



Administrator User Guide

CONTENTS

1	STAYLINKED SOLUTION OVERVIEW.....	1
1.1	StayLinked Features.....	1
1.2	StayLinked Application Components.....	1
2	GETTING STARTED.....	3
2.1	Install the StayLinked Server on your Host Platform.....	3
2.2	Install, Connect and Configure the StayLinked Administrator.....	3
2.3	Install the StayLinked Client Software onto your Wireless Devices.....	3
3	USING THE STAYLINKED ADMINISTRATOR.....	4
3.1	Running the Administrator for the First Time	4
3.2	Administrator Quick Tour.....	8
3.3	Connections List and Session Management.....	10
3.4	Telnet Host Administration	22
3.5	Device Group Administration.....	32
3.6	Managing Keyboard Maps	44
3.7	Managing Tap Spot Collections	49
3.8	Managing SmartTiles Collections.....	56
3.9	Managing Session Partnerships.....	63
3.10	Client Administration.....	65
3.11	Scan2Command and Scan2Configure Profiles.....	73
3.12	Device Management.....	77
3.13	Usage Tracking	77
3.14	StayLinked iQ	77
3.15	Administrator Management	80
3.16	Server Administration	96
4	APPENDIX – SPECIAL SCRIPTING MNEMONICS	104
5	APPENDIX – TROUBLESHOOTING.....	106
6	CONTACT INFORMATION.....	108

1 StayLinked Solution Overview

StayLinked™ is a software product that provides a complete solution for managing host Telnet and SSH sessions, improving user workflow, gathering actionable user information, and much more. This section describes the features and architecture of the StayLinked product.

1.1 StayLinked Features

StayLinked, with its Client2Host™ architecture, eliminates the typical challenges associated with deploying a wireless terminal solution in your enterprise by providing:

- Reliable wireless user remote control of host-based application sessions.
- Centralized wireless session/client configuration, monitoring and control.
- Secure end-to-end wireless data transmission between clients and the application host.
- Programmable telnet host screen recognition, reformatting and SmartTE modernization.
- Tracking of unique StayLinked devices and their usage of the StayLinked system.
- Visibility of analytical system and application data using a web-based user interface.

1.2 StayLinked Application Components

There are three basic components that make up the StayLinked system: the host-based server application, which initiates and preserves all wireless terminal user sessions on the application host computer; the thin client application that resides on the various wireless devices; and a Windows-based administrator console that provides centralized visibility, configuration, and management of all connected devices.

1.2.1 The StayLinked Server Application

The StayLinked server is a Java application that runs on the application host computer or on a separate computer connected to the host computer(s). The server listens for connection requests from devices running the StayLinked thin client application and initiates the appropriate 5250, 3270, VT100/220/420, SSH, or TESS emulation sessions to the requested host.

The server owns and maintains the telnet session at the host computer, sending screen updates to the device and forwarding user inputs from the device to the session. The server also recognizes desired screens and can take actions when these screens are recognized and/or reformat these screens to fit on small-screen devices or just to have a different look and feel.

The StayLinked Server runs natively on a wide variety of reliable host computing platforms:

- IBM AS/400 – iSeries – i5 – System i – IBM i (OS/400, i5/OS, IBM i)
- IBM RS/6000 – pSeries – p5 – System p (AIX)
- HP9000 (HP-UX)
- Sun Solaris
- SCO OpenServer, OpenUnix & UnixWare
- Linux (x86)
- Microsoft Windows
- Apple OS X

The installation of the StayLinked server application is described in section 2 of this user guide, in more detail in the server-specific installation guides, and operationally in the server tuning documentation.

1.2.2 The StayLinked Thin Client Application

A StayLinked thin client application is installed on each device that will connect to the host computer. Since each device type is somewhat unique, the client applications are written for specific devices or families of devices. The ultra-thin client software installs quickly and provides the local support for display, keystrokes, scanning, radio communications, and diagnostics.

Upon startup, the client requests a session from the StayLinked server application. The client sends keystrokes, scans and touch events to the server and receives screen updates back from the server. In addition, many diagnostic utilities are included with the client application to help identify various problems with the device and wireless network.

StayLinked thin client applications are available for a wide range of devices, including but not limited to; Wired, RF/Wireless and Cellular network devices from Zebra, Motorola, Symbol, Intermec, Honeywell, DataLogic, PSC, HHP, Psion and others, running DOS, PocketPC/Windows Mobile, and Windows CE/CE.Net, Android, iOS and Windows desktop and tablet operating systems.

The installation of the StayLinked thin client application is described in general in section 2 of this user guide and in more detail in the various device-specific client support guides. StayLinked client application features and functions are described in detail in the various OS-specific client user guides.

1.2.3 The StayLinked Administrator Application

The StayLinked administrator provides centralized device and session management. This powerful application can be installed on one or more Windows PCs and enables administrators to:

- View and sign on to one or more StayLinked servers
- Set up properties for one or more telnet hosts
- Specify screens that can be recognized and configure actions to be taken when these screens are recognized and/or reformat these recognized screens to fit better or look different on the devices
- Set up properties for one or more device groups
- Manage keyboard maps, tap spots and client settings
- View and control connected StayLinked devices
- Send messages, files, and remote commands to devices
- Prepare and deploy client software updates to devices
- Create partnerships between two or more devices to share the same terminal session
- View, share, transfer or completely take over device sessions
- Troubleshoot device and network problems
- Build and print 'Scan2Configure' and 'Scan2Command' profiles that allow you to configure and control the StayLinked Client software by scanning barcodes
- Track the usage of each unique device that connects to the StayLinked Server
- Configure the StayLinked IQ Technology Preview settings and launch the StayLinked IQ user interface using a web browser.
- Manage and control the users that are allowed to run the StayLinked Administrator

The installation of the StayLinked administrator application is described in section 2 of this user guide. The entire set of StayLinked administrator features and functions are described in detail in section 3 of this user guide.

2 Getting Started

This section contains an overview of the basic steps required to get your StayLinked Solution operational. Detailed administrator and server installation, upgrade, and uninstall instructions are contained in the various platform-specific installation guides.

After completing the basic steps described below, you will be able to take advantage of the reliable wireless terminal emulation and centralized management features that are provided by the StayLinked solution.

2.1 Install the StayLinked Server on your Host Platform

- Download and review the appropriate StayLinked Installation Guide
- Review and meet the software and hardware requirements
- Download the appropriate StayLinked Server setup program
- Install the StayLinked Server program
- Configure any platform-specific settings
- Configure the server to start automatically when the host system is restarted
- Start the StayLinked Server

2.2 Install, Connect and Configure the StayLinked Administrator

- Review the StayLinked Administrator section of the Installation Guide
- Review the StayLinked Administrator section of this User Guide
- Select a non-dedicated PC to be used for managing your StayLinked Server
- Download the StayLinked Administrator setup program
- Install the StayLinked Administrator onto the selected PC
- Start the StayLinked Administrator
- Add a StayLinked Server entry to the Administrator and connect to the StayLinked Server
- Install your evaluation or permanent license key
- Add Keyboard Maps for your Wireless Devices
- Review and manage Telnet Hosts, Device Groups and Tap Spots and other settings

2.3 Install the StayLinked Client Software onto your Wireless Devices

- Download the appropriate StayLinked Client Software for your Wireless Devices
- Download and review the StayLinked User Guide for the specific device
- Install the StayLinked Client Software onto the device
- Configure the Radio and Network settings for the device and verify connectivity
- Configure the Client Settings, pointing the client to the IP address of the StayLinked Server
- Connect the client to the StayLinked Server and go to work

3 Using the StayLinked Administrator

This section describes the StayLinked Administrator application, which provides centralized management of your StayLinked servers, hosts, and wireless devices. The section begins by walking you through your first use of the administrator, connecting to your StayLinked server, retrieving the server serial number, and installing the license key. After that, the various functions of the administrator are described.

3.1 Running the Administrator for the First Time

This section walks you through your first use of the administrator: the splash screen, connecting to your StayLinked server, retrieving the server serial number, and installing the license key.

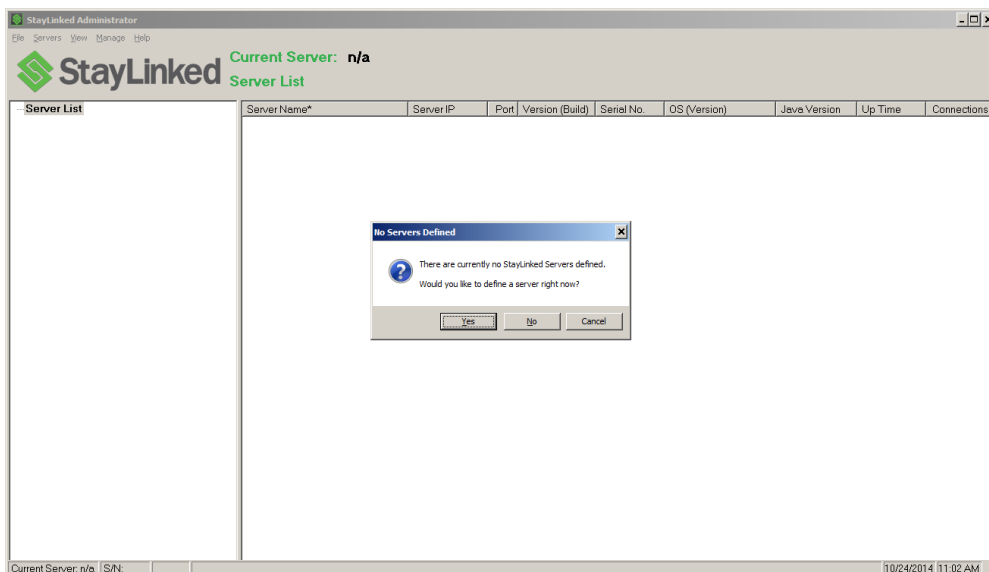
3.1.1 The Administrator Splash Screen

When the StayLinked Administrator is executed, you will see the following splash screen for a few moments.

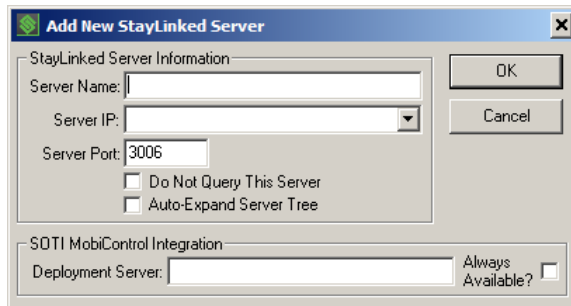


3.1.2 Connecting to the StayLinked Server

The first time you run the StayLinked Administrator, it will not know about any StayLinked servers you may have running. If no servers have been defined yet, the StayLinked Administrator will prompt you to add a server upon startup.



If you answer “Yes”, you will be prompted to add the server information. The following dialog will be presented:



Server Name: Enter a name to identify the StayLinked Server – anything will do – no more than 50 characters (15-20 characters is a good size).

Server IP: Enter the IP address or host DNS name where the StayLinked server can be found. Of course, you will need to have a route to the server system from the Administrator PC.

Server Port: Enter the UDP port number on the StayLinked Server to which the administrator connects. The default port is 3006.

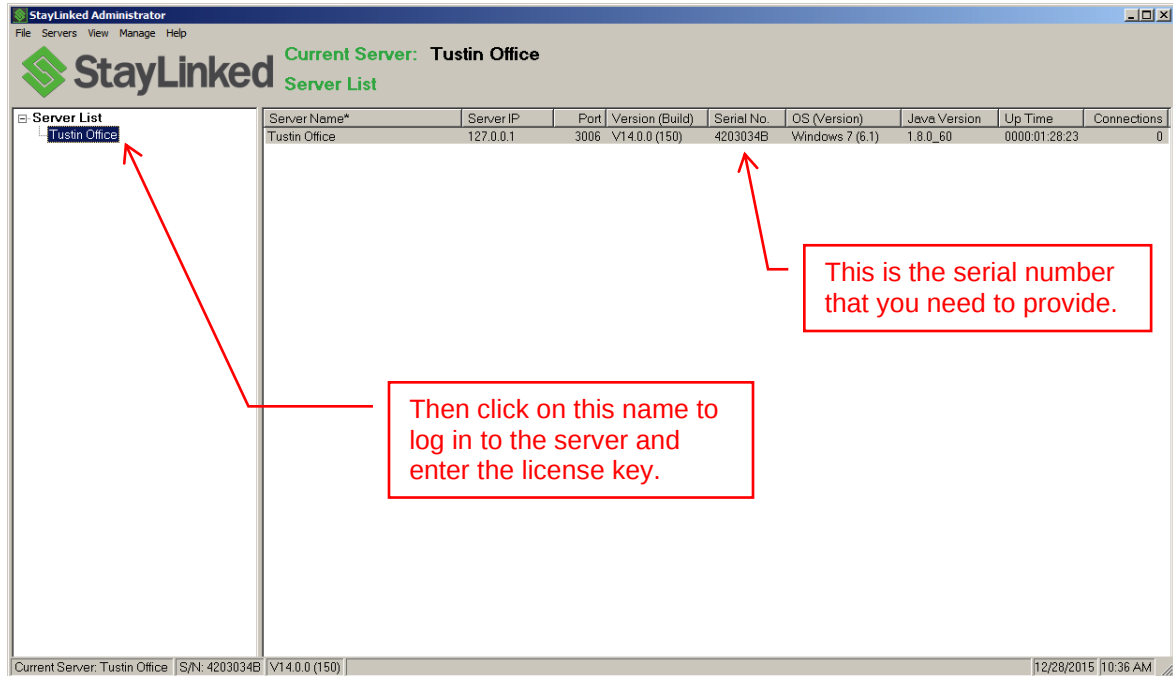
Do Not Query This Server: You can specify that the Administrator not query this server, in case the server is not always available. If you check this box, the server list will show that this server has been ‘skipped’, but you can still select it to connect.

Auto-Expand Server Tree: Check this option to have the Server Tree be expanded automatically when you log onto the server.

SOTI MobiControl Integration: Additionally, you can enable integration with SOTI MobiControl by entering the URL of the MobiControl Deployment Server. This value can be a Host Name or IP address of the SOTI MobiControl Deployment Server. To make this feature available from the ‘Connections List’ of the Administrator, make sure to check the ‘Always Available?’ checkbox.

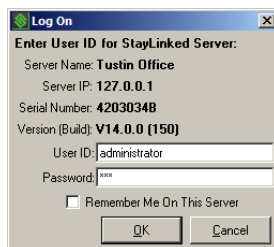
3.1.3 Retrieving the Server Serial Number

Once you have added the server definition, the server will appear on the Administrator console. If the IP address you provided is correct and the StayLinked server is currently running, you will see the server build and serial number in the Server List panel. Provide the serial number to the StayLinked customer service team to obtain your free evaluation license key, otherwise the server will run in 'Demo Mode' which will limit your ability to fully evaluate the software. If running a 'Demo Mode' license, the administrator will warn you when you log onto the server. A StayLinked Server running in 'Demo Mode' will be restricted to a maximum of three connections for one hour at a time.



3.1.4 Installing the License Key

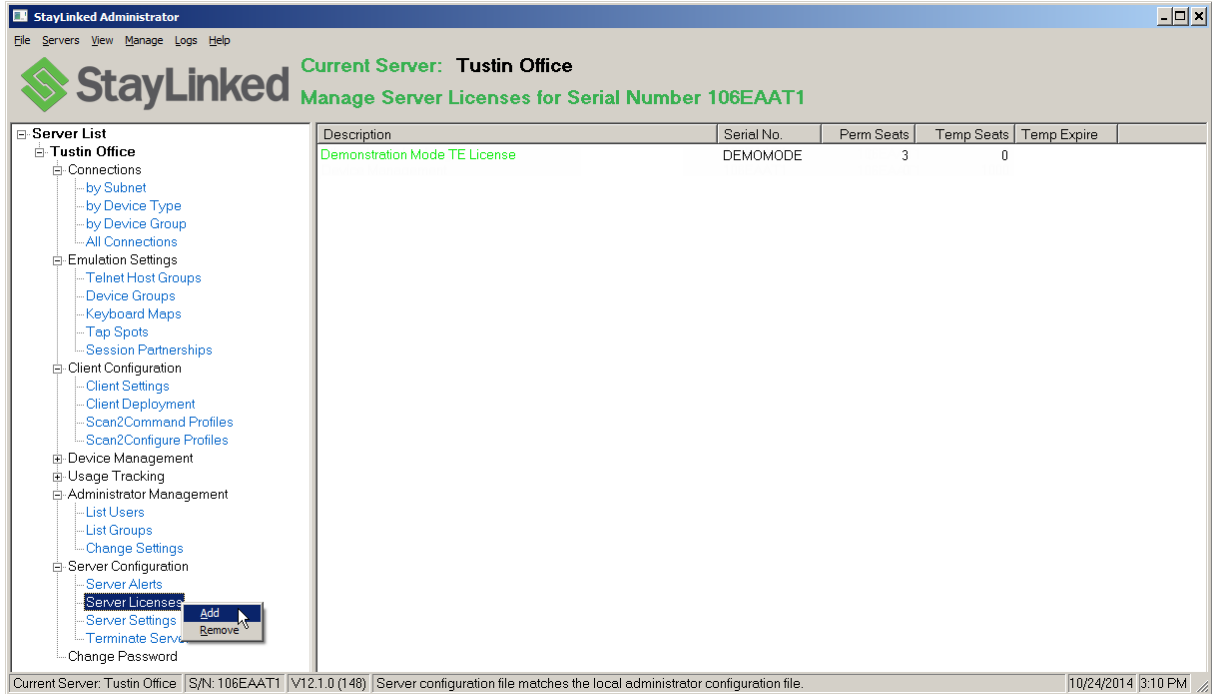
To install your license key, you must first log in to the server. This is done by clicking on the server name. The following dialog box will appear.



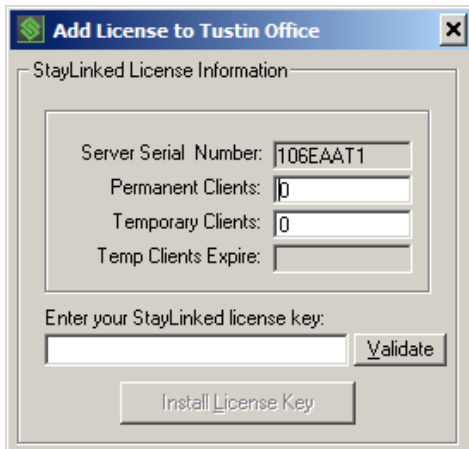
Enter the default User ID "administrator" and the default Password 'esp' for your server. Check the 'Remember Me On This Server' if you would like your User ID to be remembered. Click OK.

Detailed information about Stay-Linked Administrator User Management can be found in the Administrator Management section of this guide.

After logging in to the StayLinked server, you will see a list of available functions appear in a tree on the right side of the Administrator, under the server. Expand the 'Server Configuration' branch of the tree. Use the right mouse button and click on the 'Server Licenses' function. A small menu will appear. Select the 'Add' function from the menu to enter your license key.



Fill-in the appropriate client quantities. The 'Permanent Clients' value and the 'Temporary Clients' value must match the values provided with your license information. Cut-and-paste your 23 character license key into the text box.



Click 'Validate' and then click 'Install License Key'. You will be prompted to replace the currently installed DEMO license key. Click the 'Yes' button to complete this step. Finally, after the new license is installed, you will be automatically logged off the server. Please re-select the Server and log back on after installing a license.

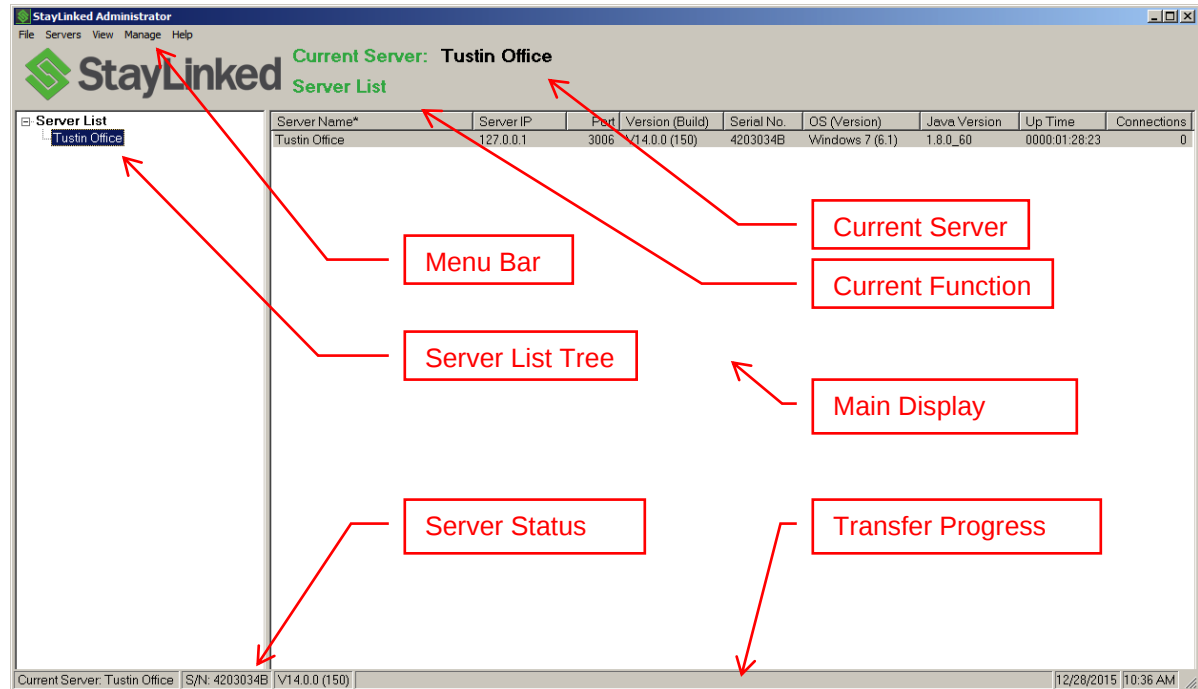
Note that some features or options may not be available unless the appropriate license type is installed on your system.

3.2 Administrator Quick Tour

This section provides a quick overview of the StayLinked Administrator user interface.

3.2.1 The Administrator Screen

The following screen shot details the various sections of the Administrator screen, followed by a brief description of each section.



- **Menu Bar** – The pull-down menu bar is used to access and various Administrator functions.
- **Servers Tree** – This Explorer-style outline control provides a list of all defined servers. Indented below each server are additional branches describing function groups. These group branches can be expanded to show the server functions for that group. Click on a function name to select it. Depending upon the function, a pop-up window or a list may appear in the main display panel. In some cases, a second click of the function name with the right mouse button will show a small menu of additional options.
- **Main Display Panel** – Shows a list of defined servers, server functions, or function details pertaining to the current function. In some cases, double-clicking an item in the list will perform a default action. In some cases, clicking on items in the list with the right mouse button will show a small menu of additional options.
- **Current Server** – Shows the currently-selected server. All functions apply to this server.
- **Current Function** – Shows the function whose list appears in the main display panel.
- **Server Status Bar** – Shows currently-selected server, it's serial number and version.
- **Transfer Progress Bar** – Shows the progress and status of file transfer transactions between the Administrator and the Server.

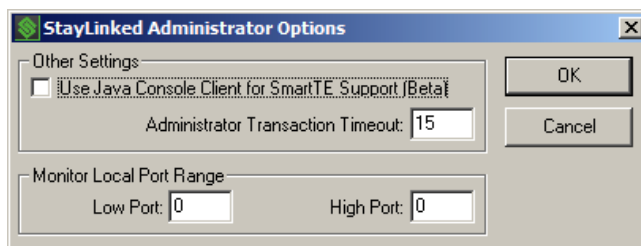
3.2.2 The Administrator Menus

The menu bar at the top of the Administrator screen provides access to a number of features and functions. Following is a brief description of each menu item.

- **File Menu** – Allows you to set Administrator Options and to Exit the program.
- **Servers Menu** – Allows you to Add, Edit, and Delete server definitions for this Administrator. Also provides methods to import and export the server configuration and to print and export the current server list. Options are also provided to Log On and Log Off of a server. All of the Server menu options refer to the currently selected server with the exception of the Add option. Additionally, there is a 'Quick Connect' option that will provide temporary access to servers that have not been added to the list.
- **View Menu** – Provides an option to refresh the List that appears in the main display panel. Another option provides a means of forcing the main display panel to Display the Server List. The last option lets you toggle the Server Tree view on and off.
- **Manage Menu** – Provides a nested menu of all the server functions. These functions are available from the server tree (when visible) and from the main display panel when the Manage Server list is displayed. The Manage menu option provides an alternate method of selecting these functions when the server tree is not being displayed. The selected function will apply to the currently selected server. Note: The available options depend upon Administrator User permissions.
- **Logs Menu** – Provides a list of various server logs. The selected log will be retrieved from the current server. These logs provide various types of details about the server and are a valuable tool for diagnosing the overall health of the server and any issues that may be occurring.
Note: This Logs menu is visible only if Administrator User permissions allow. Your administrator version will determine to log options available.
- **Help Menu** – Provides access to the StayLinked web site and application version information.

3.2.3 Administrator Options

When you select the File->Options menu, the Administrator Options dialog will be displayed:



Use Java Console Client for SmartTE Support (Beta): Check this box to use the Beta Java Console Client when performing the Monitor, Share, Take Control or Start Console Session functions. The Java Console Client is capable of displaying SmartTE graphical elements rendered on dynamic graphical or reformatted graphical telnet screens. If this option is not checked, the original DOS Console Client will be used for these features and graphical elements will not be available. The Java Console Client requires that you have a current version of the Java Runtime installed on your Administrator PC.

Transaction Timeout: Configure this option to adjust the transaction timeout value. If a StayLinked Server is located at a remote location with a poor network connection, it is possible that when the Administrator requests a transaction with the Server, the transaction could timeout. This option configures the maximum amount of time that the Administrator will wait for a response from the server before declaring a transaction timeout.

Monitor Local Port Range: Configure a Monitor UDP port range to match your Firewall if needed.

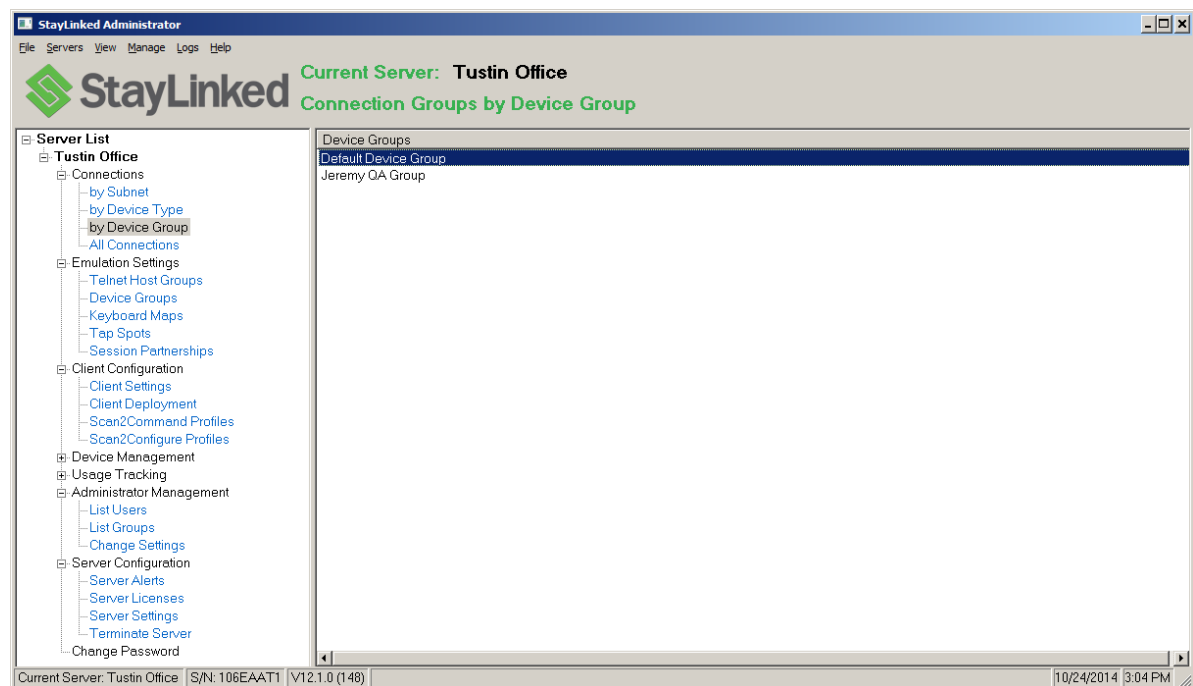
3.3 Connections List and Session Management

This section describes the various methods provided to centrally manage your client sessions. Topics include selecting and viewing a list of connected sessions.

3.3.1 Selecting a Connection List Group Option

When you select Connections from the server tree or the Manage menu, a list of connection group options will appear in the main display panel. Also, if you expand the Connections branch of the server tree (by clicking on the '+' sign), the list of connection group options will appear in the server tree, indented below the Connections branch.

These group options allow you to subset your list of connections by device IP address subnet, by device type, or by device group. You can also view all connections without grouping. If you select a group option, a list of groups will appear in the main display panel. The list will contain all the groups that currently have a session connection. For example, you may have 10 device groups defined, but only two of them currently have a device with a connected session, so only those two groups appear in the list.



Select a group by double clicking on the group name in the list. A list of connections that belong to the selected group will appear in the main display panel.

3.3.2 Connections by Subnet – Subnet Description

When you select the option to display connections 'by Subnet', a list of subnets is displayed that reflect the currently connected devices. You can assign a description to each of these 'subnets' by right-clicking on the subnet row and selecting the 'Edit Description' menu option. The description that you enter will be stored with, displayed on and affect only your Administrator installation.

3.3.3 The Connections List

After selecting your connections group, a list of the currently running sessions is displayed. The list contains many columns of useful information about the session and the device. You can also double click on a specific session in the list to view the details in a separate window.

Session ID*	MAC Address	Device Type	Device Name	IP Address	Session Started	Last Activity	Session Status
193EE	0017231EF91B	ITC_CV61	OPADEV0002	10.10.225.216	10-08-2014 11:34:49	10-08-2014 11:35:09	TE-5250
1F406	70F395EB3A9A	HNY97W6_45	OPADEV0005	10.10.225.163	10-14-2014 08:31:59	10-14-2014 08:34:48	TE-5250
1F410	002368BC8D9A	MC9190C_53	{Automatic}	10.10.225.167	10-14-2014 09:24:33	10-14-2014 09:24:33	Selecting Host
1F41A	000B6B1D7D90	CV30WM5_59	OPADEV0003	10.10.225.157	10-14-2014 13:20:50	10-14-2014 13:21:12	TE-5250
1F41B	002368D214DD	MC9190M_53	OPADEV0004	10.10.225.176	10-14-2014 14:12:28	10-14-2014 14:14:45	TE-5250
2041E	4083DE17B5EA	MC92N0M_53	OPADEV0006	10.10.225.218	10-15-2014 12:19:23	10-20-2014 11:57:06	TE-5250
2744D	002368D214DD	MC9190M_53	OPADEV0001	10.10.225.176	10-22-2014 10:38:11	10-22-2014 10:42:47	Scanner Test
29459	001C426DB380	SLWIN7	OPADEV000D	192.168.100.124	10-24-2014 12:43:40	10-24-2014 13:05:20	TE-5250

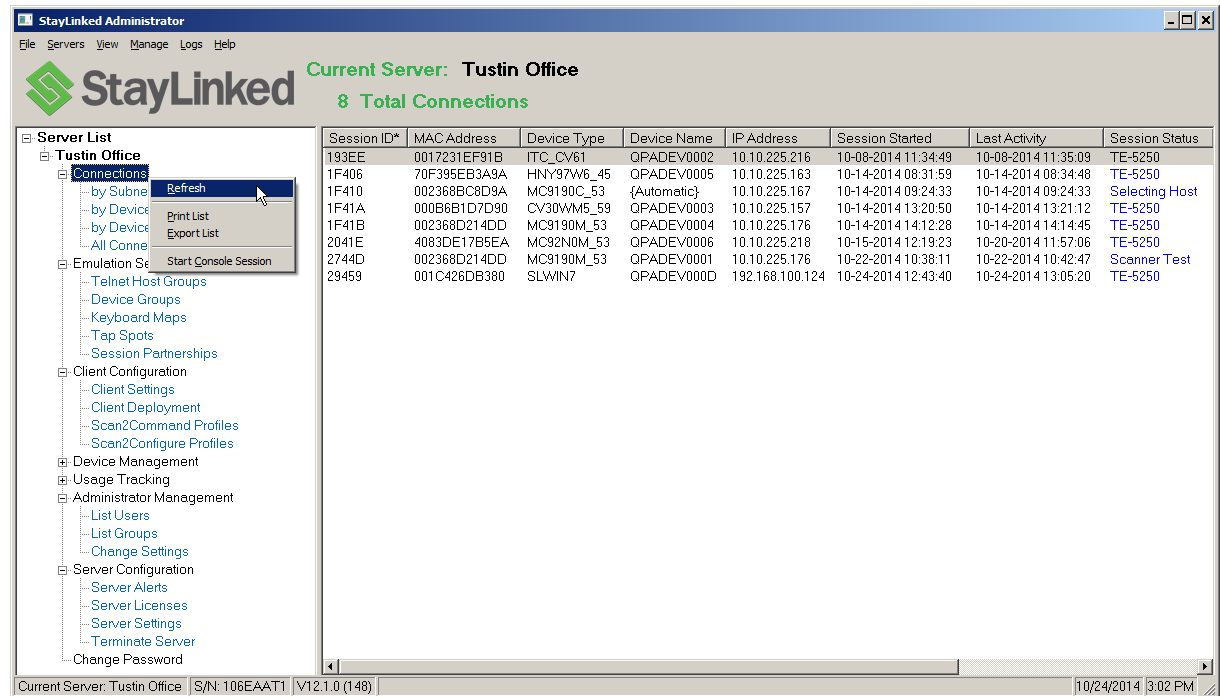
The Connections List information can be sorted into ascending or descending order by clicking on any of the column headers. The currently sorted column will be indicated by an asterisk (*). You can also drag the columns into any arrangement that you desire. The information displayed in the columns of the list and in the Connection Details list includes the following:

- **Session ID** – A unique identifier for the session.
- **Device Type** – The code that identifies the specific type of the device.
- **Device Name** – The Device Name that has been assigned to the device in the Device Group. Often used for the 5250 Device Description (*DEV D) name associated with the device. This value will be displayed as '{Automatic}' if the device is not assigned a device name.
- **MAC Address** – The hardware address of the network interface contained in the device.
- **IP Address** – The IP address assigned to the TCP/IP stack in the device. If the device is running behind a NAT server, then this value will reflect the PublicIP – PrivateIP.
- **Session Started** – This is the date and time when the session was established.
- **Last Activity** – This is the date and time of the last activity on the device, keystrokes, etc.
- **Session Status** – The status of the StayLinked session. The status text is color-coded to display in 'black' if the device is likely powered-on and available. The status text will be displayed in 'blue' if the device is likely powered-off and unavailable.
- **Client Version** – Identifies the version and build of the StayLinked Client software that is running on the device.
- **User ID** – Identifies the user of the device. The contents of this column depend upon the 'Device Identification' setting for the StayLinked Server. If 'Device Identification' is enabled, then this column will display the value that the user provided when the connection was established. You can also populate this column by using functions of the 'Screen Recognition' feature set. Otherwise, this column will always display '[unidentified]'.
- **Device Mgmt **** – Identifies the status of 'Device Management' software that might be running on the device. This column will be displayed only when Device Management licensing is installed on the server.

**** Note that Device Management features have been discontinued as of September 2015 and removed from the product effective v15.1 build 208.**

3.3.4 The Connections List Menu

When you click on the Connections branch of the server tree, or the blank area of the connections list, a small menu will appear with certain options that affect the connections list.



Refresh – This menu option will cause the currently displayed connections list to be refreshed from the server. There is no automatic or periodic refresh of this data, so you will need to take this option or press F5 whenever you want to get the latest connection list.

Print List – This menu option will send the list of connected devices to a report on your current Windows default printer. The report will include columns for Device Type, Device Name, MAC Address, IP Address, Client Version and User/Device ID.

Export List – This menu option will export the list of connected devices to a 'Comma Separated Variable' (.csv) file of your choice. The export will include all the connections and columns that are displayed in the Connections List. This format is appropriate for import into common spreadsheets and databases.

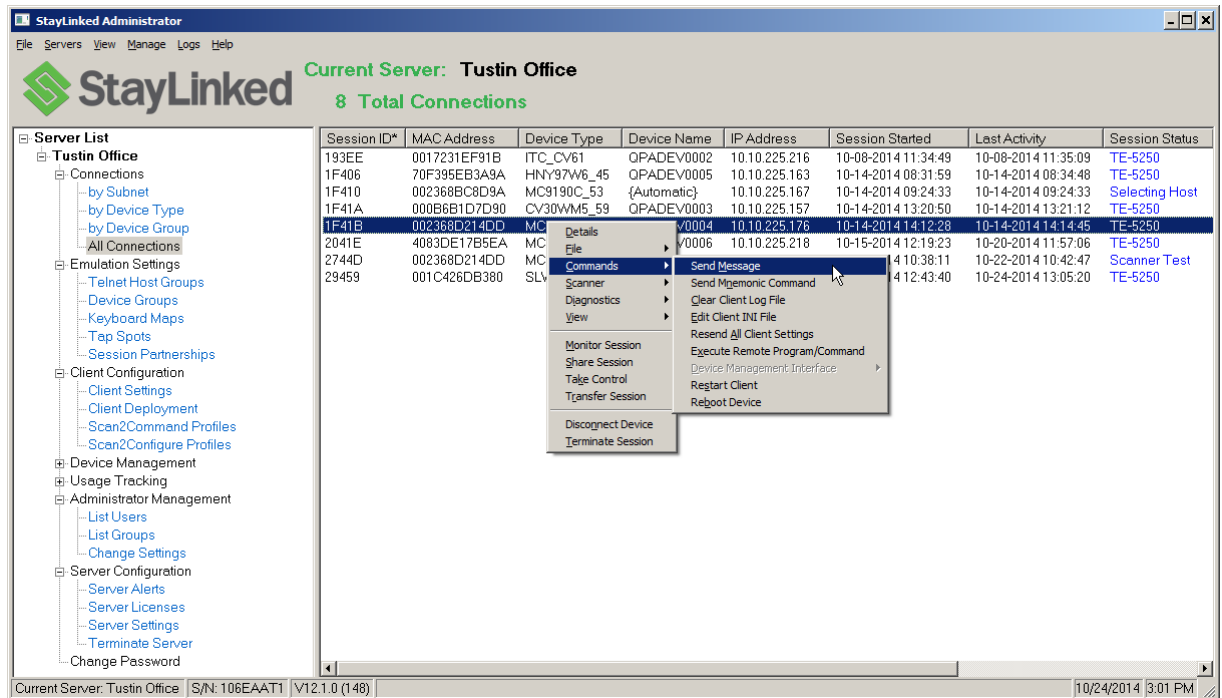
Start Console Session – This menu option will establish a connection to the current StayLinked Server using the built-in StayLinked DOS or Java Console Client. This feature provides an easy way for the administrator to confirm the operation of the StayLinked Server. The StayLinked Console Client runs on the Administrator PC and is a fully functional StayLinked Client for Windows.

Note: *Start Console Session does not work with TESS emulations.*

When you are finished running a Console Session, press the 'Esc' key to "Quit Session" and then press the 'Y' key to end the session. Finally, press the '0' key to exit the Console Client (DOS) or select the File->Exit menu option (Java).

3.3.5 Connections Menu

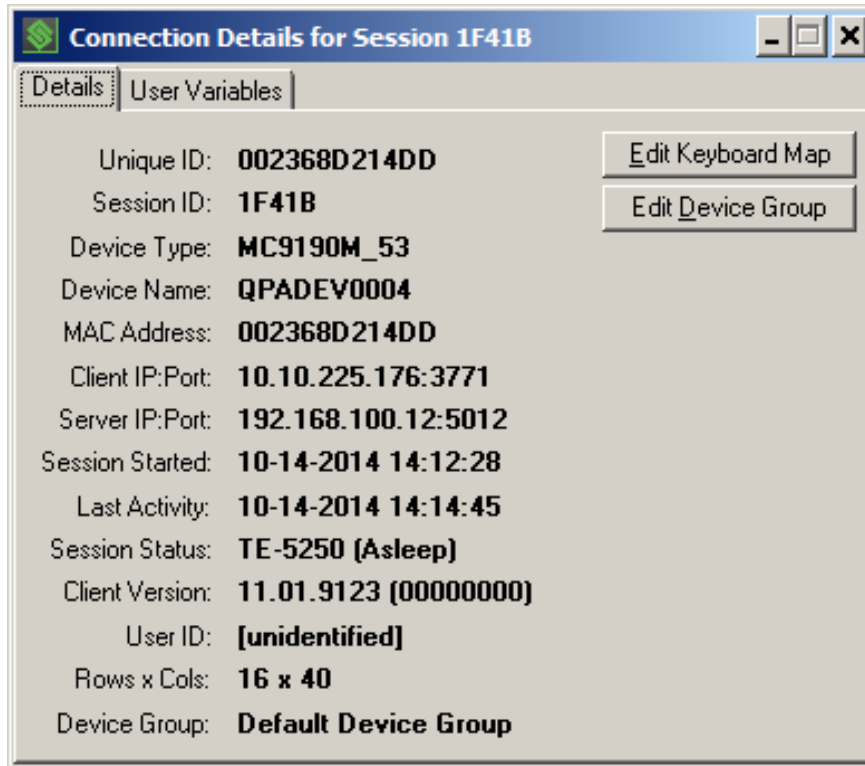
When you view the connections list in the main display panel of the Administrator, the Connections menu is available by clicking the right mouse button over the specified connection in the connections list. Some menu options will function over multiple selections, which means you can highlight multiple connections in the list and then right mouse click. The Commands, Diagnostics, Device Disconnect and Session Terminate menu options will then process all of the selected connections.



When selecting and terminating multiple sessions, the Administrator will display a progress bar. Sessions will be terminated at a rate of one-per-second until all selected sessions have ended, as displayed by the progress bar.

3.3.6 Connections Menu – Details

The first item in the connections menu is the Details window. Select this option to open a window showing details about a particular connection. As noted above, this is the default menu option, which means you can open the Details window by double-clicking a connection list entry. You may open multiple Detail windows at one time as desired.



Details Tab: This tab displays information about the device, connection and session.

- You can right-click on Session ID, Device Type, Device Name, MAC Address and Client IP to copy any of these values to the clipboard.
- You can double-click on the Client IP Address to attempt a 'Reverse DNS' to resolve a 'host name' for the client device.

Edit Keyboard Map: Click this button to launch the Keyboard Map editor for this connection.

Edit Device Group: Click this button to launch the Device Group editor for this connection.

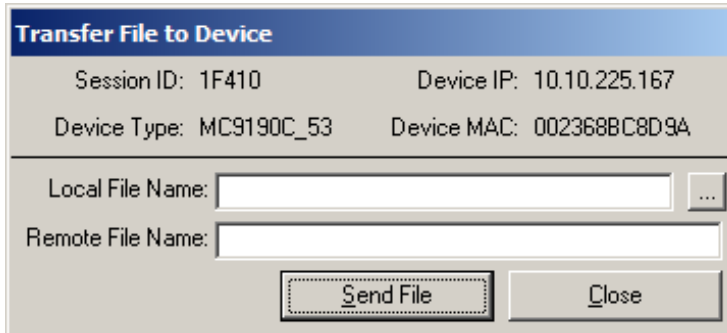
User Variables Tab: This tab will display any defined 'User Variables' that have been assigned for this connection. User Variables are implemented using Host APIs and Screen Recognition features.

3.3.7 Connections Menu – File

Select this option to send a file to the client or receive a file from the client.

File: Send to Device – This panel allows the administrator to send files to the device using the StayLinked Reliable protocol. The files will be stored on the writable media on the device.

NOTE: This option is also available using 'drag-and-drop' from Windows Explorer.



- **Local File to Send:** This is the full path to the file that will be sent to the device. You may use the Browse button to locate this file.
- **Remote File Name:** This is the name of the file that will be stored on the device. You can include the file path. The path must exist on the device and be writable on the device.
- **Send File Button:** Click this button to send the file to the device.
- **Close Button:** Use this button to close the 'Transfer File to Device' dialog.

File: Receive from Device – This panel allows the administrator to receive files from the device using the StayLinked Reliable protocol. The files will be retrieved from the writable media on the device.



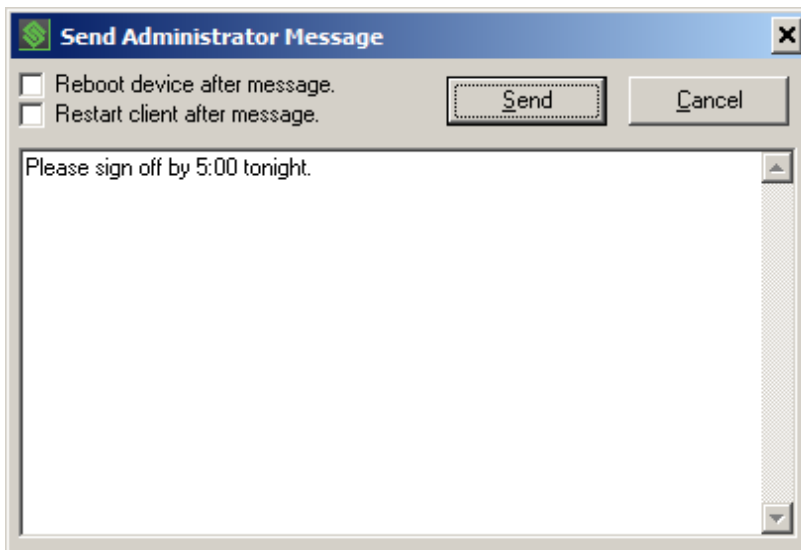
- **Local File Name:** This is the full path to the file that will be received from the device. You may use the Browse button to specify this file name.
- **Remote File Name:** This is the name of the file that will be retrieved from the device. You may include the file path.
- **Receive Button:** Click this button to receive the file from the device.
- **Close Button:** Use this button to close the 'Receive File from Device' dialog.

3.3.8 Connections Menu – Commands

Select this option to perform any of the following commands with one or more selected devices in the connection list:

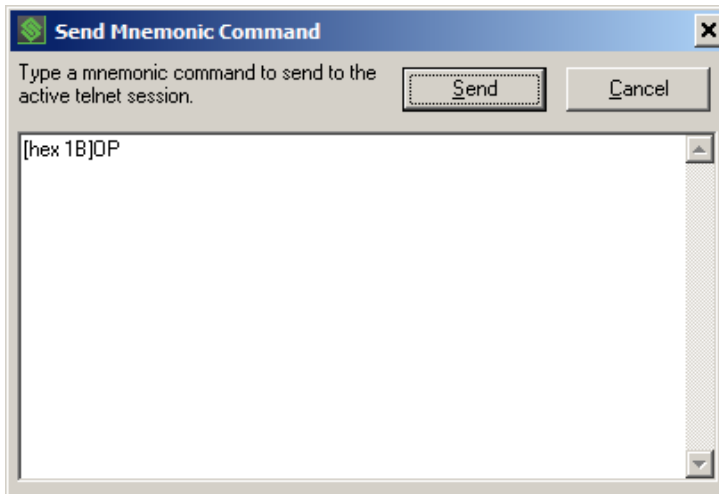
- Send Message
- Send Mnemonic Command
- Clear Client Log File
- Edit Client INI file
- Resend All Client Settings
- Execute Remote Program/Command
- Device Management Interface -> Start/Stop
- Restart Client
- Reboot Device

Commands: Send Message – This panel allows the administrator to send administrative messages to the selected devices. The message will appear on the device screen and you will be required to press a specific key combination to answer the message and proceed. A typical use for this feature is to notify a device user that a software update is about to be installed.



- **Reboot device after message:** This option allows the administrator to have the device automatically reboot after the device user answers the message. After rebooting, the device will automatically reconnect to the same session and display the same screen and cursor to the device user. You can seamlessly continue the previous task after the reboot and reconnect is completed.
- **Restart client after message:** This option allows the administrator to have the client software automatically restart after the device user answers the message. After restarting, the device will automatically reconnect to the same session and display the same screen and cursor to the device user. You can seamlessly continue the previous task after the restart and reconnect is completed.
- **Message Text Box:** Type your message into this text box.
- **Send Button:** Click this button to send the message to the device.
- **Cancel Button:** Use this button to close the 'Send Administrator Message' dialog.

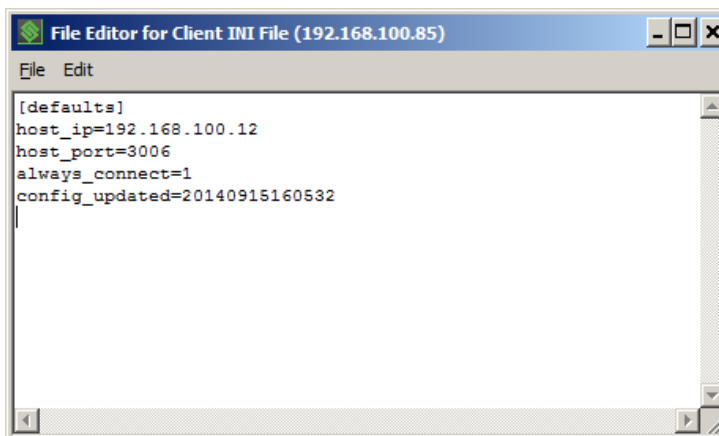
Commands: Send Mnemonic Command – This panel allows the administrator to send mnemonic commands to the telnet sessions running for the selected device. The mnemonic command will be transmitted to the telnet host after substitution script processing. A typical use for this feature is to test VT escape sequences for specific functions against the telnet server and application.



- **Send Button:** Click this button to send the mnemonic command to the telnet session.
- **Cancel Button:** Use this button to close the 'Send Mnemonic Command' dialog.

Commands: Clear Client Log File – This command causes the log file on the client to be cleared. The client log file is named staylink.log and is stored on the device's writable media. StayLinked Support generally uses the client log file for debugging and problem analysis.

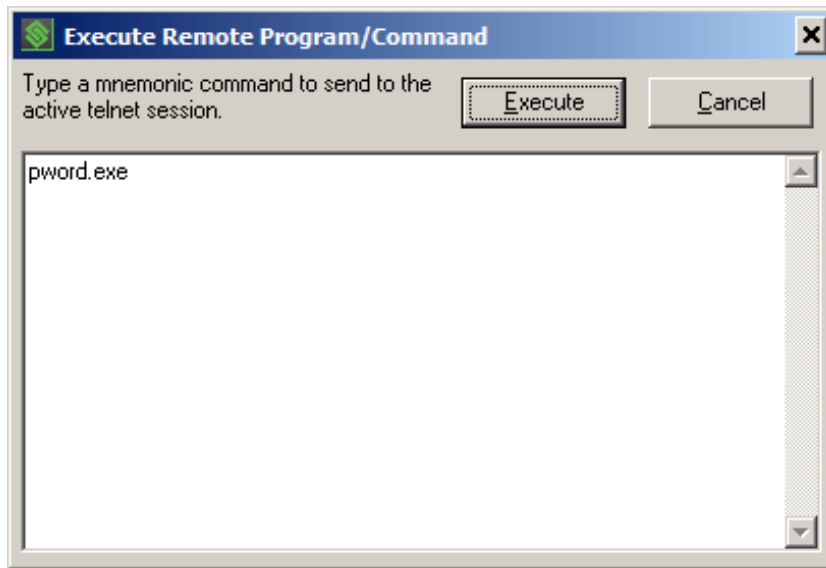
Commands: Edit Client INI File – This panel allows for quickly editing the Client Configuration File. The Client Configuration file is named staylink.ini and is stored on the device's writable media.



- **File -> Save Changes to the Device:** Select this menu option to cause the edited Client INI file to be saved and the file to be transferred back to the device. The device must be awake and on the network in order to transfer the file back to the device.
- **File -> Exit:** Select this menu option to close the dialog without sending any changes.
- **Edit -> Find and Edit -> Find Again:** Select this menu option to preset a 'Find' dialog that will search the configuration file for your desired text.

Commands: Resend All Client Settings – This command causes the server to send all active client settings to the client device, replacing any previous values found there. This is an override to the existing “smart” client settings update that occurs during the device connection request. This command will not trigger a transmission of any ‘Configuration File Transfer’ client settings.

Commands: Execute Remote Program/Command – This command allows you to specify a command to run locally on the device. The command can call a program that is installed on the device or invoke a local OS command on the device. Please note that commands that are valid on one OS (DOS) may not be valid on another OS (PPC, iOS, Android).



- **Show ‘Press Any Key’:** This option will cause a ‘Press any key’ message to be displayed on the client device after the command has been executed.
- **Clear Device Screen:** This option will cause the screen to be cleared on the client device prior to executing the command.
- **Command Text Box:** Type the command/program to call into this text box.
- **Execute Button:** Click this button to send the command to the device.
- **Cancel Button:** Use this button to close the window.

Commands: Device Management Interface -> Start/Stop – These commands are only available if the client is running the tightly integrated StayLinked Device Management components. Using these commands, the Device Management Interface (service) on the device can be stopped and started. *(removed v15.1 build 208)*

Commands: Restart Client – This command causes the client software to exit the active session and return to the Main Menu. The active session will not be terminated. When the device user selects the ‘Connect to Host’ option on the Main Menu, the device will automatically reconnect to the same session and display the same screen and cursor to the device user. The user can seamlessly continue the previous task after the reboot and reconnect is completed.

Commands: Reboot Device – This option allows the administrator to have the device automatically and immediately reboot. After rebooting, the device will automatically reconnect to the same session and display the same screen and cursor to the device user. The user can seamlessly continue the previous task after the reboot and reconnect is completed.

3.3.9 Connections Menu – Scanner

Select this option to initiate any of the following scanner laser functions on one or more selected devices in the connection list (only applies to devices that support soft-scan laser functions):

- Trigger a Soft Scan
- Disable Scanner Laser
- Enable Scanner Laser

3.3.10 Connections Menu – Diagnostics

Select this option to initiate any of the following diagnostic utilities on one or more selected devices in the connection list:

- Radio Stats
- Echo Test

These tools are described in detail in the Client User Guide that matches the client version on the target devices.

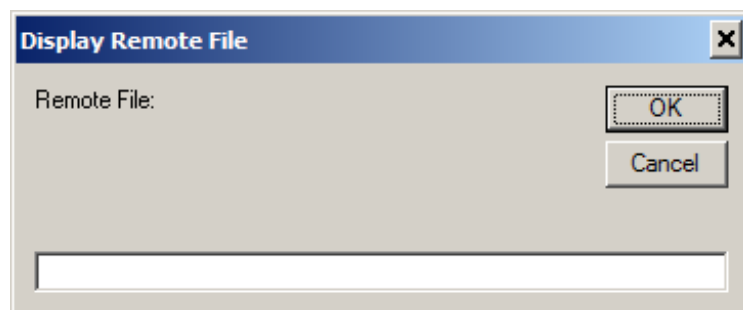
3.3.11 Connections Menu – View

View: Radio Config – This option allows the administrator to view the contents of the Radio Configuration file. The Radio Configuration file is named pkt.ini and is stored on the device's writable media. Some devices do not utilize a pkt.ini file and in this case, you will get a 'File Not Found' message when you try to view the file. Or, the client may be designed to synthesize a pkt.ini file and will provide that file containing important radio configuration information.

View: Network Config – This option allows the administrator to view the contents of the Network Configuration file. The Network Configuration file is named net.cfg and is stored on the device's writable media. Some devices do not utilize a net.cfg file and in this case, you will get a 'File Not Found' message when you try to view the file. Or, the client may be designed to synthesize a net.cfg file and will provide that file containing important network configuration information.

View: Client INI File – This option allows the administrator to view the contents of the Client Configuration file. The Client Configuration file is named staylink.ini and is stored on the device's writable media.

View: Remote File – This option allows the administrator to view the contents of a specified file on the client device.



- **Remote File:** Type the file name that you wish to view into this text box.
- **OK Button:** Click this button to send the request to the device.
- **Cancel Button:** Use this button to close the window.

View: Client, Session, Handler, and Socket Logs – These options allow the administrator to view the contents of the specified log file from the client device or from the server.

View: ZIP All Session Logs – This option allows the administrator to collect and package available logs for the selected session into a single compressed ZIP file.

View: Usage Tracking – This option allows the administrator to view the 'Usage Tracking' information for the currently selected device. The user interface will be transformed into the Usage Tracking List for the specific Unique ID for the selected device.

View: Session Screen Dump – This option allows the administrator to view a special 'Screen Dump' text file that is generated by the StayLinked Server and reflects the current status of the session screen for the selected device. This screen dump file is useful for screen localization efforts, especially for foreign language font glyph support.

View: Device Screen Capture – This option is only available if the client is running the tightly integrated StayLinked Device Management components. This option allows the administrator to capture an image of the device screen in the JPEG file format. The screen will be displayed in the application that is currently associated with the JPG file extension.

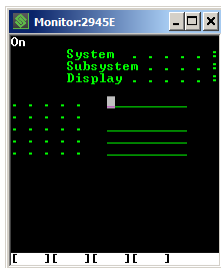
Device Management has been end-of-life since September, 2015.

View: Export Screen Map – This feature will generate a screen map of the current session telnet screen. The screen map is used for Screen Recognition and Screen Reformatting 'Designer' feature. After the screen map is prepared and transferred to the Administrator, you will be prompted for a unique name for the screen map. You can read more about this option in the 'StayLinked Screen Recognition and Reformatting User Guide'.

Note that screen maps can also be captured using a keyboard map entry To optimize the collection of screen maps for your application, you can use a new [screen_map] mnemonic that can be added to your device's keyboard map. While navigating your screens in a StayLinked Session, you can press the key combination that you have mapped to the [screen_map] mnemonic and the StayLinked Server will immediately capture a map of the current telnet screen and save it into the Screen Maps master file. The screen map will be automatically named using this pattern: 'PushButtonScreenMap_SSSSS_yyyymmddhhmmss' where 'SSSSS' indicates the Session ID and 'yyymmddhhmmss' is a date/time stamp representing the moment that the screen map was captured. After you have completed capturing all of your desired screen maps, you can use the 'Telnet Host Groups -> Manage Screen Maps' dialog to review and rename your screen maps for use in screen recognition and reformatting. This option should not be available to users, as it directly writes to a server configuration file and multiple simultaneous entries can cause file write issues. These features are not currently available for SmartTEK devices or TESS emulations.

3.3.12 Connections Menu – Monitor Session

This feature provides the administrator with the ability to view and monitor the selected device session in a window on the PC. This option behaves as a toggle, turning the monitor feature on and off, depending upon the current monitor state. Devices that are currently being monitored will have a checkmark on the Monitor menu option. When you start the monitor, you will be prompted to confirm and then the monitor window is displayed and the current screen from the device will be shown:

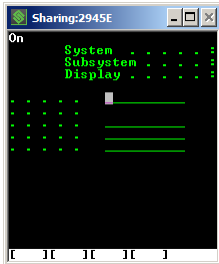


This monitor window will be updated in real time as the device is utilized. You may monitor more than one device at a time, depending upon the available space on your desktop. In order to terminate a monitor session, find the device in the connection list and select the 'Monitor' menu option again to toggle this feature off. The monitor window on your PC will close automatically. Or, just click on the [X] in the Monitor Window to close the monitor session. NOTE: Monitor Session is not available for sessions running Blowfish encryption.

Resizing this window, skewed or shifted monitors can be corrected using configuration options in the console window. Review the knowledgebase article regarding skewed monitor issues for more details. Do not drag or pull edges to resize this window.

3.3.13 Connections Menu – Share Session

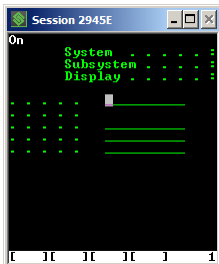
This feature provides the administrator with the ability to collaborate with the selected device session. The shared session will be displayed in a window on the PC.



As the administrator, you are able to type into this window and drive the session. The original user will see your changes on the device. Inputs from the device, will also affect the session, appearing in your share window. You may share more than one session at a time, depending upon the available space on your desktop. In order to exit a shared session, press the 'Esc' key and you will be prompted to 'EXIT SESSION? (Y)es or (N)o'. Press 'Y' to quit the session. The original user will be able to continue. Shared sessions appear in the Administrator's connections list with a status noting the share and original session id.

3.3.14 Connections Menu – Take Control

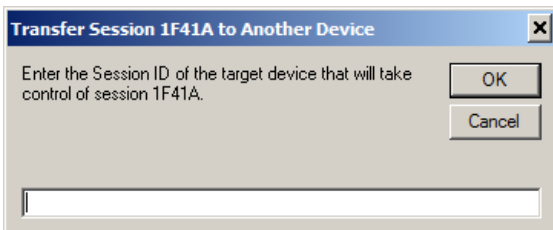
This feature provides the administrator with the ability to take over the selected session in a window on the PC. This removes the session from the remote device and brings it to the Administrator PC. When you select to Take Control, you will be prompted to confirm and then the session window is displayed and the current screen from the session will be shown:



You can now type and operate the session as if you had started the session yourself. The Take Control function is not reversible. Once you take control of a session, the device will not be able to regain control of that session. The device might be able to start a new session. This feature is especially useful to complete sessions after a device has been damaged or otherwise disabled and can no longer be used. Administrator sessions can be transferred to a device as mentioned below.

3.3.15 Connections Menu – Transfer Session

This feature provides the administrator with the ability to transfer a session from one device to another. This feature is especially useful when a device has become disabled while it was in the middle of an important operation. In this case, the session that was associated with the damaged device can be transferred to an operational device, at which point the important operation can be completed using the target device. When you select this option, you will be presented with a dialog that will ask for the target device to which the session will be transferred. This device must already be connected to the StayLinked server:



Enter a valid session ID and, if verified, the session will be transferred to the target device.

3.3.16 Connections Menu – Disconnect Device

After a confirmation, this option will send a directive to the device(s) to disconnect from the session and return to the main screen. The session stays alive on the server waiting for the device to reconnect. This option will cause a device that is running in the 'Always Auto-Connect' mode to exit back to the main screen.

3.3.17 Connections Menu – Terminate Session

After a confirmation, this option will send a directive to the server to immediately terminate the selected device connection(s). When multiple sessions are selected, the Administrator will display a progress dialogue and terminate sessions individually at one-second intervals until all selected sessions have been ended.

3.3.18 Connections Menu – Launch MobiControl

This version of the StayLinked Administrator supports basic integration with the MobiControl Deployment Server. You can configure the MobiControl settings for the current StayLinked Server in the 'Edit StayLinked Server' dialog as described in the 'Connecting to the StayLinked Server' section of this guide. If the 'Always Available?' option is selected for the MobiControl integration, then this 'Launch MobiControl' menu option will be available. This option will launch a Web Browser session and connect to the MobiControl Deployment Server and display the Remote Control dialog. If the device is awake, the MobiControl Agent is running on the device, and if the MobiControl Deployment Server is aware of this device, then this menu option will provide quick access to the MobiControl system.

3.3.19 Connections Menu – Manage Device

If the tightly-integrated StayLinked Device Management software is installed and detected on the device, then this option will be available to access all of the interactive device management options provided by the StayLinked Device Management feature set. Please review the 'StayLinked Device Management User Guide' for full details of these interactive features. **Integrated 'Device Management' features have been end-of-life since September, 2015 and replaced with SOTI MobiControl integration. These features are removed in v15.1 build 208 and newer.**

3.4 Telnet Host Administration

This section describes the various means provided to group and define your Telnet hosts that will be accessed from each StayLinked server. You can define one or more Telnet hosts per server to which your wireless users will connect.

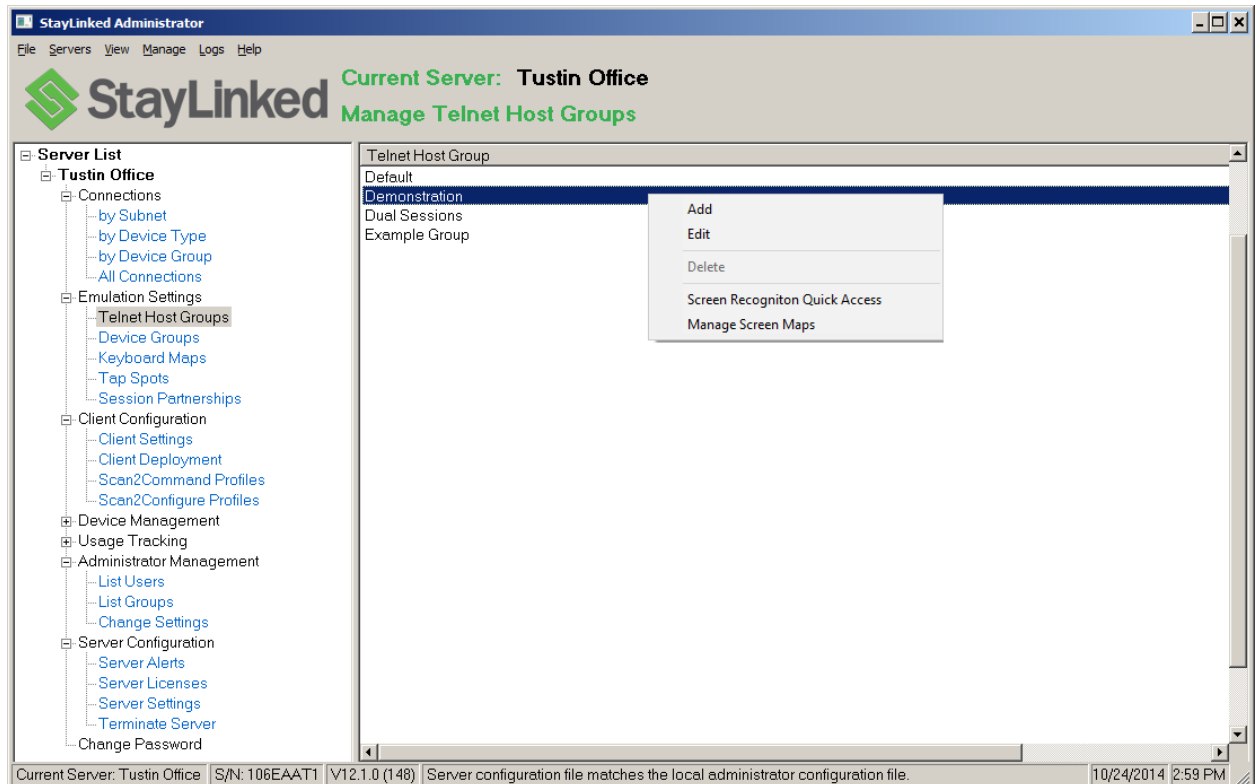
Telnet Hosts are organized into 'Host Groups' that can be assigned to 'Device Groups', allowing you to control what Telnet hosts are available to specific devices. Various host groups can be created to provide multiple configurations of hosts, as required by your architecture. When more than one host is defined for a host group, the list of hosts will appear as a menu on the wireless device when a new session is started and the user will be able to select the Telnet host to which they'd like to connect.

This selection process can also be automated using the "preferred host" setting. Clients using the custom configuration file 'connections.ini' can receive a new version of this file from the StayLinked server. For those devices not configured for Multiple Connections, the preferred host setting can be distributed to client for using the Administrator's client settings.

In the following example, you can see the mandatory 'Default' host group, plus we have defined a few additional host groups. The 'Default' host group may be changed, but not deleted.

3.4.1 Maintaining Host Groups

When you select 'Telnet Host Groups' from the server tree or the Manage menu, the Telnet Host Groups list will appear in the main display panel. Each StayLinked server will have a 'Default' host group, and you can add other host groups as required. Clicking the right mouse button in a blank area or on a host group will cause a small menu to appear with options to Add, Edit, or Delete a group.

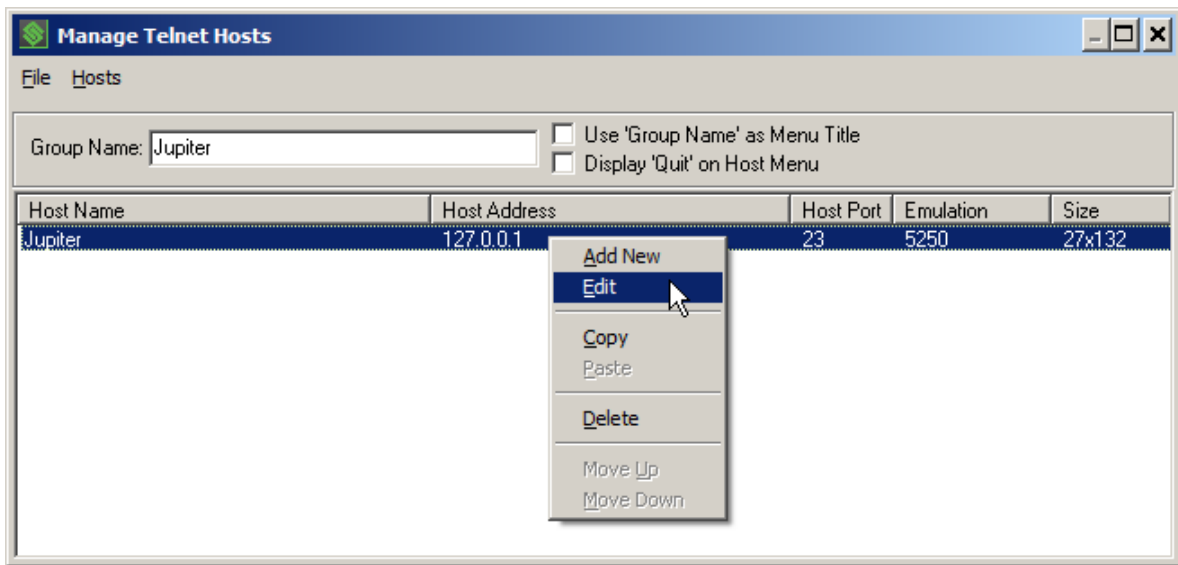


Additional options include:

Screen Recognition Quick Access – This allows the Administrator to open all of the existing screen recognition events in this telnet host group for quick adjustments. It does not allow the creation of new events, which must still be completed by navigating the to desired host entry.

Manage Screen Maps – This opens a list of all screen maps for all hosts. Management of screen maps outside of the host entries allows renaming to be applied to all references among all host entries, even those in multiple host groups. Screen maps referenced in any host group cannot be deleted until the reference is removed.

When you select the Delete option, you are prompted for confirmation. If you select the Add or Edit options, the following window will appear where you can enter/edit the host group definition.



The host group has a 'Group Name' plus two additional options. These options will only affect host groups that contain more than one host entry. If there is more than one host entry, a user creating a new connection will be presented with a menu on the device screen from which they can select the desired host. If the menu is displayed, you can control these two options:

- **Use 'Group Name' as Menu Title:** Check this option to have the 'Host Group Name' displayed as the title of the host selection menu on the device screen. If this option is not checked, then the menu title will default to 'Select a Host'.
- **Display 'Quit' on the Host Menu:** Check this option to include a 'Quit StayLinked' option on the host selection menu. The 'Quit StayLinked' menu option enables you to cancel the connection and return to the main StayLinked Client Menu on the device, without connecting to a Telnet Host.

For the host group, you may also add, edit, copy, paste, delete and change the order of the Host entries using the "Hosts" menu or by clicking with the right mouse button in the host list.

Copy and Paste for Host Entries: These options provide a convenient method to copy a pre-configured Telnet Host Entry from one Host Group and paste it into the same or another Host Group.

The two additional options are not available for the 'Default' Host Group. If you want to take advantage of the **Use 'Group Name' as Menu Title** option or the **Display 'Quit' on the Host Menu** option, then you will have to add a new Host Group where these options will be available. You can then use the 'Device Group' feature to make your new Host Group available to your devices.

3.4.2 Maintaining Host Settings

When you add or edit a Host Entry within a host group, the following window will appear that shows the current host settings and allows you to make changes.

Update Host Entry

Manage Properties

Host Information

Name: Jupiter

Address: 127.0.0.1 Telnet Port: 23

Emulation: 5250 Size: 24x80

ViewPort

☒ Locked Row: 1 Col: 1 ☒ Follow the Cursor

Host Options

☐ Caps Lock ☐ Clear Field on Data Entry

Keyboard-Only Field Attribute: Always Allow Scan Entry Scan-Only Field Attribute: Always Allow Keyboard Entry

Tap Spots Collection: Default Tap Spots for 5250

Host API Configuration

Separator Char: 0x7E Row: 1 Col: 2 ☐ Show API Screens

Host Startup Script

sldemo[fldext]sldemo[enter]

Insert Mnemonic:

Reconnect Script

Emulation Properties

Property	Value

Name: This is a descriptive name for the Telnet Host, i.e.: "Production SAP".

Address: This is the Host Name or IP address for the Telnet Host.

Telnet Port: This is the Telnet Port for the Telnet Host, typically port 23.

Emulation: Select the type of client emulation to use when connecting to the Telnet Host.

- **Emulation Types:** 5250, 3270, TESS or many VT emulations, including UTF8 and SSHv2, to choose from. (See Secure Communications Guide for details about SSL-Telnet and SSH connections.) Note that SmartTek licensing is only usable by select Zebra devices and is required in order to connect to TESS emulation hosts.

- **SHARE-IP, SHARE-ID or SHARE-MAC:** These SHARE options will enable a device to share a session with another StayLinked device that has already established a terminal session. The one requirement for 'Sharing' a session is to identify the device that is running a session that you want to share. The server will prompt the user for this identification value, depending upon the SHARE-type selected here. The user will be required to scan or type the target device's MAC Address, IP Address or Device ID. Once this value is provided, then the server will look for a running session that matches the value provided. If a session is not found, then the user will be notified and will be prompted to re-enter the identifier. If an active session is found, then the device will be connected to that session and begin sharing the terminal session with the original device. The original device still 'owns' the session and this device is only sharing the session. Both devices can type or scan into the session and both devices will see screen updates to the session. When the device is done sharing the session, the user should select to 'Exit' the session. The owner device will still have control of the session and will be able to continue processing.
- **PGMCALL:** The PGMCALL emulation type enables the StayLinked Server to cause the device to run a program that is installed locally on the device. So, if you select this Host Menu option, rather than connecting to a telnet session, the specified program will be run locally on the device. When you select PGMCALL, only two other settings are used by the system. The 'Name' entry will contain the description of the program call that will be displayed on the host menu on the device. The 'Address' entry will be used to enter the name of the program to be called on the device.
Example: Emulation: PGMCALL, Description: Print a Label, Address: PRINTLBL.EXE
For some DOS devices with limited RAM, you can cause the StayLinked Client to be removed from memory before running the local program. Just enclose the program name in square brackets []. The square brackets will notify the StayLinked Client that you want to use the entire available RAM to run the local program. In this case, the StayLinked Client will exit, the local program will run, and when complete, the StayLinked Client will automatically restart.
- **DMONLY:** The DMONLY emulation type enables the StayLinked Server to cause the device to run a Device Management Only session. There will be no Telnet or SSH access provided in this Device Management Only session. The client software will behave much differently on the device when the client is running a Device Management Only session.
The 'Device Management' features have been end-of-life since September, 2015.

Size: You can select the size of the Telnet Session Screen. This value refers to the 'telnet session screen' that resides on the StayLinked server, not the size of the device view port. The available values depend upon the type of client emulation selected.

ViewPort: These settings describe how to handle the device view port for the Telnet Host. For example, a small wireless device might have a screen that can support 20 columns and 15 rows. The Telnet host is putting out 80 columns and 24 rows. The view port then is that part of the full screen that is displayed on the small device screen.

- **Locked:** Check this box and set the Col and Row for the upper-left corner of the locked view port.
- **Follow the Cursor:** Check this box to ensure that the view port on the device will follow the cursor if the application positions the cursor outside of the current view port.

Caps Lock: Check this box to force all keyboard entry to this Telnet Host to be capitalized.

Clear Field on Data Entry: For 5250 and 3270 hosts, check this box to cause the current field to be cleared when data is typed into the first position of, or when a barcode is scanned into the field.

Keyboard-Only Field Attribute: For 5250 and 3270 hosts, select the field attribute that will designate a 'keyboard-only' field. All fields that match the selected attribute will allow only keyboard data to be entered into the field. Scanner data will not be allowed into these fields.

Scan-Only Field Attribute: For 5250 and 3270 hosts, select the field attribute that will designate a 'scan-only' field. All fields that match the selected attribute will allow only barcode scans to be entered into the field. Keyboard entry will not be allowed into these fields. This attribute must be different from the Keyboard-Only Field Attribute.

Tap Spots Collection: You can select the Tap Spots Collection that you wish to use with this Telnet Host.

Host API Configuration: These options control the behavior of the StayLinked Host APIs.

- **Separator Char:** You can specify the hexadecimal value of the displayable character that will be used as the separator within the Host API data on the screen. (default is 0x7E for tilde, ~)
- **Row and Col:** Allows you to specify the row and column where your end-user applications will display StayLinked Host API data. The row and column should reflect the screen position of the first separator character in the API command specification. The default Host API location is row 1 and column 2.
- **Show API Screens:** You can use this checkbox to select whether or not to show the screen containing the Host API data to the user on the device.

Host Startup Script: You may define a startup script for this Telnet Host. The startup script will be processed only when a new session is established. The script will not be run when a device reconnects to an existing session. The script will always be processed against the first host screen that is presented to the device, typically a logon screen. The script can be up to 255 characters in length. The script can contain any combination of characters and emulation mnemonic keywords. Emulation mnemonic keywords are contained within square brackets []. Special scripting mnemonics are detailed in the appendix at the end of this document. You can select mnemonic keywords from the 'Insert mnemonic' drop-down list, causing the selected mnemonic to be automatically inserted at the current cursor location within the script textbox. Syntax errors in the script will not cause errors, but may cause portions of your script to be ignored by the emulation host.

- Startup Script example: myuserid[fldexit]mypasswd[enter]

The example 5250 Startup Script above is designed to be processed against a 5250 logon screen. The user profile 'myuserid' will be automatically typed into the first field on the screen and then the 'Field Exit' mnemonic will be processed, moving the cursor to the next field on the logon screen. Then, the password 'mypasswd' will be typed into the current field and the 'Enter' key mnemonic will be processed. This script would cause a user to be automatically signed onto the target IBM I Telnet host.

Reconnect Script: You may define a reconnect script for this Telnet Host. The reconnect script will be processed only when a device reconnects to an existing session, or when a device switches between multiple sessions. The reconnect script is most valuable for voice-enabled sessions and can be used to notify the application that it should repeat the last Text-to-Speech instructions and the last Voice Rules instructions.

Emulation Properties: Depending upon the emulation type selected, you will have additional properties available that can be used to adjust the behavior and settings of the Telnet client. A list will appear at the bottom of the Host Properties window showing the emulation properties that have already been defined for this host and their values.

You can right-click within the list area or use the Properties menu to add, edit and delete the Emulation Properties for this Telnet host. Emulation properties that have been added to this list box will no longer appear in the pulldown. Some emulation properties will have different names, usage or options depending on your emulation type. TESS emulation properties are described in the support guide for TESS emulation. 5250, 3270 and VT properties include:

- **Host Backup 1 & 2 Name/IP** – Determines the 1st and 2nd backup host IPs or hostnames.
- **Host Backup 1 & 2 Port** – Determines the 1st and 2nd backup host port numbers.

- **Telnet Session Inactivity Timeout** – Specifies the number of seconds of inactivity before the Telnet Session is automatically terminated (60 to 2073600 seconds).
- **Telnet Session Inactivity Script** – You can enter a script that will be run before the session is terminated because of a Telnet Session Inactivity Timeout event.
- **Telnet Input Throttle** – You can enter the number of milliseconds that will elapse between user input into the Telnet Session (0 to 100).
- **Avoid Duplicate Workstation IDs** – Set to true to append characters in the range of 1-9 and A-Z to the end of the workstation ID. This ensures that the 5250 workstation ID does not conflict with the workstation IDs from this or other devices.
- **Truncate Workstation IDs** – Specify to truncate from the beginning or from the end of the 5250 workstation ID, when necessary. The workstation ID must not exceed 10 characters.
- **Maximum Attempts to Avoid Duplicates** – Enter the maximum number of attempts allowed to avoid a duplicate 5250 workstation ID (1 to 250, Default = 10).
- **Fixed Foreground Color** – Select a fixed foreground color that will always be used for this session.
- **Fixed Background Color** – Select a fixed background color that will always be used for this session.
- **Screen Print Format Script** – Enter the printer formatting script to append to the beginning of the screen print text.
- **Print Completion Action Override** – Enter the print completion action that will override the action defined in the Device Group.
- **Print Continue Action Override** – Enter the print continue action that will override the action defined in the Device Group.
- **Print Cancel Action Override** – Enter the print cancel action that will override the action defined in the Device Group.
- **Reject Scan Too Long for Field** – Set to true to cause scanned data too long for the field to be rejected. (5250 and 3270 only)
- **Reject Input While Inhibited** – Set to true to cause any data input to be rejected while the host is Inhibited [INH]. (5250 and 3270 only)
- **Allow Input While Not In A Field** – Set to true to allow input to be processed when the cursor is not on an input field. (5250 and 3270 only)
- **Beep After Inhibited** – Select the type of beep to sound after the host returns from being Inhibited [INH]. (5250 and 3270 only)
- **Auto-Reset Locked Keyboard** – Set to true to automatically reset the keyboard if locked [LCK]. (5250 and 3270 only)
- **Auto-Field Exit on CHECK(FE/RB/RZ) Fields** – Set this value to True to cause StayLinked to add a Field Exit to Barcode Scans and insert a Field Exit when you press Enter on a CHECK(FE/RB/RZ) field, except when the cursor is in the first position. (5250 only)
- **Strictly Enforce Numeric Only Fields** – Set this value to True to cause StayLinked to validate keyboard input only for strictly 'Numeric Only' fields. Default validated any numeric field (5250 only)
- **Enable ENPTUI** – Enables limited support for Enhanced Non-Programmable Terminal Interface features.
- **Enhanced RLE Encoding Support** – Set to true to force enhanced RLE encoding for this host entry. Enhanced RLE support reduces the number of packets sent to full-screen devices, but requires that the client supports the Enhanced RLE Encoding feature.
- **Tap Cursor Action** – Enter the action to be performed when the current cursor location is tapped.
- **Tap Cursor Proximity** – Select how close to the current cursor location a user must tap.

- **Tap Cursor Movement** – Allow the cursor to be moved to the screen location that was tapped. This setting overrides the same option that is defined in the 'Tap Spot Configuration'.
- **Tap Numbers** – Allow any numbers on the screen to be tapped and used for input. This setting overrides the same option that is defined in the 'Tap Spot Configuration'.
- **Tap Number Maximum Value** – Enter the maximum value of numbers found on the telnet screen which will be processed as tap numbers. (0 = *NOMAX)
- **SSL Session** - To request an encrypted session, set this property to True.
- **SSL Client Certificate Provided** - Determines whether the client has a certificate.
- **SSL Client Certificate URL** - URL of the client certificate.
- **SSL Client Certificate Password** - Password of the client certificate.
- **SSL CustomizedCAs.p12 Alternate File** – Fully qualified path and name of the alternate CustomizedCAs.p12 file.
- **SSL CustomizedCAs.p12 Alternate Password** – Password for the alternate CustomizedCAs.p12 file.
- **Host Code Page** – Determines the language (Code Page) supported by the host telnet server.
- **Host Code Page Unicode Processing** – Specifies whether the selected Host Code Page requires Unicode character processing.
- **Host Keyboard Language Type** – Determines the KBDTYPE and CHRID values that will be set for the 5250 Device Description.
- **Convert 5250 Column Separators** – Determines if 5250 Column Separator attributes will be converted to the selected alternate attribute for display.
- **Convert 5250 High Intensity** – Determines if 5250 Column Separator attributes will be converted to the selected alternate attribute for display.
- **Hidden Field Character** – Enter the single character that will be used to replace non-space characters in a hidden (password) field that is input capable. Space is default. (5250 and 3270)
- **Enable Telnet Proxy Logging** – Causes the Telnet Session to connect through an integrated proxy that will record the inbound and outbound telnet traffic to a log file. (5250 and 3270 only)
- **Enable Telnet Proxy Processing** – Causes the Telnet Session to connect through an integrated proxy that will record the inbound and outbound telnet traffic to a log file and/or scrub telnet traffic of invalid VT ESC Sequences. (VT only)

Proxy Scrubbing was added in v12.1 build 128 to aid in the processing of unsupported sequences from the telnet host data stream. The original implementation removed the combination of escape followed by any control code.

0x1B plus 0x00 thru 0x1F is converted to two spaces

The setting for Proxy scrubbing was enhanced in Server v15.0 build 206 to nullify the following Digital Equipment Corporation (DEC) escape sequences from the telnet data stream:

0x1B 0x7E (ESC ~) DEC sequence for Locked Shift - Map G1 into GR

Starting in Server v15.0 build 208 the following additional sequences are removed by Proxy Scrubbing:

0x1B 0x56 (ESC V) DEC sequence for Start Protected Area

0x1B 0x57 (ESC W) DEC sequence for End Protected Area

0x1B 0x46 (ESC F) DEC sequence for Start Selected Area

0x1B 0x47 (ESC G) DEC sequence for End Selected Area

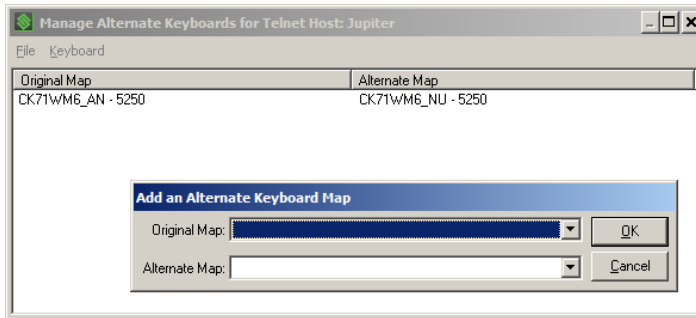
- **Connection Timeout** – Determines the number of seconds to wait before trying a backup host. (VT only)
- **Session Screen Size** – Specifies the number of rows and columns to be used for the VT telnet session screen size. (VT only)
- **Enable Connection Keep Alive** – Determines if the Stay-Linked host-based telnet client will close the connection when the destination address is no longer available. (VT only)
- **Connect to Last Backup Host without Timeout** - Determines whether to timeout when attempting to connect to the last Backup Host. (VT only)
- **Terminal ID** - An ASCII value passed to the host machine to represent the VT terminal type symbolically. This value is usually referenced in the 'termcap' file on the VT telnet host. (VT only)
- **VT ESC Sequence Processing** – Select 'Raw' if your VT Telnet Server requires ESC sequences to be delivered from the client in a single packet only. (VT only)
- **VT Printing Enabled** - Determines if VT Printer Passthrough is enabled. (VT only)
- **Answer Back Message** – Message sent to the host in response to the x05 command. (VT only)

- **Reject Null Key Characters** – Determines whether to reject key characters that are null (0x00). (VT only)
- **New Line Behavior** – Determines the behavior of the new line operation. (VT only)
- **Backspace Behavior** – Determines the behavior of the backspace operation. (VT only)
- **Cursor Movement Behavior** – Determines the behavior of cursor movement. (VT only)
- **Default Keypad Behavior** – Determines the behavior of the keypad. (VT only)
- **Local Echo Behavior** – Determines the behavior of local keyboard echo. (VT only)
- **Autowrap Behavior** – Determines the behavior of autowrap. (VT only)
- **VT Bold Foreground Color** – Select a foreground color to display for characters with a BOLD attribute. (VT only)
- **VT Bold Background Color** – Select a background color to display for characters with a BOLD attribute. (VT only)
- **SSH Terminal Type** – For VT-SSH sessions, select a terminal emulation type. (VT-SSH only)
- **Use SSH Public Key Authentication** – To use Public Key Authentication for the SSH session, set this property to True. (VT-SSH only)
- **SSH Public Keystore File Path** – Path and File of the SSH Public Keystore. (VT-SSH only)
- **SSH Public Keystore Password** – Password of the SSH Public Keystore. (VT-SSH only)
- **SSH Public Key Alias** – Key alias of user's private key stored in the KeyStore file. (VT-SSH only)
- **SSH Public Key Alias Password** – Password of the Public Key Alias. (VT-SSH only)
- **Enhanced TN Session** - Determines whether the session will use enhanced Telnet negotiation features. (3270 only)
- **Session LU Name** - Must be a valid LU name or LU pool name. (3270 only. Requires 'Enhanced TN Session' enabled)

Manage - Alt Keyboards (menu option) Alternate Keyboard Maps: For Telnet Hosts, you can override the keyboard map that a device would normally use and specify a different keyboard map to be used as an alternate.

Keyboard maps are used by the StayLinked system as a cross-reference between the many and varied device keyboards and the various host types (5250, 3270, and VT). With StayLinked, you can use the default keyboard map or alter it to suit the specific needs of your device users and

their applications. In addition, you can create alternate keyboard maps to support variations needed for a specific host or group of users.



In this example, when an Intermec CK71 Windows Mobile 6, Alpha-Numeric keypad device connects to this Host, the alternate keyboard map for the Intermec CK71 Windows Mobile 6, Numeric keypad device will be used instead.

You may add and delete these alternate keyboard maps using the Keyboard menu (the Add New Alternate Map selection window is shown above). The Original Map and Alternate Map dropdowns provide a list of available keyboard maps from which to choose.

In case you are using Custom Device Types for your devices and you want to map them to an existing standard keyboard map, you may select the special value '** Enter a Custom Device Type **' as the 'Original Map'. Then select the desired existing 'Alternate Map'. When you click OK, you will be prompted for a 'Custom Device Type' value that will be used for the 'Original Map' value.

Select "Save Changes" from the "File" drop-down menu to save any changes that you have made to the currently selected host group.

Manage - Barcodes (menu option) Barcode Settings at the Telnet Host Level: If your device belongs to a 'Host Group' that contains more than one host with different emulation types, then it might be valuable to have different barcode settings for the different types of emulation hosts. For instance, if your Host Group contains a 5250 Telnet host entry and also contains a VT220 Telnet host entry, then you might require different barcode suffixes for the different hosts, like a Field Exit [fldext] for the 5250 host and an Enter [enter] for the VT host. The configuration of barcode settings for a Telnet Host entry is identical to the configuration of barcode settings for 'Device Groups' as described in the Managing Barcodes section of this guide. The barcode settings that you define at the 'Device Group' level have priority over any barcode settings that you define at the 'Telnet Host Entry' level.

Manage – Screen Recognition (menu option): For telnet hosts, you can define screens to be recognized and actions to take for those recognized screens. You can grab 'Variables' from the screen text that can be used as arguments in 'Host APIs' or 'Auto-Responses' associated with the recognized screen. You can specify 'Host APIs' to be processed when the screen is recognized. You can specify 'Auto-Responses' which are scripts to be processed when the screen is recognized. You can specify 'Input Modifiers' to adjust the input allowed for the recognized screen. And, you can use the 'Screen Designer' to create a textual or graphical reformatted version of the recognized screen to be displayed on device screens with smaller or different display sizes. The details of the 'Screen Recognition' feature are described in the 'StayLinked SmartTE and Screen Recognition User Guide'. These features are not currently available for SmartTEK devices or TESS emulations.

Manage – Dynamic Screen Settings (menu option): For StayLinked Clients that support rendering of graphical TE elements, you can define how telnet application screens can be automatically and dynamically transformed into modern graphical screens without requiring manual graphical screen reformatting using the designer tool. The details of the 'Dynamic Screen Settings' feature are described in the 'StayLinked Screen Recognition and Reformatting User Guide'. These features are not currently available for SmartTEK devices or TESS emulations.

3.5 Device Group Administration

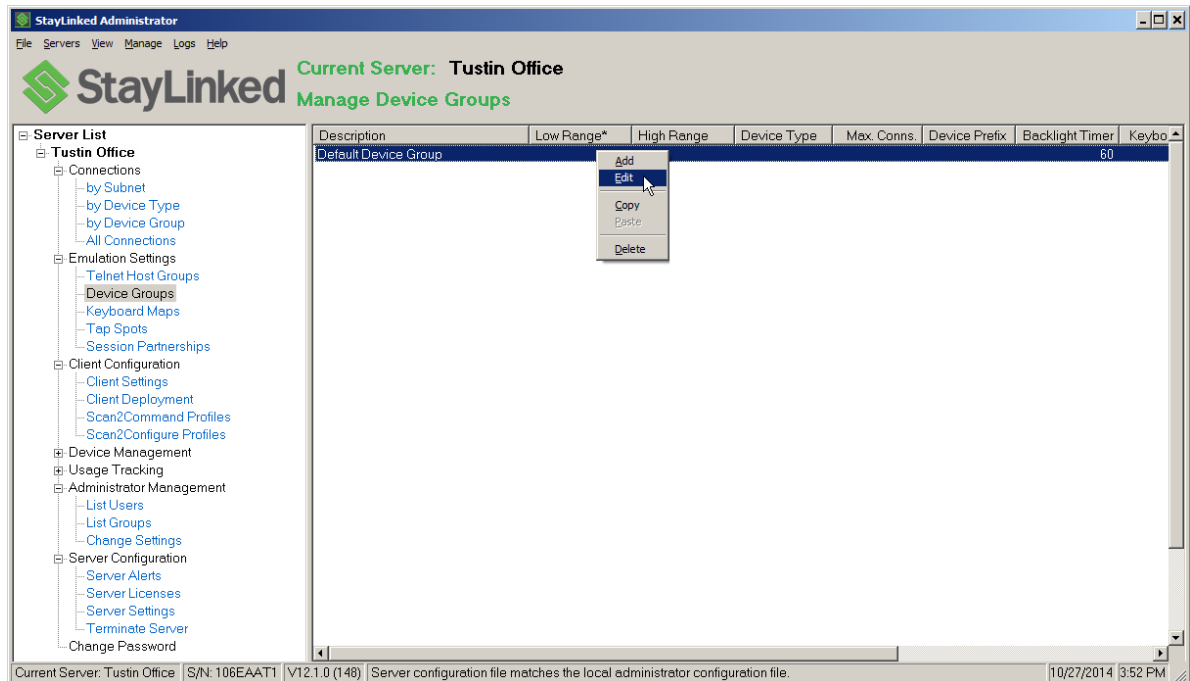
This section describes the various means provided to define your device groups for each StayLinked server. All StayLinked clients that request a session through a server are assigned to a device group by that server. The device group contains many of the vital settings and attributes that control the way a connected device will interact with a telnet host and how it will be handled by the StayLinked server.

Multiple device groups can be defined for each server, but all servers will always have at least a 'Default Device Group'. Initially, all devices that connect to the server are assigned to the default group. You can configure the attributes for the default device group, but it cannot be deleted.

You can also create and manage 'Specific Device Groups'. Specific device groups allow you to manage device configuration information for express subsets of devices. Device groups are defined to control devices within a specific range of IP addresses and for specific device types within that IP range. When each device initiates its connection request, it is assigned to a particular device group based on its local IP address and device type. The device will be assigned to, and use the attributes of, the device group that most closely matches the device's IP address and device type. If the device is not assigned to one of the specific device groups, then the device will be assigned to, and inherit the attributes of the Default Device Group.

3.5.1 Managing Device Groups

When you select Device Groups from the server tree or the Manage menu, the Device Groups list will appear in the main display panel. The Device Groups information can be sorted into ascending or descending order by clicking on any of the column headers. The currently sorted column will be indicated by an asterisk (*). Each StayLinked server will have a Default Device Group and you can add other, more specific device groups as required. Clicking the right mouse button on a device group will pop up a context menu with options to Add, Edit, Copy, Paste or Delete a group.



3.5.2 Maintaining Device Group Settings

When you add, edit, or copy a device group, the following window will appear that shows the current device group settings and allows you to make changes.

Group Description: This is a descriptive name for the Device Group, i.e.: "Shipping Department".

Group IP Address Range: This is the range of device IP addresses for this group.

Device Type: This is the device type filter for this group. The combination of IP Range and Device Type are used to determine which devices will be a member of this device group. Leave this value blank to include all devices in the IP range, regardless of their Device Type.

Maximum Connections: This value will control the number of connections that are allowed to use this device group. (0 or blank = unlimited connections)

Host Group: This is the Host Group that defines which emulation hosts will be available to devices in this device group. If the selected host group is not available at the time a device connects, then the device will automatically use the 'Default' host group. A special host group named 'Device Management Only' is also available for selection. This host group will cause the device to run a Device Management Only session. There will be no Telnet or SSH access provided in this Device Management Only session. The client software will behave much differently on the device when the client is running a Device Management Only session. **The 'Device Management' features have been end-of-life since September, 2015 and removed from the product effective v15.0 build 208.**

Keyboard/Suspend/Sleep Timeout: This value defines how many seconds of inactivity will pass before the device goes into sleep mode. A value of zero will cause the device to never timeout. This timeout requires that the 'Application Lockdown' Client Setting be enabled. The behavior of this timeout is device-dependent.

Backlight Timeout: Defines the number of seconds that the backlight will stay lit between keystrokes or scans on the device. A value of zero will cause the backlight to never timeout. This timeout requires that the 'Application Lockdown' Client Setting be enabled. The behavior of this timeout is device-dependent.

Allow Connections: This checkbox provides the administrator with the ability to determine which devices can establish sessions. This checkbox must be checked in order for devices belonging to this device group to be able to connect to a telnet session.

Allow Multi Sessions: This checkbox provides the ability to control which devices will be allowed to run Multi Sessions. This option will only have an effect if a Multi Session License is installed.

Display 5250/3270 OIA Area: Make sure that this checkbox is selected if you wish for the devices in this group to display the Operator Indicator Area at the bottom of the screen when running 5250 or 3270 sessions. The OIA looks like this: [][][] and notifies you of Input Inhibit, Keyboard Lock, Message Waiting and Insert status. If all indicators were displayed, the area would look like this: [INH][LCK][MSG][INS]. For Version 14 Servers, you can select a 'Graphical Operator Indicator Area' for devices that support graphical elements. This option is configured in the 'Telnet Host Entry' by selecting the 'Dynamic Screen Settings' option under the 'Manage' menu.

Debug OIA: This option provides an enhanced OIA at the bottom of the device display that shows the standard OIA indicators as well as alpha/numeric field attributes, view port origin and the current cursor position. The fully-populated Debug OIA looks like this: [ILM^A 01/001 01/001] The Debug OIA generates much more network traffic as it is updated every time the cursor is moved, so it should only be used to setup attributes like 'Viewport Locking' and Font Size settings.

Allow Color: For devices that are capable of displaying color screens, use this checkbox to control which devices will be allowed to display color. If this option is not checked, color-capable devices will display white text on a black background.

Auto Add DM License: Check this box to cause all DM-capable devices in this group to be automatically added to the Device Management database. Devices in this group will be added to the DM database only if the server is licensed for DM and if there are DM seats available to be issued to the device. (This option has been removed in v15.1 build 208 and newer)

Auto Add Speech: Check this box to cause all Speech-capable devices in this group to be assigned a Speech license seat. Devices in this group will be assigned a Speech License seat only if the server is licensed for Speech and if there are Speech seats available to be issued to the device.

Auto Add SpeechLink: Check this box to cause all SpeechLink-capable devices in this group to be assigned a SpeechLink license seat. Devices in this group will be assigned a SpeechLink License seat only if the server is licensed for SpeechLink and if there are SpeechLink seats available to be issued to the device.

Device Name Prefix: The 5250 device descriptions for all RF devices falling within this device group IP address range will get this prefix. For each RF device in this device group, the name of the device description on the IBM i will be this Device Name Prefix followed by a unique suffix calculated based upon the IP address of the connecting device and the Suffix Octets and Decimal Suffix settings. If you leave this field blank, then device naming will not be enabled for this device group. If you wish to create a device name with no prefix, use the reserved prefix 'NULL' which will cause the system to generate a device name using only the suffix. The device name prefix can be any length up to 10 characters. If your configuration will cause a device name to be generated that is longer than 10 characters, you will be notified and a corrective measure will be suggested.

If you wish to manage your device names at the individual device, then you can specify [deviceid] as the Device Name Prefix and this will cause the client software to retrieve either the 'Device Name' from the PPC/CE.Net operating system, or use the 'device_id' client setting from the client INI file, and use that identifier as the entire 'Device Name'.

Suffix Octets: The maximum size of the device suffix is 6 characters. This setting allows you to control the size of the device name suffix. If you select Decimal Suffix, then each decimal octet will require 3 positions and you can select 1 or two octets. If you de-select Decimal Suffix, then each octet will require 2 positions and you can select from 1 to 3 octets. You may select 0 octets only if the Low and High IP Address Range for the group are the same IP address.

Decimal Suffix: This option allows you to specify whether to use decimal or hexadecimal values to build the device name suffix.

Device Naming Examples:

- Device Name Prefix = SHP_
Suffix Octets = 3
Decimal Suffix = Unchecked
RF device IP 192.168.100.25 will be converted to IBM i Device Name SHP_A86419.
- Device Name Prefix = SHP_
Suffix Octets = 2
Decimal Suffix = Checked
RF device IP 192.168.100.25 will be converted to IBM i Device Name SHP_100025.
- Device Name Prefix = SHP_
Suffix Octets = 1
Decimal Suffix = Checked
RF device IP 192.168.100.25 will be converted to IBM i Device Name SHP_025.
- Device Name Prefix = DEVICE0001
Suffix Octets = 0
Group IP Low Range = 192.168.100.25
Group IP High Range = 192.168.100.25
RF device IP 192.168.100.25 will be converted to IBM i Device Name DEVICE0001.
- Device Name Prefix = NULL
Suffix Octets = 1
Decimal Suffix = Checked
RF device IP 192.168.100.25 will be converted to IBM i Device Name 025.
- Device Name Prefix = [deviceid]
PPC/CE.Net Device Name = WHSDEV1
RF device IP 192.168.100.25 will use IBM i Device Name WHSDEV1.

VT Alarm ID Column: For VT sessions, you can specify the column where the VT Alarm ID Character will be found.

Row: For VT sessions, you can specify the row where the VT Alarm ID Character will be found.

VT Alarm ID Char: For VT sessions, you can specify a character, which when found in the location defined by the VT Alarm ID Column and Row, will cause the Alarm to be sounded on the device as specified in the 'Handle Alarms' setting.

Hide ID: For VT sessions, this setting will cause the VT Alarm ID Character to be hidden (non-visible) on the device.

Handle BELs & Alarms: You may select which type of audible indicator will be used when a 5250 display contains the ALARM DDS keyword or a VT BEL or VT Alarm ID is encountered. The options are None, Short Beep, Long Beep, Double Beep or Vibrate.

Handle 5250 Messages: You may select the method that will be used to display messages that appear on the message line 24 of the 5250 screen.

- **Snap-To Message:** This method emulates IBM's Wireless Connect behavior causing the device window to snap down to the lower-left corner of the 5250 screen, allowing you to see the message. This method requires that you send a [RESET] key if the 5250 session keyboard becomes locked.
- **Pop-Up Message:** This method causes a pop-up message to be displayed that contains the entire text of the message. This method will automatically send a [RESET] key to unlock the 5250 keyboard when appropriate.
- **Take No Action:** Select this option if you want no action taken when messages appear.
- **Popup Msg. Location:** You may select the area on the device screen where system messages will be displayed. The choices are 'Top', 'Center' or 'Bottom' of the device screen. The default is to have system messages displayed at the 'Top' of the device screen.

Message Notification: You may select which type of audible indicator will be used when a new message appears on the message line. The options are None, Short Beep, Long Beep, Double Beep or Vibrate.

Manage Barcodes: Click this button to access a dialog that will allow you to configure barcode types for this device group.

Manage Program Calls: Click this button to access a dialog that will allow you to configure client-side program calls for this device group.

Manage Printing: Click this button to access a dialog that will allow you to configure client-side printing options for this device group.

Manage Startup Scripts: Click this button to access a dialog that will allow you to configure session start-up scripting options for this device group.

Manage Alt. Keyboards: Click this button to access a dialog that will allow you to assign alternate keyboard maps to be used by devices that are members of this group.

3.5.3 Managing Barcodes

For each device group, you may control the manner in which barcodes are scanned for that device group. The following window is presented when you click on the Manage Barcodes button on the Update Device Group window. The window contains some device group level barcode settings and a list of specific barcodes defined for this device group.

Type	Decode	Min Length	Max Length	Trim Begin	Trim End	Use First	Prefix	Suffix	Notes
Code 3 of 9	True	0	0	0	0	0			
Code 128	True	0	0	0	0	0			
UPC A/E	True	0	0	0	0	0			

Enable Undefined Barcodes: This option works in conjunction with the list of barcode types that

are configured for this device group. Check this box if you want to allow the device to scan barcode types that are not specifically configured for this device group.

Append Field Exit to Short Scan (5250): For 5250 sessions, select this option to cause a Field Exit to be automatically appended to barcodes that are shorter than the field into which they are being scanned. This option is often used to enhance scanning into display fields that cause an automatic end-of-record advance via the CHECK(ER) display attribute. (This setting has no effect for 3270 or VT emulation).

Append Enter on Last Field (5250 & 3270): For 5250 and 3270 sessions, select this option to cause an Enter to be automatically appended to barcodes that are scanned into the last field on the current application screen. (This setting has no effect for VT emulation).

Barcode Scan Prefix: This feature provides for the definition of characters to be inserted as a prefix to the scanned data. Select from the Drop-down list, or key in your prefix characters. This setting will affect all barcode symbologies unless a specific prefix is defined for a specific symbology.

Barcode Scan Suffix: This feature provides for the definition of characters to be inserted as a suffix to the scanned data. Select from the Drop-down list, or key in your suffix characters. This setting will affect all barcode symbologies unless a specific suffix is defined for a specific symbology.

You may add, edit, and delete Barcode Type entries using the “Barcode” menu or by right clicking on a specific Barcode Type entry in the list. When adding or editing barcode types for this device group, the following window will be displayed.

This dialog allows you to configure specific settings for specific barcode symbologies and lengths. You can add more than one configuration for various lengths of a single symbology so long as the Minimum Length matches the Maximum Length and you do not already have a setting defined for the specific length. There can be only one setting for a symbology where the Minimum Length and the Maximum Length are different or are zero. Using these length settings, you can have different barcode settings for the same symbology where the barcode values have different lengths.

Update Barcode

Regular Expression

Barcode Type: Code 3 of 9

Decode this type: ☒

Minimum Length: 0 Maximum Length: 0

Trim all spaces from: Neither Side

Substitute Char with Char

Substitute all embedded Control Codes with this character:

Trim from Beginning: 0 Trim from End: 0

Use First ## Digits: 0 (Enter Zero to keep the entire barcode)

Regular Expression Processing:

Expression	Replacement

Scan Prefix: Scan Suffix:

Notes:

Set both Min Length and Max Length to zero to impose no length restriction

The following criteria are used to determine if the scanned barcode data will be affected by this particular barcode setting:

Barcode Type: Use this drop-down list to select the barcode type that you wish to define.

Minimum Length: Specifies the minimum value length to have this setting apply.

Maximum Length: Specifies the maximum value length to have this setting apply.

- **Note:** Input length restrictions for barcode types can be eliminated by setting both the Minimum and Maximum parameters to zero (0).

If the scanned barcode meets the criteria for this barcode setting, then you can control whether the scanned barcode is allowed to be processed using the following option:

Decode this type: Use this checkbox to enable the use of the scanned barcode in the session. If this option is checked, then the barcode is allowed, and the barcode data manipulation functions are applied. If this option is not checked, then the scanned barcode is rejected, and the device will beep.

For scanned barcodes that meet the criteria defining this barcode setting, the following barcode data manipulation functions will be applied in dialog order, from the top down:

- Trim all spaces from
- Substitutions
- Substitute embedded Control Codes
- Trim from Beginning/End
- Use First ### digits
- Regular Expressions
- Adding Scan Prefix and Suffix.

Trim all spaces from: This option determines how leading and trailing spaces in the barcode data will be handled. You can select to have spaces trimmed from neither side, the left side, the right side or both sides of the barcode data.

Substitute: This option allows you to specify a character or string within the barcode data to be replaced by a different character or string. Single character substitutions must be represented in the hexadecimal (0x00) format to differentiate them from string substitutions. To remove data, use [null] as the substitution string value or use 0x00 as the substitution character value.

Substitute all embedded Control Codes with this character: Allows you to specify a character to be used as a substitute for all control codes that are embedded in the barcode data. Control Codes are defined as characters with values less than 0x20. This substitution character must be represented in the hex (0x##) format. Enter a value of 0x00 to remove all control codes from the barcode data.

Trim from Beginning: Specifies the number of characters to trim from the beginning of the scanned data. Type in the number of characters to trim, or select the option to trim 'to fit field' which will trim characters from the beginning when the barcode data is longer than the field length.

Trim from End: Specifies the number of characters to trim from the end of the scanned data. Type in the number of characters to trim, or select the option to trim 'to fit field' which will trim characters from the end when the barcode data is longer than the field length.

Use First ## Digits: Specifies the number of characters from the beginning of the scanned data to use. This value is evaluated after the 'Trim' attributes have been applied. Set this value to Zero (0) to cause all of the remaining barcode data to be used.

Regular Expression Processing: Provides the ability to use sophisticated 'Regular Expression Processing' to manipulate barcode data. You can enter one or more 'Expressions' that are evaluated against the barcode data. If an expression matches the scanned barcode data, then the 'Substitution' will be processed against the barcode data. Regular Expression Processing for barcode data is covered in detail in the 'StayLinked Barcode Regular Expression User Guide'.

Scan Prefix: Specifies the characters to be inserted as a prefix to the scanned data. Select from the Drop-down list, or key in your prefix characters. This setting will override the device group level setting for this specific barcode symbology.

Scan Suffix: Specifies the characters to be inserted as a suffix to the scanned data. Select from the Drop-down list, or key in your suffix characters. This setting will override the device group level setting for this specific barcode symbology.

Notes: This is a convenience field that has no effect on barcode processing. It can, however, help you to organize and manage your barcode rules by providing a place to record why you created this symbology-specific barcode rule for future reference.

3.5.4 Managing Program Calls

For each device group, you may define up to three client-side program calls that can be mapped to specific keys on your device keyboard. The following window is presented when you click on the Manage Program Calls button on the Update Device Group window. The programs that are defined in this dialog must be installed on the individual devices. These program calls are often used for printing barcodes and other functions that must be processed on the device.

User Message: This parameter allows you to display a message on the device screen during the time that the client-side program is running. If you leave this parameter blank, then no message is displayed.

Screen Dump File: This parameter gives you the option of dumping an image of the entire current 5250 screen to a text file on the read/write drive on the device. The file will be written to the device before the client-side program is called. Do not specify a drive letter with the file name, as the StayLinked client determines what drive is available for writing, depending upon the device make and model. If you leave this parameter blank, then no screen image is written to the device.

Command/Program: This parameter specifies the DOS command or client-side program that is to be called. If the program does not exist, no action will be taken, and no error message is displayed. When the program has completed its processing, the session continues normally.

3.5.5 Managing Printing

For each device group, you may configure a group of settings that define how the server will identify and handle client-side printing for devices that belong to that device group. For VT Telnet Hosts, StayLinked supports the standard VT printing pass-through escape sequences.

Additionally, StayLinked provides a facility by which printer commands can be communicated to the device by reading the printer commands from a special application display screen and transmitting those commands to the device. This special application display screen is designed by the end user and is integrated into the end-user application. When this screen is displayed and identified by the StayLinked Server, the printer commands embedded in the screen will be extracted and delivered to the device where they will be transmitted to the printer via the selected COM port settings.

Manage Printing Settings for Shipping Department

Screen-Based Printing Setup

☒ Enable Screen-Based Printing

☐ Display Screen Containing Printer Data

Start ID Row: Start ID Col:

Printer Data Start ID:

Printer Data Continue ID:

Printer Data End ID:

Printer CRLF ID:

☒ Enable Print Transaction Throttling

Post-Printing Actions

Printing Completion Action:

Printing Continue Action:

Printing Cancel Action:

Printer Device Setup

Printer Device:

COM Settings

Baud Rate: Print Timeout: (0-255 secs.)

Data Bits: Stop Bits:

Parity: Flow Control:

OK Cancel

Enable Screen-based Printing: This option will enable or disable client-side printing for this device group for host applications where screen recognition is required.

Display the Screen Containing Printer Data: This parameter determines whether or not the screen, which has been identified as containing printer command, is displayed on the device.

Enable Print Transaction Throttling: Forces acknowledgments for each printer data packet sent. It is recommended to select this option for labels or documents that contain a large amount of printer instructions.

Start ID Row: This option defines the display row where the server will look for the Print Data Start ID and the Print Data Continue ID.

Start ID Column: This option defines the display column where the server will look for the Print Data Start ID and the Print Data Continue ID. This value is not included in the extracted printer data.

Print Data Start ID: This option describes the string of characters that, when found at the Start ID Column and Row, identifies this screen as containing a new set of printer commands.

Print Data Continue ID: This option describes the string of characters that will notify the StayLinked Server that more printing data is to be expected on subsequent screens. This ID should be used at the end of a screen when there will be more data displayed on the next screen. This ID should also be positioned at the Start ID Column and Row of the next screen that contains additional printer commands. This ID would be used when the printing commands are too complex to fit on a single application display screen.

Print Data End ID: This option describes the string of characters that will identify the end of the printer commands. When this ID is encountered, all of the collected printer data will be transmitted to the device. This value is not included in the extracted printer data.

Print CRLF ID: This option describes the string of characters that will identify the CRLF indicators on this screen. The CRLF indicators that are found in the extracted printer data will be replaced with an actual carriage return/line feed sequence when that data is transmitted to the device.

Printing Completion Action: This option controls how the server will respond when the printer attached to the device has successfully processed the printer commands. The action defined here will be sent to the printing command screen. For instance, if the printer completes printing, the Enter key can be sent to the screen to cause the printer command screen to be dismissed.

Printing Continue Action: This option controls how the server will respond when a screen of printer data is ended with a Printing Continue ID. This action would be used to trigger the display of the next screen that contains the additional printer commands.

Printing Cancel Action: This option controls how the server will respond when the printer attached to the device fails to process the printer commands. If you cancel the printing operation on the device, then this action will be sent to the printing command screen. For instance, if you cancel printing, the F12 key can be sent to the screen to cause the printer command screen to be dismissed. The value selected for these three actions will depend upon how the end user application has been programmed.

Printer Device: This setting configures the StayLinked client to support Serial COM communications with printer devices. If you wish to use RF or Bluetooth communication protocols, you will need to configure 'Client Settings' for the StayLinked client to support your printer. In the 'Printing' group of Client Settings, you will find the 'Printer Type' setting where you can choose 'Generic RF' or 'Generic Bluetooth' printers. Plus, there are some additional 'RF Printer' settings available.

Baud Rate: This option describes the Baud Rate of the printer connected to the device.

Data Bits: This option describes the Data Bits setting of the printer connected to the device.

Parity: This option describes the Parity setting of the printer connected to the device.

Print Timeout: This option defines how long the StayLinked client will wait for responses from the attached printer device.

Stop Bits: This option describes the Stop Bits setting of the printer connected to the device.

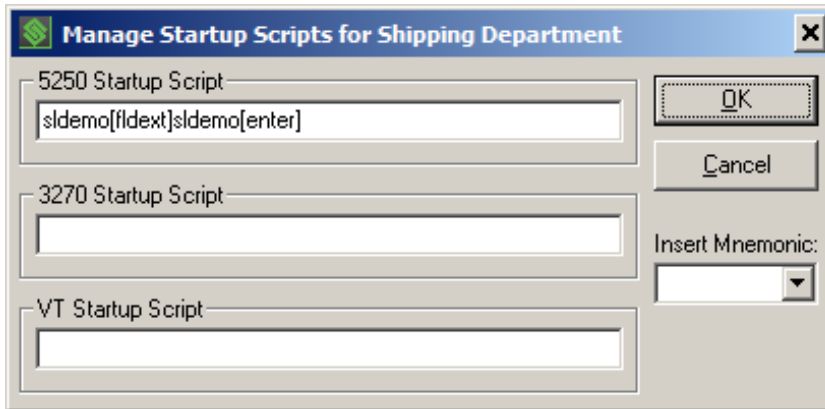
Flow Control: This option describes the Flow Control setting of the printer connected to the device.

3.5.6 Managing Startup Scripts

For each device group, you may define a startup script for each type of emulation available. The startup script will be processed only when a new session is established. The script will not be run when a device reconnects to an existing session. The script will always be processed against the first host screen that is presented to the device, typically a logon screen.

Each script can be up to 255 characters in length. Each script can contain any combination of characters and emulation mnemonic keywords. Emulation mnemonic keywords are contained within square brackets []. You can select mnemonic keywords from the 'Insert mnemonic' drop-down list, causing the selected mnemonic to be automatically inserted at the current cursor location within the script textbox. Startup Scripts should be carefully designed to function appropriately for the type of emulation, targeted host and end-user application. Syntax errors in the script will not cause errors, but could cause some part of your script to be ignored by the emulation host.

The following window is presented when you click on the Manage Startup Scripts button on the Update Device Group window. The example 5250 Startup Script below is designed to be processed against a 5250 logon screen. You profile 'myuserid' will be automatically typed into the first field on the screen and then the 'Field Exit' mnemonic will be processed, moving the cursor to the next field on the logon screen. Then, the password 'mypasswd' will be typed into the current field and an 'Enter' key mnemonic will be processed. This script would cause a user to be automatically signed onto the target IBM I emulation host.



5250 Startup Script: Enter the startup script to be used when connecting to a 5250 Telnet host.

3270 Startup Script: Enter the startup script to be used when connecting to a 3270 Telnet host.

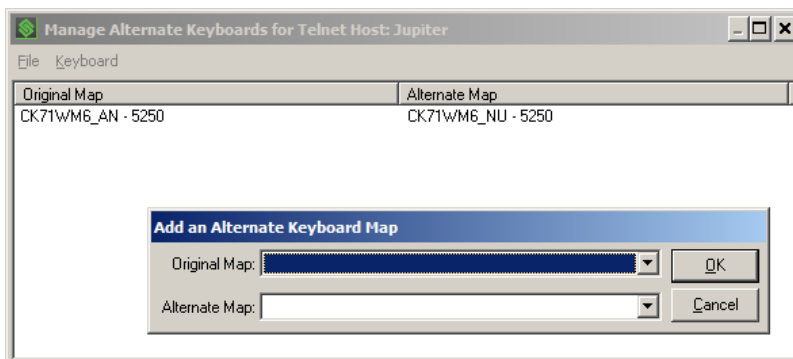
VT Startup Script: Enter the startup script to be used when connecting to a VT Telnet host.

3.5.7 Managing Alternate Keyboard Maps

For each device group, you can override the keyboard map that a device would normally use and specify a different keyboard map to be used as an alternate.

Keyboard maps are used by the StayLinked system as a cross-reference between the many and varied device keyboards and the various host types (5250, 3270, and VT). With StayLinked, you can use the default keyboard map or alter it to suit the specific needs of your device users and their applications. In addition, you can create alternate keyboard maps to support variations needed for a specific group of devices.

The following window is presented when you click on the Manage Alt. Keyboards button on the Update Device Group window.



In this example, when an Intermecc CK71 Windows Mobile 6, Alpha-Numeric keypad device connects to this Host, the alternate keyboard map for the Intermecc CK71 Windows Mobile 6, Numeric keypad device will be used instead.

You may add and delete these alternate keyboard maps using the Keyboard menu (the Add New Alternate Map selection window is shown above). The Original Map and Alternate Map dropdowns provide a list of available keyboard maps from which to choose.

In case you are using Custom Device Types for your devices and you want to map them to an existing standard keyboard map, you may select the special value '** Enter a Custom Device Type **' as the 'Original Map'. Then select the desired existing 'Alternate Map'. When you click OK, you will be prompted for a 'Custom Device Type' value that will be used for the 'Original Map' value.

Select "Save Changes" from the "File" drop-down menu to save any changes that you have made to the currently selected host group.

3.6 Managing Keyboard Maps

This section describes the methods provided to specify and tailor the keyboard maps used by the devices that connect to the server. Keyboard maps are used by the StayLinked system as a cross-reference between the many and varied device keyboards and the various host types (5250, 3270, VT, and TESS). With StayLinked, you can use the default keyboard map or alter it to suit the specific needs of your device users and their applications. In addition, you can create alternate keyboard maps to support variations needed for a specific host or group of devices.

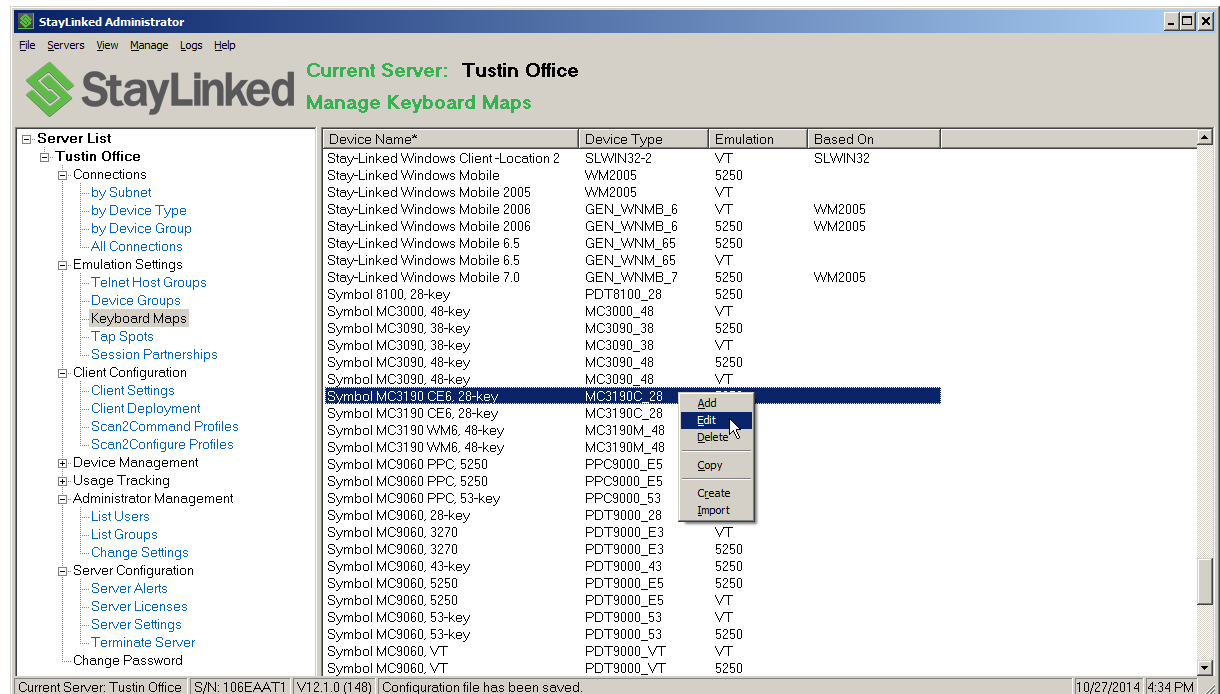
Note that TESS keyboard maps are available only for selected Zebra device models.

3.6.1 Managing Keyboard Maps

When you select Keyboard Maps from the server tree or the Manage menu, the Keyboard Maps list will appear in the main display panel, showing all the keyboard maps that are currently installed for the selected server and available for use by devices upon connection. Typically, this list should contain maps only for those devices that are in use at your installation. Other keyboard maps should be removed from this list as a security measure. The Keyboard Maps information can be sorted into ascending or descending order by clicking on any of the column headers. The currently sorted column will be indicated by an asterisk (*).

Only devices that have a keyboard map listed in this dialog will be able to connect to the StayLinked Server and run Telnet sessions.

Clicking the right mouse button on a keyboard map or in the blank area of the list will cause a small menu to appear with options to Add, Edit, Delete, Copy, Create or Import a keyboard map.



If you want to delete multiple keyboard maps from your server, you can multi-select keyboard maps in the list, right-click and select the 'Delete' menu option to perform a mass delete.

If you would like to compare two keyboard maps, then select exactly two entries in the list, right-click and select the 'Compare' menu option to display a keyboard compare dialog. You must select two keyboard maps for the same emulation type in order to perform a comparison.

Keyboard Map - Add – Select this menu option in order to add a new keyboard map based upon a pre-defined keyboard layout definition for a specific device.



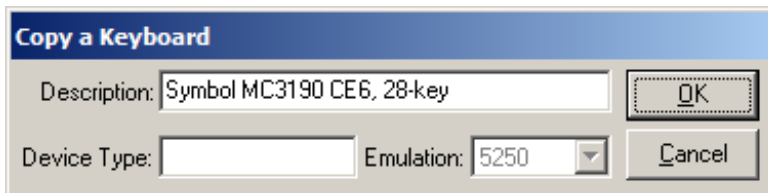
The 'Select a Keyboard' dialog box has a blue title bar. It contains two dropdown menus: 'Manufacturer' with 'Apple' selected and 'Device - Host' with 'SL_IPHONE (5250) Apple iPhone' selected. There are 'OK' and 'Cancel' buttons on the right.

Select the Manufacturer and then the Device and Host type from the drop-down lists of pre-defined keyboard definitions. Once selected, click OK and you will be presented with the Keyboard Map Editor dialog (see below).

Keyboard Map - Edit – Select this menu option in order to modify the keyboard mappings for the selected keyboard map using the Keyboard Map Editor (see below).

Keyboard Map - Delete – Select this menu option in order to remove the selected keyboard maps from the list.

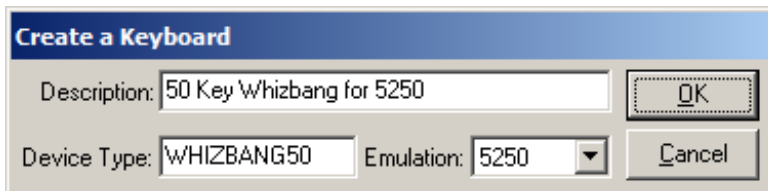
Keyboard Map - Copy – Select this menu option in order to copy the selected keyboard map to an alternate keyboard map.



The 'Copy a Keyboard' dialog box has a blue title bar. It contains a text field for 'Description' with 'Symbol MC3190 CE6, 28-key' and a dropdown for 'Emulation' with '5250' selected. There are 'OK' and 'Cancel' buttons on the right.

You can change the description and enter the device type that you wish to use for this copied keyboard map. The device type is the name you will use when referring to this keyboard map, and as such, must be unique in the list of keyboard maps for this StayLinked Server. This option is useful for creating alternate keyboard maps that can be assigned to Telnet Hosts and to Device Groups. Once entered, click OK and you will be presented with the Keyboard Map Editor dialog (see below).

Keyboard Map - Create – Select this menu option in order to create a new keyboard map from scratch.

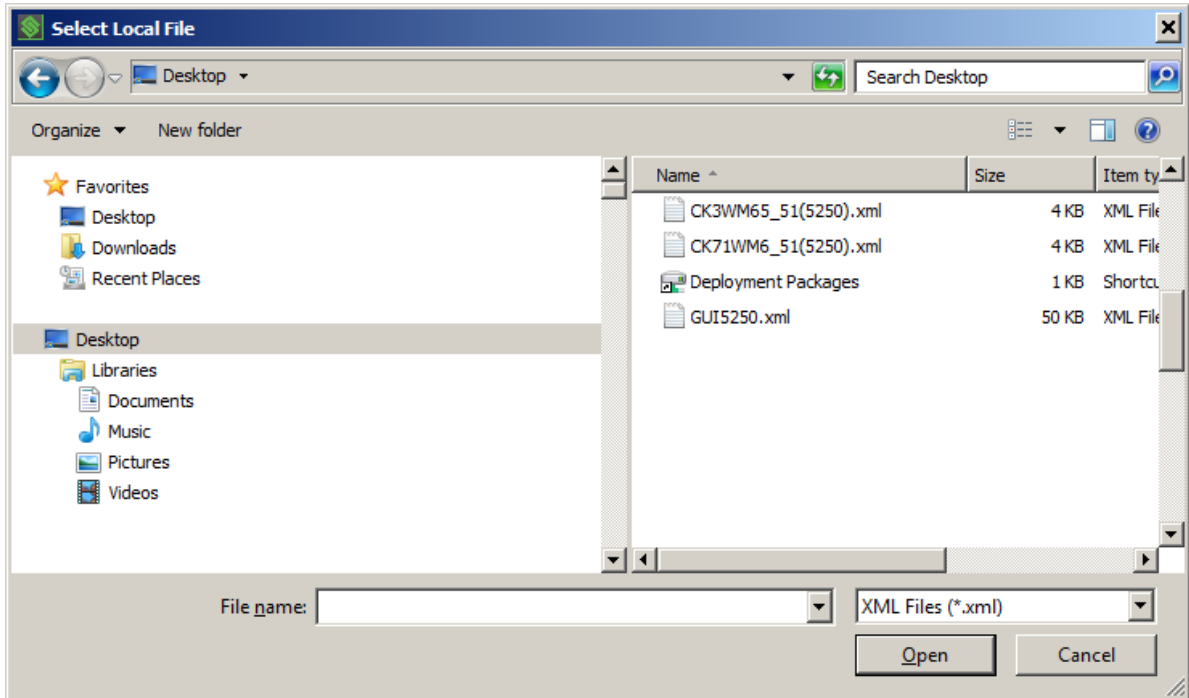


The 'Create a Keyboard' dialog box has a blue title bar. It contains a text field for 'Description' with '50 Key Whizbang for 5250' and a dropdown for 'Emulation' with '5250' selected. There are 'OK' and 'Cancel' buttons on the right.

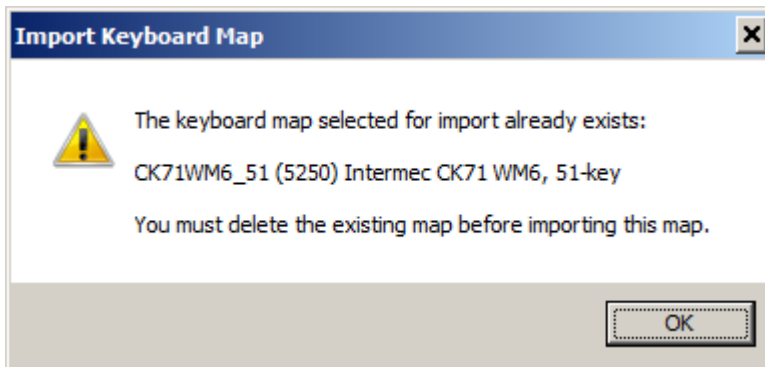
You must provide a description for this map and enter the device type that you wish to use for this copied keyboard map. The device type is the name you will use when referring to this keyboard map, and as such, must be unique in the list of keyboard maps for this StayLinked Server. Finally, select the emulation type for which this map will be used. This option is typically used to support devices for which there is no pre-defined keyboard map. If the device does not appear in the 'Select a Keyboard' dialog, then use this option to build a map from scratch. Once entered, click OK and you will be presented with the Keyboard Map Editor dialog (see below).

NOTE: Keyboard maps that are 'created' and are not based upon a pre-defined keyboard definition will only contain keys that you define. Whereas keyboard maps that are based upon keyboard definitions contain all possible key combinations that are reasonably available on the device, even if those keys have not been mapped to anything specific.

Keyboard Map - Import – Select this menu option in order to import a new keyboard map from an XML file that had been exported from the 'Edit Keyboard Map' dialog. See 'Editing a Keyboard Map' > File > Export Keyboard' below for more details.

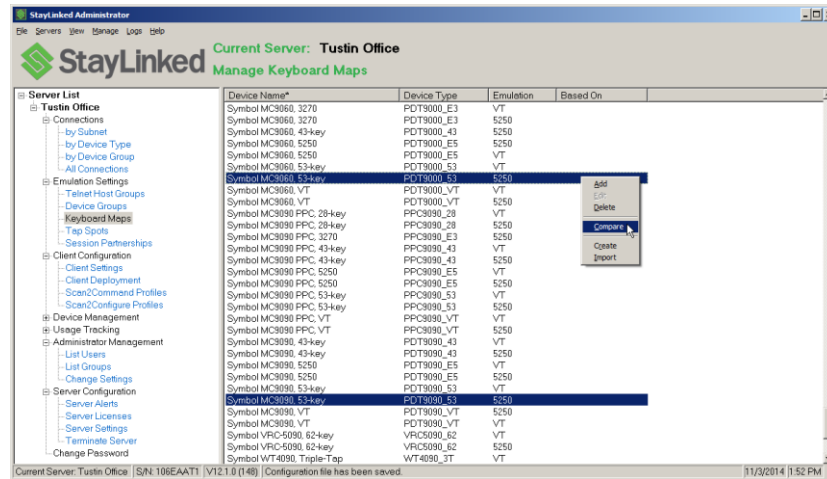


If the keyboard map that you are attempting to import already exists on this server, you will be prompted with an error message.

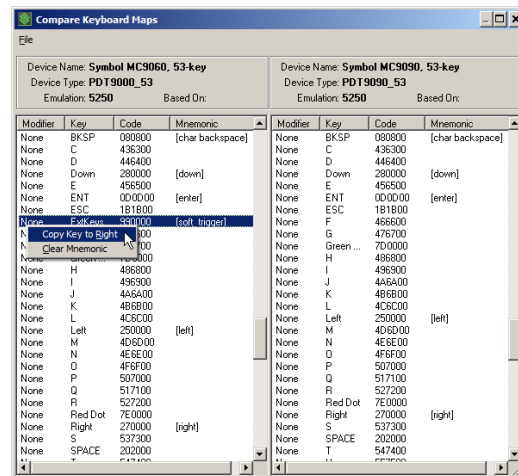
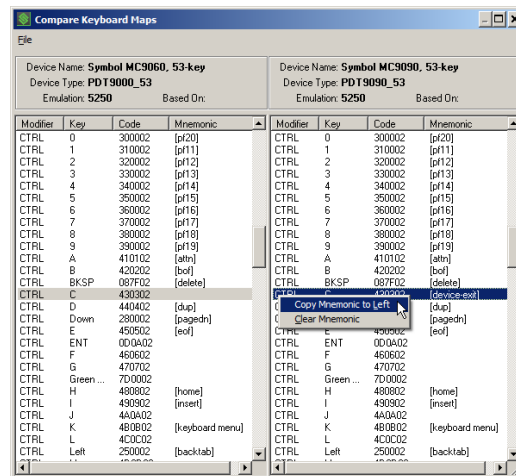


In this case, you must delete the existing map before you can import the new map.

Keyboard Map - Compare – Select this menu option while selecting exactly two keyboard maps for the same emulation type.



A dialog will be presented that will allow you to compare two keyboard maps and copy mappings between the two maps. When you exit the dialog, you will be prompted to save any changes made.



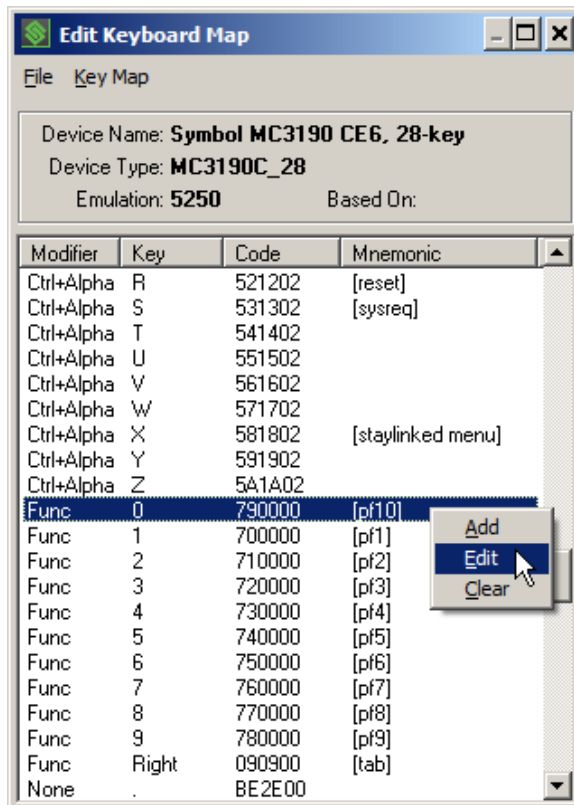
When you left click on a key entry in either list, an attempt will be made to locate a key entry with a matching key code in the other list. If a matching key code is found, that key entry in the other list will be selected and made visible. If a matching key code is not found, then no entry in the other list will be selected.

When you right-click on a key entry in either list, that key entry will be selected and the selected item in the other list will not be changed. Also, when you right-click on a key entry and there is a mnemonic entered for that key, a context menu will appear with options for manipulating the key mappings.

- **Copy Mnemonic to Left/Right:** Select this menu option to have the current mnemonic copied to the selected key entry in the other keyboard map.
- **Copy Key to Left/Right:** Select this menu option to copy the entire key entry to the other keyboard map. This option will only appear when the selected key code does not exist in the other keyboard map.
- **Clear Mnemonic:** Select this menu option to clear the mnemonic from the selected key entry.

3.6.2 Editing a Keyboard Map

Whether you choose to add, edit, copy, create or import a Keyboard Map, the following Keyboard Map Editor dialog will be used to map the model-specific RF device keys to emulation mnemonics, scripts, letters, text or combinations of these. You may right-click on a key map entry to bring up a Key Map context menu.

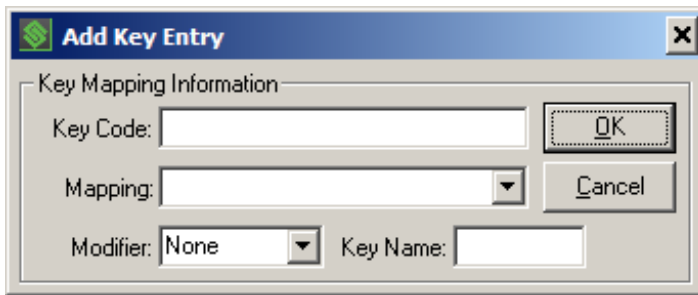


From the File Menu:

- **Save Changes:** Select this menu option to save the current keyboard mappings.
- **Load Defaults:** Select this menu option to load the default keyboard map for this Device Type and Emulation.
- **Print Keyboard:** Select this menu option to send a hard copy of the current keyboard map to the default printer.
- **Export Keyboard:** Select this menu option in order to export this keyboard map to an XML file. We recommend using the suggested export file name, but you can change it if needed. You can then import this map to a different StayLinked Server if desired. Any changes to the current keyboard map must be saved before you can export the keyboard map.
- **Exit:** Select this menu option to close this dialog.
- **From the Key Map Menu (or right mouse click within the list):**
 - **Add:** Select this menu option to add a key map entry for a key code that is not defined in the keyboard definition.
 - **Edit:** Select this menu option to update the selected key map entry.
 - **Clear:** Select this menu option to clear/remove the mapping for the selected key. This option will only be available on keys that have a value in the 'Mnemonic' column.

Add Key Entry Dialog: Use this feature to add a key that generates a key code that is not already listed in the pre-defined keyboard definition for this device. This dialog will allow you to enter the new key code and to select the mnemonic, function or script you wish to associate with

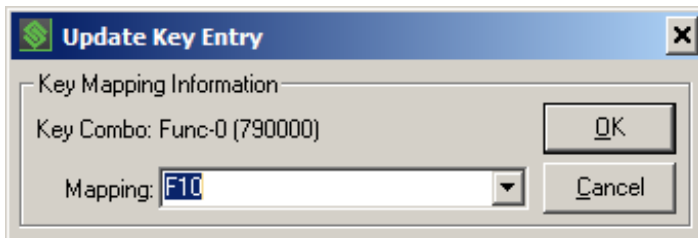
the selected key combination.



The 'Add Key Entry' dialog box has a title bar with a green icon and a close button. It contains a section titled 'Key Mapping Information' with three input fields: 'Key Code' (a text box), 'Mapping' (a dropdown menu), and 'Modifier' (a dropdown menu set to 'None'). There is also a 'Key Name' text box. 'OK' and 'Cancel' buttons are located to the right of the input fields.

- **Key Code:** StayLinked Clients on DOS devices will have a 'Keyboard Test' option on the 'Diagnostics' menu. StayLinked Clients on PPC/CE/Android/iOS devices will have a 'Key Test' option on the 'Tools' menu. Use this test to determine what 'Key Code' is generated by the possible key combinations on the device. If this 'Key Code' is not listed in the pre-defined keyboard map, you can add the key to the map by entering the six-digit key code here.
- **Mapping:** You can select a mnemonic from the drop-down list, or type in the character, text or script that you wish to map to this key.
- **Modifier:** For reference only, select from the list, or type in, the most appropriate modifier based on the key combination you are mapping.
- **Key Name:** For reference only, enter the name of the key you are mapping (i.e., A).

Update Key Entry Dialog: Use this dialog to select the mnemonic or function you wish to associate with the selected key combination.



The 'Update Key Entry' dialog box has a title bar with a green icon and a close button. It contains a section titled 'Key Mapping Information' with two input fields: 'Key Combo' (a text box showing 'Func-0 (790000)') and 'Mapping' (a dropdown menu showing 'F10'). 'OK' and 'Cancel' buttons are located to the right of the input fields.

- **Mapping:** You can select a mnemonic from the drop-down list, or type in the character or text that you wish to map to this key.

3.7 Managing Tap Spot Collections

In addition to traditional keyboard and scanner input to your data collection application, your users can also interact with the screen to provide input to your data collection application. StayLinked allows you to configure the session to provide specific input to your application when users tap on specific plain text or graphical buttons on the screen of the device. For each Telnet Host Entry, you will be able to specify a collection of these 'tap spots' that will be processed on the screens that are displayed to the user on the device. There are two kinds of 'Tap Spot Collections' that you can configure and then assign to your 'Telnet Host Entry' so that users can interact with text or graphical buttons on the device screen.

3.7.1 Classic Tap Spot Collections

- Classic tap spot collections are associated with plain text that appears on the telnet screen.
- Classic tap spot collections are processed in response to a user tapping on a location on the device screen.
- Classic tap spot collections require that a list of delimiters be configured to identify tapped text.

When using Classic tap spot collections, a user will tap on a word or number on the device screen and the device will send to the server a message containing the row and column that was tapped. Using the defined delimiters, the server will then analyze any text that may exist at the tapped location on the application screen and see if the text is properly delimited. If so, the delimited text will be compared to the 'spot text' in each spot entry contained in the classic tap spot collection. If a match is found, the 'mapping' will be sent to the telnet host which will forward the input to the data collection application for processing. The classic tap spots work well for identifying single words, numbers and other simple text on the application screen. The classic tap spots are compatible with all StayLinked Clients that have touch-capable screens.

Classic tap spot collections can be further configured at the Telnet Host Entry where you can use 'Emulation Properties' to make adjustments to classic tap spot processing for a specific Telnet host. Additionally, you can take advantage of the 'Screen Recognition and Reformatting' feature set in StayLinked to customize classic tap spots on a screen-by-screen basis for a specific Telnet host.

3.7.2 SmartTE Tap Spot Collections

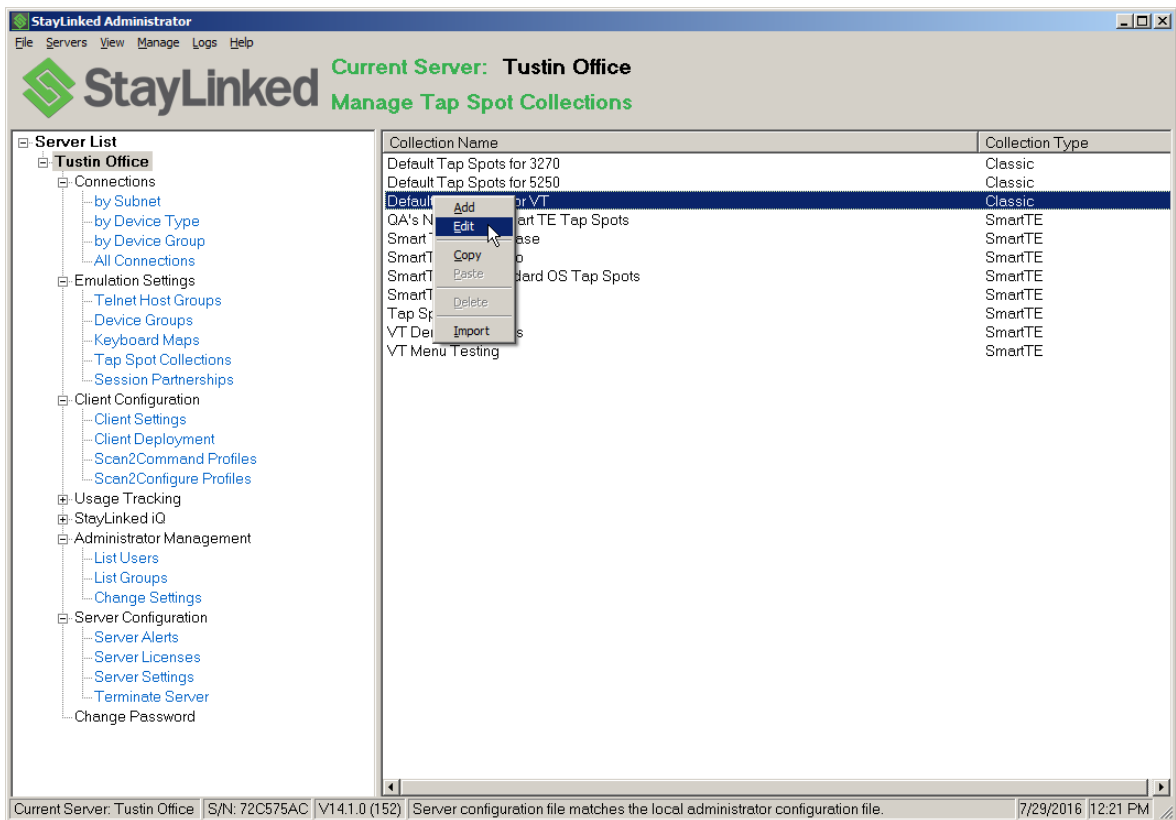
- SmartTE tap spot collections generate graphical buttons that appear on the device display.
- SmartTE tap spot collections are processed as each telnet screen presentation event is received, analyzed and forwarded to the device screen.
- SmartTE tap spot collections use literals and regular expressions to identify patterns on the screen that can be converted into graphical buttons for display on the device screen.

The SmartTE implementation of tap spot collections are processed as each telnet screen presentation event is detected. Each affected row of text on the telnet screen is processed and scanned for patterns that match the tap spots contained in the collection. Every matched pattern is converted into a graphical button that is sent to the client for display. The button will have a caption and a mapping. The caption can be literal text or variable text extracted from the pattern. The mapping can be literal or variable. The button will be positioned on the telnet screen at the location where the matching pattern was located. If the button is pressed, the associated 'mapping' will be sent to the telnet host which will forward the input to the data collection application for processing. The SmartTE tap spot collections are compatible only with StayLinked Clients that have SmartTE graphical capabilities. More information about SmartTE Tap Spots can be found in the 'Screen Recognition, Reformatting and SmartTE Guide.'

This section describes the methods provided to configure and tailor the Tap Spot Collections feature.

3.7.3 Selecting a Tap Spot Collection

When you select Tap Spot Collections from the server tree or the Manage menu, a list of collections will appear in the main display panel. There are three 'pre-defined' Classic Tap Spots collections that are used as the 'default' for each emulation type, 3270, 5250 and VT. These pre-defined collections cannot be renamed or deleted.



Add – Select this menu option to add a new tap spot collection.

Edit – Select this menu option to edit an existing tap spot collection.

Copy – Select this menu option to copy a tap spot collection so that it can be pasted into this or another StayLinked Server that you are managing.

Paste – Select this menu option to paste the last copied tap spot collection into this StayLinked Server.

Delete – Select this menu option to delete an existing tap spot collection.

Import – Select this menu option to import a previously exported tap spot collection into this StayLinked Server.

3.7.4 Tap Spot Collection Maintenance

This dialog provides the ability to map specific screen text to their corresponding emulation mnemonics, letters, text or combinations of these. You may right-click on a key spot entry to bring up a context menu.

Spot Text	Mapping	Caption Text	Background	Caption	Border	Alignment	Row Range	Notes
[regex]s\d\d\d\s	\$1[enter]	[caption-5,57]	COLOR	COLOR	COLOR	Left	All Rows	OS Menu Items 2-digit
[regex]s\s\d\d\s	\$1[enter]	[caption-5,57]	COLOR	COLOR	COLOR	Left	All Rows	OS Menu Items 1-digit
[regex]F\d\s=	[p\$1]	[caption 13]	COLOR	COLOR	COLOR	Center	All Rows	Caption Text
[regex]F\d)=(w+)\$	[p\$1]	\$2	COLOR	COLOR	(default)	Center	22 - 23	Function Keys 1-digit at end...
[regex]F\d)=(w+\s\w*\s\w*)	[p\$1]	\$2	COLOR	COLOR	(default)	Center	22 - 23	Function Keys 1-digit
[regex]F\d)=(w+)\$	[p\$1]	\$2	COLOR	COLOR	(default)	Center	22 - 23	Function Keys 2-digit at end...
[regex]F\d)=(w+\s\w*\s\w*)	[p\$1]	\$2	COLOR	COLOR	(default)	Center	22 - 23	Function Keys 2-digit
More...	[pagedn]	More	COLOR	COLOR	COLOR	Center	All Rows	More Indicator

Tap Spot Collection Name: Enter a unique name for this collection.

Delimiters: This option controls the 'kind' of this Tap Spot Collection. If you leave this option completely blank, then this will be a 'SmartTE Tap Spot Collection'. If you enter a string of characters to be used as 'delimiters', then this will be a 'Classic Tap Spot Collection'. If you do enter delimiters, each character will be used to identify the limits of a word or number that is tapped upon.

Fill Short Number: Use this drop-down selection to cause either a Field Exit key, an Enter key or Nothing to be automatically appended to tapped numbers that are shorter than the field into which they are being entered. (Applies to Classic Tap Spot Collections only.)

Allow Tap Cursor Movement?: This option, if selected, will allow the cursor to be moved to the location that was tapped, so long as that location did not contain a Classic Tap Spot. Deselect this option to prevent inadvertent movement of the cursor to protected areas of the display.

Tap Numbers?: This option, if selected, will cause all numbers that appear on the session screens to be treated as tap spots (useful for numbered menu lists, etc.). (Applies to Classic Tap Spot Collections only.)

The information displayed in the columns of the tap spot collection list includes the following:

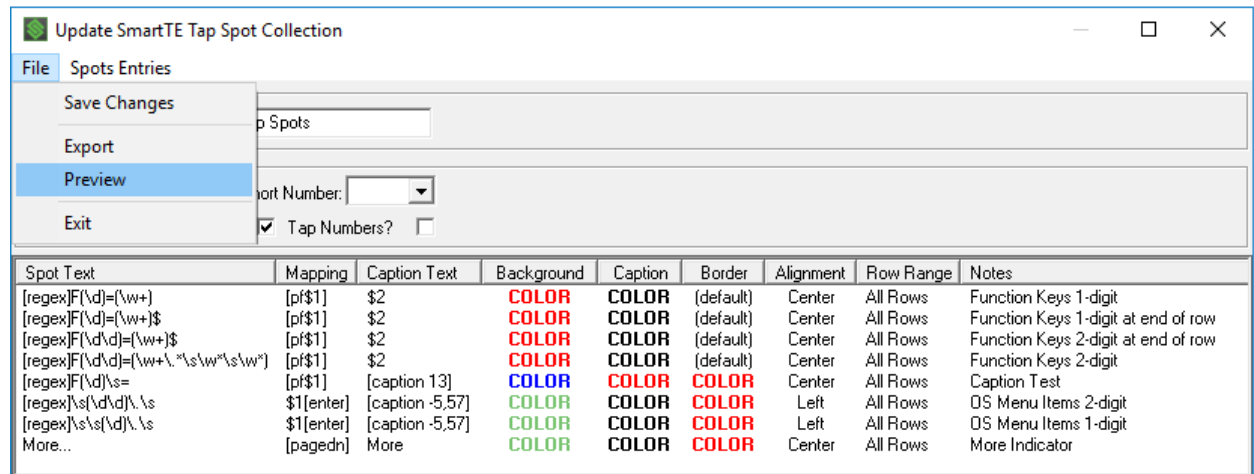
- **Spot Text** – The unique text used to find a tap spot.
- **Mapping** – The action that will be taken when a tap spot is tapped upon.
- **Caption Text** – For SmartTE tap spots, this is the caption that will be displayed in the graphical button.
- **Background** – For SmartTE tap spots, this represents the button background color.
- **Caption** – For SmartTE tap spots, this represents the button caption text color.
- **Border** – For SmartTE tap spots, this represents the button border color.
- **Alignment** – For SmartTE tap spots, this describes the alignment of the button caption text.
- **Row Range** – For SmartTE tap spots, this describes the range of rows on the host screen for which this tap spot entry will be processed.
- **Notes** – Provided for your convenience. These notes have no effect on tap spot processing. They can, however, help you to organize and manage your tap spot entries by providing a place to record the purpose of this tap spot entry for future reference.

From the File Menu:

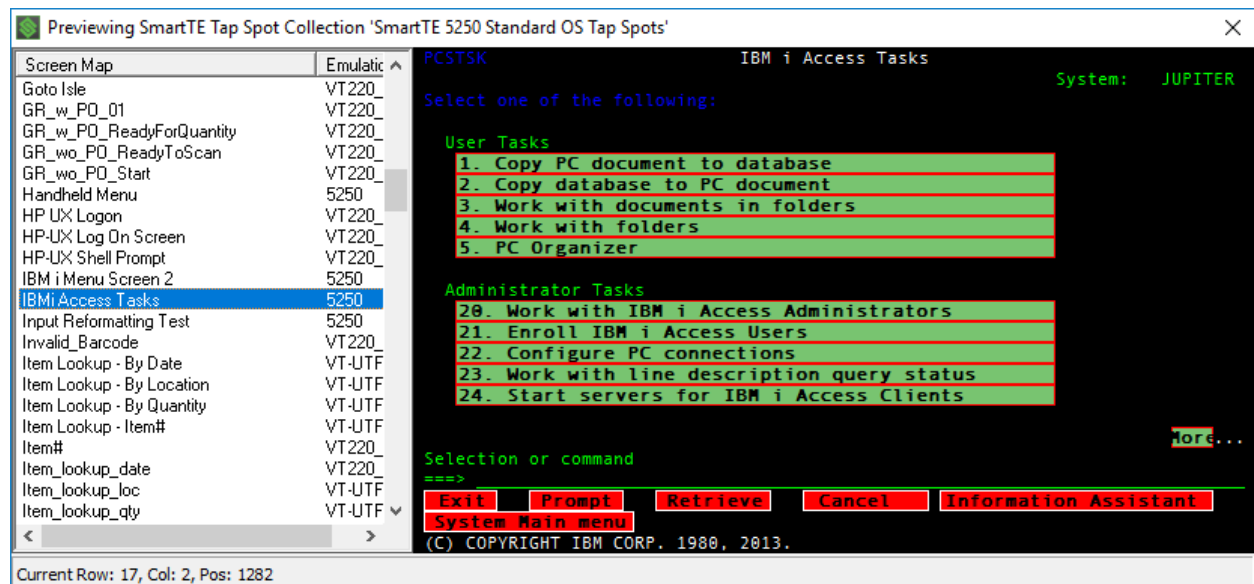
Save Changes: Select this menu option to save the current tap spot collection.

Export: Select this menu option to export the entire tap spot collection to a file.

Preview: This option is available in SmartTE tap spot collections only and will not appear in classic tap spot collections. Select this menu option to display how these tap spots would be displayed against screen maps that have been captured from emulation sessions. Screen Maps are described later in this document or in the SmartTE Guide. This option opens the list of screen maps and applies the SmartTE dynamic tap spots to your screen maps so you can see how they will appear in production.



Note – Leaving your cursor over a button that appears in the preview will show you a tooltip with the ‘Notes’ and ‘Mapping’ that created that particular button.



Exit: Select this menu option to close this dialog.

From the Spot Entries Menu:

Add: Select this menu option to add a new tap spot entry.

Edit: Select this menu option to edit the selected tap spot entry.

Delete: Select this menu option to delete the selected tap spot entry or entries.

Copy Spot: Select this menu option to copy the selected tap spot entry to the clipboard.

Paste Spot: Select this menu option to add a copied tap spot entry from the clipboard.

Copy Attributes: Select this menu option to copy the attributes of the selected tap spot entry to the clipboard.

Paste Attributes: Select this menu option to update all of the selected tap spot entries with the attributes from the clipboard.

Load Defaults: Select this menu option to replace the current list of tap spot entries with a default standard list of tap spot entries.

Add Tap Spot Entry Dialog: Use this dialog to enter a new tap spot entry to the list and its associated mnemonic/text.

Classic

SmartTE

Spot Text (Classic): Enter the text, as it will appear on the screen, which you wish to make tap sensitive. The text can only be entered in any case, but the matching is not case sensitive. The text on the screen must appear between two of the defined delimiters.

Spot Text (SmartTE): Enter either literal text or a Regular Expression. The updated area of the telnet screen will be scanned for matches to the literal text or for pattern matching with the Regular Expression. To enter a Regular Expression, you must add the [regex] prefix to the Spot Text. This prefix will cause the screen analyzer to handle this tap spot entry using Regular Expression processing.

Mapping (Classic): You can select a mnemonic from the drop-down list, or type in the character or literal text that you wish to map to this entry.

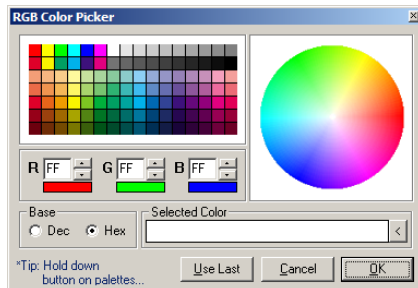
Mapping (SmartTE): You can select a mnemonic from the drop-down list, type in a character, type in literal text or specify a regex substitution expression that you wish to map to this entry.

Caption (SmartTE): Enter literal text or a regex substitution expression that will be used for the graphical button caption.

From Row / To Row (SmartTE): Enter a from and to row which will restrict processing of this tap spot entry to only this range of rows on the host telnet screen.

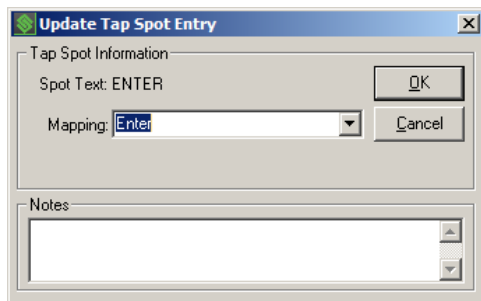
Notes: Provided for your convenience. These notes have no effect on tap spot processing. They can, however, help you to organize and manage your tap spot entries by providing a place to record the purpose or function of this tap spot entry for future reference.

Sample (SmartTE): This button will display a sample rendering of the current graphical button attributes for Background, Caption, Border colors and Caption text alignment. Click on this button to present a menu from which you can select which attribute to modify. When you select the options for Background, Caption or Border color, you will be presented with a dialog that you can use to specify the RGB color value that will be used for the graphical button attribute color.



Using the RGB Color Picker, you can select pre-defined colors from the grid palette or choose a color from the disc palette. If you know specific RGB values that you wish to use, you can type them into the R, G and B textboxes in either decimal or hexadecimal. The 'Selected Color' preview will show the current color assigned to the caption and will be updated based upon changes you make in the dialog. For convenience, you can also recall the last used color by clicking the 'Use Last' button.

Update Classic Tap Spot Dialog: Use this dialog to update the selected Classic Tap Spot Entry.

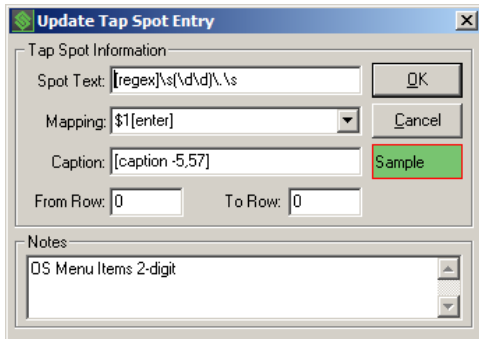


Spot Text: Once a Classic Tap Spot entry is created, you cannot update the Spot Text. Instead, delete the tap spot entry and add a new tap spot entry.

Mapping: You can make changes by selecting a mnemonic from the drop down list, or typing in the character or literal text that you wish to map to this spot.

Notes: You can update your notes to help you manage this tap spot entry.

Update SmartTE Tap Spot Dialog: Use this dialog to update the selected SmartTE Tap Spot Entry.



Spot Text: You can make changes to the literal text or Regular Expression. This example will find a menu item on the screen by looking for the Regular Expression pattern of (1) space, followed by (2) digits, followed by (1) period, followed by (1) space. The two digits are enclosed in parenthesis which causes the value to be 'remembered' and referenced using the \$1 special value. You can have multiple 'remembered' values, each referenced using the \$# special value.

Mapping: You can make changes by selecting a mnemonic from the drop-down list, typing in a character, typing in literal text or specifying a regex substitution expression. This example uses the \$1 special value to reference the two digits that were found on the screen. The two digits will be followed by the [enter] mnemonic which effectively types in the menu number and presses ENTER when you click on the graphical button on the device display.

Caption: You can make changes to the caption that will be displayed on the graphical button. This example uses special values to control the look and text of the graphical button caption. [rgb #####] is a caption prefix which specifies an RGB color value to be used for the button background color. [caption 57] is a special value which causes the button caption to contain 57 characters of text from the screen directly to the right of the matched pattern. In this case, the buttons generated by this regular expression will all be exactly 57 characters long creating a nice row of buttons, one for each menu option.

From Row / To Row: Enter a from and to row which will restrict processing of this tap spot entry to only this range of rows on the host telnet screen.

Notes: You can update your notes to help you manage this tap spot entry.

3.8 Managing SmartTiles Collections

StayLinked SmartTiles offer customized on-screen buttons for various tasks that are independent of the emulation screen. These tiles can be globally set based on standard client settings or customized to provide the desired on-screen buttons to work with the context presented to the users.

SmartTiles are primarily used to create custom keyboards. They allow you to place buttons as simple as single characters or more complex macros. They can be used for navigation, screen placement and other features, much like the options available in SmartTE.

Organized into 'collections' each set of tiles can include any desired buttons organized into pages. This allows you to use centralized configuration tools to create a custom interface for different device types and screen sizes.

By example, you might create three collections, one for a 'landscape orientation' wrist wearable, another for a 'portrait' style handheld computer and a third for a full screen vehicle mount or desktop computer. Each of these collections might have multiple pages, allowing the user to cycle between different types of tiles.

These collections are then served to the devices configured to use them. Clients must be at least version 14.4 or newer to take advantage of these features.

SmartTiles Collections are configured in the Emulation Settings section of the Administrator. You can right click in the blank area of the SmartTiles Collections window for a list of options:

Add: Create a new collection from scratch.

Design: Make adjustments to the selected collection

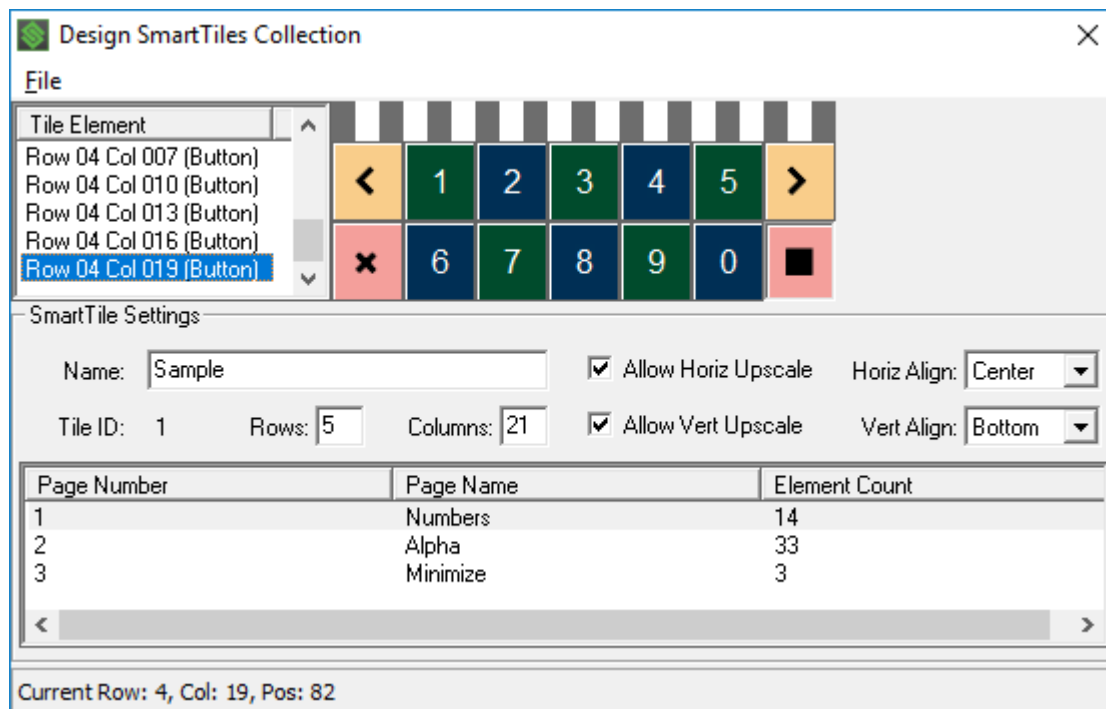
Copy: Copies the selected collection to the Administrator Clipboard.

Paste: Use a copied collection create a new collection.

Delete: Remove the selected collection.

Import: Create a new collection that is a copy of an exported collection. This allows you to import collections from outside sources or use a template. Your installation may include various samples and templates. Additional templates may become available for import from the StayLinked downloads site.

Unused areas of a collection will become transparent, showing the emulation screen contents. You can see these areas in the image below as the grey and white checkered area. Buttons created in this area share the SmartTE button design options. The configuration panels include the options listed below. Each page in a collection will be the same dimensions, with the selected page showing in the design area at the top of the screen.

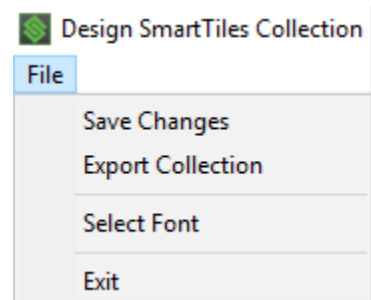


The top File menu has the following options.

Save Changes: Saving your collection will cause changes to take effect as the user navigates or refreshes pages within any existing sessions that are using that collection.

Export Collection: Writes the selected collection out to an XML file that can be imported on any v14.4 or newer StayLinked server.

Select Font: This option allows you to change the font size and aspect ratio of the designer. Changing fonts will shape the designer to the height and width of the font selected, but will not change the display font. Changing the font size will resize the design area to be larger or smaller making it easier to work with the space on your PC.



Note that collection pages will not be presented to devices with a viewport using a smaller row and column size than the assigned SmartTiles Collection. You can confirm the viewport dimensions of any session by double clicking the session in the Administrator's connections list, or with a right click > Details.

The Tile Elements list box will show each button that has been added to the selected page. You can click on the buttons or on the elements in the list for any commands that affect that button.

The following options are available in each collection:

Name: The description or title for each SmartTiles collection is for general information.

Allow Horiz Upscale: This option allows the collection to fit into a device screen that is wider than the collection size.

Horiz Align: Used when the SmartTiles collection is not as wide as the device screen, this allows you to set collections to the left, center, or right edge of the device screen without having to exactly match the width of the device screen as long as the collection is smaller than the device screen.

Tile ID: This value is automatically assigned a key number used when configuring devices to use SmartTiles. Tile collections are referenced using a Tile ID and a page number, separated by a comma. See the section below for more information about implementing collections on your client devices.

Rows: Sets the height of the tile collection.

Columns: Sets the width of the tile collection.

Allow Vert Upscale: This option allows the collection to fit into a device screen that is taller than the collection size.

Vert Align: Used when the SmartTile collection assigned to a device is not as tall as the device screen, this allows you to set collections to the center, top, or bottom of the device screen without having to exactly match the height on the device screen as long as the collection is smaller than the device screen.

The following items are displayed in the list box columns at the bottom of the panel. Adding additional pages can be done by right clicking in this list box.

Page Number: This is the number of each page in the collection. The page numbers are automatically assigned. You can change the page number and order by dragging or moving pages up or down in the list box. Context menu options include Move Up and Move Down when alternate clicking on an individual page in the list box.

Page Name: The descriptive name of each page in the collection.

Element Count: The number of buttons on each page of the collection.

You can add new buttons once you've created a new collection and page.

The button dialogue includes the following configuration options:

Row and Column: Set the position on the tiles area based on the upper-left corner of the button.

Height and Width: Set the size of the button. Buttons can span multiple rows and columns, and will stretch to fit the area.

Transparency: Set the alpha level of the button from 0 (opaque) to 100 (transparent). Higher numbers are more transparent allowing the emulation space behind the button to show through. Note that the Administrator Tile Designer will not show transparency and transparency should be tested on a device screen for best results.

Starting in v15.1 build 208, clients can be configured (`smarttile_caption = 0 or 1`) to ignore transparency settings for the caption on buttons that are at least partially transparent. This is available as a client setting and applied to all SmartTile buttons with transparency. Both the client and server versions are required for the support of this feature.

Caption: Enter the label to be displayed on the button to describe the action the button provides.

Script: The action script to be executed when the button is used.

Fonts: Use this button if the Tile button caption should be displayed using a font other than the device default. This also applies to the Administrator design tool, which defaults to the Roboto font for standard button display. See the section below about FontAwesome for more information.

Buttons have the following display settings, accessed by clicking the 'sample' button in the right edge of the panel.

Background Color: Sets the background color using the RGB color picker or select 'use last' to repeat the previous color.

Caption Color: Sets the text color using the RGB color picker.

Border Color: Sets the button border color using the RGB color picker. Client settings can be used to change the size of the button border if desired.

Alignment: Set the caption to left, center or right aligned on the button area.

Restore Defaults: Sets the button properties back to the default values.

Right clicking on in the design area provides the following options:

Edit: Allows you to adjust the options within that button configuration.

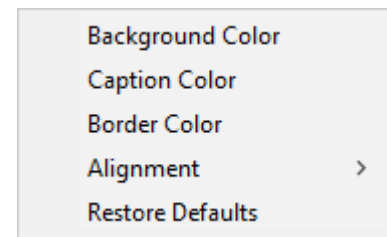
Delete: Remove the selected button.

Copy Button: Make a copy of a button, allowing you to paste in into a blank area of the designer.

Paste Button: Place a copied button into the selected area.

Copy Attributes: Copy the colors and caption alignment of a button.

Paste Attributes: Apply the colors and caption alignment from the copy attributes of a button.



3.8.1 Switching Between Tile Pages

SmartTiles are organized into pages to keep pertinent content on the display and avoid showing users options they might not need. SmartTiles collections used for customized keyboards are commonly organized by pages of function keys, scripts, numeric, and alphabetical buttons. Most handheld devices would not be able to clearly show any screen contents if all of these buttons were included on the same tile.

The following mnemonics can be used in buttons or keyboard map entries to step through the various tiles in a collection:

[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 StayLinked server. This allows you to immediately see any changes on the collection page on your device without having to change pages or reconnect.

In addition to these mnemonics, there is also a client setting that can replace the typical Keyboard button on SmartTE devices with a SmartTiles button. This button acts like the [tile_toggle] mnemonic above, but also replaces the standard two finger tap gesture. Without this setting, a two-finger tap would hide or display the Smart Keyboard, but this setting will change the gesture to perform a [tile_toggle] on the current SmartTiles page.

Add Client Setting

Setting Information

Group: SmartTE OK

Setting: SmartTile Menu Button Cancel

Choose to change the Keyboard Menu Button to a SmartTile Menu Button. ☐ Enabled ☒ Show Advanced

Level Information

Setting Level: Device Type

Device Type: *

Setting Value

Value: On

Notes

3.8.2 Implementing SmartTiles Collections

Once your collection is created, you can enable it on devices using several methods.

The mnemonics listed above will not work until a collection has been assigned to the device. You can assign an initial collection by setting a default collection client setting, or using a Screen Recognition Host API for the 'SmartTiles Commands' with the [tile_show #,#] mnemonic. Note that using a collection ID with a page of 0 will assign the current collection but will not display a page. Once the collection is assigned, you can use the mnemonics above to navigate the various collections and pages. Note that using these features to change collections will set the new current collection, causing the mnemonics above to cycle through that collection until a new collection is selected.

Client settings will be the best choice for a fixed set of pages on a particular model or type of device. The client setting can set the default collection and page for the client to start with. In the example below, the device would be assigned to collection number one but no page would be displayed until additional SmartTile mnemonic commands are issued by the user or StayLinked server.

Update Client Setting

Setting Information
Setting: **SmartTE - SmartTile Startup ID**
Enter ID,Page for the SmartTile Collection that you want to load on the SmartTE device when a connection is completed (e.g., 1,1). ☒ Enabled

Level Information
Setting Level: Device Type
Device Type: *

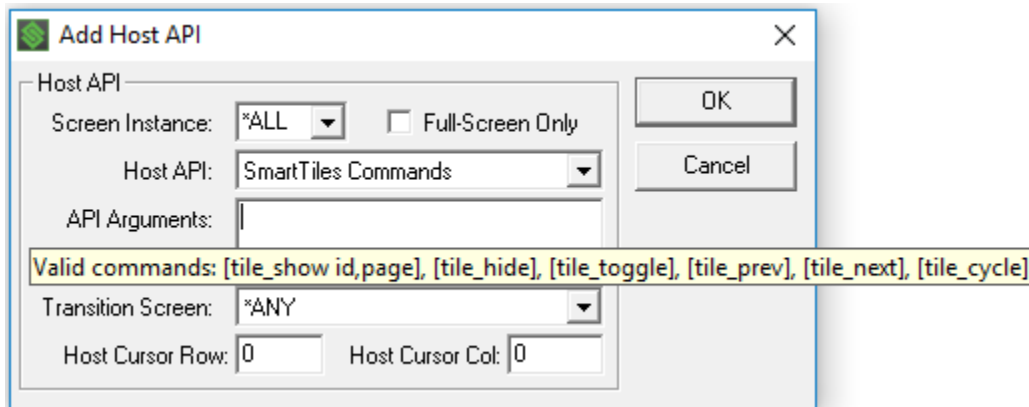
Setting Value
Value: 1,0

Notes

Note: Make sure your clients support this feature before sending the client setting. Clients that are not at least v14.4 will not write the setting and will not try to implement the setting unless the setting date is adjusted on the StayLinked Server. Clients should show the default collection number and page in the ini file when successfully implemented. Based on the example above, the entry in the client configuration would read:

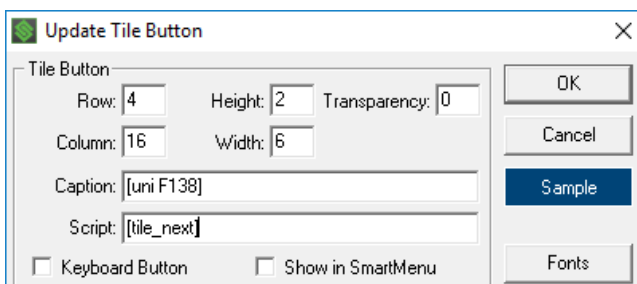
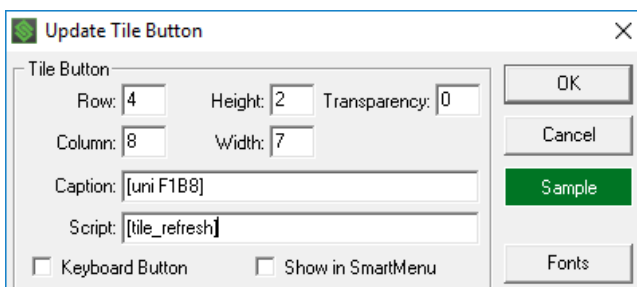
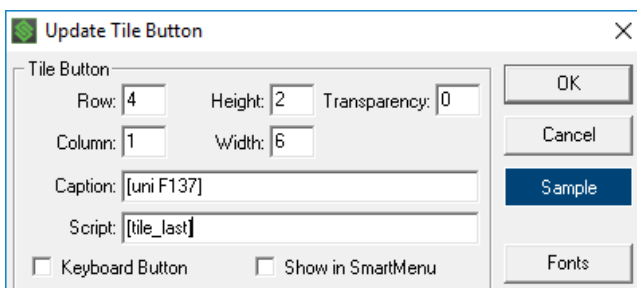
```
smarttile_startup_id = 1,0
```

For a more intuitive implementation, StayLinked Screen Recognition features can be used to display a collection and page. This is accomplished using the Host APIs section of screen recognition. This might be used to show the tile page that best supplies valid options to your users. For example, moving to a screen that prompts for the entry of quantities might take the user to a tile with numeric buttons and common quantity amounts.



3.8.3 SmartTiles and FontAwesome

Similar to the implementation of SmartTE, SmartTiles can take advantage of the icons in FontAwesome. By changing the font to FontAwesome, buttons can access the [uni XXXX] range of characters in the FontAwesome library. A comprehensive list of these icons can be found online by searching for FontAwesome Cheatsheet. These three icons for example:

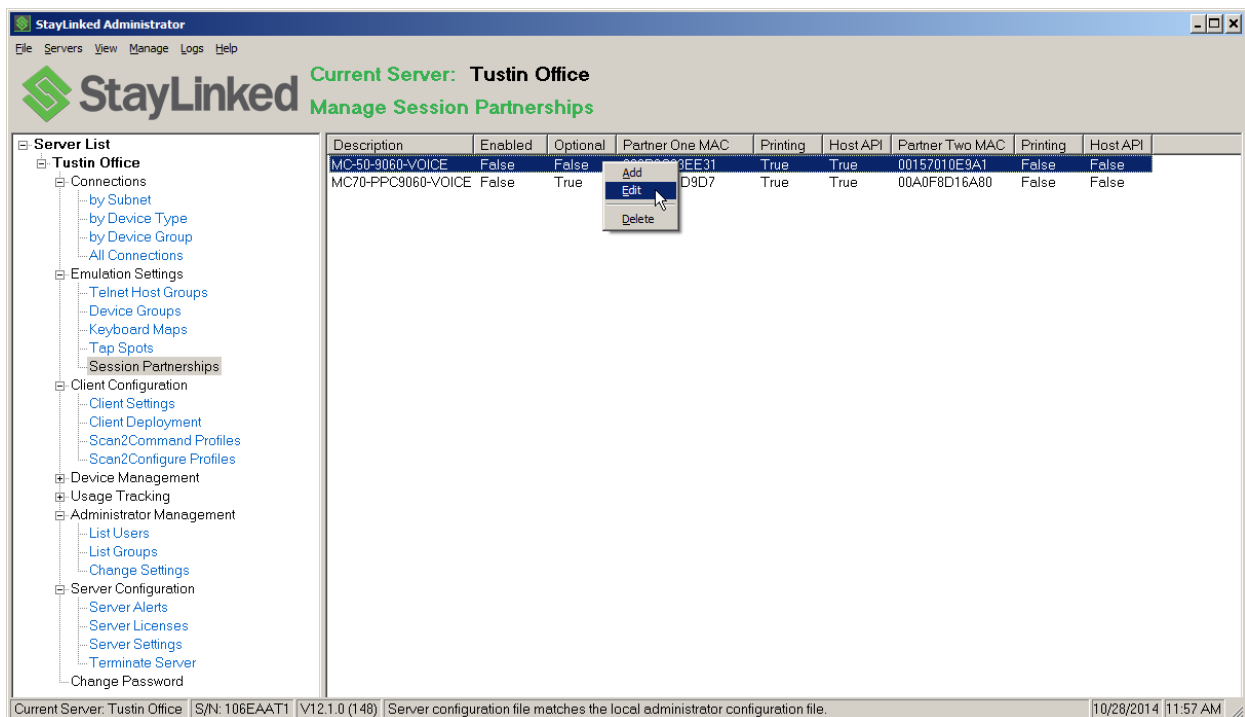


3.9 Managing Session Partnerships

Session Partnerships are a powerful feature that is exclusive to the StayLinked Advanced Terminal Session Management solution. Using the Session Partnerships feature, it is now possible to create a partnership between two wireless terminal devices which will enable these two devices to share the same telnet session. When partner devices are sharing a telnet session, both devices will see the same application screens and will be able to cooperatively enter data into the shared telnet session.

A practical application for this feature would be for a forklift-based warehouse worker. Typically, with a vehicle-mount terminal, the user must use a 'dumb' scanner that is tethered to the VMU (Vehicle-Mounted Unit). Even if the 'dumb' scanner is wireless, there will still be no user interface visible on the scanner gun to show the user the current context of his terminal session. Rather than having this user remain tethered to his VMU, you can instead create a partnership between his VMU and a handheld RF terminal device. Now, the forklift user can see a screen on his VMU, and when necessary, the user can leave the forklift carrying a hand-held terminal that is sharing the same telnet session. After doing some remote data entry with the hand-held terminal, the user can return to the forklift where the VMU will be displaying the same application screen as the partner hand-held terminal. The screen on the VMU and on the partnered hand-held device will remain synchronized at all times because they are sharing the same telnet session.

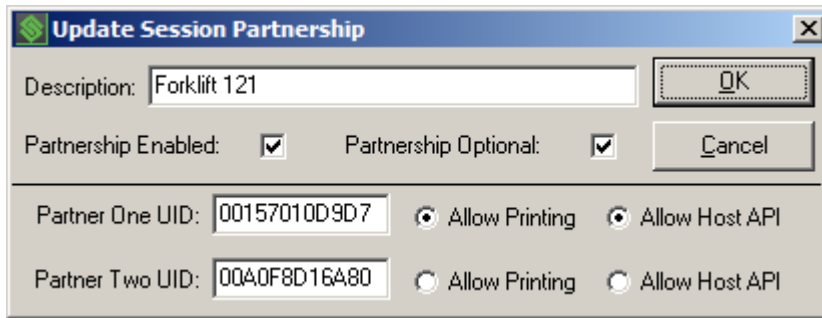
This section describes the configuration and usage of the Session Partnership feature. When you select Session Partnerships from the server tree or the Manage menu, a list of current session partnerships will appear in the main display panel. Clicking the right mouse button on a partnership will cause a small menu to appear with options to Add, Edit, and Delete a session partnership.



Session Partnerships - Add – Select this menu option in order to add a session partnership.

Session Partnerships - Edit – Select this menu option in order to modify the attributes of the selected partnership.

Session Partnerships - Delete – Select this menu option in order to remove the selected partnership from the list.



Description – Enter a meaningful description of the session partnership.

Partnership Enabled – Check this box to make the partnership active.

Partnership Optional – Check this box to make the partnership optional. When selected, the device joining an existing session started by the partner will be prompted to join the session or not. If this option is not selected, the device will join an existing partner session immediately and automatically.

Partner One/Two UID – Enter the 12-digit StayLinked Unique ID (UID) of one of the partner devices. A partner UID can only appear as a partner once in the system.

Partner One/Two Allow Printing – Only one of the partner devices is allowed to process client printing instructions from the telnet session. Select this option to have the partner respond to printing instructions.

Partner One/Two Allow Host API – Only one of the partner devices is allowed to process Host API instructions from the telnet session. Select this option to have the partner respond to Host API instructions.

Running Partner Sessions

Following is an example of the operation of a Session Partnership between a Vehicle-Mount Unit (VMU) on a forklift and a Hand-Held Terminal. In this case, the partnership was created with the 'Optional' selection and the VMU was selected to 'Allow Printing' and also to 'Allow Host APIs'.

The warehouse user grabs the hand-held terminal that is partnered with his VMU and heads to the forklift. Once at the forklift, the VMU is powered on and a StayLinked Session is created. The user logs onto the host and is presented with the application 'Picking Menu'. Now, the user grabs the hand-held terminal and powers it up. The hand-held creates a StayLinked Session. The StayLinked Server recognizes the session partnership and determines that a session is already started for one of the partners. Since the partnership is optional, the hand-held terminal displays a message allowing the user to either 'Join' or 'Skip' the partner session. In this case, the user selects to join the partner session and the current session screen is displayed immediately. Now, the user holsters the hand-held terminal and, using the VMU, determines the first picking location. Upon driving to the location, the user retrieves the item from an upper rack and scans the location with the VMU tethered long-range scanner. The system shows the user the next item to pick, which turns out to be a small item just one rack over and at knee height. So, the user exits the forklift, walks over to the next rack and locates the item. The user grabs the hand-held terminal from the holster and scans the location tag into the current partnered session screen. The user can see on the hand-held screen that the third item to pick is one shelf up, so he grabs that item and scans the location from the rack using the hand-held. Since item four is on the next aisle, the user holsters the hand-held and returns to the forklift with items two and three. Now the user can drive to the next aisle and continue picking the order, using the tethered scanner or the partnered hand-held terminal as desired. Upon completion of the shift, the user terminates the session on the VMU which automatically terminates the partner session on the hand-held terminal.

3.10 Client Administration

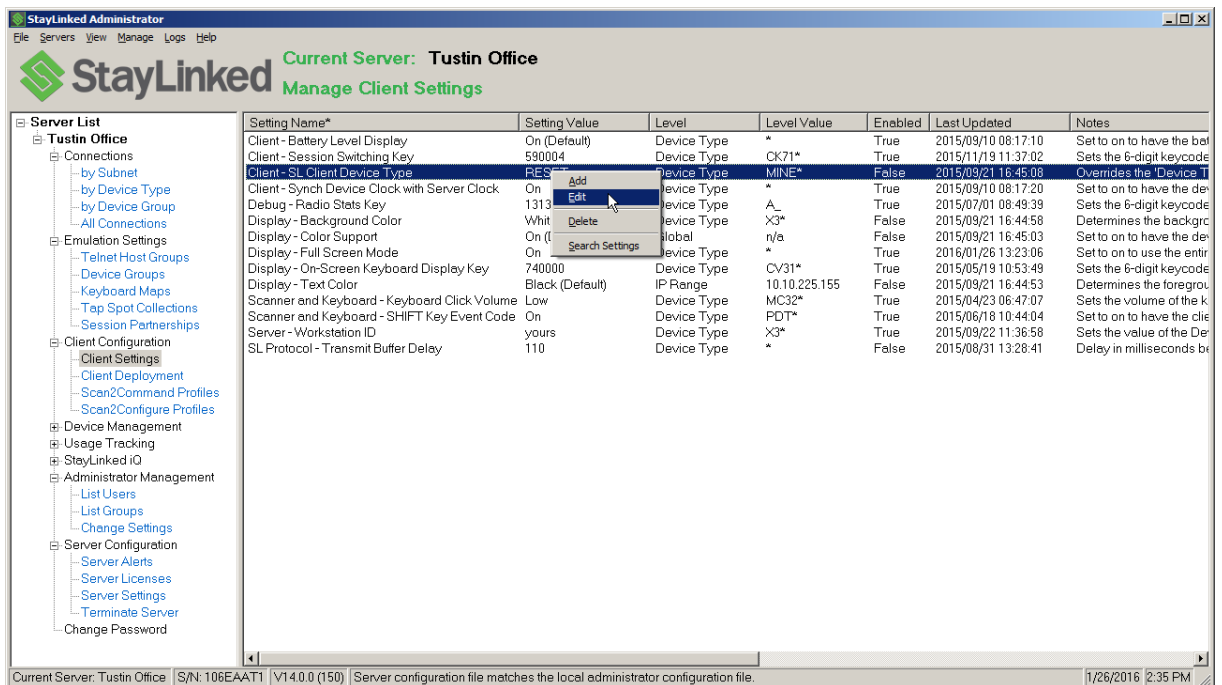
This section describes the various methods provided to centrally manage the StayLinked Client software on your devices. Topics include managing the client control settings, deploying client configuration files and managing automated client software deployment.

3.10.1 Managing Client Settings

Client Settings are stored on the device in the 'staylink.ini' file and they control the behavior of the StayLinked Client on the device. A powerful component of the StayLinked feature set is the ability to set and control many of the client settings right from the administrator. You can even specify to which device or group of devices the setting is targeted. This feature will save you all the time and headaches of trying to make setting changes on individual devices. Configured client settings are transferred to the clients when they start their next new StayLinked session or can be pushed immediately to specific, connected devices.

When you select Client Settings from the server tree or the Manage menu, a list will appear in the main display panel, showing all of the client settings that are currently defined for the selected server. You can sort the client settings listing by clicking on the appropriate column headers.

Clicking the right mouse button in a blank area of the list or on a client setting will cause a small menu to appear with options to Add, Edit, Delete or Search Settings.



Client Settings - Delete – Select this menu option in order to delete a client setting from the list.

Client Settings – Search Settings – Select this menu option to access a search dialog that can help you find the Client Setting that you wish to add to the list. The search dialog will provide a text box where you can enter a search term. Press ENTER to have the results list populated with any Client Settings that contain your search term found in the 'Setting Name' or the 'Setting Description'. When you find the desired Client Setting in the list, double-click on it to open the 'Add' dialog.

Client Settings - Add – Select this menu option in order to add a new client setting to the list.

Add Client Setting

Setting Information

Group: Client

Setting: Auto Connect

Controls if and how the device automatically connects to the server.

☐ Enabled

☒ Show Advanced

Level Information

Setting Level: Global

Setting Value

Value: Always

Notes

All of our devices should always automatically connect to the StayLinked server.

Group: Use this drop-down list to select a group of client settings to work with.

Setting: Use this drop-down list to select from the client settings included in the selected group. After a selection is made, a brief description of the setting is provided below. You can hover your mouse-pointer over the 'setting' to display a 'tool-tip' that will show the syntax for the current client setting and the selected value.

Enabled: Check this option to enable the setting. Only enabled settings will be kept current on the targeted devices. If this option is not checked, the server will completely ignore the setting.

Show Advanced: Check this option to have the contents of the 'Setting' drop-down list include less-frequently used advanced settings. This option will be remembered the next time you use this dialog.

Setting Level: Use this drop-down list to select from the following distribution groups:

Global – Setting applies to all devices

Device Type – Setting applies only to the specified device type (a text box will appear for you to enter the device type or a drop-down list of devices will be provided if the setting only applies to certain devices). Note: when specifying a device type, enter the value exactly as reported by the device. The only exception to this would be the use of the '*' wildcard character at the end of your entry. This will allow you to cover multiple, similar devices with a single entry. Use this option to define a setting for all devices of a specific type.

IP Range – Setting applies only to the specified range of IP addresses (3 text boxes will appear for you to enter the Low and High IP addresses plus a Device Type filter).

MAC Address – Setting applies only to the specified MAC address (a text box will appear for you to enter the MAC Address). Use this option to define a setting for a single device.

Setting Value: Depending on the Setting, you enter a value into a text box or select from a drop-down list of available options.

Notes: Provided for your convenience. These notes have no effect on setting processing. They can, however, help you to organize and manage your client settings by providing a place to record why you created this client setting for future reference.

Client Settings - Edit – Select this menu option to update an existing client setting in the list.

Setting: Displays the current setting and a description below. You can hover your mouse-pointer over the 'setting' to display a 'tool-tip' that will show the syntax for the current client setting and the selected value.

Enabled: Check this option to enable the setting. Only enabled settings will be kept current on the targeted devices. If this option is not checked, the server will completely ignore the setting.

Setting Level: Use this drop-down list to select from the following distribution groups:

Global – Setting applies to all devices

Device Type – Setting applies only to the specified device type (a text box will appear for you to enter the device type or a drop-down list of devices will be provided if the setting only applies to certain devices). Note: when specifying a device type, enter the value exactly as reported by the device. The only exception to this would be the use of the '*' wildcard character at the end of your entry. This will allow you to cover multiple, similar devices with a single entry. Use this option to define a setting for all devices of a specific type.

IP Range – Setting applies only to the specified range of IP addresses (3 text boxes will appear for you to enter the Low and High IP addresses plus a Device Type filter).

MAC Address – Setting applies only to the specified MAC address (a text box will appear for you to enter the MAC Address). Use this option to define a setting for a single device.

Setting Value: Depending on the Setting, you enter a value into a text box or select from a drop-down list of available options.

Notes: Provided for your convenience. These notes have no effect on setting processing. They can, however, help you to organize and manage your client settings by providing a place to record why you created this client setting for future reference.

3.10.2 Managing Client Configuration File Deployment

The StayLinked Client Software determines most of its behavior by using settings from the 'staylink.ini' file. The previous section of this document describes how to centrally manage the settings that are stored in this file. There are, however, additional configuration files that might be used by the StayLinked Client Software to control other aspects of the behavior of the device or the client software. Here is a list of some of these files:

EXTKEYS.INI – Configures the tap-able button bar that can be displayed on PPC/CE devices.

SCANNER.INI – Configures the OEM scanner engine on devices that have no native user interface.

LOCALE.INI – Provides localization support for alternate language fonts on PPC/CE devices.

SERVERS.INI – Provides access to multiple and/or backup StayLinked Servers from a client.

CONNECTIONS.INI – Provides access to multiple, individually configured connections to one or more StayLinked Servers from a client.

COLORS.INI – Configures alternate host foreground/background color mapping on the devices.

These configuration files can also be managed centrally from the StayLinked Administrator in a manner that is very similar to the management of the individual device settings. You can use the 'Device Settings' management feature to deploy various versions of these files to specific devices. Clicking the right mouse button in a blank area of the 'Device Settings' list or on a device setting will cause a small menu to appear. Select the 'Add' option and then in the 'Setting' drop-down list, find and select the 'All – Configuration File Transfer' device setting. The following dialog will be displayed:

Add Client Setting

Setting Information

Group: All

Setting: Configuration File Transfer

This setting describes a configuration (.INI) file to be transferred from the server to the device.

☐ Enabled

☒ Sort Settings

Level Information

Setting Level: Global

File Transfer Details

Import File Name:

Server File Name:

Device File Name:

Notes

Enabled: Check this option to enable the setting. Only enabled settings will be kept current on

the targeted devices. If this option is not checked, the server will completely ignore the setting.

Setting Level: Use this drop-down list to select from the following distribution groups:

Global – Setting applies to all devices

Device Type – Setting applies only to the specified device type (a text box will appear for you to enter the device type or a drop-down list of devices will be provided if the setting only applies to certain devices). Note: when specifying a device type, enter the value exactly as reported by the device. The only exception to this would be the use of the '*' wildcard character at the end of your entry. This will allow you to cover multiple, similar devices with a single entry. Use this option to define a setting for all devices of a specific type.

IP Range – Setting applies only to the specified range of IP addresses (3 text boxes will appear for you to enter the Low and High IP addresses plus a Device Type filter).

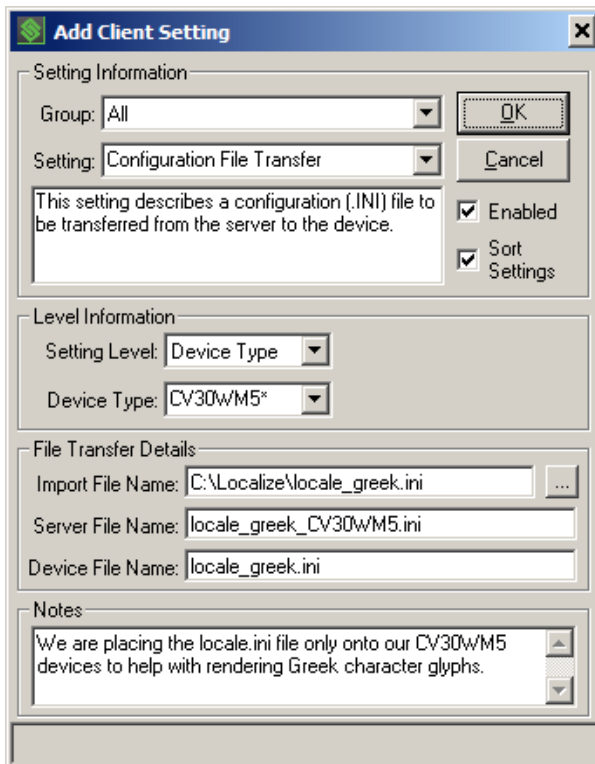
MAC Address – Setting applies only to the specified MAC address (a text box will appear for you to enter the MAC Address). Use this option to define a setting for a single device.

Import File Name: Use the 'browse' button to the right of this textbox to locate and select the configuration (.INI) file that you wish to transfer for this entry. This file will be transferred to the server and stored there to be deployed to devices that are selected for this setting.

Server File Name: Enter a unique file name to be used for this file when it is stored on the server. All of the files selected for 'Configuration File Transfer' settings will be stored in a single folder on the StayLinked Server machine at '..\stay-linked\deploy\files'. Each of these files must have a unique file name in this folder on the server.

Device File Name: Enter the name of this file as it should be stored on the device. You should provide a path as part of the name only if the file is not one that is recognized by and managed by the StayLinked Client on the device. The files listed at the top of this section are automatically handled by the StayLinked Client and so only that name needs to be specified for this value.

Notes: Provided for your convenience. These notes have no effect on setting processing. They can, however, help you to organize and manage your client settings by providing a place to record why you created this client setting for future reference.

Client Configuration File Deployment Example:


Add Client Setting

Setting Information:

Group: All

Setting: Configuration File Transfer

This setting describes a configuration (.INI) file to be transferred from the server to the device.

☒ Enabled

☒ Sort Settings

Level Information:

Setting Level: Device Type

Device Type: CV30w/M5*

File Transfer Details:

Import File Name: C:\Localize\locale_greek.ini

Server File Name: locale_greek_CV30w/M5.ini

Device File Name: locale_greek.ini

Notes:

We are placing the locale.ini file only onto our CV30w/M5 devices to help with rendering Greek character glyphs.

This example shows the dialog for sending a 'locale.ini' file to devices that are of a specific device type, in this case Symbol PDT9000 devices.

Import File Name: The original 'locale.ini' file was located on the Administrator PC in the 'c:\localize' folder with the name 'locale_greek.ini'. This file will be transferred to the server.

Server File Name: The unique file name to be used for this file when it is stored on the server has been entered as 'locale_greek_pdt9000.ini'. Since all of the files selected for 'Configuration File Transfer' settings will be stored in a single folder on the StayLinked Server machine, each of these files must have a unique file name in this folder on the server. The files are stored on the StayLinked Server at '..\stay-linked\deployfiles'.

Device File Name: The name of this file as it will be stored on the device is 'locale.ini'. The 'locale.ini' is a special configuration file that is recognized and managed by the StayLinked Client. In this case, it is not necessary to provide a path for the file on the device.

After configuring the dialog for 'Add Device Setting', press the OK button to validate the dialog. Once validated, the file will be transferred from the Administrator to the StayLinked Server where it will be stored for deployment to qualifying devices. When a StayLinked device creates a new connection to the StayLinked Server, and both 'Configuration File Deployment Settings' and 'Device Settings' are to be sent to the device, first the 'Configuration Files' will be transferred to the device and then immediately the 'Device Settings' will be sent to the device. The StayLinked Client will restart automatically after receiving these files and settings and then, upon connection, those settings will take effect immediately.

3.10.3 Managing Client Deployment

The StayLinked Client Deployment feature provides a method to centrally manage and wirelessly upgrade StayLinked Client software running on your devices. From the StayLinked online portal, you can download StayLinked Client Deployment Packages for your specific wireless devices. These deployment packages can be imported into the StayLinked Administrator which will install the package onto the StayLinked Server. Using the StayLinked Administrator, you can control when these packages will be deployed, to what devices and how to deploy them. When a device starts a new StayLinked session, if it has a different version of client software waiting, then depending upon the configuration of the package on the server, they may be prompted to upgrade the client software or they may have no choice. If the client software is upgraded, the user will be shown a progress indicator on the device screen and after the software package is transferred, the software will be installed and the devices will be rebooted or restarted, depending upon the platform.

When you select Client Deployment from the server tree or the Manage menu, a list will appear in the main display panel, showing all of the client packages that are currently installed onto the selected server.

Clicking the right mouse button on a client package will cause a small menu to appear with options to Import, Edit, or Remove a client package and control the number of concurrent client updates that are allowed to be processed at one time. You can also 'double-click' a package to 'Edit' the package.

StayLinked Administrator

File Servers View Manage Logs Help

Current Server: Tustin Office

Manage Client Deployment

Package Name	Version(Build)	Release Date	Enabled	Mandatory	Deploy DM	Low IP Range
Honeywell 70E - WM 6.5	v12.1.0(124)	7/17/2014	False	False	False	
Psion VH10 CE 6.0	v11.0.0(120)	3/19/2013	False	False	False	
Psion XT15/RT15 CE 6.0	v11.0.0(120)	5/16/2013	False	False	False	
Psion XT15/RT15 WM 6.5	v11.0.0(120)	7/22/2013	False	False	False	
Stay-Linked Android Client	v1.0(122)	3/20/2014	False	False	n/a	
Stay-Linked Windows Client	v1.0(121)	9/20/2013	True	False	n/a	
Stay-Linked Windows-7 Client	v1.0(123)	5/14/2014	False	False	n/a	
Symbol MC3090	v1.0(120)	7/24/2013	True	False	True	
Symbol MC9190 - MOBILE 6.5	v1.0(119)	10/18/2012	True	False	True	
Symbol MC92N0 - CE 7.0	v12.1.0(124)	7/11/2014	True	False	True	
Symbol MC92N0 - MOBILE 6.5	v12.1.0(125)	8/28/2014	True	False	False	
Symbol VC70 - CE 7.0	v11.0.0(120)	5/10/2013	True	False	False	
Symbol WorkAbout Pro G4 CE 6.0	v12.1.0(125)	8/5/2014	False	False	False	
Symbol WorkAbout Pro G4 WM 6.5	v12.1.0(125)	8/27/2014	False	False	False	
Symbol WT4090 - CE 5.0	v11.0.0(120)	2/25/2013	False	False	False	
Symbol WT41N0 - CE 7.0	v12.1.0(126)	9/24/2014	True	False	True	

Current Server: Tustin Office | S/N: 106EAAT1 | V12.1.0 (148) | The configuration file was retrieved from the server. 10/28/2014 12:31 PM

When you select the Import option from the menu, the following window will appear:

The 'Import a Deployment Package' dialog box features a title bar with the same text. It contains a 'Package File:' label followed by a text input field and a browse button (...). Below this, there are labels for 'Package:', 'Version(Build):', and 'Date:'. The 'Import Status:' is displayed in red text as 'Waiting to verify selected package.' At the bottom, there are two buttons: 'Verify' and 'Close'.

Package File: Type or browse for the client deployment package file name (with the .sdp extension) that you wish to import. Client deployment package files are available on the StayLinked portal site.

Verify: Click on this button to verify the deployment file and contents. If the file is a valid deployment package, the Package information will be displayed in the window and the 'Verify' button will transform into an 'Install' button.

Install: Click this button to install the package onto the StayLinked server. By default, when a new package is installed, it will be disabled until it has been manually reviewed and enabled. While the package is being imported to the server, the 'Import Status' will be updated.

When you select the Edit option from the menu, or double-click on the package, the following window will appear:

The 'Deployment Package Maintenance' dialog box has a title bar with a green icon and the text 'Deployment Package Maintenance'. It includes a 'File' menu icon. The main area displays package details: 'Package Name: Symbol MC92N0 - CE 7.0', 'Version(Build): v12.1.0[124]', and 'Package Date: 7/11/2014'. Below these are 'Client File: StayLinked_MC92N0CE_ARMv4i.CAB', 'Deploy CRC File: deploy/symbol/MC92N0C/StayLinked_MC92N0CE_AR', and 'Deployment File: deploy/symbol/MC92N0C/StayLinked_MC92N0CE_AR'. A section for settings includes 'Package Enabled' (checked), 'Mandatory Update' (unchecked), and 'Deploy DM Agent' (unchecked). There are input fields for 'Deployment Address Range' with 'Low' and 'High' sub-fields. At the bottom, a list of 'Package Devices' includes MC92N0C_28, MC92N0C_43, MC92N0C_53, MC92N0C_E3, MC92N0C_E5, and MC92N0C_VT. A context menu is open over the list, showing 'Add Custom Device Type' and 'Delete' options.

Package Enabled: Use this check box to indicate that this deployment package is enabled and should be transferred to the appropriate client devices. If this option is not checked, the server will completely ignore the package.

Mandatory Update: Use this check box to indicate that this deployment package is mandatory, and that the client will not be allowed to run a StayLinked session until the update has been accomplished. If this check box is not selected, the user will be given a choice to update now or to update later.

Deploy DM Agent: Use this check box to cause the 'Device Management Agent', if included in the Deployment Package, to be transferred to and installed onto the device.

Deployment Address Range: Enter the range of device IP addresses that will be affected by this client deployment package.

Package Devices: Displays a list of device types to which this client deployment package will be applied. This list is predefined and is not managed by the administrator. The client software in the package is designed for the device types that appear in this list.

Add Custom Device Type: This right-click menu option for the Package Devices listing will allow you to add a custom device type to the list of devices that will be upgraded using this deployment package. You must make sure that any device types added here are compatible with this deployment package.

Delete: This right-click menu option for the Package Devices listing will allow you to delete a device type from the list of devices that will be upgraded using this deployment package.

When you select the Remove option from the menu, you will be prompted to have the client deployment package removed from the list of packages. This option does not physically remove the client package from the server. This option only removes the entry from the list of deployment packages, making it no longer be available for deployment. You may re-import the package again in order to make it available to devices.

When you select the Set Max Transfers option from the menu, you will be prompted for the number of concurrent transfers that you wish to allow from this server to the devices. This feature provides you with control over the bandwidth that will be available for client software updates. If a device starts a new session, is eligible for a client software update, but there are already the maximum allowed number of transfers in process, then the user at the device will be notified and given the choice to try the upgrade again or to start a session using their current client software.

3.11 Scan2Command and Scan2Configure Profiles

The Scan2Command and Scan2Configure Profiles management options, introduced with Version 9.0.0 of StayLinked, provides a method by which you can design and print sheets of barcodes that can be scanned by devices running the StayLinked client. These barcode sheets can be used both to configure the client software and also to command the client or the telnet sessions.

3.11.1 Scan2Command Profiles

The Scan2Command Profiles will provide barcode sheets that can contain any StayLinked mnemonic or other client commands or scripts to be executed on the device or in the Telnet Session. There are three types of values that can be represented in a Scan2Command Profile.

Mnemonics – These values, when scanned, will command the telnet session to take some action, like press Enter, or press a Function Key, etc.

Client Commands – These values, when scanned, will instruct the StayLinked Client software to take some action locally on the device. Examples are, toggle the SIP, switch sessions, switch font sizes, exit the session, etc.

Scripts - These values, when scanned, will command the telnet session to follow a script of instructions. An example would be a single barcode that the user can scan to log onto the Telnet Server.

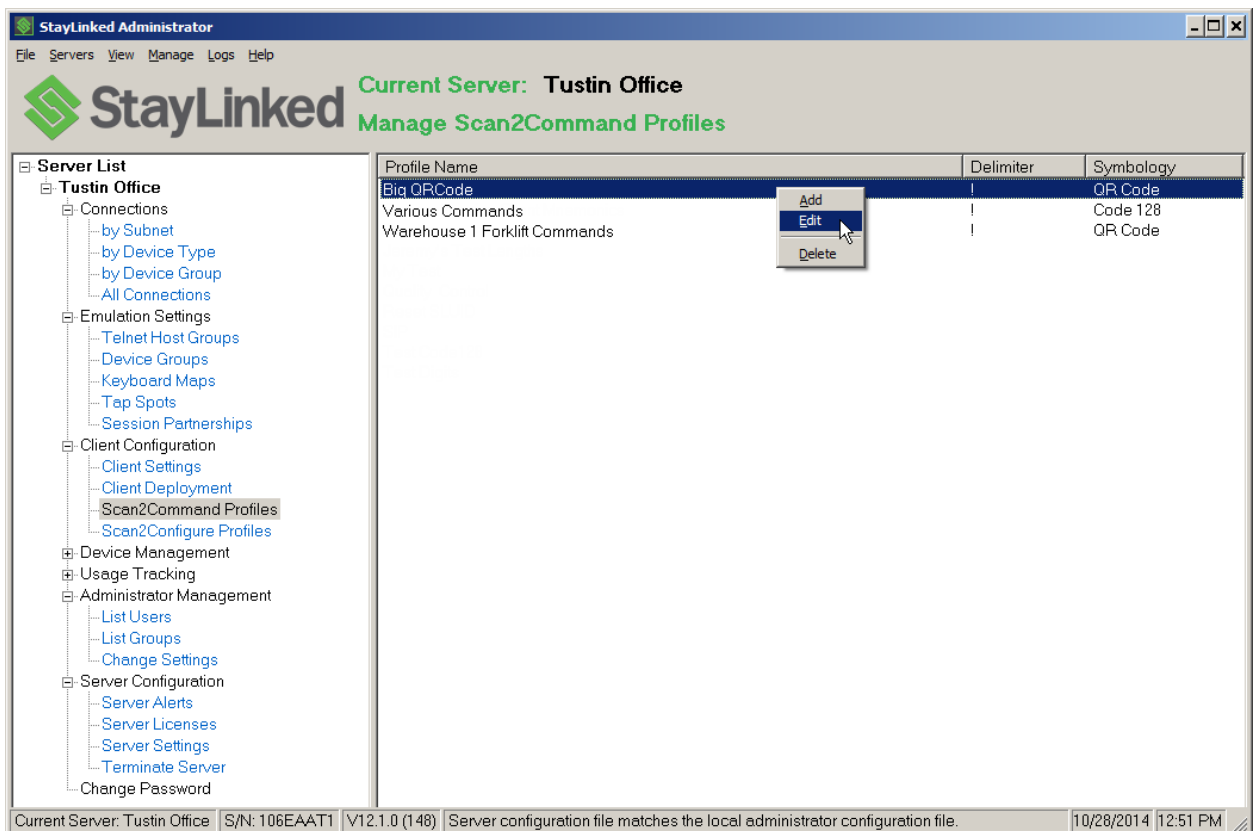
Here is a sample logon script for a 5250 session: [clear]myuserid[fldext]mypassword[enter]

Here is a sample logon script for a VT session: myuserid[enter][delay]mypassword[enter]

3.11.2 Scan2Configure Profiles

The Scan2Configure Profiles will provide barcode sheets that can contain one or more 'Client Settings' that will be used to configure the behavior of the StayLinked Client on the device. These barcode sheets can be printed using 1D symbologies where each client setting is represented in a single barcode. Or, you can print the Scan2Configure profile sheet using 2D symbologies where all of the client settings are combined into one (or more) 2D barcodes images that can be scanned to configure the device. The Scan2Configure profile sheets are typically scanned using the client-side 'Scan Test' user interface, or they can be scanned while running a StayLinked Session. The Scan2Configure profiles can also include an optional 'Restart Client' post-config command that will be acted upon after all of the client settings have been processed, causing all of the new settings to be loaded on startup.

This section describes the configuration and usage of the Scan2Command and Scan2Configure features. When you select one of these options from the server tree or the Manage menu, a list of current profiles will appear in the main display panel. Clicking the right mouse button on a profile will cause a small menu to appear with options to Add, Edit, and Delete a profile.

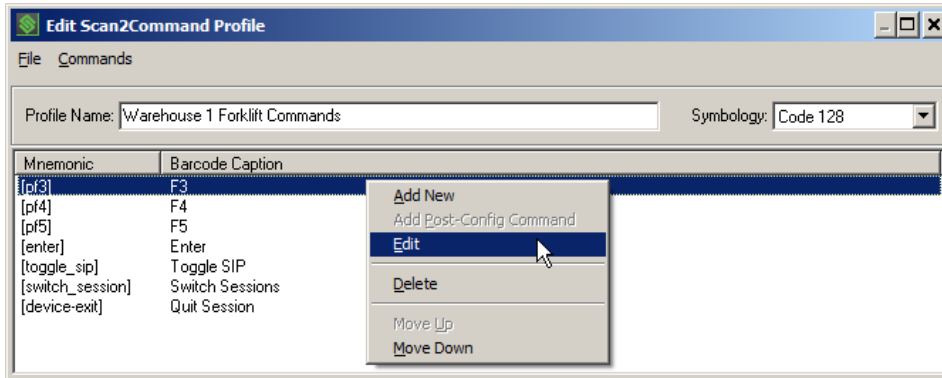


Scan2Command/Scan2Configure - Add – Select this menu option in order to add a new profile.

Scan2Command/Scan2Configure - Edit – Select this menu option in order to modify the contents and attributes of the selected profile. You can also use this option to print an existing profile.

Scan2Command/Scan2Configure - Delete – Select this menu option in order to remove the selected profile from the list.

When you 'Add' or 'Edit' a profile, you will be presented with the Profile dialog:



Profile Name: This text box is used to enter the unique name for this Scan2Command or Scan2Configure Profile.

Symbology: Select from this list the symbology to be used for printing the profile barcode sheet. You can select from the following symbologies: Code 39 Full ASCII (1D), Code 128 (1D), PDF417 (2D), QRCode (2D) or DataMatrix (2D).

Symbology Notes: If you select Code 39 Full ASCII, then you must ensure that your scanners are configured to read Code 39 Full ASCII. If you select a 2D symbology for your Scan2Configure profiles, this will cause the client settings to be combined into one (or more) 2D barcode images.

From the File Menu:

Save Changes: Select this menu option to save the current profile.

Print: Select this menu option to print the current profile.

Print Preview: Select this menu option to preview the printed current profile.

Settings – Barcode Delimiter: Select this menu option to change the delimiter used to identify a Scan2Command or Scan2Configure barcode to the StayLinked Client software.

Settings – Barcode Spacing: Select this menu option to change the vertical spacing between printed barcodes.

From the Commands/Settings Menu:

Add New: Select this menu option to add a new command or setting.

Add Post-Config Command: Select this menu option to add a post-configuration command. This option is only available for Scan2Configure profiles.

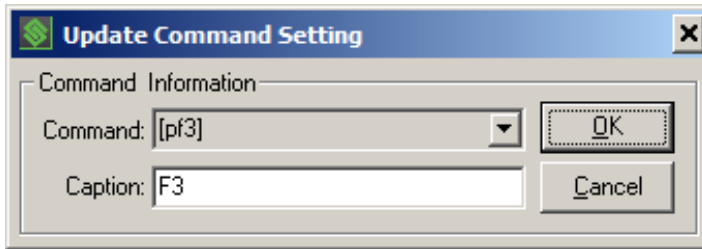
Edit: Select this menu option to edit the selected command or setting.

Delete: Select this menu option to delete the selected command or setting.

Move Up: Select this menu option to move the selected command or setting up in the list.

Move Down: Select this menu option to move the selected command or setting down in the list.

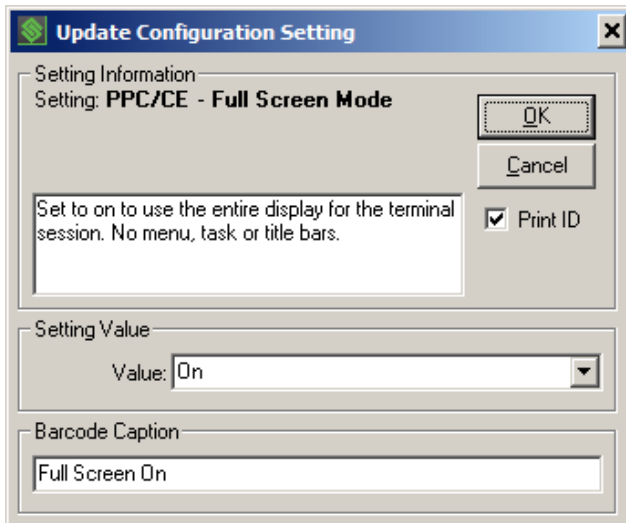
If you select to Add or Edit a Scan2Command Command entry, you will be presented with a dialog similar to this:

The dialog box is titled "Update Command Setting" with a close button (X) in the top right corner. It contains two sections: "Command Information" and "Buttons". The "Command Information" section has a "Command:" label followed by a text box containing "[pf3]" and a drop-down arrow to its right. Below this is a "Caption:" label followed by a text box containing "F3". The "Buttons" section contains "OK" and "Cancel" buttons.

Command: You can select a command from the drop down list, or directly type in a command or script to be encoded into the barcode.

Caption: Type in a meaningful caption that will be printed below the barcode image.

If you select to Add or Edit a Scan2Configure Setting entry, you will be presented with a dialog similar to this:

The dialog box is titled "Update Configuration Setting" with a close button (X) in the top right corner. It contains three sections: "Setting Information", "Setting Value", and "Barcode Caption". The "Setting Information" section has a "Setting:" label followed by a text box containing "PPC/CE - Full Screen Mode". Below this is a text box containing "Set to on to use the entire display for the terminal session. No menu, task or title bars." and a "Print ID" checkbox which is checked. The "Setting Value" section has a "Value:" label followed by a text box containing "On" and a drop-down arrow to its right. The "Barcode Caption" section has a text box containing "Full Screen On". The "Buttons" section contains "OK" and "Cancel" buttons.

Setting: In Add mode, you can select a client setting from this drop-down list.

Setting Value: Depending on the selected Client Setting, you enter a value into a text box or select from a drop-down list of available values.

Barcode Caption: Type in a meaningful caption that will be printed below the barcode image.

Print ID: Check this box if you would like to have the 'Setting ID' encoded into the barcode data rather than having the 'Setting Name' encoded into the barcode data. The 'Setting ID' is a three-digit numeric value that will create a smaller barcode that if you encode the 'Setting Name'.

3.12 Device Management

The 'Device Management' features have been end-of-life since September, 2015. Systems without a device management license installed will not see various settings relating to these features. These features are completely removed from the product starting in version 15.1 build 208.

In addition to providing world-class, host-based Telnet Terminal Session management, StayLinked can also provide Device Management features for PPC, Windows Mobile and CE devices as follows:

- System Information
- File Management
- Registry Management
- Network Management
- Device Remote Control
- Software Provisioning

Please review the 'StayLinked Device Management User Guide' for full details of these features.

3.13 Usage Tracking

StayLinked Version 11 and later provides the ability to track the usage of StayLinked devices. Using this feature, you can track unique devices that have connected to the server. For each unique device, you can also track Sessions, Activity, Statistics and User IDs. Usage Tracking is also used to manage licensing for StayLinked Speech and StayLinked SpeechLink products.

Please review the 'StayLinked Usage Tracking User Guide' for full details of these features.

3.14 StayLinked iQ

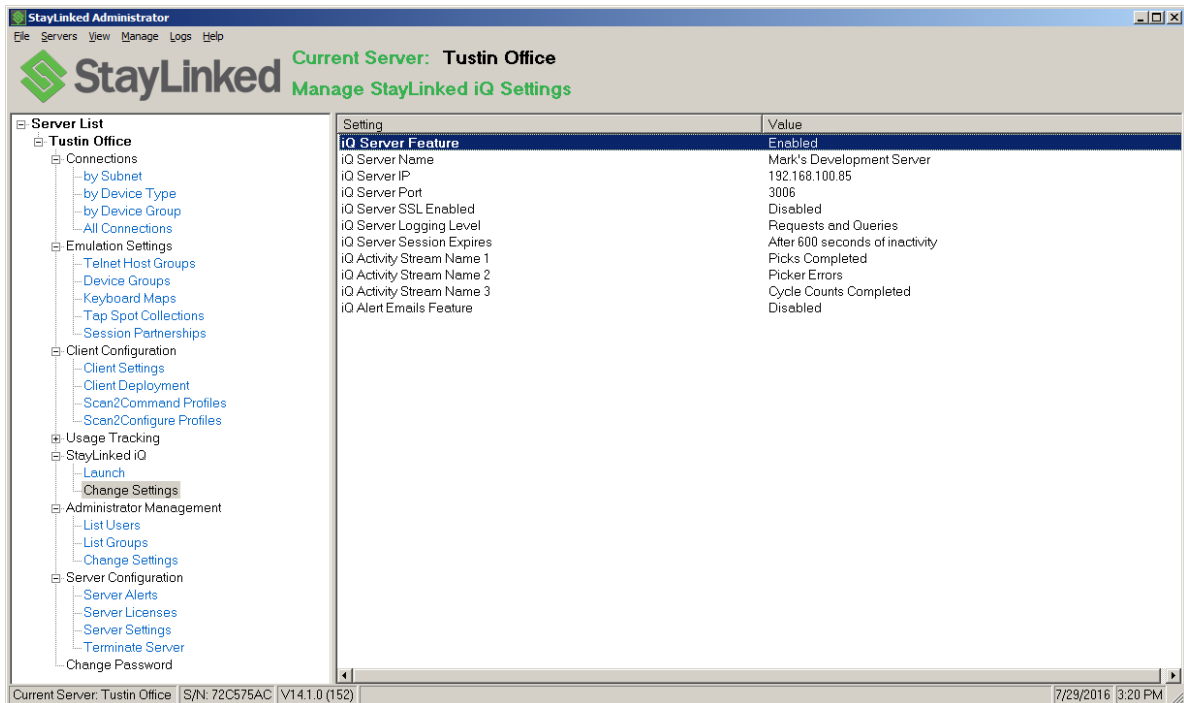
StayLinked Version 14 and later provides a technology preview of a powerful tool specifically targeted at Terminal Emulation environments. Building on StayLinked's unique architecture, StayLinked iQ measures and helps to optimize all the aspects of the TE solution stack including:

- Device performance including battery, scanner, radio and data entry mechanisms
- Worker behavior
- Worker interaction with device and application
- Network availability performance
- Server performance
- Application performance
- Business process
- And, ultimately, worker productivity

Having this comprehensive visibility across the whole solution enables iQ to have a truly holistic view. This is a rare and very valuable capability. StayLinked captures comprehensive data relating to the above areas and pushes it into iQ. Please review the Technical Reference Guide titled 'Implementing StayLinked iQ' in order to get started using these features. Following are details related to configuration and usage.

3.14.1 Change Settings

When you select 'Change Settings' from the server tree, a list of Settings will appear in the main display panel. The various settings can be configured to enable and control the features and options available for the StayLinked iQ Technology Preview.



You must double-click on one of the settings in the list in order to make changes to that setting.

iQ Server Feature: Double-click on this option to select whether the StayLinked iQ Server should be enabled or disabled.

iQ Server Name: Double-click on this option to be prompted to enter a name for the StayLinked iQ Server. This name will be displayed on the iQ Server login screen and on the iQ Dashboard. The name change will take effect immediately.

iQ Server IP: Double-click on this option to be prompted to enter the local IP address to which the StayLinked iQ Server will bind. By default, the StayLinked iQ Server will bind to all active IP addresses. This option allows you to have the iQ Server bind to a specific IP address. You can review the iQ Server log file to determine the results of changing this value. The change will take effect immediately.

iQ Server Port: Double-click on this option to be prompted to enter the TCP Port to which the StayLinked iQ Server will bind. By default, the StayLinked iQ Server will bind to TCP Port 3006. This option allows you to have the iQ Server bind to a specific TCP Port of your choice. You can review the iQ Server log file to determine the results of changing this value. The change will take effect immediately.

iQ Server SSL Enabled: Double-click on this option to be prompted to run the SSL protocol for the StayLinked iQ Server. If you select to run SSL, you must provide a Java Key Store file containing your server certificate. The key store must be in JKS format with the exact name of 'iqserver.jks' and this file should be stored in the 'stay-linked' folder where the StayLinked Server is installed. The password for the JKS file must be 'staylinkediq'. You can review the iQ Server log file to determine the results of changing this value. The change will take effect immediately.

iQ Server Logging Level: Double-click on this option to be prompted to select a logging level for the StayLinked iQ Server. The choices are:

- 0 = Minimum Logging
- 1 = Requests Only
- 2 = Requests and Queries

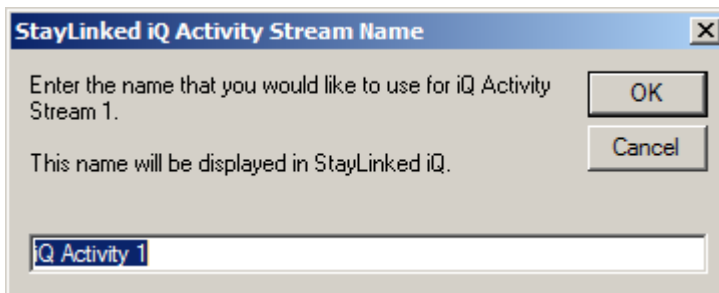
Any changes will take effect immediately.

iQ Server Session Expires: Double-click on this option to be prompted for the number of seconds of inactivity before the StayLinked iQ Browser Session is expired. The choices are:

- 0 = Expires when the browser is closed
- 60 to 86400 seconds of inactivity.

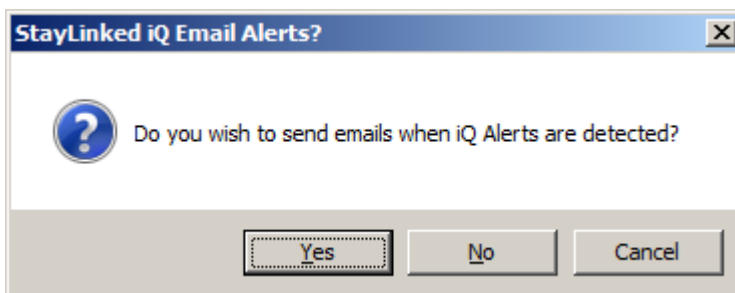
Any changes will take effect immediately.

iQ Activity Stream Name 1, 2 and 3: If you double-click on one of these options, you can define the name of each of the three 'Activity Streams' that you can track on the iQ Dashboard. These activity streams will be available for selection in the Screen Recognition 'Record Usage Activity' Host API dialog.



In this dialog, you can type the name of the activity that you wish to track and record in StayLinked iQ.

iQ Alert Emails Feature: If you double-click on this option, you can enable or disable the sending of emails when iQ Alerts are detected. In the Technology Preview, Alerts will be detected when temporary license keys are about to expire. In the full iQ product, Alerts will be able to be detected and emails sent for many configurable events. If you enable iQ Alert email delivery, you must further configure the required SMTP settings so that the StayLinked Server can send emails when alerts are detected.



If you wish to have emails sent out when StayLinked iQ Alerts are detected, click Yes, otherwise click No. You can click Cancel to make no changes to this setting.

3.15 Administrator Management

This section describes Administrator Management, introduced with Version 9.1.0 of StayLinked. This feature enables the management of the User IDs that are used to control access to the StayLinked Server using the StayLinked Administrator software.

3.15.1 Administrator Management Overview

Following are the primary features of Administrator Management:

- A User ID and password is required to access a server.
- Each StayLinked Server manages its own database of User IDs that have access to that server.
- Each User ID describes in high detail the features of the Administrator that the User ID is permitted to access on that server.
- Each User ID can describe the subsets of devices that are available to be managed on the server.
- Each User ID can be restricted to specific PCs allowed to access the server by origination IP address.
- User IDs and Passwords are case-sensitive.
- Groups can be defined to describe common sets of permissions available for use in the Administrator.
- User IDs can be assigned to a Group and will inherit the available Administrator permissions defined for that Group.
- Administrator Management Settings control the usage properties of User IDs.
- User IDs can become disabled if there are too many unsuccessful attempts to log on.
- Passwords for User IDs can be expired at a specified interval, requiring the user to set a new password the next time they log on.
- Attributes can be set to control the creation of passwords.

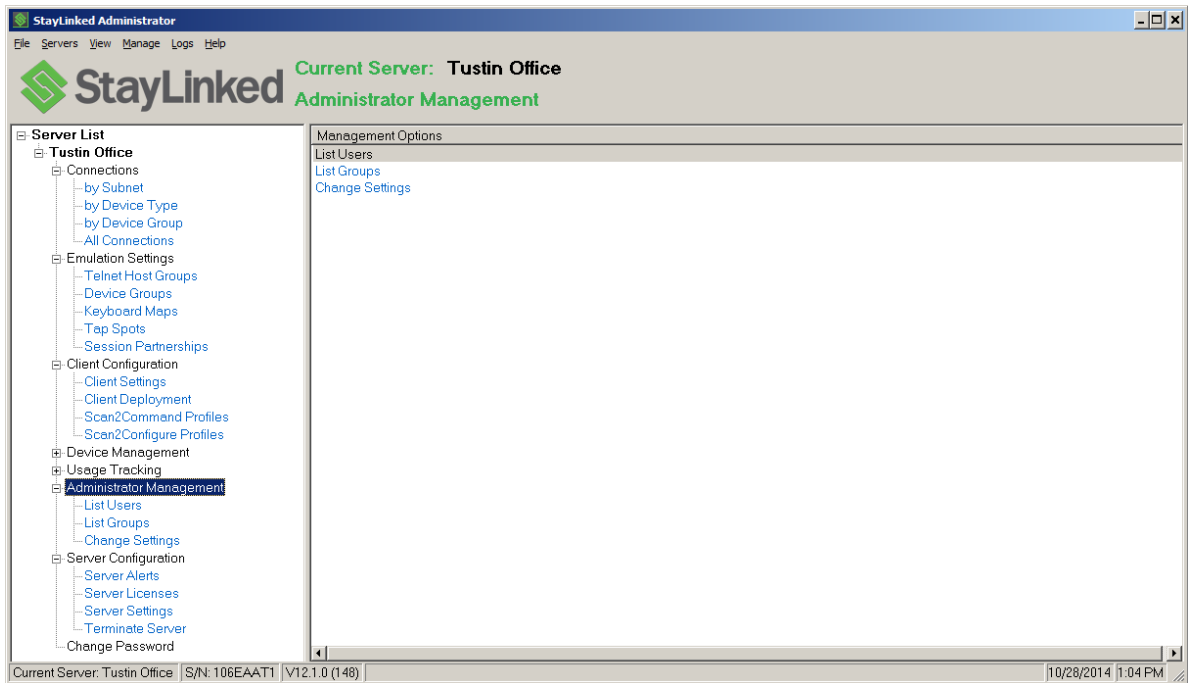
3.15.2 The 'administrator' Master User ID

Every StayLinked Server has an 'administrator' User ID defined. This is the master User ID for each server and this User ID has permissions to access all of the features and functions of the Administrator for this server. The default password for the 'administrator' User ID is 'esp'. This password can be changed to control access to this User ID. The 'administrator' User ID cannot be deleted.

IMPORTANT: It is recommended that you create at least one additional User ID with 'Administrator Management' permissions. This way, if the master 'administrator' User ID becomes disabled, or you cannot remember the password, there will be a way to reset the master 'administrator' User ID. If, however, the master 'administrator' User ID becomes disabled or otherwise cannot be accessed, there is a way to reset it. You will need to create an empty file named 'resetadmin.xml' and place that file onto the server in the '..\stay-linked\config' folder. Then, the next time the StayLinked Server process is started, the master 'administrator' User ID will be reset to its default state. The 'administrator' User ID will be re-enabled and the password will be reset to 'esp'. However, a server process restart is required.

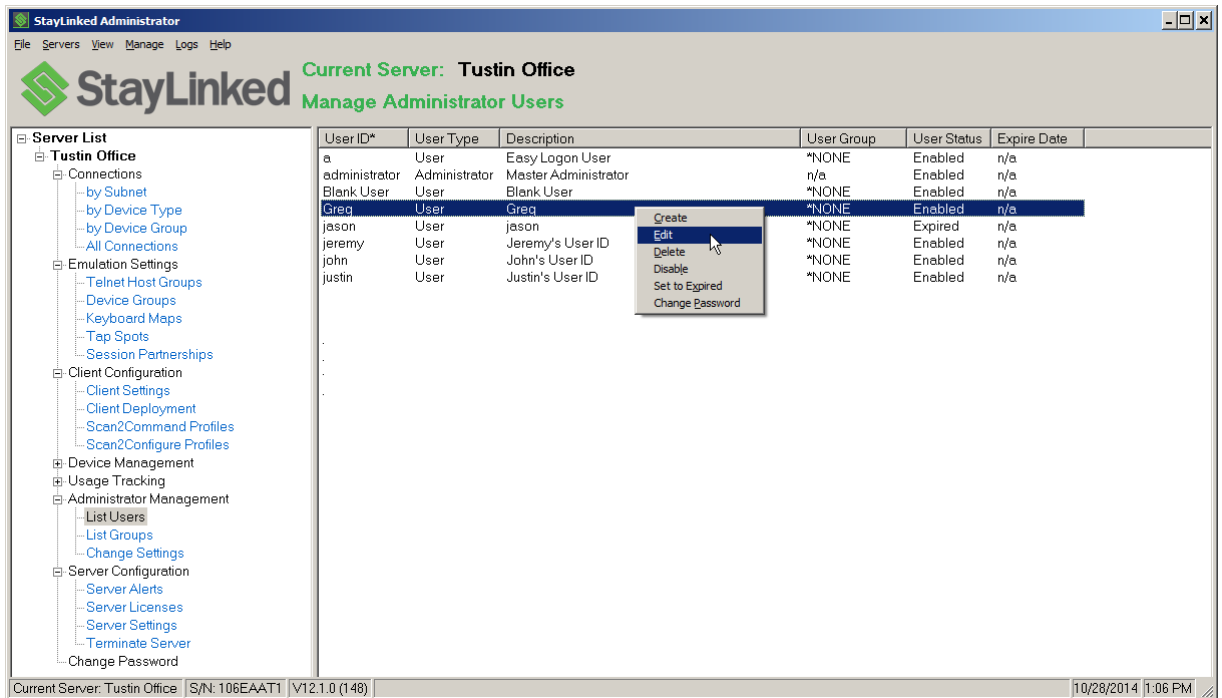
The Administrator Management functions are divided into three groups of configuration settings:

- **List Users** – Display and edit User IDs that are allowed to manage this server.
- **List Groups** – Display and edit Groups that predefine groups of permissions for this server.
- **Change Settings** – Display and edit settings that control the Administrator Management functions.



3.15.3 List Users

When you select 'List Users' from the server tree or the Manage menu, a list of User IDs will appear in the main display panel. Each StayLinked server will have a default 'administrator' User ID, and you can add other User IDs as required.



User ID: This column displays the User IDs that have been defined on this server.

User Type: There are two types of users. There will be only one 'Administrator' type user with the User ID of 'administrator'. All other User IDs that you defined will be of type 'User'.

Description: This is a free-form description that you can enter to help identify a user.

User Group: This column displays the group that the User ID belongs to. If the User ID does not belong to a group, then this column will display the special value of '*NONE'.

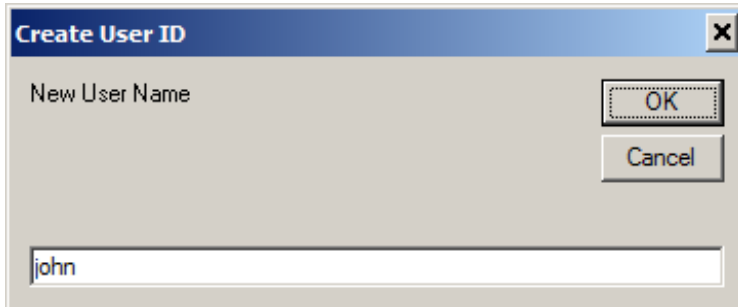
User Status: This column displays the status of the current user as either 'Enabled', 'Disabled' or 'Expired'.

Expire Date: This column displays the date that the password will expire for the User ID. If the Password Expiration Interval setting is set to zero, then this column will display 'n/a'.

Clicking the right mouse button in a blank area or on a User ID will cause a small menu to appear with options you can perform.

3.15.4 Creating a User ID

If you select the menu option to 'Create' a User ID, you will be prompted for the name for the new User ID.

A screenshot of a 'Create User ID' dialog box. The dialog has a title bar with the text 'Create User ID' and a close button (X). Inside the dialog, there is a label 'New User Name' followed by a text input field. The input field contains the text 'john'. To the right of the input field are two buttons: 'OK' and 'Cancel'.

The User ID name is case-sensitive. You can enter any name that does not already exist on this server. The names 'John' and 'john' are considered to be unique names and they can both exist on the server at the same time. It is recommended to use lower-case User IDs for consistency and simplicity. When a User ID is created, the password is set to match the new User ID name. The User ID is also created in the expired status and the user will be forced to change the password the first time they log on using this new User ID. Once the User ID is created, it will appear in the User List and you can then configure the permissions for the user as desired.

3.15.5 Editing a User ID

If you double-click on, or select the menu option to 'Edit', the selected User ID, you will be presented with this dialog:

Edit User ID 'john' on Tustin Office

File View

User Information

User ID: **john** User Status: **Enabled**

Description: Expire Date: **n/a**

User Group:

Module	Function	Setting	Value
Server Logs	Viewing	*YES	*YES
Server Alerts	View	*YES	*YES
Server Alerts	Clear	*YES	*YES
Connection List	Access	*YES	*YES
Connection List	View Details	*YES	*YES
Connection List	File Transfer	*YES	*YES
Connection List	Send Message	*YES	*YES
Connection List	Commands	*YES	*YES
Connection List	Create Partners	*YES	*YES
Connection List	Scanner Control	*YES	*YES
Connection List	Diagnostics	*YES	*YES
Connection List	Viewing Files	*YES	*YES
Connection List	Viewing Logs	*YES	*YES
Connection List	Monitor Session	*YES	*YES
Connection List	Share Session	*YES	*YES
Connection List	Session Take Control	*YES	*YES
Connection List	Transfer Session	*YES	*YES
Connection List	Disconnect Device	*YES	*YES
Connection List	Terminate Session	*YES	*YES
Connection List	Launch Athena	*YES	*YES
Connection List	Manage System	*YES	*YES
Connection List	Manage Files	*YES	*YES

From this dialog, you can perform these functions:

Update the User Description: You can enter a description to help identify the user.

Assign the User ID to an existing Group: If assigned to a Group, the User ID will adopt the permissions assigned to that Group. You can then override individual permissions for this User ID as desired.

Change User ID Permissions: The permissions list enumerates the various available Modules and Functions that can be individually controlled by setting these permissions.

View and change the Allowed Origin IPs: This feature provides the ability to restrict access to this server for a given User ID by the origination IP address of the Administrator PC.

View and change the Connection Filters: This feature provides control over the connections that this User ID can view and manage in the Administrator Connections List.

Save Changes: Select the 'Save Changes' option from the File menu to save your changes to this User ID.

The various elements of this dialog are:

User ID – The User ID that is being edited.

User Status – The current status of this User ID.

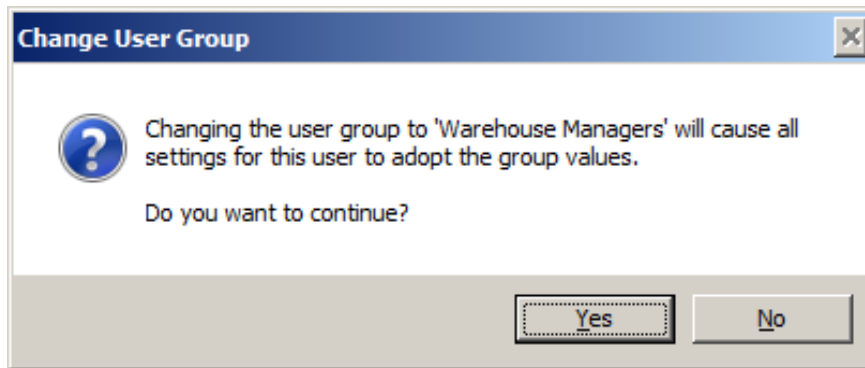
Enabled – The user ID is active and available to be logged on.

Disabled – The User ID is not available to be logged on. A User ID can become disabled by manually changing the status, or if the system is configured to disable the User ID after too many failed logon attempts.

Expired – The password for this User ID is expired. The next time a user attempts to log on with this User ID, they will be prompted to change their password. A User ID can be manually expired or the system can be configured to automatically expire the password at a specified interval.

Description – The description for the User ID that is being edited.

User Group – The Group to which this User ID is a member. If the User ID is not a member of a Group, then the value will be *NONE. If the User ID is assigned to a Group, then the User IDs permissions will be adopted from that Group. When you select a Group from the drop-down list, you will be warned that all of the permissions will be changed to match the selected Group permissions.



Expire Date – The date that the User ID will expire and require the user to enter a new password. If this value is displaying 'n/a', then this means that the server is configured to never expire User IDs.

Permissions List – This list contains all of the modules and functions that can be controlled using permissions. The list displays these columns:

Module – The module in the Administrator to which the permissions apply.

Function – The specific function within the module to which the permission applies.

Setting – The configurable setting that controls the effective permission for this module/function.

Value – The effective permission for this module/function based upon the selected setting.

If the User ID has any 'Connection Filters' defined, then there will be no 'Connection List' module functions displayed in this 'User Information' permissions list. Instead, you will select the 'Connection Filters' option from the 'View' menu to access the 'Connection Filters' that have been defined for this User ID. When you edit a 'Connection Filter', you can configure the permissions that will apply for the 'Connection List' module for the Connections to which the user is allowed access according to that Connection Filter.

3.15.6 Changing User ID Permissions

From the Edit User ID dialog displaying the User ID Information, you can see the permissions list. Each item in this list represents a unique function within a module of the Administrator. You can set the permissions that this user has for the individual function in the module by right-clicking on the item in the permissions list. A context-sensitive menu will appear with the available permissions for this selected item. If the User ID is a member of a Group, then the possible settings for the item are:

- *GROUP** – Set the permission to the value defined in the Group for this module and function.
- *YES** – Give the user permission to this module and function, overriding any Group settings.
- *NO** – Deny the user permission to this module and function, overriding any Group settings.

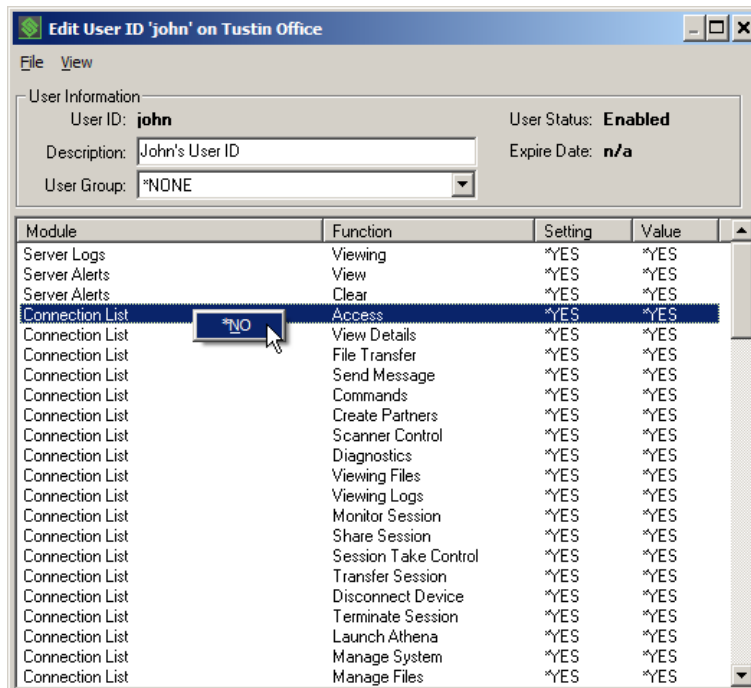
The menu options that will appear are based upon the current setting for this item and the Group membership for the User ID.

If the User ID is not a member of a Group, then depending upon the current setting, the only possible menu options will be either *YES -or- *NO.

If the User ID is a Group member, then depending upon the current setting, the menu options could be either *YES and *NO -or- *GROUP and *YES -or- *GROUP and *NO.

When setting permissions, you can select multiple items from the permissions list and apply your desired setting to all of them at once. If you use Ctrl-Click, then you can select multiple individual items from anywhere in the list. If you use Shift-Click, then you can select a contiguous block of items. Right-click on the selected items and a context menu will appear with the available permissions, depending upon whether the User ID is a member of a Group or not.

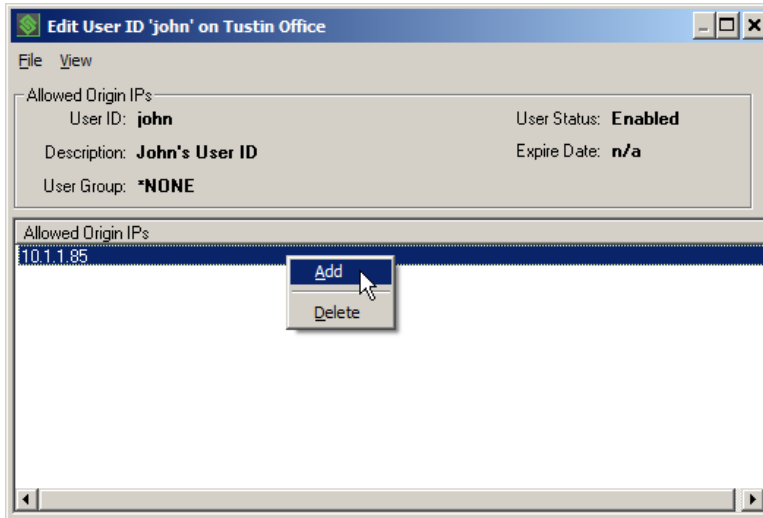
If the User ID is not a member of a group, then the menu options will include both *YES and *NO. If the User ID is a group member, then the menu options will include *GROUP and *YES and *NO. The permission that you select from the menu will be applied to all selected items in the list.



3.15.7 View and change the Allowed Origin IPs

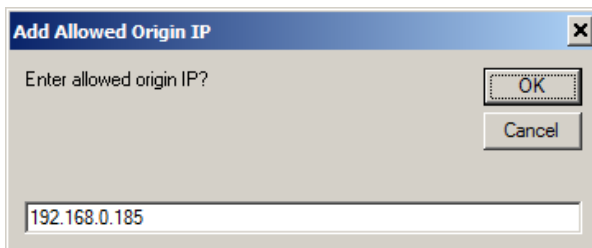
For each User ID, you can control which Administrator PCs can be used to manage the server. You can specify a list of Allowed Origin IPs for the Administrator PCs that can be used to manage the server and this User ID will only be able to sign on to the server from one of those PCs. If you do not specify one or more Allowed Origin IPs, then the user will not be restricted and can sign on from any Administrator PC.

To view and change the Allowed Origin IPs, select the 'Allowed Origin IPs' option from the 'View' menu. Clicking the right mouse button in a blank area or on a Origin IP will cause a small menu to appear with options you can perform.

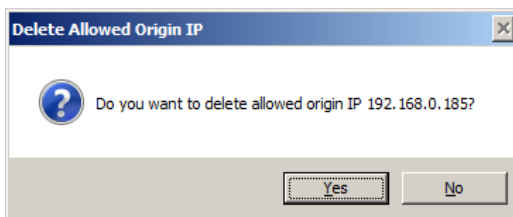


You can Add and Delete Allowed Origin IPs from the list.

Add – Select this menu option to add a new Allowed Origin IP for this User ID. You will be presented with a dialog into which you can type the Allowed Origin IP address:



Delete – Select this menu option to delete the currently selected Allowed Origin IP. You will be prompted to delete the Allowed Origin IP.



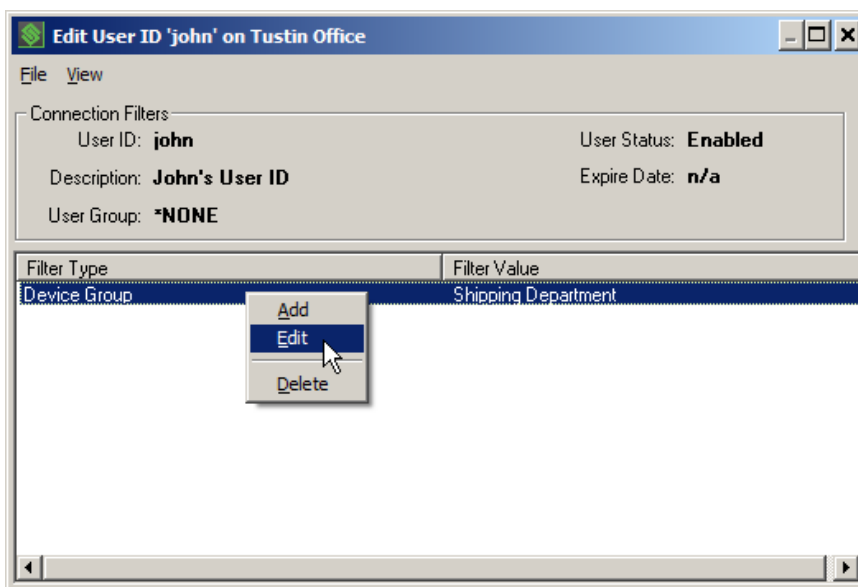
3.15.8 View and change the Connection Filters

For each User ID, you can control which connections can be viewed and managed from the Administrator Connections list. There are two types of Connection Filters that you can create to determine which connections will be visible in the Connection List and what management options will be available for those connections.

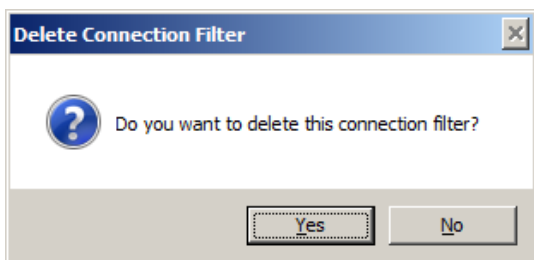
by Device Group – This connection filter type selects connections based upon the 'Device Group' to which the connection belongs.

by IP Range – This connection filter type selects connections based upon the device's local IP address being contained in the IP range defined for the connection filter.

To view and change the Connection Filters, select the 'Connection Filters' option from the 'View' menu. Clicking the right mouse button in a blank area or on a Connection Filter will cause a small menu to appear with options you can perform.

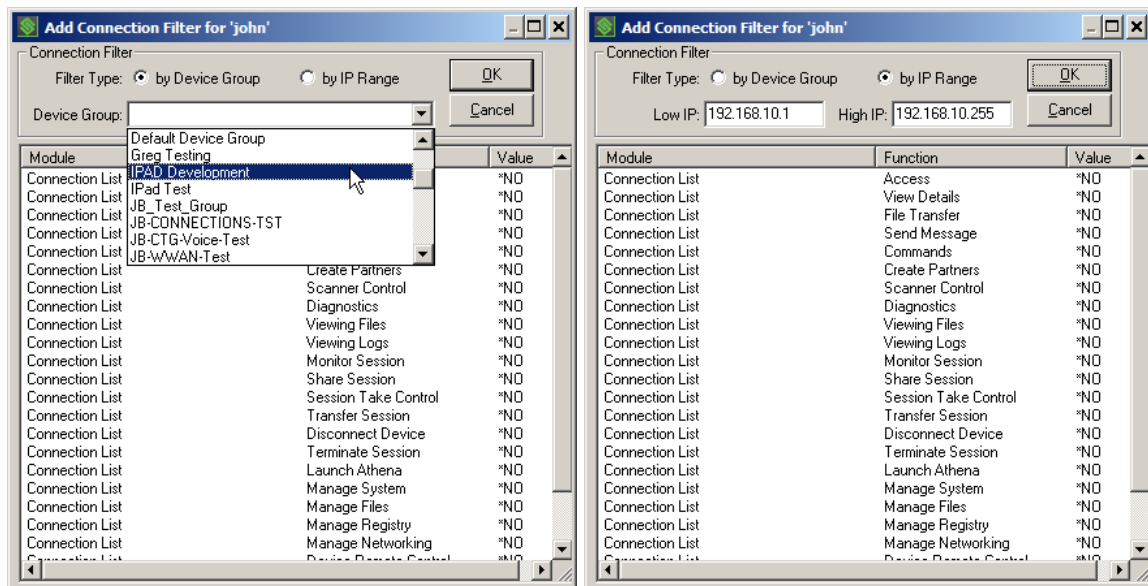


Delete – Select this menu option to delete the currently selected Connection Filter. You will be prompted to delete the Connection Filter.



Edit – Select this menu option to edit the currently selected Connection Filter. You will be presented with the Edit dialog where you can change the Filter Type if desired. You can also use this dialog to change permissions for the various connection list functions.

Add – Select this menu option to add a new Connection Filter for this User ID. You will be presented with a dialog into which you can configure the Connection Filter options:



On the Add Connection Filter dialog, you can select your desired Filter Type as either 'by Device Group' or 'by IP Range'. Depending upon your selection, the dialog will change to enable configuration of the Connection Filter for that Filter Type.

by Device Group – This option allows this User ID to access connections based upon the 'Device Group' to which the connection belongs. The dialog will provide a 'Device Group' drop-down list from which you can select the desired 'Device Group' for this connection filter.

by IP Address – This option allows this User ID to access connections based upon the device's local IP address being contained in the IP range defined for this connection filter. This dialog will provide a 'Low IP' and a 'High IP' text box where you can enter the desired IP Range for this connection filter.

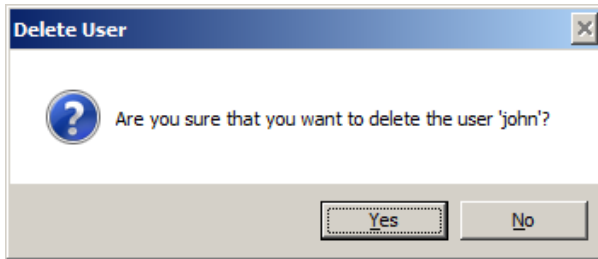
Changing Permissions – The permissions list will contain all of the possible functions that are available from the Connections List. You can set the permissions that this user has for the individual function by right-clicking on the item in the permissions list. A context-sensitive menu will appear with the available permissions for this selected item. Depending upon the current setting, the only possible menu option will be either *YES -or- *NO.

When setting permissions, you can select multiple items from the permissions list and apply your desired setting to all of them at once. If you use Ctrl-Click, then you can select multiple individual items from anywhere in the list. If you use Shift-Click, then you can select a contiguous block of items. Right-click on the selected items and a context menu will appear with the available permissions, both *YES and *NO. The permission that you select from the menu will be applied to all selected items in the list.

Select the 'Save Changes' option from the File menu to save your changes to this User ID.

3.15.9 Deleting a User ID

If you select the menu option to 'Delete' a User ID, you will be prompted to delete the User ID.



Click 'Yes' to delete the User ID from the system.

3.15.10 Enabling and Disabling a User ID

Each User ID will be in one of the three valid statuses, either 'Enabled', 'Disabled' or 'Expired'. Depending upon the User ID's current status, the menu will display either a 'Enable' option or a 'Disable' option.

If you select the 'Disable' menu option, then the User ID will be disabled and will not be available for use until you manually 'enable' the User ID.

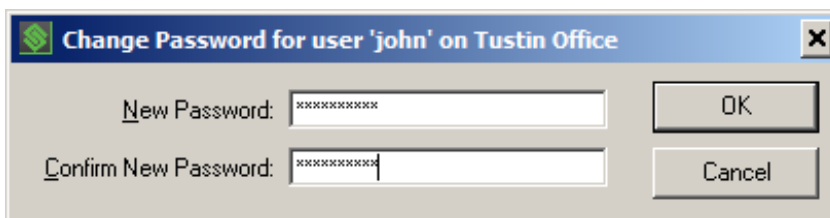
If you select the 'Enable' menu option, then the User ID will be enabled and if the User ID was expired, the 'password last changed' date will be reset so that the User ID is no longer expired.

3.15.11 Setting a User ID to Expired

You can use the 'Set to Expired' menu option to force a user to change their password the next time they successfully log on to the server. This is a common option to use after manually changing the password for a User ID. If the User ID has been disabled, then this menu option will not be available.

3.15.12 Changing the Password for a User ID

If you select the menu option to 'Change Password', you will be prompted for a New Password:

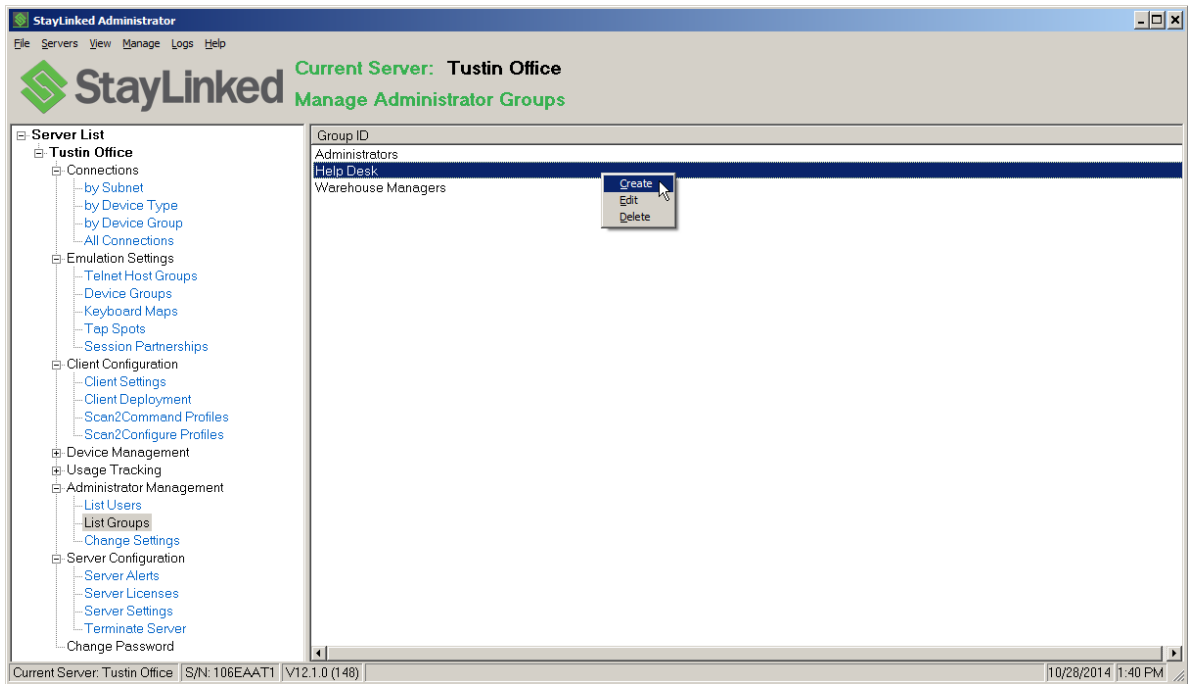


Type in the 'New Password' and then retype the password into the 'Confirm New Password'.

The password that you enter must validate against any password configuration settings that may be in effect on this server, like 'Minimum Password Length', 'Maximum Password Length' or 'Require Digits in Password'.

3.15.13 List Groups

When you select 'List Groups' from the server tree or the Manage menu, a list of Groups will appear in the main display panel. You can create Groups to help you manage pre-defined sets of permissions that can be adopted by selected User IDs.



Clicking the right mouse button in a blank area or on a Group will cause a small menu to appear with options you can perform.

3.15.14 Creating a Group

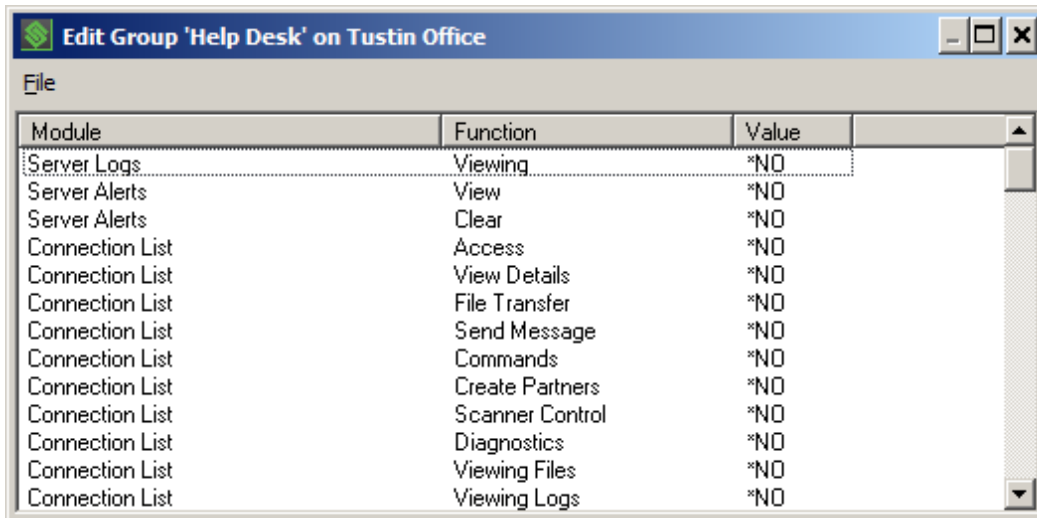
If you select the menu option to 'Create' a Group, you will be prompted for the name for the new Group.



The Group name is case-sensitive. You can enter any Group name that does not already exist on this server. The names 'Warehouse' and 'warehouse' are considered to be unique Group names and they can both exist on the server at the same time. Once the Group is created, it will appear in the Group List and you can then configure the permissions for the Group as desired.

3.15.15 Editing a Group

If you double-click on, or select the menu option to 'Edit', the selected Group, you will be presented with this dialog:



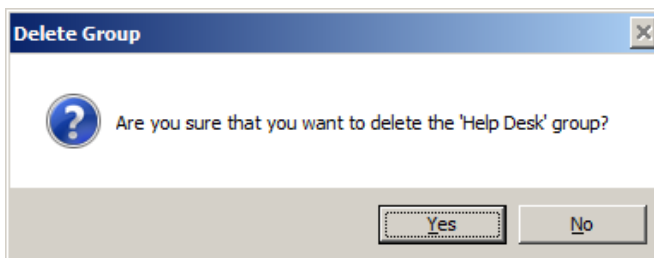
The Group Permissions List will contain all of the possible module functions that are available to be pre-configured for a Group. You can set the permissions that this Group has for the individual function by right-clicking on the item in the permissions list. A context-sensitive menu will appear with the available permissions for this selected item. Depending upon the current setting, the only possible menu option will be either *YES -or- *NO.

When setting permissions, you can select multiple items from the permissions list and apply your desired setting to all of them at once. If you use Ctrl-Click, then you can select multiple individual items from anywhere in the list. If you use Shift-Click, then you can select a contiguous block of items. Right-click on the selected items and a context menu will appear with the available permissions, both *YES and *NO. The permission that you select from the menu will be applied to all selected items in the list.

Select the 'Save Changes' option from the File menu to save your changes to this Group.

3.15.16 Deleting a Group

If you select the menu option to 'Delete' a Group, you will be prompted to delete the Group.

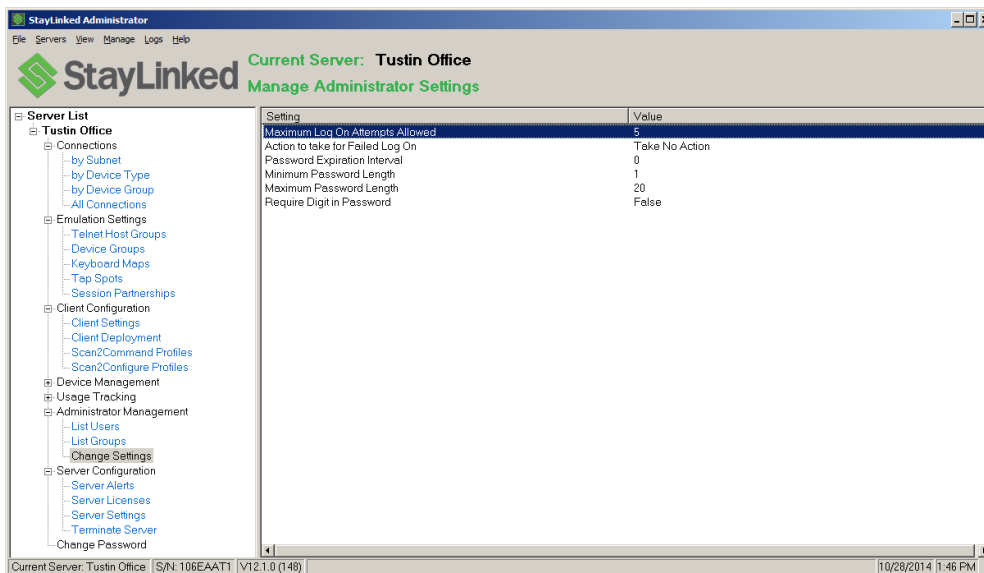


Click 'Yes' to delete the Group from the system.

If the Group is assigned to any User ID, you will not be allowed to delete the Group.

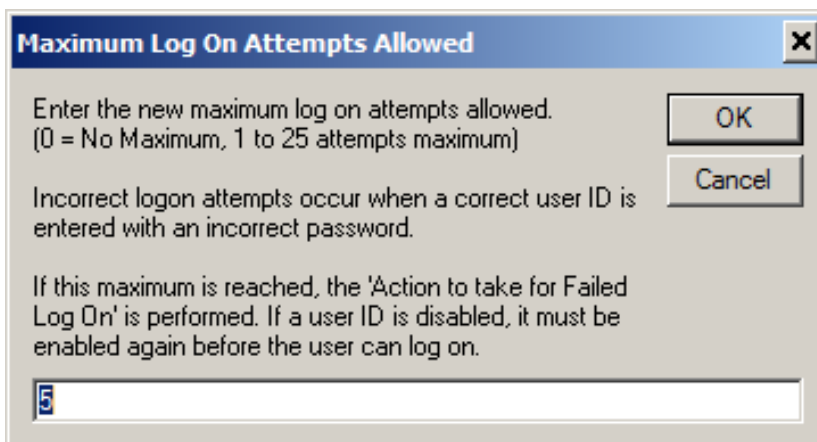
3.15.17 Change Settings

When you select 'Change Settings' from the server tree or the Manage menu, a list of Settings will appear in the main display panel. The various Settings can be configured to control the options available for Administrator Management features.



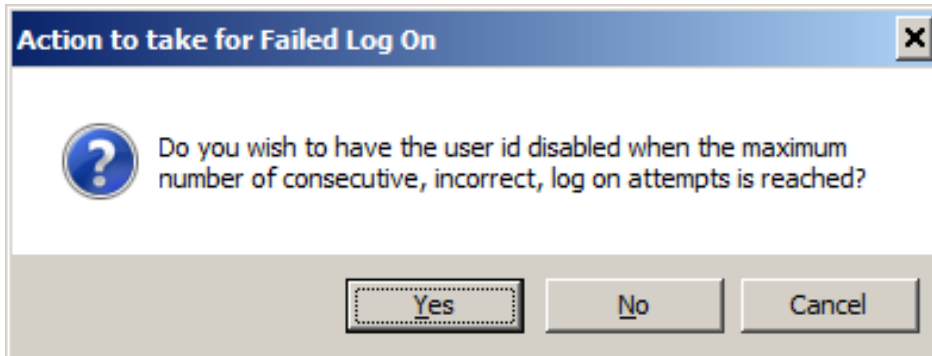
You must double-click on one of the settings in the list in order to make changes to that setting.

Maximum Log On Attempts Allowed: If you double-click on this option, you can define the maximum Log On attempts allowed before the system will perform the 'Action to take for Failed Log On' function.



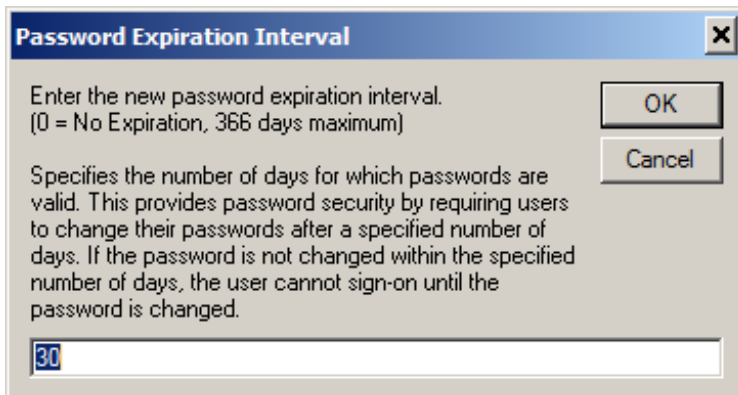
In this dialog, you can type a value from zero to 25. A value of zero (0) will specify that there is no maximum log on attempts defined and in this case, users will be able to retry their passwords indefinitely. If you set this value from 1 to 25, then users who fail to log on in that number of attempts will be subject to the 'Action to take for Failed Log On'.

Action to take for Failed Log On: If you double-click on this option, you can specify the action to take when a user fails to log on and exceeds the maximum log on attempts allowed.



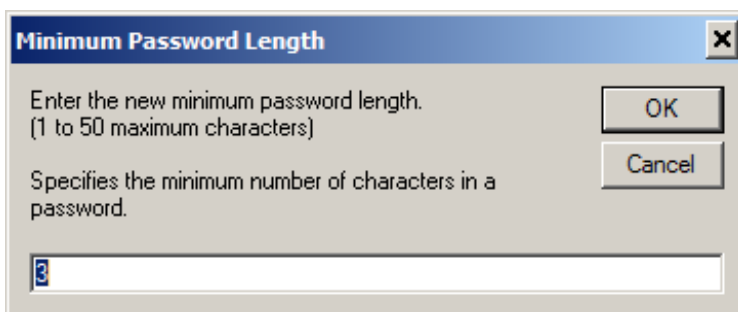
If you wish to have the User ID be disabled, click 'Yes'. If you wish to take no action, click 'No'. To leave the current setting, click 'Cancel'.

Password Expiration Interval: If you double-click on this option, you can specify the number of days for which passwords are valid. This provides password security by requiring users to change their passwords after a specified number of days. The user cannot sign-on until the password is changed.



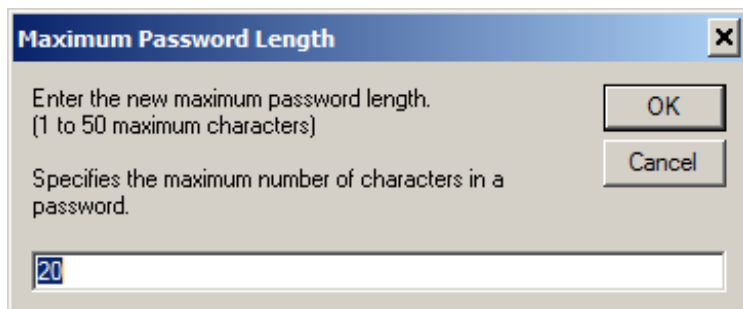
Enter the new password expiration interval. Enter zero (0) if you want the passwords to never expire. Enter a value of 1 to 366 days to cause passwords to expire after that number of days.

Minimum Password Length: If you double-click on this option, you can specify the minimum number of characters in a password.



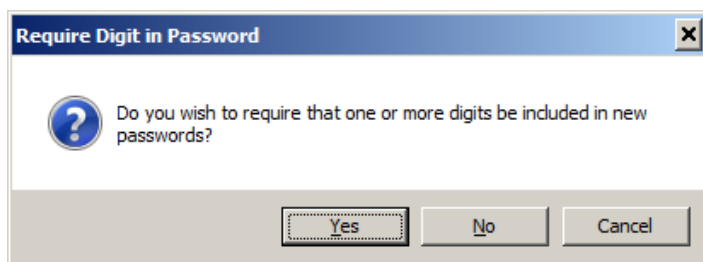
Enter a value between 1 and 50 and then press OK. To leave the current setting, press Cancel.

Maximum Password Length: If you double-click on this option, you can specify the maximum number of characters in a password.

A dialog box titled "Maximum Password Length" with a close button (X) in the top right corner. The main text reads: "Enter the new maximum password length. (1 to 50 maximum characters)". Below this, it says: "Specifies the maximum number of characters in a password." There are two buttons on the right: "OK" and "Cancel". At the bottom, there is a text input field containing the number "20".

Enter a value between 1 and 50 and then press OK. To leave the current setting, press Cancel.

Require Digit in Password: If you double-click on this option, you can specify whether one or more numeric digit be included in any new password.

A dialog box titled "Require Digit in Password" with a close button (X) in the top right corner. On the left is a question mark icon. The text reads: "Do you wish to require that one or more digits be included in new passwords?". At the bottom, there are three buttons: "Yes", "No", and "Cancel".

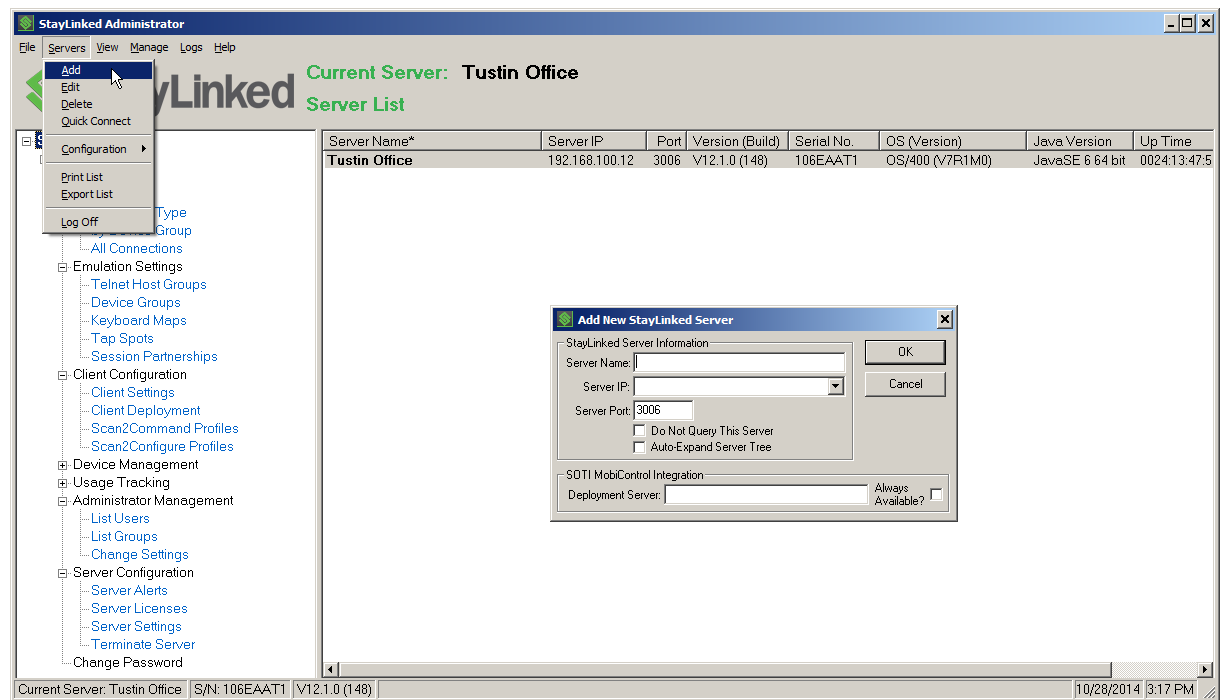
If you wish to require digits in passwords, click 'Yes'. If not, click 'No'. To leave the current setting, click 'Cancel'.

3.16 Server Administration

This section describes the various means provided to administer StayLinked servers. One or more servers can be defined for each instance of the administrator application. The level of access to the server is controlled by Administrator user IDs and passwords that are defined on each server.

3.16.1 Defining Servers to the Administrator

From the Servers menu, you can Add, Edit or Delete server definitions for this administrator (note: this has no effect on the server itself). You can 'Quick Connect' to a server temporarily. There is an option to Import or Export Server Configuration Files, Print or Export the Server List and you can also log on or log off of a server.



3.16.2 Logging On and Logging Off of a Server

Each time you start the Administrator, the list of defined servers will appear in the server tree. The first time you select a server from this list, you will be asked to log on to that server. You will enter your administrator user ID and password for the selected server and will be provided the level of access defined for that specific user ID on that server. The default user ID for each server is 'administrator' and the default password is 'esp'. The default 'administrator' user ID has full access to all of the functions of the StayLinked Administrator and Server.

You can log off of a server by clicking the right mouse button over the server name and selecting the Log Off option. You will need to log back on again if you want to perform any administration. You will also need to log back on to a server if the server has been restarted since the time you logged on or if you modify any server licensing.

Detailed information about Stay-Linked Administrator User Management can be found in Section 3.15 of this guide.

3.16.3 Quick Connect to a server

In an Enterprise environment, you might be charged with managing dozens or even hundreds of StayLinked Servers distributed across your wide-area network. You could add each server to the administrator where they will be always available for selection. Or, you can simply 'Quick Connect' to a server when needed and the server will remain in the servers list until you exit the StayLinked Administrator. When you restart the Administrator, that server will no longer be in the list.

3.16.4 Export and Import the Server Configuration

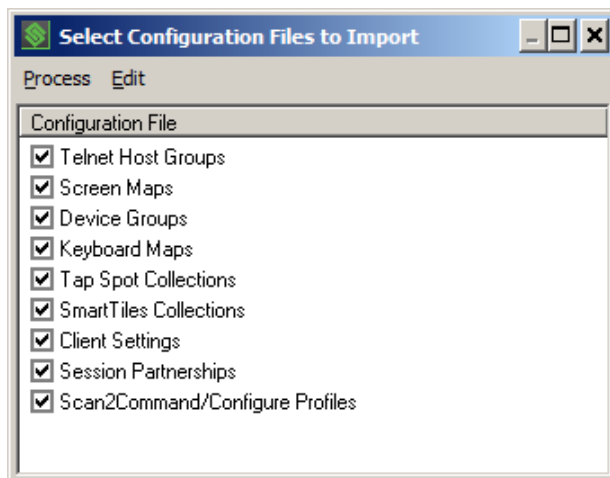
You may wish to manually backup your StayLinked Server configuration or transfer the configuration to another machine running the StayLinked Server. Using the 'Configuration->Export' and 'Configuration->Import' menu options, you can perform these functions. If your Administrator user account is allowed to edit 'Server Settings', then these menu options will be available.

Export Server Configuration

When you select to export the server configuration, you will be prompted for a location to save the 'StayLinked Configuration (.slc)' file that has a default file name that matches the server name. The export function will create an SLC file at this location that contains the configuration files for 'Telnet Host Groups', 'Device Groups', 'Keyboard Maps', 'Tap Spots', 'Client Settings', 'Session Partnerships' and 'Scan2Command/Configure Profiles' exported from the current StayLinked server.

Import Server Configuration

When you select to import the server configuration, you will be prompted for the location of the 'StayLinked Configuration (.slc)' file that you wish to import into the current StayLinked server. Once you select a valid SLC file, you will be presented with an 'Import' dialog that will allow you to select one or more of the various configuration files that are contained in the "StayLinked Configuration (.slc)" file:



Using this dialog, you may select/deselect the configuration files that you wish to import into the current selected StayLinked Server. Once you have selected the desired configuration files for import, select the 'Process->Import' menu option and you will be prompted to confirm that you wish to proceed with the import of the selected configuration files. Then, a final confirmation will be offered to ensure that you wish to alter the configuration of the current StayLinked Server by importing the selected configuration files into that server. If you are absolutely sure that you wish to proceed with the import, click the 'Yes' button. After the selected configuration files have been imported into the current StayLinked Server, any new StayLinked Sessions started on this server will be using the newly imported configuration files.

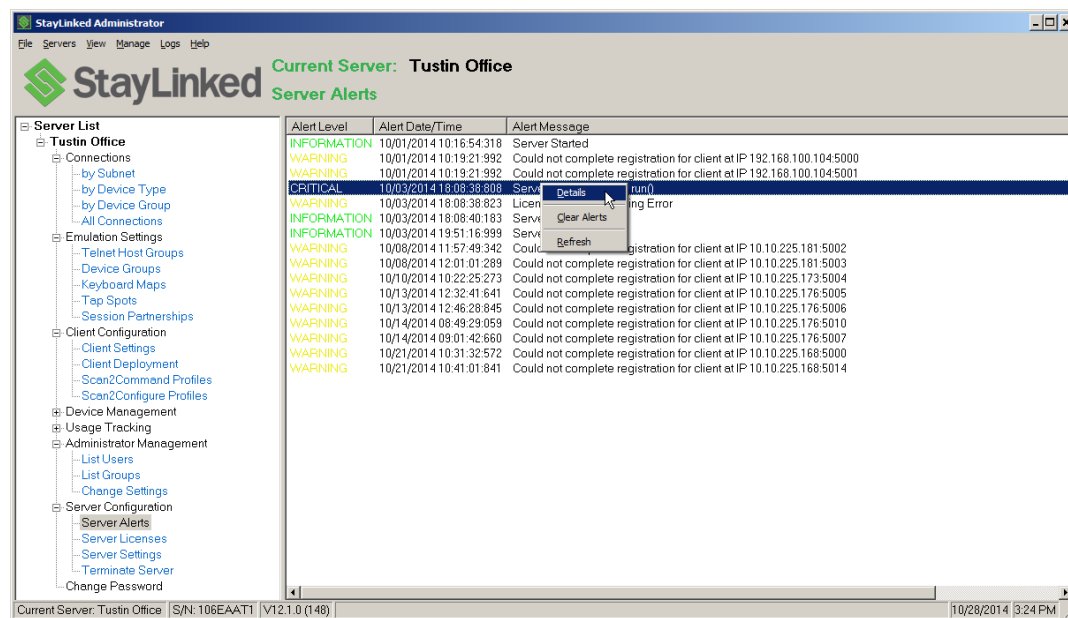
3.16.5 Printing and Exporting the Server List

Print List – This menu option will send the list of connected devices to a report on your current Windows default printer. The report will include columns for Device Type, Device Name, MAC Address, IP Address, Client Version and User/Device ID.

Export List – This menu option will export the list of connected devices to a 'Comma Separated Variable' (.csv) file of your choice. The export will include all of the connections and columns that are displayed in the Connections List. This format is appropriate for import into common spreadsheets and databases.

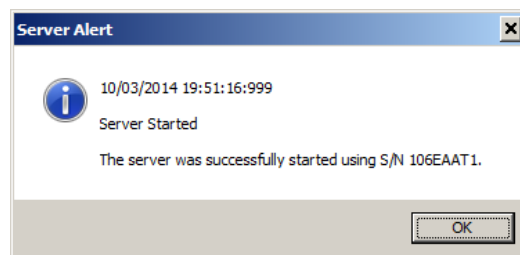
3.16.6 Viewing Server Alerts

The StayLinked Server records information regarding server status and important events that occur during server operation. When you select 'Server Alerts' from the server tree or the Manage menu, the Server Alerts list will appear in the main display panel.



The Server Alerts are classified as one of three levels, Information, Warning and Critical. Each Alert records the Alert Level, Alert Date/Time and the Alert Message. You may view more details of a selected alert by double-clicking or selecting the Alerts-Details menu option. The Details will usually recommend actions that can be taken to resolve Warning or Critical alert conditions. Clicking the right mouse button over an alert line will cause a small menu to appear with the following options:

Details: This menu option displays the details of the selected alert item.



Clear Alerts: Select this option to clear the Server Alert Log that is stored on the server.

Refresh: This menu option reloads the Server Alert listing with the most recent alerts.

3.16.7 Managing Server Licenses

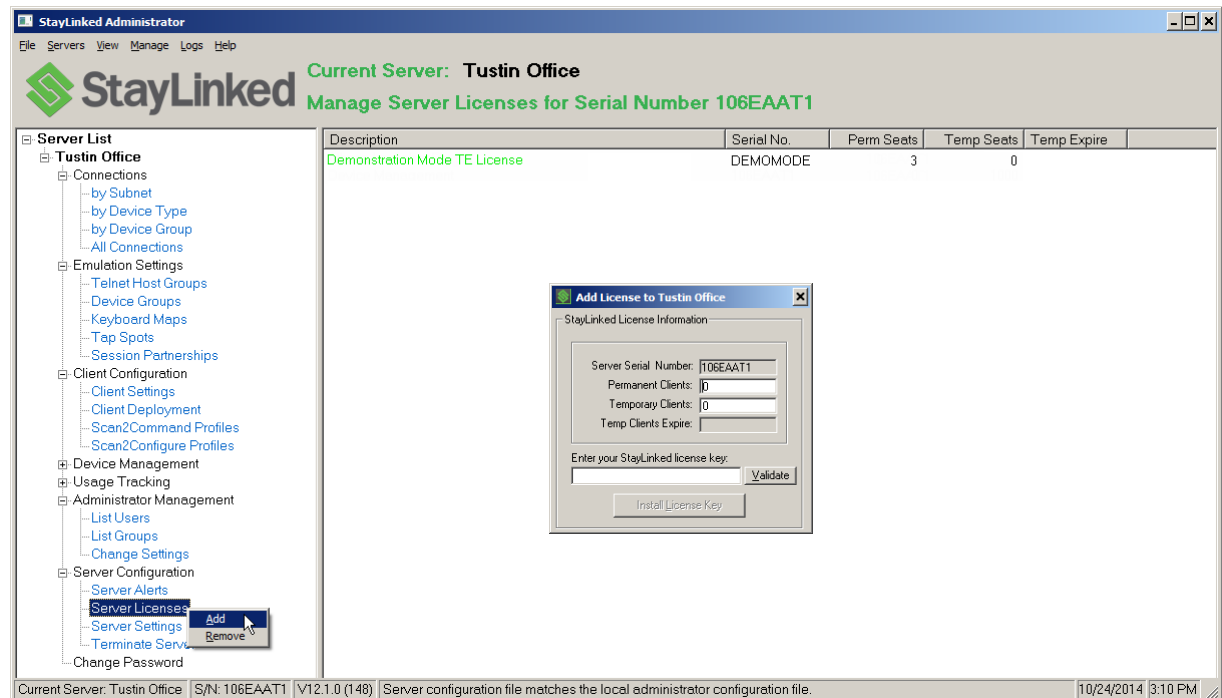
At least one license must be installed before any clients will be able to start sessions on the StayLinked Server. The StayLinked Server is pre-loaded with a 'Demo Mode' license key. This Demo Mode license should be removed if the server will be used with Pre-Licensed devices.

When you select 'Server Licenses' from the server tree or the Manage menu, a list of server licenses will appear in the main display panel, showing the type of key, serial number and number of permanent and temporary seats.

Any installed temporary license keys that are about to expire will trigger a warning dialog prompting the user to contact StayLinked Technical Support to acquire an extension or a permanent license. This list is color-coded with Green signifying active keys and Red signifying inactive, invalid or expired keys.

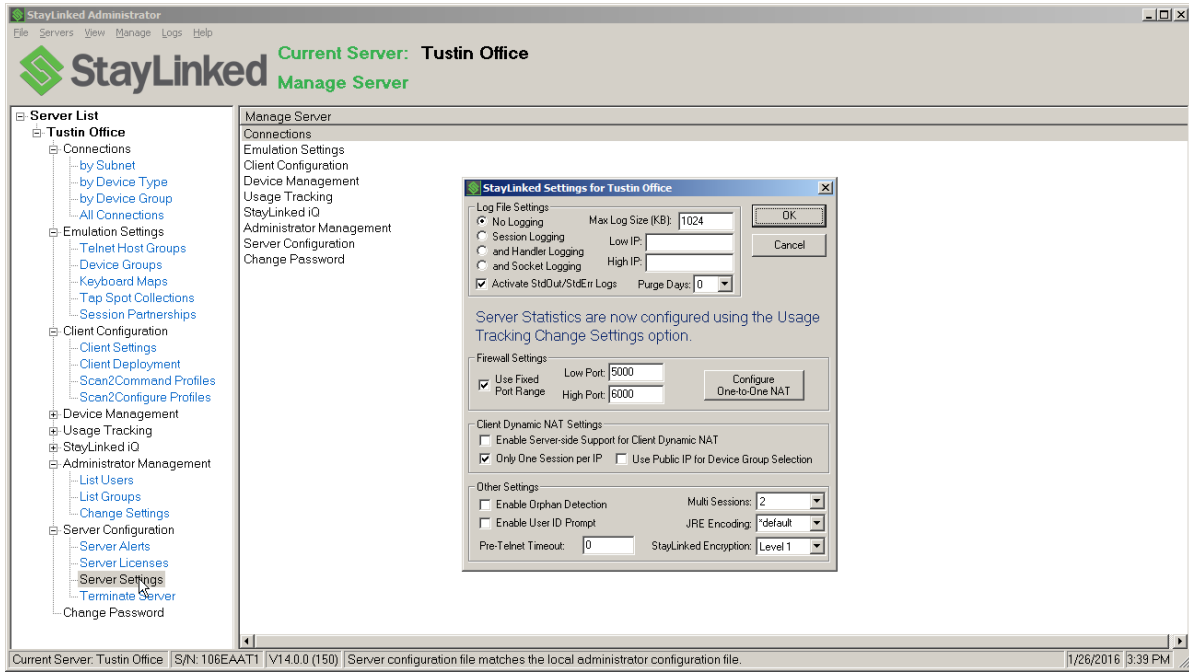
Right mouse click the Server Licenses function or anywhere on the main display panel when the list is shown to display a small menu. From this menu, you can add a new key, remove an existing key or view license key details. If you select the Remove option, you will be prompted to confirm. If you select the Add option, the Add License window will appear. Using the license information provided to you, enter the Permanent Clients Quantity, the Temporary Clients Quantity and then cut and paste the License Key into the field provided. Click 'Validate' and the dialog will be updated to show your license information. Click 'Install License Key' button to complete the procedure. If the license is successfully installed, then it will be added to the list of licenses for the current server. When a new key is installed, you will be automatically logged off the current server and then be required to logon again.

A new key for the same product will overwrite an existing key, so it is not necessary to remove the existing key first. In fact, the new key can be entered at any time, and will take immediately take effect on the server (without having to stop and re-start the server).



3.16.8 Configuring Server Settings

When you select Server Settings from the server tree, the Manage Server list or the Manage menu, a window will appear that shows the current server settings and allows you to make changes.



Log File Settings: These options are used to control the server logs. The server logs are used by technical support to analyze connectivity issues. This option should be set to 'No Logging' unless otherwise directed by technical support. The Max Log Size value controls the size of the log files. If desired, you can control the devices that generate logs by specifying a low and high IP range. You can disable collection of StdOut and StdErr Java Log files by unchecking the 'Activate StdOut/StdErr Logs' checkbox option. You can configure 'Purge Days' to have old logs purged after they have aged by some number of days that you can choose.

Server Statistics Settings: These options have been moved to the 'Usage Tracking' feature set. More information on server statistics logging can be found in the Technical Reference, Server Statistics Guide.

Firewall Settings: If your devices are connecting to the StayLinked server through a firewall, then you may need to restrict the ports that are assigned to devices and configure a server that is running behind one-to-one NAT.

Use Fixed Port Range: You may enable this option and then specify a range of ports that the server should use for device connections. You will need to ensure that you specify a range that is large enough to accommodate the number of licenses that you are running. When there are no further open ports available, then devices will no longer be able to connect to the server.

Configure One-to-One NAT: If your server is behind One-to-One NAT (Static NAT), then you will need to use the 'Configure One-to-One NAT' dialog to specify the server's mapped external IP and its physical internal IP address.

Client Dynamic NAT Settings: If your devices are running Dynamic NAT behind a NAT Server, then you can configure the StayLinked Server to support this network architecture.

Enable Server-Side Support for Client Dynamic NAT: Select this option to have the StayLinked Server identify and handle 'port re-assignment' events. These events are generated by the NAT server when the port assignment cross-reference times-out due to inactivity. Typically, additional traffic from the device will be re-assigned to a different port by the NAT server. This setting will allow the server to identify these port re-assignments and handle them

appropriately.

Use Public IP for Device Group Selection: This option only applies when the 'Server-side Support for Client Dynamic NAT' option is enabled. This option will cause the 'Public IP' of the NAT Server to be used for selecting Device Groups, rather than using the private, internal IP of the device itself.

One Session per IP: This option determines how existing sessions are handled when a device connects to the server. Check this option to ensure that each device consumes only one session. This option prevents duplicate sessions for a single IP. This option only applies to devices running against single session licenses. This option is automatically disabled and locked when the 'Server-side Support for Client Dynamic NAT' option is enabled.

Enable Orphan Detection: Check this option to enable the server to identify devices that have lost their 'Session ID' values. The server will then detect and reconnect devices to any session that has been orphaned for that device based upon MAC address only. This setting will typically apply to devices that store their 'Session ID' values in volatile memory on the device where it can easily be lost if the battery is removed for too long, or if the battery is exhausted. This setting is only available if the server is running 'single session' licensing only and is not running any 'multi session' licenses.

Enable User ID Prompt: This option will enable the collection of User Identification information for each device. The User ID Prompt can be used to assist with Asset Management or for other purposes. When a device creates a new connection, you will be prompted to enter an User ID value that will be visible on the Connection List, recorded in the Device Identification Log file and recorded in the Usage Tracking database if User ID tracking is enabled. The value entered by the user can be accessed in subsequent scripting and substitution using the special [userid] mnemonic value.

Pre-Telnet Timeout: Enter the number of seconds of inactivity, prior to starting a telnet session, before terminating the connection. This timeout will work when the user is on the 'User ID Prompt', waiting to enter SSH credentials or sitting on a 'Select a Host' menu.

Multi Sessions: This drop-down list provides for the configuration of the number of sessions that will be allowed per device when the server is licensed for Multi Session TE. The valid values are from 2 sessions to 10 sessions per device. This option will not be available if you do not have a Multi Session TE License installed on the server. The default value for this setting is 2 sessions.

JRE Encoding: This is a legacy setting that will only affect Servers prior to version 10. This setting selects the code page for Java string encoding used by the server. Generally, this value should be set to '*default'. This value may need to be set to match the code page of the machine upon which the server is running. If running servers older than Version 10, and the session screens on the devices are not displaying the expected characters, then you might need to adjust this value. For instance, in order to properly render VT line-draw characters, we recommend setting this value to 'cp437'. For servers running Version 10 and newer, you can get VT line-draw support by running your Telnet Host Entry with 'VT-UTF8' terminal emulation.

Encryption: Select whether to enable encryption for all StayLinked sessions:

None – No StayLinked packets will be encrypted.

Level 1 – StayLinked data transferred between the Stay-linked Thin Client and the StayLinked Server will be encoded using a proprietary 64-bit encryption scheme.

Blowfish – StayLinked data transferred between the Stay-linked Thin Client and the Server will be encoded using the Blowfish/CBC/PKCS5Padding encryption algorithm.

(See Secure Communications Guide for details about Encrypted connections)

Using Blowfish Encryption: Blowfish encryption provides a very high level of data security for the StayLinked packets that are transmitted between the StayLinked Thin Client and the StayLinked Server. StayLinked Blowfish encryption is available only for PPC/WM/CE/CE.Net devices that are running a StayLinked Client of at least Version 9.1.0. Blowfish encryption is not available for any DOS devices. When you select 'Blowfish' as the StayLinked Encryption option, you are presented with the following dialog:

StayLinked Settings for Tustin Office

Log File Settings

☒ No Logging Max Log Size (KB): 1024

☐ Session Logging Low IP:

☐ and Handler Logging High IP:

☐ and Socket Logging Purge Days: 0

☒ Activate StdOut/StdErr Logs

OK Cancel

Server Statistics are now configured using the Usage Tracking Change Settings option.

Firewall Settings

☒ Use Fixed Port Range Low Port: 5000 High Port: 6000

Configure One-to-One NAT

Client Dynamic NAT Settings

☐ Enable Server-side Support for Client Dynamic NAT

☒ Only One Session per IP ☐ Use Public IP for Device Group Selection

Other Settings

☐ Enable Orphan Detection Multi Sessions: 10

☐ Enable User ID Prompt JRE Encoding: 8859_1

Pre-Telnet Timeout: 0 StayLinked Encryption: Blowfish

Blowfish Encryption Settings

Key 1:

Key 2:

Key 3:

Key 4:

☒ Allow Unencrypted Sessions Key Rotation Interval (mins): 10

Key 1, Key 2, Key 3 and Key 4: You may specify one to four blowfish keys. Each key can be from 8 characters to 56 characters in length. The keys are case sensitive. The Encryption capabilities of the Java Runtime used by the server will determine the maximum key length that can be used. If the Java Runtime does not support a key of the length that you have entered, that key will be automatically trimmed until it can be used. The server will only use Key 1 unless you specify a 'Key Rotation Interval'.

Allow Unencrypted Sessions: This option will determine whether sessions will be allowed for clients that do not support Blowfish encryption. If you have a mix of DOS and PPC devices and you want them all to be able to run sessions, and you want to use Blowfish encryption for the PPC devices, then you must check this option to allow the unencrypted sessions from the DOS devices. In this case, the DOS devices will utilize the 'Level 1' encryption instead of the Blowfish encryption. If you want to restrict your server to allow sessions only for devices that support Blowfish encryption, then uncheck this option. In this case, any unsupported device that tries to start a session will get a 'Device Not Allowed' message displayed when a session is started. Those devices that do not support Blowfish encryption will not be able to run any sessions.

Key Rotation Interval (mins): If you enter more than one Blowfish key, then you may have the StayLinked Server automatically rotate between those keys at your specified interval in minutes. The valid range for the Key Rotation Interval is 5 minutes to 1440 minutes. The StayLinked Client and Server will automatically rotate between keys at each rotation interval during the entire duration of the StayLinked session.

3.16.9 Terminating a Running StayLinked Server

The Terminate Server option is used to disconnect all client sessions and terminate the server jobs. On the IBM i platform, the server subsystem is not terminated by this command, but all subsystem jobs are terminated. All client sessions will be sent a terminate message. Those devices that are asleep at this moment will not receive the terminate message. Upon waking, these devices will go to a [Session Ended] state if the StayLinked Server is running or they will go into a [Linking] state if the StayLinked Server is not running.

When you select Terminate Server from the server tree or the Manage menu, you will be prompted for, and must enter your password in order to terminate the server.

4 Appendix – Special Scripting Mnemonics

Here are some scripting mnemonics that are available for special use:

[devicename] – This script mnemonic is used to substitute the device name into the script.

[deviceip] – This script mnemonic is used to substitute the device IP into the script.

[devicemac] – This script mnemonic is used to substitute the device MAC address into the script.

[hex #####] – This script mnemonic is used to substitute Hexadecimal values into the script.

[uni #####] – This script mnemonic is used to substitute Unicode values into the script.

[var ##] – This script mnemonic is used to substitute 'User Defined Variables' into the script.

[delay] – This script mnemonic is used to insert a 1/10 second delay into the startup script.

[long_delay] – This script mnemonic is used to insert a 1 second delay into the startup script.

[userid] – This script mnemonic is used to insert 'device identifier' value into the startup script.

[deviceid] – This script mnemonic is used to insert the PPC/CE.Net Device Name into the script. For all Version 9.1 clients, you can specify a 'Device ID' value in the StayLinked Client's configuration dialog. Or, you can use 'Client Settings' to assign a 'Device ID' value to individual devices. For older PPC/CE clients, you can specify the 'Device ID' in the operating system configuration. For CE.Net devices, this value is configured at the 'Start – Settings - Control Panel - System - Device Name Tab – Device Name' dialog. For PPC devices, this value is configured at the 'Start – Settings – System Tab – About – Device ID Tab – Device Name' dialog. For DOS devices, this value is managed using the Device Settings file (STAYLINK.INI) and the 'device_id' setting.

[devicetype] – This script mnemonic is used to insert the StayLinked Client Device Type value into the script.

[encrypt #,%%] – This scripting mnemonic is used to cause scripted text to be encrypted in the configuration files. There are two arguments provided to this mnemonic, the first is a unique sequence number and the second is the text to be encrypted. An example would be the use of a 5250 logon sequence in a 'Startup Script'. In this case, your script for logon could be entered like this:

```
[encrypt 1,myuserid][fldext][encrypt 2,mypassword][enter]
```

The text enclosed in the [encrypt #,%%] mnemonic will be stored in the configuration files in an encrypted format and will no longer be displayed in clear text in the Administrator user interface.

[cursor row#, col#] – This script mnemonic is used to move the current telnet cursor location to a specific row and column. This scripting mnemonic is used for both VOICE input processing and for Screen Reformatting input processing.

[inputloc row#, col#] – This script mnemonic is used to the next user input to be targeted to a specific row and column. This scripting mnemonic is used for Screen Reformatting input processing.

[wait] – This script mnemonic is used for VT emulation to cause the processing to wait for the next telnet screen presentation event to occur before continuing with further script processing.

[send] – This script mnemonic is used for VT emulation to force the current script segment to be sent to the host immediately.

Scripting Mnemonic Examples:

The mnemonic [hex 0D] will insert an ASCII CR (Carriage Return) into the script.

If you need to include any square brackets in your script, you should include two of them.

The mnemonic [hex 1B5B32347E] is the equivalent of 'ESC[24~' or the VT F12 key.

This script '[hex 1B][[24~' is also the equivalent of 'ESC[24~' or the VT F12 key.

These special scripting mnemonics are available for the following StayLinked Features:**VT Telnet Host Property – ANSWER BACK MESSAGE**

[devicename], [deviceip], [devicemac], [hex ##], [uni #####], [userid], [deviceid], [devicetype]

Telnet Host and Device Group Startup Scripts

[devicename], [deviceip], [devicemac], [hex ##], [uni #####], [var ##], [delay], [long_delay], [userid], [deviceid], [devicetype], [encrypt #,%%]

Keyboard Mappings

[devicename], [deviceip], [devicemac], [hex ##], [uni #####], [var ##], [userid], [deviceid], [devicetype], [encrypt #,%%], [screen_map]

Tap Spot Collections

[devicename], [deviceip], [devicemac], [hex ##], [uni #####], [var ##], [userid], [deviceid], [devicetype], [screen_map]

Barcode Prefix and Suffix, Printing Completion and Cancellation Actions

[hex ##], [uni #####], [var ##], [delay]

5250 Device Name Prefix (Device Groups)

NULL, [deviceid]

VOICE input commands

[cursor row#, col#]

Screen Recognition Auto-Responses

[devicename], [deviceip], [devicemac], [hex ##], [uni #####], [userid], [deviceid], [devicetype], [encrypt #,%%], [wait], [send]

Screen Recognition and Reformatting Regular Expression Input Modifiers

[cursor row#, col#], [inputloc row#, col#]

5 Appendix – Troubleshooting

The following server error messages may appear on the device screen after connecting to the StayLinked server. Most of these errors refer to StayLinked Server or host configuration issues.

eSP Error ID:	Error Message Text	Possible Causes and Solutions
eSP0001	No Hosts Defined	No Host defined in the StayLinked Administrator. Use the StayLinked Administrator to define Telnet hosts.
eSP0002	Host Not Responding	Bad Host address or port. Confirm the Host address and Telnet port information in the Telnet Host configuration. Host might be unreachable on the network. Confirm that the Telnet Host is currently available on the network.
eSP0003	No Keymap Found	The Device Type is not cross referenced to a keyboard map for this Host Emulation. Use the StayLinked Administrator to add a keyboard map for this Device Type and Host Emulation combination. Possible unknown Device Type.
eSP0004	Bad License Key Authentication Error Admin. Config. Error No TE Seats Available No Multi Seats Remain	Use the StayLinked Administrator to review the license information. Does the key refer to the correct Server Serial Number? For IBM i Platforms, the STAYLINKED user profile might be disabled or have no password. Review the STAYLINKED user profile.
eSP0005	WSID Not Available	The 5250 session is unable to allocate the specific device description. The device description on the IBM I does not exist or is not varied on. Or, the device description has no interactive subsystem in which to run.
eSP0006	Device Not Allowed Device Group Is Full Blowfish Required	The device is assigned to a Device Group that is set to not allow connections or has a maximum session limit defined. See 'Manage Device Groups'. The server is configured to require Blowfish Encryption and the StayLinked Client does not support that encryption. See 'Server Settings'.
eSP0007	Client Not Compatible	The old eSP-Link Client installed on the device is not compatible with the new StayLinked Server. Please upgrade the Client software on the device to the latest StayLinked build, which is available on the http://www.stay-linked.com web site.
eSP0008	Could not get device config.	The server was unable to communicate with the device to retrieve the device configuration. Probable network traffic problems. Simply re-attempt the connection.
eSP0009	Multi Sessions Denied	The device is a member of a Device Group that does not allow multi sessions. Review the device group settings for this device.

eSP0010	Unable to connect to Shared Session.	The server was unable to connect to the shared session. Simply re-attempt the connection.
eSP0011	Various SSH Errors	Bad SSH User/Password SSH Password Expired Unsupported Authentication SSH Disconnected
eSP0012	SSH Not Supported	SSH Support for StayLinked requires at least Java JRE 1.4.2-06 and the latest StayLinked Support JAR files.
eSP0013	SSH Logon Cancelled	The user cancelled the SSH logon prompt screens.
eSP0014	Various SSL Errors	Server Cert. Not Trusted Client Cert. Not Provided Client Cert. Not Found Client Cert. Bad Password
eSP0015	Device Not DM Capable	The device is not capable of running a DM Only session. You must install the StayLinked Device Management Components onto the device to make it capable.

6 *Contact Information*

For further information or technical assistance, please contact your StayLinked Certified Partner or our technical support team.



13700 Alton Parkway
Suite 160
Irvine, CA 92618
714.918.7700

<http://www.StayLinked.com/>