



# Honeywell SmartTE Powered by StayLinked

## Client User Guide

## CONTENTS

<b>1</b>	<b>INTRODUCTION.....</b>	<b>1</b>
1.1	Starting the SmartTE Client .....	1
1.2	Closing the client .....	1
<b>2</b>	<b>CLIENT DIALOGUES.....</b>	<b>2</b>
2.1	Host.....	2
2.1.1	Connect	2
2.1.2	Disconnect	2
2.1.3	Quit Session	2
2.2	Host > Configure.....	2
2.2.1	Server	4
2.2.2	Display	5
2.2.3	Miscellaneous	6
2.2.4	Scanner-As-Wedge	7
2.2.5	Smart Keyboard	8
2.2.6	Voice	9
2.2.7	GUI Image Cache	10
2.3	Tools .....	10
2.3.1	Radio Stats	11
2.3.2	Ping	12
2.3.3	Scan Test	13
2.3.4	Key Test	14
2.4	About.....	15
<b>3</b>	<b>OTHER FEATURES .....</b>	<b>16</b>
3.1	Smart Menu.....	16
3.2	SmartTiles .....	16
3.3	Smart Keyboard.....	16
3.4	Extended Keys .....	18
3.5	Security .....	20
3.6	Running Third-Party Programs .....	21
<b>4</b>	<b>SPECIAL CONFIGURATION FILES .....</b>	<b>22</b>
4.1	Multiple/Backup Honeywell Servers (servers.ini) .....	22
4.2	Troubleshooting.....	26

# 1 Introduction

Honeywell SmartTE powered by StayLinked is a three-part solution consisting of a Server process, Administrator management console and a Client.

The Honeywell Client software is an "ultra-thin" client that connects to a Honeywell Server to provide terminal emulation (5250, 3270, VT). Clients are available for various device operating systems including; Android, iOS, Windows CE, Pocket PC, Windows Mobile, Linux, DOS and Windows desktop-based family of devices.

Honeywell clients have local configuration options. These options are primarily related to the display of screen information, but does not include emulation settings that are controlled by the Honeywell server. Honeywell clients cannot provide terminal emulation access without connecting to a Honeywell Server.

This guide describes the options found in a typical Honeywell client, as well as the Honeywell SmartTE powered by StayLinked options available in this client version.

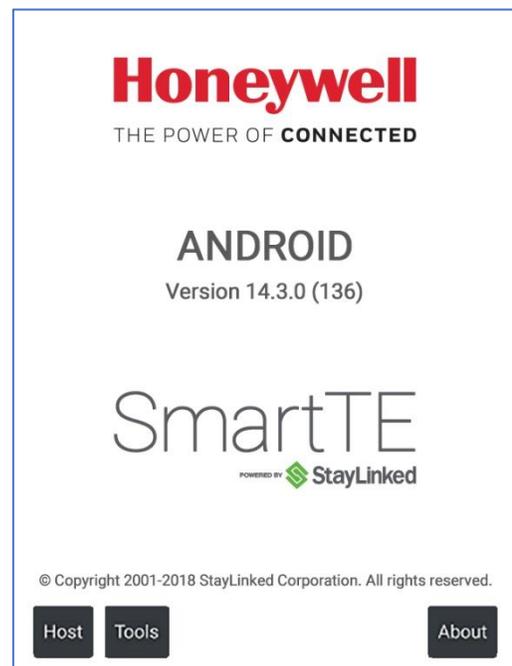
## 1.1 Starting the SmartTE Client

Launch SmartTE via the Start Menu or desktop icon: SmartTE can also be started by navigating to the installation directory

The Honeywell TE Client application displays the Honeywell splash screen on startup.

**Device Type:** This value is used by Honeywell to identify the type of hardware for selection of keyboard maps, client settings, device groups, and software deployment. The default value can be configured to a new type using the Administrator's 'client settings' feature, or by manually adding a line to the staylink.ini file that specifies device\_name=xxxxxxx.

**Client Version:** These numbers represent the client major version, minor version, service release and (build). This guide represents the features included in all client software packages of this version.



## 1.2 Closing the client

Using File > Exit will prompt for a password if the client is set to 'application lockdown' of hide or show. The default password is esp. this will not end a client-server session. Rebooting the device or restarting the client will also reconnect to an existing session.

## 2 *Client Dialogues*

---

One key difference between traditional clients and the newer device operating systems is the extent to which the client can control the device interface. Windows clients could operate in full screen mode and completely hide the operating system menu and program bars, displaying “0 for Options” on the splash screen. With full screen mode disabled, these clients display menus for; File, Host, and Tools. Clients for these new operating systems cannot completely hide the OS navigation menus.

The sections that follow will discuss the menu options in order. Most often you will choose the “Host - Connect” menu option to start your sessions. The client must be able to establish a connection with the Honeywell Server using UDP-based transactions. For help configuring your network and radio settings please refer to the manufacturer documentation. Once your settings are complete, the Tools > Ping option can help confirm that network connectivity has been properly established.

### 2.1 Host

---

The ‘Host’ menu provides options for connecting to the host, disconnecting from the host, quitting a session and configuring the settings of the Honeywell client. Some client versions will offer a toggle SIP option, which will show or hide the on-screen input panel for tap capable keyboard input.

#### 2.1.1 Connect

---

Select the ‘Connect’ option from the ‘Host’ menu to start a connection to the Honeywell Server. The client will step through connecting to your Honeywell server, but may provide the Host Timeout error message if the handshake cannot complete. Once connected, the device will typically display a Telnet Session sign-on screen.

More information on the client-server handshake can be found in the troubleshooting section, or in the guide for Host Timeout.

#### 2.1.2 Disconnect

---

Select the ‘Disconnect’ option from the ‘Host’ menu to disconnect from an active session. This option is only available if the device is connected to an active session. If you disconnect from an active session, the session remains active on the Honeywell Server, waiting for the device to reconnect at a later time. If you wish to terminate the active session, then select the ‘Quit Session’ menu option.

#### 2.1.3 Quit Session

---

Select ‘Quit Session’ option from the ‘Host’ menu to terminate an active session. This option is only available if the device is connected to an active session. If you quit an active session, the session is removed from the Honeywell Server, freeing up a licensed seat.

### 2.2 Host > Configure

---

Under the host menu, the configuration of the client contains only a small number of the

available settings. In this section you can enter the Honeywell host address, and port number, configure display options, control the behavior of the Honeywell client application on the device, and adjust the scanning options for wedge scanning devices. (Scan as Wedge does not appear on all devices)

Only the most common features are configured directly on the client. Several configuration options are available using the Client Settings feature of the Administrator. These settings are not only cold boot persistent, but can automatically be deployed to all of your devices without the need to configure each device manually. Please see the Administrator User's guide for additional details.

## 2.2.1 Server

The settings on the Server tab allow you to configure the IP and Port of the Honeywell Server. In cases where the device may need to connect to one of multiple Honeywell servers, you would configure the device to use a supplemental configuration file called servers.ini. Please see the section below for details about the options and format of this configuration file.

**Server IP:** Host name or IP address of your Honeywell server. The Operating System must be configured and able to resolve host names to use them as a valid address. Some client version may limit the number of characters allowed.

**Server Port:** Port number server is listening on. The Honeywell server is configured by default to listen for new connections on port 3006.

**Use Device ID:** Allows you to specify a [deviceid] value specific to this device. This value can be used in Honeywell scripts or will be used for iSeries virtual device names when the client connects to a device group that contains the [deviceid] mnemonic in the device name prefix field. Devices that do not contain a Device ID value in the Honeywell client will use the windows system name.

**Max Connections:** This setting will change the server address dialogue to include multiple Honeywell servers. When the option is selected for only one server, the user will automatically be connected to that server when selecting 'Connect'. If multiple servers are added to this list, the user will be presented with a selection under the connect menu.

When a value higher than one is selected, the client will offer connection parameters for each possible connection. Android and iOS clients will list each connection, which can be configured independently. Windows clients will display a table that require you to press enter to populate each cell in the server list.

All clients populate a connections.ini file. This file can be copied from one device to others if you want to mirror the configuration options. Note that you must also configure the max connections option for the table to be used. Without increasing the max connections, the connections.ini configuration file will not be used, instead using the standard staylink.ini options.

```
[connection1]
name = AS/400 WMS                <- Name that appears on the Client Connection Menu(s)
server = Honeywell.mycorp.com    <- Host/IP of Honeywell Server (matches entry
in 'servers.ini' for HA/Backup support)
port = 3006                      <- Port of Honeywell Server
deviceid = 45                    <- Device ID
for this connection, [deviceid] on the server.
columns = 80                     <- Viewport Columns for this connection
rows = 25                        <- Viewport Rows for this connection
voice_grammar =                  <- Vanguard Voice Grammar File Name for this
connection (MANUAL CONFIG)
hotkey = 310000                  <- Keycode of Hot Key that switches to this
connection (MANUAL CONFIG)
preferred_host_name = AS/400 WMS <- Determines the automatic selection of a Telnet
Host when the 'Select a Host' menu is processed (MANUAL CONFIG)

[connection2]
name = SAP Console
server = Honeywell.mycorp.com
port = 3006
deviceid = 45A
columns = 80
rows = 25
voice_grammar =
hotkey = 320000
preferred_host_name = SAP Console
```

## 2.2.2 Display

The following options are available on the Display configuration tab (right):

**Use Bold Font** will force all characters into a high-intensity display. Disabling this options will result in narrower characters and allow more characters to be displayed on the screen at any given time.

**Fixed Rows and Columns** are available to set the dimensions of the display space.

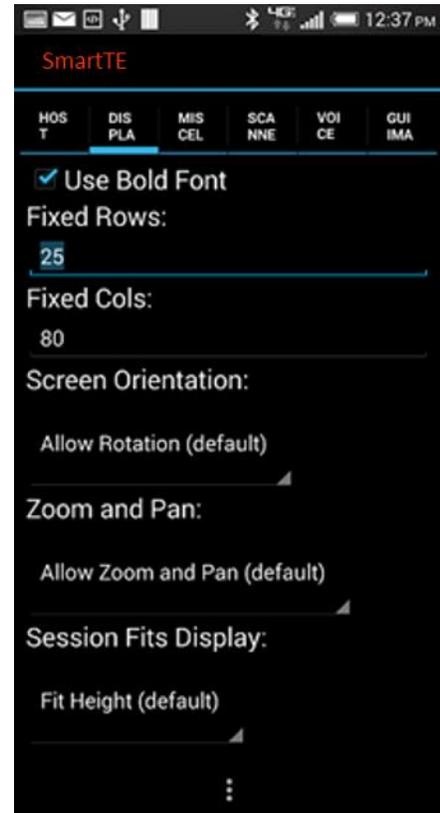
Terminal emulation screens are typically 24 rows by 80 columns. Some emulation specifications can be larger, but most devices cannot clearly display that much text on a usable screen. The portion displayed by the client is called the viewport.

Multi-touch devices should be configured to use the entire emulation space. With these clients, you are able to pan and zoom across the entire emulation space (optional). Reducing the row and column will prevent users from accessing this area on your devices.

**Screen Orientation** selects the rotation options, allowing or restricting the user from turning the device to switch between portrait and landscape views.

**Zoom and Pan** allows the user to dynamically grow and shrink the display size and shift the display left to right and up or down to see different sections of the display space.

**Session Fits Display** sets the default zoom size to fit the height or width of the display space to the screen size.



### 2.2.3 Miscellaneous

The Miscellaneous settings are typical of any Honeywell client.

**Auto Connect** will default to never, which requires the user to manually connect to the server to start a session. Setting the value to once will automatically start a connection when the client is started. Using a setting of always will start a new session any time the user ends the current session. This will also disable the client ability to disconnect from an active session. Honeywell recommends a setting of never or once on devices that perform functions other than terminal emulation. Sessions started using the 'always' connection option can still be disconnected from the Honeywell Administrator's Connections List.

**Full Screen** configures the Client to remove operating system dialogue bars whenever possible. This option is disabled by default, and should not be used when third-party programs are being used to secure your devices.

**Extended Keys** will allow the client to display a 'ribbon' along the base of the screen. This ribbon slides left and right, and displays many common commands. The ribbon can be customized by creating an extkeys.ini file with your desired options. This file and the configuration options are described in section 2 of this guide.

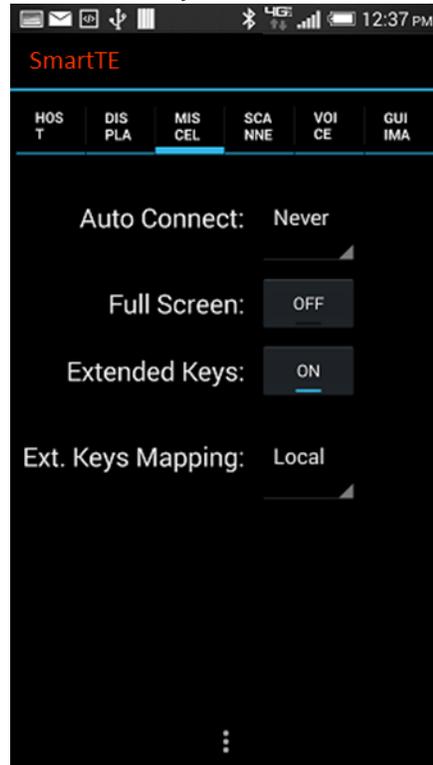
**Extended Keys Mapping** changes the processing of extended keys options from the Client to Honeywell Server. This option has no effect if you create a custom 'extkeys.ini' to make your own custom extended keys toolbar.

**Local** – The client sends 'mnemonics' to the server, [pf3] if you press the F3 toolbar button, [enter] if you press the Enter toolbar button, etc.

**Server** – The client sends the appropriate keycode as if you pressed a button on the keyboard. Since these items generate keyboard event codes, the keyboard map on the server is used to determine what action to take for each toolbar button.

The 'Extended Keys Mapping' option controls only the behavior of the 'built-in' toolbar button ribbons, All, Input, Cursor and FKeys.

More details regarding the extended keys configuration and options can be found in the extended keys section later in the document or in the general Client User Guide found in the documentation section of the Honeywell downloads site.

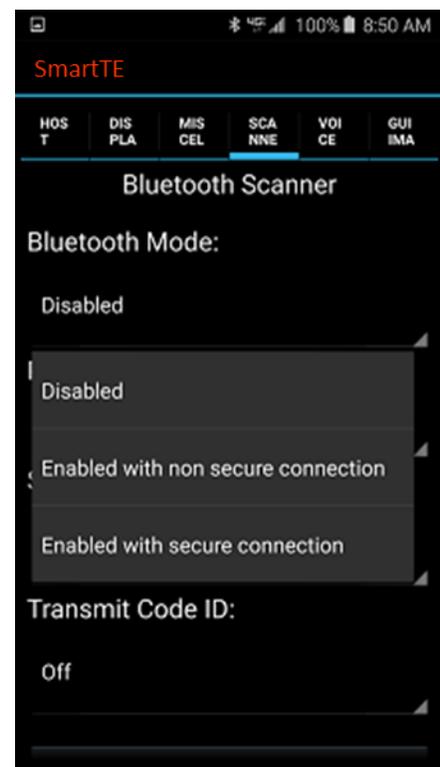
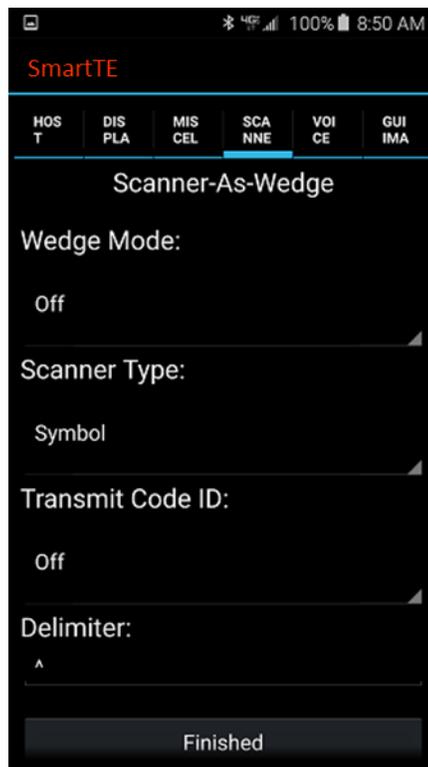
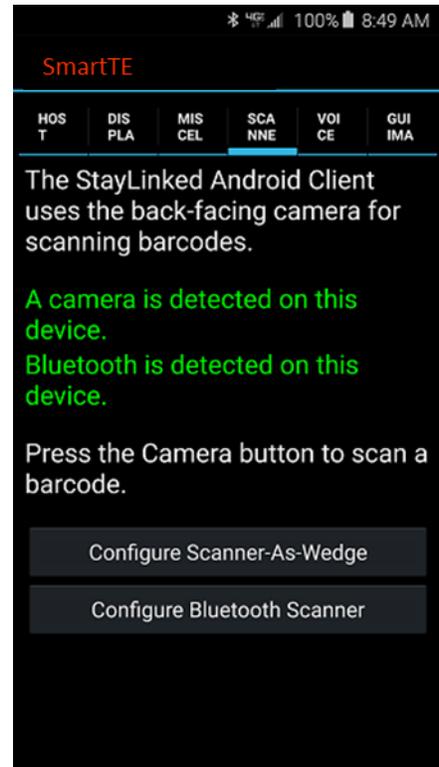


### 2.2.4 Scanner-As-Wedge

Devices with an integrated scanner will typically work automatically, supporting the scanner test and reporting a barcode symbology. Devices that attach an external or Bluetooth scanner may require additional configuration. Scan devices operating in HID mode will require standard scanner-as-wedge configuration as described in our scanner-as-wedge technical reference document. These clients also support the 'autowedge' feature when configured with a scan delimiter of 0. Devices operating in SPP mode can be natively operated by the SmartTE Client, but require that the scan device is paired with the Android device before it can be selected from the SmartTE Client scanner configuration screen.

Both scanner-as-wedge and Bluetooth mode are displayed as options below. Bluetooth mode will offer a selection of all Bluetooth devices, and often include an icon that suggests the type of paired device.

More information on scan configuration can be found in the technical reference for scan configuration. Also note that without a symbology id, barcodes will report their symbology as unknown/unsupported.



### 2.2.5 Smart Keyboard

Keyboards also support the operating system swipe gesture to switch between keyboards. This gesture is supported by the device operating system and hardware, so tuning and control would be accomplished in the device operating system.

A single long press or press and hold will hide the Honeywell menu bar that displays File, Host and About.

A two-finger tap will show and hide the keyboard.

Smart Keyboard options include the following:

**Keyboard Transparency:** SmartTE keyboards support alpha levels. This sets how transparent the keyboard is, which can allow the user to see the screen through the keyboard.

**Off** – Disables transparency allowing the keyboard to block the emulation screen behind it. This is an alpha level of 100.

**Low** – Low transparency is a slightly transparent keyboard. This is an alpha level of 80.

**Medium** – Medium transparency is the mid-level transparent keyboard. This is an alpha level of 60.

**High** – High transparency shows more of the emulation space than the keyboard. This is an alpha level of 40.

**Fade While Pressed:** This option will dim the keyboard if pressed and held. The keyboard will return to the normal transparency when released.

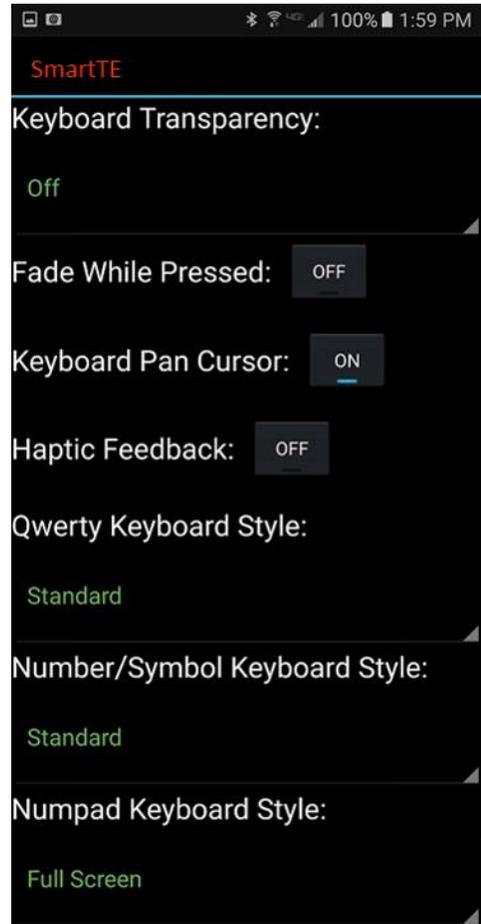
**Keyboard Pan Cursor:** This option will shift the display if the cursor is behind the on-screen keyboard. Disabling this option will leave the cursor behind the keyboard, which would still be visible if the keyboard is at least partially transparent.

**Haptic Feedback:** Not all devices support vibration options. If supported, the device will slightly vibrate for each keypress to help users know when a key has been entered.

**QWERTY Keyboard Style:** Select the default QWERTY keyboard style between the options; Disabled, Standard, Small, AZERTY, Full Screen, 4-Column Right, 4-Row Full, and 4-Column full.

**Number/Symbol Keyboard Style:** Select the default Number/Symbol style between Standard and Azerty keyboard layouts.

**Numpad Keyboard Style:** Select the default Number Pad keyboard style between the



options; Disabled, Full Screen, 2-Row, 3-Row, 2-Column Right, 5-Row and 3-Column Right. In addition to the Smart Keyboard options list above, the following standard options are available on most SmartTE devices.

When a client attempts to connect to the Honeywell server it will check for a keyboard map. You can add a keyboard using the Honeywell Administrator. Navigate to the emulation settings section and select keyboard maps. Then right click in the list of keyboards and select add.

Once the keyboard map is opened, select File and Save Changes to add it to your server's list of installed keyboards. Additional information on keyboard maps and their use can be found in the Technical Reference on the subject in the Documentation section of our portal site.

If your device displays the error message "eSP0003 No VT Keyboard Map Found", you have not added the keyboard map that matches your device type and emulation. This message will show one of the three main device types of VT, 5250 or 3270, based on the emulation type specified in your telnet host entry.

This Client provides several different on-screen keyboards for emulation use. These generate keyboard event codes in the same manner as other Honeywell Clients. More information on keyboard maps can be found in the Keyboard Map Technical Reference document on the Honeywell downloads site.

### Alpha QWERTY



### Function Keys



### Numeric



---

### 2.2.6 Voice

Voice and Text to speech will allow the client to provide voice feedback when licensed by the Honeywell Server. Speech products may incur an additional cost.

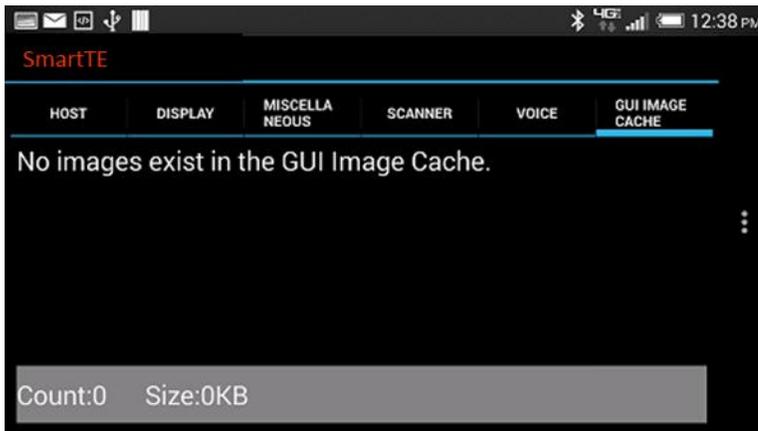
Please contact your Honeywell reseller for details.

### 2.2.7 GUI Image Cache

---

provides a list of images that have been replicated to your Client device for display speed. Graphical telnet mode requires additional Server configuration options to map these image files to display elements.

More information on GUI telnet mode can be found in the Honeywell Administrator User's Guide.



## 2.3 Tools

---

Various tools are available for the testing of a SmartTE client. Not all devices support all features, but the available features will include the same possible options.

Note that this section of the client does not allow for any configuration, but only the reporting and display of information.

### 2.3.1 Radio Stats

**Network Type:** Shows if the device reports that the network is established by cellular or wifi.

**IP Address:** Current IP address of the device.

**MAC:** Current MAC address of the device.

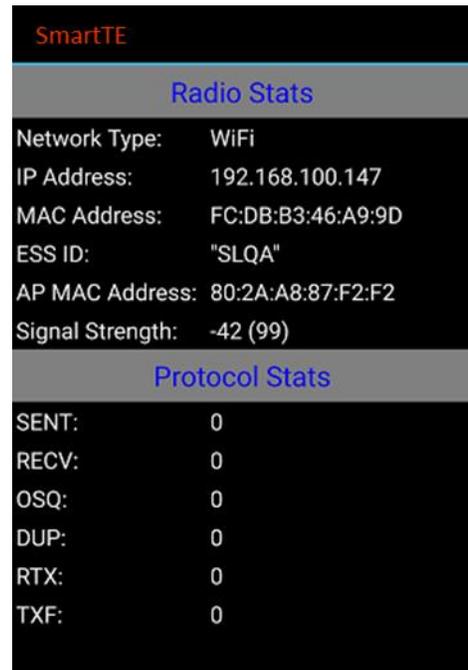
**ESSID:** Station ID of the Access Points to which the device is connecting.

**AP Mac:** MAC Address of the Access Point to which the device is currently associated.

**Signal:** Depending on whether or not the device is currently in radio coverage, one of the following will be displayed in the "Signal:" field.

- Signal strength expressed as a percentage
- "Not Associated"

As the device is moved in/out of radio coverage, the value of the "Signal:" field will toggle between the values above. Where the "Signal:" value changes to "Not Associated" indicates dead zones, obstructions in the communication path, or fringe areas of radio coverage.



The image shows a screenshot of the SmartTE interface. At the top, it says "SmartTE" in red. Below that is a grey header with "Radio Stats" in blue. The main content area has a black background with white text. It lists several network statistics: Network Type: WiFi, IP Address: 192.168.100.147, MAC Address: FC:DB:B3:46:A9:9D, ESS ID: "SLQA", AP MAC Address: 80:2A:A8:87:F2:F2, and Signal Strength: -42 (99). Below this is another grey header with "Protocol Stats" in blue. The main content area continues with a black background and white text, listing protocol statistics: SENT: 0, RECV: 0, OSQ: 0, DUP: 0, RTX: 0, and TXF: 0.

Radio Stats	
Network Type:	WiFi
IP Address:	192.168.100.147
MAC Address:	FC:DB:B3:46:A9:9D
ESS ID:	"SLQA"
AP MAC Address:	80:2A:A8:87:F2:F2
Signal Strength:	-42 (99)

Protocol Stats	
SENT:	0
RECV:	0
OSQ:	0
DUP:	0
RTX:	0
TXF:	0

Stats information is sometimes hidden for wired devices, or devices running a client that can't request details from the device's network stack.

The Stats section displays radio and Honeywell protocol performance data.

**TxRate:** Current transmit rate in Mega bits per second.

**TxRetry:** Number of transmit retries.

**Sent:** Number of Honeywell packets sent.

**Recv:** Number of Honeywell packets received.

**OSQ:** Number of out-of-sequence Honeywell packets.

**RTX:** Number of Honeywell packets retransmitted.

High values in the OSQ and RTX fields may indicate network issues. Honeywell will only transmit net changes to your devices. This means that packets received out of sequence will be discarded until the next sequential packet is received at the device.

## 2.3.2 Ping

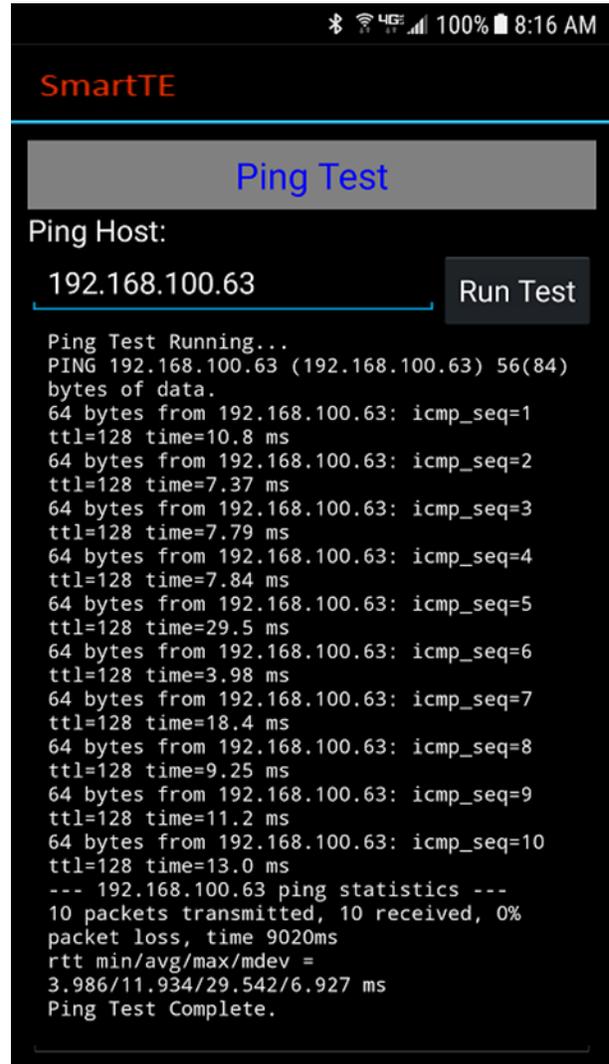
Select the 'Ping' option from the 'Tools' menu to test network access between the Honeywell client and the selected host machine.

During a typical ping, the results will be displayed in the number of milliseconds that the packet took to make the round trip to the destination and back. Lower numbers are better. If you numbers become excessively high, connectivity will be sluggish or unreliable.

If the results say Host Unreachable, no route was available to make the round trip or the packets were dropped before the round trip could complete.

If the results report Unable to Resolve, the name used was not listed in the name server, or the name server was not reachable.

Enter the host IP address (defaults to the Honeywell Server) and choose "Ping" to cause the client to attempt to ping the host.

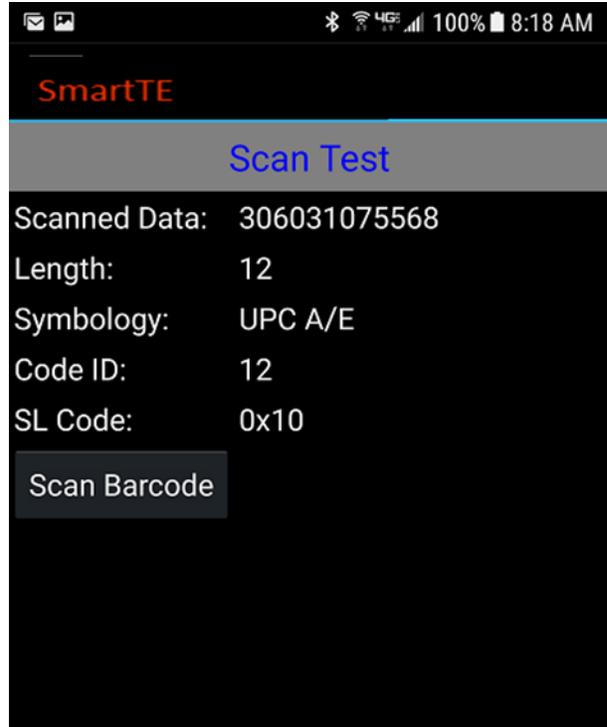


### 2.3.3 Scan Test

Select the 'Scan Test' option from the 'Tools' menu to test scanning on the device.

If you scan data when this test screen is displayed, you should see the scanned data, the length of the scanned data and the symbology type of the scanned data. If you do not see your scanned data on this screen, then it is most likely caused by an external scanner that is not or has not been configured to identify scan data.

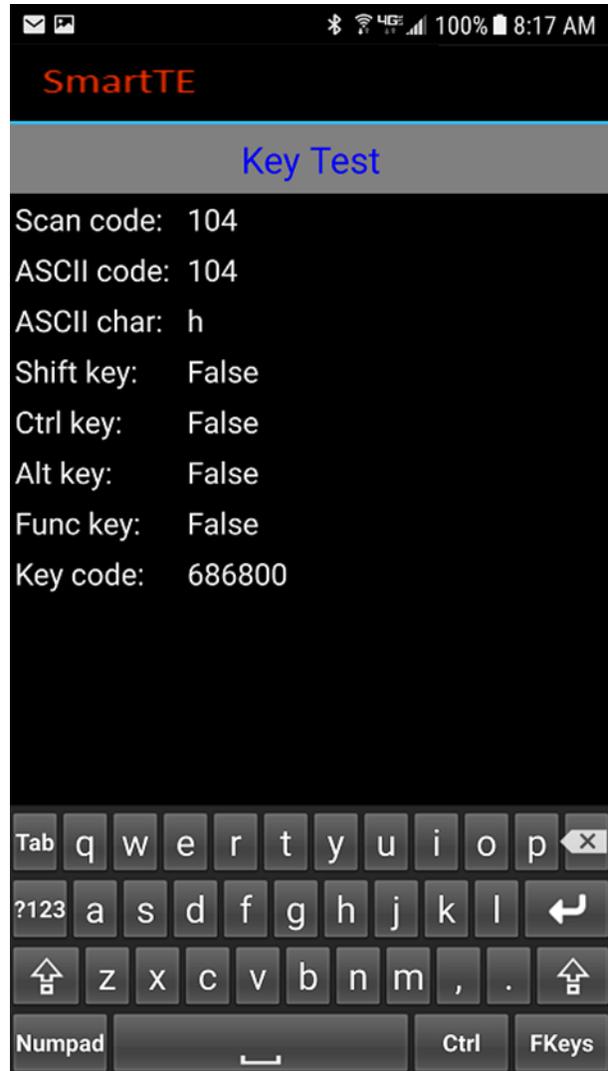
More information on scanning can be found in the guide for scan configuration on our downloads site.



### 2.3.4 Key Test

Select the 'Key Test' option from the 'Tools' menu to test the keyboard on the device.

Press any key on the keyboard to display its Scan code, ASCII code and Key code. The Key code is an important reference value to be used when programming keyboard maps using the Honeywell Administrator. Dismiss the dialog with a tap on the back button.



### 2.4 About

---

Select the 'About' option from the 'File' menu and the 'About' dialog will be displayed.

This dialogue allows a reset of the unique value used by the Honeywell server to identify this device. When reset, the value will be repopulated based on the hardware in which the client is installed. This is typically required only in cases when the unique ID was replicated to multiple devices by cloning the installation. This UID value is referenced in the HoneywellManager.log file when devices connect to the server during an initial connection request.

SmartTE capable devices will offer several menu options that don't appear on traditional TE clients. This includes links to Honeywell on the web and access to the public demo server.

The public demo server offers multiple versions of the same application. These options demonstrate what traditional, dynamic and designed SmartTE screens might look like. There are also options for tablet, full screen, handheld and wearable version of the demo in order to represent what it might appear like on different device screen sizes.

### 3 Other Features

Many options are automatic or require special configuration files.

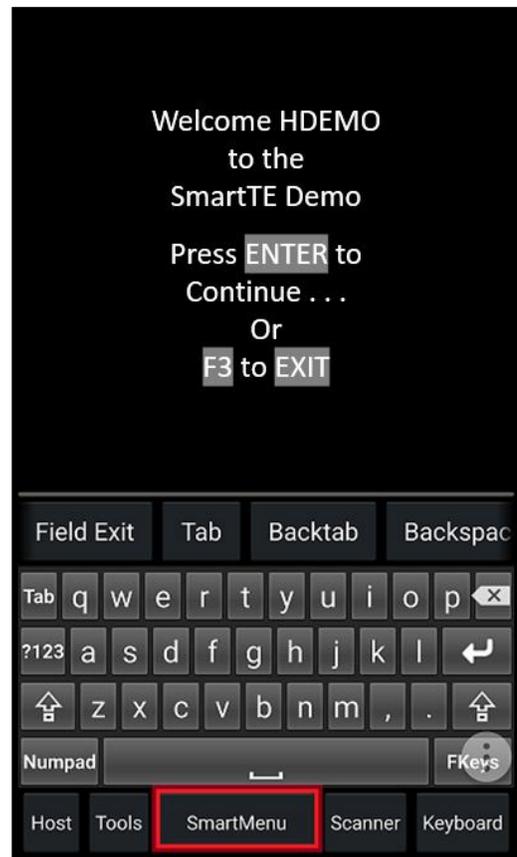
The following options are available with standard SmartTE capable clients.

#### 3.1 Smart Menu

Devices connecting to a SmartTE Server that displays a screen with more than one smart menu objects will automatically generate a client menu option called SmartMenu. This will provide a OS style pop-up menu for all menu objects that are tap-able on the current screen. This allows screens with multiple small buttons to be presented in a large format scrolling list.

This feature requires Honeywell Server version 14.0 or higher and smart menu object configurations.

Using screen recognition features on your server allows you to create an API that automatically presents the Smart Menu to the user.



#### 3.2 SmartTiles

Devices connecting to a v14.4 or newer Honeywell Server have the option to display SmartTiles. These tiles overlay the emulation space with customizable buttons or keyboards. Each tile set allows for multiple tiles, presented by the Honeywell server based on user inputs or screen recognition features.

SmartTiles include the option to replace the standard Keyboard button on the menu-bar with a SmartTiles button. This is commonly used to create custom keyboards and context sensitive menu options without the need to adjust the emulation screens.'

More information on SmartTiles can be found in the Administrator User's Guide and other references.

#### 3.3 Smart Keyboard

Honeywell clients version 14.3 and newer support a range of new keyboards and transparency options. The keyboards can be called using the [keyboard\_xxxxxx] mnemonics

described in the extended keys section, or executed from the server using keyboard mapping or screen recognition.

### Gestures

A single long press or press and hold will hide the Honeywell menu bar that displays File, Host and About.

A two-finger tap will show and hide the keyboard.

A single finger swipe across the keyboard will slide to the next or last keyboard.

### Smart Keyboard options include the following:

**Keyboard Transparency:** SmartTE keyboards support alpha levels. This sets how transparent the keyboard is, which can allow the user to see the screen through the keyboard.

**Off** – Disables transparency allowing the keyboard to block the emulation screen behind it. This is an alpha level of 100.

**Low** – Low transparency is a slightly transparent keyboard. This is an alpha level of 80.

**Medium** – Medium transparency is the mid-level transparent keyboard. This is an alpha level of 60.

**High** – High transparency shows more of the emulation space than the keyboard. This is an alpha level of 40.

**Fade While Pressed:** This option will dim the keyboard if pressed and held. The keyboard will return to the normal transparency when released.

**Keyboard Pan Cursor:** This option will shift the display if the cursor is behind the on-screen keyboard. Disabling this option will leave the cursor behind the keyboard, which would still be visible if the keyboard is at least partially transparent.

**Haptic Feedback:** Not all devices support vibration options. If supported, the device will slightly vibrate for each keypress to help users know when a key has been entered.

**QWERTY Keyboard Style:** Select the default QWERTY keyboard style between the options; Disabled, Standard, Small, AZERTY, Full Screen, 4-Column Right, 4-Row Full, and 4-Column full.

**Number/Symbol Keyboard Style:** Select the default Number/Symbol style between Standard and Azerty keyboard layouts.

**Numpad Keyboard Style:** Select the default Number Pad keyboard style between the options; Disabled, Full Screen, 2-Row, 3-Row, 2-Column Right, 5-Row and 3-Column Right. In addition to the Smart Keyboard options list above, the following standard options are available on most SmartTE devices.

### 3.4 Extended Keys

---

For added touch screen functionality we have created a toolbar that will show at the bottom of the device screen. This toolbar serves as additional area for designating pre-defined functions.

The file that controls the functions and labels of the toolbar is named **extkeys.ini**. The contents of this file (a simple ASCII format) simply list the button number, the text to be displayed on the button and the mnemonic to be issued when the button is used.

In this example, replace statements within the < > with the appropriate information.

Button<#> = <Button Text> , <mnemonic>

*By example: button1=Tab,[tab]*

This would cause the first button to be labeled “Tab” and perform the [Tab] function (which moves the cursor position to the next field) each time it is activated.

The following is a sample layout of the extkeys.ini file. This file must be in a true txt file format. Any formatting information in the file will prevent it from being used by the client software. Any errors found on a line of the file will cause the line to be ignored.

```
[display]
font_size=8
[defaults]
button1=Tab,[tab]
button2=F Exit,[fldext]
button3=Enter,[enter]
button4=F1,[key=990100]
button5=F2,[key=990200]
button6=F3,[key=990300]
button7=F4,[key=990400]
button8=F5,[key=990500]
button9=F6,[key=990600]
button10=EXIT,[device-exit]
button11=HOME,[home]
button12=PgUP,[device-pageup]
button13=PgDN,[device-pagedown]
button14=KbMnu,[keyboard menu]
```

**Please note that all mnemonics (the text in square brackets) should be lower case characters only.**

The font\_size option in this file will control the size of the characters used to describe each button. On small devices it is recommended that no more than 3 characters are used and on vehicle mounts or full screen devices no more than 5 characters. If more characters are used the software will center the text on the button and could cut off the edges on large fonts or long descriptions.

Note that any key code not listed in the keyboard map will perform the ASCII value represented by the center two characters. For example, the code [key=993199] would perform an ASCII 31, which is a number 1. An entry of [key=FF32FF] would perform an ASCII 32, which is a number 2.

**Map-able Mnemonic options**

Each button on the toolbar may be configured to perform one of the following actions:

Cursor Positioning	Paging Support	Function Keys	Custom Options
[backspace]	[device-up]	[pf1]	[call1]
[tab]	[device-down]	[pf2]	[call2]
[clear]	[device-left]	[pf3]	[call3]
[down]	[device-right]	[pf4]	[device-exit]
[left]	[device-pageup]	[pf5]	[keyboard menu]
[right]	[device-pagedown]	[pf6]	[Honeywell menu]
[up]	[device-pageleft]	[pf7]	[toggle_sip]
[delete]	[device-pageright]	[pf8]	[switch_session]
[enter]	[device-fullup]	[pf9]	[disconnect_device]
[eof]	[device-fulldown]	[pf10]	[minimize_client]
[fldext]	[device-fullleft]	[pf11]	[execute_program]
[home]	[device-fullright]	[pf12]	[increase_font]
[insert]	[device-followcursor]	[pf13]	[decrease_font]
[pageup]		[pf14]	[renegotiate]
[pagedn]		[pf15]	[soft_trigger]
[printhost]		[pf16]	[key=xxxxxx]
[reset]		[pf17]	[keyboard_qwerty]
		[pf18]	[keyboard_numsym]
		[pf19]	[keyboard_numpad]
		[pf20]	[keyboard_fkeys]
		[pf21]	[keyboard_ctrl]
		[pf22]	[keyboard_cycle]
		[pf23]	[tile_show]
		[pf24]	[tile_show #,#]
			[tile_hide]
			[tile_toggle]
			[tile_prev]
			[tile_next]
			[tile_cycle]
			[tile_refresh]
			[disabled]
			[hide]

The number of keys will vary depending on the size of the device display. Typical configurations will have 8 available buttons, with vehicle mounts having a maximum of 14 keys. The default toolbar appears with F11-F24 if the extkeys.ini file is not found. Each button will appear as the default function key if any errors in formatting are found in that line of the extkeys.ini file.

While many of the settings are self explanatory, the following may be helpful in some environments:

- [soft\_trigger] - Activates the device's scanning laser as though the trigger had been depressed.
- [renegotiate] - Toggles the display between the maximum and configured font sizes.
- [minimize\_client] - Moves the Honeywell client to the background and displays the device desktop.
- [device-exit] - Ends the Honeywell session and the telnet session. Always requests confirmation.
- [toggle\_sip] - Hides or shows the Soft Input Panel, also known as the tappable keyboard.
- [disconnect\_device] - Disconnects the client from the server but leaves the telnet session active. The device will return to the last state once it is re-connected to the Honeywell server.
- [execute\_program] - This option must be accompanied by a program call configured in the

staylink.ini file.

[key=xxxxxx] - Acts as a keyboard key by generating a code that can be configured in the Administrator keyboard definition for the specific device type.

### SmartKeyboard Commands

[keyboard\_XXXXX] These various commands will show the keyboard type defined in the mnemonic, or hide that keyboard if it the current keyboard.

### SmartTile Commands

[tile\_show #,#] - This will take the user directly to a tile collection ID and page, as entered in the number options. For example, [tile\_show 4,3] would display page three of tile collection four.

[tile\_show ,3] - would display page three of the current collection. [tile\_show] would show the current page in the current collection.

[tile\_hide] - This removes the current tile from the screen, allowing the user to see the emulation space. Once hidden, the user would need to select an extended keys or keyboard map entry to show a new collection and page.

[tile\_toggle] - This is a combination of the hide and show mnemonics which will hide the tile if it is currently displayed, or show it if it was currently hidden.

[tile\_prev] - Displays the previous page in the current SmartTile collection. Using this mnemonic on the first page will wrap back to the last page of the current collection.

[tile\_next] - Displays the next page in the current SmartTile collection. Using this mnemonic on the last page will wrap back to the first page of the current collection.

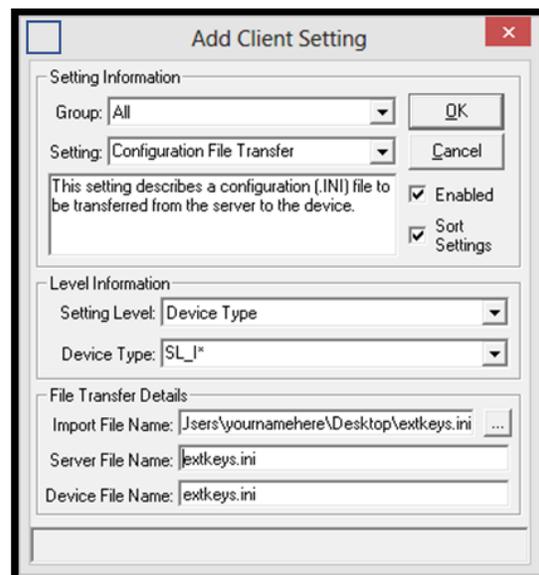
[tile\_cycle] - This mnemonic works much like the next option, except that it includes a blank or hide option after the last page of the collection.

[tile\_refresh] - Used primarily during initial testing and design, this mnemonic will request the latest copy of the collection page from the Honeywell server. This allows you to immediately see any changes on the collection page on your device without having to change pages or reconnect.

## Distributing toolbar configurations

Toolbar configurations can be standardized by creating a client setting that distributes the extkeys.ini file. This is done in the [Honeywell Administrator](#) and will be pushed to qualified devices when a new session is started. The sample dialogue on right can be found by creating a new setting in the Administrator's Client Settings section. Details on this and other features of the Administrator can be found in the Administrator User's Guide in the Documentation section of our downloads site. To copy the configuration of the toolbar from one device to another, simply copy the desired extkeys.ini file into the Honeywell directory of the destination computer. This is easily completed if you start a Honeywell session and use the reliable file transfer to copy the file to the desired devices. Please note that the client software will store your settings file in persistent space if you transfer the file from the Honeywell Administrator.

If changes are made to this file they will not take effect until the Honeywell device software is restarted, which can also easily be done from the Honeywell Administrator.



## 3.5 Security

Some menu options, such as "Host > Configure" require a password.

The default password is “**esp**”.

You can specify a new password for the device by using the ‘Client Settings’ feature of the Honeywell Administrator. Client Settings allows you to centrally manage many of the device-specific settings of the Honeywell Client software on the device.

### **Client to Server Communications Security**

Honeywell provides multiple possible levels of security for the transactions between the Honeywell client and server. These settings are discussed in detail in the Honeywell Administrator User’s Guide.

Controlled through the Administrator’s ‘Server Settings’ dialogue, two options are available.

- **None** – No Honeywell packets will be encrypted.
- **Level 1** – Honeywell data transferred between the Honeywell Thin-Client and the Honeywell Server will be encoded using a proprietary 64-bit encryption scheme.
- **Blowfish**– Honeywell data transferred between the Honeywell Thin-Client and the Server will be encoded using the Blowfish/CBC/PKCS5Padding encryption algorithm.

**Using Blowfish Encryption:** Blowfish encryption provides a very high level of data security for the Honeywell packets that are transmitted between the Honeywell Client and the Honeywell Server. Note that high level encryption may impact the performance of devices that do not have sufficient processing power.

## 3.6 Running Third-Party Programs

---

During the use of an emulation client, it may be important to open another application. This can be anything from calculator to signature capture programs. The most common methods of calling these programs include: use a ‘program call’ from the Honeywell server, from the connections list as a ‘remote program’, using a screen formatted to invoke API 12, or within screen recognition under the APIs tab. The format for these programs can vary based on the operating system and their default path.

### **Android**

These clients create a file called **activities.txt** when the client starts up. This is a list of the other applications on the device at that time. you must uninstall and reinstall the client to regenerate this file, though need applications can be called even if they are not in the activities.txt on a particular device.

You can view this file by gathering it from the Administrator’s connections list and right clicking the device. Select View > Remote File > activities.txt to get that client’s local copy.

## 4 *Special Configuration Files*

---

Honeywell provides support for several features that are not part of the configuration panels available within the client. These configuration options are available through the Settings Deployment features of the Honeywell Administrator only by replacing the complete configuration files. This option can be found among the “All –“ options and is called Configuration File Transfer. Please refer to the Administrator User Guide for details using this method of settings management.

### 4.1 *Multiple/Backup Honeywell Servers (servers.ini)*

---

The purpose of this enhancement is to provide a mechanism by which the Honeywell Client can select from and connect to multiple Honeywell Servers and to support the ability of the Honeywell Client to fail-over to a backup Honeywell Server. Devices may also be configured with a connections.ini file, that is easily created within the client. Connections.ini can be copied to multiple devices using the same methods as a servers.ini implementation. Devices that require configuration options specific to each server address should use connections.ini.

#### **Basic Implementation:**

The new enhancement will only be available if the new SERVERS.INI file exists on the device. If this file does not exist, or the contents of the file are malformed, then the client will revert to the original functionality as provided by the contents of the **STAYLINK.INI** file.

#### **Multiple Server Handling:**

The SERVERS.INI file will provide the ability to specify multiple Honeywell Server to be available to the client for connections. When only a single server is specified, then the user will not be presented with a selection but will instead be connected directly to the server. If there are multiple server specified, then the user will be able to select from a menu that lists these servers. Once a connection is established to a server, that server will be the 'current server' and the connection will be persistent until the user 'Exits the Session'. If the client receives commands to 'Restart the Client', or receives new client software or new device settings, then the device should automatically reconnect to the same 'current server'. Session switching commands should also apply to the 'current server'.

#### **Backup Server Handling:**

If a backup server is specified, then special handling of connection failures will be processed. If the backup server is optional, then when a connection failure to the primary server occurs, the user will be presented with a menu of options. If the backup server is mandatory, and the 'failover retries' are exceeded, the client will automatically connect to the backup server. Once a connection to the backup server is established, it will be considered to be the 'current server' and handling will proceed as described in the 'MULTIPLE SERVER HANDLING' section of this document. If the connection to the backup server fails, then the entire backup processing mechanism will be reset and the next connection attempt will be to the primary server.

### SERVERS.INI Overview:

The SERVERS.INI file describes the list of Honeywell Servers and the backups that are available to the Honeywell Client. This file is stored in the 'Persistent' Honeywell folder on your device. If the file does not exist in the persistent folder, any cold boot operation may result in the loss of the file. If the SERVERS.INI file is transferred to the device using the Administrator's reliable file transfer, then the file will be recognized by the Honeywell Client and handled appropriately, being transferred to persistent storage if possible.

### SERVERS.INI Sections:

SERVERS.INI contains two sections. Firstly, a [servers] section that will describe one or more Honeywell Servers that will be made available to the Honeywell Client for connections. Secondly, an [options] section that can describe options to control the conditions and actions to follow when the primary selected server fails to connect.

#### [servers] Section:

Each server line, or key, in the [servers] section begins with server#' where the # refers to the number of the server entry beginning with one. It is recommended that these key names are sequential. Duplicate key names will cause one or in some cases, all of the lines to be ignored. Key values are limited to 10 entries. If there is only one server entry in this section, then the device will immediately connect to that server. If there are multiple servers defined in this section, then the device will display the list of available servers for the user to select from. Each comma-delimited entry in this file will describe a Honeywell Server Name, IP or Host Name, and Port. Optionally, the entry can also contain a backup IP or Host Name and Backup Port. Here is a sample of the contents of the [servers] section:

#### [servers]

```
server1=WMS Server,server.Honeywell.com,3006,192.167.140.23,3006
server2=PTL Server,192.168.140.4,3006,192,167,140.24,3006
server3=Test Server,test.Honeywell.com,3006
```

Key: **server#**=**ServerName**,**ServerAddress**,**ServerPort**,**BackupAddress**,**BackupPort**

#### [options] Section:

The [options] section contains the options that affect the behavior of these features. The following options are available:

**allow\_quit** - Describes whether or not a 'Quit' menu option will be displayed at the bottom of the server selection menu. Valid values are 1=Show the Quit option (Default), 0=Do not show the Quit option.

**failover\_optional** - If a selected server also contains backup server data, then this option determines whether the failover is optional or mandatory. If optional, then the user will be presented with options when the client is unable to connect to the primary server. Valid values are 0=Mandatory, 1=Optional (Default).

**failover\_retries** - If the failover is mandatory, then this option describes how many retries will be attempted after the initial attempt before the client automatically tries to connect to the backup server. Valid Values are a range from 1 to 5 retries with a default of 2.

Excluding any of these items from the options section will use the normal default value in its place.

If failover is optional and the client fails to connect to the primary server (occasional host timeouts are expected in most environments and simply means the client dropped or transposed a packet during the handshake with the server), then a connection failure menu will be displayed like this:

```
Err: Host Timeout
-----
1 - Retry Primary
2 - Use Backup
3 - Quit
```

If the user has selected to connect to the backup, and that connection fails, then a connection failure menu will be displayed like this:

```
Err: Host Timeout
-----
1 - Retry Backup
2 - Use Primary
3 - Quit
```

If failover is mandatory, and the client fails to connect to the primary server, then the dialog will display the following form, based on your specific server information:

```
Host=102.168.100.95
Port=3006
Primary Retry 1 of 3 <--- This line appears only during retry failures
Connecting...
Err: Host Timeout
* Now Using Backup * <--- This line appears only after the last retry to the primary server
Press any key
```

After all retries to the primary have failed, the next connection attempt will be to the backup server. If the client fails to connect to the backup server, then the client will revert to the primary server.

```
Host=102.168.100.12
Port=3006
Backup Retry 1 of 3 <--- This line appears only during retry failures
Connecting...
Err: Host Timeout
Press any key
```

After all retries to the backup server have failed, the client will return to the main Honeywell menu unless 'Always Auto-connect' is set. When 'Always Auto-connect' is set, the client will automatically restart the connection process from the beginning.

**[options] Section Sample:**

```
[options]
allow_quit=0
failover_optional=0
failover_retries=5
```

### Server Selection Menu:

When there are multiple servers defined in the [servers] section of SERVERS.INI, then the user will be presented with a menu from which to select the desired server. Each menu option will use the Server Number and the Server Name to create the menu text. A sample server menu follows:

```
Select a Server
-----
1) WMS Server
2) PTL Server
3) Test Server
4) Quit
```

### Session ID Management:

Honeywell tracks each session with a unique session ID number. These session IDs are managed by interaction between the client and server process. The following information is provided for reference only. Manually adjusting session ID values may result in lost or orphaned sessions.

If a device is allowed to connect to multiple servers, then it will track session IDs for each server. As always, the session IDs will be managed in the SESSION.INI file. If the device is not using the SERVERS.INI file, then the session information will be stored in the [defaults] and [alternate] sections like this:

```
[defaults]
session_id=124D7
session_number=2
[alternate]
session_id=124D6
session_number=1
```

If the device is using the SERVERS.INI file, then there will be a section created in SESSION.INI for each server like this:

```
[server1_defaults]
session_id=114B9
session_number=1
[server1_alterate]
session_id=114BA
session_number=2
```

Each alternate section applies only to servers using dual session licensing.

## 4.2 Troubleshooting

---

Honeywell clients are designed to return various messages. Each message represents a specific set of issues. This means that the first step in troubleshooting will be to confirm the message presented by the client at the time of the issue.

The following are the most common messages and the steps you might take to resolve the issue:

**Server Code esp0003:** This message is returned when the device type and emulation do not have a keyboard defined on your server. Adding a keyboard map can be done using the Honeywell Administrator console and is explained in detail in the Administrator User's Guide.

*Upgrading a client version may result in improved recognition of the device model, resulting in a new device type. The server requires a keyboard installed for each unique device type and emulation group.*

*Part of the device type may be returned by the device operating system. In some cases, updates or changes to the device may change this response and require the installation of a new keyboard map to match the new device type.*

**Server Code esp0004:** These messages are returned when the connection cannot be created because of Honeywell licensing issues. The Honeywell Administrator can be used to review the current license keys, the Honeywell server process' serial number, and the current number of seats in use. In many cases, terminating old sessions can free up seats for new devices. More information on automating the cleanup of sessions can be found in the user experience guide.

**Other esp00XX Error Codes:** These messages are described in detail in the Administrator User's Guide troubleshooting section. If the device returns the same message multiple times, please review the Administrator User's Guide for troubleshooting tips.

**Out-of-range:** Indicates that the device's radio is reporting that it is not associated with an access point. During normal operation, the Honeywell client will request the association status of the device radio. If the operating system reports that it is not associated, it will display the 'Out of Range' message to the user. Common causes of "out-of-range" conditions:

- Device is physically moved outside the radio coverage area supported by the radio hardware.
- Communication path to access point is obstructed.
- Antenna on the device is bad.
- Unsupported Radio hardware or firmware.

When an "out-of-range" state is detected the device will display an "!" character in the top right corner of the screen. The "!" will alternate between normal and inverse video for a short period as the device monitors the out-of-range state. If the device detects that it is back in radio coverage it will return to the session screen.

The first step is to review the device radio configuration and make sure it is able to reach the Honeywell server. If the device can ping the Honeywell server, adding a line to the device file `staylink.ini` `always_in_range=1` will force the client to ignore association status.

**Linking:** Indicates that the client and server are not exchanging packets in a timely manner.

Diagnosing interruptions in network are best completed with Ping and other network tools.

When a "Linking" state is detected, the device will display an "\*" character in the top right corner of the screen. The "\*" will alternate between normal and inverse video for a short period as the device monitors the link state. If the device detects that the link is restored, it will return to the session screen.

More information on troubleshooting steps can be found in the client-server communications guide.

**Host Timeout:** indicates that the connection between the client and Honeywell server has failed. Occasional host timeout messages are not uncommon in a wireless environment. Continued host timeout messages indicate network difficulties and should be resolved using typical network diagnostics. More information on the Honeywell handshake can be found in the Host Timeout technical reference guide.

**Telnet Timeout:** indicates that the telnet host is not responding, or has denied the request for a telnet session. The first step will be to confirm that your Honeywell server is properly configured with a valid telnet host entry and that your device falls in to a device group that uses your desired host entry.

**WSID Timeout:** It can also be important to make sure the telnet server is enabled on your telnet host. For the iSeries, the virtual device name may not be available or cannot be created. Some versions of the Honeywell server may return a Telnet Timeout that may also indicate a required subsystem or QAUTOCFG is disabled. Review of the iSeries configuration, virtual device names and subsystems may be required.