ThinManual
11

Version 1 — January 15, 2019

ThinManager - A Rockwell Automation Technology | 1220 Old Alpharetta Road, Suite 390 | Alpharetta, GA 30005 | USA

Table of Contents

This manual is a condensed guide to understanding and configuring ThinManager.

Selecting the F1 button while in the program will launch a context-sensitive help document within the ThinManager program.

ThinManager® with Relevance® is explained in greater detail in the **ThinManager User Guide** found at http://www.thinmanager.com/support/manuals/

1. Terminology

These terms are used in this document:

Terminal is the all-inclusive term for clients that connect to a server.

Thin client is a terminal without a hard drive

Fat client is a terminal with a hard drive.

Terminal Server is the all-inclusive term for a computer that acts like a mainframe, allowing clients to log in, start sessions, and run apps on the server but display the results on a terminal.

Remote Desktop Server is a 2008 R2 or 2012 terminal server.

ThinManager Server is a computer running the ThinManager interface and the ThinServer service.

ThinManager - ThinManager is the graphic user interface component of the ThinManager system. It is the interface that is used to control and configure the ThinServer database.

ThinServer is a database engine that contains the ThinManager configuration. It runs as a Windows service. ThinManager hardware will communicate with this service in order to receive their firmware, configuration, and to get information related to their Relevance setup.

Relevance – Relevance is a function of ThinManager that controls access to applications and assets through Location or User Permissions.

Access Group – An Access Group provides the Relevance permissions that control access to a location, application or function.

Content - Content describes the data, sessions, or information that is being delivered to a thin client, terminal, or mobile device. It could be an HMI, a document, access to a full desktop, a camera image, or a shadow of another client. Content is deployed as Display Clients

Fencing - Fencing is a Location hierarchy. Fencing has a resolver at a top level location that must be resolved before using a resolver of a lower level. This provides an additional security layer to restrict access to a location.

Location - A Location is a configured element that can is used as an end point for content deployment. It can contain Display Clients for content, be assigned a Windows user account, contain Resolver Actions, and be assigned to a terminal. An individual Location is configured in a manner similar to Terminals and TermSecure users in ThinManager.

Mobile Device - Mobile devices are Apple, Android, or Windows devices that have the appropriate ACP ThinManager application installed and configured. They can interact with the ThinManager Platform through Relevance.

Resolver - A Resolver is an item that the mobile device uses to identify a particular area. Specific types of resolvers include QR codes, Bluetooth beacons, iBeacons, GPS, and Wi-Fi access points.

Relevance ID - A Relevance ID specifies a unique Resolver. When a new Resolver device is added to the system, it is assigned a unique ID and name in the system.

Resolver Actions - These are the functions that are authorized on a mobile device by a resolver. These actions include Shadow, Transfer, Forced Transfer, and Clone.

TermSecure – TermSecure is the former name for the security component of ThinManager whose functionality has been expanded in Relevance. It grants or denies access to content.

Installation ID – An identifier used in licensing. It is found at the bottom of the Licensing window that is launched by selecting *Install>Licenses*.

2. Setup Overview

Microsoft

- ❑ Build a terminal server with the Microsoft Windows Server 2008/2008R2 or Server 2012/2016 operating system. Enable the Remote Desktop Server (Terminal Services) role. See Section 3.2 on page 9.
- ❑ Create a Microsoft Licensing Server and add a RDS CALs (Remote Desktop Services CALs for each thin client. These are called Terminal Server Client Access License, or TS CAL, in Server 2003.
  The servers also require a normal CAL. See Section 3.4 on page 12.
- ❑ Create a Microsoft user profile for each terminal on the terminal server. Make sure that the user is a member of the Remote Desktop Users Windows group. See Section 3.5 on page 13.
- ❑ Apply appropriate security to each user profile using the standard Microsoft techniques.

ThinManager Installation & Activation

- ❑ Install the ThinManager software onto a computer to create a ThinManager Server. See Section 6.2 on page 16.
- ❑ If using ThinManager Master Licensing:
  - o Create a Master ThinManager License and add enough Product Licenses for each ThinManager-managed Terminal. See Section 7 on page 18.
- ❑ If using FactoryTalk Activation:
  - o Install the FactoryTalk Activation Manager on each computer where ThinManager is installed.
  - o Download the FactoryTalk Activations for ThinManager.
  - o Change the License Mode in ThinManager to FactoryTalk Activation and assign the newly downloaded activations. See Section 7.3 on page 22.

ThinManager Configuration

- ❑ Define the Terminal Servers using the Display Servers > Remote Desktop Servers > Remote Desktop Server Wizard. See Section 9.1 on page 23.
- ❑ Define the Display Clients using the Display Clients > Terminal Services > Display Client Wizard to deploy the applications. See Section 10 on page 24.
- ❑ Define the Terminals using the Terminal > Terminal Configuration Wizard. See Section 11 on page 28.
- ❑ Associate the hardware to the terminal configuration. See Section 12 on page 29.

Network

Thin clients and Remote Desktop Servers need a reliable network.

Make sure that the following network ports are unblocked in all software and hardware firewalls:

- ❑ **UDP/4900** - TFTP - Used for the TFTP download of the firmware.
- ❑ **TCP/2031** - Configuration - Used to pass the configuration from the ThinManager Server to the ThinManager thin clients.
- ❑ **UDP/67** – IP Address Assignment – Used by the PXE Server (if using PXE boot).
- ❑ **UDP/69** – TFTP – Used by the PXE Server (if using PXE boot).

- ❑ **UDP/4011** – UEFI Boot – Used when the DHCP server is on the ThinManager server or when using the Unified Extensible Firmware Interface (UEFI) BIOS to boot.
- ❑ **TCP/1494** - Citrix - Used by the ICA protocol (if using ICA instead of RDP).
- ❑ **TCP/3389** - RDP - Used by the RDP protocol (if using RDP in v2.4.1 or later).
- ❑ **TCP/5900** - Shadowing - Used to shadow Terminals. This can be changed on the Shadow Configuration page of the ThinManager Server Configuration Wizard.
- ❑ **UDP/1758** – Used if the default Multicast is used. If the network MTU size is not the default then the packet size needs changed on the Multicast Configuration page of the ThinManager Server Configuration Wizard.
- ❑ **TCP/3268** – Used for LDAP queries targeted at the global catalog.
- ❑ **ICMP Echo Packets (Ping)** – Used by WinTMC and Enforce Primary.
- ❑ **DHCP (Dynamic Host Configuration Protocol)** - This needs configured, as needed.

VLANs and Subnets

- ❑ You should only have one PXE server per network. It is a good idea to have a separate VLAN for each ThinManager Server pair that will be replying to PXE requests.

Network Level Authentication (NLA)

- ❑ ThinManager supports Network Level Authentication (NLA) with firmware package 7.1.113 and later.
- ❑ If a Terminal has a valid Windows account entered in its configuration for an automatic login then the client will pass that info through NLA to authenticate. The client will login and start a session without the operator noticing.
- ❑ If a Terminal does not have a valid Windows account entered in its configuration then an NLA login screen will be displayed requiring a valid user account and password. This gets passed to the Remote Desktop Server for the login. A Windows Security/Login window is never displayed.

Note: NLA must be turned off on the Remote Desktop Servers if you want to use a Smart Card for authentication

Hardware

- ❑ Establish the IP addressing scheme for the thin clients. ThinManager Ready thin clients can use Static IP or DHCP. ThinManager Compatible thin clients need to use PXE boot. See Section 12.1.
- ❑ If using Static, open the IP Address menu on the thin client and list the IP address of the thin client and the ThinManager Server. See Section 12.1.1.
- ❑ If using DHCP, configure Option 066 to list the IP address of the ThinManager Server. See Section 12.1.1.
- ❑ If using PXE Boot, enable PXE boot by selecting Manage>PXE Server to launch the PXE Server wizard. See Section 12.1.4.
- ❑ Attach the terminals to ThinManager by either:
  - o Turning on the terminal and selecting the "Create New Terminal" option when the offline terminals are listed.
  - o Pre-creating the terminals in ThinManager and selecting the proper terminal name when the terminal is turned on and offline terminals are listed.

Results

- ❑ **Step 1:** The clients will connect to the ThinManager Server and download the firmware and configuration.
- ❑ **Step 2:** The configuration will send them to the Remote Desktop Server to login and start a session, as well as deliver any additional content assigned to the Terminal's configuration.

3. Microsoft Remote Desktop Services

These Microsoft tips are offered as a service to our customers.

Please see the official Microsoft® documentation for the latest information.

Note: We try to distinguish between Server 2008 and Server 2012 techniques and terminology. The terms Terminal Services and Terminal Services Client Access License (TS CAL) are used in Server 2008 while Windows Server 2008 R2 and Server 2012 use Remote Desktop Services, Session Hosting, and Remote Desktop Services Client Access License (RDS CAL).

3.1. Role of Remote Desktop Servers

A remote desktop server is a Windows Server 2008, Server 2012 or Server 2016 that has remote desktop services enabled. This configures the server to use mainframe-style client/server architecture. A client logs into the server and starts a session. Keystrokes and mouse movements are sent from the client to the session on the server. All processing takes place on the server and the resulting graphics are sent to the client for display.

The ThinManager configuration sends the ThinManager Ready thin client to the server(s) to start a session(s).

3.2. 2008/2008R2 Remote Desktop Server Setup

- ❑ Build a Windows Server 2008/2008 R2 computer. A fresh install is preferred. Virtual servers are fine.
- ❑ Add the Remote Desktop Services role. This is called Terminal Services in Windows 2008.
- ❑ Install the desired applications using the *Install Application on Terminal Server* program found in the Control Panel.
- ❑ Create the users on the Remote Desktop Server and add them to the *Remote Desktop Users* group.
- ❑ Go to the *RemoteApp Manager* and either allow unlisted applications or add permission the applications you want to run.

3.2.1. Remote Desktop Services Configuration in 2008

The Windows 2008 Server Manager is a console that provides tools for configuring Remote Desktop Services. It is launched from *Administrative Tools*.

Here are a few settings of note:

- ❑ *Server Manager > Roles > Remote Desktop Services>RemoteApp Manager*
    - o *RD Session Host Server Settings* – Microsoft allows connections to desktops only by default. Allow connection to all applications here for AppLink or white list the needed applications.
- ❑ *Server Manager > Roles > Remote Desktop Services>RD Session Host>Connections>RDP-tcp.*

  - *Sessions* – This is where you configure a session to end if disconnected.
  - *Client Settings* – This is where you set Audio and video playback, COM Port mapping, and the RDP Clipboard.

❑ *Server Manager > Roles > Remote Desktop Services>RD Session Host>Settings*

  - *Remote Desktop license mode* – This is where you set the licensing mode, either Per User or Per Device.
  - *Remote Desktop license servers* - Specify license server or use automatic discovery.

❑ *Server Manager > Roles > Remote Desktop Services>Remote Desktop Services Manager*

  - List of active and disconnected sessions

3.3. Windows 2012/2016

3.3.1. Setup Remote Desktop Services

With Windows Server 2012, it is highly advised that the server be part of a domain as the Remote Desktop Services graphical configuration is only available to Domain Admins. This section will assume that your new Remote Desktop Services Server is already part of a domain and you have credentials for a Domain Admin user account.

It is possible for you to setup Active Directory for a stand-alone server, and make that server also a Domain Controller. That setup is outside the scope of this section.

Detailed information for Windows Server 2012 configuration can be found at https://kb.thinmanager.com/images/d/d3/2012_ServerR2_Domain.pdf.

❑ Log into the Server with a Domain Admin account.

❑ Run ***Server Manager***.

❑ Select ***Add roles and features***.

❑ Click ***Next*** to launch the ***Add Roles and Features Wizard***.

❑ Select ***Remote Desktop Services installation***, and then press ***Next***.

❑ Select ***Quick Start***, and press ***Next***.

❑ Select ***Session-based Desktop deployment***, and press ***Next***.

❑ It should select automatically create a server pool, and add your local server. Press ***Next***.

❑ Check the ***Restart the destination server…*** box, and press ***Deploy***.

A progress screen will appear and display information on the new deployment progress. The server will automatically restart if the deployment is successful. It may also restart one or more times during the deployment process. After each restart, it will go back into Server Manager and post the status of the deployment.

❑ After the deployment completes successfully press ***Close***.

At this point, your Remote Desktop Server is setup and will allow you to make Remote Desktop connections to this server.

3.3.2. AppLink Configuration

If you would like to access individual applications using AppLink, follow these steps:

- ❑ In the **Server Manager Dashboard**, press ***Remote Desktop Services*** in the link on the left side of the window.
- ❑ On the next window, select ***QuickSessionCollection***, and then press the link for ***Publish RemoteApp Programs***.
- ❑ Select the applications you want to launch from the list that appears. If you don't see your specific application, then use the ***Add…*** button to browse for it. If it still does not appear, make sure the application is properly installed on this server.
- ❑ Press ***Next*** once you have selected your applications.
- ❑ Verify that all of the applications you want to run are listed, and press ***Publish***.

Once it completes, it will go back to the previous screen.

3.3.2.1. Command Line Options

You need to allow Command Line Parameters to specify specific files or URLs.

- ❑ Right click on the published application and select Edit Properties. This opens the Properties window.
- ❑ Select Parameters and select Add any command-line parameter. This will allow you to specify a file, URL, *.CLI, *.SCU, or other file to run using AppLink

3.3.3. Quick Session Collection

At this point, we need to now look at some of the other settings.

- ❑ In the Server Manager, with ***Remote Desktop Services > Collections > QuickSessionCollection*** selected, press on the ***Task*** drop down and then select ***Edit Properties***.
- ❑ If you would like to change the name of the collection to something other than **QuickSessionCollection** you can do it under the ***Task > Edit Properties*** drop down, and press the ***Apply*** button.
- ❑ Select the **User Groups** item in the menu on the left, and add the User Groups that you want to be able to remotely connect to your server. Use the ***Add*** button, and ***Apply*** once you've finished.
- ❑ Select the **Session** item in the left menu, and make any adjustments you would like to use for your system. The defaults here will work fine for ThinManager. Press ***Apply*** when complete.
- ❑ Press the **Security** item in the Menu to the left. Make sure your settings match those shown in the image below. Key for ThinManager clients is that you **UNCHECK** the **Allow Connections Only from…** item.
- ❑ Press ***Apply*** once finished.
- ❑ Select the **Client Setting** item in the menu to the left. Select the items you wish to change, and press ***Apply***. The default settings should work fine for you ThinManager system.

❑ You may now press the ***OK*** button to close the dialog box. At this point, your server is ready for ThinManager to use it as a Remote Desktop Server (Terminal Server).

3.3.1. Remote Desktop Services Configuration in 2012

The Windows 2012 Server Manager is a console that provides tools for configuring Remote Desktop Services. It is launched from Administrative Tools.

❑ *Server Manager> Remote Desktop Services> Collections> Tasks> Edit Deployment> Deployment Properties> RD Licensing* allows you to choose between Per Device and Per User.

❑ *Server Manager> Remote Desktop Services > Collections> QuickSessionCollections> Properties> Tasks> Edit Properties> Session* is where you configure a session to end if it is disconnected.

❑ *Server Manager> Remote Desktop Services > Collections> QuickSessionCollections> Properties> Tasks> Edit Properties> Security> Allow connections only from computers running Remote Desktop with Network Level* is where you turn off NLA if you want to use a Smart Card for a login tool.

❑ *Server Manager> Remote Desktop Services > Collections> QuickSessionCollections> Properties> Tasks> Edit Properties> Client Settings>* is where you allow Smart Cards, Audio and video playback, and the RDP clipboard.

❑ *Server Manager> Remote Desktop Services > QuickSessionCollections> RemoteApp Programs> Tasks> Publish RemoteApp Programs>* is where you white list applications to allow ThinManager to control access through AppLink instead of issuing the complete desktop that Microsoft uses as a default deployment.

3.3.2. Virtual Memory

❑ Set the Virtual Memory page file to 2.5 times the size of the physical memory to increase performance.

❑ Go to *Control Panel > System > Advanced System Options > the Advanced tab > Performance Settings* to launch the Performance Options.

❑ Select the Virtual Memory *Change* button on the *Advanced* tab.

❑ Set the *Initial size* and *Maximum size* to the same value to speed performance.

❑ Changing the virtual memory requires a computer reboot.

3.4. Microsoft Licensing

Each terminal or user will require a RDS CAL, Remote Desktop Services Client Access License, to access the Remote Desktop Servers. The RDS CALs are not pooled but allow connection to an unlimited number of Remote Desktop Servers.
The RDS CAL was known as the TSCAL, Terminal Services Client Access License in servers before Server 2008 R2.
Each terminal or user also needs a standard CAL, Client Access License.

❑ Add a Remote Desktop License Server (RDLS) to the network. This is not a separate piece of hardware but an application to install and run on an existing server.
In Server 2008 select *Roles>Add Roles>TS Licensing* in the Server Manager.
In Server 2008 R2 and Server 2012 select *Roles>Add Roles and Features> Remote Desktop Services> Remote Desktop Licensing* in the Server Manager

- ❑ Activate the RDLS by selecting *Start>Programs>Administrative Tools>Remote Desktop Licensing* on the Remote Desktop License Server and selecting *Action>Activate Server* from the menu to launch the licensing wizard. Follow Microsoft's instructions.
- ❑ Activate the RDS CALs on the RDLS through the licensing wizard following Microsoft's instructions.

Terminals will connect without a Remote Desktop License Server and receive a 120-day temporary RDS CAL. When this expires the terminal will display an "Unable to connect to terminal server" error message in the top left corner of its monitor. The cause of the error, lack of a RDLS and RDS CALs, can be found in the terminal server event log where it will show a "Client license is unable to be issued" error message. Add RDS CALs to an activated RDLS to solve this issue.

3.5. Microsoft Users

Terminals require a valid Windows user account to start a session on the remote desktop servers. These can be domain accounts or local accounts on each server.

- ❑ Create a **unique user account** for each terminal or user.
  In Server 2008 and Server 2012 use the Server Manager. Highlight the *Users* folder in *Configuration /Local Users and Groups* and select *Action> New User* from the menu.
- ❑ Add the users to either the *Remote Desktop Users* group or the *Administrators* group to allow access to the Remote Desktop Server.
- ❑ Apply any group policies as needed.

3.6. Microsoft Tools

Terminal Services has several commands that aid in managing the Remote Desktop Server.

3.6.1. Alternative Terminal Keystrokes

Certain keystrokes are not available in a terminal session. Microsoft has provided these alternatives.

Keystroke	Function
ALT+PAGE UP	Switches between programs from left to right.
ALT+PAGE DOWN	Switches between programs from right to left.
ALT+INSERT	Cycles through the programs in the order they were started.
ALT+HOME	Displays the Start menu.
CTRL+ALT+BREAK	Switches the client between a window and full screen.
CTRL+ALT+END	Brings up the Windows 2000 Security dialog box.
ALT+DELETE	Displays the Windows menu.
CTRL+ALT+Minus (-) symbol on the numeric keypad	Places a snapshot of the active window, within the client, on the Remote Desktop Server clipboard (provides the same functionality as pressing PrintScrn on a local computer.)
CTRL+ALT+Plus (+) symbol on the numeric keypad	Places a snapshot of the entire client window area on the Remote Desktop Server clipboard (provides the same functionality as pressing ALT+PrintScrn on a local computer.)

3.6.2. Microsoft Commands

Command	Action
`change logon`	Temporarily disables logons to a Remote Desktop Server
`change port`	Changes COM port mappings for MS-DOS program compatibility
`change user /install`	Puts the server into “Install Mode”
`change user /execute`	Removes the server from “Install Mode”
`ipconfig`	Displays the IP addresses of the network card
`logoff`	Logs off a user from a session and deletes the session from the server
`net send` ***`username`*** ***`“message”`***	Sends a message to a user. ***username*** is the NT/2000 user name that the person or terminal is logged in as. “***message***” is the text of the message. Quotation marks are needed for any messages containing a space.
`query process`	Displays information about processes running on a Remote Desktop Server
`query session`	Displays information about sessions on a Remote Desktop Server
`query termserver`	Displays a list of all Remote Desktop Servers on the network
`query user`	Displays information about user sessions on a Remote Desktop Server
`reset session`	Resets a session to known initial values
`shadow`	Monitors another user's session
`tsdiscon`	Disconnects a client from a Remote Desktop Server session
`tsshutdn`	Shuts down the Remote Desktop Server in an orderly manner

Commands to launch useful Microsoft programs include:

Command	Action
`gpedit.msc`	Launches the Group Policy Editor
`secpol.msc`	Launches the Local Security Policy
`tscc.msc`	Launches the Terminal Services Configuration Console
`tsadmin`	Launches the Terminal Services Manager

4. Network

Thin clients and Remote Desktop Servers need a reliable network.

Make sure that the following network ports are unblocked, including in the Windows firewall:

- ❑ **UDP/4900** - TFTP - Used for the TFTP download of the firmware.
- ❑ **TCP/2031** - Configuration - Used to pass the configuration from the ThinManager Server to the thin client.
- ❑ **UDP/67** – IP Address Assignment – Used by the PXE Server (if using PXE boot).
- ❑ **UDP/69** – TFTP – Used by the PXE Server (if using PXE boot).
- ❑ **UDP/4011** – UEFI Boot – Used when the DHCP server is on the ThinManager server or when using the Unified Extensible Firmware Interface (UEFI) BIOS to boot.
- ❑ **TCP/1494** - Citrix - Used by the ICA protocol (if using ICA instead of RDP).
- ❑ **TCP/3389** - RDP - Used by the RDP protocol (if using RDP in v2.4.1 or later).
- ❑ **TCP/5900** - Shadowing - Used to shadow terminals. This can be changed on the Shadow Configuration page of the ThinManager Server Configuration Wizard.
- ❑ **UDP/1758** – Used if the default Multicast is used. If the network MTU size is not the default then the packet size needs changed on the Multicast Configuration page of the ThinManager Server Configuration Wizard.
- ❑ **TCP/3268** – Used for LDAP queries targeted at the global catalog
- ❑ **ICMP Echo Packets (Ping)** – Used by WinTMC and Enforce Primary.
- ❑ **DHCP** – The Dynamic Host Configuration Protocol can be used to deliver IP addresses to thin clients.

5. The Thin Client Boot Process

All versions of ThinManager support the use of ThinManager Ready thin clients. ThinManager 5 and later with the Xli license allows the PXE booting of ThinManager Compatible thin clients. PXE Server and PXE boot are covered in section 12.2.

- ❑ The terminal is turned on and connects to the network.
- ❑ The terminal receives an IP address either through the default DHCP, PXE boot, or by being configured with static IP.
- ❑ The terminal connects to a ThinManager Server (defined in Option 066 of DHCP, the PXE server, or by static IP) and downloads its configuration.
- ❑ This configuration sends the terminal to the Remote Desktop Server(s).

6. ThinManager

6.1. Role of ThinManager

- ❑ ThinManager allows the configuration of ThinManager Ready thin clients.
- ❑ A ThinManager Ready thin client needs to connect to a ThinManager Server and receive its profile configuration.
- ❑ This profile sends the ThinManager Ready thin client to a Remote Desktop Server(s) to start a session and run.
- ❑ ThinManager allows an administrator to monitor and manage the thin client system.

❑ ThinManager provides control and ease of management to the thin client system.

❑ ThinManager allows you to control access to applications and assets.

6.2. ThinManager Installation

❑ Install on a server or a workstation.
It is not required to be on the Remote Desktop Server although that is a common practice.
Servers are preferred over workstations because of the flexibility of their configuration.

❑ ThinManager contains both a 32-bit and 64-bit version. The install will give you five checkboxes during installation.

- *ThinManager* and *ThinManager x64* are the interfaces that allow control and configuration of the ThinServer engine.
- *ThinServer* and *ThinServer x64* are the engines that run the program.
- *ThinManager Tools* are additional tools like touch screen calibration.

Normally all three are selected. Select *ThinManager Utilities* and either *ThinManager* and *ThinServer* for a 32-bit install or *ThinManager x64* and *ThinServer x64* for a 64-bit install.

You will only be presented with the 32-bit choice on 32-bit machines. An upgrade of ThinManager will show the same version as the installed version type.

6.2.1. ThinManager Server Setup in 2008/2008R2

❑ Install ThinManager using the *Install Application on Terminal Server* (*Install Application on Remote Desktop Server* in 2008R2) program found in the Control Panel.

❑ Go to the firewall and allow all inbound communications or open ports in the firewall to allow UDP port 4900 and TCP port 2031 traffic.

❑ You may need to go to the *Local Security Policy* and change the *User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode* to *Elevate without prompting*.

6.2.2. ThinManager Server Setup in 2012/2016

❑ Install ThinManager in compatibility mode. Right-click on the installer and click properties. Set the compatibility mode for Server 2008.

❑ You may need to go to the *Local Security Policy* and change the *User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode* to *Elevate without prompting*.

6.2.3. ThinManager versus ThinServer

❑ The ThinManager program is composed of two parts, a ThinServer engine and a ThinManager interface.

❑ ThinServer is the database engine that does the work. It supplies the firmware, controls SmartSession, and holds the licenses and configuration.

❑ ThinManager is the interface that is used to control and configure the ThinServer database.

6.3. Redundant ThinManagers

Because each ThinManager Ready thin client needs to contact ThinManager to retrieve its configuration the use of a second redundant ThinManager Server can be useful to prevent downtime due to the loss of the primary ThinManager Server. Redundant ThinManager Servers should be synchronized so that it doesn't matter which ThinManager Server the thin client boots from.

6.3.1. Failover versus Redundancy

❑ A ThinManager Ready thin client needs to connect to a ThinManager Server and receive its configuration.

❑ This configuration sends the ThinManager Ready thin client to a Remote Desktop Server(s) to start a session and run.

❑ **Redundancy** describes having two ThinManager Servers so that a ThinManager controlled thin client can always find a ThinManager Server to boot from and receive its configuration.

❑ **Failover** describes having multiple Remote Desktop Servers that the thin client always has a Remote Desktop Server it can connect and start a session.

Note: When a ThinManager thin client boots it loads its configuration into memory. The thin client will continue to run until the memory is cleared when it is rebooted even if the ThinManager computer fails.

6.3.2. Full Redundancy

Full Redundancy uses two synchronized ThinServer engines and has two ThinManager interfaces for control from either computer.

❑ Install ThinManager on two computers. Make sure they are the same version of ThinManager.

❑ Purchase Redundant ThinManager Product License(s).

❑ Auto-synchronize the ThinManager Servers as described in section 6.3.5 so that the Install IDs of both ThinManager Servers are displayed in the Licensing Window (*Install>Licenses* on the ThinManager menu bar).

❑ Create a Master License with Full Redundancy. Add the Product Licenses, activate with the Installation IDs, and apply. See section 7.2.3.

❑ Configure each ThinManager Ready thin client to boot from both ThinManager Servers. See 12.1 for details.

6.3.3. Mirrored Redundancy

Mirrored Redundancy uses two synchronized ThinServer engines but allows administrative functions only on the designated primary ThinManager Server.

❑ Install ThinManager on two computers. Make sure they are the same version.

❑ Purchase Mirrored ThinManager Product License(s).

❑ Auto-synchronize the ThinManager Servers as described in section 6.3.5 so that the Install IDs of both ThinManager Servers are displayed in the Licensing Window (*Install>Licenses* on the ThinManager menu bar).

❑ Create a Master License with Mirrored Redundancy. Add the Product Licenses, activate with the Installation IDs, and apply. It is important to enter the Primary Installation ID in the Primary Installation ID field on the license activation site. See section 7.2.3.

❑ Configure each ThinManager Ready thin client to boot from both ThinManager Servers. See 12.1 for details.

6.3.4. Single ThinManager

- ❑ Install ThinManager on a single computer.
- ❑ Create a Master License. Add the Product License, activate with the Installation ID, and apply. See section 7.2.3.

6.3.5. Auto-Synchronization

- ❑ Open the ThinManager Server List Wizard by selecting *Manage> ThinManager Server List* from the ThinManager menu bar.
- ❑ Select the *Automatic Synchronization* checkbox on the Auto-synchronization Selection window.
- ❑ Define the primary and secondary ThinManager Servers by selecting the *Edit* button and adding the server name and IP address.
- ❑ Select the *Finish* button to accept the change.

It is important to keep a backup copy of you ThinManager configuration. See 23.4 to see how to schedule automatic backups.

6.4. ThinManager Interface

ThinManager has an interface based on the Outlook template.

- ❑ Menu commands are displayed as icons on a ribbon bar.
- ❑ The tree is organized by branches, each with its own icon.
- ❑ A Quick Access Tool Bar is customizable with commonly used commands at the top left of the program interface.
- ❑ The interface color and tab design are changeable on the View tab.
- ❑ Tabs can be re-ordered or torn away from the interface.

7. ThinManager Licensing

ThinManager 11 introduced Rockwell Automation’s FactoryTalk Activation to the ThinManager platform. You can choose the traditional ThinManager Licensing or FactoryTalk Activation by selecting *Install>License Mode* from the ThinManager menu bar.

- See ThinManager Demo Code on page 18.
- See ThinManager License Activation Overview on page 19.
- See FactoryTalk License Activation on page 22.

7.1. ThinManager Demo Code

A Demo Code is a temporary activation used to trial the product or to restore licensing in an emergency. It is activated with the Installation ID from ThinManager.

- ❑ Open the ThinManager Licensing window by selecting *Install>Licenses* from the ThinManager menu bar.
- ❑ The Installation ID is found at the bottom of the ThinManager Licensing window.
- ❑ Go to https://thinmanager.com/licensing/ and select the Demo Code link.

❑ Fill in the information on the Demo Code form. Use a proper e-mail as the Demo Code will be sent to that e-mail address. Check your Junk and Spam folders if the Demo Code doesn't arrive within 5 minutes.

❑ Select the Install Demo Code button on the ThinManager Licensing window. Enter the Demo Code in the Demo Code field. This will provide 30 days of unlimited functionality.

Note: The Demo Code can only be activated every 120 days on a computer. Contact support@thinmanager.com I f the License site doesn't allow an activation.

7.2. ThinManager License Activation Overview

The traditional method of ThinManager license activation is:

❑ Purchase a Product License(s) from a ThinManager distributor.

❑ Register as a user on the ThinManager License Site at www.thinmanager.com/licensing/

❑ Log in to the ThinManager License Site.

❑ Create a Master License by selecting the Create Master License link.

❑ Add the purchased Product License(s) to the Master License.

❑ Activate the Master License with the Installation ID that is found at the bottom of the ThinManager Licensing window. This is opened by selecting *Install>Licenses* from the ThinManager menu bar. If the Product License includes Redundancy then activate it with the Installation IDs from both ThinManager Servers.

❑ Download the license file and transfer it to the ThinManager Server.

❑ Open the ThinManager Licensing window by selecting *Install>Licenses* from the ThinManager menu bar.

❑ Select the *Install License* button. Browse to the downloaded license and select *Open*.

❑ The license will be installed.

An expanded licensing section follows.

7.2.1. ThinManager License Types

ThinManager has three licensing types.

- **Enterprise Server Licenses** provide unlimited connections of terminals. It includes full redundancy for a synchronized pair.
- **Standard Licenses** are available in 5, 10, and 25-connection packs. These can be bought as stand-alone, mirrored redundancy, of with full redundancy.
- **Flex Packs** are pools of 100 connection licenses. They can be divided up into smaller numbers. This allows a company to put 17 at one site, 23 at another, etc. until the licenses are all assigned.

Enterprise Server Licenses have Full Redundancy. Standard Licenses can be purchased with Full or Mirrored Redundancy, See Redundant ThinManagers on page 16.

7.2.1.1. Enterprise Server Licenses

❑ Enterprise Server provides licenses for two ThinManager Servers for full redundancy.

❑ The Enterprise Server has unlimited ThinManager connection licenses. The XLr version also has unlimited Redundancy licenses

❑ The redundant ThinManager Servers are licensed with a Redundant Master License that uses the Install IDs from both ThinManager Servers.

❑ Each ThinManager Server can run the ThinManager interface for configuration and control.

❑ ThinManager Ready thin clients should be configured to boot from both ThinManager Servers

❑ The two ThinManager Servers should be auto-synchronized so that the configurations are the same. See section 6.3.5.

7.2.1.2. Standard Licenses

❑ Standard Licenses provide licenses in packs of 5, 10, and 25 connections.

❑ ThinManager 8.1 and later is available in the XLr product license. This adds Relevance to ThinManager and provides all of the ThinManager functionality.

❑ The standard licenses are added to your Master License as Product Licenses. See 7.2.6.

7.2.1.3. Flex Licenses

❑ Flex Licenses are sold in packs of 100.

❑ The customer can sub-divide the licenses in smaller custom packs to deploy across the company network.

7.2.2. Product License

ThinManager 8.1 and later has one Product License type available, the XLr product license.

The XLr Product License bundles all the ThinManager and Relevance functionality into a single product license. This includes the Terminal Connection, MultiMonitor, TermSecure, WinTMC, iTMC, PXE boot, Locations, Fencing, and mobile devices.

Previous versions sold these functions as separate product licenses.

❑ The XLr Product License is added to a Master License.

7.2.3. Master Licenses

ThinManager requires a license for each terminal that connects through ThinManager. These are assigned when the terminal retrieves its configuration.

❑ Licenses should be activated in the name of the end customer and not the name of a system integrator or consultant.

❑ ThinManager 4 and later use a Master License. This acts as a basket to hold the individual Product Licenses.

❑ Master Licenses are created and activated through the ThinManager web site. The activation process requires Product License Numbers and an Installation ID.

❑ The Product License Number is the purchased “paper” license.

❑ The Install ID ties the license to the hardware. It is found on the Licensing Window by selecting *Install>Licenses* from the ThinManager menu bar.

❑ The downloaded master license file is installed through ThinManager.

7.2.4. ThinManager License Account

- ❑ Each person who wants to access the license database needs to register on the License Activation site by creating an account with contact information for the user. This user account allows the user to activate licenses.
- ❑ Select the *New User* link at the ThinManager website at www.thinmanager.com/licensing/ and fill out the appropriate fields to create the account.
- ❑ Once the account is created the password of the account will be sent to the email address defined in the account.

7.2.5. Master License Creation

- ❑ ThinManager licenses are activated at the ThinManager website at www.thinmanager.com/licensing/ A *License Activation* link will be prominently displayed on the main page.
- ❑ The licensee needs to login to the License Activation site with their created user account. See Section 7.2.4.
- ❑ The logged-in user should select the *Create Master License* link in the menu bar.
- ❑ Enter a description of the ThinManager Server and its location in the *Server Name/Site Description* fields. Enter the end user information in the *Company Name* and *Address* fields.
- ❑ Select the *Submit* button to create the Master License.

7.2.6. Adding Product Licenses to Master License

- ❑ A Master License without a Product License is an empty container. Product Licenses need to be added to the Master License. The Product License Number is the purchased “paper” license. It may be found inside the ThinManager CD case or e-mailed by the seller.
- ❑ Select the *Manage Master Licenses* link in the menu bar of the licensing web site.
  A list of all your master licenses will be displayed.
- ❑ Select the *Add Product License* link for your master license. Add the product license in the field that is displayed.
  Repeat for each product license.

7.2.7. Activating the Master License

ThinManager Licenses are activated at http://www.thinmanager.com/licensing/

- ❑ The Master License needs activated once the product license(s) have been added.
- ❑ Select the *Activate License* link in the table for your master license.
- ❑ Enter the Installation ID in its field. The Installation ID is found by selecting *Install>Licenses* in ThinManager to display the Licensing window.
- ❑ If you are using Redundancy or Mirrored Redundancy you need to enter both the primary and secondary installation IDs in the proper fields. The IDs are in the Licensing window of ThinManager.
- ❑ Select *Submit* to download the file. Don’t save it in the ThinManager folder but save it to a directory that ThinManager has access to.

Note: If you plan on a redundant system but only have one ThinManager Server to start you should create a Redundant Master License and activate the license with the Installation ID from the first ThinManager Server.
You can reactivate the master license with both the primary and secondary Install IDs later when both ThinManager Servers are ready.

7.2.8. Installing the Master License

- ❑ Open the Licensing window in ThinManager by selecting *Install>Licenses* from the menu.
- ❑ Select the Install License button. Browse to the downloaded master license file and select *Open*. ThinManager will install the file.

7.2.9. Single Product Licenses on Redundant Master License

- ❑ You can add a non-redundant product license to a redundant master license using the steps described in 7.2.6. You will be asked to assign the product license to either the primary or backup ThinManager Server.

7.2.10. Reactivating Licenses

- ❑ The master license will need reactivated each time a new product license is added or the ThinManager is upgraded to a later version.

7.3. FactoryTalk License Activation

ThinManager 11 introduced FactoryTalk Activation to provide client licenses to a ThinManager System.

- ❑ Select *Install>License Mode* from the ThinManager menu bar and select the *FactoryTalk Activation* radio button.
- ❑ Select *Install>License* from the ThinManager menu bar to open the FactoryTalk Activations window.
- ❑ Select the Add Activations button to open the Add Activations from ThinManager window.
- ❑ Highlight the ThinManager license (TM.CLI.#.#) and select OK to add. There is a field that lets you pull a portion of the licenses into ThinManager.
- ❑ When done the FactoryTalk License will be displayed in the FactoryTalk Activation window.
- ❑ The FactoryTalk Activation window can be opened by selecting *Install>License.*

8. ThinManager Configuration

ThinManager uses Wizards to aid in the configuration of the terminals.

Note: Selecting the F1 button while in a wizard will launch a context-sensitive help document within the ThinManager program for guidance.

The wizards can be run to pre-configure the terminals or the wizards can be launched automatically when the new terminal is connected to ThinManager for the first time.

- ❑ Normally it is best to define the Remote Desktop Servers as Display Servers first, define the applications as Display Clients second, and then configure the terminals.

See **Section 9, *Configuration - Display Servers***, on page 23.

See **Section 10, *Configuration - Display Clients*** , on page 24.

See **Section 11, *Configuration - Terminal***, on page 28.

See **Section 12, *Configuration - Hardware*** , on page 29.

Note: If in doubt, the default settings are your friends.

9. Configuration - Display Servers

- □ Display Servers are devices that provide content that can be displayed on the client. Examples include the traditional Remote Desktop Server and IP cameras.
- □ The Remote Desktop Server List Wizard allows configuration of Terminal Services Display Servers.
- □ The Camera Configuration Wizard allows configuration of Camera Display Servers. See 9.2.
- □ The VNC Server Wizard allows configuration of VNC Servers. See 9.3.

9.1. Remote Desktop Server Configuration

- □ Remote Desktop Servers are defined in the Remote Desktop Server Wizard. This can be launched by selecting the *Server* icon in the tree selector at the bottom of the tree and right clicking on the Remote Desktop Servers branch of the ThinManager tree and selecting *Add Remote Desktop Server*.

Proceed through the pages of the wizard. The highlights are:

- □ **Terminal Server Name** - Enter the Microsoft computer name in the *Name* field.
- □ **Terminal Server Name** - Enter the IP address in the *IP Address* field or use the *Discover* button to automatically fill in the IP address.
- □ **Terminal Server Name** - Enter the user name and password for an administrative account on the terminal server into the *User Name* and *Password* field to allow ThinManager to import the Terminal Services Manager information into ThinManager. This is important for SmartSession load balancing.
The *Search* button allows the administrator to pull the user accounts from a domain Active Directory.
- □ **Terminal Server Capabilities** - Select *Available for Display Clients using SmartSession Groups* if the terminal server will be used for SmartSession.
- □ **Data Gathering** - Select a Data Gathering Interval. This is the frequency that ThinManager polls the terminal server for the Terminal Services Manager information. Select the *Next* button to continue.
- □ **SmartSession Configuration -** This allows the SmartSession parameters to be changed from the defaults.

Note: If in doubt, the default settings are your friends.

9.2. Camera Configuration

ThinManager originally supported the Motion Jpeg protocol. It now supports the Real Time Streaming Protocol (RTSP), the Motion JPEG protocol, and USB cameras.

❑ Camera sources are defined as Display Servers. Their output is configured as a Display Client. See 10.3.

❑ Cameras are defined in the Camera Configuration Wizard. This can be launched by right clicking on the Camera branch of the Display Server branch of the ThinManager tree and selecting *Add Camera*.

Proceed through the pages of the wizard. The highlights are:

❑ **Camera Name** - Enter a name for the camera in the *Camera Name* field.

❑ **Camera Name** – Select the protocol in the *Type* drop-down.

❑ **Camera Name** – Enter the camera IP address and port if the camera is an IP camera. See your camera documentation for instructions on setting these.

❑ **Camera Name** – Select the host terminal if the camera is defined as a USB camera.

Note: USB cameras are plugged into a terminal them and defined as a Display Server. They are defined by selecting the host terminal in the *Terminal* field once the USB Camera is selected as the *Type* on the Camera Name page.

❑ **Camera Authentication** – Add a *Username* and *Password* if required.

❑ **Camera Authentication** – Add the URL that the camera uses to supply the video stream in the *Custom URL* field.

❑ Select *Finish* to complete the wizard.

9.3. VNC Configuration

ThinManager supports the ability to shadow VNC servers from the ThinManager console or from terminals using a VNC display client.

❑ Define your VNC sources as VNC Display Servers. This can be launched by right clicking on the VNC Server branch of the Display Server branch of the ThinManager tree and selecting *Add VNC Server*.

❑ **VNC Server Name** - Enter the name of the source VNC server *VNC Server Name* field.

❑ **VNC Server IP Address**- Enter the IP address of the VNC source.

❑ **Port** – Enter the VNC port you will use. 5900 is the default.

❑ **Password** – Enter the VNC Server password, if needed.

❑ Select *Finish* to complete the wizard.

10. Configuration - Display Clients

Display Client is the term used to denote the graphic rendering of the output from a Display Server. This could be a traditional Remote Desktop Services session, IP Camera display, Terminal-to-Terminal Shadow session, Workstation deployment, VNC shadow or a Virtual Screen.

10.1. Display Client Groups

A Display Client Group can be created to contain several Display Clients. This allows you to add a collection of Display Clients to a terminal in one step instead of adding several at a time.

You create the Display Client Group then add the Display Clients you want as members.

- ❑ Launch the Display Client Wizard by selecting the Display Client icon in the tree selector at the bottom of the ThinManager tree, right clicking on the Display Client branch of the tree, and selecting *Add Display Client Group*.
- ❑ **Client Name** - Enter the name of the Display Client in the *Client Name* field.
- ❑ **Client Name** – Select the *Finish* button to create the Display Client Group.
- ❑ Open each Display Client that you want in the Display Client Group and Select the *Change Group* button to open the Select Display Client window.
- ❑ Highlight the Display Client Group and select the *OK* button to add the Display Client.
- ❑ Repeat as needed until all the Display Clients you want are in the group.

10.2. Remote Desktop Services Display Clients

- ❑ Terminal Services Display Clients are defined in the Display Client Wizard.
- ❑ Launch the Display Client Wizard by selecting the Display Client icon in the tree selector at the bottom of the ThinManager tree, right clicking on the RDS branch of the tree, and selecting *Add Display Client*.

Proceed through the pages of the wizard. The highlights are:

- ❑ **Client Name** - Enter the name of the Display Client in the *Client Name* field.
- ❑ **Client Name** - Select Terminal Services in the *Type Display Client* drop-down.
- ❑ **Display Client Options –** Select the *Include Camera Overlays* checkbox if you want to add camera output to the Display Client.
- ❑ **Display Client Options –** Select the *Virtual Screen Overlays* checkbox if you want to add a Virtual Screen to the Display Client.
- ❑ **Display Client Options –** Select the *Include Virtual Screen Overlays* checkbox if you want to add a Virtual Screen to the Display Client.
- ❑ **Relevance Options** – The *Allow Local Access* and *Allow Remote Access* controls local and remote deployment when using Relevance.
- ❑ **Terminal Services Display Client Type** – Choose the default Remote Desktop Protocol or other protocol to use for client communication.
- ❑ **Remote Desktop Services and Workstation Options –** Select the options needed:
  - *Allow Auto-Login* to let the session start automatically. Uncheck this to force the user to manually login.
  - *Application Link* for application deployment.
  - *SmartSession for load balancing.*
  - *Enforce Primary* to set one computer as the preferred Remote Desktop Server.
  - *Instant Failover* to launch two instances of the application for quick failover.
- ❑ **Session Resolution / Scaling Options** – The Session Scaling Options allow you to scale the session while maintaining the aspect ratio of the session.
- ❑ **Session Resolution / Scaling Options** – This allows you to set the screen resolution of the display client and override the terminal setting.
- ❑ **Display Client Members** - Select the Remote Desktop Servers that should be used by the Display Client by moving the desired Remote Desktop Servers into the *Selected Terminal*

Servers list. Select the *Edit Server List* button to launch the Remote Desktop Server Configuration Wizard if you need to define terminal servers.

❑ **SmartSession Settings -** If the Display Client uses SmartSession you can change the SmartSession settings from the defaults, if needed.

❑ **AppLink -** Enter the path to a program in the *AppLink Path* field if you want the Display Client to run a specific program instead of a desktop.

❑ Select the *Finish* button to complete the Display Client configuration.

10.3. Camera Display Clients

❑ Camera Display Clients are defined in the Display Client Wizard.

❑ Launch the Display Client Wizard by selecting the Display Client icon in the tree selector at the bottom of the ThinManager tree, right clicking on the Camera branch of the tree, and selecting *Add Display Client*.

Proceed through the pages of the wizard. The highlights are:

❑ **Client Name** - Enter the name of the Display Client in the *Client Name* field.

❑ **Client Name** - Select *Camera* in the *Type of Display Client* drop-down.

❑ **Overlay Layout** – Select the layout format from the *Choose Camera Layout* drop-down. You can selct a pre-configured template or add custom overlays.

❑ **Overlay Cameras** – A page will be displayed for each overlay. You can let the user choose from all the cameras by selecting the *All Cameras Available* or you an unselect that and add cameras with the *Add* button.

10.4. Terminal Shadow Display Client

❑ Terminal Shadow Display Clients are defined in the Display Client Wizard.

❑ Launch the Display Client Wizard by selecting the Display Client icon in the tree selector at the bottom of the ThinManager tree, right clicking on the Terminal Shadow branch of the tree, and selecting *Add Display Client*.

Proceed through the pages of the wizard. The highlights are:

❑ **Client Name -** Enter the name of the Display Client in the *Client Name* field.

❑ **Client Name** - Select Terminal Shadow in the *Type of Display Client* drop-down.

❑ **Display Client Options –** Select the *Include Camera Overlays* checkbox if you want to add camera output to the Display Client.

❑ **Terminal Shadow Display Client** – Leave the *All Terminals Available* checkbox selected to allow any terminal to be shadowed or un-select it and use the *Add* button to add one or more terminal to the list or available terminals to shadow.

❑ **Terminal Shadow Display Client** – Leave the *Interactive Shadow* checkbox selected to allow the user to control the shadowed session or un-select it to limit a user to viewing the session.

10.5. Workstation Display Clients

The Workstation Display Client allows you to connect to a workstation and display the console remotely at a thin client. This can be either a physical workstation or a virtual workstation.

The Workstation Display Client acts as a template that configures how the terminal will use the workstation template. You add the specific workstation in the Terminal Configuration wizard after adding a workstation display client.

Workstation Display Client Wizard

- ❑ Right-click on the Workstation icon in the Display Clients tree and select *Add Display Client* to launch the Workstation Display Client wizard.
- ❑ Launch the Display Client Wizard by selecting the Display Client icon in the tree selector at the bottom of the ThinManager tree, right clicking on the Workstation branch of the tree, and selecting *Add Display Client*.
- ❑ Name the client. The Display Client Options page and the Remote Desktop Services and Workstation Options are the same as a regular display client.
- ❑ The *Application Link* checkbox does not work on operating systems after Windows XP.
- ❑ Select the *Finish* button to finalize the wizard.

Adding the Workstation Display Client

- ❑ Apply the Workstation Display Client to the desired thin client on the *Display Client Selection* page of the Terminal Configuration Wizard. Once it is added the next screen will be the *Complete the Workstation Display Client Configuration* page that allows you to specify the desired workstation.
- ❑ Selecting the *Add Workstation* button will allow you to point to a physical workstation.
- ❑ Selecting the *Add Virtual Workstation* button will allow you to point to a virtual workstation on a defined VCenter Server.
- ❑ You can add multiple workstations for failover. You will have one in use at a time per added Workstation display client.

Configuring the Workstation

- ❑ Each workstation you plan on connecting to will need remote access enabled on the Remote tab on the System Properties of the workstation.

10.6. VNC Display Client

- ❑ VNC Display Clients are defined in the Display Client Wizard.
- ❑ **Client Name** - Enter the name of the Display Client in the *Client Name* field.
- ❑ **Client Name** - Select VNC in the *Type of Display Client* drop-down.
- ❑ **VNC Display Client** – The *All VNC Servers Available* will let you connect to any defined VNC server by picking one out of a menu displayed on the display client on the terminal. You can uncheck this and select a specific VNC server by clicking the *Add* button and selecting a VNC server from the list. You may add multiple VNC servers and be shown a list to select from.
- ❑ **VNC Display Client** – The Interactive Shadow checkbox allows you to control the VNC session. Unchecking it will give you a ‘look but not touch’ mode.

10.7. Virtual Screen Display Client

Virtual Screens allow you to subdivide a display client into multiple overlays bringing MultiMonitor functionality to single monitors or spanned monitors in a MultiMonitor system.

The overlays are added and managed much like Camera Display Client overlays.

❑ Virtual Screen Display Clients are defined in the Display Client Wizard.

❑ **Client Name** - Enter the name of the Display Client in the *Client Name* field.

❑ **Client Name** - Select Virtual Screen in the *Type of Display Client* drop-down.

❑ **Display Client Options –** Select the *Include Camera Overlays* checkbox if you want to add camera output to the Display Client.

❑ **Select or Create the Virtual Screen Layout –** Select the number of overlays and their layout from the *Choose Layout* drop-down. The templates have one to sixteen overlays.

❑ **Select or Create the Virtual Screen Layout –** Select the *Screen Resolution* of the display client.

❑ **Select or Create the Virtual Screen Layout –** Use the *Add* button to define custom overlays if you select the *Custom* option in the *Choose La*yout drop-down.

❑ **Virtual Screen Configuration** – The wizard will navigate a page for each overlay to allow you to assign the display clients each overlay. Use the *Add* button to select the display clients. You may add multiple display clients to each overlay.

❑ **Virtual Screen Configuration** – The *Screen Option* button allows you to configure the group selector for each overlay.

❑ **Virtual Screen Configuration** – Navigate through the wizard until each overlay has display clients.

11. Configuration - Terminals

❑ Launch the Terminal Configuration Wizard by selecting *Edit>Add* from the ThinManager menu or by selecting the *Terminal* icon in the tree selector at the bottom of the tree, right clicking on the Terminals branch of the tree, and selecting *Add Terminal*.
If a terminal is connected to ThinManager without a configuration it will launch the wizard automatically.

Proceed through the pages of the wizard. The highlights are:

❑ **Terminal Name** - Enter the desired name of the terminal. This name should be 15 characters or less.
Add the terminal to a group, if desired, by selecting the *Change Group* button.

❑ **Terminal Hardware** - Select the hardware make and model. This is optional, as the terminal will correctly identify itself when it connects to ThinManager.
PXE boot clients need to use *GENERIC/PXE* in the *Make/Model* drop-down.
WinTMC clients need to use *GENERIC/WinTMC* in the *Make/Model* drop-down.

❑ **Terminal Options** – Shadow access can be controlled in the *Shadowing* section.

❑ **Terminal Mode Selection** – Choose *Enable MultiMonitor* to use more than a single monitor.
Chose *Enable Relevance User Services* to use Permission to control application access on the terminal.
Chose *Enable Relevance Location Services* to use Locations on the terminal.

❑ **Display Client Selection** – Apply Display Clients to the terminal by adding them to the *Selected Display Clients* list on the right. If Display Clients haven't been defined then select the *Edit Display Clients* button to launch the needed configuration wizard.

❑ **Terminal Interface Options** and **Hotkey Configuration** – A terminal using multiple Display Clients need a method to switch between sessions. These are configured on these two pages.

- ❑ **Relevance Options** – This allows you to assign a location to the terminal.
- ❑ **Relevance Options** – This allows you to use Bluetooth, GPS, or Wi-Fi as Resolvers on the terminal.
- ❑ **Log In Information** - Enter a valid Windows user name and password into the *Username* and *Password* fields if you want the terminal to automatically login when it connects to the Remote Desktop Server.
  The *Search* button allows the administrator to pull the user accounts from a domain Active Directory.

Note: The Log In Information can be left blank if a Location is going to provide the user credentials.

- ❑ **Video Resolution** - Set the desired video resolution for the terminal.
- ❑ **WinTMC Settings** – These are settings specific to a PC running the WinTMC application to become a managed fat client.
- ❑ **Mobile Device Options** - These are settings specific to a mobile device for use with Relevance.
- ❑ **Module Selection** - Add any modules that are needed by selecting the *Add* button. See *Modules* in section 17 for details.
- ❑ **ThinManager Server Monitor List** – This was used for manual synchronization before automatic synchronization was introduced.
  This page is hidden when using Auto-synchronization.
- ❑ **Monitoring Configuration** – This sets the rate at which the terminal polls the Remote Desktop Server to determine if the Remote Desktop Server is available for connections.
- ❑ If the wizard was launched when the terminal connected to ThinManager it will continue to boot and login as defined once the *Finish* button is selected. If the wizard was run as a pre-configuration, this profile will be available for selection when new hardware is added.

11.1. Terminal Group Configuration

- ❑ Terminals can be organized by adding them to a Terminal Group.
- ❑ Groups can be nested into other Groups.
- ❑ A Terminal Group is created by selecting *Edit>Add Group* from the ThinManager menu or by right clicking on the *Terminals* icon in the Terminals branch of the ThinManager tree. The Group Configuration Wizard resembles the Terminal Configuration Wizard with the addition of the *Group Setting* checkbox.
- ❑ A property that is set as *Group Settings* is applied to everybody in that group.
- ❑ Terminals can join a group by the selection of the *Change Group* button on the Terminal Name page of the Terminal Configuration Wizard.

12. Configuration - Hardware

ThinManager Ready thin clients contain a ThinManager BIOS and need little configuration at the terminal except an IP address and the IP address of a ThinManager Server to connect on the network. Units are shipped using DHCP by default but can be configured to use static IPs or PXE servers.

ThinManager Compatible thin client use the PXE boot function to connect to ThinManager.

12.1. IP Addressing

12.1.1. DHCP Only

- ❑ ThinManager Ready thin clients are set by default to use DHCP to receive their IP address.
- ❑ The DHCP server needs *Option 066 – Boot Server Host Name* configured to list the IP address of the ThinManager Server. Redundant ThinManager Servers can be listed, separated by a space.
  See Hybrid IP (DHCP & Static) in section 12.1.3 for another method.
- ❑ Launch the Scope Options page by opening the DHCP Server, highlighting the *Scope Options*, and selecting *Action>Configure Options*.
- ❑ Check the *066 Boot Server Host Name* checkbox, enter the ThinManager Server IP address in the *String value*, and select the *OK* button field.
- ❑ Redundant ThinManager Servers can be defined by listing the IP addresses of both, separated by a space.
- ❑ Set the *Conflict detection attempts* on the DHCP Properties, Advanced tab of the DHCP Server to one or more to prevent duplication of the IP addresses.

12.1.2. Static IP Only

- ❑ ThinManager Ready thin clients can be configured to use static IP by pressing the space bar during the thin client boot when the "*Press Any Key to Configure IP Addresses*" message is displayed.
- ❑ Select "A" to define the terminal IP. Enter the desired IP and select the *Enter* key.
- ❑ Select "B" to define the primary ThinManager Server. Enter the desired IP and select the *Enter* key.
- ❑ Select "C" to define the secondary ThinManager Server if you have redundant ThinManager Servers. Enter the desired IP and select the *Enter* key.
- ❑ Select "S" to save the configuration and continue with the boot process.

12.1.3. Hybrid IP (DHCP & Static)

ThinManager Ready thin clients can be configured to use DHCP to assign the terminal IP address but use a static IP address for the ThinManager Servers. This allows a DHCP server to be used without configuring Option 066.

- ❑ Enter the IP Configuration menu by pressing the space bar during the thin client boot when the "Press Any Key to Configure IP Addresses" message is displayed.
- ❑ Leave "A" alone to keep it using DHCP for the terminal IP address.
- ❑ Select "B" to define the primary ThinManager Server. Enter the desired IP and select the *Enter* key.
- ❑ Select "C" to define the secondary ThinManager Server if you have redundant ThinManager Servers. Enter the desired IP and select the *Enter* key.
- ❑ Select "S" to save the configuration and continue with the boot process.

12.1.4. PXE Boot on ThinManager Compatible thin clients

ThinManager 5 and later include the ability to use many common generic thin clients as ThinManager Compatible thin clients.

❑ Enable the PXE Server in ThinManager or configure your DHCP server to provide the PXE boot information. See section 12.2 for details.

❑ Select a ThinManager Compatible thin client from our compatibility list at www.thinmanager.com/kb/index.php/Supported_Hardware or try a unit you have in hand.

❑ Turn on the thin client and enter the BIOS setup menu (F1, DEL, and F12 are common triggers).

❑ Set the unit to PXE Boot or Boot from LAN, save the settings, restart, and continue with the boot process.

❑ The ThinManager Compatible thin client should get an IP address, the ThinManager Server address, and boot file as described in section 12.2 and connect to ThinManager.

❑ Select a terminal from the list of available configurations or select the Create New Terminal option to launch the Terminal Configuration Wizard in ThinManager to configure the terminal.

12.2. PXE Server Setup

A ThinManager Compatible thin client requires three things to connect to the ThinManager system:

- An IP Address
- The ThinManager Server Address
- The Boot Filename

These can be assigned three ways:

- *Using Standard DHCP Server* - IP Address from your DHCP Server and the rest from the ThinManager Server
- *Using Standard DHCP Server with Boot Options*- All configured in your DHCP Server
- *Not Using Standard DHCP Server* - All configured in the ThinManager Server only

12.2.1. *Using Standard DHCP Server*

PXE Server Options using both the DHCP Server and ThinManager Server

Use this mode when you have a traditional DHCP server. The DHCP server will assign the IP Addresses and ThinManager will provide the PXE Boot information.

❑ Select *Manage* > *PXE Server* from the ThinManager menu to launch the PXE Server Wizard.

❑ Select the *Enable PXE Server* checkbox on the PXE Server Configuration page.

❑ Select the U*sing standard DHCP Server* radio button in the PXE Server Mode on the Network Interface Configuration page. Select your desired network card in the network card drop-down.

❑ Select *Finish* to activate the PXE service.

A thin client set to PXE boot will make a DHCP and PXE request. The DHCP server will respond to the DHCP request and will provide the IP address to the client. ThinManager will respond to the PXE request and provide the ThinManager IP address and the boot filename.

12.2.2. *Using Standard DHCP Server* on this Machine

PXE Server Options when the ThinManager Server has the DHCP Role installed

Use this mode when you have a traditional DHCP server installed on the same computer as ThinManager. The DHCP server will assign the IP Addresses and ThinManager will provide the PXE Boot information. **Port UDP-4011 needs to be open on this computer.**

- ❑ Select *Manage* > *PXE Server* from the ThinManager menu to launch the PXE Server Wizard.
- ❑ Select the *Enable PXE Server* checkbox on the PXE Server Configuration page.
- ❑ Select the U*sing standard DHCP Server on the machine* radio button in the PXE Server Mode on the Network Interface Configuration page. Select your desired network card in the network card drop-down.
- ❑ Select *Finish* to activate the PXE service.

A thin client set to PXE boot will make a DHCP and PXE request. The DHCP server will respond to the DHCP request and will provide the IP address to the client. ThinManager will respond to the PXE request and provide the ThinManager IP address and the boot filename.

Note: Port UDP-4011 needs to be open on this computer.

12.2.3. *Using Standard DHCP Server with Boot Options* (PXE Disabled)

PXE Server Options using DHCP Server only

The DHCP Server can provide all the PXE Boot options for ThinManager Compatible thin clients.

- ❑ Select *Manage* > *PXE Server* from the ThinManager menu to launch the PXE Server Wizard.
- ❑ Select the *Enable PXE Server* checkbox on the PXE Server Configuration page.
- ❑ Select the *Using standard DHCP Server with Boot Options* radio button in the PXE Server Mode on the Network Interface Configuration page.
- ❑ Select *Finish* to activate the PXE service.
- ❑ Go to your DHCP Server and open the DHCP options.
- ❑ Set Option 066, Boot Server Host Name, to the IP address of the ThinManager Server.
- ❑ Set Option 067, Boot Filename, to **`acpboot.bin`**.

A thin client set to PXE boot will make a DHCP and PXE request and the DHCP server will respond with all the information. It will provide an IP Address, the ThinManager IP address (option 066), and the boot filename (option 067).

12.2.4. *Not Using Standard DHCP Server*

PXE Server Options using ThinManager Server only

The ThinManager Server can provide all the PXE Boot options for ThinManager Compatible thin clients.

- ❑ Select *Manage* > *PXE Server* from the ThinManager menu to launch the PXE Server Wizard.
- ❑ Select the *Enable PXE Server* checkbox on the PXE Server Configuration page.

- ❑ Select the *Not using standard DHCP Server* radio button in the PXE Server Mode on the Network Interface Configuration page. Select your desired network card in the network card drop-down.
- ❑ Set a range of available IP addresses on the IP Address Range Configuration page by using the *Add* button to launch the IP Range Page. These IP addresses must not conflict with assigned IP addresses.
- ❑ Select *Finish* to activate the PXE service.

A thin client set to PXE boot will make a DHCP and PXE request and ThinManager will respond and provide all the information. It will provide an IP Address from the defined range, the ThinManager IP address, and the boot file.

Note: A ThinManager PXE server will only supply IP addresses to PXE boot devices. It will ignore DHCP requests from non-PXE devices.

12.2.5. Multiple PXE Servers

If you have multiple sets of PXE servers on the network this can cause troubles as you will not be sure of which PXE server will respond to the thin client PXE request. ThinManager has a method of limiting what terminals a PXE server will respond to.

Note: A synchronized pair is fine as only the master thinserver will respond. This is about multiple sets of ThinManager Servers.

- ❑ Activate the PXE Server on one ThinManager Server when you are ready to add new thin clients to that ThinManager Server.
- ❑ Select the *Allow New PXE clients* checkbox on the Network Interface Configuration page of the PXE Server wizard.
- ❑ Add the clients as needed.
- ❑ When you have added the clients you need, un-select the *Allow New PXE clients* checkbox. This let configured thin clients use this ThinManager Server but will prevent new clients from connecting to it.
- ❑ Configure the next ThinManager Server, enable the PXE server, and add the hew PXE clients. Un-select the *Allow New PXE clients* checkbox when done.
- ❑ Only check the *Allow New PXE clients* checkbox when you are doing replacements or adding new terminals. Un-check it when you are done.

13. Packages and Firmware

ThinManager 6.0 introduced the deployment of the firmware and modules as a package. Different versions of the package can be assigned to classes of terminals or individual terminals. This allows legacy hardware to keep a version that works for it while new hardware can use newer package versions to take advantage of new features.

Legacy hardware can be assigned the baseline Package 5 while newer terminals can use Package 6 or later.

Changing Package Configuration

- ❑ Open the Package Manager by selecting *Manage* > *Packages* from the ThinManager menu bar.

- ❑ You can change the default package for each make and model in the *Model Specific Default Package* drop-downs.
- ❑ Selecting the *Allow settings of the Package in the Terminal Configuration* checkbox will allow you to change the default package for each individual terminal on the Terminal Hardware page of the Terminal Configuration Wizard.

14. Failover and Instant Failover

14.1. Definitions

14.1.1. Failover versus Redundancy

- ❑ **Redundancy** describes having two ThinManager Servers so that a ThinManager Ready thin client can always find a ThinManager Server to boot from and receive its configuration.
- ❑ **Failover** describes having multiple Remote Desktop Servers that the thin client is assigned to so that it always has a Remote Desktop Server it can connect to and start a session.

14.1.2. Failover Explained

- ❑ In Failover, a ThinManager Ready thin client is assigned to a list of Remote Desktop Servers and will connect to the first one on the list.
- ❑ The ThinManager Ready thin client will detect if that Remote Desktop Server fails and will connect to the next Remote Desktop Server on the list. This normally takes 10-20 seconds.
- ❑ Once the thin client connects to the backup Remote Desktop Server it will login and launch its application. The application launch can take 1 second to 3 minutes depending on the application and the Remote Desktop Server load.
- ❑ All versions of ThinManager provide the failover function for free.

14.1.3. Instant Failover Explained

- ❑ Instant Failover configures the ThinManager Ready thin client to connect to two Remote Desktop Servers and launch a session on each at the same time.
- ❑ The terminal should be configured to auto-login and an AppLink display client to gain the full benefits of Instant Failover.
- ❑ The sessions are cascaded on the terminal monitor.
- ❑ A failure of the primary Remote Desktop Server will cause the terminal to switch to the backup session. Since the session and application are already initialized this takes just a second.
- ❑ If the terminal is assigned to three or more Remote Desktop Servers the terminal will then start a second session on the next available Remote Desktop Server.
- ❑ Instant Failover can be configured so that the user can switch between active sessions using the *CTL + F9* hotkey.
- ❑ The Instant Failover function is included in the ThinManager Terminal Connection license. It may require a second application license since you will have two active sessions.

14.2. Failover Configuration

Standard failover is configured by providing the ThinManager Ready thin client a list of Remote Desktop Servers for connection.

- ❑ Failover is configured within a Display Client group by adding two or more Remote Desktop Servers to the *Selected Remote Desktop Servers* list on the Display Client Members page of the Terminal Services Display Client Wizard.
- ❑ Open the Display Client Wizard by selecting the Display Client icon in the tree selector at the bottom of the ThinManager tree and double-clicking on the Display Client icon in the ThinManager tree.
- ❑ Add two or more Remote Desktop Servers to the *Selected Terminal Servers* list on the Display Client Members page.
- ❑ The terminal will connect to the Remote Desktop Servers in the order listed unless the Display Client has been configured for SmartSession.
- ❑ Terminals will connect to the Remote Desktop Servers in a SmartSession group based on their load, from the lightest to the heaviest load.
- ❑ Selecting the *Enforce Primary* checkbox on the Terminal Services Display Client Group Options page of the Display Client Wizard activates the Enforce Primary function. This keeps the terminal pointed at the primary remote desktop server whenever possible. Enforce Primary is not available for SmartSession groups.

14.3. Instant Failover Configuration

Instant Failover enables a terminal to login and create a session on two Remote Desktop Servers so that the backup session is initialized for a quick switch.

- ❑ Instant Failover is configured within a Display Client for terminals that use Display Clients.
- ❑ Open the Display Client Wizard by selecting the Display Client icon in the tree selector at the bottom of the ThinManager tree and double-clicking on the Display Client icon in the ThinManager tree.
- ❑ Navigate to the Terminal Services Display Client Options page of the Display Client Wizard and select the *Instant Failover* checkbox.
- ❑ Select two or more Remote Desktop Servers for the Display Client by adding them to the *Selected Terminal Servers* list on the Display Client Members page of the Display Client Wizard. Select the *Finish* button to accept the changes.
- ❑ Add the Instant Failover Display Client to a terminal by opening the Terminal Configuration Wizard for the terminal by double-clicking on it in the ThinManager Tree.
- ❑ Expanding a Display Client configured for Instant Failover will show the Remote Desktop Servers that are assigned to the group. A green lightning bolt shows the active session that is on top of the screen while a yellow lightning bolt will show the backup session that is hidden.
- ❑ The Hotkey Configuration page in the Terminal Configuration Wizard allows hotkey options for Instant Failover to be configured.

15. MultiSession

MultiSession allows a user to run several Display Client sessions on one terminal. These will be cascaded on the terminal.

MultiSession, when used with AppLink, is an easy way to deploy desired applications while preventing access to unauthorized programs.

Adding two or more Display Clients to a terminal enables MultiSession.

15.1. Configuring the Terminal for MultiSession

❑ MultiSession requires the use of Display Clients on terminals. Select *Use Display Clients* on the Terminal Server Specification page of the Terminal Configuration Wizard.

❑ Select two or Display Clients by moving them to the *Selected Display Client List* on the Display Client Selection page of the Terminal Configuration Wizard.

❑ The terminal needs a method to switch between sessions. This is configured on the Terminal Interface Options and Hotkey Configuration pages of the Terminal Configuration Wizard. See section 15.2.

❑ If the terminal is set to auto-login then it will auto-login to the MultiSession sessions. An individual Display Client can be set to force manual logins for authentication by unselecting the *Allow Auto-Login* checkbox on the Group Options page of the Display Client Wizard.

❑ A Display Client can use a different login than the terminal by using the *Override* button on the Display Client Selection page of the Terminal Configuration Wizard.

15.2. Switching Between Sessions

❑ Each terminal that uses MultiSession should be configured to switch between sessions on the Terminal Interface Options and the Hotkey Configuration pages of the Terminal Configuration Wizard. At least one method must be used.

❑ **Terminal Interface Options** - *Show Selector on Terminal* will display a drop-down menu on the terminal's screen. The default auto-hide mode can be removed by selecting the *Selector Options* button.

❑ **Terminal Interface Options** – *Enable Tiling* will tile the sessions to allow a visual selection of a session. See section 23.4.

❑ **Terminal Interface Options** - *Screen Edge Selection* will switch between sessions when the mouse is moved to the left or right edge.

❑ **Hotkey Configuration** - *Enable Display Client Hotkeys* will allow keystrokes to switch the session displayed. The default *CTL+Page Up/Down* can be changed by selecting the *Change Hotkeys* button.

16. SmartSession

SmartSession provides load balancing among designated Remote Desktop Servers.

16.1. Configuring the Remote Desktop Server Display Server

- ❑ ThinManager needs an administrative account entered in the Log In Information fields of the Remote Desktop Server Name page of the Terminal Server Wizard. This allows ThinManager access to the Remote Desktop Server to pull memory, CPU, and session data to calculate the server load.
- ❑ Remote Desktop Servers are configured to use SmartSession by selecting the *Available for Display Clients using SmartSession* checkbox on the Terminal Server Capabilities page of the Terminal Server Wizard.
- ❑ The frequency of the data polling is set on the Data Gathering page of the Terminal Server Wizard.
- ❑ The SmartSession Configuration page allows the ranges of the CPU, Memory, and Session count to be adjusted. (The defaults are your friends).

16.2. Configuring the SmartSession Display Client

- ❑ Terminal Services Display Clients can be configured to use SmartSession for load balancing.
- ❑ A Display Client becomes load balanced when the *SmartSession* checkbox on the Terminal Server Display Client Options page of the Display Client Wizard is selected.
- ❑ Only Remote Desktop Servers that have been configured to use SmartSession will be available for selection on the Display Client Members page of the Display Client Wizard. If a server isn't visible open the Terminal Server Wizard and select the *Available for Display Clients using SmartSession* checkbox.
- ❑ ThinManager polls the SmartSession Remote Desktop Servers and calculates a Server Rank number based on the CPU, Memory, and Session resources used. A terminal connecting to a Display Client using SmartSession will be sent by ThinManager to the Remote Desktop Server with the most available resources as defined by the lowest server rank number.
- ❑ The weight of the SmartSession values can be adjusted on the SmartSession Settings page of the Display Client Wizard.
- ❑ The Server Rank number for the SmartSession servers can be displayed by highlighting a Display Client using SmartSession in the ThinManager tree and selecting the Server Rank tab in the Details pane.

16.2.1. SmartSession Queuing

- ❑ SmartSession Queuing allows ThinManager to control the rate that terminals connect to the Remote Desktop Servers to prevent the server CPU from becoming overloaded and slowing down the session connection process.
- ❑ Queuing is configured on the SmartSession Settings page of the Display Client Wizard for display clients using SmartSession.
- ❑ When a CPU reaches the maximum CPU Utilization, as defined on the SmartSession Configuration page of the Terminal Server Wizard, ThinManager will delay other terminals

from connecting until the CPU utilization returns to a normal level or the maximum *Queuing Time* on the SmartSession Settings page of the Display Client Wizard is reached.

- ❑ A SmartSession Display Client can contain a single Remote Desktop Server to control the loading of that server as clients connect.

17. Modules

Modules are optional features or programs that aren't needed to run a basic thin client but can be added to expand the functions. These include screen savers, touch screen drivers, sound modules, and others.

- ❑ Modules are included in the firmware packages with the install and service packs.
- ❑ Modules are added to the terminal on the Module Selection page of the Terminal Configuration Wizard.
- ❑ Select the *Add* button to add a module.
- ❑ Select the desired module from the list and select the *OK* button. The modules can be sorted by module type to filter the selections.
- ❑ Some modules have configurable parameters. To change them highlight the added module in the Installed Module window of the Module Selection page and select the *Configure* button to launch the Module Properties window.
- ❑ Highlight the desired parameter to activate the *Value* field. Use the drop-down to change the setting then select the *Set* button to apply the parameter change. Select the *Done* button when all the parameters are set.
- ❑ Select the *Finish* button to apply the changes and restart the thin client to send the configuration change to the thin client.

17.1. Touch Screens

- ❑ Adding the appropriate Touch Screen module on the Module Selection page of the Terminal Configuration Wizard activates touch screens.
- ❑ The module needs to match the make of the touch screen controller. The make of the monitor is incidental. There is one universal USB Touch Screen Module for USB touch screens and a dozen different serial touch screens.
- ❑ Touch screen parameters can be changed by highlighting the module on the Module Selection page of the Terminal Configuration Wizard and selecting the *Configure* button.
- ❑ Touch screens can be configured so that a touch that is held will either count as a right click or launch an on-screen keyboard. It can also launch the calibration program.
- ❑ Highlighting the terminal in the ThinManager tree and selecting *Tools> Calibrate Touch Screen* on the menu can calibrate the terminal.
- ❑ A MultiMonitor thin client will need a touch screen module for each touch screen used. Selecting the *Configure* button when the module is highlighted sets the monitor number. A different touch screen can be applied to each monitor, if needed.

18. Virtualization

18.1. Virtual ThinManager Server

- ❑ ThinManager can be installed on a virtual machine and run as if on a physical machine.
- ❑ Moving, copying it, or cloning the virtual machine may change the installation ID and require a license reactivation each time the virtual machine is changed.

18.2. Virtual Remote Desktop Servers

- ❑ Virtual Remote Desktop Servers can be defined in the Display Servers/Remote Desktop Servers branch of the ThinManager as if it was a regular Remote Desktop Server. See Section 9.1.

18.3. VCenter Servers

ThinManager allows you to connect to a VMWare vCenter Server and manage the virtual machines from within ThinManager.

- ❑ Build a VMWare vCenter Server using the ESXi hypervisor independent of ThinManager.
- ❑ Launch the VCenter Wizard by selecting the VCenter icon in the tree selector at the bottom of the tree, right clicking on the VCenter Servers branch of the tree, and selecting *Add VCenter Server* to launch the VCenter Server Property.
- ❑ Enter a name and the IP address for your VCenter Server in the appropriate fields. Enter an administrative account in the Log In Information fields.
- ❑ It may take a few minutes to connect to the VCenter Server. You can highlight the VCenter Server in the tree and select the Recent Tasks to monitor the progress.
- ❑ Once ThinManager has connected to the VCenter it will populate the tree and show the installed virtual machines,

Note: If you get a permission error make sure that your Windows group has been granted the VMWare management permissions on the ThinManager Security Groups page of the ThinManager Server Configuration Wizard.

18.3.1. Power Operations

Once ThinManager has populated the VCenter with the installed virtual machines you can right-click on virtual machines to control them.

- ❑ *Power On* – Turns on a stopped or suspended virtual machine.
- ❑ *Power Off* – Turns off a stopped or suspended virtual machine.
- ❑ *Suspend* – Suspends a running virtual machine and stores the state.
- ❑ *Reset* – Cycles power to the virtual machine to restart the virtual machine.

18.3.2. Snapshot

A Snapshot is a record of the current state of the virtual machine that allows you to preserve a record of the virtual machine. This is a handy tool to use before making major changes to the virtual machines because it allows you to restore a previously functioning state.

- ❑ *Take Snapshot* – Captures and stores the state of the virtual machine.

❑ *Revert to Current Snapshot* – Reapplies the stored state of a previously saved virtual machine.

❑ *Snapshot Manager* – Launches the Snapshot management tool.

18.3.3. Other VCenter Functions

❑ *Rename* – Allows the virtual machine to be renamed.

❑ *Remove from Inventory* – Removes the virtual machine from the tree without deleting the files.

❑ *Delete* – Removes the virtual machine from the tree AND deletes the file system.

19. WinTMC

WinTMC is a Windows client that can be installed on PCs but is controlled through ThinManager.

19.1. WinTMC Advantages

❑ WinTMC can convert PC to a terminal services client reducing local maintenance of applications.

❑ PC becomes managed by ThinManager, allowing failover, Instant Failover, MultiSession, and SmartSession functions.

❑ Applications that aren't terminal services compliant like AutoCAD can be run locally while gaining the management benefits from running other applications on Remote Desktop Servers.

19.2. WinTMC Disadvantages

❑ The PC that WinTMC is installed on still requires installation and maintenance of its hard drive and operating system.

❑ Modules don't work because ThinManager doesn't control the operating system. These functions must be setup and controlled using the PC operating system. These include:

- Touch screen drivers
- Sound drivers
- Local storage
- Mouse
- Screen savers

Instant Failover and TermSecure are supported by WinTMC v2.0 and later (Black & Blue icon). MultiMonitor is supported on PCs with multiple monitors.

19.3. WinTMC Installation

Note: WinTMC should not be installed on the ThinManager Server due to a conflict over port 2031. It is meant to be installed on PCs.

❑ Install the WinTMC application on the desired PC.

❑ Using the *Add/Remove Programs* tool is recommended for installations.

❑ WinTMC allows two options during installation:

- WinTMC is the WinTMC client needed to turn the PC into a terminal.

- WinTMC Shadow Service is needed to shadow a WinTMC client. If this program is installed, the PC can be shadowed from ThinManager even if the WinTMC client is inactive.

19.4. WinTMC Configuration on the Client

❑ Once installed, launch the WinTMC program from the Windows Start menu or from a desktop icon.

❑ Select the *Configure* button on the splash screen when it is first run.

❑ Enter the IP address of the ThinManager Server(s) in the *Enter new ThinManager Server Name or IP Address* field and select the *Add* button.

❑ Select the *OK* button to connect to the ThinManager Server.

❑ The Terminal Replacement Dialog window will display any off-line terminals and a *Create a new terminal* button. Select a pre-created terminal to assume an established configuration or select the *Create a new terminal* button to launch the Terminal Configuration Wizard for that WinTMC client on the ThinManager Server.

19.5. WinTMC Configuration in ThinManager

❑ Pre-create a WinTMC client by launching the Terminal Configuration Wizard by selecting *Edit>Add Terminal* from the ThinManager menu bar. The configuration is similar to thin clients with a few exceptions.

❑ Add the computer name for the terminal name in the Terminal Name page of the wizard.

❑ Select *GENERIC* for the Make/OEM and *WinTMC* for the Model on the Terminal Hardware page of the wizard.

❑ Select the video resolution on the Video Resolution page. The default is *FullScreen*.

❑ Select the *Finish* button when the configuration is complete.

20. Shadowing

Shadowing allows a user to view a terminal. It is available in three forms:

- Terminal Shadowing through ThinManager.
- Terminal-to-Terminal shadowing through Terminal Shadow Display Clients.
- VNC Server shadowing through the VNC Display Client.

20.1. ThinManager Shadowing

❑ Terminal Shadowing through ThinManager allows an administrator to see what is displayed on a terminal's screen.

❑ Highlighting the terminal in the ThinManager tree and selecting the *Shadow* tab on the Details pane will shadow a terminal.

❑ To shadow a user must be either a member of the Administrators user group in Windows or a member of a Windows user group that was granted permission to shadow on the ThinManager Security Groups page of the ThinManager Server Configuration Wizard.

❑ Shadow settings are configured on the Terminal Options page of the Terminal Configuration Wizard. The terminal can be set to block shadowing (*NO*), ask user permission first (*ASK*), warn the user first (*WARN*), or shadow immediately (*YES*)

❑ Interactive Shadow allows the administrator to control the shadowed session. This can be allowed/disallowed on the Terminal Options page of the Terminal Configuration Wizard. It can also be turned off/on by selecting *RemoteView>Interactive Shadow* on the ThinManager menu.

❑ WinTMC requires that the WinTMC Shadow Service be installed on the client PC. Once the PC has been connected to ThinManager the PC can be shadowed even if WinTMC is not running.

❑ The WinTMC shadow service uses Port 5900. If this is in conflict with another program it can be changed on the Shadow Configuration page of the ThinManager Server Configuration Wizard.

20.2. Terminal Shadow Display Client

❑ A Terminal Shadow Display Client can be configured to show a specific terminal or present a list of terminals for the operator to choose from.

❑ The use of Terminal-to-Terminal shadowing through Terminal Shadow Display Clients allows any user on a terminal with the Terminal Shadow Display Client to shadow a terminal that is in the Terminal Shadow Display Client. See section 10.4 for configuration.

20.3. VNC Display Client

❑ A VNC Display Client can be configured to show a specific VNC Server or present a list of VNC Servers for the operator to choose from.

❑ The use of Terminal-to-Terminal shadowing through VNC Display Clients allows any user on a terminal with the VNC Display Client to shadow a VNC Server that is in the VNC Server Display Client. See section 10.7 on page 27 for configuration.

21. MultiMonitor

❑ MultiMonitor allows a single ThinManager Ready thin client to have up to 7 monitors attached at the same time.

❑ The monitors can be combined into larger “spanned” screens (double-wide/triple-wide/etc.) or run as individual single-monitor “screens”.

❑ Each monitor can be of a different video resolution or use a different touch screen. However monitors that are combined to form a spanned screen must have the same resolution.

❑ MultiMonitor required a MultiMonitor license in early versions of ThinManager. This functionality is included in the XLi and XLr License.

❑ MultiMonitor requires the use of Display Clients.

❑ Microsoft prevents you from running the same application multiple times with the same user account so use the *Override* button configure a second and third version of an application to login with a different user account.

21.1. Configuring MultiMonitor

❑ MultiMonitor is configured in the Terminal Configuration Wizard.

❑ Terminal Hardware page– Select the *Make* and *Model* of the MultiMonitor ThinManager Ready thin client.

❑ Terminal Server Specification page – Select *Use Display Clients.*

❑ Terminal Mode Selection page – Select *Enable MultiMonitor*.

❑ MultiMonitor Video Settings page – Select the *Number of Monitors* and the video resolution of each.

❑ Monitor Layout page – Select the physical layout of the monitors in the *Choose your monitor layout* window. The Main Monitor is the monitor that will display login and message windows.

❑ Monitor Layout page – Select how the monitors will be combined in the *Choose your screen layout* window. Choose whether the monitors are combined as “spanned” or kept individual as “screened”. The *TermSecure Initial Screen* is the monitor that will display TermSecure login and message windows if TermSecure is used.

❑ Display Client Selection page – Select which Display Client(s) will be displayed on which screen by highlighting the desired Display Client and selecting the appropriate arrow.

❑ Screen Options page – This configures options like the ability to move sessions, which monitor in a spanned group is the main monitor, and how MultiSession switching should take place.

❑ Hotkey Configuration page – This configures hotkey options for MultiSession and SessionTiling.

21.2. MultiMonitor WinTMC Clients

❑ MultiMonitor is supported by WinTMC clients that are running on a computer with two or more monitors.

❑ The WinTMC client can be configured to use “spanned” screens (double-wide/triple-wide/etc.) or run as individual single-monitor “screens”.

21.3. MultiStation

MultiStation extends MultiMonitor capabilities to allow a keyboard and mouse to be added to each MultiMonitor screen, allowing on thin client device to support several operators or users.

❑ Add a keyboard and mouse for each station, if desired. You can use a USB hub if needed.

❑ Check Enable MultiMonitor and Enable MultiStation on the Terminal Mode Selection page of the Terminal Configuration Wiz ard. Configuration is similar to MultiMonitor.

❑ Configure the thin client with the number of monitors, spanning, display clients, etc. as with MultiMonitor.

❑ Use the Override button on the Display Client Selection page to assign multiple user logins or leave the Login blank to force manual logins.

❑ The Station Option window on the Screen Options page allows you to turn off the keyboard and mouse. This might be needed for a touch screen only station.

❑ A Touch Screen module needs to be added for each touch screen used. The module lets you specify which screen it is applied to.

22. Virtual Screens

Virtual Screens is a feature that allows you to divide a screen into separate overlays. It allows you to deliver MultiMonitor functionality to a single physical monitor.

The method of creating the Virtual Screen overlays follows the methods of the Camera Display Clients.

22.1. Virtual Screen Display Client Wizard

- ❑ Launch the Virtual Screen Configuration Wizard by selecting the Display Client icon at the bottom of the ThinManager tree, right clicking on the Virtual Screen branch, and selecting ***Add Display Client***.
- ❑ Give the Virtual Screen Display Client a name on the *Client Name* page. You must add an overlay using the pre-defined templates or the custom overlays.

22.2. Pre-Defined Templates

The Virtual Screen Display Client has pre-defined overlay templates.

- ❑ Select a template from the *Choose Layout* drop-down on the *Select or Create Virtual Screen* page of the Display Client wizard.
- ❑ As you navigate through the wizard you will be able to add one or more display clients to each overlay, similar to adding cameras to overlays. Use the *Add* button on the Virtual Screen Configuration page to get the list of available display clients.
- ❑ The *Screen Options* button will open the *Virtual Screen Option* window that allows you to configure settings like Tiling and the Group Selector.

22.3. Adding a Virtual Screen to a Terminal

Virtual Screen Display Clients are added to the terminal on the *Display Client Selection* page of the Terminal Configuration Wizard like other display clients.

22.4. Custom Overlays

The Virtual Screen Display Client allows you to create overlays of any size and configuration.

- ❑ Launch the Virtual Screen Configuration Wizard by selecting the Display Client icon at the bottom of the ThinManager tree, right clicking on the Virtual Screen branch, and selecting ***Add Display Client***.
- ❑ Give the Virtual Screen Display Client a name on the *Client Name* page.
- ❑ Select *Custom* from the *Choose Layout* drop-down on the *Select or Create Virtual Screen* page of the Display Client wizard.
- ❑ Select the *Add* button to launch the *Custom Overlay* window.
- ❑ The *Custom Overlay* window allows you to enter the dimensions of the overlay. *Left* and *Top* are the location of the top left corner of the overlay. *Width* and *Height* control the size of the overlay.
- ❑ Add additional overlays if needed with the *Add* button.
- ❑ As you navigate through the wizard you will be able to add one or more display clients to each overlay, similar to adding cameras to overlays. Use the *Add* button on the Virtual Screen Configuration page to get the list of available display clients.
- ❑ The *Screen Options* button will open the *Virtual Screen Option* window that allows you to configure settings like Tiling and the Group Selector.

22.5. Display Client Override on Virtual Screens

Virtual Screens do not allow an override in the Terminal Configuration Wizard like a normal display client.

- ❑ Open the *Display Client Wizard* by double clicking on the *Virtual Screen* under the terminal in the Terminal tree of ThinManager.
- ❑ Navigate to the *Virtual Screen Configuration* page. A *Terminal Override* button is available.
- ❑ Highlight the display client you want to alter and select the *Terminal Override* button.
- ❑ Select the *Override* checkbox of your choice to apply the changes to the settings and select the *OK* button.

23. Additional Topics

23.1. Reports

- ❑ ThinManager has reports that can be displayed to show events and configurations.
- ❑ Selecting *View>Reports* will allow the administrator to select what reports will be displayed.
- ❑ Reports are shown by highlighting an item in the ThinManager tree and selecting the Report tab in the Details pane.
- ❑ New reports can be added by selecting *Install>Reports>Install* in the ThinManager menu. Each report has a Report Template and a SQL Query component.
- ❑ Reports can be run automatically and saved as *.csv or *.html files using the Scheduler on the System Schedule page of the ThinManager Server Configuration Wizard.
- ❑ The Report tab can be printed by selecting *View>Print* from the menu bar.

23.2. Event Log

- ❑ ThinManager has an event log that can be displayed by highlighting an item in the ThinManager tree and selecting the *Event Log* tab in the Details pane.
- ❑ The Event Log is configured on the Historical Logging page of the ThinManager Server Configuration Wizard. The events to track and the duration of the event log are configurable.
- ❑ The Event Log can be backed up automatically using the Scheduler on the System Schedule page of the ThinManager Server Configuration Wizard.

23.3. Security

ThinManager is designed to increase security.

- ❑ Only administrators, or members of Windows user groups that have been given permission on the ThinManager Security Groups page of the ThinManager Server Configuration Wizard, can run ThinManager.
- ❑ Terminals can be configured to login automatically. This obscures the username and password so that a user doesn't know the account credentials to try to access other resources.
- ❑ AppLink can limit a user to specific programs and block access to the desktop or unauthorized programs.

❑ The Key Block module can be set to trap undesired keystrokes.

❑ Relevance can be used to provide addition access control and management.

❑ Relevance can control who has access and where they can access the applications.

❑ USB flash drives are disabled by default. An administrator must allow their use with the USB Flash Drive module.

23.4. Scheduling Configuration Backups

❑ The *Schedule* button on the System Schedule page of the ThinManager Server Configuration Wizard allows the configuration to be backed up or reports run automatically on a schedule.

❑ A weekly backup the configuration with System Schedule tool is recommended.

❑ The *Schedule* button on the Terminal Options page of the Terminal Configuration Wizard also allows a terminal to be disabled, enabled, or rebooted automatically on a schedule.

23.5. SessionTiling

❑ The sessions started using MultiSession can be tiled on a terminal to display all sessions at once.

❑ This might be to monitor all the sessions at once or as a visual selection aid on terminals with touch screens that lack a keyboard for hotkey switching.

❑ Selecting the *Enable Tiling* checkbox on the Terminal Interface Options page of the Terminal Configuration Wizard enables SessionTiling. The *Tiling Options* button allows the tiling parameters to be configured.

24. Active Directory

ThinManager 8 added Active directory integration to ThinManager. The ThinManager Server must be a member of the domain to use Active Directory. Active Directory actions require a domain administrator account.

❑ The use of Active Directory can be turned off by selecting *Manage> Active Directory >Settings* and unchecking the *Enable Active Directory Integration* check box on the Active Directory System Settings window.

24.1. Using Active Directory for User Accounts

Each *Username* field has a *Search* button that allows you to access Active Directory Users.

❑ Select the *Search* button at a *Username* field to launch the Search for AD User window.

❑ Select the *Locations* button to pick the AD location to search.

❑ Select the *Search* button to load the available accounts. Select an account and select OK. The user will be entered in the Username field.

❑ Enter the password for the account. You can set the password requirement by selecting the *Password Options* button. The *Resync Account* button on the Password Maintenance Options window will allow you to send the password entered in ThinManager to the Active Directory. It will prompt you to enter Domain Administrator credentials for the password update.

❑ Selecting the *Verify* button will check that the username and password are valid.

24.1.1. Manage Active Directory Accounts

ThinManager provides tools for managing Active Directory accounts.

- ❑ Select *Manage> Active Directory >Manage Accounts* to open the Manage Active Directory Accounts window. The window contains the list of accounts added to terminals through Active Directory.
- ❑ Highlight a user account and select *Edit* to open the Password Maintenance Options window to allow configuration of password length and time limits.
- ❑ The *Convert* button will allow manually added domain accounts from previous versions to be managed by ThinManager for password updates.

24.2. Using Active Directory with Access Groups

ThinManager can import Active Directory accounts for use with Relevance Users. This is based on the TermSecure User wizard from ThinManager.

- ❑ Launch the Relevance User Configuration Wizard by selecting the User icon in the Tree Selector at the bottom of the tree, right clicking on the Relevance User branch of the tree, and selecting *Add User*.
- ❑ Check the *Active Directory User* checkbox on the Relevance User Information page and select the *Search* button to launch the *Search for AD User* window. This will create a Relevance User with the Active Directory account.
- ❑ Select the *Locations* button to pick the AD location to search. Select the *Search* button to load the available accounts. Select an account and select *OK*. The user will be entered in the Username field.
- ❑ Enter the password for the account in the *Password* field of the Windows Log In Information page. The *Resync Account* button on the Password Maintenance Options window will allow you to send the password entered in ThinManager to the Active Directory. It will prompt you to enter Domain Administrator credentials for the password update.
- ❑ The Password Maintenance settings allow you to control password length and duration.
- ❑ Selecting the *Verify* button will check that the username and password are valid. The rest of the wizard is the same as the TermSecure User wizard.

24.3. Password Management with Active Directory

ThinManager can help manage Active Directory password rules.

24.3.1. Password Settings

- ❑ Select *Manage>Settings* to open the Active Directory System Settings window. You can set the
  - Password Change Interval
  - Minimum Password Length
  - Maximum Password Length

24.3.2. Synchronize Passwords

ThinManager can send new passwords to the Active Directory. ThinManager does not extract passwords from the Active Directory.

- ❑ Select Manage > Active Directory > Synchronize Passwords to open the Synchronize Active Directory Password window. This will contain the Active Directory users that you have used in ThinManager.
- ❑ Highlight an account, enter a new password in the Password field, and select the Set Password button. This will send the new pass word to the Active Directory and update it.
- ❑ The Generate Passwords checkbox allows ThinManager to generate a hidden password that is unknown to the operator but stored in ThinManager.

25. Relevance Overview

Relevance extends the power of ThinManager to provide Location based application deployment. It provides Who, What, and Where to application control and deployment.

Relevance has several features and functions. These include:

- **Relevance User Services** – This is permission based deployment of applications. This is an extension of the TermSecure functionality from previous versions of ThinManager. See Section 26 on page 48.
- **Relevance Location Services** – This is Location based deployment. Applications can be
- **Mobile Devices** – Relevance allows mobile devices to interact with tethered terminals or to become the terminal in untethered Locations. See Section 28 on page 58.
- **Location Resolvers** – The Resolvers are tied to the Location and allow control through Location. See Section 29 on page 59.
- **Fencing** – This is a critical function that prevents mobile applications from running in unauthorized locations, like a boiler application in a cafeteria. See Section 30 on page 62.

26. Relevance User Services

The first feature of Relevance is controlling access to applications and locations based on permission and group membership. This is an expansion, and replacement, of TermSecure from older versions.

Relevance User Services has two functions; the first is to hide an application from an unauthorized person, as covered in section 26.1. The second is to deploy a user-specific application to a user anywhere in the system, as covered in section 26.2.

26.1. Hiding Applications with Permissions

The steps to control Display Client application deployment with Access Groups and Permissions are:

- Define the Permissions as Access Groups.
- Apply Permissions to Display Client applications.
- Create Users who can access applications and apply the Permission to them.
- Apply Display Clients to Terminals.
- Login to terminal to access the hidden application.

26.1.1. Define the Permissions as Access Groups

- ❑ Select ***Manage > Access Groups*** from the ThinManager menu to open the **Access Groups** window.
- ❑ Select the ***Add*** button to open the **Access Group** dialog box.
- ❑ Enter a group name, like Maintenance, Supply, Support, or Supervisors, in the ***Enter Group Name*** field and click the ***OK*** button to add the group.
- ❑ Repeat and needed to add additional groups.
- ❑ Click the ***OK*** button to close the **Access Group** window, saving the groups.

26.1.2. Apply Permissions to Applications

- ❑ Select the **Display Client** icon on the ThinManager tree to open the **Display Client** branch.
- ❑ Double click on the display client you want to control with permissions to open the **Display Client Wizard**.
- ❑ Select the ***Permissions*** button on the **Client Name** page to open the **Permissions** window.
- ❑ Remove the ***Unrestricted*** group from the ***Member of*** list and add the group you want to grant access to.
- ❑ Select the ***OK*** button to close the **Permission** window.
- ❑ Select the ***Finish*** button to accept the changes and close the **Display Client Wizard**.
- ❑ Repeat as needed.

26.1.3. Create Relevance Users Who Can Access Applications

- ❑ Select the **User** icon at the bottom of the ThinManager tree to open the **Relevance Users** branch of the tree.
- ❑ Right click on the ***Relevance Users*** branch and select ***Add User*** to open the **Relevance User Information** wizard.
- ❑ Enter a user name and password in the ***User Name*** and ***Password*** fields. You can select an existing user from Active Directory by checking the *Active Directory User* checkbox and selecting the *Search* button. This will allow you to use a Windows domain account for the Relevance user.

Note: The Relevance User account does not need to match a Windows account. It can be a Relevance/ThinManager only account.

- ❑ Apply group membership by selecting the ***Permissions*** button and launching the **Relevance Access Groups** window.
- ❑ Move the access group you want the user to join into the ***Member of*** list and select the ***OK*** button.
- ❑ If you are using the account to access the applications on the locations and not assigning specific display clients to the user you can select the ***Finish*** button and save the user.

26.1.4. Use Permissions to Control Display Client Access

- ❑ Select the **Location** icon in the ThinManager tree to open the **Location** branch.
- ❑ Double click on the location you want to control with permissions to open the **Location Configuration Wizard**.
- ❑ Navigate to the **Display Client Selection** page. Add the display clients that have permissions added to the ***Selected Display Client*** list.
- ❑ Select ***Finish*** to accept the changes.
- ❑ Select the **Terminal** icon in the ThinManager tree to open the **Terminals** branch.
- ❑ Double click on the terminal that has that location you want to control with permissions to open the **Terminal Configuration Wizard**
- ❑ Navigate to the **Terminal Mode Selection** page. Check the ***Enable Relevance User Services*** checkbox. The ***Enable Relevance Location Services*** should have been checked when the location was assigned.
- ❑ The Relevance user menu can be configured by selecting the ***Main Menu Options*** button on the **Terminal Interface Options** page. A Main Menu hotkey can be configured on the **Hotkey Configuration** page.
- ❑ Restart the terminal that is assigned to the location to apply the changes.

26.1.5. Apply to Terminals

- ❑ Open the Terminal Configuration Wizard by double clicking on the desired terminal in the Terminal Branch of the ThinManager tree.
- ❑ Select *Use Display Clients* and *Enable Relevance User Services* on the Terminal Mode Selection page.
- ❑ Add the display clients that are using the Permission to the *Selected Display Clients* list on the Display Client Selection page of the Terminal Configuration Wizard.
- ❑ The Display Client Selector will show the Main Menu and the *CTL+M* hot key is enabled by default. Other options are configurable with the *Main Menu Options* button on the Terminal Interface Options page.
- ❑ Select *Finish* to accept the changes and then restart the terminal.
- ❑ The user can open the main menu from the display client drop-down and login to reveal the hidden applications they have permission to view.

26.1.6. Testing the Log In to Access Content

- ❑ Go to the location that you configured with permissions to control access.
- ❑ Observe that the restricted display client doesn’t appear in the display client selector.
- ❑ Open the Main Menu using the hotkey or from the group selector.
- ❑ Log in with the Relevance user account that has permission to access the hidden content.
- ❑ The hidden display client should be revealed while the user is logged in and should become hidden when the user logs out.

26.2. Deploying Applications across the Plant

User-specific display clients can be assigned to Relevance Users. They can go to any allowed terminal and login to access their personal applications. To do this:

- Create a Relevance User
- Add the display clients you want them to access to their profile.
- Tie their Relevance User profile to a Windows login.
- Allow Relevance User Services on the terminals you want used by the users.

26.2.1. Create Relevance User

❑ Launch the TermSecure User Configuration Wizard by selecting the User icon in the Tree Selector at the bottom of the tree, right clicking on the Relevance User branch of the tree, and selecting *Add User*.

❑ **TermSecure User Information Page -** Enter a username and password in the *User Name* and *Password* fields. You can select an existing user from Active Directory by checking the *Active Directory User* checkbox and selecting the *Search* button. See section 24.

❑ **TermSecure User Information Page -** Select the *Permissions* button and add the desired access group to the *Member Of* list if you want them to access hidden applications.

❑ **Card/Badge Information Page** – Select the *This user will use a car, badge, or other device to login* checkbox if you are using a badge reader and enter the badge number in the *Enter Card/Badge ID number* field.

Note: This step can be automated. See section 26.3.

❑ **Display Client Selection Page** – Select the *Yes* radio button for the *Add User specific Display Clients?* selection.

❑ **Display Client Specification Page** – Move the display clients you want the user to have into the *Selected Display Client* list.

❑ **Windows Log In Information Page** – If you aren't using and Active Directory account there three are login methods.

  - o *Use Terminal Configuration Login Information*: This uses the terminal account and not the user account so it doesn't give a unique log in. It is not recommended for deploying user-specific applications.
  - o *Same as TermSecure User username/password*: This is used when the TermSecure User account matches the Windows account. This is the normal method of granting a unique user account.
  - o *Username and Password*: Entering a different Windows account than the TermSecure User account in the Username field will create an alias. The user logs in with the TermSecure account and accesses their programs, but the actual Windows account is hidden.

❑ There are others settings that can be applied. See the ThinManager manual for details.

❑ Select the *OK* button and the *Finish* button to create the user. Allow TermSecure Log Ins at Terminals

26.2.2. Apply to Terminals

- ❑ Open the Terminal Configuration Wizard for the terminals you want by double clicking on the desired terminal in the Terminal Branch of the ThinManager tree.
- ❑ Select *Use Display Clients* and *Enable Relevance User Services* on the Terminal Mode Selection page.
- ❑ Select the *Finish* button and restart the terminal.

When a Relevance User goes to a terminal that has Relevance User Services enabled they will connect to the Remote Desktop Server that has their application and run the display client at that terminal. When they log off it will be hidden from other users.

26.3. Using ID Cards and Badges

ThinManager can use HID cards with RFIdeas PC Prox card readers to use a badge or card to identify the Relevance User.
See http://www.thinmanager.com/kb/index.php/Card_Readers for details.

- ❑ Attach the card reader to the thin client, add the RF Ideas pcProx module to the terminal, and restart the terminal. The serial version uses the RF Ideas pcProx module. The USB version says USB.
- ❑ The card can be associated manually by creating the user and entering the card number into the *Enter Card/Badge ID number* field on the *Card/Badge Information* page of the Relevance User Configuration Wizard.
- ❑ The card can be associated automatically by scanning the card at a terminal card reader. This will launch a Relevance User Configuration wizard in ThinManager. You can associate the card with an existing user or create a new user from the wizard.
- ❑ The card user can be forced to use a password by setting the *Always Prompt for Password* in the TermSecure User settings or in the module settings on the terminal.

26.4. Using a Personal Identification Number (PIN)

PINs, or Personal Identification Numbers, can be assigned to a Relevance User to use instead of a password.

- ❑ The PIN is assigned by selecting the *PIN Options* button on the *Relevance User Information* page of the *Relevance User Configuration* wizard.
  Other options like length and duration are also configured here.
- ❑ The *Card/Badge Information* page of the *Relevance User Configuration* wizard allows you to select where the PIN is valid, with card readers, fingerprint scanners, or manual logins as options.

26.4.1. Temporary Personal Identification Number (PIN)

PINs, or Personal Identification Numbers, can be temporarily assigned to a user to cover a specific time period, like one shift.

- ❑ Select the *PIN Options* button on the *Relevance User Information* page of the *Relevance User Configuration* wizard to open the *PIN Maintenance Options* window.
- ❑ Select the *Use a temporary PIN* checkbox to activate the PIN for temporary use.
- ❑ Select the *Change* button to open the *Authorization Cache* window that has the setting for the number of minutes the temporary PIN is valid.
- ❑ The *Clear* button will empty the PIN cache.

26.5. Using Fingerprint Scanners

ThinManager can use DigitalPersona UareU fingerprint readers to identify in a person and grant them access through Relevance.

You need to configure the finger print reader in several places.

26.5.1. ThinManager Server Biometric Configuration

The first step is to configure the ThinManager Server for biometrics.

❑ Open the *ThinManager Server Configuration Wizard* by double clicking on the *ThinManager Server* in the ThinManager Tree.

❑ Navigate to the *Biometric Device Configuration* page.

❑ Check the *Support Finger Print Readers* checkbox.

❑ Set the data format by selecting a format in the *Fingerprint storage format* drop-down.

❑ Click *Finish* to accept.

26.5.2. Terminal Biometric Configuration

The second step is to configure the terminal to use biometrics.

❑ Add a *DigitalPersona UareU fingerprint reader* to a terminal.

❑ Open the *Terminal Configuration Wizard* by double clicking on the terminal in the Terminal Tree.

❑ Navigate to the Module page.

❑ Add the DigitalPersona UareU Fingerprint Reader module.

❑ Set the Mode (TermSecure is the default), the Data Format, and whether a password is needed.

❑ Restart the terminal to apply.

26.5.3. Relevance User Services Biometric Configuration

The third step is to configure the Relevance User to use biometrics. You need to have ThinManager open and access to a terminal with a fingerprint scanner attached.

❑ Open the Relevance User Configuration Wizard by double clicking on the user in the Relevance User Tree.

❑ Navigate to the Card / Badge Information page.

❑ Select the Enroll Fingerprint button. This launches the Enroll Fingerprint window.

❑ Select the finger to scan by either using the Select Finger to Enroll drop-down or by clicking on the fingertip in the diagram.

❑ Select the Change button to pick the terminal that has the fingerprint scanner you will use for enrollment.

❑ Select the Start Enrollment button.

❑ You will need to scan the finger 4 times

❑ Touch the reader for the scan. The light in the scanner will change when the scan is complete. The status message on the terminal and the wizard in ThinManager will also give the completed status.

❑ Repeat until the finger is read.

❑ Multiple fingers can be registered. This is a good idea in case the operator has a bandage on the primary finger.

❑ Once completed the user can login to a terminal with a fingerprint scanner.

27. Relevance Location Services

Relevance Location Services allows control display client access through locations.

A tethered location has a traditional terminal at the location but a mobile device can interact with the terminal to Shadow, Transfer, or Clone the display client.

An untethered location is a “spot on a wall” that the display client can be delivered. The mobile device becomes the terminal.

Resolvers like QR codes, Bluetooth devices, GPS co-ordinates, or Wi-Fi networks can be used to determine the location. See Section 29 on page 59.

27.1. Create Locations

Creating Locations uses a wizard similar to other ThinManager components. Decide what locations you want to use and create the locations using the Location Configuration Wizard.

❑ Open the **Locations** branch by selecting the **Globe *Location*** icon in the **Tree Selector** at the bottom of the tree.

❑ Right click on the globe ***Locations*** icon in the tree and select ***Add Location*** to open the **Location Configuration Wizard.**

❑ Name the location on the **Location Name** page.

❑ Select options on the Location Options page including manually selected functions allowed.

- ***Inactivity Timeout –*** A Relevance user will be logged off after this interval if inactive.
- ***Relevance ID Signal Loss Timeout –*** This is the interval before a Relevance user is logged off due to lack of a signal.
- ***Activate Display Client at Log In –*** This brings the display client to the forefront when the Relevance user logs in.
- ***Enforce Location Fencing –*** This controls access in an area with nested locations. If local fencing is enforced the user has to be within the fence to access the sub-locations.
- ***Inherit from parent Locations –*** This allows nested sub-locations to inherit the parent display clients.
- ***Allow Local Access –*** This allows a Relevance user to access the location from that location. Unchecking this will only allow remote access.
- ***Allow Remote Access -*** This allows a Relevance user to access the location from a remote site. Unchecking this will only allow access at the location.
- ***Reset Cloned Sessions on Logout –*** This will reset any cloned sessions once they are disconnected.
- ***Allow Location to be selected manually –*** This allows a location to be manually selected. Unchecking this will require the Relevance user to use a Resolver like QR Codes, Wi-Fi, or Bluetooth to initiate the location access. If this is selected checkboxes appear to allow selection of the three basic interactions – ***Shadowing***, ***Transferring***, and ***Cloning***.

❑ Add the display clients you want to use at the location on the **Display Client Selection** page.

❑ Each location needs a unique Windows user account added on the **Windows Log In Information** page. Enter a username and password in the *User Name* and *Password* fields. You can select an existing user from Active Directory by checking the *Active Directory User* checkbox and selecting the *Search* button. This will allow you to use a Windows domain account for the Location.

❑ Resolvers are added on the **Relevance Resolver Selection** page. This provides a way for the mobile device to authenticate to a location.
See **Associating Resolvers to Locations and Actions** at Section 29.2.

❑ Create a terminal using the Terminal Configuration Wizard for each location that will have an assigned terminal. Add the location to the terminal to utilize the display client and user account instead of assigning them to the terminal itself.

See **Assigned Location –** Upgrading a System at Section 27.2 or see Assigned Location – New System at Section 27.3.

27.2. Assigned Location – Upgrading a System

Relevance delivers content to a location. This location can have a terminal assigned to it to allow the content to be displayed on the terminal or the location can be unassigned and you access the content with a mobile device.

This section will discuss converting an existing ThinManager system to using Locations. The next section will discuss creating a terminal in a new system with Relevance.

❑ Create a Location(s) as described in Create Locations on page 54.

❑ Highlight the **Terminal** icon in the ThinManager tree to open the **Terminal** branch.

❑ Double click on the terminal that you want to convert to using a location to open the **Terminal Configuration Wiz**ard.

❑ Navigate to the **Terminal Mode Selection** page. Select ***Enable Relevance Location Services*** to use locations.
The optional ***Enable Relevance User Services*** will allow you to use access groups to control application deployment.

❑ Remove Display Clients from the ***Selected Display Client*** list on the **Display Client Selection** page. The display clients will be deployed via the location and not the terminal.

❑ Assign the location to the terminal by selecting the ***Change*** button on the **Relevance Options** page and selecting a created location from the **Select Location** popup window.

❑ Remove Windows user account from the ***Windows Log In Information*** fields on the **Log In Information** page. The user account will be deployed via the location and not the terminal.

❑ Select the ***Finish*** button to accept the changes.

27.3. Assigned Location – New System

Create a terminal using the **Terminal Configuration Wizard** for each location that will have an assigned terminal. Add a location to the terminal and assign the display client and user account to the location instead of assigning them to the terminal itself.

- ❑ Create Locations as described in Create Locations on page 54.
- ❑ Highlight the **Terminal** icon in the ThinManager tree to open the **Terminal** branch.
- ❑ Right click on the Terminals branch and select ***Add Terminal*** to launch the **Terminal Configuration Wizard**. Enter a name in the ***Terminal Name*** field and select the ***Next*** button to continue.
- ❑ Select the ***Make/OEM*** and ***Model*** of the terminal hardware from the drop-downs on the **Terminal Hardware** page. Select the ***Next*** button to continue.
- ❑ Configure any options on the **Terminal Options** page. Select the ***Next*** button to continue.
- ❑ Select ***Enable Relevance Location Services*** on the **Terminal Mode Selection** page to use locations.
  The optional ***Enable Relevance User Services*** will allow you to use access groups to control application deployment.
- ❑ Do not add display clients on the **Display Client Selection** page. The display clients will be deployed via the location and not the terminal. Select the ***Next*** button to continue.
- ❑ The **Terminal Interface Options** page has settings for switching between sessions on the terminal. Configure as desired as in ThinManager and select the ***Next*** button to continue.
- ❑ Assign the location to the terminal by selecting the ***Change*** button on the **Relevance Options** page and selecting a created location from the **Select Location** popup window. Select the ***Next*** button to continue.
- ❑ The **Hotkey Configuration** page has settings for using hot keys to switch between sessions on the terminal. Configure as desired as in ThinManager and select the ***Next*** button to continue.
- ❑ Do not enter a Windows user account in the ***Windows Log In Information*** fields on the **Log In Information** page. The user account will be deployed via the location and not the terminal.
- ❑ Select the video resolution on the **Video Resolution** page and select the ***Next*** button to continue.
- ❑ Add any needed modules on the **Module Selection** page and select the ***Next*** button to continue.
- ❑ Set the ***Monitoring Configuration*** speed on the **Monitoring Configuration** page and select the ***Finish*** button to accept the changes.

27.4. Unassigned Locations

Unassigned Locations are locations that use a resolver to deploy content but the location does not have an assigned terminal. The content is accessed through a mobile device. This allows you to deploy applications anywhere without needed to add a physical terminal. The mobile device becomes the terminal.

Create a Location as show in **Create Locations** at section 27.1 on page 54.

❑ Open the **Locations** branch by selecting the globe ***Location*** icon in the **Tree Selector** at the bottom of the tree.

❑ Right click on the globe ***Locations*** icon in the tree and select ***Add Location*** to open the **Location Configuration Wizard.**

❑ Name the location on the **Location Name** page.

❑ Select options on the Location Options page including manually selected functions allowed.

- ***Inactivity Timeout –*** A Relevance user will be logged off after this interval if inactive.
- ***Relevance ID Signal Loss Timeout –*** This is the interval before a Relevance user is logged off due to lack of a signal.
- ***Activate Display Client at Log In –*** This brings the display client to the forefront when the Relevance user logs in.
- ***Enforce Location Fencing –*** This controls access in an area with nested locations. If local fencing is enforced the user has to be within the fence to access the sub-locations.
- ***Inherit from parent Locations –*** This allows nested sub-locations to inherit the parent display clients.
- ***Allow Local Access –*** This allows a Relevance user to access the location from that location. Unchecking this will only allow remote access.
- ***Allow Remote Access -*** This allows a Relevance user to access the location from a remote site. Unchecking this will only allow access at the location.
- ***Reset Cloned Sessions on Logout –*** This will close any cloned sessions once they are disconnected.
- ***Allow Location to be selected manually –*** This allows a location to be manually selected. Unchecking this will require the Relevance user to use a Resolver like QR Codes, Wi-Fi, or Bluetooth to initiate the location access. If this is selected checkboxes appear to allow selection of the three basic interactions – ***Shadowing***, ***Transferring***, and ***Cloning***.

❑ Add the display clients you want to use at the location on the **Display Client Selection** page.

❑ Each location needs a unique Windows user account added on the **Windows Log In Information** page.

❑ Resolvers are added on the Relevance Resolver Selection page. This provides a way for the mobile device to authenticate to a location.

There are six actions that can be applied to the Relevance ID but only three are effective:

- **Clone** – This creates a new duplicate session using the mobile device Windows account.
- **Force Transfer** – This automatically transfers the Windows session to the mobile device without prompting the current user for permission.
- **Transfer** – This transfers the Windows session to the mobile device after prompting the current user for permission.

These are not applicable to an unassigned location:

- **No Action** – This initiates no new action.
- **Shadow** – There is no terminal at the location to shadow so this is invalid.
- **View Only Shadow** – There is no terminal at the location to shadow so this is invalid.

❑ Select ***OK*** to add the action to the resolver at that location.

28. Mobile Devices

- Relevance is enhanced with mobile devices like an Apple iPad, Windows tablet, or Android device.
- These mobile devices become clients that connect to Remote Desktop Servers and runs sessions controlled by ThinManager.
- The devices are needed to read the Resolvers to register them with the ThinManager system.
- The devices need a wireless access point to allow them to get on the same network as the ThinManager Server.
- The devices use the TCP-2031 port to talk to ThinManager and the TCP-3389 for the RDP connection to the sessions on the Remote Desktop Servers.
- Mobile devices are configured as terminals using the methods used in ThinManager.

28.1.1. Configuration in ThinManager

❑ Configure an iPad as a terminal in ThinManager with ***Apple/iPad*** as the **Make/Model** or an Android device as ***GENERIC/Android*** on the **Terminal Hardware** page of the **Terminal Configuration Wizard**. Windows tablets are configured as ***GENERIC/WinTMC.***

❑ Check the ***Use Display Clients***, ***Enable Relevance User Services***, and ***Enable Relevance Location Services*** on the **Terminal Mode Selection** page.

❑ Entering a default display client on the **Display Client Selection** page is optional. It can receive its display clients when it enters a location.

❑ Check which resolver types you want to use on the **Relevance Options** page.
A mobile device does not need to have a location assigned but can assume a location through resolvers.

❑ Add a unique Windows user account on the **Log In Information** page.

28.1.2. Configuration on Mobile Device

❑ Install the ThinManager iTMC app on the iPad from the Apple App Store. You can search for iTMC or ThinManager and choose the iTMC program from Automation Control Products.

❑ Install the AndroidTMC app from the ThinManager web site or the Google Android store.

❑ Install the WinTMC application on a Windows table from https://downloads.thinmanager.com/.

❑ Launch the app and select the ***Setting*** button to open the **Setting** page.

❑ Define your ThinManager Server by selecting ***Add ThinManager Server*** and entering the ***Name*** and ***IP address***, and selecting the ***Save*** button.

❑ Associate the mobile device with the configuration you created by selecting the defined ThinManager Server from the main menu, connecting to the ThinManager Server, and selecting the name of the configuration you created.

The mobile device is ready to register resolvers.

29. Location Resolvers

Resolvers tie the Location in ThinManager to a specific physical location.

There are several Resolvers in Relevance.

- **QR codes** can be created using any QR generation program.
- **Bluetooth beacons** can be purchased from ACP distributors.
- **iBeacons** are the Apple Bluetooth IPS (Indoor Positioning system).
- **Wi-Fi access points** can use the existing Wi-Fi network access points as resolvers.
- **GPS** can use the global positioning system as a resolver.

Registering the Resolvers requires a mobile device with the iTMC/AndroidTMC app installed.

29.1. Registering Resolvers

29.1.1. QR Codes

❑ Open the iTMC or AndroidTMC application and select the ***Settings*** button at the bottom of the screen.

❑ Select the ***Register QR Code*** command in the **Relevance Resolver** section.

- If you have a single ThinManager Server it will open a camera window.
- If you have two or more ThinManager Servers defined you will be asked which ThinManager Server you want the resolver registered on. Select the correct ThinManager Server and a camera window will open.

❑ Point the camera window at the QR Code. After a successful scan it will ask for a name for the resolver. Enter a name and select ***Register***.

❑ A dialog box will confirm a successful QR code registration.

❑ Repeat as needed.

29.1.2. Bluetooth Beacons

❑ Open the iTMC or AndroidTMC application and select the ***Settings*** button at the bottom of the screen.

❑ Select the ***Register Bluetooth Beacon*** command in the Relevance Resolver section.

- If you have a single ThinManager Server it will open a **Register Bluetooth** window.
- If you have two or more ThinManager Servers defined you will be asked which ThinManager Server you want the resolver registered on. Select the correct ThinManager Server and a **Register Bluetooth** window will open.

❑ Bluetooth beacons in range will show a **Received Signal Strength Indication (RSSI)** number.

- Because of the low strength of the signals the reading is shown as a negative number with the higher number (lower integer) as the nearer unit.
  For example, -42 would be closer than -65 which is closer than -92.
- ACP programmed beacons will contain an ACP prefix.

❑ A dialog box will ask for you to stand at the entrance to the zone (***Stand at Zone Entrance***) to establish the base level of the entrance signal. Enter a Location description for the Bluetooth Beacon in the dialog box and click ***OK***. A success message will be displayed if accepted.

❑ The exit strength is set automatically with a 10 dB offset. This can be changed in ThinManager in the ***Resolver Settings*** on the **Relevance Resolver** page of the **Location Configuration** wizard.

❑ Repeat as needed.

29.1.3. GPS

❑ Open the iTMC or AndroidTMC application and select the ***Settings*** button at the bottom of the screen.

❑ Select the ***Register GPS Location*** command in the Relevance Resolver section.

- If you have a single ThinManager Server it will open a **Register Location** window.
- If you have two or more ThinManager Servers defined you will be asked which ThinManager Server you want the resolver registered on. Select the correct ThinManager Server and a **Register Location** window will open.

❑ The **Register Location** screen will list the ***Latitude***, ***Longitude***, and ***Altitude*** of the device.

❑ Select the ***Tap Here to Register Location*** command to register the location.

❑ Enter a description in the dialog box and select ***OK*** to complete the registration. A success message will be displayed if accepted.

❑ The location radius is set automatically to 65 meters. This can be changed in ThinManager in the ***Resolver Settings*** on the **Relevance Resolver** page of the **Location Configuration** wizard.

❑ Repeat as needed.

29.1.4. Wi-Fi Access Points

❑ Open the iTMC or AndroidTMC application and select the ***Settings*** button at the bottom of the screen.

❑ Select the ***Register WiFi Access Point*** command in the Relevance Resolver section.

- If you have a single ThinManager Server it will open a **Register Access Point** window.
- If you have two or more ThinManager Servers defined you will be asked which ThinManager Server you want the resolver registered on. Select the correct ThinManager Server and a **Register Access Point** window will open.

❑ Wi-Fi access points in range will show a Basic service set identification (BSSID). This is the unique identifier for the access point.

❑ Select the ***Tap Here to Register*** command to register the access point.

❑ Enter a description in the dialog box and select ***OK*** to complete the registration. A success message will be displayed if accepted.

❑ Repeat as needed.

29.2. Associating Resolvers to Locations and Actions

❑ Register your resolvers as described in **Registering Resolvers** at section 29.1.

❑ Create your locations as described in **Create Locations** at section 27.1.

❑ Open the **Locations** branch by selecting the globe ***Location*** icon in the **Tree Selector** at the bottom of the tree.

❑ Right click on a location to open the **Location Configuration Wizard.**

❑ Use the ***Next*** button to navigate to the **Relevance Resolver Selection** page of the Location Configuration Wizard.

❑ Select the ***Add*** button to launch the **Choose a Relevance Resolver Selection window.**

❑ Select the registered resolver from the ***Resolver Name*** drop-down.

❑ Select the action you want the resolver to trigger from the ***Choose Action*** drop-down.

There are six actions that can be applied to the Relevance ID:

- **Clone** – This creates a new duplicate session using the mobile device Windows account.
- **Force Transfer** – This automatically transfers the Windows session to the mobile device without prompting the current user for permission.
- **No Action** – This initiates no new action. This can be used in Fencing to allow a Location to be validated without initiating a task.
- **Shadow** – This provides an interactive shadow of the location on the mobile device.
- **Transfer** – This transfers the Windows session to the mobile device after prompting the current user for permission.
- **View Only Shadow** – This provides a shadow of the current location without allowing any input from the mobile device.

❑ Select ***OK*** to add the action to the resolver at that location.

❑ Repeat as necessary to have different resolvers for different actions.
See Error! Reference source not found. at section **Error! Reference source not found.** to see how to use Access Groups to have the same resolver grant different actions based on group membership.

29.3. Use Permissions to Control Resolver Actions

Permissions can be associated with Relevance functions so that a single resolver can allow shadowing, cloning, or transferring, depending on the user's membership in a Relevance access group.

❑ Select the **Location** icon in the ThinManager tree to open the **Location** branch.

❑ Double click on the location you want to control with permissions to open the **Location Configuration Wizard**.

❑ Navigate to the **Relevance Resolver Selection** page.

❑ Select the ***Add*** button to add a resolver and select and action in the ***Choose Action*** drop-down on the Choose a Relevance Resolver window.

❑ Select the ***Permissions*** button to launch the **Permissions** window. Remove the ***Unrestricted*** group from the ***Member of*** list and add the access group you want to be able to perform the action. Select the ***OK*** button twice to close the **Permissions** window and **Choose a Resolver** window.

❑ To have the same resolver perform different functions for different permission groups add the resolver additional times, select a different action and add a different permission group each time.

❑ Select the ***Finish*** button to close the Relevance Resolver Selection wizard.

30. Fencing

Fencing is a critical function that prevents applications from running in unauthorized locations, like running the boiler application in the cafeteria.

To establish fencing you:

- Create a Location and use a passive resolver like a Bluetooth beacon, Wi-Fi network, or GPS location to resolve the location.
- Nest another Location under the top level location to create a sub-location and apply a resolver to it.
- The user has to resolve to the top level location before they can resolve and access the display client application on the sub- location. Leaving the area of the top level location will cause the user to be dropped from both locations.

30.1. Create a Top Level Location for Fencing

Create a location that will define the fence. It will become a top level location.

❑ Open the **Locations** branch by selecting the **Globe *Location*** icon in the **Tree Selector** at the bottom of the tree.

❑ Right click on the globe ***Locations*** icon in the tree and select ***Add Location*** to open the **Location Configuration Wizard.**

❑ Name the location on the **Location Name** page.

❑ Select options on the Location Options page including manually selected functions allowed.

- ***Enforce Location Fencing –*** Check this setting as it controls access in an area with nested locations and the user has to be within the fence to access the sub-locations.

❑ Leave the Selected Display Clients list empty on the **Display Client Selection** page. The fence location won't supply a display client. It will just verify that the user is in the proper location.

❑ The **Windows Log In Information** page can be left blank since this location isn't launching a Windows session to deliver a display client application.

❑ Add a Resolver on the **Relevance Resolver Selection** page. This provides a way for the mobile device to authenticate to a location. This should be a Bluetooth, Wi-Fi, or GPS resolver.
See **Associating Resolvers to Locations and Actions** at Section 29.2.

Create a terminal using the Terminal Configuration Wizard for each location that will have an assigned terminal. Add the location to the terminal to utilize the display client and user account instead of assigning them to the terminal itself.

30.2. Create a Sub-Location in the Fence

Create a sub-location that will deliver the display client applications when within the fence. It will become a sub- location.

❑ Right click on your fence Location and select the ***Add Location***. This will create a location nested under that location, making it a sub-location.

❑ Name the sub-location on the **Location Name** page.

❑ Select options on the Location Options page including manually selected functions allowed.

  - ***Enforce Location Fencing –*** Check this setting as it controls access in an area with nested locations and the user has to be within the fence to access the sub-locations.

❑ Add the display clients you want to use at the location on the Display Client Selection page.

❑ Each location needs a unique Windows user account added on the Windows Log In Information page. Enter a username and password in the User Name and Password fields. You can select an existing user from Active Directory by checking the Active Directory User checkbox and selecting the Search button. This will allow you to use a Windows domain account for the Location.

❑ Resolvers are added on the Relevance Resolver Selection page. This provides a way for the mobile device to authenticate to a location.
A QR code is a good resolver to use for sub-locations.
See Associating Resolvers to Locations and Actions at Section 29.2.

❑ Select ***Finish*** to complete the wizard.

❑ Add the sub-location to a terminal for an assigned location or leave it as an unassigned location.

A user will need to enter the top level location before it can access the sub-location. It the user walks out of the top level location it will drop access to the sub-level.