to local which is for updating the configuration Note: The file “App” can be found in the release package (typically, the path is

	package\4.System Config Update\CFG_USBConfig)
2.	Find the file “UnattendedCFG_Update.xml” in the path “App\Config\App” 
3.	Edit the content of the file and save it Note: Blank (no set any values) means that it will not change the original value in the terminal after USB Update; Empty (fill in “Empty”) means that it will clear the value in the terminal after USB Update. 
4.	Double click “CAPGen.exe” to open the sign tool Note: The corresponding tool will be placed in the folder “5.Tools” of the release package 
5.	Select “25 – AppData Files” as the Type of Header

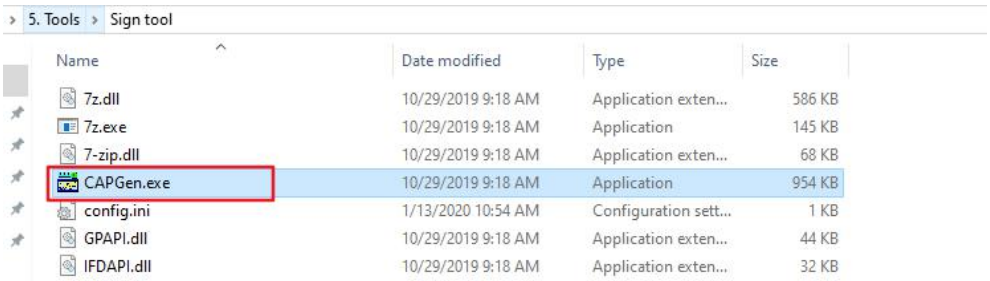
<table>
<tr><td></td><td> 
</td></tr>
<tr><td>6.</td><td>■ Select the executable folder “App” according to the path where you save it locally;
■ Input the App Name and the App Version (The APP Name should be Code_N_Go_unatt);
■ Click the button “Sign Application”
 
</td></tr>
<tr><td>7.</td><td>When the signature is completed, a folder named “output” will be generated with three files in
 
</td></tr>
<tr><td>8.</td><td>Create a mmci file with the content “output\App.mci”</td></tr>
</table>

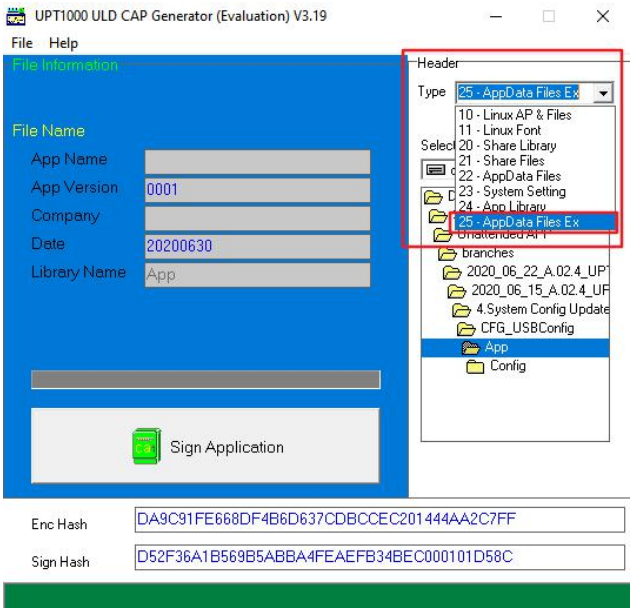
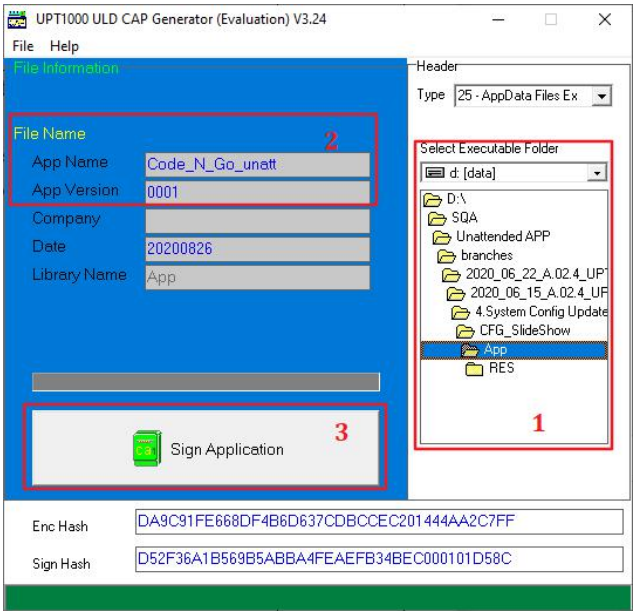
	
9.	Compress the "ouput" folder and "update.mmci" file into a zip file. The filename can be "update.zip" and you can delete the source files after compression 
10.	Copy the "update" folder which in the path "package\4.System Config Update\USB_Update" to your U-Disk, and then replace the "update.zip" file in it with the new one
11.	Insert the U-Disk to your terminal, and the next steps are same as that in the section "Update AP, FW and Patches". The terminal will restart every time parameters update.

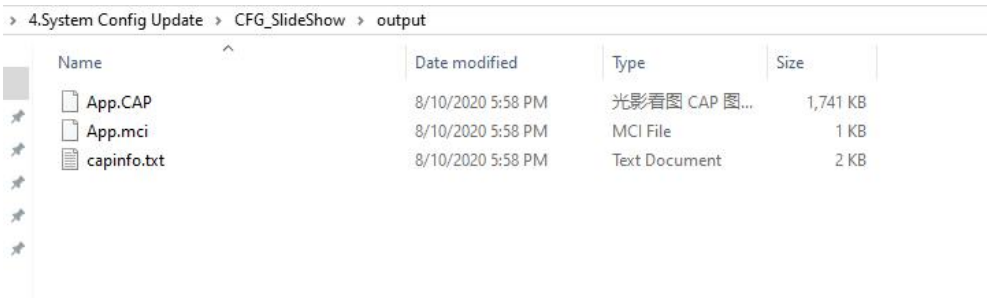
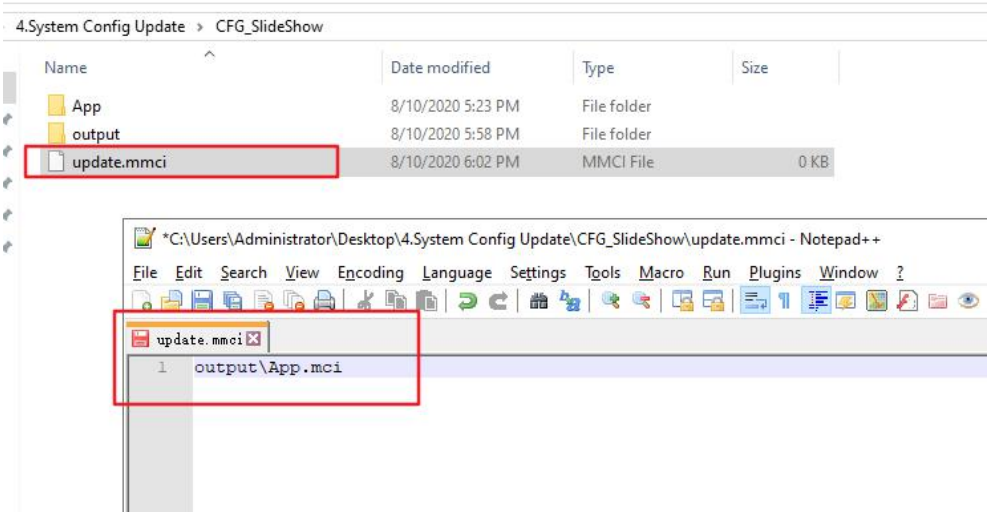
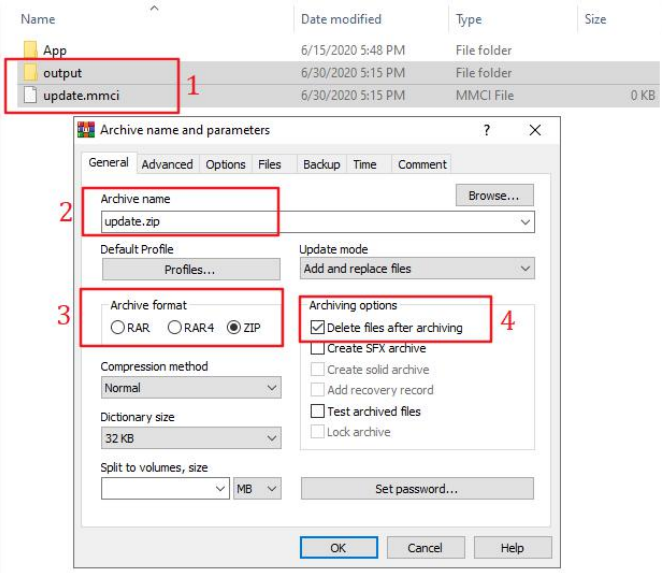
12.2.4. Update Slide Show

❖ Use the chart below to update slide show through U-Disk.

Step	Action & Display
1.	Prepare the pictures you want to play on the terminal Note: The picture format has special requirements, otherwise the Castles terminal may not be able to display pictures or happen to other problems. Here are the requirements for UPT1000F terminal: ● Picture Type: JPG

	● Dimensions: 320*360
2.	Copy the file named “App” to local which is for updating the slide show Note: The file “App” can be found in the release package (typically, the path is package\4.System Config Update\CFG_SlideShow)
3.	Find the previous pictures in the path “App\RES\Graphic\320_480\SlideShow” 
4.	Replace the previous pictures with your pictures Note: ● The picture names should not be changed ● The order in the name of the picture is also the order in which the picture is played ● If the number of pictures exceeds 10, the picture should be named like “ad_10.jpg”, “ad_11.jpg”, “ad_12.jpg” ● The default number of pictures is 10, you can change it through updating the parameter “Page Numbers”.
5.	Double click “CAPGen.exe” to open the sign tool Note: The corresponding tool will be placed in the folder “5.Tools” of the release package 
6.	Select “25 – AppData Files” as the Type of Header

	
7.	■ Select the executable folder "App" according to the path where you save it locally; ■ Input the App Name and the App Version (The APP Name should be Code_N_Go_unatt); ■ Click the button "Sign Application" 
8.	When the signature is completed, a folder named "output" will be generated with three files in

	
9.	Create a mmci file with the content “output\App.mci” 
10.	Compress the “ouput” folder and “update.mmci” file into a zip file. The filename can be “update.zip” and you can delete the source files after compression 
11.	Copy the “update” folder which in the path “package\4.System Config Update\USB_Update” to your U-Disk, and then replace the “update.zip” file in it with the new one
12.	Insert the U-Disk to your terminal, and the next steps are same as that in the section [“Update AP, FW and Patches”](#)

12.2.5. Update CAPK for Apriva

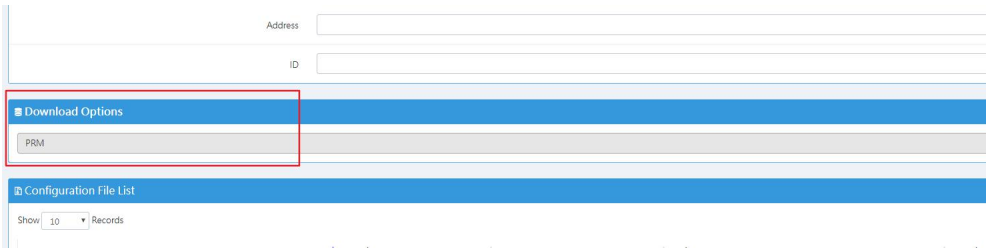
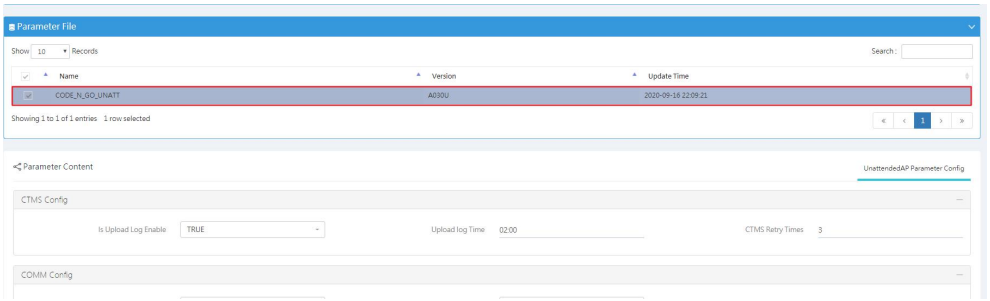
❖ The operation steps of updating CAPK through USB is same as updating parameters through USB, just the configuration file which users need to change is different. Please refer to the section "12.2.3 Update Parameters". Note that the path of "App" folder is package\4.System Config Update\CFG_USB_CAPK_Config, and the parameter files are "emv_config_Apriva.xml" and "emvcl_config_Apriva.xml".

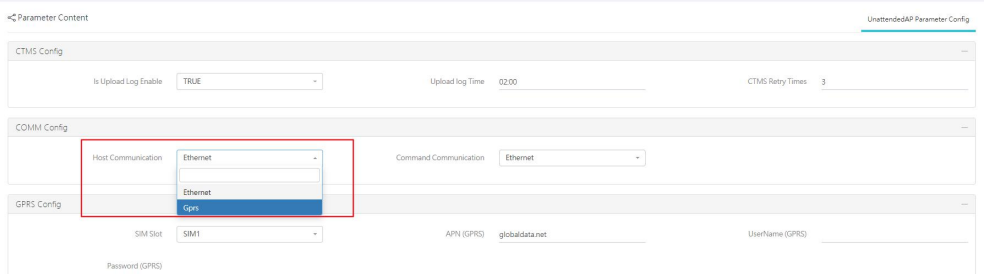
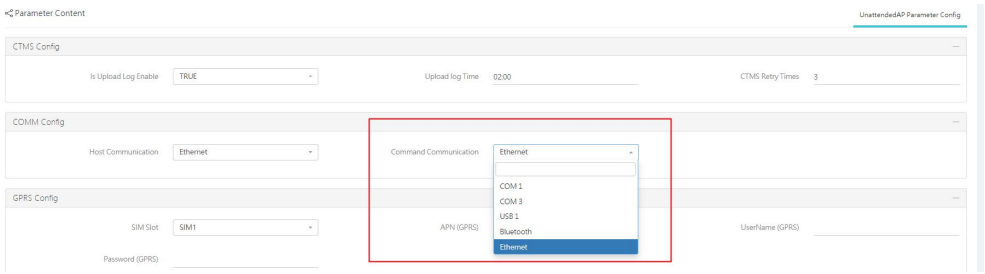
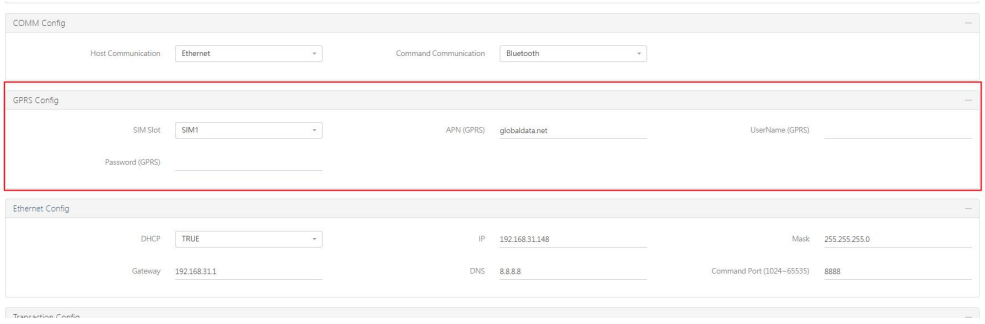
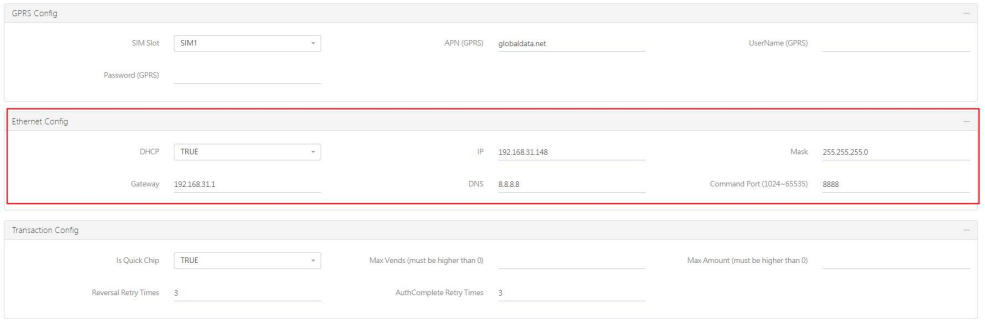
12.3. Communication Switch

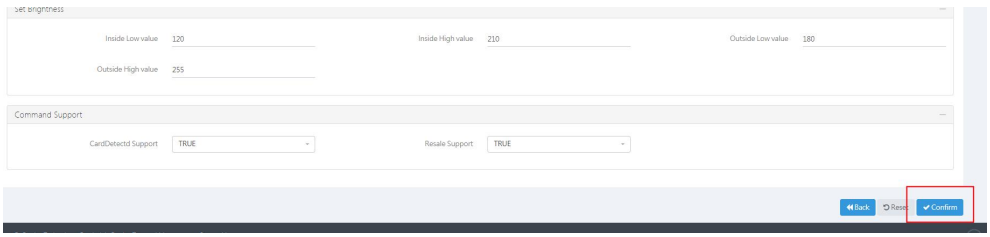
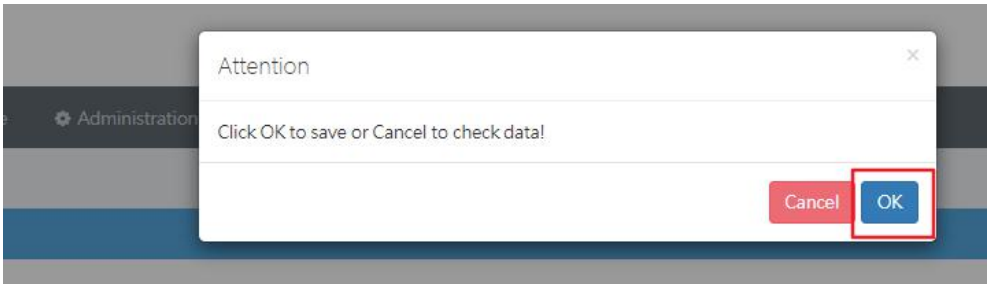
❖ It can be switched to any other type supported by the terminal, whether host communication type or command communication type. There are two parameters named "Host Communication" and "Command Communication" for users to change, please see in the annex configuration "COMM Config" to check the parameter definition.

12.3.1. Switch through CTMS

❖ Use the chart below to switch the communication type through CTMS.

Step	Action & Display
1.	Make sure that the parameter file specific for unattended application has been imported into CTMS website, and that the terminal you are working with is correctly added to CTMS website; if not, follow the steps in section "Preparation on CTMS website" to complete.
2.	Follow the steps in section "CTMS Function - Update Parameters", turn to the Terminal Modify page
3.	Scroll down to the Download Options section, make sure that the PRM option is selected 
4.	Scroll down to the Parameter File section, double click the parameter file 

5.	Scroll down to find the parameter “Host Communication” and select the type to switch to 
6.	Find the parameter “Command Communication” and select the type to switch to 
7.	If Gprs is selected, find the parameters for “GPRS Config” and fill in the correct values according to the actual situation 
8.	If Ethernet is selected, find the parameters for “Ethernet Config” and fill in the correct values according to the actual situation 
9.	Make sure that the other parameters meet your requirements. Since all parameters will be updated, it is necessary to avoid settings or functions non-conforming due to other parameter updates.
10.	Scroll down to the bottom of the page and click Confirm button

	
11.	Click OK button when prompted for attention, it will prompt "[SN: XXXX] modify successful" or other similar message 
12.	Follow the steps in section "CTMS Check", perform CTMS check to update the parameters. The message "CTMS Update OK" should be displayed in the process.

12.3.2. Switch through USB

❖ Use the chart below to switch the communication type through USB. It's only for Castles UPT1000F terminals.

Step	Action & Display
1.	Following the steps in section "USB Function - Update Parameters", open the file "UnattendedCFG_Update.xml"

2.	Find the parameter "CommType" and fill in the value corresponding to the type to switch to
	`<Config> <!-- Blank : Not set value; Empty : Clear the value; Others please refer the below -->`
	`<Debug_CFG>`
	`<USBDebugMode>`
	`<Value>Disable</Value> <!--Enable: log OPEN | Disable: log CLOSE -->`
	`</USBDebugMode>`
	`</Debug_CFG>`
	`<Local_Config>`
	`<CommType>`
	`<Value>Ethernet</Value> <!-- Ethernet / Gprs -->`
	`</CommType>`
	`<PageNumbers>`
	`<Value>10</Value>`
	`</PageNumbers>`
	`<PageInterval>`
	`<Value>1000</Value> <!-- millisecond ,default value 1000 -->`
	`</PageInterval>`
	`<Password>`
	`<Value>1234</Value> <!-- The password of entering Service Model, default value 1234(4 bytes) -->`
	`</Password>`
	`<MaxVends>`
	`<Value></Value> <!-- The maximum number of products, default blank -->`
	`</MaxVends>`
	`<MaxAmount>`
	`<Value></Value> <!-- The maximum transaction amount, default blank -->`
	`</MaxAmount>`
	`<CMDPort>`
	`<Value>0</Value> <!-- 0:com1 2:com3 4:usb_1 5:bluetooth 6:Ethernet -->`
	`</CMDPort>`

3.	Find the parameter "CMDPort" and fill in the value corresponding to the type to switch to

	`<Password>`
	`<Value>1234</Value> <!-- The password of entering Service Model, default value 1234(4 bytes) -->`
	`</Password>`
	`<MaxVends>`
	`<Value></Value> <!-- The maximum number of products, default blank -->`
	`</MaxVends>`
	`<MaxAmount>`
	`<Value></Value> <!-- The maximum transaction amount, default blank -->`
	`</MaxAmount>`
	`<CMDPort>`
	`<Value>0</Value> <!-- 0:com1 2:com3 4:usb_1 5:bluetooth 6:Ethernet -->`
	`</CMDPort>`
	`<IsQuickChip>`
	`<Value>TRUE</Value> <!-- Is support QuickChip, TRUE OR FALSE, default value TRUE -->`
	`</IsQuickChip>`
	`<ReversalRetry> <!-- Default value 3 -->`
	`<Value>3</Value>`
	`</ReversalRetry>`
	`<IsCardDetectSupport> <!-- Is support CardDetected Command -->`
	`<Value>TRUE</Value>`
	`</IsCardDetectSupport>`
	`<IsResaleSupport> <!-- Is support Re-sale Command -->`
	`<Value>TRUE</Value>`
	`</IsResaleSupport>`
	
	`</Local_Config>`

4.	If Gprs is selected, find the parameters for "GPRS Config" and fill in the correct values according to the actual situation
	`<COMM_Config> <!-- No need Modify if COMM type is not Gprs -->`
	`<EthConfig>`
	`<DHCP>TRUE</DHCP> <!-- TRUE-Dyanmic local IP, FALSE-Following static IP -->`
	`<IP></IP>`
	`<Mask></Mask>`
	`<GATEWAY></GATEWAY>`
	`<DNS>8.8.8.8</DNS>`
	`<PortForCMD>8888</PortForCMD> <!-- Network port for command is from 1024 to 65535, default value is 8888 -->`
	`</EthConfig>`
	`<GPRSConfig>`
	`<Slot>1</Slot> <!-- 1-SIM1 2-SIM2, default value: 1 -->`
	`<APN>globaldata.net</APN> <!-- default value: globaldata.net -->`
	`<UserName></UserName>`
	`<Password></Password>`
	`</GPRSConfig>`
	`</COMM_Config>`

5.	If Ethernet is selected, find the parameters for "Ethernet Config" and fill in the correct values according to the actual situation
	`<COMM_Config> <!-- No need Modify if COMM type is not Gprs -->`
	`<EthConfig>`
	`<DHCP>TRUE</DHCP> <!-- TRUE-Dyanmic local IP, FALSE-Following static IP -->`
	`<IP></IP>`
	`<Mask></Mask>`
	`<GATEWAY></GATEWAY>`
	`<DNS>8.8.8.8</DNS>`
	`<PortForCMD>8888</PortForCMD> <!-- Network port for command is from 1024 to 65535, default value is 8888 -->`
	`</EthConfig>`
	`<GPRSConfig>`
	`<Slot>1</Slot> <!-- 1-SIM1 2-SIM2, default value: 1 -->`
	`<APN>globaldata.net</APN> <!-- default value: globaldata.net -->`
	`<UserName></UserName>`
	`<Password></Password>`
	`</GPRSConfig>`
	`</COMM_Config>`

6.	Make sure that the other parameters meet your requirements. Since all parameters will be updated, it is necessary to avoid settings or functions non-conforming due to other parameter updates.
7.	Continue to follow the steps in section "USB Function - Update Parameters", complete the USB update.

13. APPENDIX A: Castles Semi-Integrated Command

13.1. REVISION HISTORY

Version	Changes	Author	Date
1.0	Creation	W Zhao	December 12, 2019
1.1	Add the “Set Data” command	W Zhao	January 02, 2020
1.2	Add the “Get Data” command	W Zhao	March 02, 2020
1.3	Remove the “Set Data” command	Brady Zhao	March 27, 2020
1.4	Add the “Card Detected” command; Add “Cancel Transaction” command	W Zhao	June 08, 2020
1.5	Add a flag in the sale response to indicate a transaction is re-sale.	W Zhao	June 15, 2020
1.6	Add flags in the sale response for emv receipt, add emv response sample	Allen Yan	June 24, 2020
1.7	Add “PreAuth” / “AuthComplete” / “CancelPreAuth” command	W Zhao	July 03, 2020
1.8	1. Add “OrigAmount” in the “AuthComplete Request” command 2. Support Token function	W Zhao	October 15, 2020
1.9	1. Add “CardType”/ “ResponseMessage” / “AuthCode” in the sale response for the Apriva host 2. Add “ResponseMessage” / “AuthCode” in the Pre-Auth response and Auth-complete response	W Zhao	November 26, 2020
2.0	Add tag “Sequence”, tag “DebitAccountType” and tag “BankResponseCode” in the sale response and pre-auth response for interact card.	W Zhao	December 24, 2020
2.1	Add tag “LocalDateTime” “TimeZone” in Sale and PreAuth response	Allen Yan	January 27, 2021
2.2	Add the “Adjust” command to support Apriva host	Allen Yan	February 09, 2021
2.3	Add “GIFT_TK2” tag in the Sale Response and PreAuth Response	Wendy Zhao	March 5, 2021
2.4	Add “LanguagePreference” tag in SaleResponse and PreAuth Response	Allen Yan	March 24, 2021

13.2. Communication Packet

13.2.1. Package Format

<STX> {Message Length} {Message Info} <ETX><LRC>

13.2.2. Control Symbol

ASCII Symbol		Description
Name	Hex Value	
STX	02h	The start of text sent by the controller to mark the start of the packet
ETX	03h	The end of text sent by the controller to mark the end of the packet
ACK	06h	The acknowledge symbol informs the packet was received correctly.
NAK	15h	The not acknowledge symbol is sent if the previous packet was not received correctly. The current session is ended.
LRC	Variable (but a single symbol)	The Longitudinal Redundancy Check is calculated by XORing all characters including the ETX symbol. The STX symbol is not included in the calculation.

13.2.3. Message Length

2 bytes' binary length of the message excluding the length field itself and <STX> <ETX> <LRC>.

The message length is used as an indicator of the length (in number of bytes) of the message. The first byte contains the quotient (in binary) of the message length (excluding the length field itself) and 256. The second byte contains the remainder of this division.

13.2.4. Message Info

Message Info is JSON format. It contains the messages which needed by the sender and receiver.

Every command should contain the "CMDType", "TXNType" and "STN" tags.

See more detail in Appendix A.

13.2.5. Protocol Handling

The communication is processed by the following method:

ACK/NAK

Both sender and receiver should check LRC to response ACK/NAK in 500ms after receiving last byte. (The interval between each byte of the same packet should be less than 50ms)

ACK, if LRC checks OK

NAK, if LRC does not match,

Sender Implementation

If send REQ/RSP packet, then wait for ACK/NAK or time out after packet is sent

Follow ACK/NAK protocol. If receive ACK then ready for next send session

Cannot send next REQ/RSP until ACK is received or timer is arrived (500ms).

Receiver Implementation

If receive buffer is empty, then filter input data as below

If ACK/NAK then notify send function

If STX then starts receiving packet assembly.

Ignore any other data received

During receiving packet assembly function

Follow packet receiving rule

If message length > max length (2000 bytes), then empty the buffer and return NAK.

If timeout (50ms) occurs and missing ETX or LRC, then ignore the data and return NAK.

Check ETX & verify LRC, send ACK/NAK based on result from LRC

If LRC is OK, then pass buffer to FW/AP for processing

13.3. Message Detail

Attributes	Definition
M	Mandatory
O	Optional
C	Conditional

13.3.1. Sale

13.3.1.1. Sale Request

Tag Name	Attributes	Value	Comments
“CMDType”	M	“Request”	
“TXNType”	M	“Sale”	
“STN”	M	“000000” – “999999”	
“TransAmount”	M	“10.00”	
“Vends”	C	3	
“Date”	M	YYMMDD	
“Time”	M	HHMMSS	
“RequestToken”	C	“TRUE”/”FALSE”	The default value in the APP is “FALSE”. When cardholder do a payment using a card, if this tag is send with the “TRUE” value, then the APP will try to get the Token of this card. and the Token value will be returned in the response message.

			(currently, only Heartland Portico USA and GP Canada support this function)
“TokenValue”	C	“335HS41MdRRioVMFPq525671”	If you want to use the Token to do the transaction, you need to fill the token value in this tag. (currently, only Heartland Portico USA and GP Canada support this function)

13.3.1.2. Sale Response

Tag Name	Attributes	Value	Comments
“CMDType”	M	“Response”	
“TXNType”	M	“Sale”	
“STN”	M	Same value with Request	
“TXNResult”	M	“Approve”	
“RspCode”	C	“00”	Will be added when the terminal gets the data from the host.
“CardBrand”	C	“VISA”	Will be added when the terminal can get this value based on the card information.
“CardNumber”	C	“**********3911”	Will be added when the terminal gets the data from the card
“STAN”	C	“000102”	Will be added when the terminal receives this value from the host
“TimeStamp”	C	“2019-12-27T07:12:50.000Z”	Will be added when the terminal receives this value from the host
“HostTXNID”	C – HL/Apriva	“1936120483”	Will be added when the terminal receives this value from the host
“POSEntryMode”	C	“INSERT” / “TAP” / “SWIPE” / “FALLBACK SWIPE”	Will be added when the terminal detected the card
“Re-Sale”	C	“TRUE” / “FALSE”	Will be added when the APP supports the “re-sale” function
“TransAmount”	M	“10.00”	If failed, the value is

			“0.00”
“AID”	C	“A0000000031010”	Application ID Number
“TSI”	C		Transaction Status Indictor
“TVR”	C		Transaction Verification Results
“IAD”	C		Issuer Application Data
“ARC”	C	“00”	Authorization Response Code
“CVR”	C	“00”	Card Verification Results
“AIDLabel”	C	“VISA Credit / Debit”	Application ID Label
“AC”	C		9F26
“TC”	C		9F26
“AAC”	C		9F26
“ATC”	C		Application Transaction Counter
“CVM”	C		Cardholder Verification Method
“LanguagePreference”	C	“fr"	Will be added if get value of tag 5F2D
“TokenValue”	C	“335HS41MdRRioVMFPq525671”	The token value of the current card. Return from the host (currently, only Heartland Portico USA and GP Canada support this function)
“CardType”	C	“Credit	“Credit” / “Debit” / “Others”
“ResponseMessage”	C	“Test Processor Success”	The response text from the host.
“AuthCode”	C	“3780167379”	The Auth code from the host.
“Sequence”	C	“000010014860”	This is the Interac sequence number.
“DebitAccountType”	C	“CHEQUING”	This is the Interac debit account type. “CHEQUING” / “SAVINGS”
“BankResponseCode”	C	“001”	Will be added when the terminal receives this value from the host.
“LocalDateTime”	M	“210127T140258”	Cashless reader datetime, Format “YYMMDDTHHMMSS”

“TimeZone”	M	“-5”	UTC-5
“GIFT_TK2”	C		This is the track 2 data of Gift Card

13.3.2. GetData

13.3.2.1. GetData Request

Tag Name	Attributes	Value	Comments
“CMDType”	M	“Request”	
“TXNType”	M	“GetData”	
“STN”	M	“000000” – “999999”	
“ModelName”	O	“”	
“SN”	O	“”	
“RTC”	O	“”	
“APPVersion”	O	“”	
“FWVersion”	O	“”	

- Note: User can specify the desired tags to return from the terminal, send the tags in the request message with empty “” value.

13.3.2.2. GetData Response

Tag Name	Attributes	Value	Comments
“CMDType”	M	“Response”	
“TXNType”	M	“GetData”	
“STN”	M	Same value with Request	
“ModelName”	O	Eg. “UPT1000F”	
“SN”	O	Serial number of the terminal, 16 digits	
“RTC”	O	Eg. “20131123143456” = 2013/11/23 14:34:56	
“APPVersion”	O	Version of the APP	
“FWVersion”	O	Version of the FW	

13.3.3. Card Detected

Tag Name	Attributes	Value	Comments
“CMDType”	M	“Notification”	
“TXNType”	M	“CardDetected”	
“STN”	M	“000000” – “999999”	
“POSEntryMode”	M	“INSERT” / “TAP” / “SWIPE” / “FALLBACK SWIPE”	

13.3.4. CancelTransaction (Cancel the transaction before the card detected)

13.3.4.1. CancelTXN Request

Tag Name	Attributes	Value	Comments
“CMDType”	M	“Request”	
“TXNType”	M	“CancelTXN”	
“STN”	M	“000000” – “999999”	

13.3.4.2. CancelTXN Response

Tag Name	Attributes	Value	Comments
“CMDType”	M	“Response”	
“TXNType”	M	“CancelTXN”	
“STN”	M	Same value with Request	
“CancelResult”	M	“Approve” / “Decline”	

13.3.5. Pre-Auth

13.3.5.1. PreAuth Request

Tag Name	Attributes	Value	Comments
“CMDType”	M	“Request”	
“TXNType”	M	“PreAuth”	
“STN”	M	“000000” – “999999”	
“TransAmount”	M	“20.00”	
“Date”	M	YYMMDD	
“Time”	M	HHMMSS	
“RequestToken”	C	“TRUE”/”FALSE”	The default value in the APP is “FALSE”. When cardholder do a payment using a card, if this tag is send with the “TRUE” value, then the APP will try to get the Token of this card. and the Token value will be returned in the response message. (currently, only Heartland Portico USA and GP Canada support this function)
“TokenValue”	C	“335HS41MdRRio VMFPq525671”	If you want to use the Token to do the transaction, you need to fill the token value in this tag. (currently, only Heartland Portico USA and GP Canada support this function)

13.3.5.2. PreAuth Response

Tag Name	Attributes	Value	Comments
“CMDType”	M	“Response”	
“TXNType”	M	“PreAuth”	
“STN”	M	Same value with Request	
“TXNResult”	M	“Approve”	
“TransAmount”	M	“20.00”	Amount approved in the host. If failed, the value is “0.00”
“RspCode”	C	“00”	Will be added when the terminal get the data from the host.
“CardBrand”	C	“VISA”	Will be added when the terminal can get this value based on the card information.
“CardNumber”	C	“**********3911”	Will be added when the terminal get the data from the card
“STAN”	C	“000102”	Will be added when the terminal receives this value from the host
“TimeStamp”	C	“2019-12-27T07:12:50.000Z”	Will be added when the terminal receives this value from the host
“HostTXNID”	C	“1936120483”	Will be added when the terminal receives this value from the host. it used for heartland. Need to be added in the Auth-Complete request or the CancelPreAuth request.
“POSEntryMode”	C	“INSERT” / “TAP” / “SWIPE” / “FALLBACK SWIPE”	Will be added when the terminal detected the card
“AID”	C	“A0000000031010”	Application ID Number
“TSI”	C		Transaction Status Indictor
“TVR”	C		Transaction Verification Results
“IAD”	C		Issuer Application Data
“ARC”	C	“00”	Authorization Response Code
“CVR”	C	“00”	Card Verification Results
“AIDLabel”	C	“VISA Credit Debit”	Application ID Label
“AC”	C		9F26
“TC”	C		9F26

“AAC”	C		9F26
“ATC”	C		Application Transaction Counter
“CVM”	C		Cardholder Verification Method
“LanguagePreference”	C	“fr”	Will be added if get value of tag 5F2D
“TokenValue”	C	“335HS41MdRRioVMFPq525671”	If you want to use the Token to do the transaction, you need to fill the token value in this tag. (currently, only Heartland Portico USA and GP Canada support this function)
“ResponseMessage”	C	“Test Processor Success”	The response text from the host.
“AuthCode”	C	“3780167379”	The Auth code from the host
“Sequence”	C	“000010014860”	This is the Interac sequence number. --reserved
“DebitAccountType”	C	“CHEQUING”	This is the Interac debit account type. “CHEQUING” / “SAVINGS”. ---reserved
“BankResponseCode”	C	“001”	Will be added when the terminal receives this value from the host.
“LocalDateTime”	M	“210127T140258”	Cashless reader datetime, Format “YYMMDDTHHMMSS”
“TimeZone”	M	“-5”	UTC-5
“GIFT_TK2	C		This is the track 2 data of Gift Card

13.3.6. Auth-Complete

13.3.6.1. AuthComplete Request

Tag Name	Attributes	Value	Comments
“CMDType”	M	“Request”	
“TXNType”	M	“AuthComplete”	
“STN”	M	“000000” – “999999”	
“TransAmount”	M	“15.00”	The Auth-complete amount
“HostTXNID”	C	“1936120483”	Must be added if the transaction host is heartland
“OrigAmount”	M	“20.00”	The amount of PreAuth transactions

13.3.6.2. AuthComplete Response

Tag Name	Attributes	Value	Comments
“CMDType”	M	“Response”	
“TXNType”	M	“AuthComplete”	
“TXNResult”	M	“Approve”	
“STN”	M	Same value with Request	
“RspCode”	M	“00”	
“TimeStamp”	O	“2018-04-23T02:54:06”	
“HostTXNID”	O	“1936120483”	
“TransAmount”	O	“20.00”	Amount approved in the host. If failed, the value is “0.00”

13.3.7. Cancel Pre-Auth (Reversal)

13.3.7.1. CancelPreAuth Request

Tag Name	Attributes	Value	Comments
“CMDType”	M	“Request”	
“TXNType”	M	“CancelPreAuth”	
“STN”	M	“000000” – “999999”	
“OrigAmount”	M	“20.00”	
“CancelAmount”	M	“20.00”	
“Date”	M	YYMMDD	
“Time”	M	HHMMSS	
“HostTXNID”	C	“1936120483”	Must be added if the transaction host is heartland

13.3.7.2. CancelPreAuth Response

Tag Name	Attributes	Value	Comments
“CMDType”	M	“Response”	
“TXNType”	M	“CancelPreAuth”	
“TXNResult”	M	“Approve”	
“STN”	M	Same value with Request	
“RspCode”	M	“00”	
“TimeStamp”	O	“2018-04-23T02:54:06”	
“HostTXNID”	O	“1936120483”	
“TransAmount”	O	“20.00”	Amount approved in the host. If failed, the value is “0.00”

13.3.8. Adjust

13.3.8.1. Adjust Request

- Note: This command support Apriva host only and not support campus card

Tag Name	Attributes	Value	Comments
“CMDType”	M	“Request”	
“TXNType”	M	“Adjust”	
“STN”	M	“000000” – “999999”	
“TransAmount”	M	“20.00”	Not support zero or less zero
“HostTXNID”	M	“1936120483”	Must be same as transaction to be adjusted

13.3.8.2. Adjust Response

Tag Name	Attributes	Value	Comments
“CMDType”	M	“Response”	
“TXNType”	M	“Adjust”	
“STN”	M	“000000” – “999999”	Same value with Request
“HostTXNID”	M	“1936120483”	Same value with Request
“RspCode”	C	“00”	Will be added when the terminal get the data from the host.
“ResponseMessage”	C	“Test Processor Success”	The response text from the host.
“TimeStamp”	C	“2018-04-23T02:54:06”	Will be added when the terminal get the data from the host.
“AuthCode”	C	“3780167379”	The Auth code from the host.

13.4. Appendix A – Tag List

Tag Name	Format	Description
CMDType	String	The type of this command. “Notification” “Request” “Response”
TXNType	String	The transaction type of this command. See more details in Appendix B
STN	String(6)	“000000” – “999999”

		This Tag is used for the POS to check if response corresponds to request. The sender will manage this data. Receiver will copy this data from the request message to the response message.
TransAmount	String E.g. “10.00”	The amount of the transaction. A decimal point is required to separate integer and decimal places.
Vends	INT E.g. 3	Total number of items.
Date	String --- YYMMDD	The date of the CMD
Time	String --- HHMMSS	The time of the CMD
TXNResult	String	The result of the transaction. See more details in Appendix C
RspCode	String	The response code of the host.
CardBrand	String	See more details in Appendix D.
CardNumber	String	Masked card number
TimeStamp	String	A timestamp
STAN	String	System Trace Audit Number(Create locally)
HostTXNID	String	Gateway transaction ID(Create in host)
Exception	String	reply to this label when the terminal unable to process the request. Value list： “CMD format error” “unknown exception”
“ModelName”	String	The model name of the terminal. E.g. “UPT1000F”
“SN”	String (16)	The serial number of the terminal.
“RTC”	String	E.g. “20131123143456” = 2013/11/23 14:34:56
“APPVersion”	String	The version of the APP
“FWVersion”	String	The version of the FW
“POSEntryMode”	String	“INSERT” / “TAP” / “SWIPE” / “FALLBACK SWIPE”
“CancelResult”	String	“Approve” / “Decline”
“Re-Sale”	String	“True”/ “False” This function is configurable. If the customer support the re-sale function, then in the sale response, we need to add this tag.
“OrigAmount”	String	The amount of PreAuth transaction which you want to reversal.

“CancelAmount”	String	The amount you want to reversal.
“RequestToken”	String	“TRUE”/ “FALSE” The default value in the APP is “FALSE”. When cardholder do a payment using a card, if this tag is send with the “TRUE” value, then the APP will try to get the Token of this card. and the Token value will be returned in the response message. (currently, only Heartland Portico USA and GP Canada support this function)
“TokenValue”	String	The token value which response from the host. (currently, only Heartland Portico USA and GP Canada support this function)
“CardType”	String	“Credit” / “Debit” / “Others”
“ResponseMessage”	String	The response message from the host. Example: “Test Processor Success”
“AuthCode”	String	“3780167379”
“Sequence”	String	This is the Interac sequence number.
“DebitAccountType”	String	This is the Interac debit account type. “CHEQUING” / “SAVINGS”.
“BankResponseCode”	String	The Bank response code of the host.
“GIFT_TK2”	String	
“LanguagePreference”	String	5F2D

13.5. Appendix B – TXNType List

TXNType	Comments
“Sale”	
“GetData”	
“CancelTXN”	
“CardDetected”	
“PreAuth”	
“AuthComplete”	
“CancelPreAuth”	

13.6. Appendix C – TXNResult List

TXNResult	Comments
“Approve”	
“DeclinebyHost”	Card is declined by the transaction host
“DeclinebyLocal”	
“Cancel-TimeOut”	Transaction is canceled due to the operation timed out
“Cancel-Button”	Transaction is canceled due to the user presses cancel button

“Decline-SelectionOverLimit”	The price of selected product exceeds the amount limit
“TransactionFail”	
“Decline-AmountNotSupport”	

13.7. Appendix D – Card Brand

Short name in the message	Description
“VISA”	VISA
“MC”	MasterCard
“AMEX”	American Express
“DISC”	Discover
“Inter”	Interact

13.8. Appendix E – Example

13.8.1. Sale

sale request

```
{
    “CMDType”: “Request”,
    “TXNType”: “Sale”,
    “STN”: “123456”,
    “TransAmount”: “10.00”,
    “Vends”: 3,
    “Date”: “191225”,
    “Time”: “153029”
}
```

sale request with transAmount 0(to get token)

```
{
    "CMDType": "Request",
    "TXNType": "Sale",
    "STN": "123456",
    "TransAmount": "0.00",
    "Date": "191225",
    "Time": "153029",
    "RequestToken ": "TRUE"
}
```

sale response 1 (no emv data)

```
{
    “CMDType”: “Response”,
    “TXNType”: “Sale”,
```

“STN”: “123456”,
“TXNResult”: “Approve”,
“RspCode”: “00”,
“CardBrand”: “VISA”,
“CardNumber”: “**********3911”,
“STAN”: “000102”,
“TxnID”: “1936120483”,
“TimeStamp”: “2019-12-27T07:12:50.000Z”,
“Re-Sale”: “FALSE”,
“TokenValue”: “335HS41MdRRioVMFPq525671”, //if RequestToken is TRUE
“TransAmount”: “10.00”,
“LocalDateTime”: “210127T140258”
“TimeZone”: “-5”
}

sale response 2（include emv data）

{
"CMDType": "Response",
"TXNType": "Sale",
"STN": "000001",
"TXNResult": "Approve",
"RspCode": "00",
"Re-Sale": "FALSE",
"TransAmount": "1.00",
"CardNumber": "**********4111",
"CardBrand": "MC",
"TimeStamp": "2020-07-22T22:41:43.5270752",
"HostTXNID": "1329731050",
"POSEntryMode": "INSERT",
"CardType": "DEBIT",
"ResponseMessage": "APPROVED 000APPROVED 858465",
"AuthCode": "858465",
"BankResponseCode": "001",
"AID": "A0000000041010",
"TSI": "E800",
"TVR": "0000208800",
"IAD": "01102040006A0000C58C00000000000000FF",
"ARC": "5A33",
"AIDLabel": "4D415354455243415244",
"AC": "F349F7DD66DF9F17",
"ATC": "06B4",
"CVM": "1F0302",
"TokenValue": "335HS41MdRRioVMFPq525671", //if RequestToken is TRUE
"LocalDateTime": "210127T140258",

"TimeZone ": "-5",
"LanguagePreference": "fr"
}

sale response 3（include emv data for Interac）

{
"CMDType": "Response",
"TXNType": "Sale",
"STN": "123456",
"TXNResult":"Approve",
"RspCode": "00",
"Re-Sale": "FALSE",
"TransAmount": "10.00",
"CardNumber": "**********1933",
"CardBrand": "Inter",
"TimeStamp": "2020-12-30T09:42:28.8124845",
"HostTXNID": "1350626776",
"POSEntryMode": "INSERT",
"CardType": "DEBIT",
"ResponseMessage": "APPROVED 000APPROVED 858465",
"AuthCode": "858465",
"BankResponseCode": "001",
"Sequence": "000010015110",
"DebitAccountType": "CHEQUING",
"AID": "A0000002771010",
"TSI": "6800",
"TVR": "8000008000",
"IAD": "06010A0364AC00",
"ARC": "3030",
"AIDLabel": "494E5445524143",
"TC": "3C4DD1F2ADFBDF91",
"ATC": "002D",
"CVM": "410302",
"TokenValue": "335HS41MdRRioVMFPq525671", //if RequestToken is TRUE
"LocalDateTime": "210127T140258",
" TimeZone ": "-5"
}

13.8.2. GetData

getdata request

{
“CMDType”: “Request”,
“TXNType”: “GetData”,
“STN”: “000001”,

"ModelName": "",
"SN": "",
"RTC": "",
"APPVersion": "",
"FWVersion": ""
}

getdata response

{
"CMDType": "Response",
"TXNType": "GetData",
"STN": "000001",
"ModelName": "UPT1000F",
"SN": "0000512182100004",
"RTC": "20200302044755",
"APPVersion": "0.01.6",
"FWVersion": "VRAB12-20191206"
}

13.8.3. Card Detected

card detected notification

{
"CMDType": "Notification",
"TXNType": "CardDetected",
"STN": "000002",
"POSEntryMode": "SWIPE"
}

13.8.4. Cancel Transaction

cancel transaction request

{
"CMDType": "Request",
"TXNType": "CancelTXN",
"STN": "000005"
}

cancel transaction response

{
"CMDType": "Response",
"TXNType": "CancelTXN",
"STN": "000005",
"CancelResult": "Approved"
}

13.8.5. Re-Sale

Re-sale request


```
{
    “CMDType”: “Request”,
    “TXNType”: “Sale”,
    “STN”: “000006”,
    “Amount”: “1.25”,
    “Date”: “191225”,
    “Time”: “123010”
}
```


Re-sale response


```
{
    “CMDType”: “Response”,
    “TXNType”: “Sale”,
    “STN”: “000006”,
    “TXNResult”: “Approve”,
    “RspCode”: “00”,
    “TxnID”: “1323664844”,
    “Re-Sale”: “TRUE”,
    “CardNumber”: “************4111”,
    “CardBrand”: “MC”,
    “TimeStamp”: “2020-06-20T03:21:05.172421”,
    “POSEntryMode”: “TAP”
    “Amount”: “1.25”
}
```


13.8.6. Pre-Auth

Pre-Auth request


```
{
    “CMDType”: “Request”,
    “TXNType”: “PreAuth”,
    “STN”: “000002”,
    “TransAmount”: “10.00”,
    “Date”: “191225”,
    “Time”: “123010”
}
```


Pre-Auth request transAmount 0(to get token)


```
{
    "CMDType": "Request",
    "TXNType": "PreAuth",
```

"STN": "000002",
"TransAmount": "0.00",
"Date": "191225",
"Time": "123010",
"RequestToken ": "TRUE"
}

Pre-Auth response 1 (no emv data)

{
"CMDType": "Response",
"TXNType": "PreAuth",
"STN": "000002",
"TXNResult": "Approve",
"TransAmount": "10.00",
"RspCode": "00",
"CardBrand": "VISA",
"CardNumber": "**********6781",
"TimeStamp": "2020-07-16T21:13:50.0513789",
"HostTXNID": "1329097621",
"TokenValue": "335HS41MdRRioVMFPq525671", //if RequestToken is TRUE
"POSEntryMode": "SWIPE",
"LocalDateTime": "210127T140258",
"TimeZone": "-5"
}

Pre-Auth response 2 (include emv data)

{
"CMDType": "Response",
"TXNType": "PreAuth",
"STN": "000003",
"TXNResult": "Approve",
"TransAmount": "10.00",
"RspCode": "00",
"CardBrand": "VISA",
"CardNumber": "**********0119",
"TimeStamp": "2020-07-20T02:04:25.2524863",
"HostTXNID": "1329506585",
"POSEntryMode": "TAP",
"ResponseMessage": "APPROVED 000APPROVED 858465",
"AuthCode": "858465",
"BankResponseCode": "001",
"TSI": "0000",
"TVR": "0000000000",
"IAD": "06010A03A00000",

"AIDLabel": "5649534120435245444954",
"TC": "14432E053BD1727B",
"ATC": "0185",
"CVM": "3F0000",
"TokenValue": "335HS41MdRRioVMFPq525671", //if RequestToken is TRUE
"LocalDateTime": "210127T140258",
"TimeZone": "-5",
“LanguagePreference”: “fr”
}

13.8.7. Auth-Complete

Auth-Complete request

{
“CMDType”: “Request”,
“TXNType”: “AuthComplete”,
“STN”: “000002”,
“TransAmount”: “5.00”,
“HostTXNID”: “1329097621”,
}

Auth-Complete response

{
“CMDType”: “Response”,
“TXNType”: “AuthComplete”,
“STN”: “000002”,
“TXNResult”: “Approve”,
“RspCode”: “00”,
“TimeStamp”: “2020-07-16T21:17:25.5322221”,
“HostTXNID”: “1329096534”,
“TransAmount”: “5.00”
}

13.8.8. Cancel Pre-Auth

Cancel Pre-Auth request

{
“CMDType”: “Request”,
“TXNType”: “CancelPreAuth”,
“STN”: “000002”,
“OrigAmount”: “10.00”,
“CancelAmount”: “5.00”,
“Date”: “191225”,
“Time”: “123010”,
“HostTXNID”: “1329097621”,

}

Cancel Pre-Auth response

{
“CMDType”: “Response”,
“TXNType”: “CancelPreAuth”,
“STN”: “000002”,
“TXNResult”: “Approve”,
“RspCode”: “00”,
“TimeStamp”: “2020-07-16T21:19:23.9589411”,
“HostTXNID”: “1329096538”,
“TransAmount”: “5.00”
}

13.8.9. Adjust

Adjust request

{
"CMDType": "Request",
"TXNType": "Adjust ",
"STN": "123456",
"TransAmount": "10.00",
"HostTXNID": "1329096538"
}

Adjust response

{
"CMDType": "Response",
"TXNType": "Adjust",
"STN": "123456",
"HostTXNID": "1329096538",
"RspCode": "00",
"ResponseMessage": "Test Processor Success",
"TimeStamp": "2020-07-16T21:19:23.9589411",
"AuthCode": "3789959479"
}

13.8.10. Gift Card

Sale Request

{
"CMDType": "Request",
"TXNType": "Sale",
"STN": "123456",
"TransAmount": "10.00",

"Vends": 3,
"Date": "191225",
"Time": "153029"
}

Sale Response

{
"CMDType": "Response",
"TXNType": "Sale",
"STN": "123456",
"TXNResult": "Approve",
"Re-Sale": "FALSE",
"TransAmount": "0.00",
"GIFT_TK2": ";604958001751006=24122011502123450000?",
"LocalDateTime": "210305T020813",
"TimeZone": "-5"
}

Auth Request

{
"CMDType": "Request",
"TXNType": "PreAuth",
"STN": "000002",
"TransAmount": "10.00",
"Date": "191225",
"Time": "123010"
}

Auth Response

{
"CMDType": "Response",
"TXNType": "PreAuth",
"STN": "000002",
"TXNResult": "Approve",
"TransAmount": "0.00",
"GIFT_TK2": ";604958001751006=24122011502123450000?",
"LocalDateTime": "210305T020908",
"TimeZone": "-5"
}

14. APPENDIX B: Unattended Project Configuration Parameters

- This chapter lists and describes all the parameters in unattended application, which can be updated by CTMS or USB.
- The parameter names and details of the following parameters are consistent with the parameters on CTMS. So when you want to do USB Update, please refer to the comments in the USB XML file to modify the parameters.

14.1. Parameter List

- The Parameter List lists all the basic parameters, for user to quickly view the name, mode and module of the parameters on CTMS. Then user can learn more about the parameters in the next section "14.2 Parameters Detail" according to the module to which the parameter belongs.

No.	Name in CTMS	Group / Terminal Mode		Module
		Apriva	Heartland Portico USA & GP Canada	
1	Is Upload Log Enable	Terminal	Terminal	CTMS Config
2	Upload log Time	Terminal	Terminal	CTMS Config
3	CTMS Host	Terminal	Terminal	CTMS Config
4	CTMS UAT Address	Group	Group	CTMS Config
5	CTMS Product Address	Group	Group	CTMS Config
6	CTMS Port	Group	Group	CTMS Config
7	CTMS Retry Times	Terminal	Terminal	CTMS Config
8	Host Communication	Terminal	Terminal	COMM Config
9	Command Communication	Terminal	Terminal	COMM Config
10	SIM Slot	Terminal	Terminal	GPRS Config
11	APN (GPRS)	Terminal	Terminal	GPRS Config
12	UserName (GPRS)	Terminal	Terminal	GPRS Config
13	Password (GPRS)	Terminal	Terminal	GPRS Config
14	DHCP	Terminal	Terminal	Ethernet Config
15	IP	Terminal	Terminal	Ethernet Config
16	Mask	Terminal	Terminal	Ethernet Config
17	Gateway	Terminal	Terminal	Ethernet Config
18	DNS	Terminal	Terminal	Ethernet Config
19	Command Port	Terminal	Terminal	Ethernet Config
20	Is Quick Chip	Terminal	Terminal	Transaction Config
21	Max Vends (must be higher than	Terminal	Terminal	Transaction Config

	0)			
22	Max Amount (must be higher than 0)	Terminal	Terminal	Transaction Config
23	Reversal Retry Times	Terminal	Terminal	Transaction Config
24	AuthComplete Retry Times	Terminal	Terminal	Transaction Config
25	Transaction Environment	Terminal	Terminal	Transaction Config
26	VI01 (Visa)	Terminal	/	Card Bin Range Config
27	MC01 (MasterCard)	Terminal	/	Card Bin Range Config
28	AX01 (American Express)	Terminal	/	Card Bin Range Config
29	DS01 (Discover)	Terminal	/	Card Bin Range Config
30	Maestro (Maestro)	Terminal	/	Card Bin Range Config
31	MSTAR01 (Military Star)	Terminal	/	Card Bin Range Config
32	URL	/	Group	Host Config for Heartland
33	HLLicenseId	/	Terminal	Host Config for Heartland
34	HLSiteId	/	Terminal	Host Config for Heartland
35	HLDeviceId	/	Terminal	Host Config for Heartland
36	HLUserName	/	Terminal	Host Config for Heartland
37	HLPassword	/	Terminal	Host Config for Heartland
38	HLUniqueDeviceId	/	Terminal	Host Config for Heartland
39	HLTxnDescriptor	/	Terminal	Host Config for Heartland
40	HLDeveloperID	/	Terminal	Host Config for Heartland
41	HLVersionNbr	/	Terminal	Host Config for Heartland
42	HLVoltageFlag	/	Terminal	Host Config for Heartland

43	AprivaTokenURL	Group	/	Host Config for Apriva
44	AprivaVoidURL	Group	/	Host Config for Apriva
45	AprivaCashSaleURL	Group	/	Host Config for Apriva
46	AprivaChargeURL	Group	/	Host Config for Apriva
47	AprivaPostAuthURL	Group	/	Host Config for Apriva
48	AprivaReversalURL	Group	/	Host Config for Apriva
49	AprivaAdjustURL	Group	/	Host Config for Apriva
50	APClientID	Terminal	/	Host Config for Apriva
51	APSecret	Terminal	/	Host Config for Apriva
52	APAcceptType	Group	/	Host Config for Apriva
53	APMethod	Group	/	Host Config for Apriva
54	APTokenContentTyp e	Group	/	Host Config for Apriva
55	APTokenScope	Group	/	Host Config for Apriva
56	APTokenAccessURI	Group	/	Host Config for Apriva
57	APTokenAuthorizati on	Group	/	Host Config for Apriva
58	APTxnPlatformKey V1	Group	/	Host Config for Apriva
59	APTxnPlatformKey V2	Group	/	Host Config for Apriva
60	APTxnAgent	Group	/	Host Config for Apriva
61	APTxnAprivaSDK	Group	/	Host Config for Apriva
62	APTxnAuthorization	Group	/	Host Config for Apriva
63	APTxnContentType	Group	/	Host Config for Apriva
64	APCREncDataProfil e	Group	/	Host Config for Apriva

65	APCRName	Group	/	Host Config for Apriva
66	APCREMVCapable	Terminal	/	Host Config for Apriva
67	APAllowPartialAuth	Terminal	/	Host Config for Apriva
68	APRegisterIdentifier	Terminal	/	Host Config for Apriva
69	Is NTP Enable	Terminal	Terminal	NTP Server
70	Time Zone	Terminal	Terminal	NTP Server
71	NTP URL	Terminal	Terminal	NTP Server
72	NTP Frequency (days)	Terminal	Terminal	NTP Server
73	NTP Time (hh:mm)	Terminal	Terminal	NTP Server
74	Page Numbers (3~32)	Group	Group	Local Config
75	Page Switching Interval (millisecond)	Group	Group	Local Config
76	Service Mode Password (4 Bytes)	Terminal	Terminal	Local Config
77	Max Days to save log (1~10)	Terminal	Terminal	Local Config
78	Speaker	Terminal	Terminal	Local Config
79	Reader Card	/	Terminal	Local Config
80	Is Close Receipt Tips	/	Terminal	Local Config
81	Is Show French First	/	Terminal	Local Config
82	User Operation Timeout (sec)	Terminal	Terminal	Timer Config
83	Host Communication Timeout (sec)	Terminal	Terminal	Timer Config
84	Comm Check Interval (sec)	Terminal	Terminal	Timer Config
85	CheckList TimeOut (sec)	Terminal	Terminal	Timer Config
86	Inside Low value	Terminal	Terminal	Set Brightness Config
87	Inside High value	Terminal	Terminal	Set Brightness Config
88	Outside Low value	Terminal	Terminal	Set Brightness Config
89	Outside High value	Terminal	Terminal	Set Brightness Config

90	CardDetectd Support	Terminal	Terminal	Command Support
91	Resale Support	Terminal	Terminal	Command Support
92	AmountZero	Terminal	Terminal	Command Support
93	Closed Loop Card For Sale	Terminal	/	Card Type Config
94	MSR Debit Card For Sale	Terminal	/	Card Type Config
95	Closed Loop Card For PreAuth	Terminal	/	Card Type Config
96	MSR Debit Card For PreAuth	Terminal	/	Card Type Config
97	Insert	Terminal	/	Entry Mode Config
98	Tap	Terminal	/	Entry Mode Config

14.2. Parameters Detail

❖ This section describes the parameters in detail, including a brief description, some notes and the node in USB file. The parameter modules outlined in this section are classified as follows:

- CTMS Config
- Ethernet Config
- Host Config
- Timer Config
- Card Type Config
- COMM Config
- Transaction Config
- NTP Server Config
- Set Brightness Config
- Entry Mode Config
- GPRS Config
- Card Bin Range Config
- Local Config
- Command Support Config

14.2.1. CTMS Config

❖ The parameters below are used for setting the configuration about CTMS.

Parameter Name	Description	Notes	Node In USB File
Is Upload Log Enable	Enable upload log to CTMS server (TRUE, FALSE)	If enabled, the terminal will attempt to upload log to CTMS when the upload log time arrived; if disabled, it will not attempt to do. Default value: TRUE	CTMS_Config/ UploadLog/ LogEnable

Upload log Time	The time when the terminal attempts to upload log automatically (Format of 00:00, hour:min)	Upload the log of the previous day. Default value: 2:00	CTMS_Config/ UploadLog/ Timer
CTMS Host	Identify which CTMS environment used (No Selection, UAT, Product)	No Selection means that it will not change the original setting in the terminal after CTMS Update; UAT means that it will use the UAT CTMS address; Product means that it will use the product CTMS address. Default Value: No Selection The corresponding values in the USB file are as follows: Blank: No Selection 1: UAT Address 2: Product Address	CTMS_Config/ URL_Config/CurHost
CTMS UAT Address	Address of CTMS test environment.	Used for test environment. Default value: "staging-ctms.castlestech.net"	CTMS_Config/ URL_Config/ UATAddr
CTMS Product Address	Address of CTMS product environment.	Used for product environment. Default value: Blank	CTMS_Config/ URL_Config/ PRODAddr
CTMS Port	Port of CTMS server address (1~65535)	Blank (no set any values) means that it will not change the original value in the terminal after CTMS Update; Empty (fill in "Empty") means that it will clear the value in the terminal after CTMS Update. Default value: Blank	CTMS_Config/ URL_Config/ HostPort
CTMS Retry Times	Number of attempts to connect with CTMS server, 0 means no retry	Default value: 3	CTMS_Config/ Control/ ReCount

14.2.2. COMM Config

- The parameters below are used for setting the communication type.

Parameter Name	Description	Notes	Node In USB File
Host Communication	The communication method of terminal connecting to the transaction server (Gprs, Ethernet)	The default value depends on the specific application	Local_Config/ CommType
Command Communication	The communication method of terminal connecting to the Kiosk (COM1, COM3, USB1, Bluetooth, Ethernet)	The default value depends on the specific application The corresponding values in the USB file are as follows: 0: COM1 2: COM3 4: USB1 5: Bluetooth 6: Ethernet	Local_Config/ CMDPort

14.2.3. GPRS Config

- The parameters below are used for setting configuration of GPRS communication. If GPRS is not used, you can ignore this part.

Parameter Name	Description	Notes	Node In USB File
SIM Slot	Allowed SIM card slot (SIM1, SIM2)	Default value: SIM1 The corresponding values in the USB file are as follows: 1: SIM1 2: SIM2	COMM_Config/ GPRSConfig/ Slot
APN (GPRS)	APN Name	Default value: globaldata.net	COMM_Config/ GPRSConfig/ APN
UserName (GPRS)	APN User Name	Default value: Blank	COMM_Config/ GPRSConfig/ UserName
Password (GPRS)	APN Password	Default value: Blank	COMM_Config/ GPRSConfig/ Password

14.2.4. Ethernet Config

- The parameters below are used for setting configuration of Ethernet

communication. If Ethernet is not used, you can ignore this part.

Parameter Name	Description	Notes	Node In USB File
DHCP	Allow a DHCP server automatically to assign an IP address and other information to each host on the network (No Selection, TRUE, FALSE)	No Selection means that it will not change the original value in the terminal after CTMS Update; if not allowed (FALSE), the IP address and other configuration should be set by the user Default value: No Selection	COMM_Comfig/ EthConfig/DHCP
IP	Ethernet IP address	Default value: Blank	COMM_Comfig/ EthConfig/IP
Mask	Ethernet Mask	Default value: Blank	COMM_Comfig/ EthConfig/Mask
Gateway	Ethernet Gateway	Default value: Blank	COMM_Comfig/ EthConfig/GATEWAY
DNS	Ethernet DNS	Default value: 8.8.8.	COMM_Comfig/ EthConfig/DNS
Command Port	Ethernet port for command (1024 ~ 65535)	Blank (no set any values) means that it will not change the original value in the terminal after CTMS Update; Empty (fill in "Empty") means that it will clear the value in the terminal after CTMS Update. Default value: Blank	COMM_Comfig/ EthConfig/PortForCMD

14.2.5. Transaction Config

❖ The parameters below are used for setting transaction configuration.

Parameter Name	Description	Notes	Node In USB File
Is Quick Chip	Identify whether or not Quick Chip for contact transaction will be supported. (TRUE, FALSE)	Used when the transaction host is Heartland Portico USA or Apriva Default value: TRUE	Local_Config/ IsQuickChip

Max Vends (must be higher than 0)	Maximum Vend Number	This parameter value must be higher than 0. Default value: Blank	Local_Config/ MaxVends
Max Amount (must be higher than 0)	Maximum Amount	This parameter value must be higher than 0. Default value: Blank Unit: $	Local_Config/ MaxAmount
Reversal Retry Times	Number of attempts to send a reversal message to server, 0 means no retry	Default value: 3	Local_Config/ ReversalRetry
AuthComplete Retry Times	Number of attempts to send a auth-complete message to server, 0 means no retry	Default value: 3	Local_Config/ AuthCompleteRetry
Transaction Environment	Identify which transaction environment used (No Selection, UAT, Product)	No Selection means that it will not change the original setting in the terminal after CTMS Update; If it is in UAT environment, it will use the test transaction host; If it is in Production environment, it will use the product transaction host. Default Value: No Selection	Local_Config/Environmentype

14.2.6. Card Bin Range Config

- Cards Bin ranges of one card type should be in the format of Low-High. A "-" is required between the low and high values and ";" between multiple ranges. This part will only be used when the transaction host is Apriva.

Parameter Name	Description	Notes	Node In USB File
VI01 (Visa)	The card Bin Range used for Visa.	Default value is: 400000-499999	AprivaCard_Bin Range/VI01
MC01 (MasterCard)	The card Bin Range used for MasterCard.	Default value is: 510000-559999;222100-272099	AprivaCard_Bin Range/MC01
AX01 (American Express)	The card Bin Range used for American Express.	Default value is: 340000-349999;370000-379999	AprivaCard_Bin Range/AX01
DS01 (Discover)	The card Bin Range used for Discover.	Default value is: 300000-305999;309500-309599;3	AprivaCard_Bin Range/DS01

		60000-369999;380000-399999;601100-601103;601105-601109;601120-601149;601174-601174;601177-601179;601186-601199;644000-650599;650601-600609;650611-659999;352800-358999	
Maestro (Maestro)	The card Bin Range used for Maestro	Default value is: 500000-509999;560000-601099;601110-601119;601150-601173;601175-601176;601180-601185;601200-601942;601946-603171;603173-621093;621095-621161;622910-623999;627000-628199;628900-643999;660000-690045;690047-699999	AprivaCard_Bin Range/Maestro
MSTAR01 (Military Star)	The card Bin Range used for Military Star	Default value: 601943-601945	AprivaCard_Bin Range/MSTAR 01

14.2.7. Host Config

- At present, the supported hosts of unattended application are Heartland Portico USA, GP Canada and Apriva. And there are two parts of the host parameter configuration, Test environment part and Product environment part.

14.2.7.1. Host Config for Heartland

- The parameters below are used for setting configuration of the Heartland Portico USA and GP Canada transaction hosts.

Parameter Name	Description	Notes	Node In USB File
URL	Host URL address.	Default value of Test: https://cert.api2-c.heartlandportico.com/Hps.Exchange.PosGateway/PosGatewayService.asmx (USA) https://cert.api2.heartlandportico.com/Hps.Exchange.PosGateway/PosGatewayService.asmx (Canada) Default value of Product: Blank Mandatory	HLInfo_Test/ HLPosGatewayUrl HLInfo_Product/ HLPosGatewayUrl
HLLicenseId	License Id	Default value of Test depends on the specific application Default value of Product: Blank Mandatory	HLInfo_Test/ HLLicenseId HLInfo_Product/ HLLicenseId

HLSiteId	Site Id	Default value of Test depends on the specific application Default value of Product: Blank Mandatory	HLInfo_Test/ HLSiteId
			HLInfo_Product/ HLSiteId
HLDeviceId	Device Id	Default value of Test depends on the specific application Default value of Product: Blank Mandatory	HLInfo_Test/ HLDeviceId
			HLInfo_Product/ HLDeviceId
HLUserName	User Name	Default value of Test depends on the specific application Default value of Product: Blank Mandatory	HLInfo_Test/ HLUserName
			HLInfo_Product/ HLUserName
HLPassword	Password	Default value of Test depends on the specific application Default value of Product: Blank Mandatory	HLInfo_Test/ HLPassword
			HLInfo_Product/ HLPassword
HLUniqueDevice Id	Unique Device Id	Default value: Blank Optional	HLInfo_Test/ HLUniqueDeviceId
			HLInfo_Product/ HLUniqueDeviceId
HLTxnDescriptor	Transaction Descriptor	Default value: Blank Optional	HLInfo_Test/ HLTxnDescriptor
			HLInfo_Product/ HLTxnDescriptor
HLDeveloperID	Developer ID	Default value of Test depends on the specific application Default value of Product: Blank Optional	HLInfo_Test/ HLDeveloperID
			HLInfo_Product/ HLDeveloperID
HLVersionNbr	Version Number	Default value of Test depends on the specific application Default value of Product: Blank Optional	HLInfo_Test/ HLVersionNbr
			HLInfo_Product/ HLVersionNbr
HLVoltageFlag	Is need Voltage Key (TRUE, FALSE)	If enabled, the transaction should be performed with the Voltage Key, otherwise it would be failed; if disabled, the transaction can be performed without the Voltage Key. Default value: TRUE	HLInfo_Test/ HLVoltageFlag
			HLInfo_Product/ HLVoltageFlag

14.2.7.2. Host Config for Apriva

❖ The parameters below are used for setting configuration of the Apriva transaction host.

Parameter Name	Description	Notes	Node In USB File
AprivaTokenURL	The Apriva URL for token Token transaction	Default value of Test: https://aibapp144.aprivaeng.com:9464/o/1049/oauth2/token Default value of product: Blank Mandatory	APInfo_Test/ APTokenURL APInfo_Product/ APTokenURL
AprivaVoidURL	The Apriva URL for void transaction	Default value of Test: https://aibapp144.aprivaeng.com:9467/pay/v2/payments/void Default value of product: Blank Mandatory	APInfo_Test/ APVoidURL APInfo_Product/ APVoidURL
AprivaCashSaleURL	The Apriva URL for cash sale transaction	Default value of Test: https://aibapp144.aprivaeng.com:9467/pay/v1/payments/cash/sale Default value of product: Blank Mandatory	APInfo_Test/ APCashSaleURL APInfo_Product/ APCashSaleURL
AprivaChargeURL	The Apriva URL for charge transaction	Default value of Test: https://aibapp144.aprivaeng.com:9467/pay/v2/payments/charge Default value of product: Blank Mandatory	APInfo_Test/ APChargeURL APInfo_Product/ APChargeURL
AprivaPostAuthURL	The Apriva URL for post auth transaction	Default value of Test: https://aibapp144.aprivaeng.com:9467/pay/v2/payments/capture Default value of product: Blank Mandatory	APInfo_Test/ APPostAuthURL APInfo_Product/ APPostAuthURL
AprivaReversalURL	The Apriva URL for reversal transaction	Default value of Test: https://aibapp144.aprivaeng.com:9467/pay/v2/payments/reverse Default value of product: Blank Mandatory	APInfo_Test/ APReversalURL APInfo_Product/ APReversalURL
AprivaAdjustURL	The Apriva URL for adjust transaction	Default value of Test: https://aibapp144.aprivaeng.com:9467/pay/v2/payments/adjust Default value of product: Blank Mandatory	APInfo_Test/ APAdjustURL APInfo_ Product/ APAdjustURL

APClientID	Client ID	Default value of Test: castle1 Default value of product: Blank Mandatory	APInfo_Product/ APReversalURL APInfo_Product/ APClientID
APSecret	Secret	Default value of Test: c8b1c8992d8f4145a4d6c22f7f8349b Default value of product: Blank Mandatory	APInfo_Test/ APSecret APInfo_Product/ APSecret
APAcceptType	Accept Type	Default value of Test: Accept: application/json Default value of product: Blank Mandatory	APInfo_Test/ APAcceptType APInfo_Product/ APAcceptType
APMethod	Method	Default value of Test: POST Default value of product: Blank Mandatory	APInfo_Test/ APMethod APInfo_Product/ APMethod
APTokenContentType	Token Content Type	Default value of Test: Content-Type: application/x-www-form-urlencoded Default value of product: Blank Mandatory	APInfo_Test/ APTokenContent Type APInfo_Product/ APTokenContent Type
APTokenScope	Token Scope	Default value of Test: https://ws.api.apriva.com/auth/user Default value of product: Blank Mandatory	APInfo_Test/ APTokenScope APInfo_Product/ APTokenScope
APTokenAccessURI	Token Access URI	Default value of Test: https://aibapp144.aprivaeng.com:9467 Default value of product: Blank Mandatory	APInfo_Test/ APTokenAccess URI APInfo_Product/ APTokenAccess URI
APTokenAuthorization	Token Authorization	Default value of Test: Authorization: Basic Default value of product: Blank Mandatory	APInfo_Test/ APTokenAuthori zation APInfo_Product/ APTokenAuthori zation
APTxnPlatformKeyV1	Transaction Platform Key V1	Default value of Test: APK: e4d1c5d1-3cdc-41a0-8bce-24bd83d5d261-1049-D144	APInfo_Test/ APTxnPlatformKeyV1

		Default value of product: Blank Mandatory	APInfo_Product/ APTxnPlatformKeyV1
APTxnPlatformKeyV2	Transaction Platform Key V2	Default value of Test: Apriva-Platform-Key: e4d1c5d1-3cdc-41a0-8bce-24bd83d5d261-1049-D144 Default value of product: Blank Mandatory	APInfo_Test/ APTxnPlatformKeyV2 APInfo_Product/ APTxnPlatformKeyV2
APTxnAgent	Transaction Agent	Default value of Test: Apriva-Agent: Castles Default value of product: Blank Mandatory	APInfo_Test/ APTxnAgent APInfo_Product/ APTxnAgent
APTxnAprivaSDK	Transaction Apriva SDK	Default value of Test: Apriva-SDK: 2.0 Default value of product: Blank Mandatory	APInfo_Test/ APTxnAprivaSDK APInfo_Product/ APTxnAprivaSDK
APTxnAuthorization	Transaction Authorization	Default value of Test: Authorization: Bearer Default value of product: Blank Mandatory	APInfo_Test/ APTxnAuthorization APInfo_Product/ APTxnAuthorization
APTxnContentType	Transaction Content Type	Default value of Test: Content-Type: application/json Default value of product: Blank Mandatory	APInfo_Test/ APTxnContentType APInfo_Product/ APTxnContentType
APCREncDataProfile	CR Encrypted Data Profile	Default value of Test: generic Default value of product: Blank Mandatory	APInfo_Test/ APCREncDataProfile APInfo_Product/ APCREncDataProfile
APCRName	CR Name	Default value of Test: Castles Default value of product: Blank Mandatory	APInfo_Test/ APCRName APInfo_Product/ APCRName
APCREMV	CR EMV Capable	Default value of Test: TRUE	APInfo_Test/

Capable	(TRUE, FALSE)	Default value of product: Blank Mandatory	APCREMVCapable
			APInfo_Product/ APCREMVCapable
APAllowPartialAuth	Allow Partial Auth (TRUE, FALSE)	Default value of Test: TRUE Default value of product: Blank Mandatory	APInfo_Test/ APAllowPartialAuth
			APInfo_Product/ APAllowPartialAuth
APRegister Identifier	Register Identifier	Default value of Test: 20464887-b9a7-4c50-b1d4-bc2880a76c1d Default value of product: Blank Mandatory	APInfo_Test/ APRegisterIdentifier
			APInfo_Product/ APRegisterIdentifier

14.2.8. NTP Server

❖ The parameters below are used for setting the configuration about NTP.

Parameter Name	Description	Notes	Node In USB File
Is NTP Enable	Enable NTP Check (TRUE, FALSE)	If enabled, the terminal will check the RTC value when the trigger time arrived; if disabled, it will not attempt to do. Default value: TRUE	NTPCheck/ EnableNTP
Time Zone	Time Zone used for checking the RTC value of the terminal. (0 ~ 30)	About the meaning of the values, please refer to the comment below the table. If the value is smaller than 0 or larger than 30, use 24 (UTC-5) as default. Default value: Eastern Standard Time(UTC-5)	NTPCheck/ TimeZone
NTP URL	Host address of the NTP server	For USA, default value: “us.pool.ntp.org” For Canada, you should fill in a valid security address.	NTPCheck/ UpdateNTPURL

NTP Frequency (days)	The frequency to check the RTC value of the terminal.	A value of 1 means check NTP once a day; a value of 2 means check NTP every 2 days. Default value: 1 Unit: days	NTPCheck/ UpdateNTPFrequency
NTP Time (hh:mm)	The time to check the RTC value of the terminal (Format of 00:00, hour:min)	Default value: 06:00	NTPCheck/ UpdateNTPTime

❖ The corresponding UTC time zone is as follows:

0 - Greenwich Mean Time (UTC+0)
1 - European Central Time (UTC+1)
2 - Eastern European Time (UTC+2)
3 - (Arabic) Egypt Standard Time (UTC+2)
4 - Eastern African Time (UTC+3)
5 - Middle East Time (UTC+3:30)
6 - Near East Time (UTC+4)
7 - Pakistan Lahore Time (UTC+5)
8 - India Standard Time (UTC+5:30)
9 - Bangladesh Standard Time (UTC+6)
10 - Vietnam Standard Time (UTC+7)
11 - China Taiwan Time (UTC+8)
12 - Japan Standard Time (UTC+9)
13 - Australia Central Time (UTC+9:30)
14 - Australia Eastern Time (UTC+10)
15 - Solomon Standard Time (UTC+11)
16 - New Zealand Standard Time (UTC+12)
17 - Midway Islands Time (UTC-11)
18 - Hawaii Standard Time (UTC-10)
19 - Alaska Standard Time (UTC-9)
20 - Pacific Standard Time (UTC-8)
21 - Phoenix Standard Time (UTC-7)
22 - Mountain Standard Time (UTC-7)
23 - Central Standard Time (UTC-6)
24 - Eastern Standard Time (UTC-5)
25 - Indiana Eastern Standard Time (UTC-5)
26 - Puerto Rico and US Virgin Islands Time (UTC-4)
27 - Canada Newfoundland Time (UTC-3:30)
28 - Argentina Standard Time (UTC-3)
29 - Brazil Eastern Time (UTC-3)
30 - Central African Time (UTC-1)

14.2.9. Local Config

❖ The parameters below are used for common settings of the terminal.

Parameter Name	Description	Notes	Node In USB File
Page Numbers (3~32)	The numbers of pictures to show in the slide show. (3 ~ 32)	If the value is smaller than 3, the value will be set to 3; If the value is larger than 32, the value will be set to 32; If the value is not set, use 10 as default. Default value: 10	Local_Config/ PageNumbers
Page Switching Interval (millisecond)	The display time of each picture.	Default value: 1000 Unit: milliseconds	Local_Config/ PageInterval
Service Mode Password (4 Bytes)	The password to enter the service mode menu.	It must be 4 bytes. Default value: 1234	Local_Config/ Password
Max Days to save log (1~10)	The maximum number of days to store logs. (1 ~ 10)	If the value is 5, then when the sixth log file is formed, the first file will be deleted automatically. Default value: 5	Log_Config/ MaximumDays
Speaker	Identify whether or not speaker is on (No Selection, OFF, ON)	No Selection means that it will not change the original value in the terminal after CTMS Update; if the speaker is on, it will say something during the transaction such as "Please make selection"; if it is off, it will not say something Default value: No Selection The corresponding values in the USB file are as follows: Blank: No Selection 0: OFF 1: ON	Local_Config/ Speaker
Reader Card	The Card Bin Range of Gift Card	Used when the transaction host is GP Canada Default value: 6049580-6049589	Local_Config/ CardReader

Is Close Receipt Tips	Identify whether or not Receipt Tips will be printed during the Interac transactions (TRUE, FALSE)	Used when the transaction host is GP Canada. If the value is "TRUE", it will do not print receipt prompt during the Interac transactions Default value: FALSE	Local_Config/ IsCloseReceiptTips
Is Show French First	Identify whether or not French will be shown firstly on the bilingual UI (TRUE, FALSE)	Used when the transaction host is GP Canada. If the value is "TRUE", French is displayed on the bilingual UI prior to English. Default value: FALSE	Local_Config/IsFrenchFirst

14.2.10. Timer Config

❖ The parameters below are used for setting the timer.

Parameter Name	Description	Notes	Node In USB File
User Operation Timeout (sec)	Timeout for all user interaction interfaces.	Default value: 90 Unit: seconds	TimeOut_Config/ OperationTimeout
Host Communication Timeout (sec)	Timeout for communication with the transaction host.	Default value: 100 Unit: seconds	TimeOut_Config/ CommTimeout
Comm Check Interval (sec)	The interval of checking communication of the terminal with host.	Default value: 300 Unit: seconds	TimeOut_Config/ CommCheck
CheckList TimeOut (sec)	Timeout for the Check List menu	Default value: 120 Unit: seconds	TimeOut_Config/CheckListTimeOut

14.2.11. Set Brightness Config

❖ The parameters below are used for setting the screen brightness.

Parameter Name	Description	Notes	Node In USB File
Inside Low value	Absolute value of brightness. This value should be less than 256	Default value: 120	SetBrightness/ InsideLow
Inside High value		Default value: 210	SetBrightness/ InsideHigh
Outside Low value		Default value: 180	SetBrightness/ OutsideLow
Outside High value		Default value: 255	SetBrightness/ OutsideHigh

14.2.12. Command Support

- In addition to standard commands (for example: Sale), we also support some optional commands. You can choose whether to enable these optional commands by modifying the configuration file.

Parameter Name	Description	Notes	Node In USB File
CardDetectd Support	Identify whether or not Card Detected function will be supported. (TRUE, FALSE)	When an available card is detected, cashless terminal will send a command to inform the controller that transaction is processing. Default value: TRUE	Local_Config/ IsCardDetectSupport
Resale Support	Identify whether or not Resale function will be supported. (TRUE, FALSE)	When a sale command is processing, before detecting an available card, the cashless terminal allows the transaction amount to be modified by receiving another Sale command. Default value: TRUE	Local_Config/ IsResaleSupport
AmountZero	Identify whether or not the transactions with an amount equal to zero will be supported. (TRUE, FALSE)	If supported, the “Sale” or “Pre-auth” requests with an amount equal to zero will be accepted. If not supported, the requests with an amount equal to zero will be rejected. Default value: TRUE	Local_Config/IsAm ountZeroSupport

14.2.13. Card Type Config

- The parameters below are used for setting whether some special cards are supported for Apriva transaction host.

Parameter Name	Description	Notes	Node In USB File
Closed Loop Card For Sale	Identify whether or not Closed Loop card will be supported for sale transaction (TRUE, FALSE)	Used when the transaction host is Apriva Default value: TRUE	Local_Config/IsClos edLoopCardSupport

MSR Debit Card For Sale	Identify whether or not MSR Debit card will be supported for sale transaction (TRUE, FALSE)	Used when the transaction host is Apriva Default value: TRUE	Local_Config/IsMSRDebitSupport
Closed Loop Card For PreAuth	Identify whether or not Closed Loop card will be supported for pre-auth transaction (TRUE, FALSE)	Used when the transaction host is Apriva Default value: FALSE	Local_Config/IsClosedLoopSupportForPreAuth
MSR Debit Card For PreAuth	Identify whether or not MSR Debit card will be supported for pre-auth transaction (TRUE, FALSE)	Used when the transaction host is Apriva Default value: TRUE	Local_Config/IsMSRDebitSupportForPreAuth

14.2.14. Entry Mode Config

❖ The parameters below are used for setting the supported POS Entry Mode for Apriva transaction host.

Parameter Name	Description	Notes	Node In USB File
Insert	Identify whether or not contact card will be supported (TRUE, FALSE)	Used when the transaction host is Apriva Default value: TRUE	Local_Config/IsInsertSupport
Tap	Identify whether or not contactless card will be supported (TRUE, FALSE)	Used when the transaction host is Apriva Default value: TRUE	Local_Config/IsTapSupport