THINMANAGER
A ROCKWELL AUTOMATION TECHNOLOGY

ThinManager 11.2 User Guide

TM-UM002A-EN-P

Version 11.2 — July 15, 2020

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

www.thinmanager.com | Toll-Free 1-877-239-4282 | 678-990-0945

1. ThinManager 11.2 Additions 8
1.1. ThinManager 11.2 Database Encryption 8
1.2. Portrait Mode 10
2. Quick Setup Overview 12
3. Terminology 14
4. ThinManager Introduction 15
4.1. ThinManager 15
4.2. Relevance User Access 17
4.3. Relevance Location Services 18
5. ThinManager Interface 19
5.1. Menus 21
5.2. Customizing the Toolbar 25
5.3. Icons 26
6. Licensing 34
6.1. ThinManager Master License 34
6.2. FactoryTalk Activation 42
7. Users in a ThinManager System 44
7.1. Windows Users 44
7.2. ThinManager Security Group Users 44
7.3. Relevance Users 45
8. Sources – Remote Desktop Servers 45
8.1. Microsoft Configuration 45
8.2. Defining Remote Desktop Servers in ThinManager 47
8.3. Remote Desktop Server Graph 59
8.4. Remote Desktop Server Status 60
8.5. Remote Desktop Server Group 64
9. Sources – IP Cameras 75
9.1. Configure the IP Camera 75
9.2. Define the IP Camera as a Display Server 76
9.4. Define the USB Camera as a Display Server 81
10. Sources – VNC Server 87
11. Sources - Workstations 90
12. Sources – VCenter Servers 92
12.1. Snapshots 96
12.2. Adding a Virtual Server 98
13. Content – Remote Desktop Services Display Client 102
13.1. Desktop 103

13.2. Single Application Deployment with AppLink 111
13.3. Deployment Options 123
13.4. Allow Auto-Login 123
13.5. Application Link 123
13.6. SmartSession 129
13.7. Enforce Primary 133
13.8. Failover 133
13.9. Instant Failover 136
14. Content – Camera Display Clients 138
14.1. Camera Overlay Template 141
15. Content – Terminal Shadow 162
15.1. Shadow Any Terminal 163
15.2. Shadow a Specific Terminal 166
15.3. Shadow of the Terminal 170
16. Content - Workstation Deployment 173
16.1. Step 1 – On the PC 173
16.2. Step 2 – Workstation Display Client 175
16.3. Adding the Workstation Display Client to the Terminal 181
17. Content – VNC Shadow 188
17.1. Shadow Any VNC Server 189
17.2. Shadow a Specific VNC Server 191
18. Content – Virtual Screens 195
18.1. Virtual Screen Display Client Wizard 195
18.2. Pre-Defined Templates 198
18.3. Adding a Virtual Screen to a Terminal 206
18.4. Custom Overlays 210
18.5. Display Client Override on Virtual Screens 224
19. Devices – Terminal Configuration 227
19.1. Terminal Configuration Wizard in ThinManager 228
19.2. User Accounts in the Terminal Configuration Wizard 253
19.3. Copy Settings from another Terminal 268
19.4. Using Groups for Organization 271
19.5. Using Groups for Configuration 279
20. Devices – IP Configuration 290
20.1. ThinManager Ready Thin Client IP Configuration 291
20.2. Adding and Configuring Thin Clients 296
20.3. PXE Server and PXE Boot 298

20.4. Local WinTMC Configuration 314
20.5. WinTMC Configuration in ThinManager 316
21. Devices – Mobile Devices 321
21.1. Configuring an iPad in ThinManager 321
21.2. Configuring an Android Device in ThinManager 337
22. Users - Active Directory User Login Account 343
23. Packages 348
23.1. Firmware, Packages and Modules 348
23.2. Configuring Packages for a Model of Thin Client 357
23.3. Configuring Packages for an Individual Thin Client 359
24. Modules 362
24.1. Module List 362
24.2. Adding a Module (Keyboard > Key Block Module) 365
24.3. Individual Module Details 369
24.4. ICA Modules 369
24.5. Keyboard Modules 370
24.1. Language Modules 373
24.2. Local Storage Modules 373
24.3. Miscellaneous Modules 375
24.4. Mouse Modules 378
24.5. Network Modules 381
24.6. RDP Modules 382
24.7. Relevance Modules 384
24.8. Screen Saver Modules 391
24.9. Sound Modules 393
24.10. TermSecure Modules 395
24.11. Touch Screen 395
24.12. Video Driver Modules 400
25. MultiMonitor 401
25.1. MultiMonitor Layout Page 404
25.2. MultiMonitor Display Client Selection Page 410
25.3. Override Function 411
25.4. Share Keyboard and Mouse Module 415
26. ThinManager Server Configuration Wizard 419
27. Reports 441
27.1. Selecting Reports 441
27.2. Report Tab 442

27.3. Print Report 443
27.4. Report Template Installation 444
28. Scheduling 445
28.1. System Scheduling of Reports 446
28.2. Scheduling Configuration Backups 452
29. Introduction to Relevance 455
30. Relevance User Services Introduction 456
31. Permission Deployed Applications in Relevance 457
31.1. Permission Deployed Applications Diagram 457
31.2. Relevance Access Group Creation 460
31.3. Add Access Group to a Display Client 463
31.4. Configure Terminals for Relevance 467
31.5. Create the Relevance User without a Windows Account 472
31.6. Relevance Results 476
31.7. Logging On to Relevance 477
31.8. Logging Out of Relevance 482
32. Assigning Roaming Display Clients to a Relevance User 482
32.1. Roaming Display Clients in Relevance Diagram 482
32.2. Create the Relevance User using Active Directory 484
32.3. Relevance Configuration Wizard 492
32.4. Adding User-specific Display Clients 494
32.5. Logging On with a Relevance User Account 501
32.6. Logging Out of Relevance 506
32.7. Roaming Applications for Non-Domain Users 506
33. Relevance User Groups 516
33.1. Adding a Relevance User to a Relevance User Group 523
33.2. Batch Create Relevance Users using Active Directory OU 527
34. Password and Account Management 535
34.1. Active Directory - Manage Accounts Management 535
34.2. Active Directory – Convert Accounts 538
34.3. Active Directory - Synchronize Password 543
34.4. Active Directory - Settings 546
34.5. Shortcut Method of Adding Relevance Access Groups 547
34.6. Relevance User Schedule 550
35. Card Readers and Fingerprint Scanners 553
35.1. Card and Badge Configuration for a Relevance User 553
35.2. Fingerprint Reader 568

36. Relevance Location Services 579
36.1. Creating a Location with the Location Configuration Wizard 580
36.2. Adding a Location to a Terminal 591
37. Using Mobile Devices to Interact with Relevance 599
38. Manual Interaction with Locations 602
38.1. Shadow 605
38.2. Transfer 609
38.3. Clone 615
39. Using the Mobile Device to Add Resolver Codes 618
39.1. QR Codes 619
39.2. Bluetooth Beacons 632
39.3. Wi-Fi Access Points 648
39.4. GPS 659
40. Adding Actions to Resolver Codes 670
41. Interacting with the Location 674
41.1. Shadow 675
41.2. Forced Transfer 677
41.3. Transfer 681
41.4. Clone 686
42. Unassigned Locations 689
42.1. Create an Unassigned Location 689
43. Fencing and Sub-Locations 697
43.1. Parent Locations 698
43.2. Child Sub-Locations 702
44. Relevance User Access 710
44.1. Creating a Location with Restricted Applications 711
44.2. Adding a Restricted Application to a Location 714
44.3. Putting It Together 719
45. One QR Code, Multiple Actions 723
46. Calculating Permissions 726
47. Guided Access on the iPad 728
48. TermMon ActiveX and Relevance 731
48.1. Registering the Control 731
48.2. Read-Only Properties 732
48.3. Read-Write Properties 733
48.4. Events 733
48.5. Methods 734

1. ThinManager 11.2 Additions

ThinManager has two major features added in ThinManager 11.2. These are a stronger database encryption that requires a password for the encryption key, and the ability to display the portrait mode on monitors.

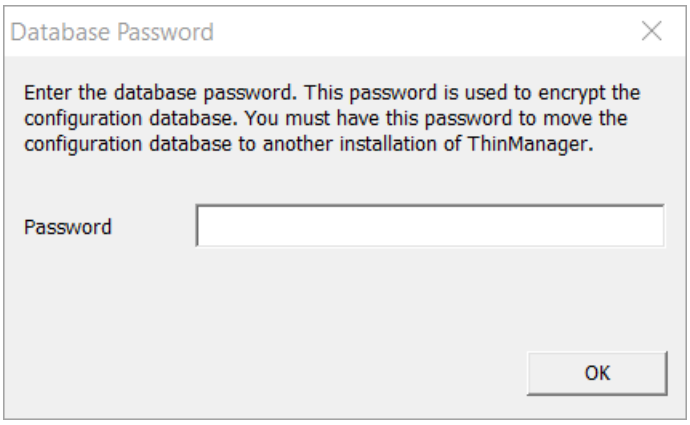
1.1. ThinManager 11.2 Database Encryption

ThinManager 11.2 has a major encryption change, with AES, the Advanced Encryption Standard, being used to encrypt the ThinManager database instead of the previous encryption key. This has led to a few important changes.

The database requires a password to be used as part of the encryption key and will prompt for a password as soon as it is installed or updated.

Installation

When ThinManager 11.2 is first run, a dialog box will appear asking for a new database password.



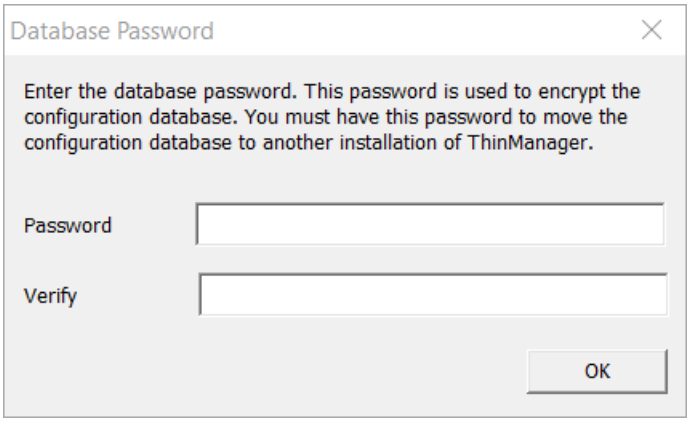
Database Password Dialog

The password entered into the *Password* field for the **Database Password** is used for the encryption key when the database is configured. There are no requirements for length or complexity. This password can be blank.

Note: This password is unrecoverable if lost.

Manual Backup

When a user manually backs up the configuration using *Manage>Backup*, the user will be prompted to create a password for the backup.



Database Password Dialog

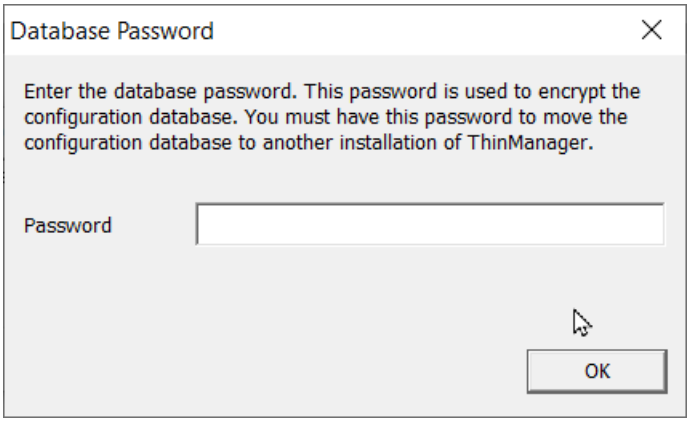
This password is for the copy of the database as a backup only, not the running database. This allows a user to backup the configuration with a short password to send to support without sending the main database password.

There are no requirements for length or complexity of the backup password. The password can be blank.

Note: This password is unrecoverable if lost.

Manual Restore

If an encrypted backup is restored with *Manage>Restore*, the Database Password dialog will launch and prompt for the password for the backup.



Database Password Dialog

This is asking for the password applied to the backup database, not the original database password.

Automatic Backup

ThinManager can be configured to automatically backup the configuration. These automatic backups will use the original password that was originally set when ThinManager 11.2 was set up.

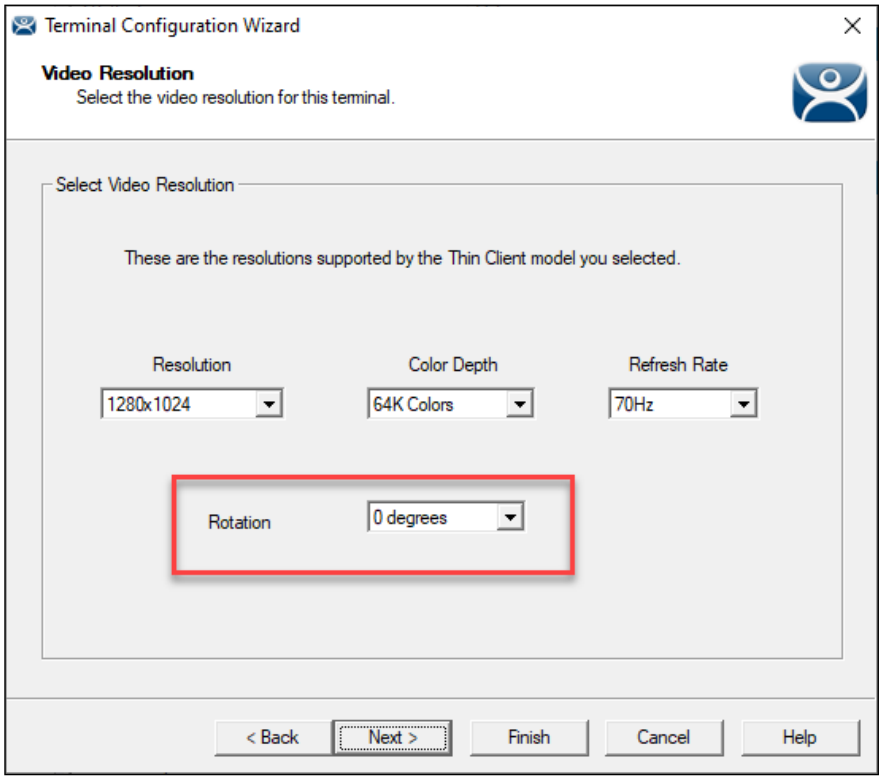
The backups will now be saved in ***C:\ProgramData\Rockwell Software\ThinManager*** instead of *C:\Program Files (x86)\Rockwell Software\ThinManager*.

1.2. Portrait Mode

ThinManager 11.2 introduces Portrait Mode, the ability to rotate a monitor to Portrait mode instead of the traditional Landscape mode. This is done with a Rotation drop-down.

1.2.1. Single Monitor Mode

A *Rotation* drop-down is on the **Video Resolution** page of the **Terminal Configuration Wizard**.



The default is *0 degrees* which provides landscape mode.

Selecting an option from the *Rotation* drop-down will change the display. The options are

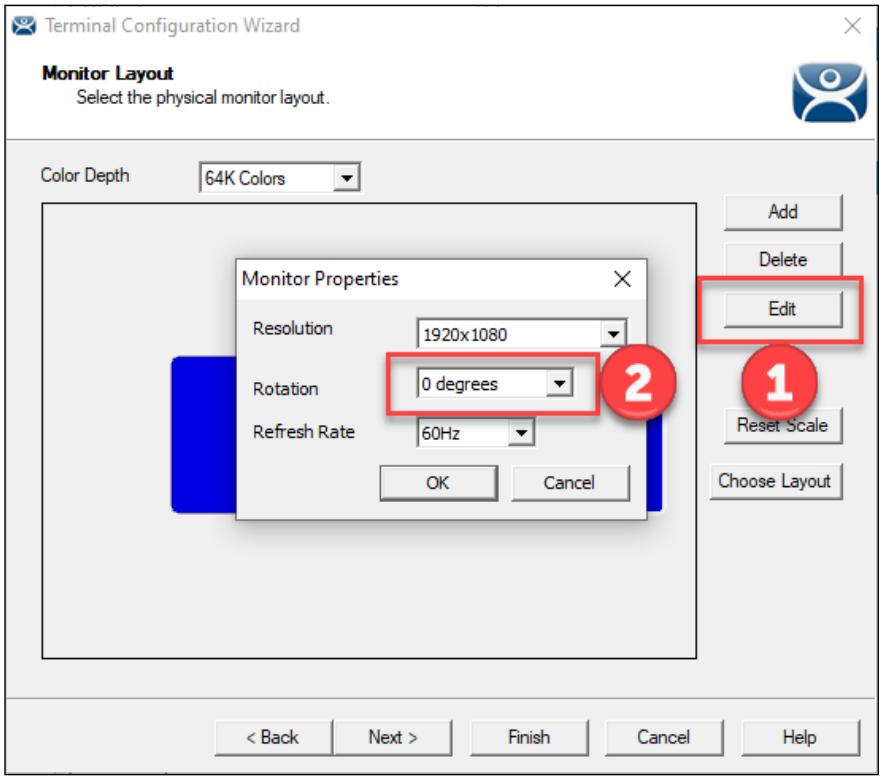
- 0 degrees (default)
- 90 degrees
- 180 degrees
- 270 degrees.

Select the angle which matches the monitor orientation, save, and reboot.

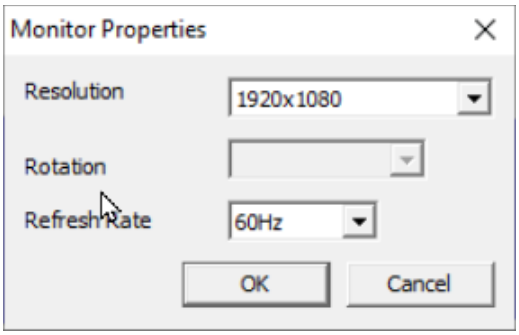
1.2.2. MultiMonitor Mode

Configuration of MultiMonitor monitors has additional steps.

- Open the **Terminal Configuration Wizard** for the terminal and navigate to the **Monitor Layout** page.
- Highlight the desired monitor and select the *Edit* button to open the **Monitor Properties** window.
- Select the desired rotation from the **Rotation** drop-down.
- The wizard will show the new orientation in the **Monitor Layout** window.
- Select the *OK* button to close the windows and save the changes.
- Reboot your terminal to apply the changes.



Note: The *Rotation* drop-down on the **Monitor Layout** window will not be active until the wizard has been saved and re-opened.



If the **Rotation** is grayed out, close the wizard and re-open the wizard.

2. Quick Setup Overview

Microsoft

- ❑ Build a Remote Desktop Server with the Microsoft Windows Server 2008/2008R2, 2012 or 2016 operating system. Enable the Remote Desktop Services (Terminal Services) role.
- ❑ Create a Microsoft Remote Desktop Licensing Server and add RDSCALs (Remote Desktop Services Client Access Licenses) for each thin client. These were previously called Terminal Server Client Access License, or TSCALs, in Server 2003. The servers also require a normal CAL.
- ❑ It is common to have each ThinManager managed Terminal automatically login to the Remote Desktop Server when it boots up. Therefore, create a unique Windows user for each ThinManager managed Terminal. For domain deployments, this will be done within Active Directory. For workgroup deployments, this will be done on each Remote Desktop Server. Make sure that each user has the permission to start Remote Desktop Server sessions on each Remote Desktop Server.
- ❑ 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.
- ❑ If using ThinManager Master Licensing:
    - Create a Master ThinManager License and add enough Product Licenses for each ThinManager-managed Terminal.
- ❑ If using FactoryTalk Activation:
    - Install the FactoryTalk Activation Manager on each computer where ThinManager is installed.
    - Download the FactoryTalk Activations for ThinManager.
    - Change the License Mode in ThinManager to FactoryTalk Activation and assign the newly downloaded activations.

ThinManager Configuration

- ❑ Define the Remote Desktop Servers using the *Display Servers* > *Remote Desktop Servers* > *Remote Desktop Server Wizard*.
- ❑ Define the Display Clients using the *Display Clients* > *Remote Desktop Services* > *Display Client Wizard* to deploy the applications.
- ❑ Define the Terminals using the *Terminal* > *Terminal Configuration Wizard*.
- ❑ Associate the hardware to the Terminal configuration.

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 ThinManager managed Terminals. ThinManager Ready thin clients can use Static IP or DHCP. ThinManager Compatible thin clients use PXE boot, and therefore require DHCP.
- If using Static addressing, open the IP Address menu on the thin client and enter the IP address of the thin client and the ThinManager Server.
- If using DHCP, configure Option 066 for the IP address of the ThinManager Server, and Option 067 as acpboot.bin.
- If using PXE Boot, enable PXE boot by selecting Manage>PXE Server to launch the PXE Server wizard.
- Attach the Terminals to ThinManager by either:
    - Turning on the Terminal and selecting the "Create New Terminal" option when the offline Terminals are listed.

- 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. 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 that connects to a server.

Fat client is a Terminal with a hard drive that connects to a server.

Terminal Server is the original term for a Windows 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 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.

UEFI - Unified Extensible Firmware Interface – UEFI is a new BIOS format for ThinManager Compatible PXE boot thin clients. It requires Port UDP-4011 open.

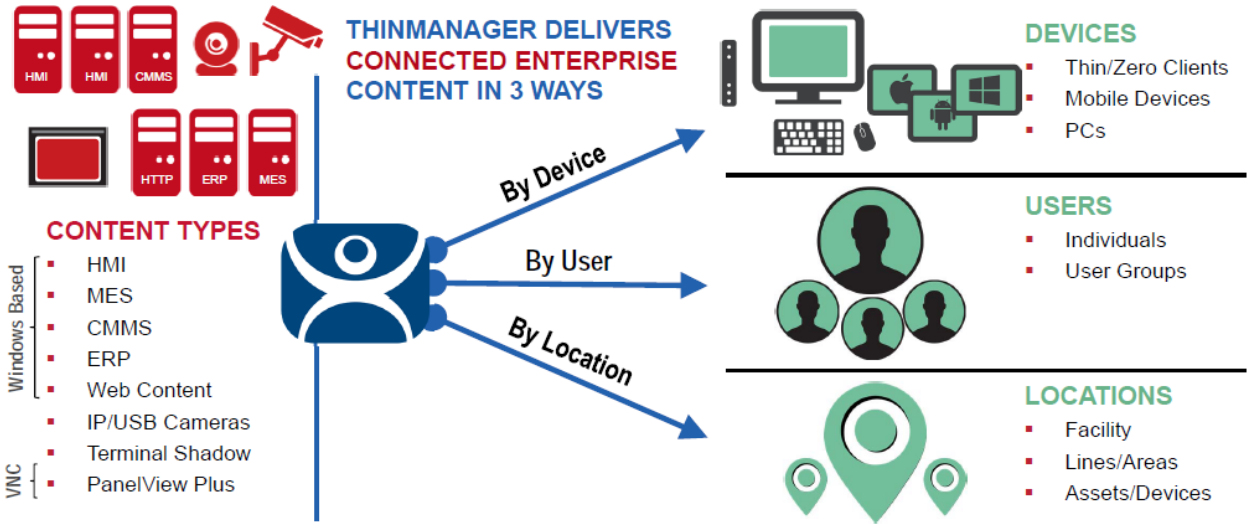
4. ThinManager Introduction

4.1. ThinManager

ThinManager is a content delivery system. ThinManager delivers content from a source to a device where a user can view and interact with the content.

ThinManager is the management system. Relevance is an extension that allows you to grant or deny access based on location or user permissions.

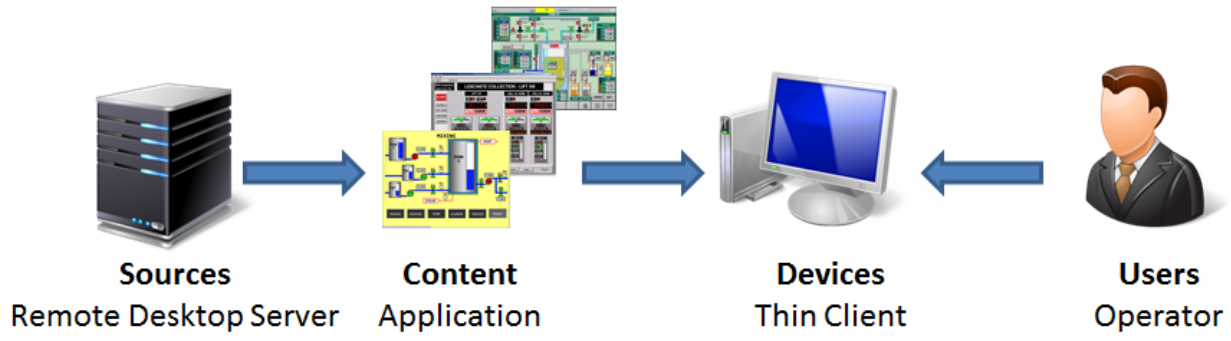
This manual will cover the variations of content deployment using ThinManager® with Relevance®.



ThinManager Content Delivery by Device, User, or Location

ThinManager is the tool that allows you to define sources, deploy content, configure devices, and allow user access. ThinManager is a software program that is installed on a computer in your system. Each device connects to it to receive its configuration and instructions.

The simplest use of ThinManager is to deploy a Windows application from a Windows Remote Desktop Server to a ThinManager Ready device.



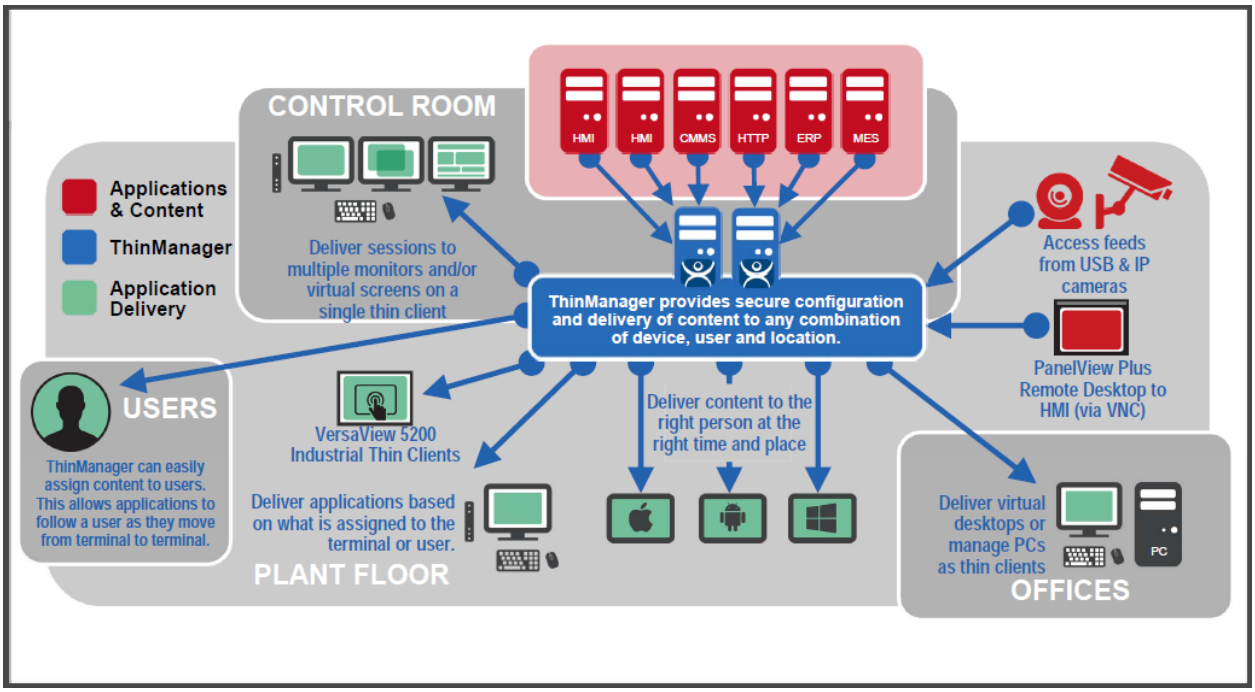
Typical Simple Deployment

However ThinManager provides many more options for deploying applications.

Sources Display Servers	Content Display Clients	Devices Terminals	Users
Remote Desktop Servers	Windows Applications	ThinManager Ready thin clients	Manual Login
Virtual Servers	Workstations	ThinManager Compatible thin clients	Auto-Login
Workstations	IP Cameras	WinTMC on PC	Relevance User
IP Cameras	Shadowed Terminals	iTMC on iPad	HID Card and Reader
Terminals via Shadow	VNC Server Shadow	AndroidTMC on Android	Fingerprint Reader
VNC Servers			Smart Card

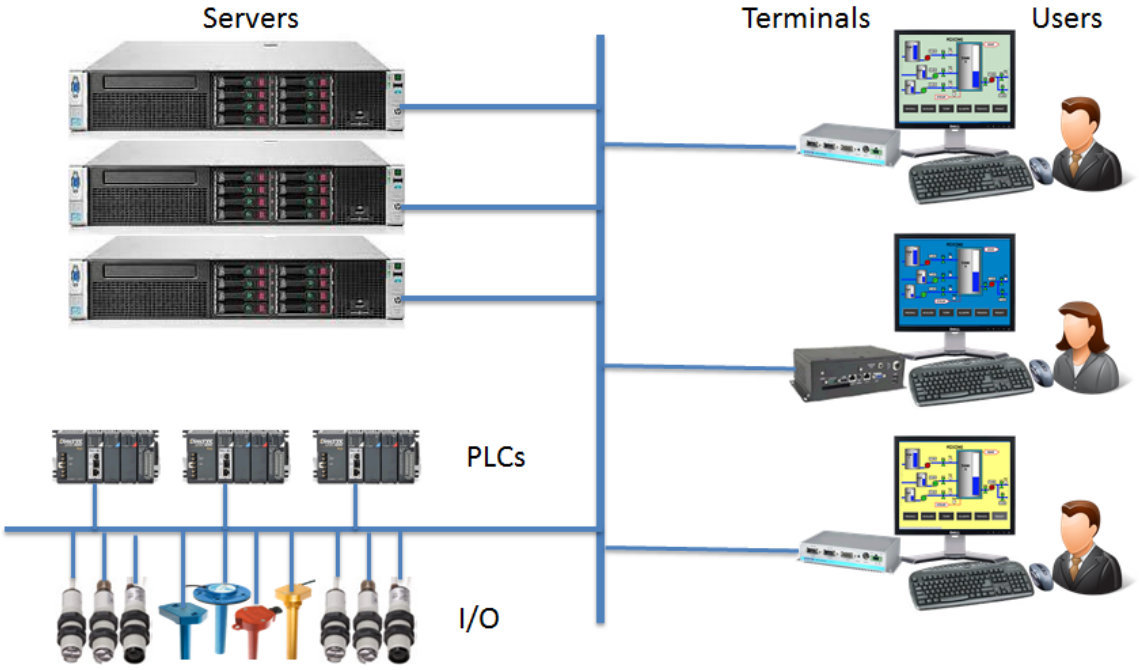
Sources, Content, Devices, and User Options

These options allow a robust content delivery system.



ThinManager Content Deployment

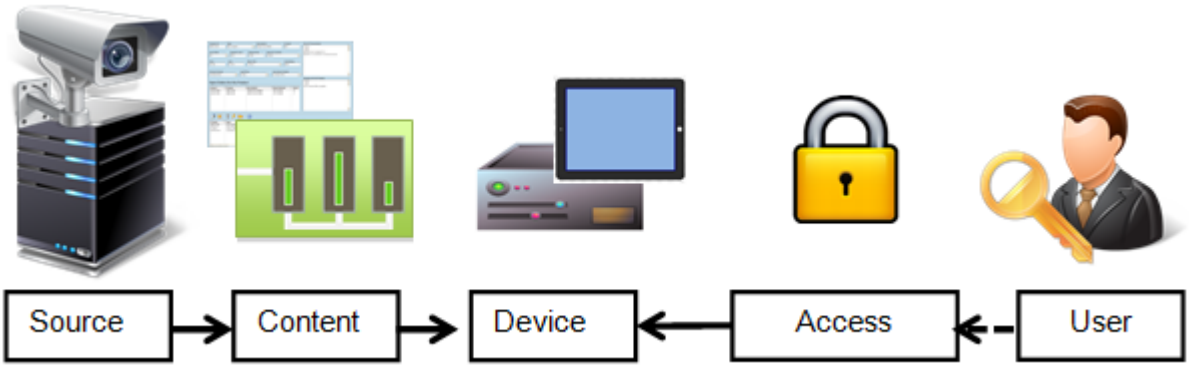
ThinManager centralizes content servers in a computer room and deploys the content to the plant floor, office, or control room as needed.



Standard Industrial Architecture

An industrial network will pull the I/O to the PLCs. The Remote Desktop Server will host the sessions that run the HMI and talk to the PLCs to gather and display the data.

4.2. Relevance User Access

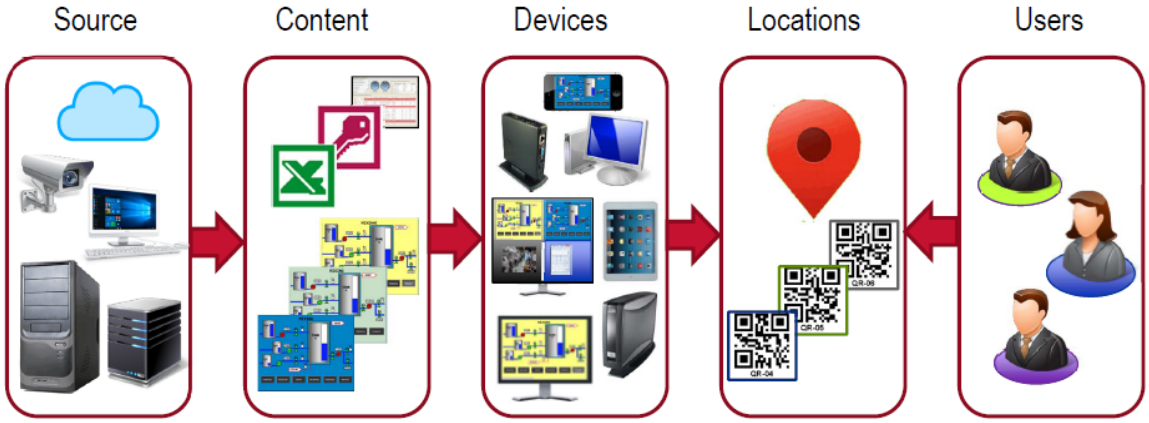


Access

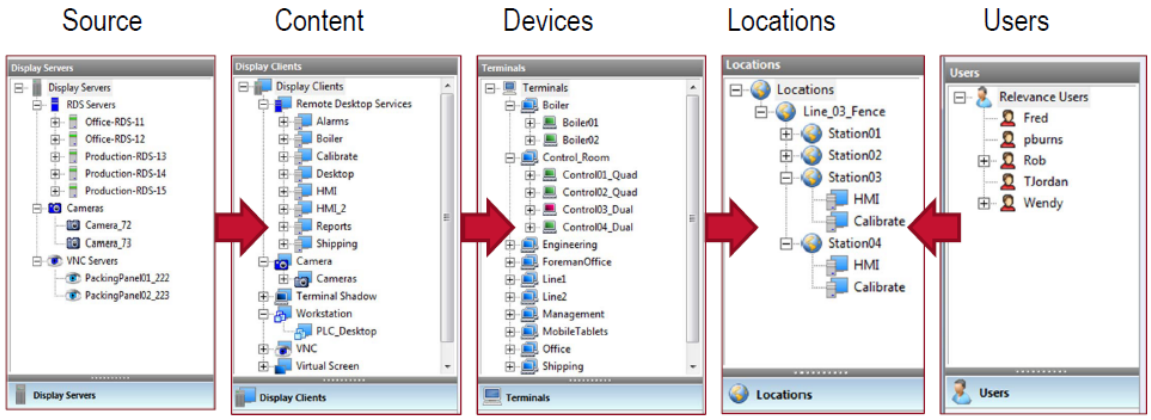
ThinManager has an additional security system that controls deployment of applications to users. This was called TermSecure and is integrated in ThinManager® with Relevance® as Access.

4.3. Relevance Location Services

The Relevance component builds on the ThinManager system by adding location to the application delivery. This allows content to be sent to the right person at the right place at the right time.



Stylized Content Deployment



Content Deployment in ThinManager Tree

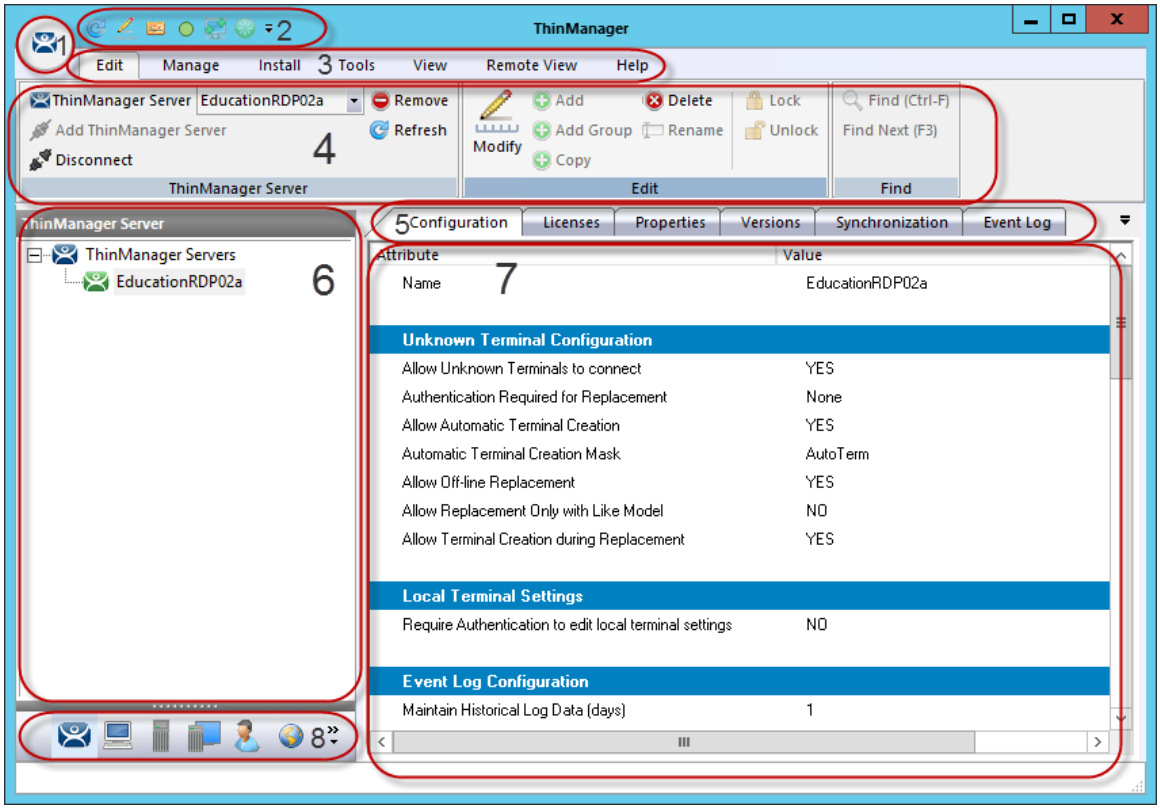
ThinManager uses wizards to configure the ThinManager components.

You create Locations in Relevance and send content to the locations. These can be assigned locations with a tethered Terminal or can be unassigned locations that have no Terminal at the location and are accessed solely by mobile devices.

Locations can be resolved manually or by using QR codes, Bluetooth beacons, Wi-Fi networks, or GPS.

5. ThinManager Interface

The ThinManager interface was changed in ThinManager 7.0 to a style based on the Microsoft Outlook template. This section will lead you through the important sections. You may find specific information by pressing the F1 key while in the ThinManager program.

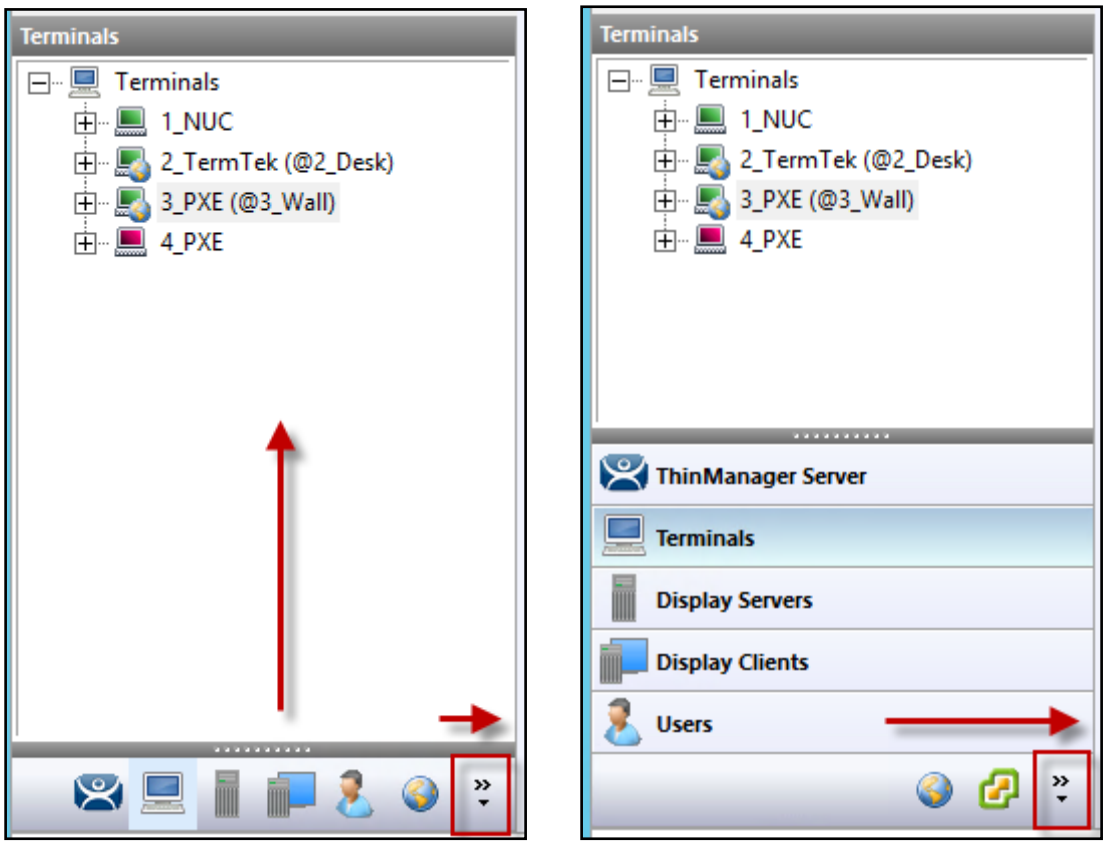


ThinManager Interface

The ThinManager Interface has several components.

1. **Application Button** – This launches the ThinManager Server Configuration wizard to configure global ThinManager settings.
2. **Quick Access Toolbar** – This lets you add icons of commonly used tasks from the menu bar, like Restart, Send Message, Modify, Backup, and Shadow. Select the **Quick Access drop-down** arrow to customize this tool bar.
3. **Menu Bar** – The menu bar separates the functions into categories.
4. **Ribbon Bar** – The menu bar now has the ribbon with icons for the functions. The ribbon can remain visible or hidden when unused. This is controlled by the ***Minimize the Ribbon*** command on the **Quick Access drop-down** arrow menu.
5. **Detail Pane Tabs** - The Detail Pane has tabs that allow you to choose what details you want to display. The tabs and detail selections change depending on what is selected in the tree. You can drag the tabs to change the order.
6. **Tree** – The tree shows the components of ThinManager. The tree now uses the Outlook Bar Tab control so the branches of the ThinManager tree are shown one at a time.
7. **Detail Pane** – The Detail Pane displays the information for the selected tab for the highlighted tree component. You can tear away the detail pane by dragging the tab away from ThinManager. You can re-dock the pane by dragging the pane title bar back to the tabs.

8. **Tree Selector** – The selector buttons at the bottom of the tree control select which branch is active and visible. These can be pulled upwards to stack the buttons, or pulled down to minimize the buttons.



Tree Selector Buttons

Minimized Buttons at the Bottom *Buttons Stacked*

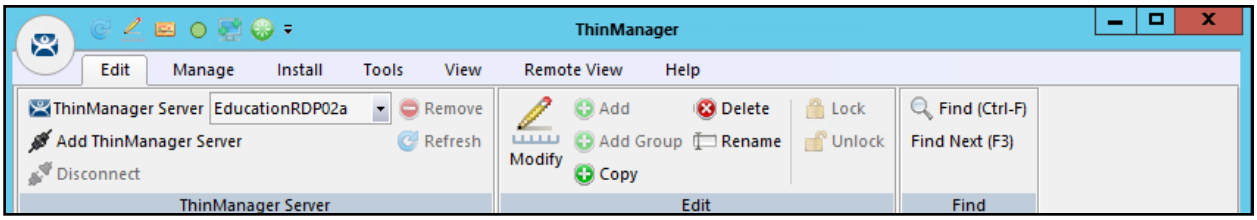
Stacking the buttons is provides quicker switching but the minimized buttons allows more room to show components in a larger system

There is an arrow that allows customization, tasks like hiding branches or reordering the branches of the tree

5.1. Menus

The menus of ThinManager use the Microsoft Outlook ribbon but contain similar functions as previous versions.

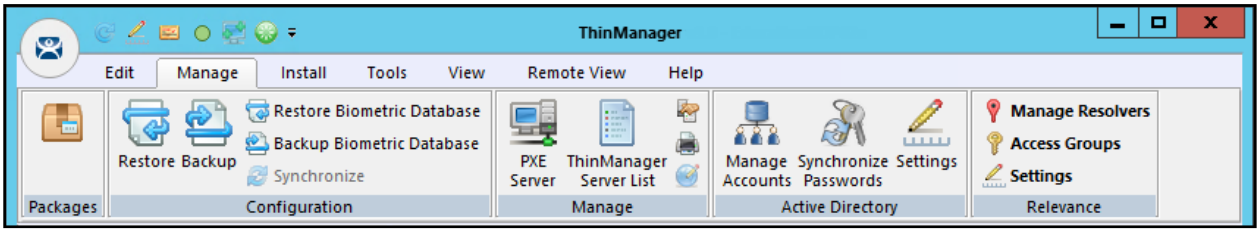
This is a brief description. Many of these functions will be explained in greater details in the sections of the manual that cover setup and configuration.



Edit

Edit includes:

- **Add ThinManager Server** – This allows you to connect to, and manage other ThinManager Servers from your local interface. You need the appropriate permissions on the remote computer for access. This is intended for a remote connection and not the partner in a synchronized pair.
- **Disconnect** – This breaks the connection to the remote ThinManager Server.
- **Remove** – This deletes the remote ThinManager Server from the local list. It doesn't affect the remote ThinManager Server.
- **Refresh** – This refreshes the data.
- **Modify** – This will open the configuration wizard for whatever item is highlighted in the tree.
- **Add** – This will launch a new configuration wizard for whatever branch is highlighted in the tree.
- **Add Group** – This will launch a group configuration wizard for whatever branch is highlighted in the tree.
- **Copy** – This will launch a dialog that allows you to create a copy of a highlighted item.
- **Delete** – This will allow you to delete a highlighted item.
- **Rename** – This allows you to rename a highlighted item.
- **Lock** – This will allow you to lock a highlighted item.
- **Unlock** – This will allow you to unlock a locked item.
- **Find** – This will allow you to search for names, descriptions, IP addresses, and other data in the tree.
- **Find Next** – This allows you to repeatedly search for a term.

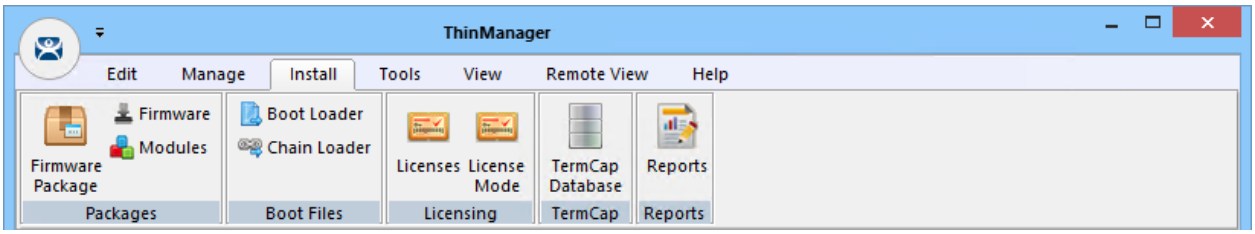


Manage

Manage includes:

- **Packages** – This opens the Package Manager window.
- **Restore** – This opens a file browser to let you restore a previously saved ThinManager configuration.
- **Backup** – This opens a file browser that lets you backup and save a ThinManager configuration for emergency restoration. This backup can be automated using the Scheduler.
- **Restore Biometric Database** – This opens a file browser to let you restore a previously saved Biometric database.

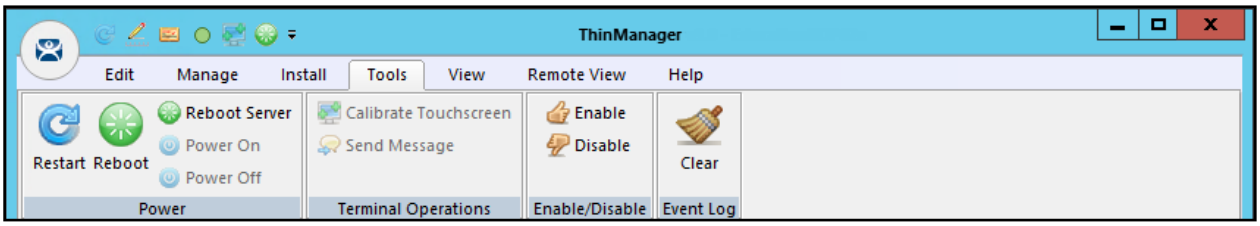
- **Backup Biometric Database** – This opens a file browser to let you save your Biometric data.
- **Synchronize** – This allows you to manually synchronize a pair of ThinManager Servers if you aren't using the recommended automatic synchronization.
- **PXE Server** – This launches the PXE Server configuration wizard.
- **ThinManager Server List** – This opens the ThinManager Server configuration wizard for automatic synchronization.
- **DNS Configuration** – This opens the DNS configuration wizard to allow ThinManager to resolve names using your DNS.
- **Configure Default Terminal** – This allows configuration of the default Terminal if you are using auto-creation of Terminals.
- **Web Management** – This will allow you to manage web access when it is implemented in the future.
- **Manage Accounts –** This allows you to manage passwords of Active Directory accounts. See Active Directory - Manage Accounts Management on page 535 for details.
- **Synchronize Passwords** – This allows you to synchronize the passwords between ThinManager and the Active Directory for the chosen accounts. See Active Directory - Synchronize Password on page 543 for details.
- **Settings (Active Directory) –** This allows you to use Active Directory, set Password Settings, and select whether to use Windows Security Groups or Active Directory Organizational Units for Relevance. See Active Directory - Settings on page 546 for details.
- **Manage Resolvers** – This opens the Resolver Management window that lets you Add, Delete, and Edit resolvers added through a mobile device. See Using Mobile Devices to Interact with Relevance on page 599.
- **Access Groups** – This opens the Access Groups window where you create access groups for Relevance User Services. See Relevance User Services on page 456 for details.
- **Settings (Relevance)** – This opens the Relevance Settings window that lets you define iBeacons and manage Bluetooth filtering.



Install

Install includes:

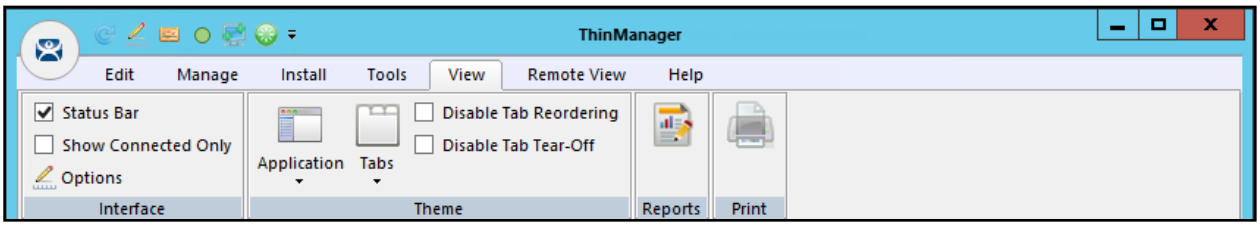
- **Firmware Package** – This allows you to update your firmware packages. The firmware package is a firmware version and the modules for that version.
- **Firmware** – This allows you to update the firmware without updating modules.
- **Modules** – This allows you to update a module without updating the firmware.
- **Boot Loader** – This allows you to update the boot loader used in PXE boot.
- **Chain Loader** – This allows you to update the chain loader used in PXE boot.
- **Licenses** – This launches the Licensing window to add licenses to ThinManager.
- **Licenses** – This allows you to select between the traditional ThinManager licensing or the Rockwell Automation FactoryTalk activation.
- **TermCap Database** – The Terminal Capability Database has information on the abilities of every ThinManager Ready thin client. A new version is released with every newly supported thin client. Service packs update the TermCap but this allows you to update the TermCap if a new unit you have isn't listed.
- **Reports** – This allows you to add a report and SQL query if you need a newly released one before it is added in a service pack.



Tools

Tools include:

- **Restart** – This will resend the configuration to a highlighted Terminal.
- **Reboot** – This will cycle power to a highlighted Terminal and reload the firmware and configuration.
- **Reboot Server** – This will cycle power to a highlighted Remote Desktop Server. Although it will give you a warning prompt, don't select this unless you are serious about restarting a Remote Desktop Server. All sessions end abruptly when the server is rebooted.
- **Power Off** – This will power off a highlighted virtual machine or a thin client with a Wake-On-LAN function enabled.
- **Power On** – This will power on a highlighted virtual machine or a thin client with a Wake-On-LAN function enabled.
- **Calibrate Touchscreen** – This will initiate the calibrate touchscreen program on a highlighted Terminal.
- **Send Message** – This will send a message to a highlighted Terminal.
- **Enable** – This command will re-enable a disabled Terminal, Remote Desktop Server, or location.
- **Disable** – This will disable a highlighted Terminal, Remote Desktop Server, or location.
  A Terminal will stop showing the session but will show a ThinManager splash screen instead. The session will continue running on the Remote Desktop Server.
  A disabled Remote Desktop Server will kick all the ThinManager thin clients off the Remote Desktop Server, forcing them to a backup server. The Remote Desktop Server is still functional and will allow RDP connections from other sources. This is useful for forcing failover to a backup so you can update your Remote Desktop Servers on the fly.
  A location will stop showing the session when disabled.
- **Clear** – This will allow you to clear the event log for the highlighted Terminal or Remote Desktop Server.

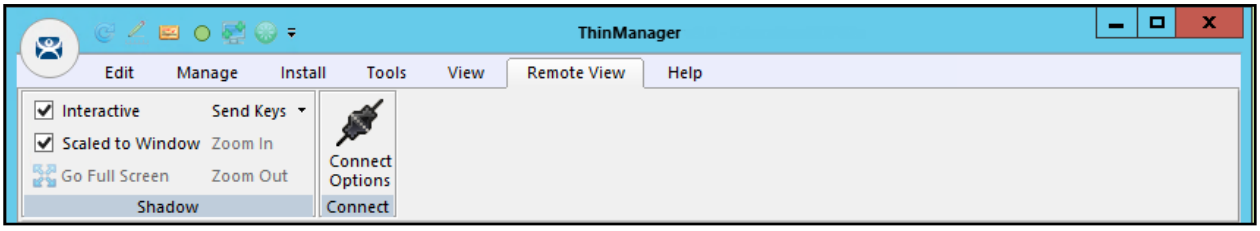


View

View includes:

- **Status Bar** – This checkbox shows the status bar at the bottom of the ThinManager interface.
- **Show Connected Only** – This will hide any unpowered or unconnected thin clients. Although it can be useful it is best left checked as it can be confusing when the unpowered Terminal as hidden.
- **Options** – This launches the Options window with the settings for license notifications, and allows new Terminals and users to initiate a Terminal Configuration Wizard or Relevance User Configuration Wizard.
- **Application** – This lets you choose the color scheme for ThinManager.

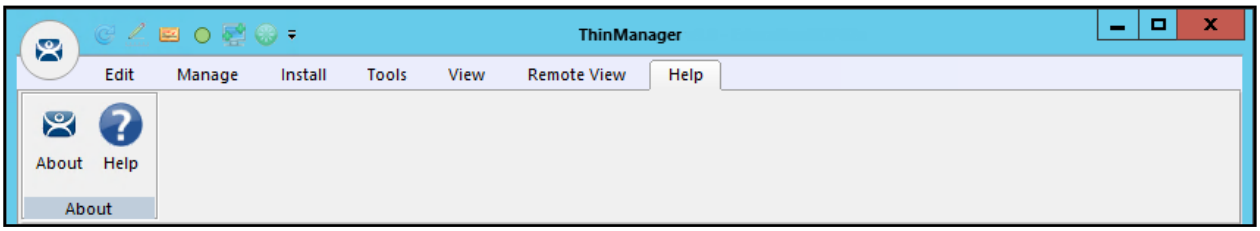
- **Tabs** – This allows you to choose the tab scheme for ThinManager.
- **Disable Tab Reordering** – Normally the Detail Pane tabs can be rearranged. This locks the tabs in their current position.
- **Disable Tab Tear-Off** – Normally the Detail Pane tabs can be dragged free from the ThinManager console. This locks the tabs in their current position.
- **Select Reports** – This opens the Select Reports window that lets you select the reports for the various components. Select the Report tab for a highlighted component to see the actual report or use the Scheduler to generate a report automatically.
- **Print** – This allows you to print a highlighted Report tab.



Remote View

Remote View includes:

- **Interactive** – This allows you to click into a shadowed session and control the session. Unchecking this will make it a "look but don't touch" system.
- **Scaled to Window** – This shrinks the shadowed Terminal to fit into the details pane. Unchecking this will show it in the correct resolution with scroll bars to give you a closer view.
- **Go Full Screen** – This will make the shadowed Terminal's image full screen. This can be reversed by selecting the ***CTL+ALT+Break*** buttons. If you go full screen and forget the key sequence use ***ALT+F4*** to close ThinManager. It will close the full screen session.
- **Send Keys** – This sends the selected key sequence to a shadowed Terminal.
- **Zoom In** – This allows you to click inside a shadowed session and zoom in for detail. The Interactive checkbox must be unchecked.
- **Zoom Out** – This allows you to click inside a shadowed session and zoom out for an overview. The Interactive checkbox must be unchecked.
- **Connect Options** – This allows you to configure the RDP settings when you connect to a Remote Desktop Server console from ThinManager.



Help

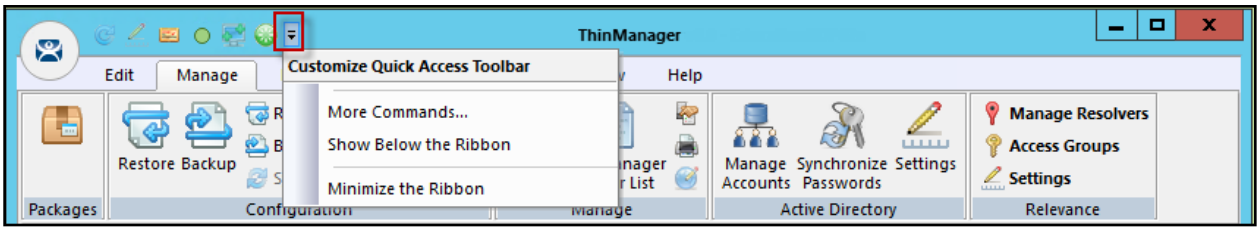
Help includes:

- **About** – This will show the version and build number of ThinManager.
- **Help** – This launches the ThinManager help.

5.2. Customizing the Toolbar

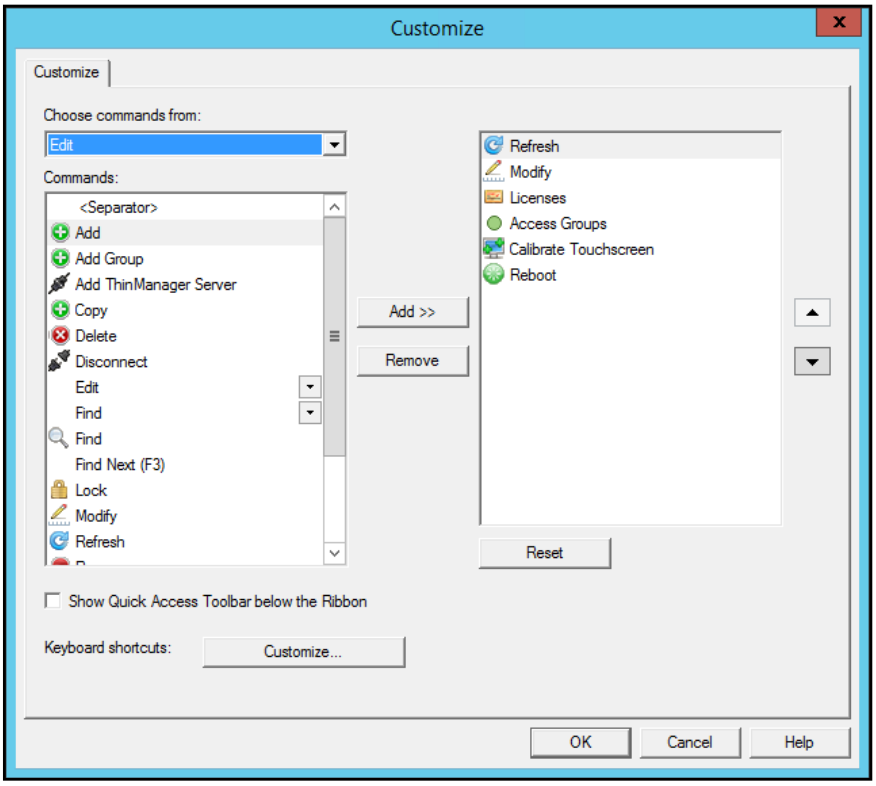
The ThinManager toolbar has a Quick Access area in the title bar that can be customized by adding icons of your most commonly used functions.

Launch the Customize window by selecting the small drop-down arrows to the left of the ThinManager title.



Customize Quick Access Toolbar Menu

Select ***More Commands…*** from the **Customize Quick Access** Toolbar Menu. This will launch the Customize window.



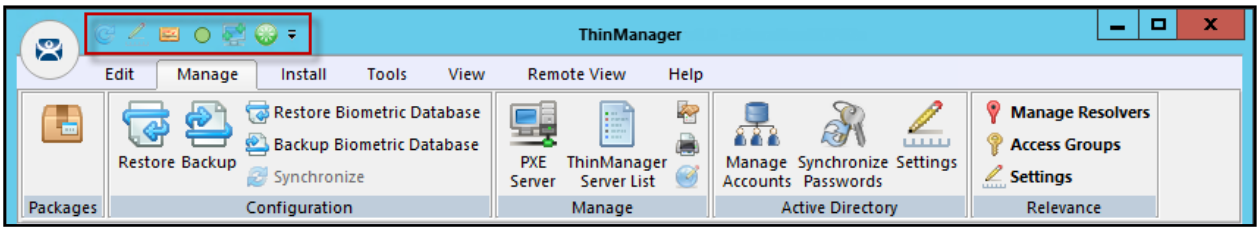
Customize Window

The Commands list on the left is the available command options. Selecting one and moving it to the right list will add it to the **Quick Access** bar.

The ***Choose commands from*** drop-down allows you to select commands from each menu group.

The ***Show Quick Access Toolbar below the Ribbon*** checkbox will move the Quick Access bar.

Once you have selected your commands, and adjusted the order using the ***Up*** and ***Down*** arrows, you can save your commands by selecting the ***OK*** button.



Quick Access Tool Bar

The icons for the selected functions will appear in the Quick Launch menu. Clicking one will launch that function or wizard.

5.3. Icons

The ThinManager Tree has Icons to show the status of the components.

5.3.1. ThinManager Server

ThinManager Server Tree Icons

The ThinManager Server branch has two ThinManager icons.

- **Green ThinManager –** This means that the ThinManager console is talking to the ThinServer**.**
- **Red ThinManager –** This means that the ThinManager console is not talking to the ThinServer. Right click on the icon and select Reconnect from the right click menu.

Note: You should not add the second ThinManager Server of a synchronized pair in the tree of your Primary ThinManager Server. The data is the same.
Adding a second ThinManager Server is intended to display a remote connection to a different system.

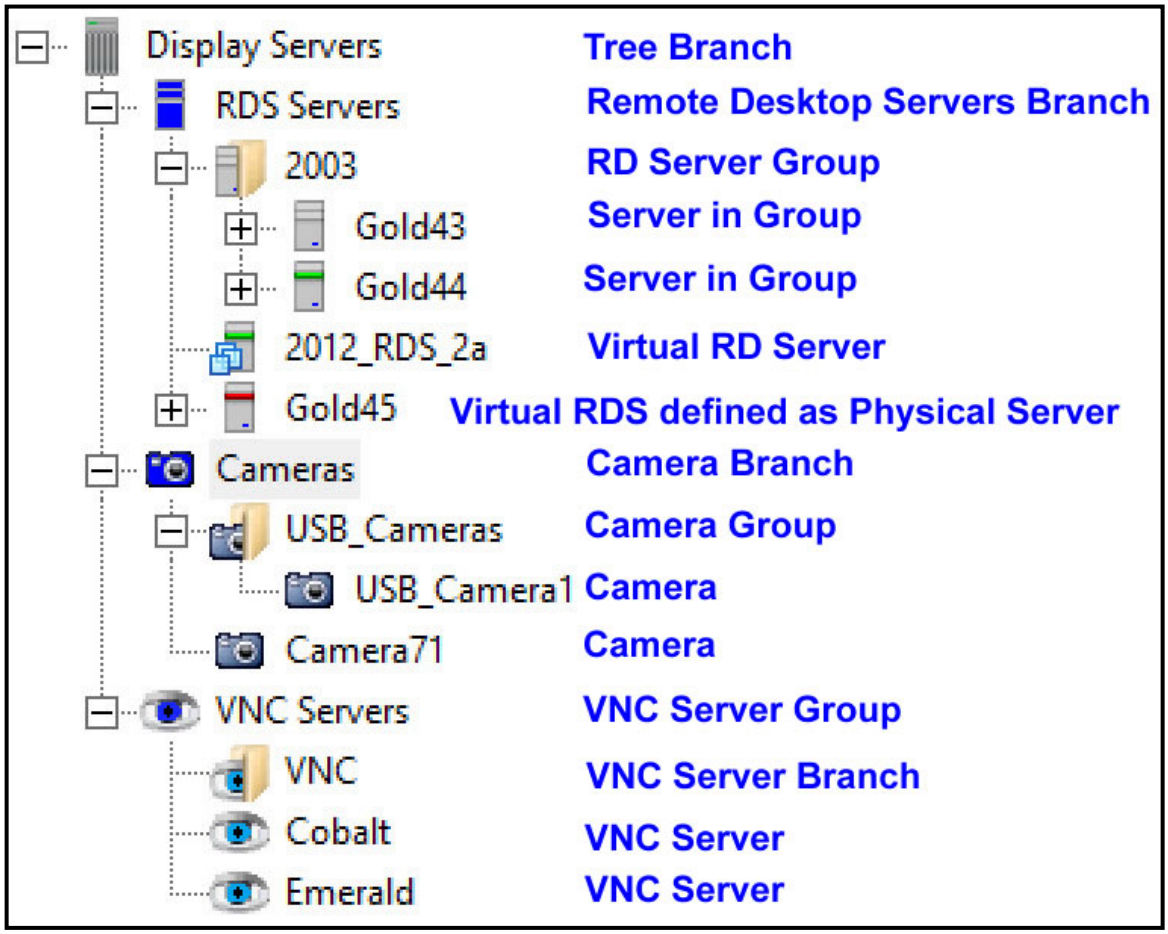
5.3.2. Terminals

Terminal Tree Icons

The Terminal branch of the ThinManager tree has several different icons.

- **Dual Monitor** – This represents a Terminal Group.
- **Lock** – This represents a Terminal that has its configuration wizard open.
- **Exclamation Mark** – This represents a Terminal that has had its configuration changed and needs a restart.
- **Globe** – This represents a Terminal with an assigned Location. The location will be shown in parentheses.
- **Green Monitor** – This represents a Terminal that is booted and connected to the ThinManager Server.
- **Yellow Monitor** – This represents a Terminal that is going through the boot process.
- **User** – This represents a Terminal that has a Relevance User logged in to the Terminal. The user name will be shown in parentheses.
- **Red Monitor** – This represents a Terminal that is either turned off or not able to communicate with the ThinManager Server.
- **Red X** – This represents a Terminal that was Disabled using the ***Tools>Disable*** command.

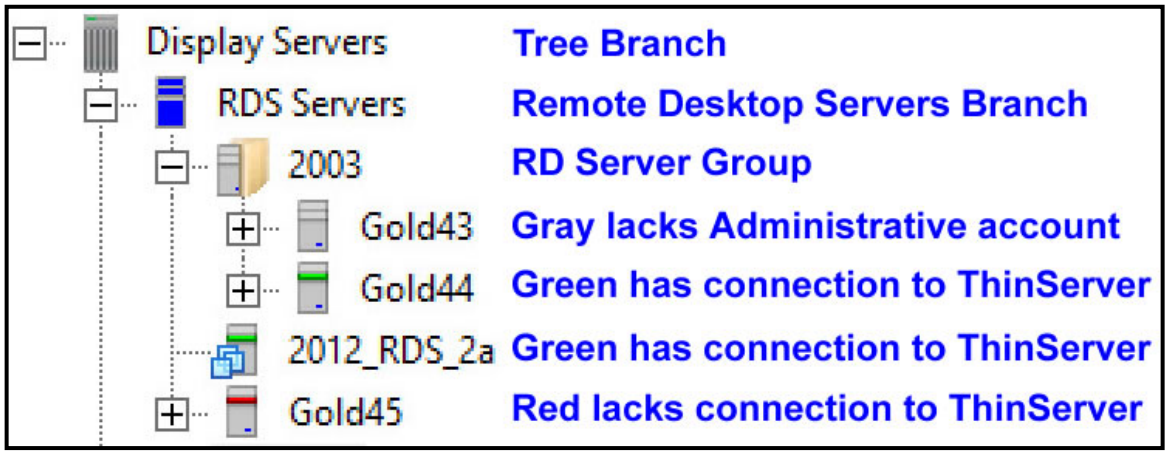
5.3.3. Display Servers



Display Server Tree Icons

The Display Server tree has several different icons.

- **Blue Server** – This represents the Remote Desktop Server branch.
- **Server with Folder** – This represents a Remote Desktop Server Group.
- **Server with Gray Stripe** – This represents a Remote Desktop Server without an administrative account.
- **Server with Green Stripe** – This represents a Remote Desktop Server with a connection to the ThinServer using an administrative account.
- **Server with Red Stripe** – This represents a Remote Desktop Server with an account but unable to make a connection to the ThinServer.
- **Server with Virtual Boxes** – This represents a Virtual Server defined through the VCenter Server tool.
- **Blue Camera** – This represents the Camera branch.
- **Camera with Folder** – This represents a Camera Group.
- **Gray Camera** – This represents a Camera.
- **Blue Eye** – This represents the VNC Server branch.
- **Cyan Eye with Folder** – This represents a VNC Server Group.
- **Cyan Eye** – This represents a VNC Server.



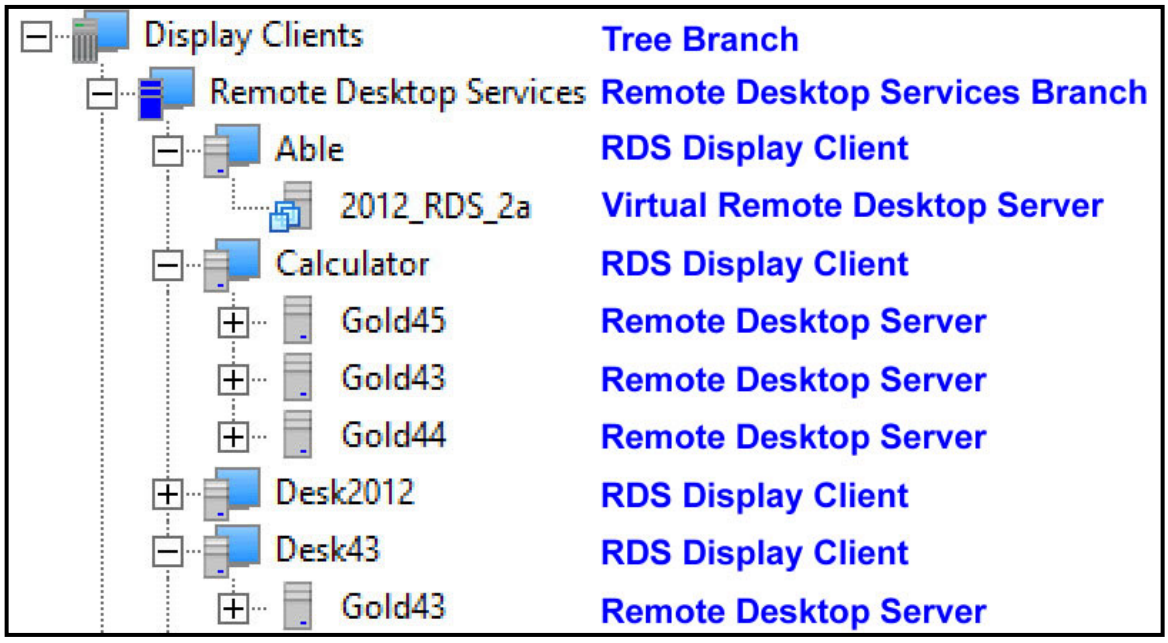
Remote Desktop Server Icon Colors

The color stripe on a Remote Desktop Server icon indicates its connection status.

- **Server with Gray Stripe** – This represents a Remote Desktop Server without an administrative account.
- **Server with Green Stripe** – This represents a Remote Desktop Server with a connection to the ThinServer using an administrative account.
- **Server with Red Stripe** – This represents a Remote Desktop Server with an account but unable to make a connection to the ThinServer.

Note: A red stripe does not mean that a Terminal can't connect to the Remote Desktop Server. It only indicates the status of the ThinManager Server to Remote Desktop Server communication.

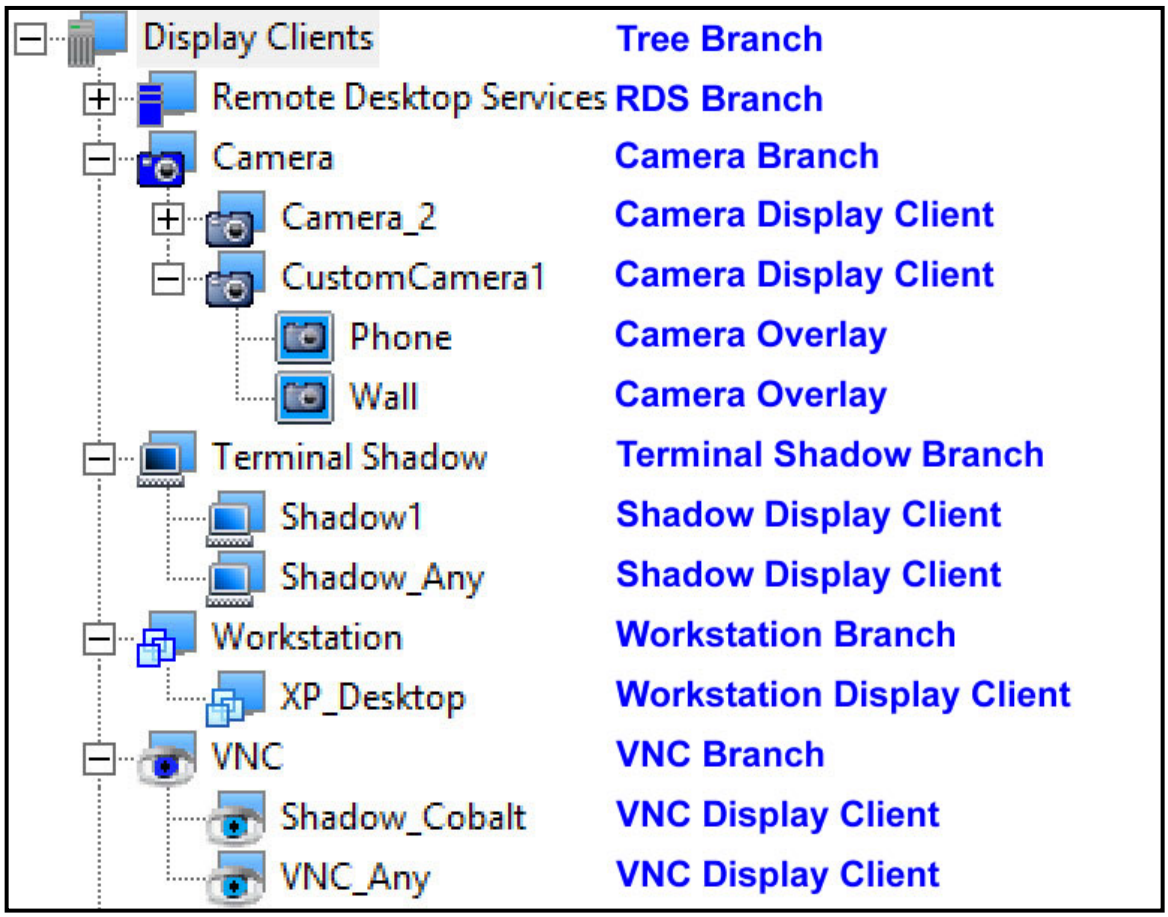
5.3.4. Display Clients



Remote Desktop Services Display Client Branch Icons

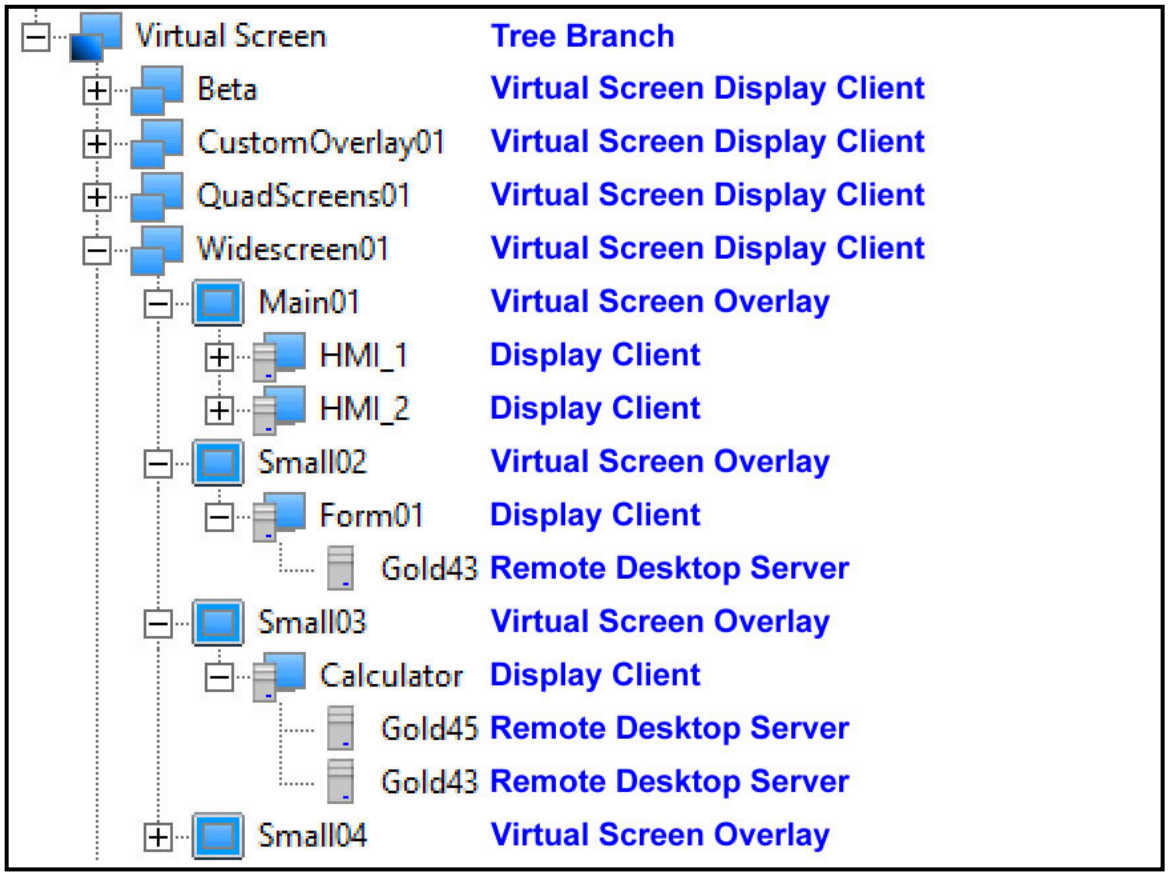
The Display Client branch has several icons.

- **The Dark Gray Server and Blue Monitor** – This represents the Display Client Tree Branch.
- **The Blue Server and Blue Monitor** – This represents the Remote Desktop Services Branch.
- **A Light Gray Server and Blue Monitor** – This represents a Remote Desktop Services Display Client.
- **A Gray Server** – This represents a Remote Desktop Server assigned to a Display Client.



Other Display Client Branch Icons

- **The Dark Gray Server and Blue Monitor** – This represents the Display Client Tree Branch.
- **The Blue Server and Blue Monitor** – This represents the Remote Desktop Services Branch.
- **The Blue Camera and Blue Monitor** – This represents the Camera Branch.
- **A Gray Camera and Blue Monitor** – This represents a Camera Display Client.
- **A Gray Camera inside a Blue Box** – This represents a Camera Overlay assigned to a Display Client.
- **The Dark Blue Terminal and Blue Monitor** – This represents the Terminal Shadow Branch.
- **The Light Blue Terminal and Blue Monitor** – This represents the Terminal Shadow Display Client.
- **The Dark Blue Virtual Boxes and Blue Monitor** – This represents the Workstation Display Client Branch.
- **The Medium Blue Virtual Boxes and Blue Monitor** – This represents the Workstation Display Client.
- **The Dark Blue Eye and Blue Monitor** – This represents the VNC Server Branch.
- **The Light Blue Eye and Blue Monitor** – This represents the VNC Server Display Client.



Virtual Screen Display Client Branch Icons

- **The Dark Blue Monitor and Blue Monitor** – This represents the Virtual Screen Branch.
- **The Blue Monitor and Blue Monitor** – This represents the Virtual Screen Display Client.
- **The Blue Square within a Blue Monitor** – This represents the Virtual Screen Overlay.
- **A Light Gray Server and Blue Monitor** – This represents a Display Client. Assigned to the Overlay.
- **A Light Gray Server** – This represents a Remote Desktop Services Server assigned to the Display Client on the Overlay.

5.3.5. Lightning Bolts

Icons with lightning bolts indicate the connection status.

Lightning Bolts

- **Green Lightning Bolt** – This is a connection that is active and visible in the foreground.
- **Yellow Lightning Bolt** – This is a connection that is active but not visibly displayed. It is usually running in the background. An Instant Failover display client will show servers with a green and a yellow to show the main and secondary session.
- **Red Lightning Bolt** – This is a connection that is defined but not active.

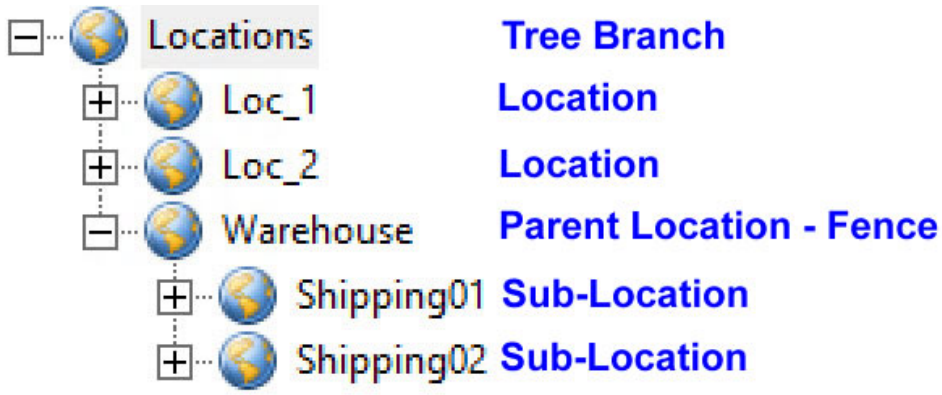
5.3.6. Relevance Users

Relevance Users Tree

- **The Light Blue Person** – This represents the Relevance User Tree Branch
- **Two People** – This represents a Relevance User Group.
- **Red Person** – This represents a Relevance User.

- **Red Person with Blue Monitor** – This represents a Relevance User that is logged into a Terminal or Location. The Terminal will be displayed in parentheses.

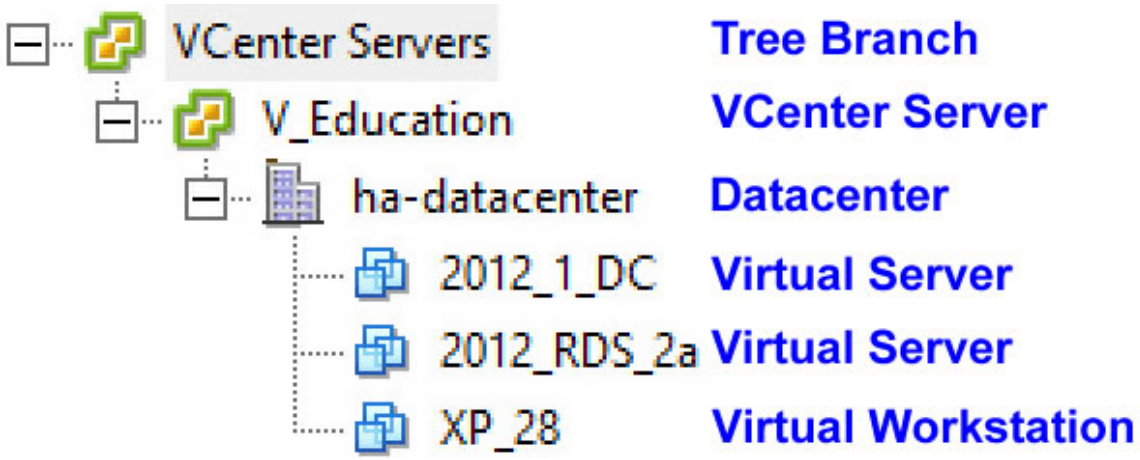
5.3.7. Locations



Locations Tree

- **Globe** – This represents the Location Tree Branch, Locations, Parent Locations, and Sub-Locations.

5.3.8. VCenter Servers



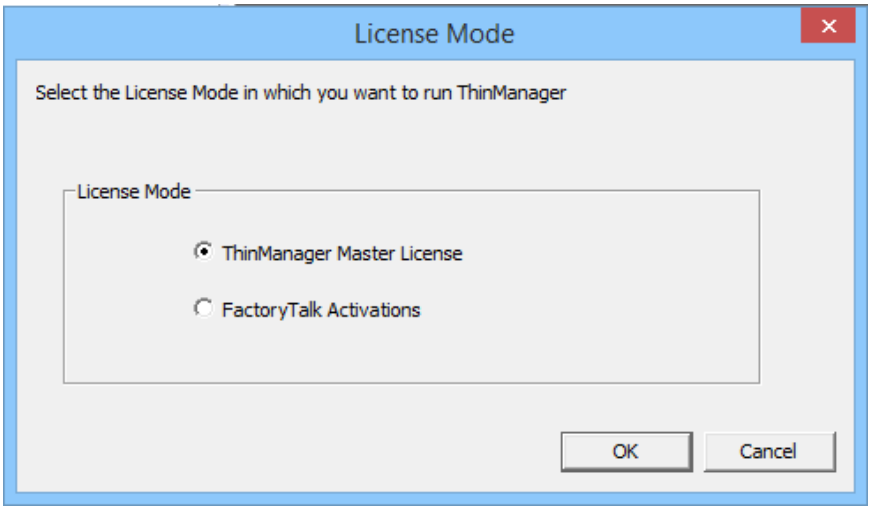
VCenter Servers

- **Green and Yellow Squares** – This represents either the VCenter Tree Branch or a VCenter Server.
- **Gray Building** – This represents a VCenter Server Datacenter.
- **Blue Virtual Squares** – This represents a Virtual Machine, both server and workstation.

6. Licensing

ThinManager has two licensing modes, **ThinManager Master License** and **FactoryTalk Activations**.

Opening ***Install>License Mode*** from the ThinManager menu will open the **License Mode** window to let you select the mode.



License Mode Window

6.1. ThinManager Master License

The ThinManager Master License is the traditional ThinManager license. The ThinManager license is composed of three components:

- **Product License** – This is the license that provides the permission for Terminals to connect and controls what features and functions the Terminals have. This is purchased from a ThinManager distributor.
- **Master License** – The Master License is a container for the Product Licenses. It is created by the user on the ThinManager License site and has the Product Licenses added to it and then is activated with the Installation ID from the Licensing window of the ThinManager application.
- **Activated License File** – This is a file generated from the Master License and Installation ID on the ThinManager License site. It is downloaded and applied the ThinManager.

Product Licenses are connection licenses purchased from ThinManager distributors. The standard license pack is available as in 5-pack, 10-pack, and 25 pack quantities. There is also an Enterprise Server with unlimited connections.

Note: Greater detail on ThinManager licensing is found in the ThinManager Knowledge Base at https://kb.thinmanager.com/index.php/License_Activation.

6.1.1. ThinManager Redundancy

Standard Product Licenses can be purchased with Redundancy. Enterprise Server licenses include full redundancy.

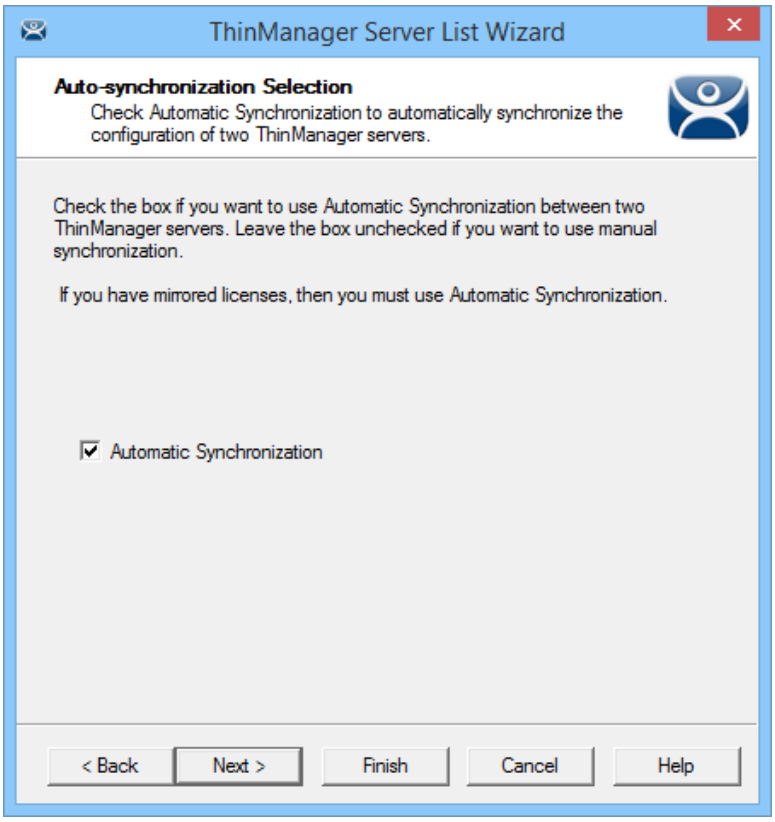
- **Full Redundancy** will license a synchronized pair of ThinManager Servers so that one ThinManager Server will be available if one it offline. Both synchronized ThinManager Servers will have the administrative console available.

- **Mirrored Redundancy** will also license a synchronized pair of ThinManager Servers so that one will be available if one it offline but the less expensive Mirrored Product License only activates the administrative console on one ThinManager Server. The ThinManager Server with the administrative console is designated as the Primary ThinManager Server. The other ThinManager Server is designated as the Secondary. Terminals can boot from the secondary but ThinManager console is view only.
- **Stand Alone ThinManager** will license one stand-alone ThinManager. If the stand-alone ThinManager goes offline the Terminals will continue to run. However if a Terminal reboots it will wait until the ThinManager Server is online before it can rejoin the system.

6.1.2. Auto-synchronization for Redundancy

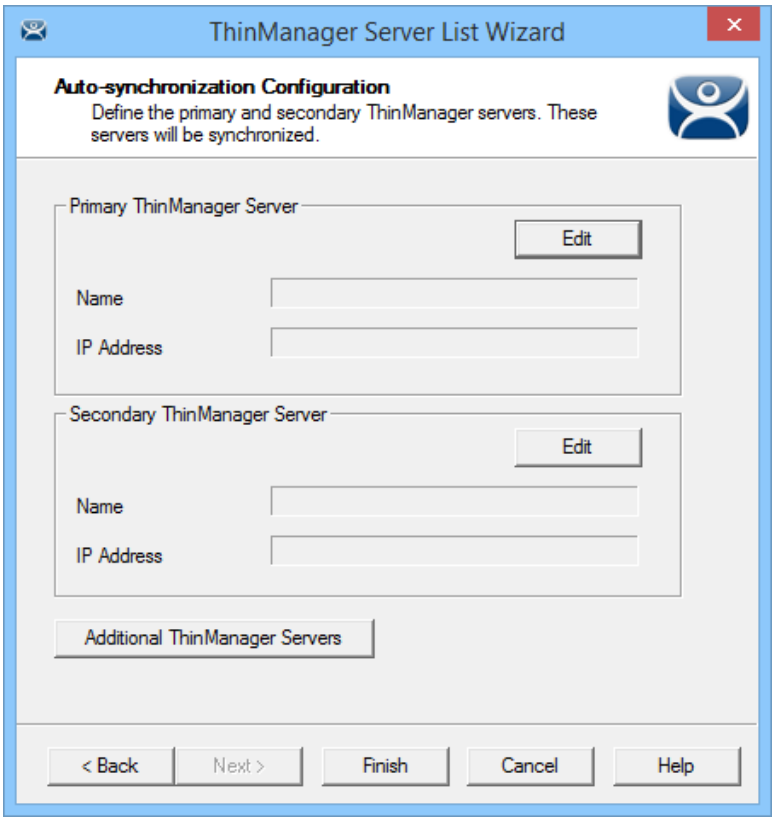
If you plan on having a Redundant ThinManager system you need to configure Auto-synchronization.

1. Install ThinManager on two servers
2. Open the ThinManager Server List wizard on your Primary ThinManager Server by selecting ***Install>ThinManager Server List*** from the menu bar.
3. Select the ***Automatic Synchronization*** checkbox on the **Auto-synchronization Selection** page.



Auto-synchronization Selection Page

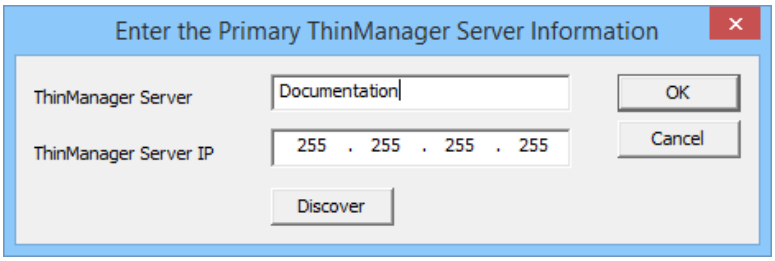
Checking the ***Automatic Synchronization*** checkbox on the **Auto-synchronization Selection** page starts the synchronization configuration.



Auto-synchronization Configuration Page

4. Enter a Primary ThinManager Server and a Secondary ThinManager Server on the **Auto-synchronization Configuration** page.

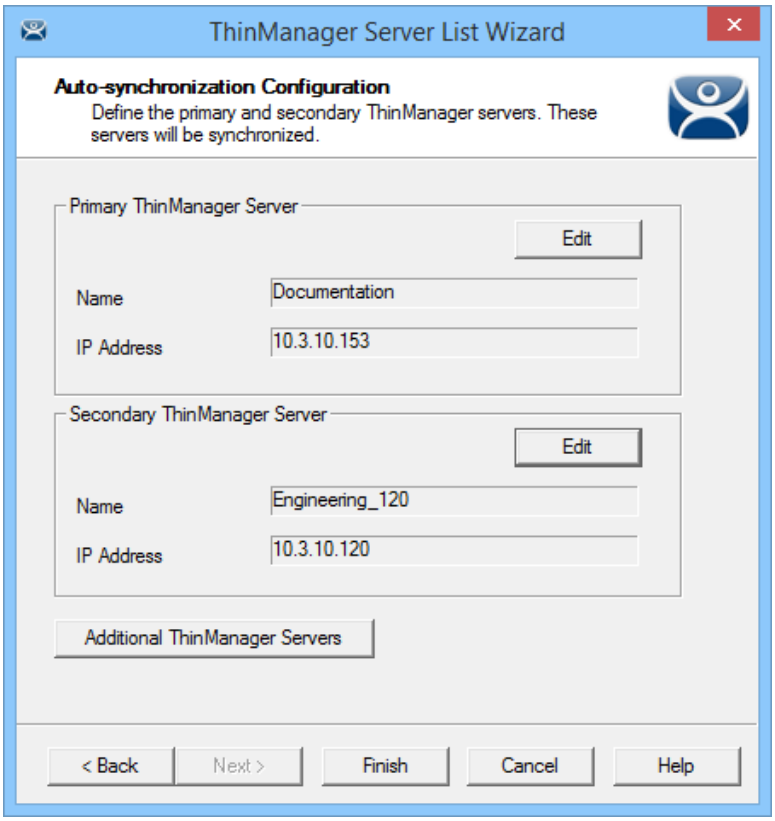
Selecting the ***Edit*** button will open a window that allows you to designate your ThinManager Servers.



Enter the ThinManager Server Information Window

Enter the name of your Primary ThinManager Server in the **ThinManager Server** field and select the ***Discover*** button to automatically populate the IP address in the **ThinManager Server IP** field. This field can be filled manually.

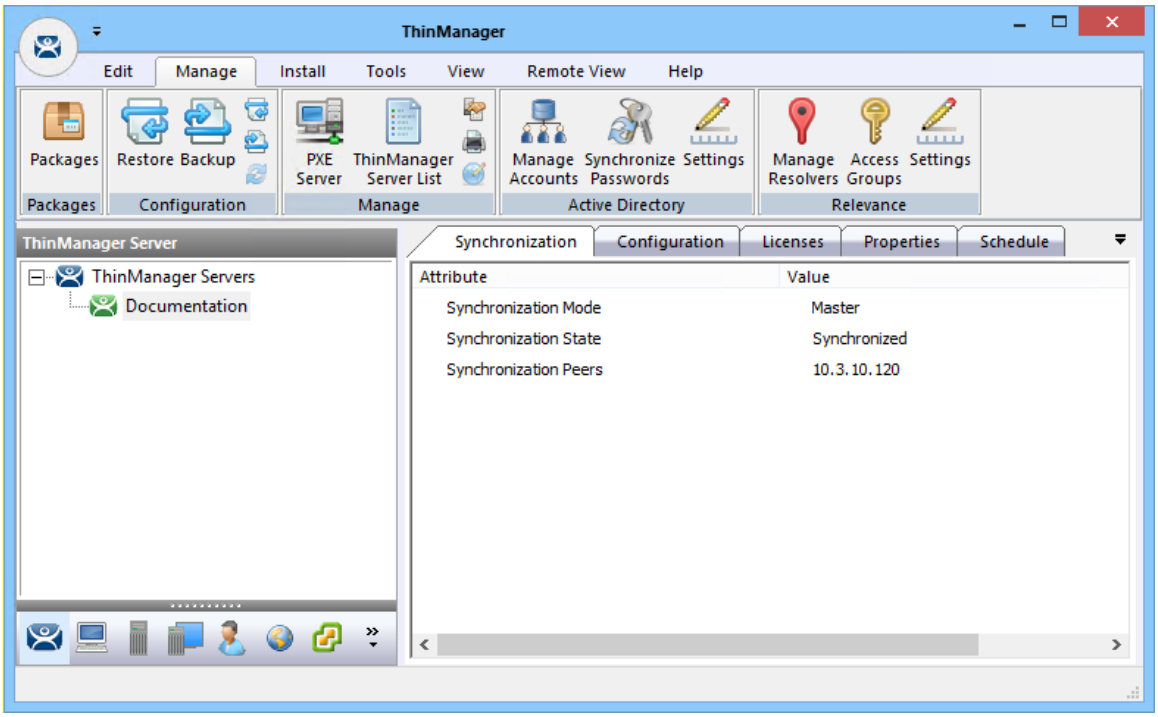
Repeat with the Secondary ThinManager Server by selecting the second ***Edit*** button.



Auto-synchronization Configuration Page

Once the ThinManager Servers are entered and the wizard is closed the auto-synchronization will begin.

Note: It is important to select the Primary and Secondary carefully because only the Primary ThinManager Server will have an administrative console with a Mirrored License. The Secondary is view only.



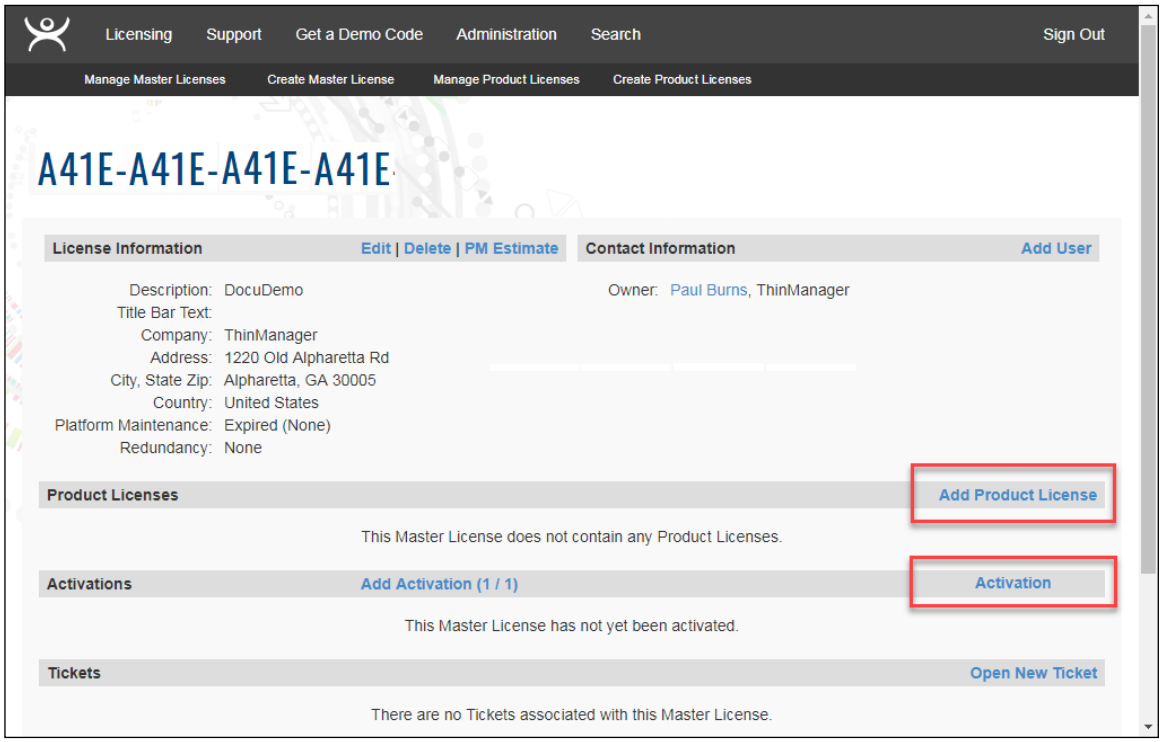
Synchronization Tab

Synchronization can be checked on the **Synchronization** tab when the ThinManager Server is highlighted in the ThinManager Server branch of the ThinManager tree.

6.1.3. ThinManager Licensing Process

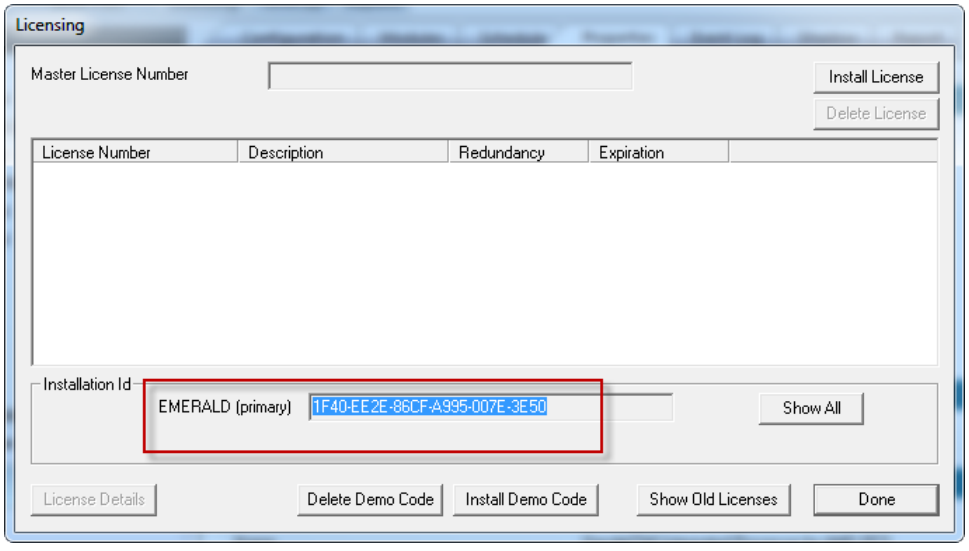
The steps for ThinManager Licensing are:

1. Purchase a Product License from a ThinManager distributor.
2. Synchronize two ThinManager Servers if you have a redundant product license. See Auto-synchronization for Redundancy on page 35.
3. Go to the ThinManager Licensing site at https://thinmanager.com/licensing/.
4. Log in to the site or register as a new user and log in with the new user account.
5. Select the ***Create Master License*** link on the License Site menu bar.
6. Enter a description and fill in the other fields. Select the ***Create*** button.



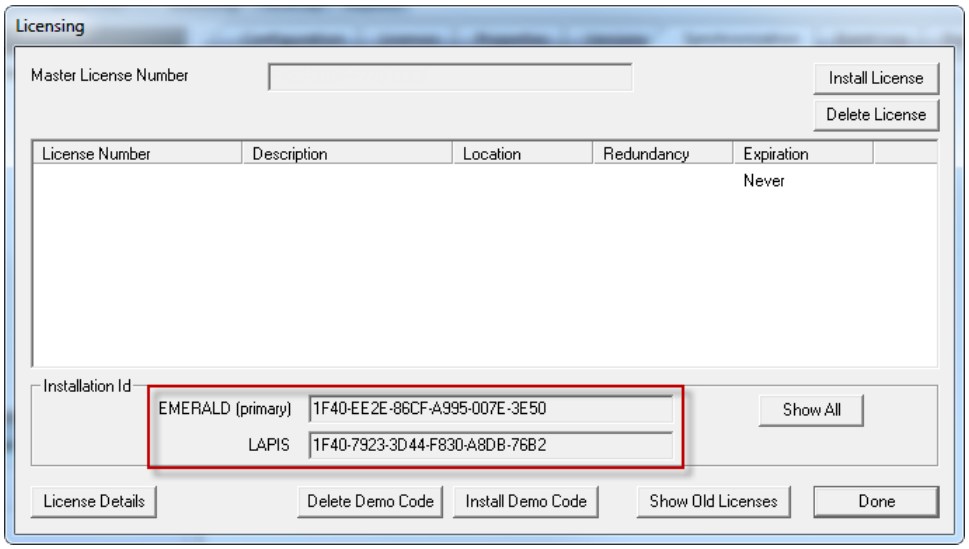
Master License Page of ThinManager Licensing Site

7. The License site will show the Master License. Select the ***Add Product License*** link and enter the Product License.
8. Select the ***Activation*** link once the Product License(s) are added. Enter the Installation IDs. These are found on the Licensing Window that is opened by selecting ***Install>Licenses.***



Installation ID on the Licensing Window

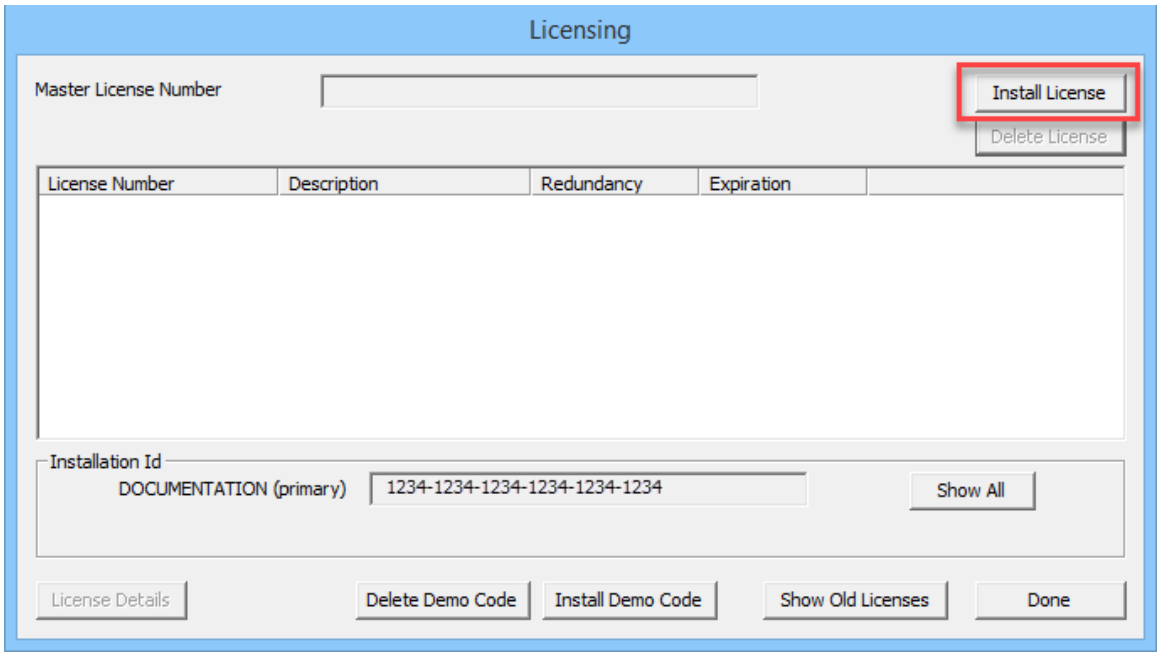
A stand-alone ThinManager will have a single Installation ID at the bottom of the **Licensing** window.



Installation ID on the Licensing Window

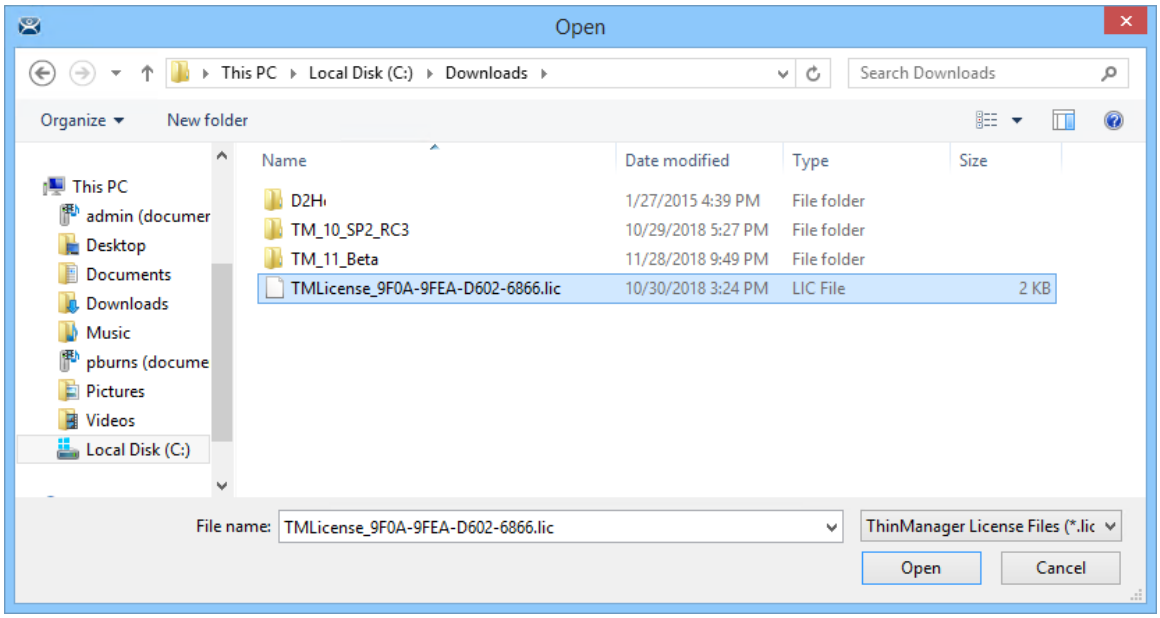
A synchronized ThinManager system will display both the Primary and Secondary Installation ID at the bottom of Licensing window.

9. Select the ***Create*** button at the bottom of the form once the Installation IDs are added.
10. Select the ***Download Li***cense link and save the license file. Move the license file to the ThinManager Server but not into the ThinManager folder.
11. Open the **Licensing** window by selecting ***Install>Licenses*** in the ThinManager menu.



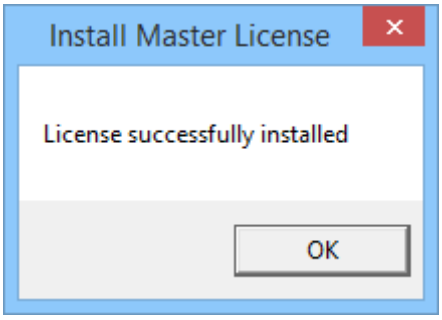
Install License Button on the Licensing Window

12. Select the ***Install License*** button.



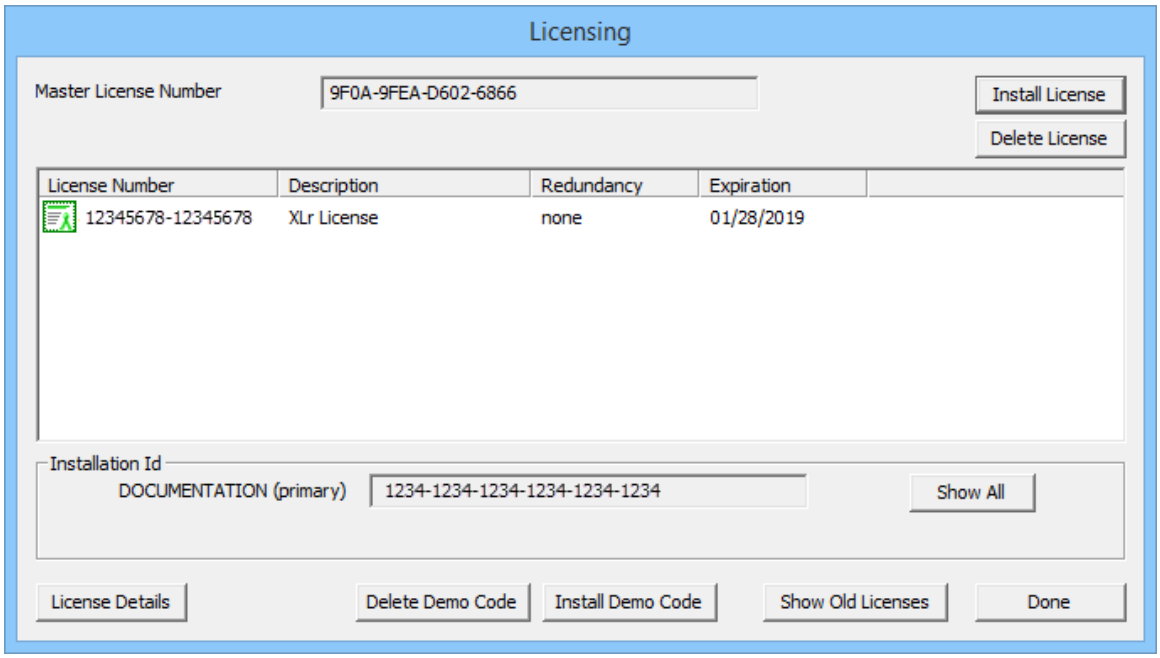
File Browser

13. Browse to the License file and select the ***Open*** button.



Install Master License Dialog

A properly installed license will show a notification.



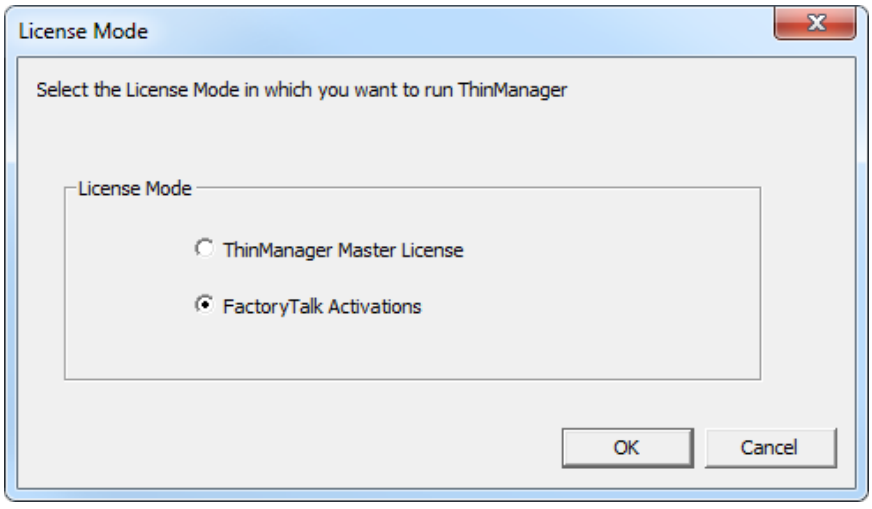
Installed License

A successfully installed license will show the Master License in the field at the top, the Product License(s) in the box in the center, and the Installation ID(s) in the field at the bottom.

6.2. FactoryTalk Activation

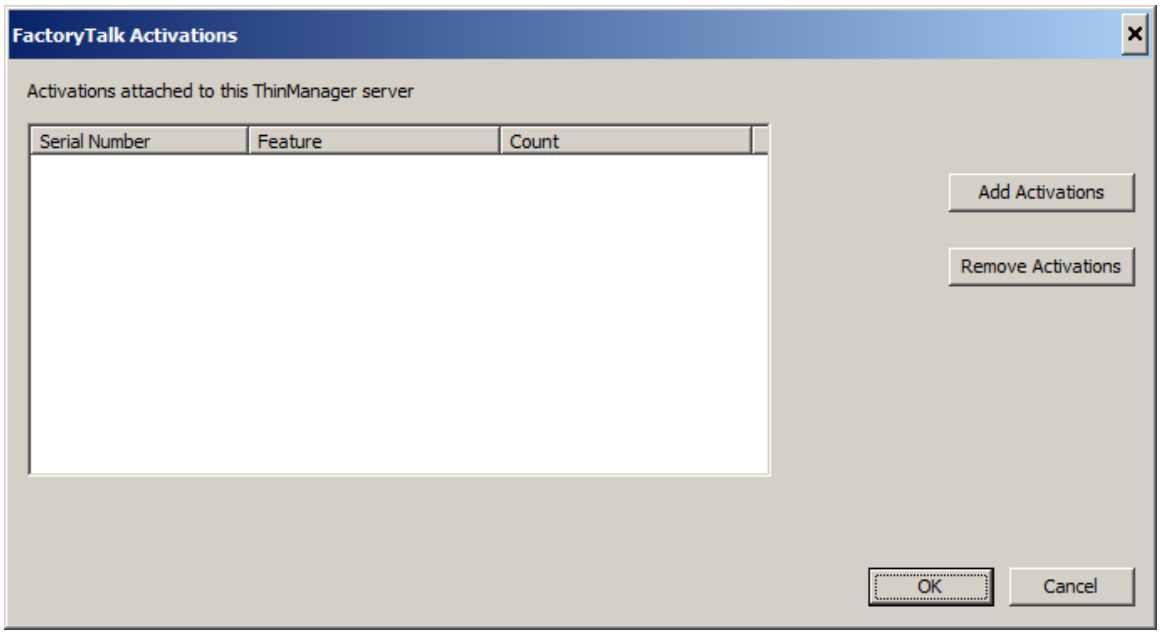
ThinManager has two licensing modes, **ThinManager Master License** and **FactoryTalk Activations**.

Opening ***Install>License Mode*** from the ThinManager menu will open the License Mode window to let you select the mode.



FactoryTalk Activation

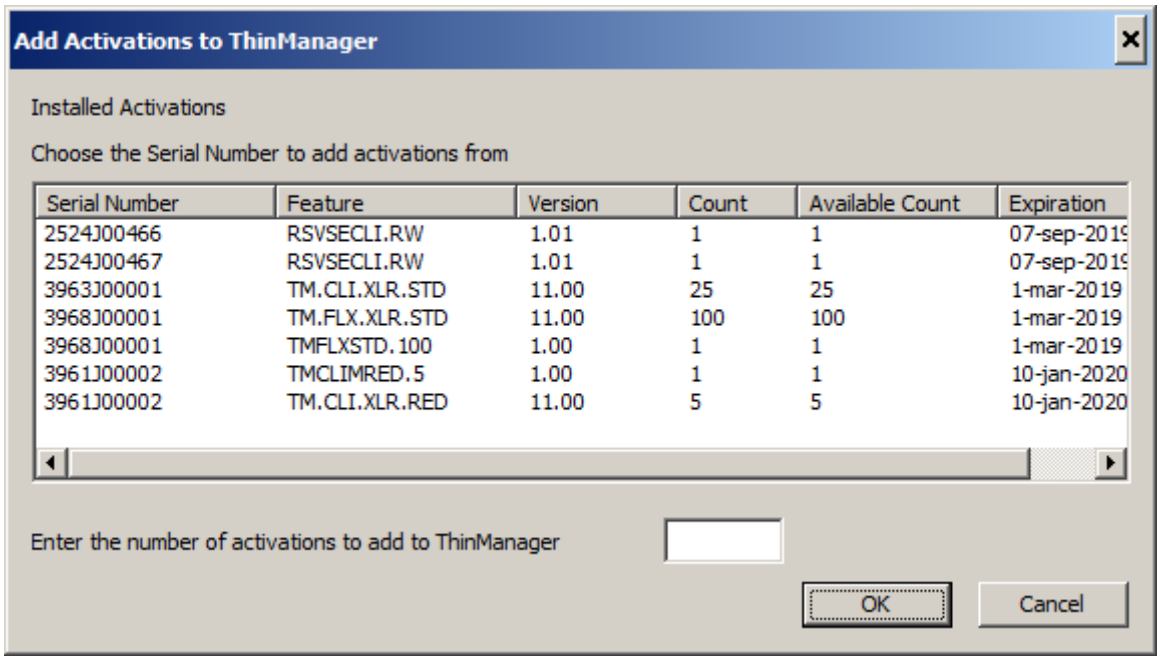
Select the ***FactoryTalk Activations*** radio button and select the ***OK*** button to go into the FactoryTalk Activation Mode.



FactoryTalk Activations

Select ***Install>Licenses*** to open the **FactoryTalk Activations** window once ThinManager has been put into the FactoryTalk Activation mode.

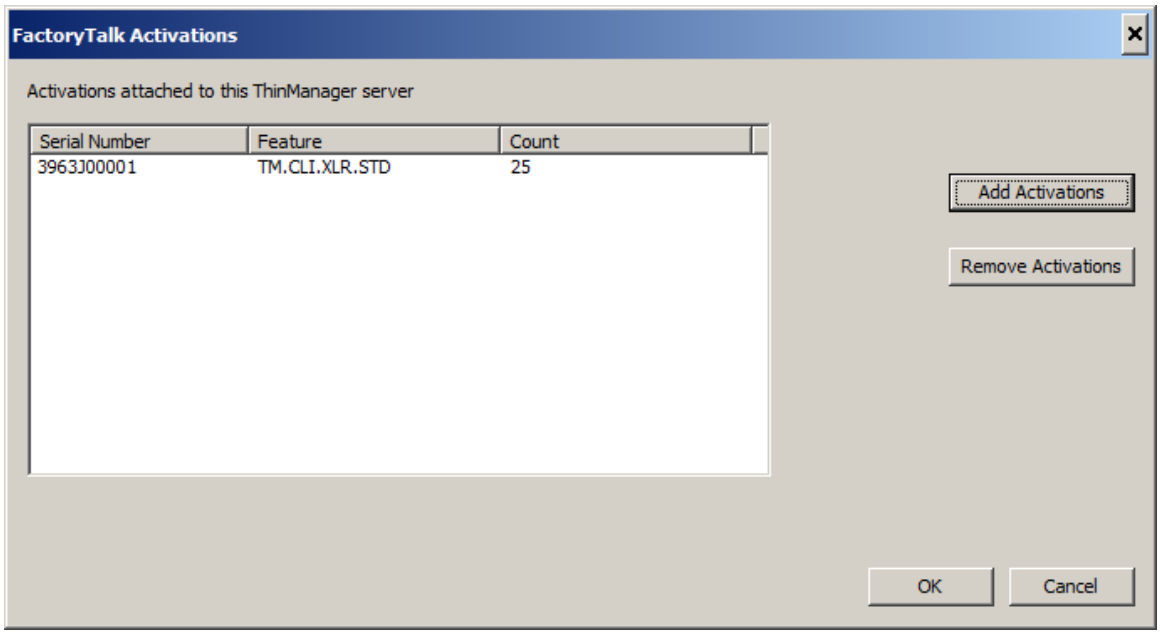
Select the ***Add Activation*** button to launch the **Add Activations to ThinManager** window.



Add Activations to ThinManager Window

The **Add Activations to ThinManager Window** will search the FactoryTalk activations and display them in the window.

Highlight the license you want to use with ThinManager and select the ***OK*** button. You can specify how many licenses to add by entering a number in the ***Enter the number of activations to add to ThinManager*** field.



FactoryTalk Activations Window

The **FactoryTalk Activations** window will show the FactoryTalk licenses transferred once you select the ***OK*** button.

7. Users in a ThinManager System

There are three types of users in a ThinManager system. They are Windows Users, Relevance Users, and ThinManager Security Group Users. The Windows users may be local accounts or domain accounts.

7.1. Windows Users

Windows Users are the Microsoft accounts created in Windows that allow access to the Windows Remote Desktop Servers. These are configured within Windows and authenticated by Windows. They can be given varying levels of access and power using Windows User Groups and Group Policies.

All users and Terminals need a Windows account to log in to a Remote Desktop Server. These accounts need to be members of the Remote Desktop User group.

Note: Each Terminal or Location needs a unique Windows account as a Microsoft best practice.

ThinManager 8 introduced **Active Directory** integration to the ThinManager system. This is covered in Users - Active Directory User Login Account on page 343.

7.2. ThinManager Security Group Users

ThinManager Security Group Users are Windows User Group members who have been configured in the ThinManager Server Configuration Wizard to have varying levels of access and control within the ThinManager program. This is about access to the administrative console of ThinManager and not access to a Windows application.

ThinManager Security Groups are configured on the **ThinManager Security Groups** page of the **ThinManager Server Configuration wizard**. See ThinManager Server Configuration Wizard on page 419.

7.3. Relevance Users

Relevance Users are users who can go to a ThinManager Ready thin client and receive access to specific Display Clients due to their membership in an Access Group. The login and authentication is done by ThinManager a level above the Windows login. This feature was originally called TermSecure but has been integrated into the Relevance suite of functions.

Relevance User Services gives additional powers to grant or deny access to Windows applications but still relies on a Windows user account to login to a Remote Desktop Server.

There are different strategies for Relevance Users.

- ❑ If a user is using a **Terminal-specific Application** then they don't require a Windows account since they will be accessing the application belonging to the Terminal. They do need the Permission from an Access Group to open a hidden application.
- ❑ If a user is accessing their own **User-specific Applications** then they need a Windows account associated with them so they can log in and start these sessions.
  - The Relevance User can be created from an Active Directory account.
  - The Relevance User can be created to match the name of a Windows account and use that Windows account without using Active Directory.
  - The Relevance User can be created with one name and be associated to a Windows account of a different, aliased name.

See Users - Active Directory User Login Account on page 343 for details.

8. Sources – Remote Desktop Servers

Microsoft servers with the Terminal services or remote desktop role provide the foundation of thin client computing. It consolidates management of the Windows environment to mainframe architecture. This was originally called Terminal Services but is now called Remote Desktop Services. This document will use Remote Desktop Server for the computer and operating system and will use Remote Desktop Services for the connection using the Remote Desktop Protocol.

First you need to build and configure the server using standard Microsoft practices.

Second, you need to define the server as a Display Server in ThinManager.

8.1. Microsoft Configuration

Note: Microsoft is the authority on their servers and you should refer to them for instructions on the use and configuration of their server. This information is included as a courtesy.

Here are a few common tips.

- ❑ Build a Remote Desktop Server with Microsoft 2008, 2008R2, 20012, or 2016 Server operating system. Enable Terminal Services in 2008 Server or Remote Desktop Services in 2008R2, 2012, and 2016 Server.
  The 2012 and 2016 Servers usually require a domain.
- ❑ Create a Microsoft Licensing Server and add a Remote Desktop Services Client Access License, or RDS CAL, for each thin client. These are called TS CALs (Terminal Services CALs) in Server 2008 and earlier.
  This does not need to be a separate physical server but can be a role added to an existing server. The servers also require a normal CAL.
- ❑ Create a unique Microsoft user profile for each Terminal on the Remote Desktop Server. Make sure that the user is a member of the Remote Desktop Users Windows group.

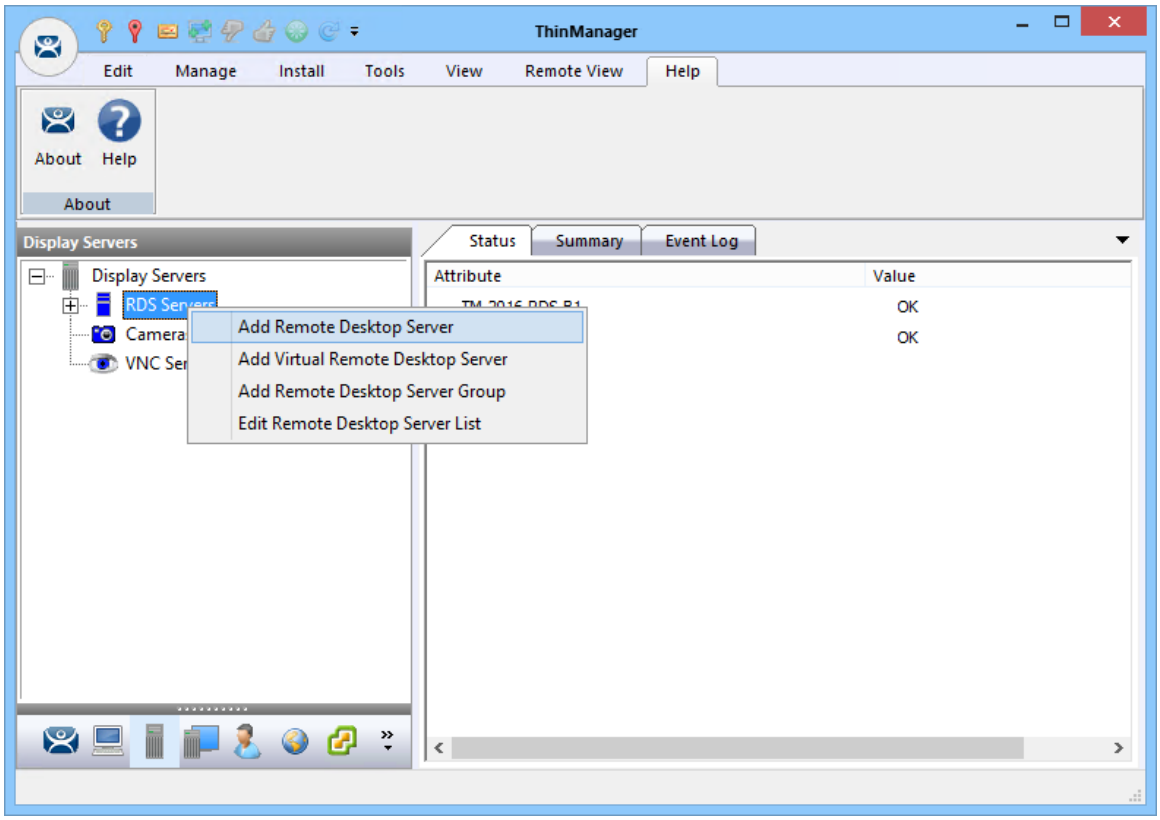
- Apply appropriate security to each user profile using the standard Microsoft techniques.
- Install all applications in the **Install** Mode. This can be done by typing **`change user /install`** in a command window or by using the ***Install Application on Remote Desktop Server*** in the Control Panel.

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.
- **TCP/1494** - Citrix - Used by the ICA protocol if using ICA instead of RDP.
- **TCP/3389** - RDP - Used by the Microsoft RDP protocol.
- **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. The MTU packet size can be changed on the Multicast Configuration page of the ThinManager Server Configuration Wizard.
- **TCP/3268** – Used for LDAP queries targeted at the global catalog with Active Directory.
- ICMP Echo Packets (Ping) – Used by WinTMC and Enforce Primary.

8.2. Defining Remote Desktop Servers in ThinManager

Once the Remote Desktop Servers are built you must define them as Display Servers in ThinManager.



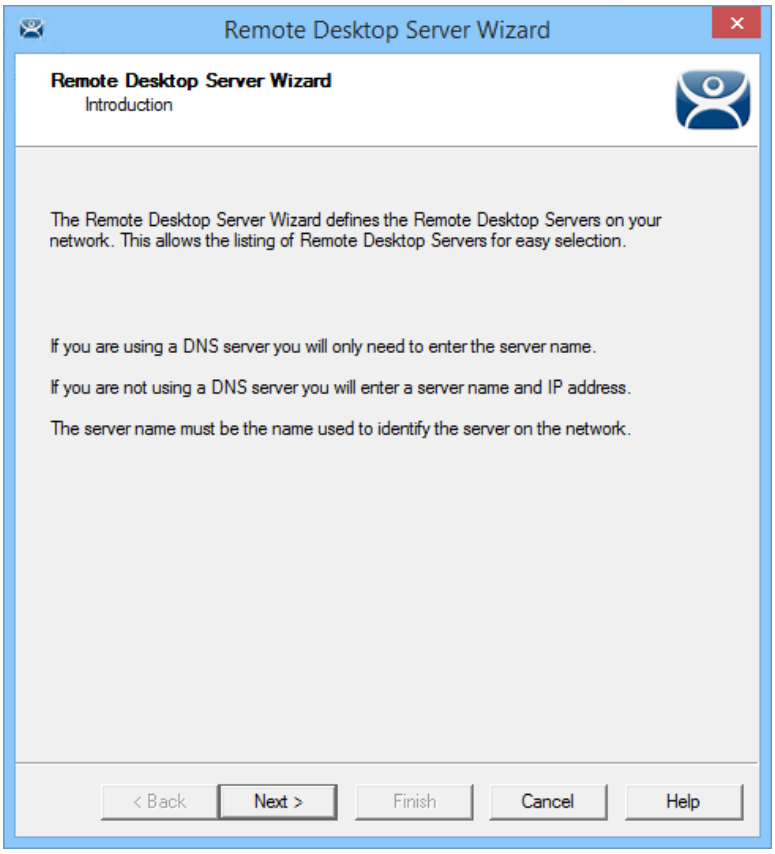
Display Server Branch of the ThinManager Tree

Go to the **Display Server** branch of the ThinManager tree.

Right Click on the **RDS Servers** branch to open the menu.

Select ***Add Remote Desktop Server*** to launch the **Remote Desktop Server Wizard** to define the Remote Desktop Server.

Run the wizard for each Remote Desktop Server you want to add to the system.

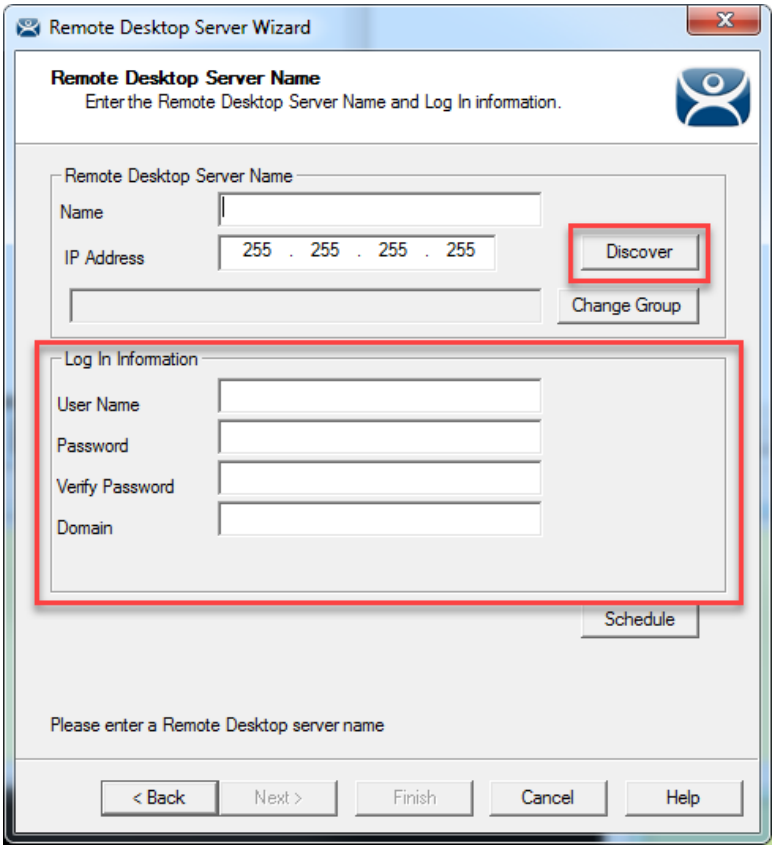


Introduction - Remote Desktop Server Wizard

The first page of the wizard talks about DNS. Go to ***Manage > DNS Configuration*** to define your DNS server if you are using one. If this is done you just need to use the name and not the IP addresses.

8.2.1. Non-Domain Remote Desktop Server

The **Remote Desktop Server Name** page allows you to define the Remote Desktop Server.



Remote Desktop Server Name - Remote Desktop Server Wizard – Non-Domain

List your Remote Desktop Server in the ***Remote Desktop Server Name*** field of the **Remote Desktop Server Name** page.

✓ **Use the *Discover* button to validate the server name and automatically fill in the IP addresses.**

Clicking the ***Discover*** button will validate the name and will fill in the ***Remote Desktop Server IP*** if the name is correct and the server is reachable. This is a great tool that checks spelling mistakes and prevents connection problems.

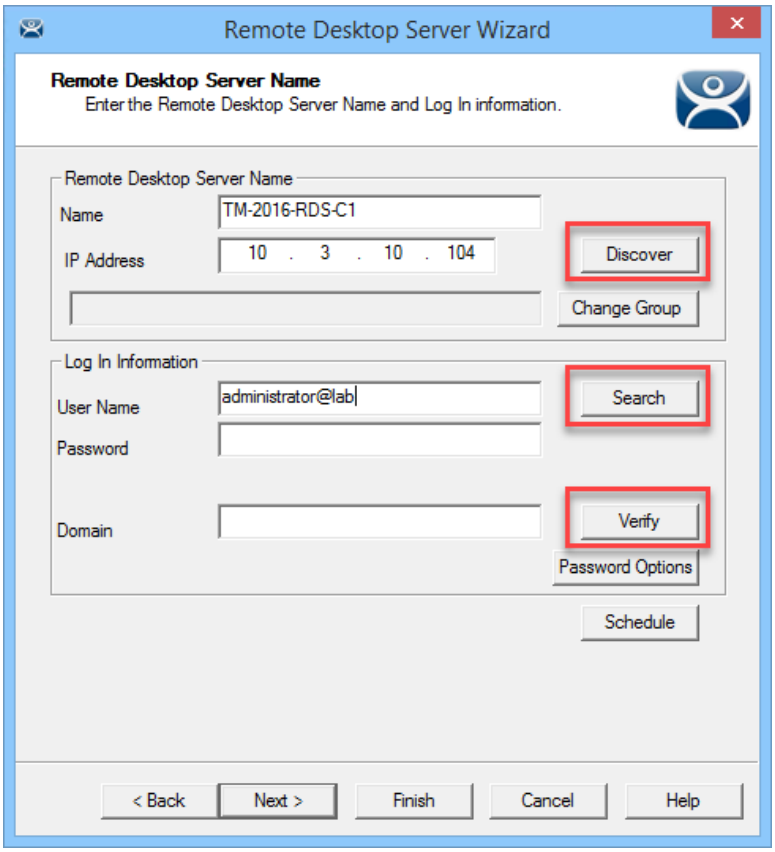
✓ **Add an administrative account to the Log In Information fields.**

The ***Log In Information*** fields are for an administrative account on the Remote Desktop Server. This is needed for SmartSession load balancing and server management from ThinManager. The ThinServer will connect to the Remote Desktop Server to retrieve CPU, Memory, and Session status for load balancing but the Microsoft server will only give the information to an administrator. By entering an administrative account from the remote server the ThinServer will be able to access the information that is critical for SmartSession load balancing.

The ***Change Group*** button will allow you to add the Remote Desktop Server into a Remote Desktop Server Group as a configuration short cut.

The wizard will warn you if the passwords don't match.

8.2.2. Domain Member Remote Desktop Server

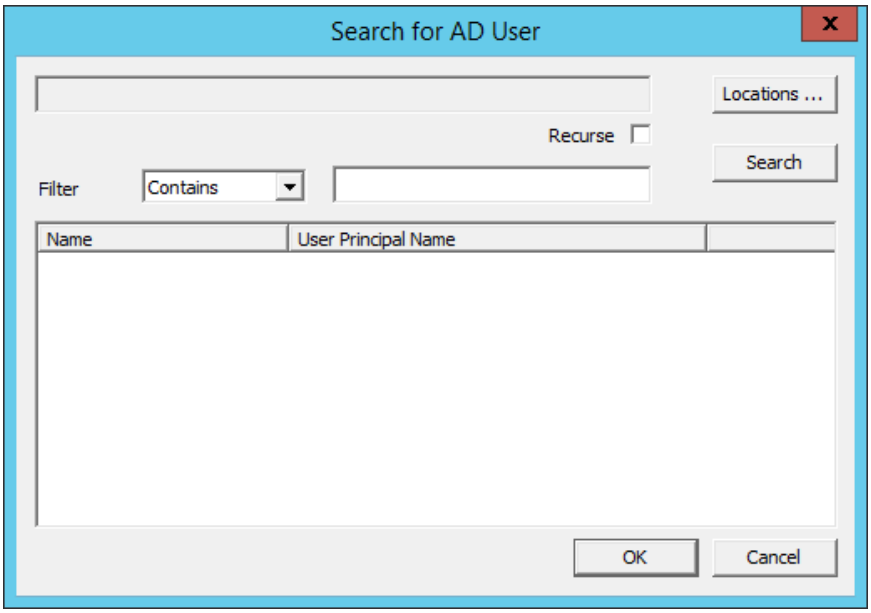


Remote Desktop Server Name - Remote Desktop Server Wizard –Domain

A ThinManager Server is a domain has a ***Search*** button in addition to the ***Discover*** button. This launches a series of windows that allow you to select a domain user account for the administrative login.

✓ **Use the Search button to add an administrative account to the Log In Information fields.**

Selecting the ***Search*** button will launch a **Search for AD User** window that allows you to select an Active Directory user.



Search for AD User Window

The **Search for AD User** window has a Location button that allows you to search the Active Directory locations.

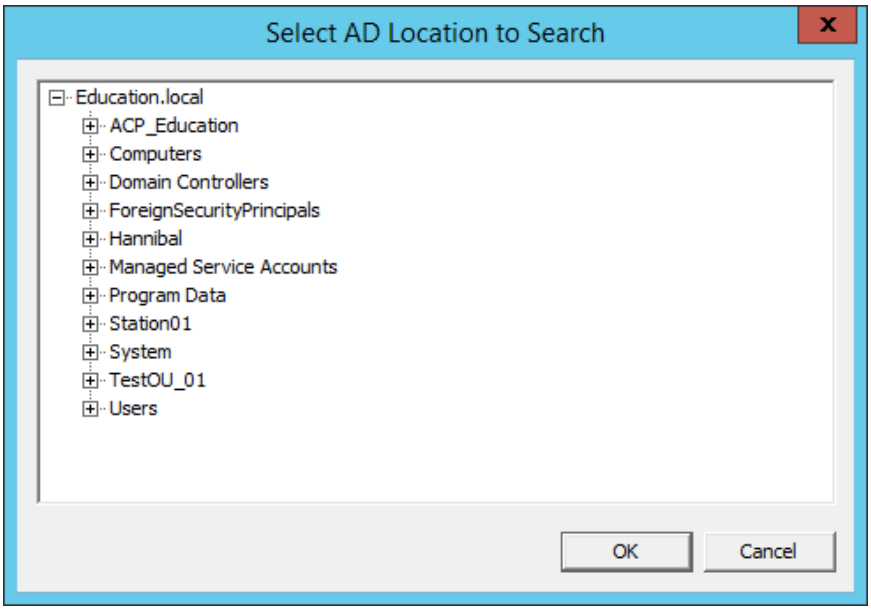
Buttons:

- ***Locations*** – This opens the **Select AD Location to Search** window to select the Organizational Unit (OU) to search.
- ***Search*** – This searches the selected OU and populates the ***Name*** field with the OU members.

Options:

- ***Filter*** – This drop-down will filter the results with either the ***Contains*** or ***Starts With*** function and the entry of the textbox.
- ***Recurse*** – This sets the ***Search*** function to search nested Windows Security Groups when searching a Windows Security Group. The ***Choose AD Synchronization Mode*** needs to be set to **Security Group** on the **Active Directory System Settings** window to work. This window is opened from ***Manage > Active Directory > Settings***.

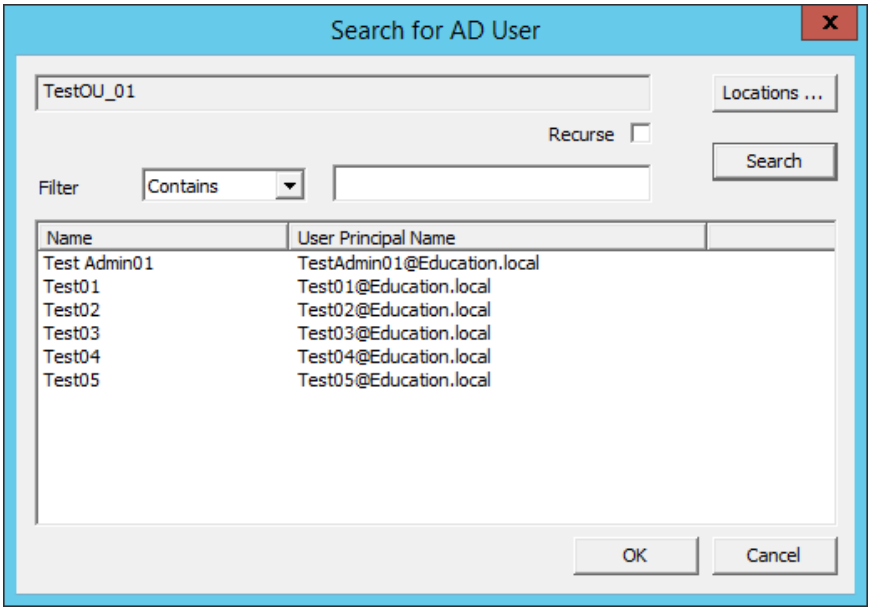
Select the ***Locations…*** button to launch the **Select AD Location to Search** window.



Select AD Location to Search Window

Continue with the wizard by selecting the branch of the Active Directory tree that contains your administrative user account.

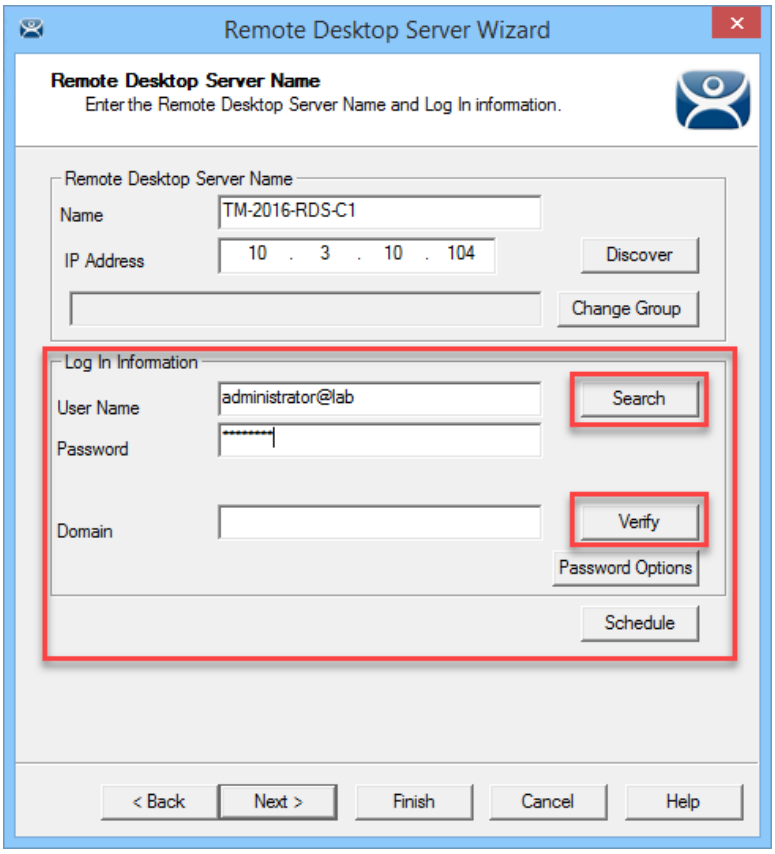
Highlight it and select the ***OK*** button.



Search for AD User Window

Highlighting an Active Directory branch in the **Select AD Location to Search** window and selecting the ***OK*** button will re-open the **Search for AD User** window with the list of domain users from that branch.

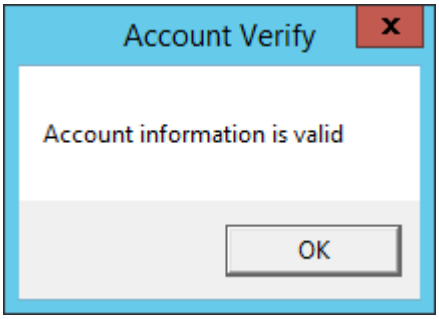
Highlight the desired user and select ***OK***. This will add the domain user to the ***User Name*** field of the Remote Desktop Server Wizard.



Remote Desktop Server Name - Remote Desktop Server Wizard –Domain

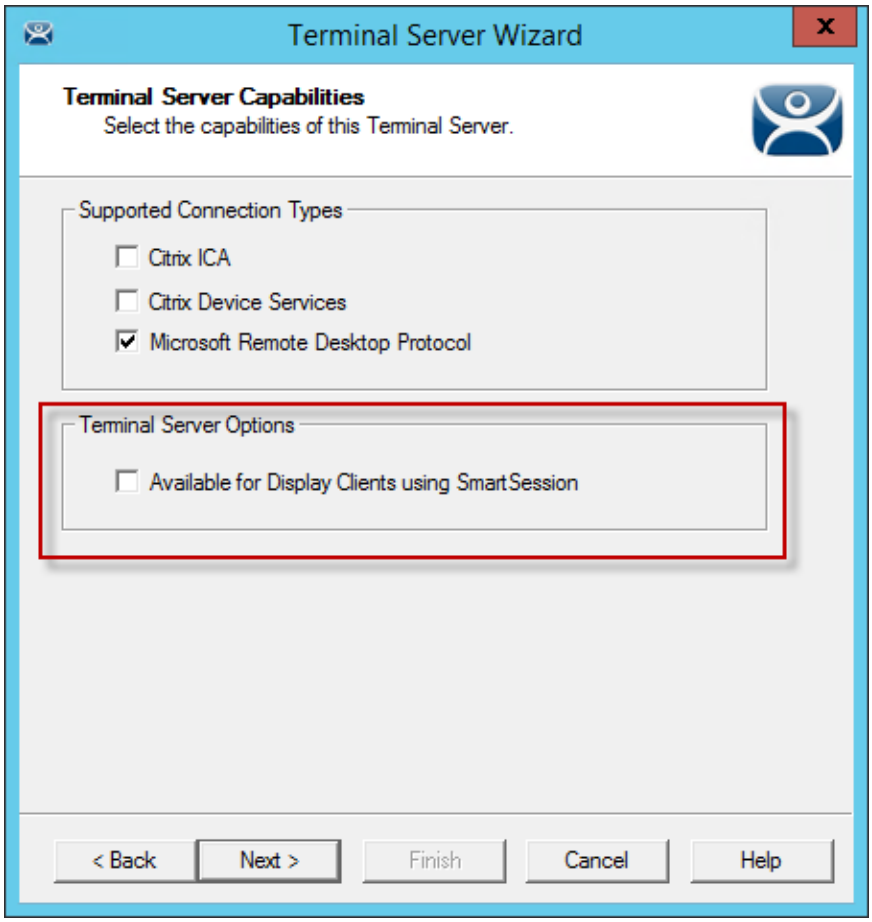
Once the domain user is in the ***User Name*** field of the Remote Desktop Server Wizard you need to add the correct password to the ***Password*** field.

The ***Verify*** button will check the entered password and tell you if it is valid or incorrect.



Account Verify Dialog

Once you have received a positive result select the ***Next*** button to continue with the wizard.

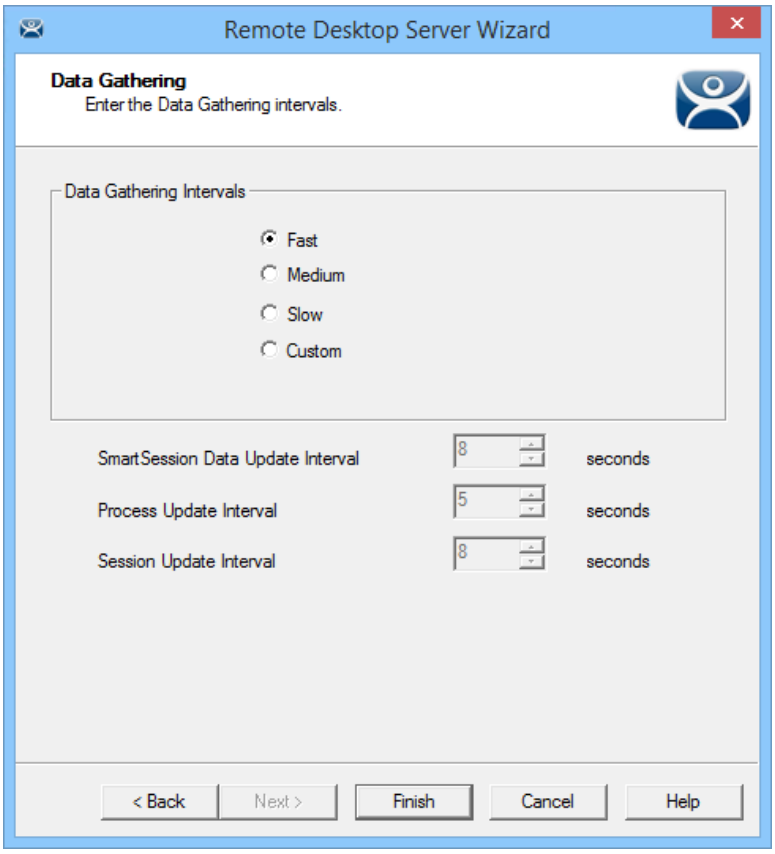


Remote Desktop Server Capabilities - Remote Desktop Server Wizard

✓ **Check the "Available for Display Clients using SmartSession" checkbox to use the Remote Desktop Server with SmartSession**

SmartSession load balancing uses the **CPU levels**, **Memory usage**, and **Session coun**t to calculate the resources available for the Terminals. ThinManager needs to poll the server every 8 seconds to maintain accurate status levels. However, you don't need to poll the server if you aren't using SmartSession. For this reason SmartSession polling is turned off by default.

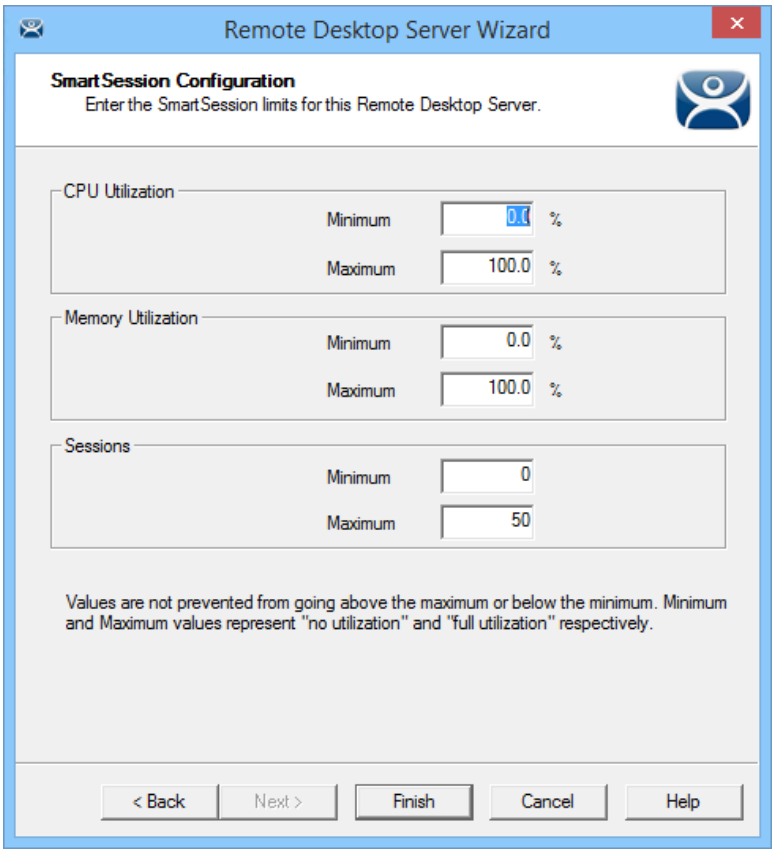
You need to check the ***Available for Display Clients using SmartSession*** checkbox to activate SmartSession.



Data Gathering Page - Remote Desktop Server Wizard

The **Data Gathering** page allows you to set the speed and frequency that ThinManager polls the Remote Desktop Servers. This covers both SmartSession and the data on the Users, Sessions, and Processes tabs of the server.

The default ***Fast*** interval should be fine but it can be changed for less frequent polling or set to custom values.



SmartSession Configuration Page - Remote Desktop Server Wizard

If you activate SmartSession load balancing by checking the ***Available for Display Clients using SmartSession*** checkbox on the Remote Desktop Server Capabilities page then the wizard will show the SmartSession Configuration page that allows you to tweak SmartSession load balancing.

Note: Values are not prevented from exceeding the maximum or minimum. The values represent the levels that 'No Utilization' or 'Full Utilization' is reached.

See SmartSession on page 129.

Select the ***Finish*** button to accept the changes and close the wizard.

✓ **Repeat for each Remote Desktop Server that you will use.**

8.2.3. Citrix Servers

Support for Citrix ICA has been deprecated starting with ThinManager Server 9.0. As such, the ability to configure a Remote Desktop Services Display Client to use Citrix ICA has been removed by default. This decision was made because ICA is a proprietary protocol that prevents it from being fully supported by all of the latest features of ThinManager (i.e.: cannot be used with mobile clients, Tiling, Virtual Screens, etc.). With that said, it is still possible to enable ICA in ThinManager. To allow ICA configuration for ThinManager 9.0 and newer, follow the steps below:

Open the registry editor and navigate to one of the below options depending on your deployment:

- 32-bit Windows, or 64-bit ThinManager on 64-bit Windows:
  - HKEY_LOCAL_MACHINE\SOFTWARE\Automation Control Products\ThinManager
- 32-bit ThinManager on 64-bit Windows:

- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Automation Control Products\ThinManager

Add a new DWORD value named SupportICA with a value of 1

Restart the ThinServer service

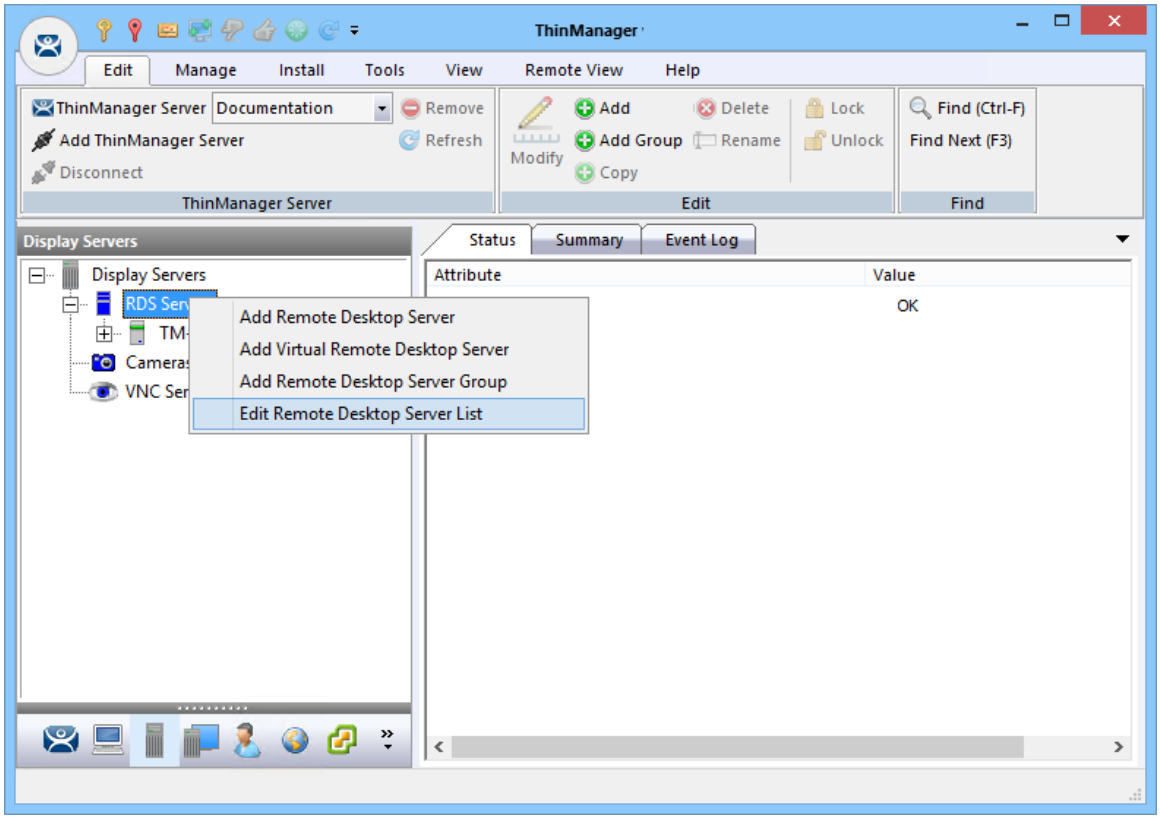
If this is a redundant system, you will want to make this change on both servers. This is a onetime change, you will not have to make it again in the future, for example after upgrading.

It should also be noted that ThinManager only supports the Citrix PNAgent, not StoreBrowse. Therefore, Citrix 7.x and newer installations will have to enable PNAgent since it is no longer enabled by default.

8.2.4. Automatically Find Remote Desktop Servers

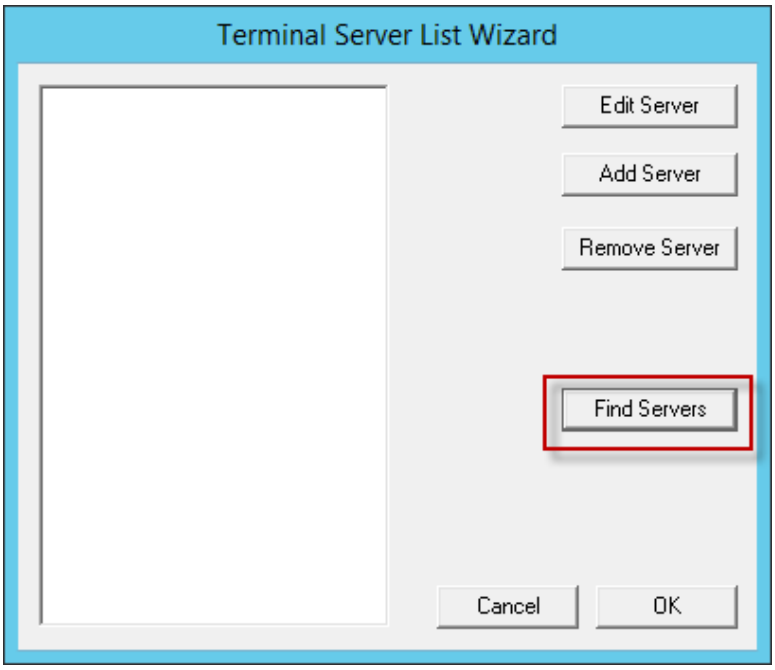
ThinManager has a search function that will find Remote Desktop Servers on the network to speed your configuration.

Go to the **Remote Desktop Server** branch of the **Display Server** tree.



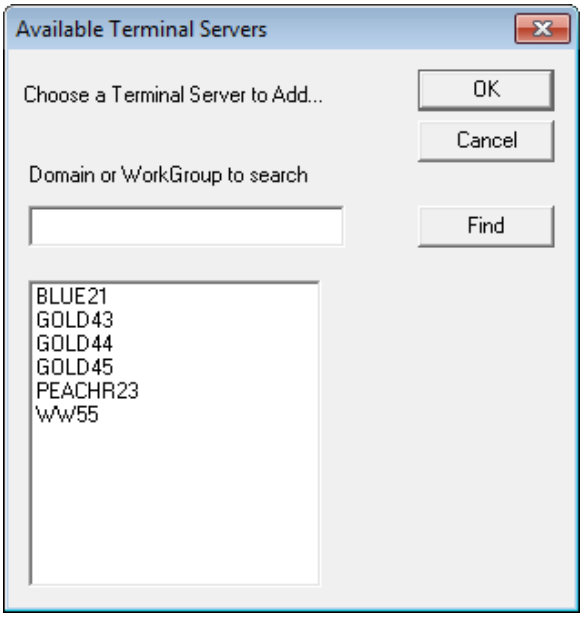
Remote Desktop Server branch of the Display Server tree

Right click on **Remote Desktop Servers** and select ***Edit Remote Desktop Servers***. This will launch the **Remote Desktop Server List Wizard**.



Remote Desktop Server List Wizard

Click the ***Find Servers*** button on the **Remote Desktop Server List Wizard**. This will launch the **Available Remote Desktop Servers** list.



Available Remote Desktop Servers list

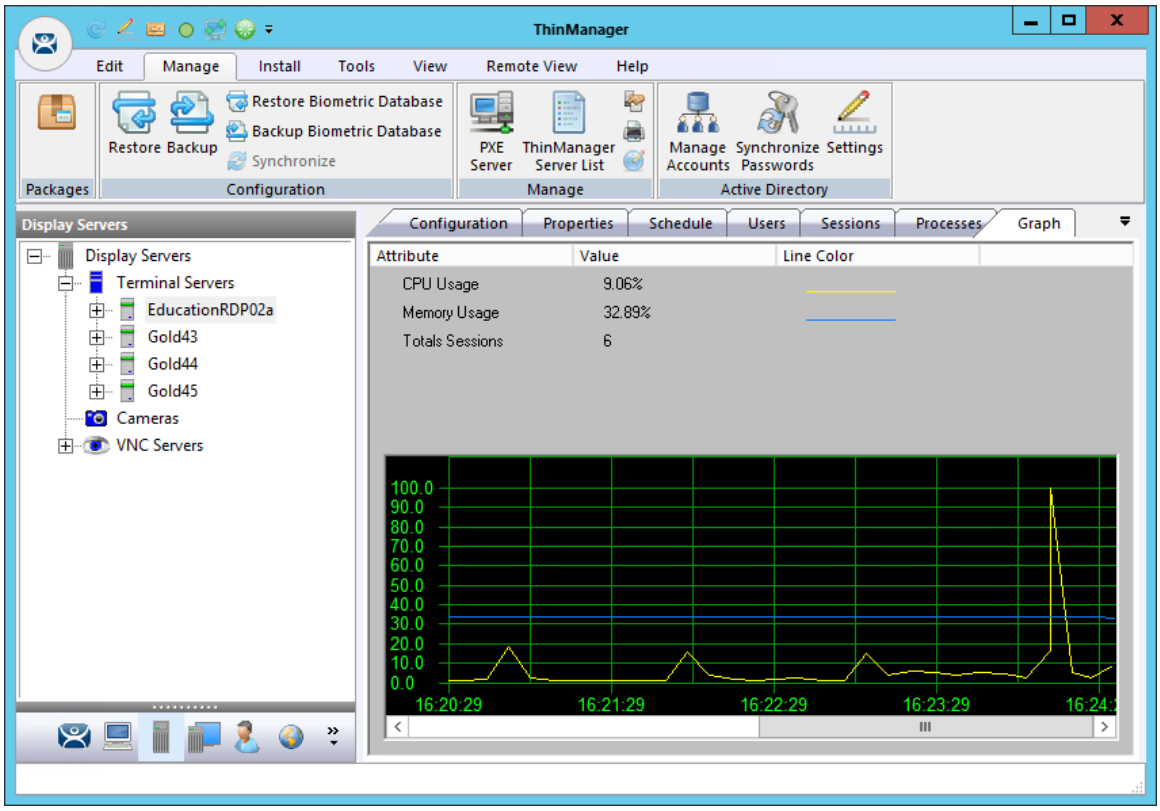
The **Available Remote Desktop Servers** list will show all the Remote Desktop Servers that ThinManager can communicate with in a workgroup. **This does not work in a domain**.

Highlight the one you want to add and select ***OK***. This will launch the Remote Desktop Server Wizard with the name and IP address filled in.

There is a ***Domain or Workgroup*** field to allow you to expand the search. Enter the workgroup and click the ***Find*** button to search again.

8.3. Remote Desktop Server Graph

Highlight a Remote Desktop Server in the Remote Desktop Servers branch of the ThinManager tree and select the Graph tab to see the performance levels of the server.



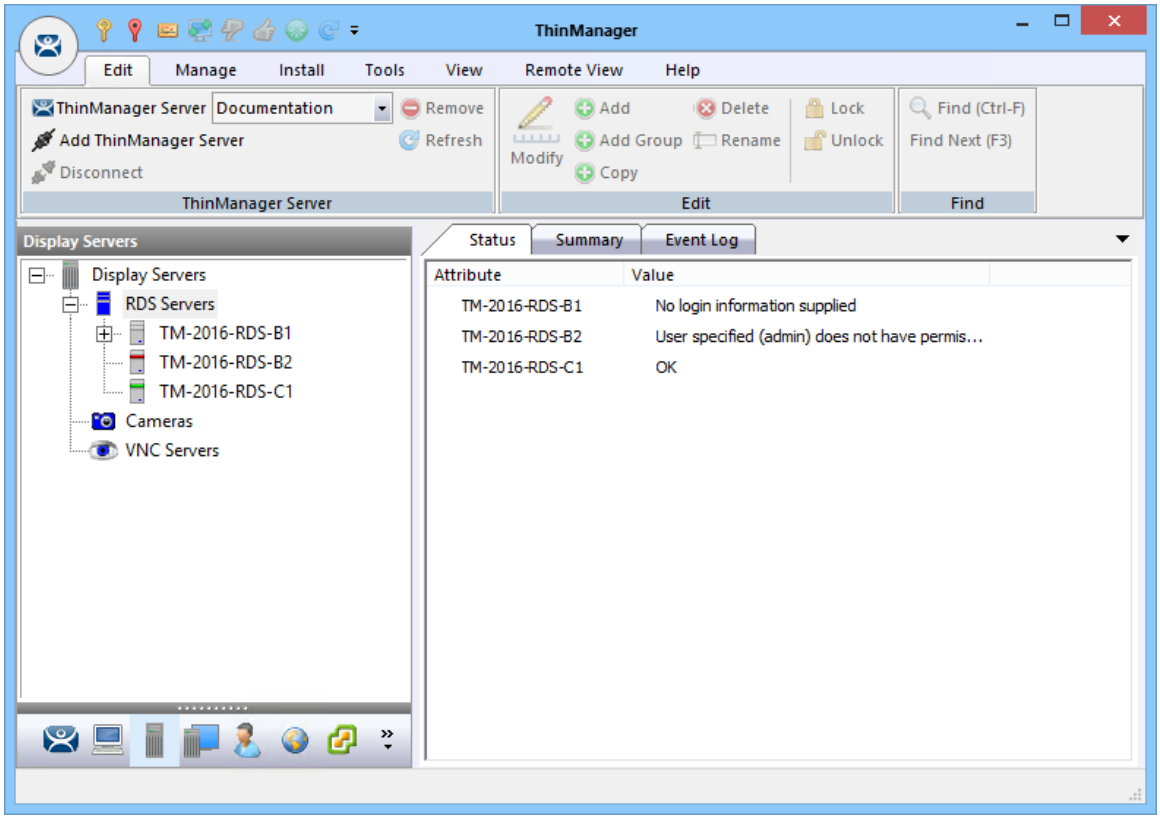
Remote Desktop Server Performance Graph

The CPU usage, memory usage, and session count are the values that ThinManager uses to calculate the SmartSession resource load.

Note: This graph will only be displayed for Remote Desktop Server that have a valid administrative account on the Remote Desktop Server Name page, have the Available for Display Clients using SmartSession checkbox checked, and have an active connection (green light status) to the ThinManager Server.

8.4. Remote Desktop Server Status

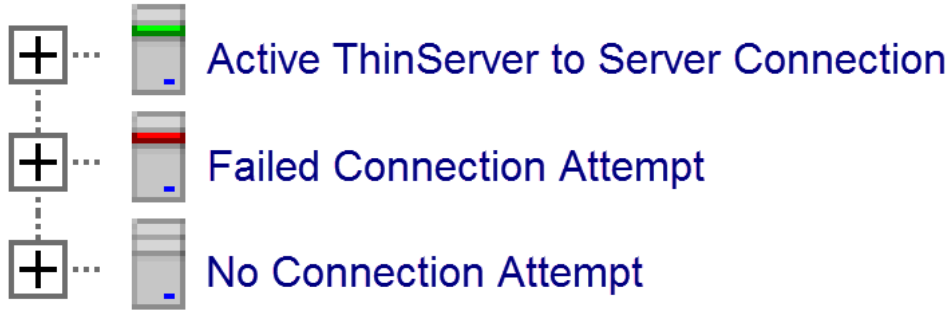
Highlighting the Remote Desktop Servers branch of the ThinManager tree will show the connection status between ThinManager and the servers. Ideally the Remote Desktop Servers are configured properly so that ThinManager will communicate with them and be able to pull load status into ThinManager for use in management and SmartSession load balancing.



Remote Desktop Server Status

A properly connected Remote Desktop Server will show a green bar in its icon and show “OK” in the Status tab.

Sometimes the connection fails and the icon shows red.



Remote Desktop Server Status Lights

- **Green** – This means that the ThinServer can talk to the Remote Desktop Server and pull data using the administrative account you are using.
- **Gray** – This shows that the administrative account was left blank and the ThinManager Server isn’t trying to communicate with the server.

- **Red** – This means that the server is offline or the administrative account failed to connect to the server.

Note: A Red or Gray icon does not mean that the Terminals can't login and run on the servers. This only indicates the ability of ThinManager to access the resources on the server.

Fixes:

If your icon shows **gray** re-open the **Remote Desktop Server Wizard** and enter an administrative account in the ***Log In Information*** fields on the **Remote Desktop Server Name** page.

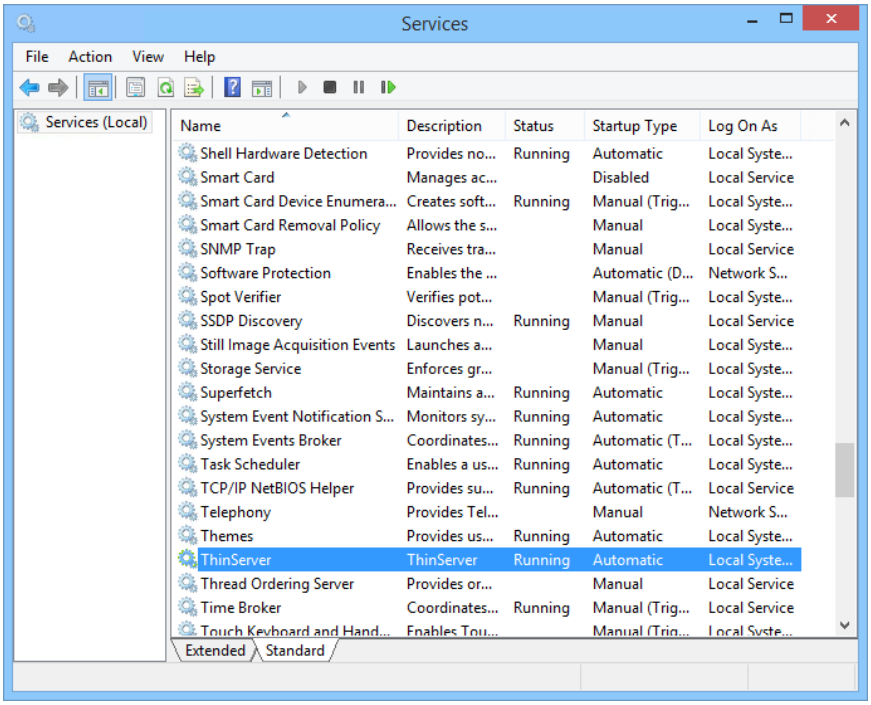
If your icon shows **red** and the status message says that the "User specified does not have permission to connect" re-open the **Remote Desktop Server Wizard** and correct the administrative account in the ***Log In Information*** fields on the **Remote Desktop Server Name** page.

If your icon shows **red** and the status message says "The RPC Server is unavailable" or the "WTSAPI32.dll failed" then the Remote Desktop Server is offline or is missing the Terminal Services/Remote Desktop Protocol role.

8.4.1. Local Administrative Login for ThinServer

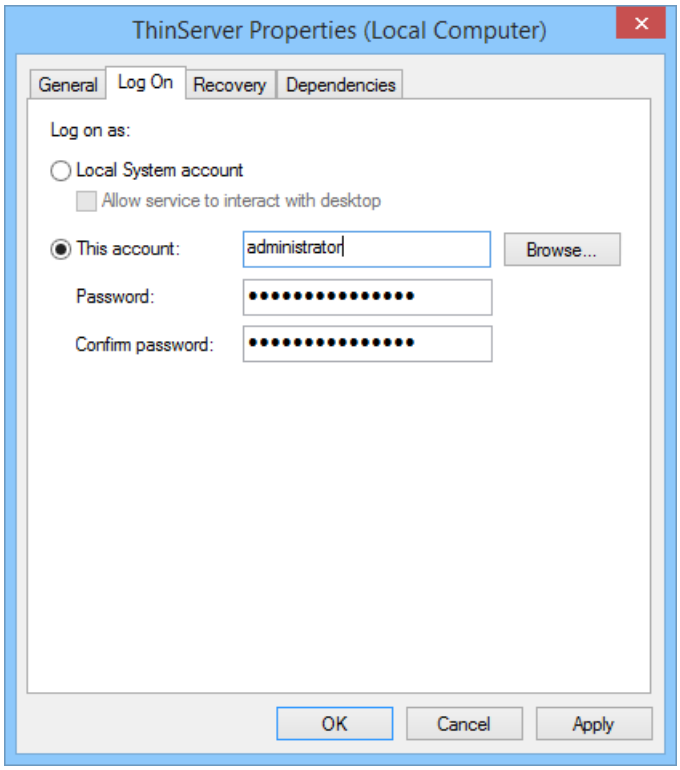
Large domains sometimes have issues where the connection will time out before the domain controller can validate the user name. A simple solution is to create a local administrative user account on each server. Then have the ThinServer login in with this account. This will speed up the data retrieval.

You change the ThinServer service login in Microsoft Services on your ThinManager Server. This may be found in the **Administrative Tools** or in the **Server Manager**.



Services in Windows 2012

Double click on the **ThinServer** service on your ThinManager Server to open the **Service Properties** window.



ThinServer Properties

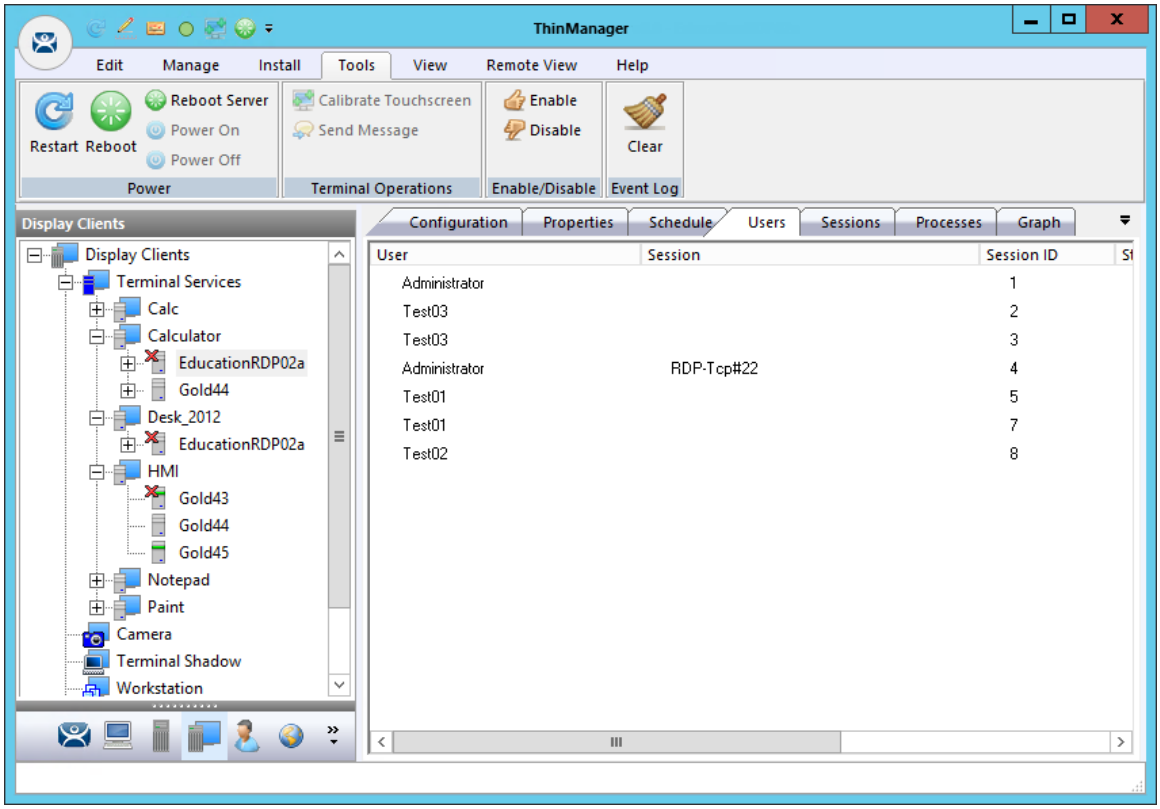
Select the **Log On** tab on the **ThinServer Properties** window.

Change the log in account from the **Local System** account and specify the local administrative account you want to use. Make sure it is a member of the Administrative Group.

Select the ***OK*** button and restart the ThinServer service to apply the changes to the login.

8.4.2. Disabling Remote Desktop Servers for Failover Tests and Updates

ThinManager allows you to disable a Remote Desktop Server by highlighting the Remote Desktop Server icon in the ThinManager tree and selecting ***Tools > Disable***. This will force ThinManager controlled thin clients to drop their connection to the server and switch to an alternate server.



Display Client Tree Showing Disabled Remote Desktop Servers

This is a useful tool for testing Failover and Instant Failover. The Terminals should switch to their back up server. The network card on the server isn't disabled and you can make RDP connections from a PC but the ThinManager thin clients will stop using the server.

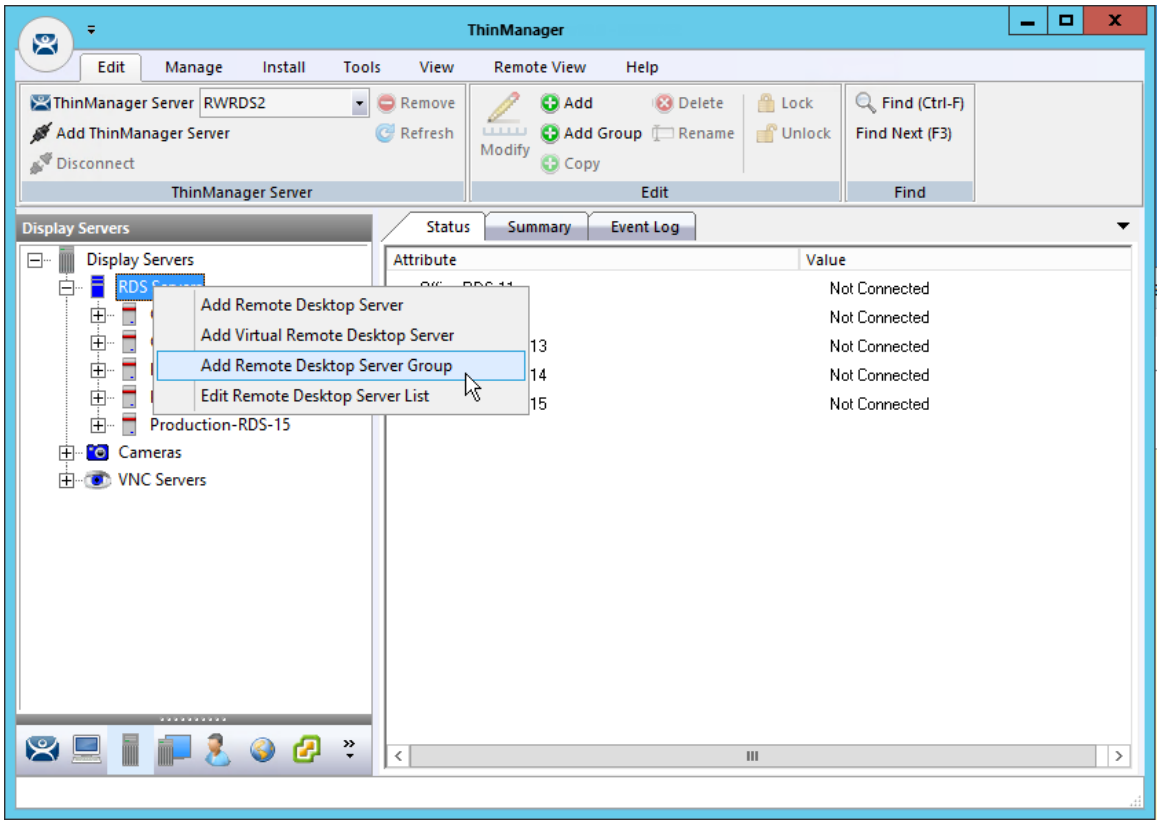
You can also use this for updates during the normal production hours. Once you disable the Remote Desktop Server you can reset the sessions by right clicking on the sessions on the Sessions tab and selecting ***Reset Session***. Once the server is clear of sessions you can patch and update the server and applications, and even reboot it if necessary. This won't impact production as all the Terminals are using a backup server.

Once your updating is finished you can enable the server from ***Tools > Enable*** to allow the Terminals to use the server again.

This ***Disable/Enable*** tool allows you to move servers offline one at a time for updating.

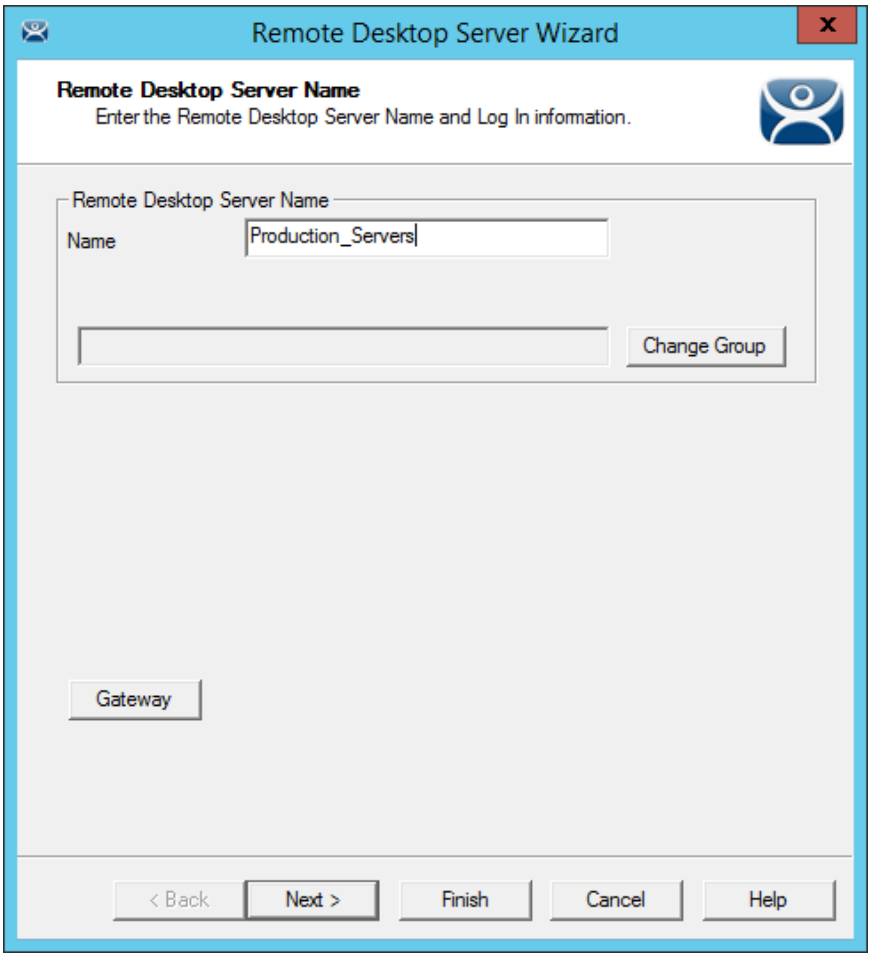
8.5. Remote Desktop Server Group

A **Remote Desktop Server Group** can be created to speed configuration by selecting a pool of servers instead of individual server.



Add Remote Desktop Server Group

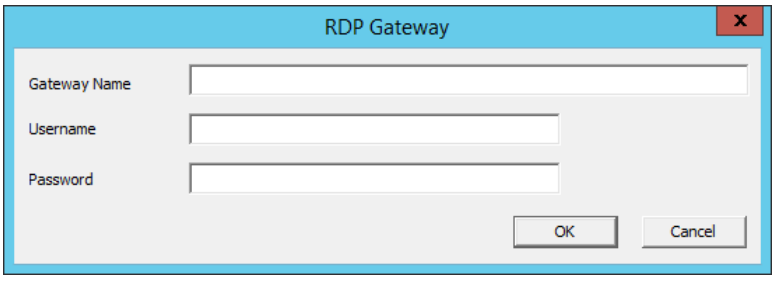
The configuration wizard is launched by right clicking on **RDS Servers** in the Display Server branch of ThinManager and selecting ***Add Remote Desktop Server Group***.



Remote Desktop Server Wizard – Remote Desktop Server Name Page

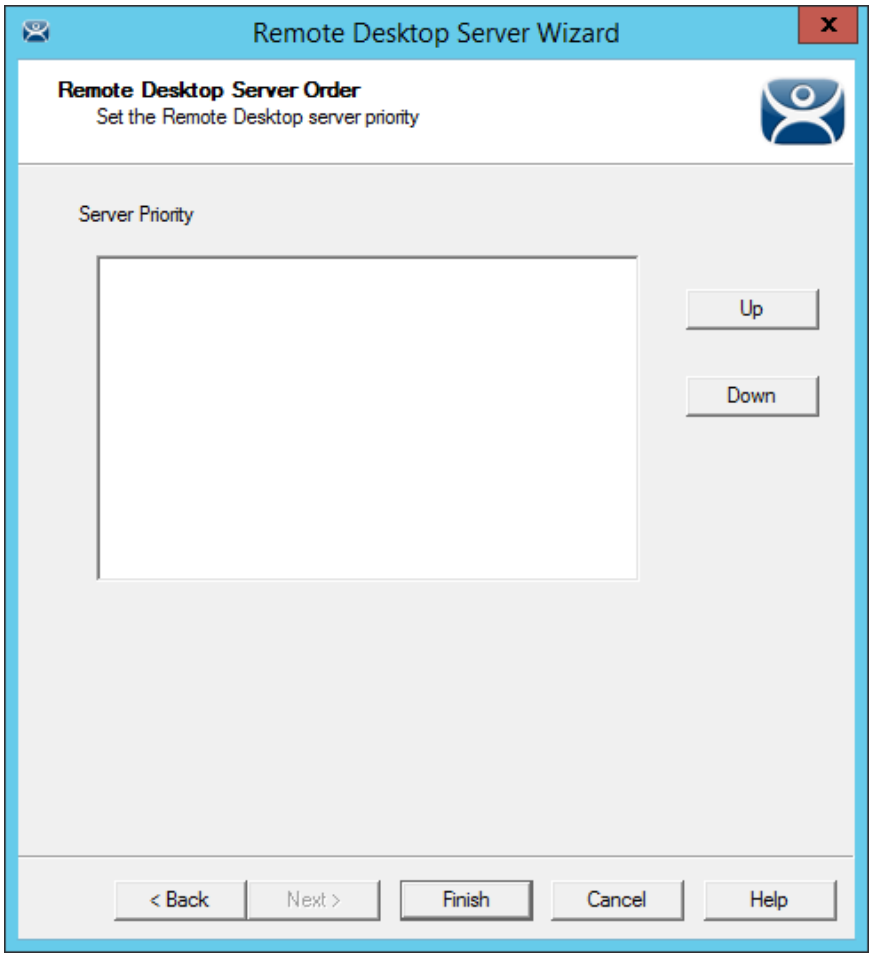
Enter a name for the Remote Desktop Server Group in the ***Name*** field.

The ***Gateway*** button launched the **RDP Gateway** window.



RDP Gateway

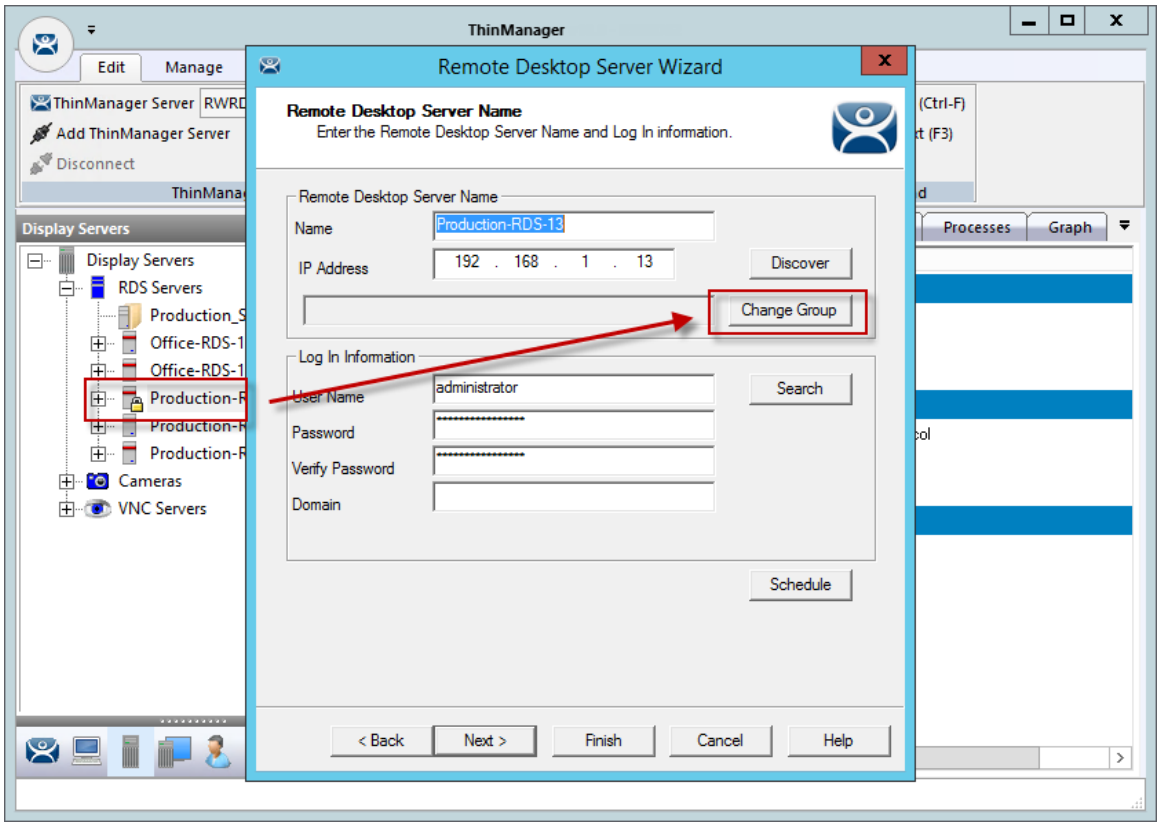
The **RDP Gateway** allows the Remote Desktop Servers to use the Microsoft RDP Gateway to connect to resources on other subnets.



Remote Desktop Server Order Page

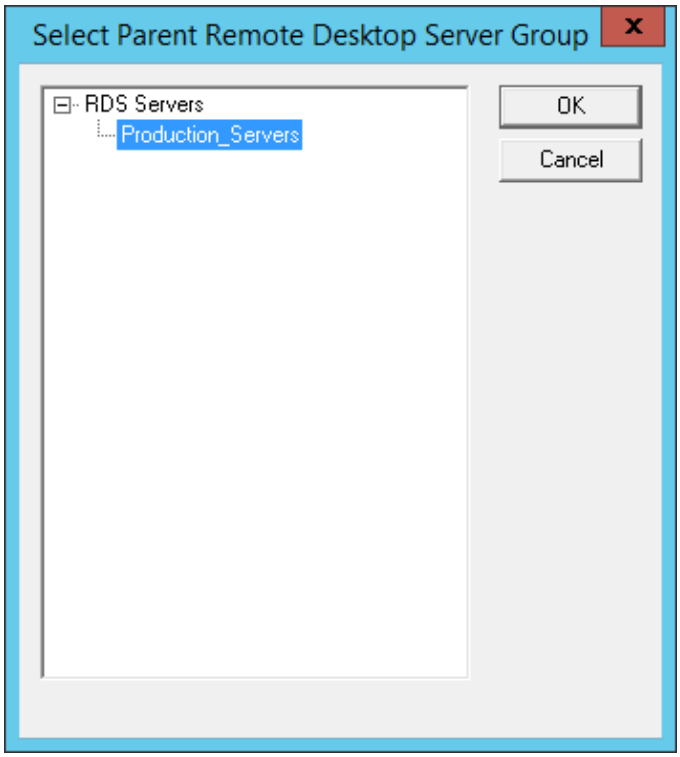
The Remote Desktop Server Group is created as an empty group as shown on the **Remote Desktop Server Order** window.

The Remote Desktop Servers are added individually in **the Remote Desktop Server Wizard**.



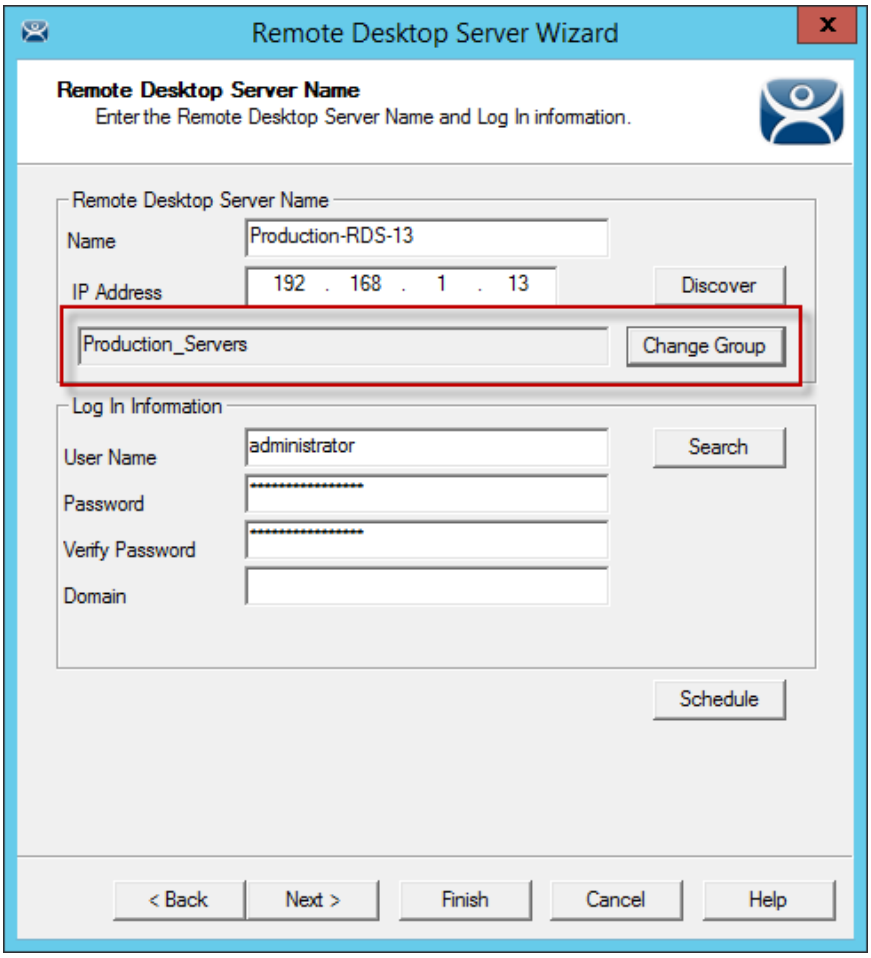
Remote Desktop Server Wizard – Remote Desktop Server Name Page

Open the **Remote Desktop Server wizard** by double clicking on the server under **RDS Servers** in the **Display Server** branch. Navigate to the **Remote Desktop Server Name** page and select the ***Change Group*** button. This will launch the **Select Parent Remote Desktop Server Group** window.



Select Parent Remote Desktop Server Group Window

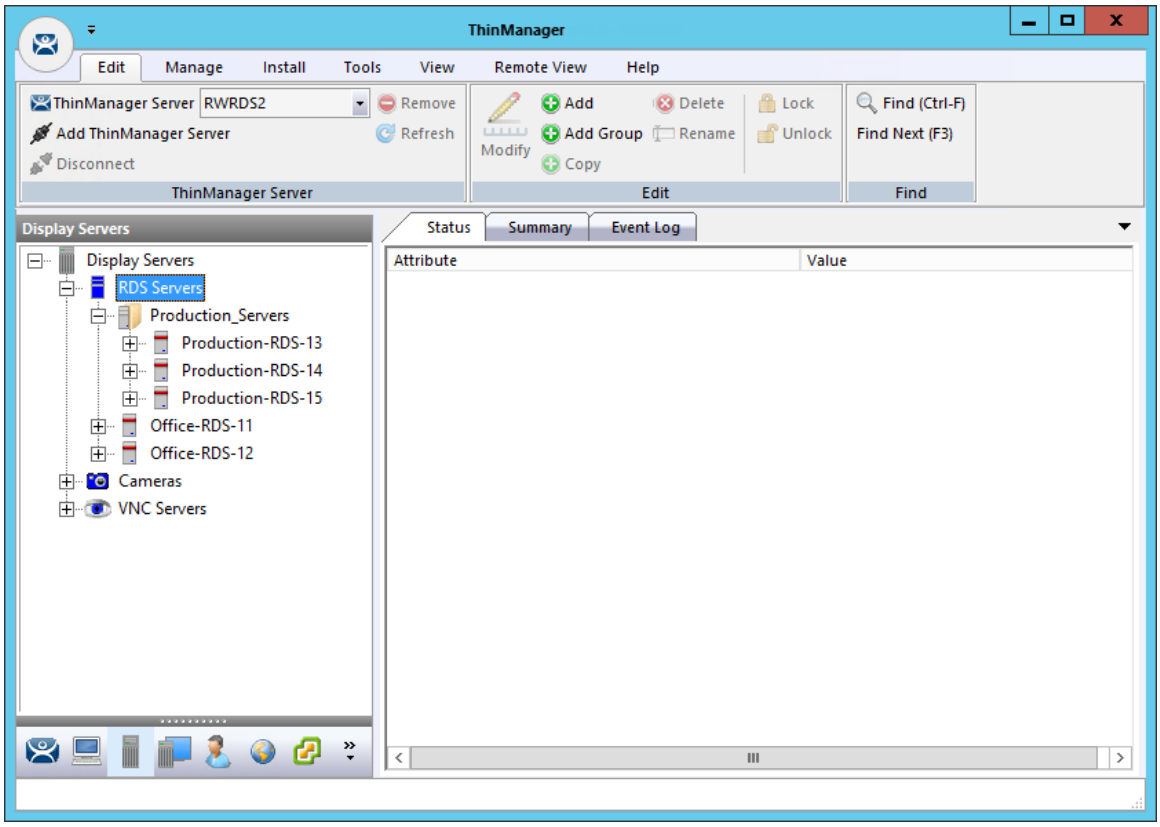
Select the desired Remote Desktop Server by highlighting the name, and then select ***OK*** to accept the changes.



Remote Desktop Server Name Page with Remote Desktop Server Group Membership

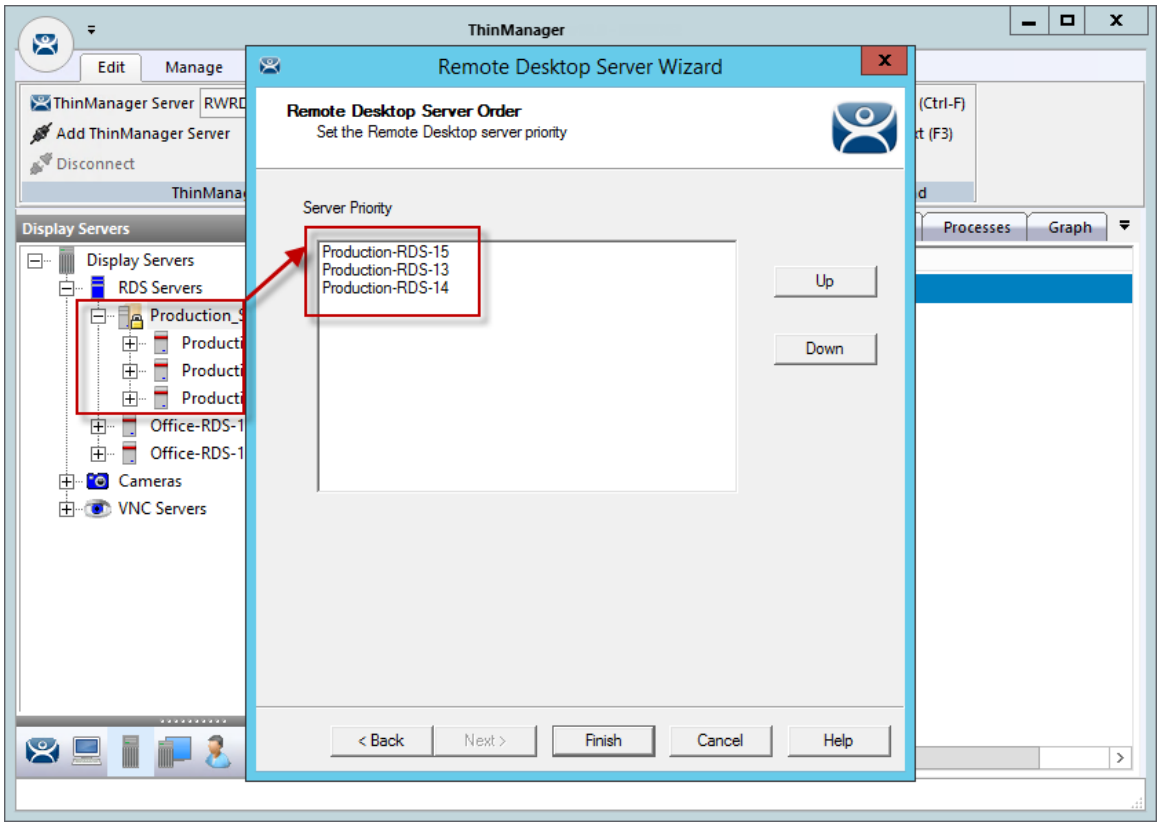
The Remote Desktop Server is now a member of the Remote Desktop Server Group.

Repeat as needed.



Remote Desktop Server Group with Member Remote Desktop Servers

The tree will now show the member Remote Desktop Servers in the RDS Server group.



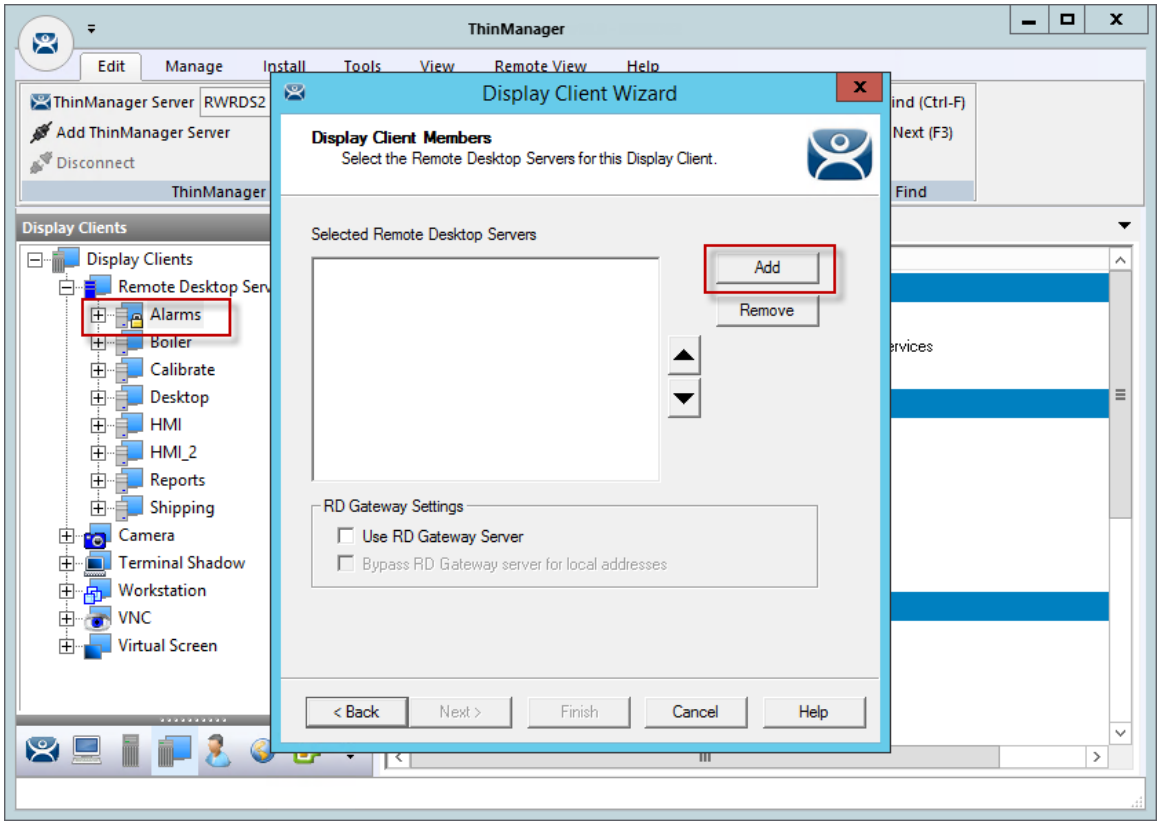
Remote Desktop Server Wizard – Remote Desktop Server Order Page

Opening the Remote Desktop Server Group wizard and navigating to the **Remote Desktop Server Order** page will show the members of the Remote Desktop Server Group.

The order that the Remote Desktop Servers will be used is the order listed. This can be changed by highlighting a member server and using the ***Up*** and ***Down*** buttons to change the order.

8.5.1. Remote Desktop Server Groups and Display Clients

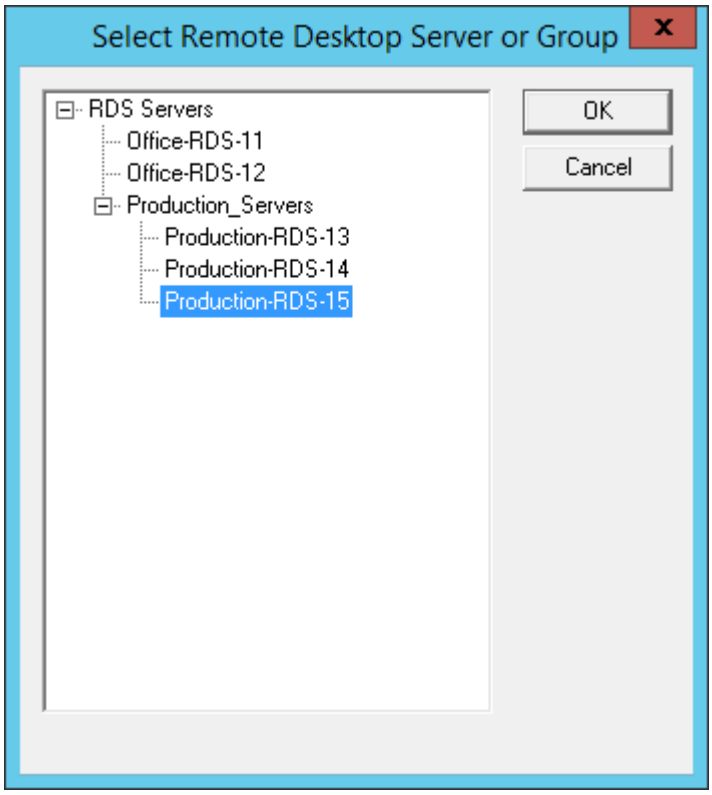
Remote Desktop Server Groups changes the way that the Display Client wizard is displayed.



Display Client Wizard – Display Client Member Page

Open a Display Client by double clicking on it in the Display Client branch of the ThinManager tree. Navigate to the Display Client Members page.

Selecting the ***Add*** button opens the **Select Remote Desktop Server or Group** window that allows selection of the Remote Desktop Server or Server Group.



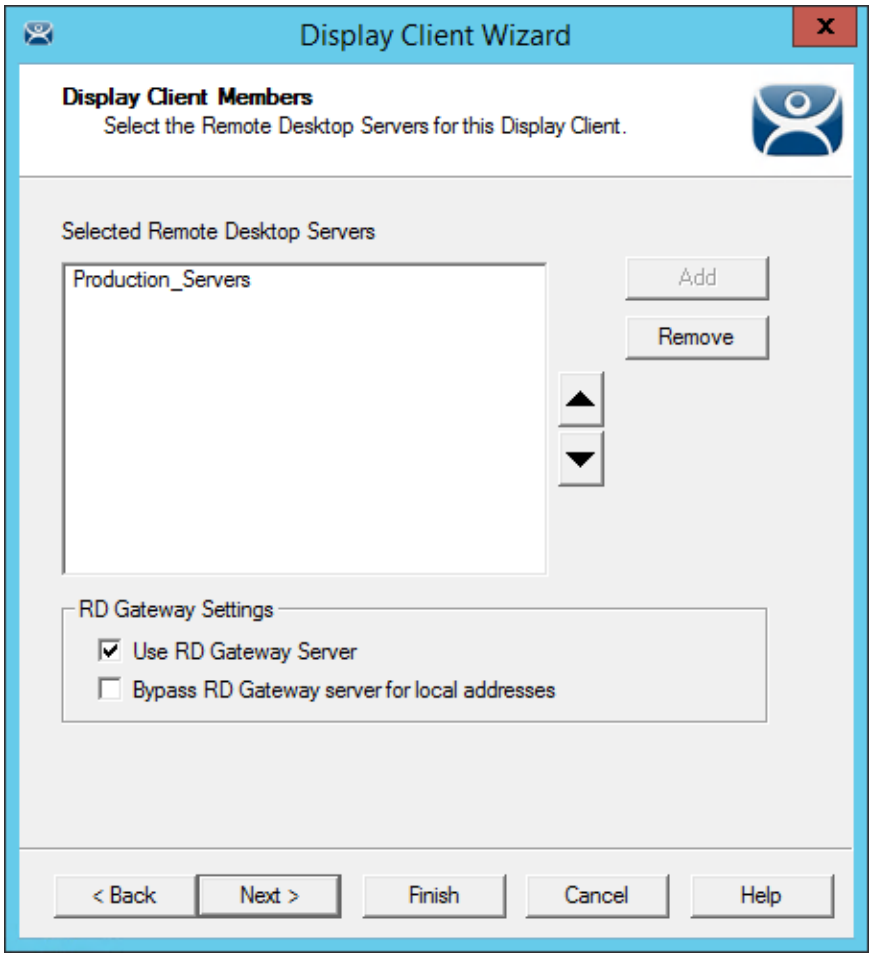
Select Remote Desktop Server or Group Window

The **Select Remote Desktop Server or Group** window allows the selection of the Remote Desktop Servers for the Display Client.

You may select a Remote Desktop Server Group, and individual Remote Desktop Server, or a Remote Desktop Server that is a member of a Remote Desktop Server Group.

Highlight the desired Remote Desktop Server or group and select ***OK*** to accept the addition.

Repeat as necessary.



Display Client Wizard – Display Client Member Page

Once a Remote Desktop Server or Remote Desktop Server Group is selected it will be shown in the Selected Remote Desktop Servers list.

Two checkboxes will be displayed to control the use of the Microsoft RDP Gateway.:

- **Use RD** Gateway – This checkbox, if selected, prompts the Display Client to use the Microsoft RD Gateway.
- **Bypass RD Gateway server for local address** – This checkbox, if selected, allows the Display Client to use a Remote Desktop Server without going through the RD Gateway if the Terminal and Remote Desktop Server are on the same subnet.

The remainder of the Display Client wizard follows the Display Client Wizard that is displayed if Remote Desktop Server Groups are not configured.

9. Sources – IP Cameras

ThinManager supports camera in the ThinManager system. Cameras, either IP cameras or USB cameras, can be configured to provide the camera feed to display clients on Terminals. This section covers defining the cameras as a Display Server. Delivering the video to a Camera Display Client will be covered in Content – Camera Display Clients on page 138.

There are three steps in integrating an IP camera into the ThinManager system.

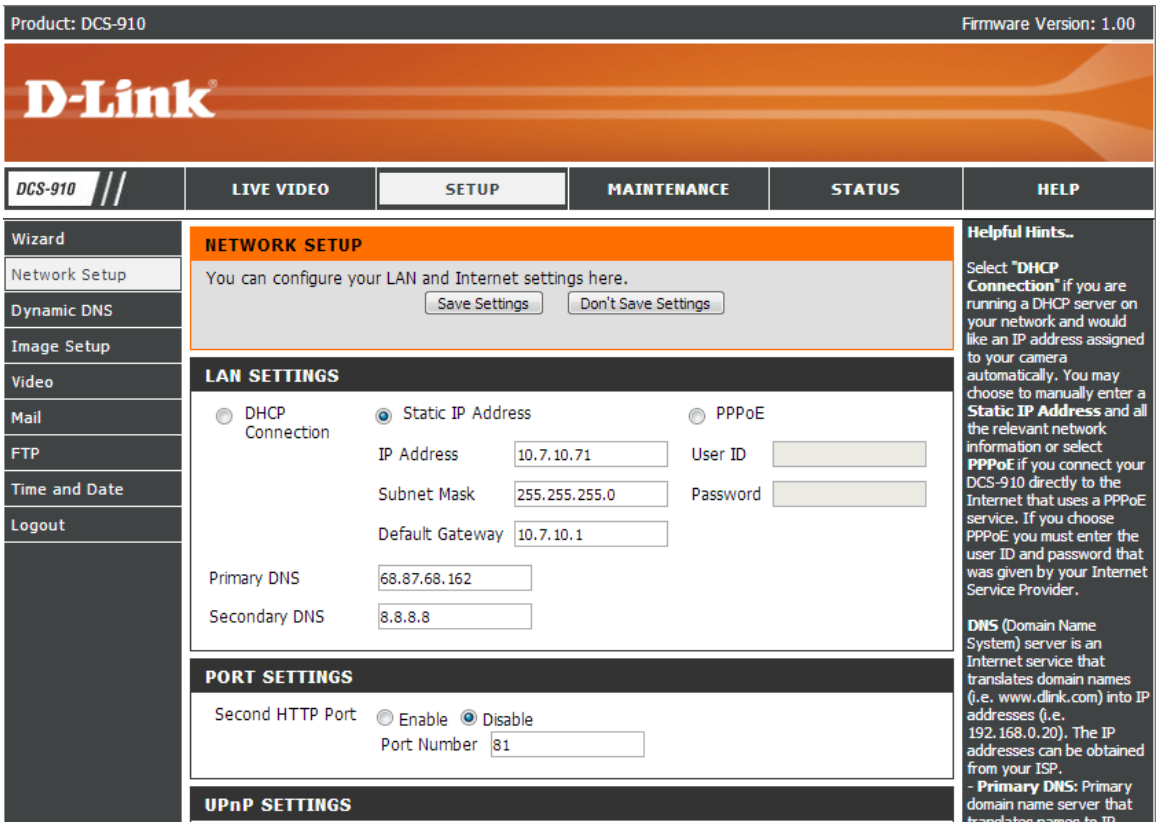
- ✓ **First, configure the camera and add it to your network using the guidelines from the camera maker.**
- ✓ **Second, add the configured camera to ThinManager as a Display Server source.**
- ✓ **Third, deploy the content of the cameras by creating a camera display client and applying it to the Terminals.**

USB cameras are added to a Terminal and configured. See Define the USB Camera as a Display Server on page 81.

9.1. Configure the IP Camera

Each camera manufacturer sends out their cameras with a default IP address and a default administrative account. This will need to be configured to add the camera to your network. Methods vary from vendor to vendor but a web interface id common.

- ✓ **Please follow the instructions from the camera manufacturer to configure your camera for use.**

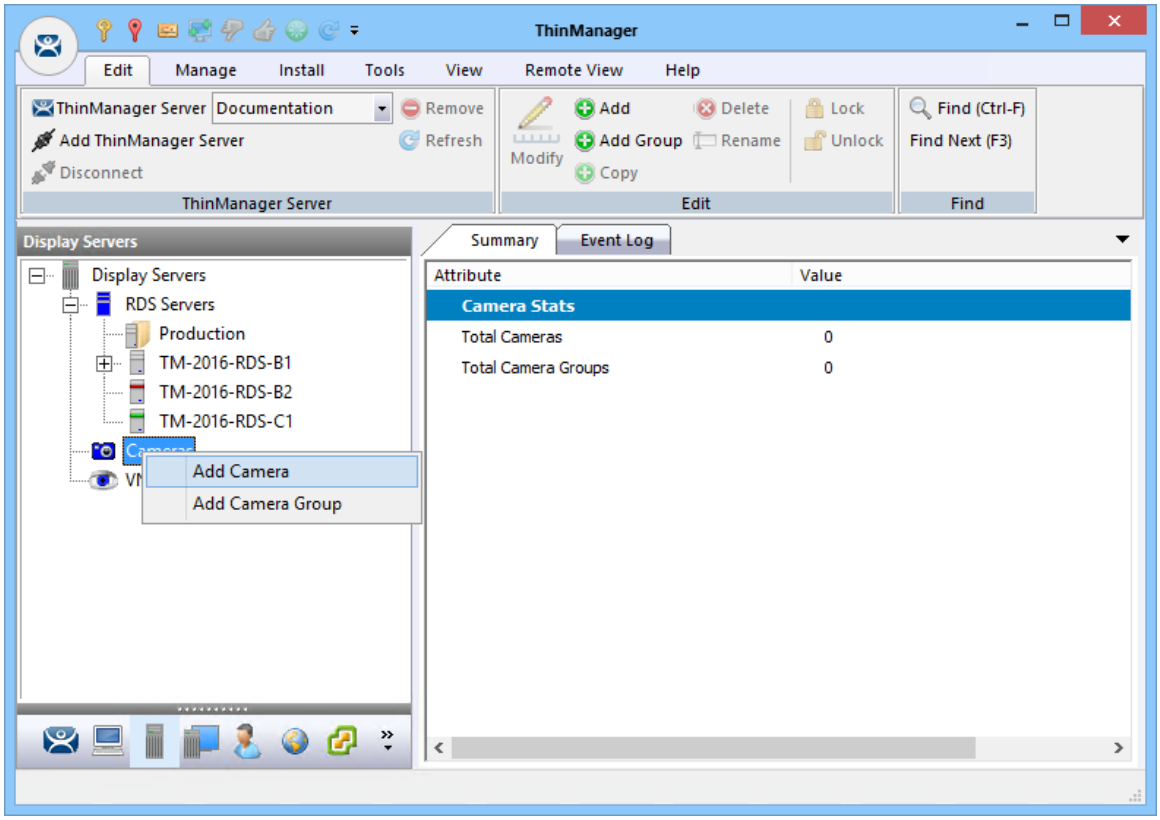


Browser Based Camera Configuration

9.2. Define the IP Camera as a Display Server

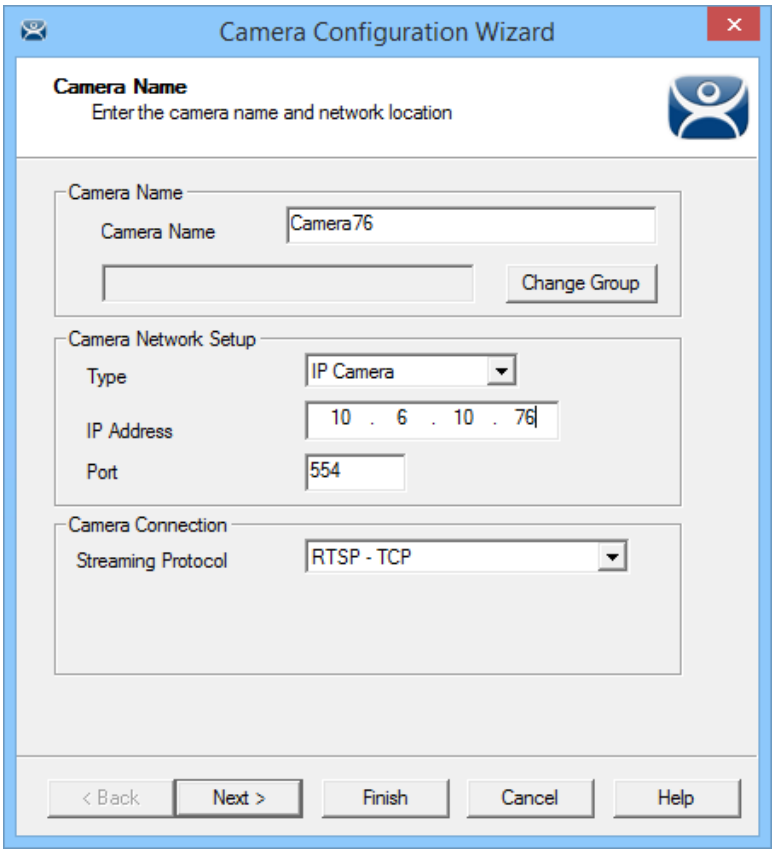
The **Camera Configuration Wizard** is launched from the **Camera** branch of the **Display Server** tree.

Open the **Display Server** tree by selecting the **Display Server** icon at the bottom of the ThinManager tree.



Camera Branch of the Display Server Tree

Right click on the Cameras branch and select ***Add Camera*** to launch the **Camera Configuration Wizard**.



Camera Name Page

Enter a name for the camera.

Select the **Camera Network Setup**, either *USB Camera* or *IP Camera*, from the ***Type*** drop-down.

9.3. IP Camera

ThinManager supports IP cameras added to the network. A thin client that has a camera added will make a connection to the camera and stream the video feed directly. The video does not go through the ThinManager Server. ThinManager only tells the thin client to stream the video feed.

Select the protocol that the camera will use. The choices are:

- Legacy Motion JPEG.
- Motion JPEG
- RTSP-HTTP
- RTSP-TCP
- RTSP-UDP
- RTSP-UDP multicast

9.3.1. Legacy Motion JPEG

This was the original method of configuring IP cameras in ThinManager. Cameras were tested and verified by the ThinManager development team and the information was added to the TermCap database.

Once a ***Make*** and ***Model*** are selected from a list contained in the TermCap database and ThinManager filled in the necessary URL

This method has been updated by adding support for the more common Real Time Streaming Protocol (RTSP) for IP cameras.

9.3.2. Motion JPEG

ThinManager improved the deployment of **Motion JPEG** in the ThinManager system. You can choose ***Motion JPEG*** from the ***Streaming Protocol*** drop-down on the **Camera Name** page.

Each camera uses a specific Motion JPEG URL specified by the camera manufacturer. Enter this URL, usually found in the manufacturer's documentation, in the ***Custom URL*** field on the **Camera Authentication** page.

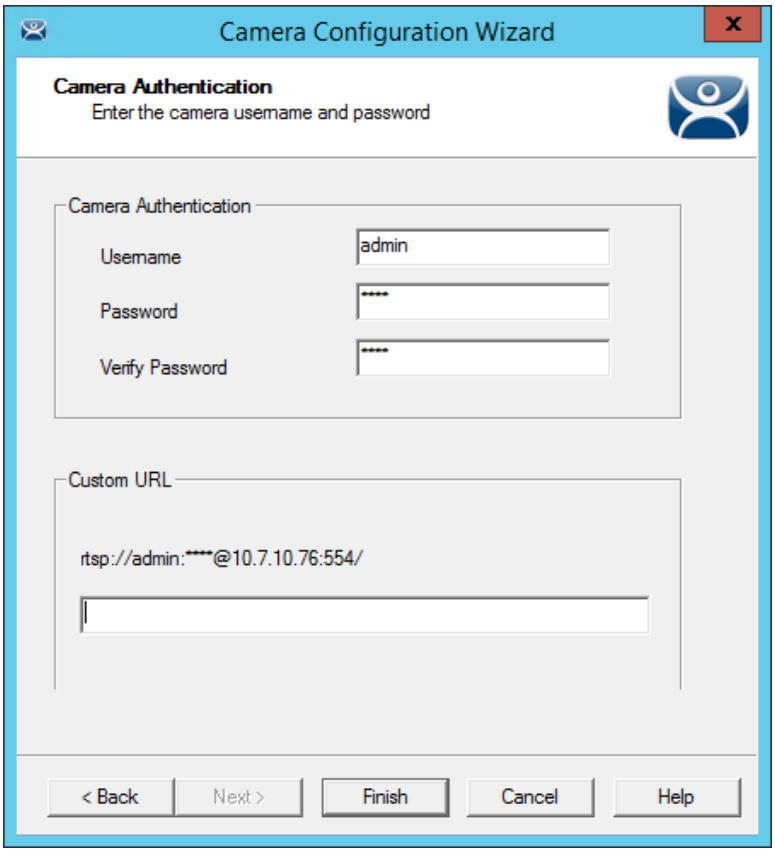
This method gives you flexibility in your camera choices because are you aren't required to use a camera from the TermCap database.

9.3.3. Real Time Streaming Protocol

ThinManager supports the Real Time Streaming Protocol (RTSP) for IP cameras. This is the preferred method as RTSP has the widest support from camera companies.

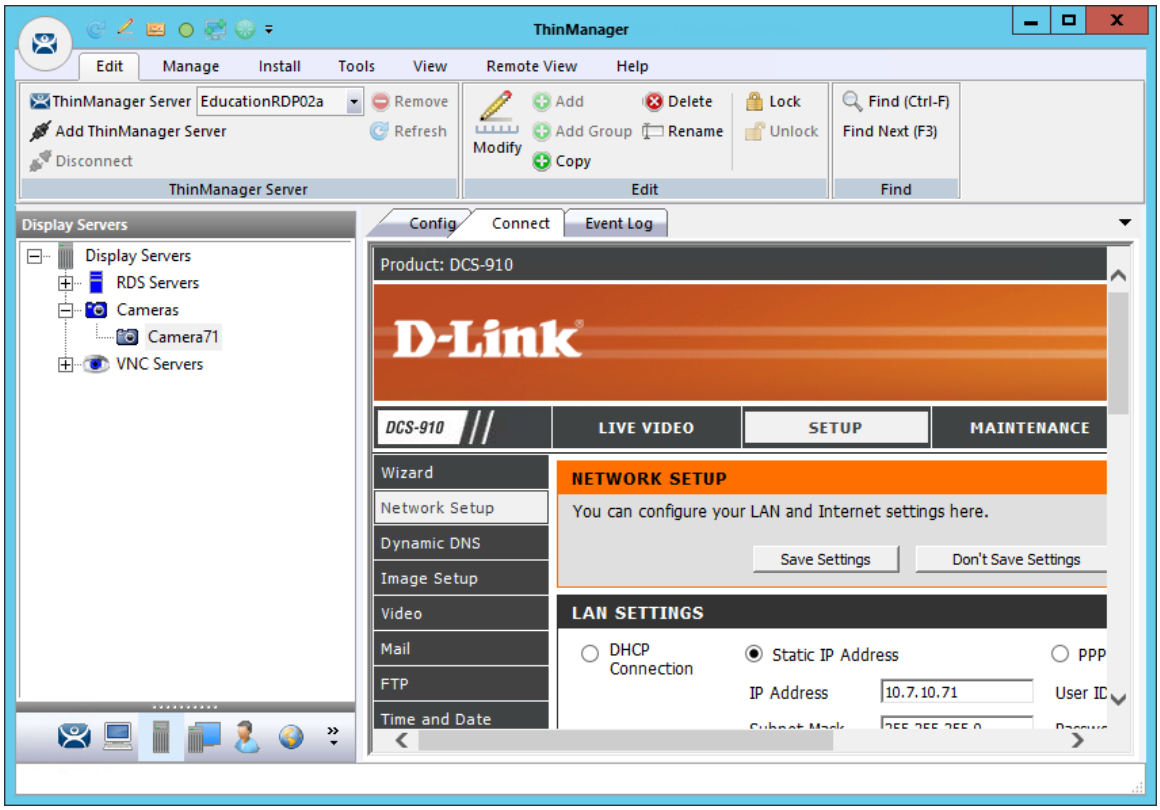
RTSP has several transport layers, RTSP-http, RTSP-tcp, RTSP-udp, and RTSP-udp multicast. One needs to specify the URL that that specific camera uses for the video stream.

- Select ***IP Camera*** from the **Type** drop-down.
- Enter the IP address of the camera in the ***IP Address*** field.
- Select the desired transport method from the ***Streaming Protocol*** drop-down.
- Select the ***Next*** button.
- Enter an account for the camera that allows streaming unless the camera allows anonymous access.
- Enter the ***RTSP URL*** specified by the camera manufacturer.
- Select ***Finish*** to close the wizard and finish the configuration.



Camera Authentication Page

Enter an account for the camera that allows streaming unless the camera allows anonymous access. The thin client will be unable to access the video feed without it.



Camera Management Screen

One the camera is defined in ThinManager properly you can access the camera's browser control panel by highlighting the camera in the ThinManager tree and selecting the Connect tab. You can make changes as needed.

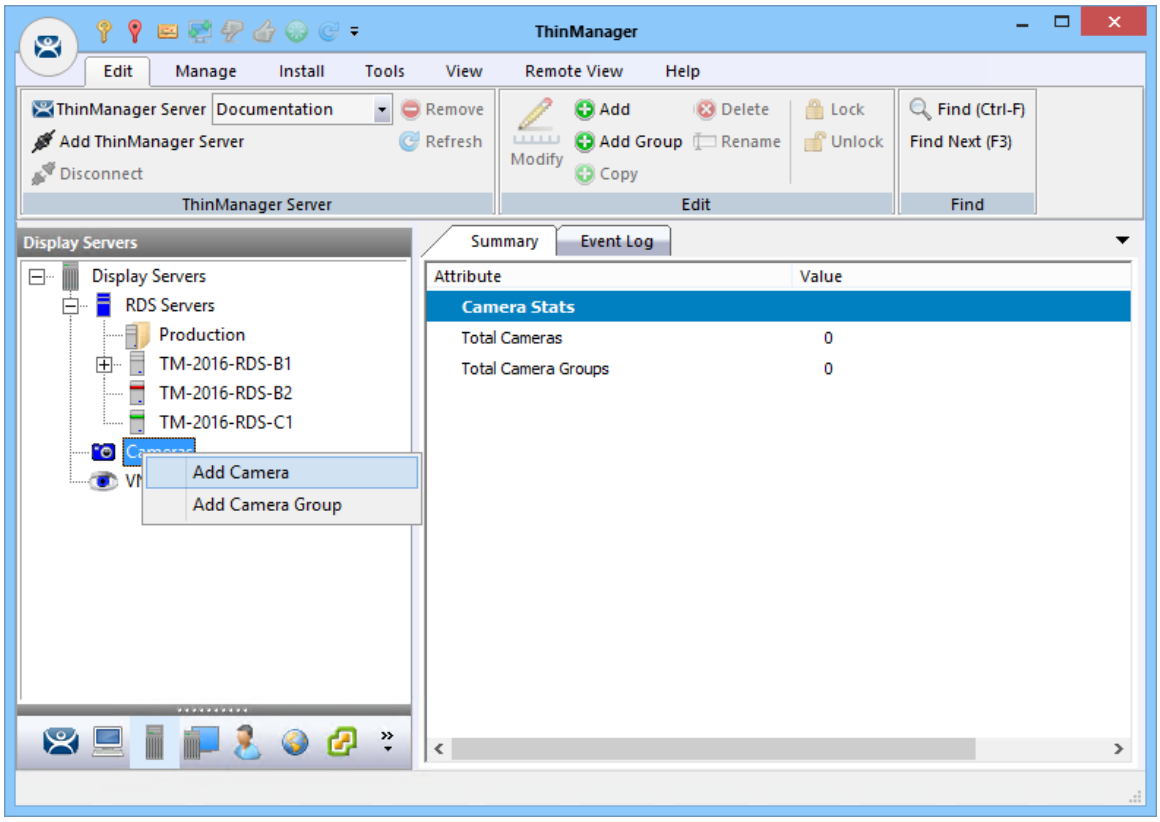
Note: If a camera uses a 32-bit ActiveX then it can be connected and viewed within a 32-bit ThinManager but not a 64-bit ThinManager.
If a camera uses a 64-bit ActiveX then it can be connected and viewed within a 64-bit ThinManager but not a 32-bit ThinManager.
The network settings and configuration is available but not the live video feed.

9.4. Define the USB Camera as a Display Server

USB cameras can be attached to ThinManager thin clients and the video feed sent to display clients on any ThinManager thin client.

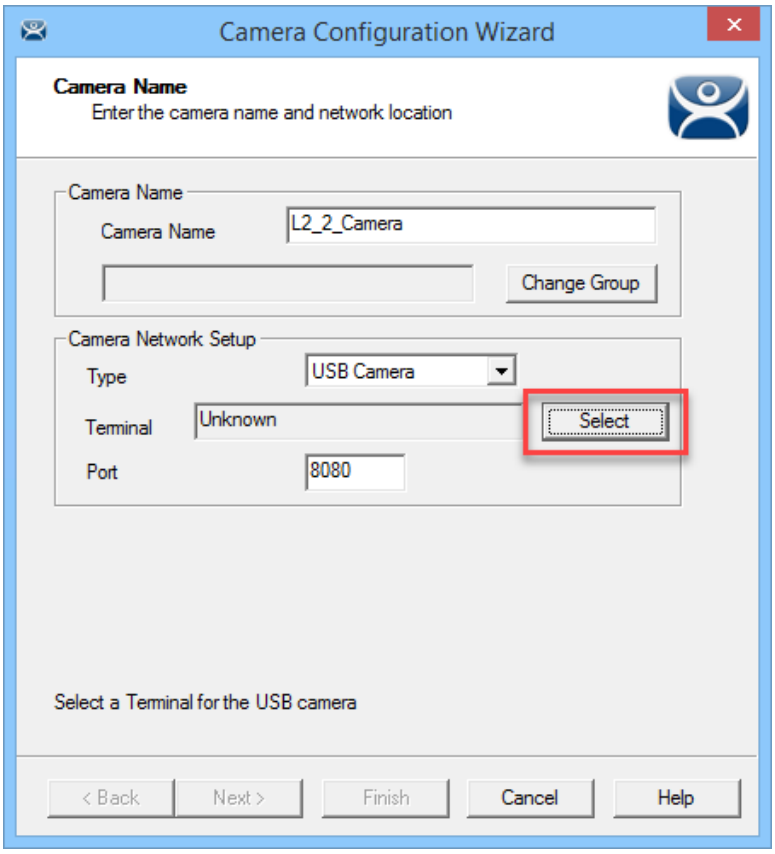
The **Camera Configuration Wizard** is launched from the **Camera** branch of the **Display Server** tree.

Open the **Display Server** tree by selecting the **Display Server** icon at the bottom of the ThinManager tree.



Camera Branch of the Display Server Tree

Right click on the Cameras branch and select ***Add Camera*** to launch the **Camera Configuration Wizard**.



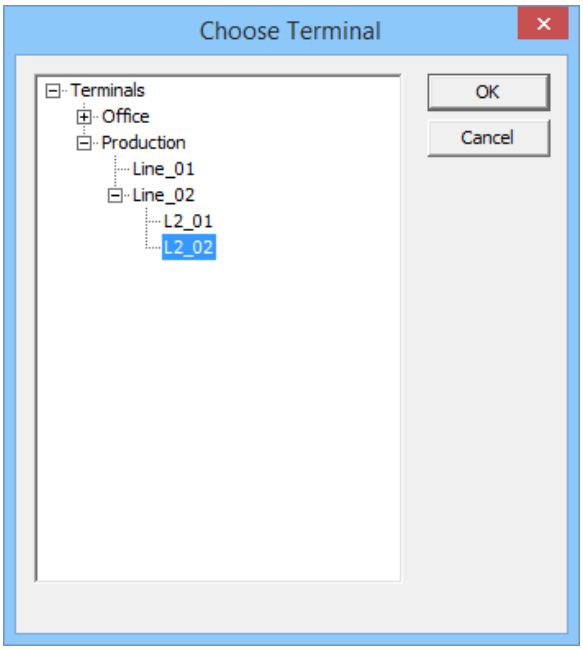
USB Camera on Camera Name Page

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

Select ***USB Camera*** from the **Type** drop-down.

Once ***USB Camera*** is selected a ***Terminal*** field will be revealed with a ***Select*** button.

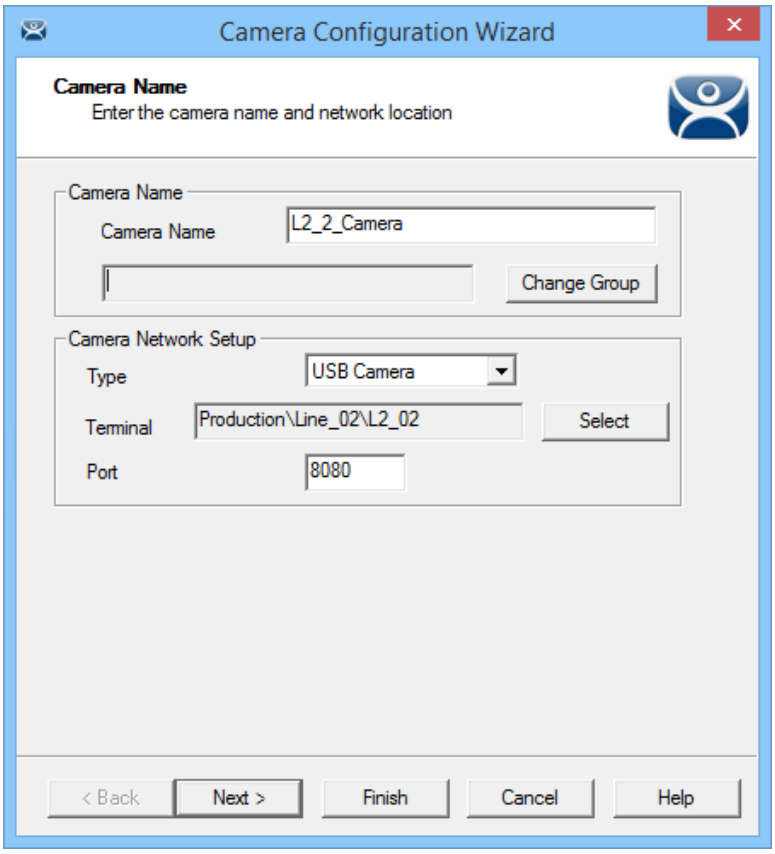
Click the ***Select*** button to choose the Terminal that the USB camera is plugged in to.



Choose Terminal Dialog

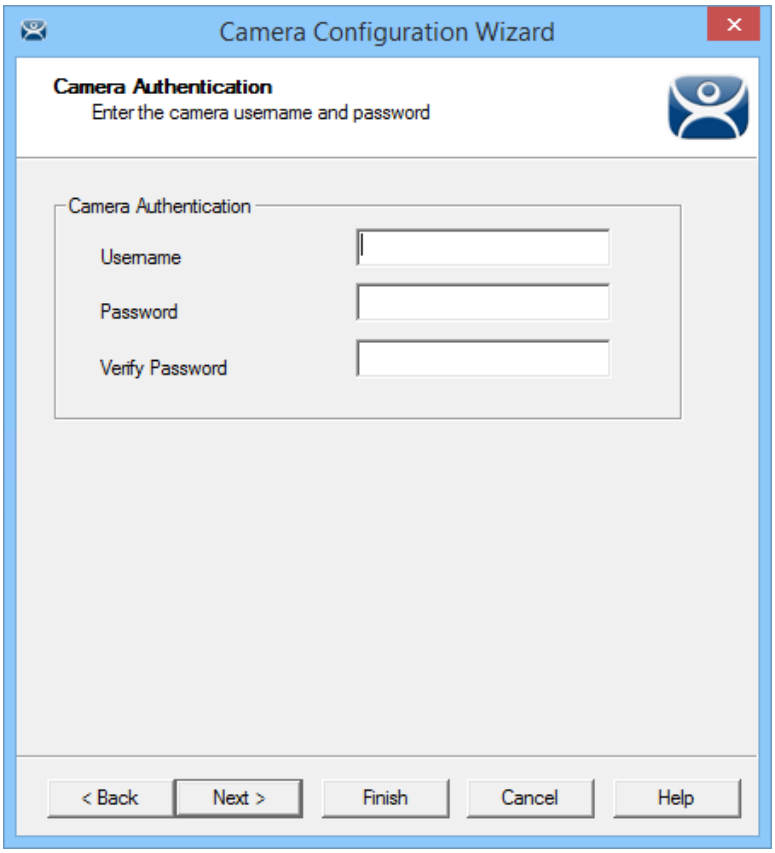
The ***Select*** button will launch the **Choose Terminal** dialog that allows you to specify which Terminal the USB camera is connected to.

Highlight the correct Terminal and select the ***OK*** button.



Terminal Name in the Camera Name Page

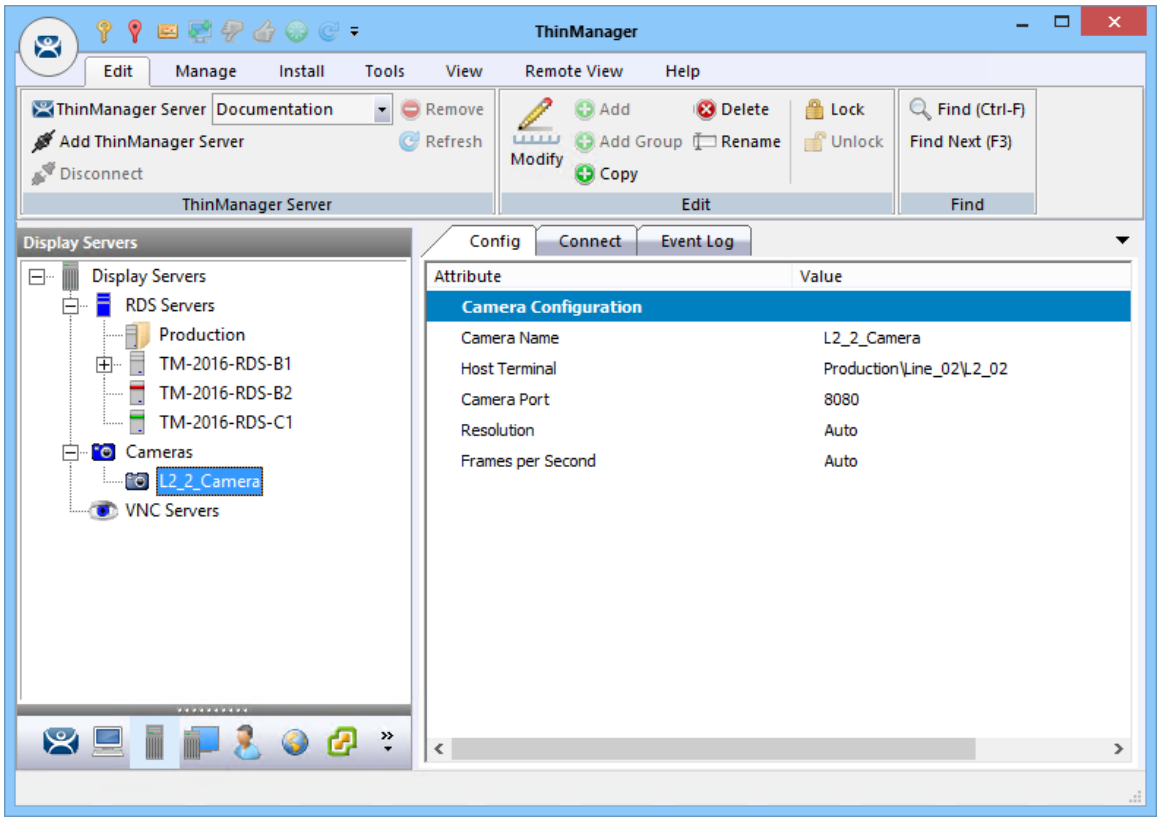
Once a Terminal is selected on the **Choose Terminal** dialog it will appear in the ***Terminal*** field.



Camera Authentication Page

Enter the administrative user account and password if your USB cameras uses authentication.

Click the ***Finish*** button to close the configuration wizard.



Cameras in Display Server Tree

Once the configuration wizard is closed the camera will show up in the Display Server tree.

Note: You cannot connect to a USB camera and manage it from the **Connect** detail pane in the ThinManager console.

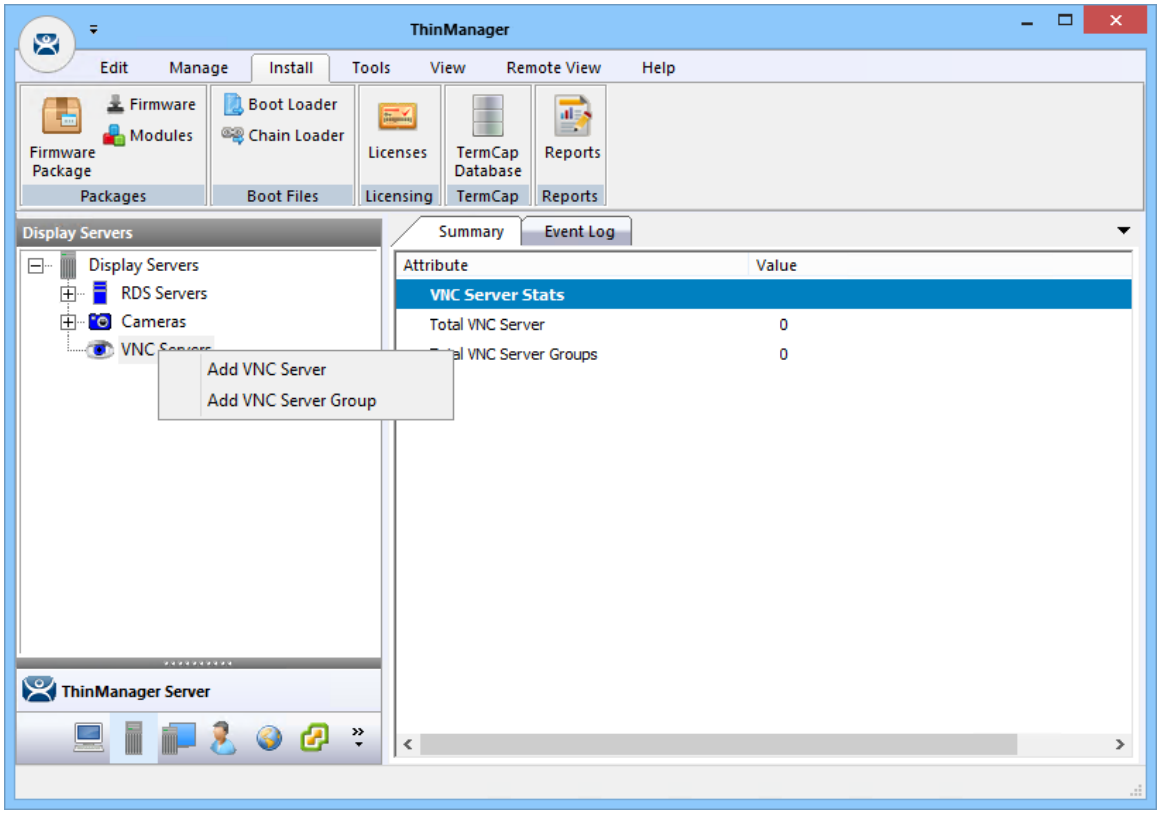
---

10. Sources – VNC Server

ThinManager has used the VNC protocol, or Virtual Networking Computing protocol, to shadow thin clients from within the ThinManager Server console or from another Terminal using a Terminal Shadow Display Client for many versions. Now ThinManager allows you to connect to any VNC Server to either shadow from the administrative console or through a display client.

This is useful in shadowing PanelView Plus panels.

The first step is to define the VNC server.

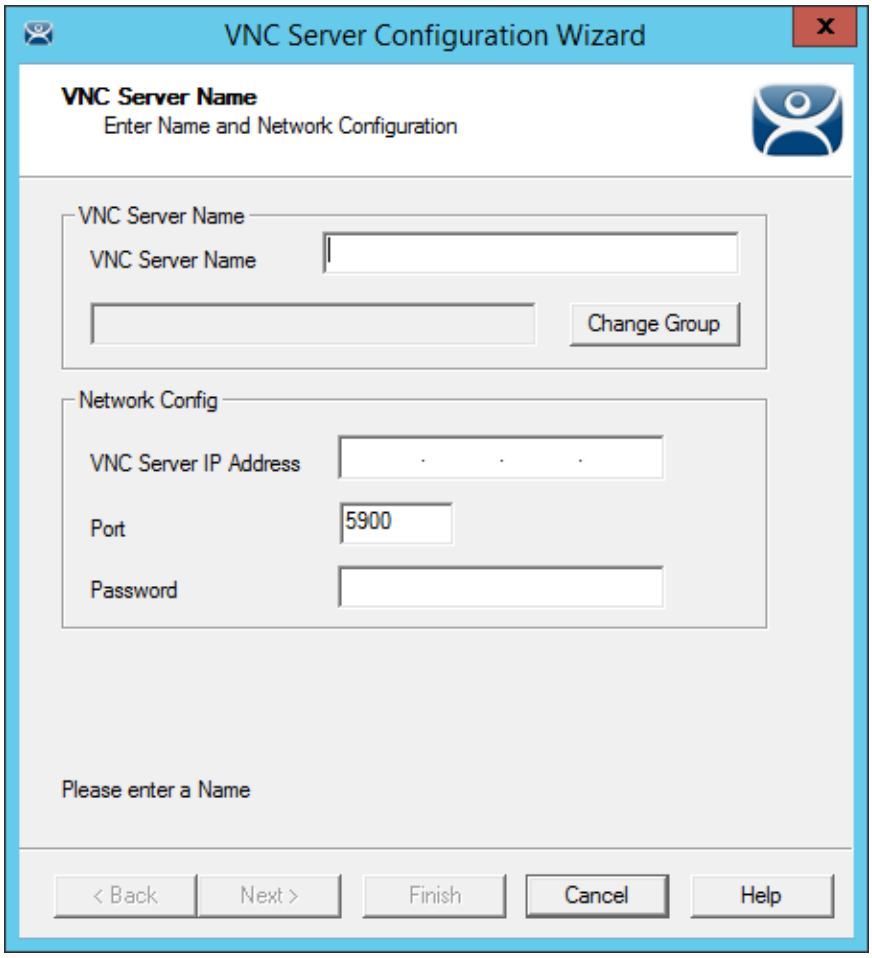


VNC Server Branch of the Display Server Tree

The **VNC Server Configuration Wizard** is launched from the **VNC Server** branch of the **Display Server** tree.

Open the **Display Server** tree by selecting the **Display Server** icon at the bottom of the ThinManager tree.

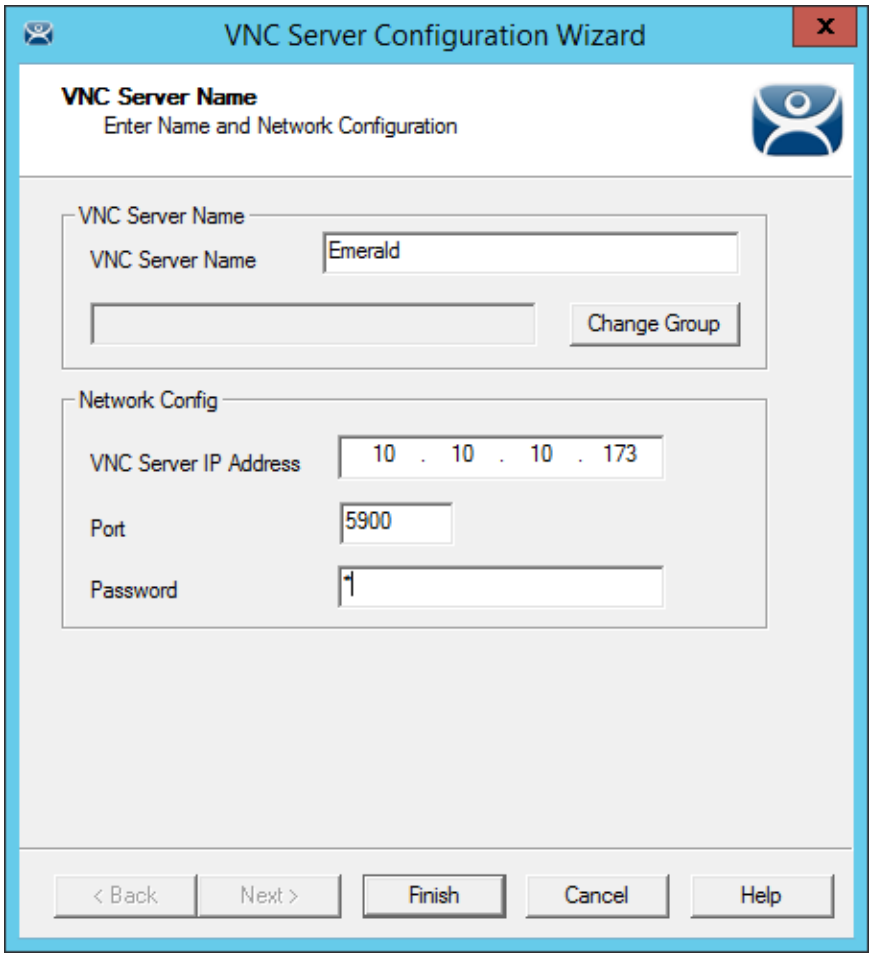
Right click on the VNC Server branch and select ***Add VNC Server*** to launch the **VNC Server Configuration Wizard**.



VNC Server Name Page of the VNC Server Configuration Wizard

The VNC Server has several required settings:

- **VNC Server Name** – Enter the name of the device that is acting as the VNC server.
- **VNC Server IP Address** – Enter the IP address of the device that is acting as the VNC server.
- **Port** – Enter the port your VNC server is using. The default is 5900
- **Password** – Enter a password for the VNC server, if needed.



VNC Server Name Page of the VNC Server Configuration Wizard

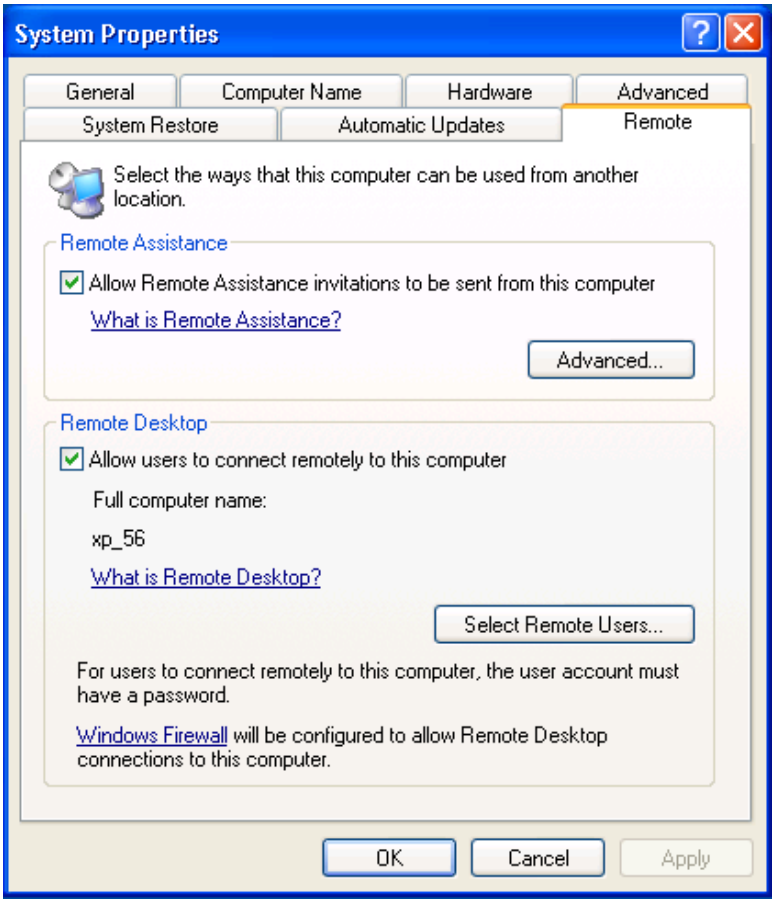
Select the ***Finish*** button to accept the configuration when the data is completed for the VNC Server.

You will need to create a VNC Display Client to deploy the VNC shadow. See Content – VNC Shadow on page 188 for details.

11. Sources - Workstations

Microsoft built RDP connectivity into the XP Pro, Vista Pro, and Windows 7 Pro workstations. You can make an RDP connection to them and transfer the desktop to another computer. ThinManager takes advantage of this feature to allow you to port a workstation to a thin client. These may be physical workstations or virtual workstations.

- ✓ **Go to the workstation and activate the remote desktop function.**



Workstation System Properties

Open the workstation System Properties either by right clicking on the My Computer icon and select Properties or by double clicking on the System icon in the Control Panel.

- ✓ **Check the Allow users to connect remotely to this computer checkbox.**

You can specify which users can access the workstation by clicking the ***Select Remote Users*** button.

Remote Desktop Users

Clicking the ***Select Remote Users*** button will open the **Remote Desktop Users** window. Use the ***Add*** button to grant permission to users.

This makes the workstations a source. You deliver the workstation to the thin client by defining Workstation Display Clients as shown in the Content section.

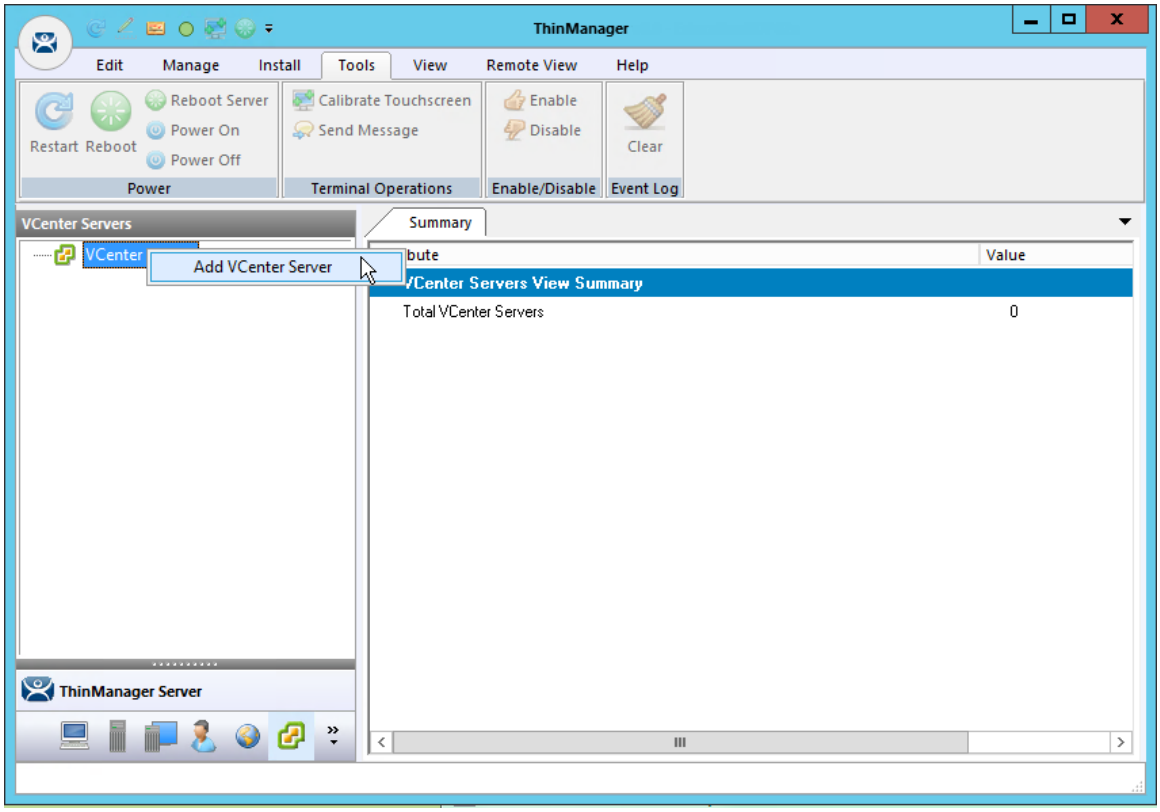
See Content - Workstation Deployment on page 173.

12. Sources – VCenter Servers

ThinManager plays well with virtual machines. The easiest way to handle virtual machines is to treat them as physical machines. ThinManager doesn't care if they are physical or virtual.

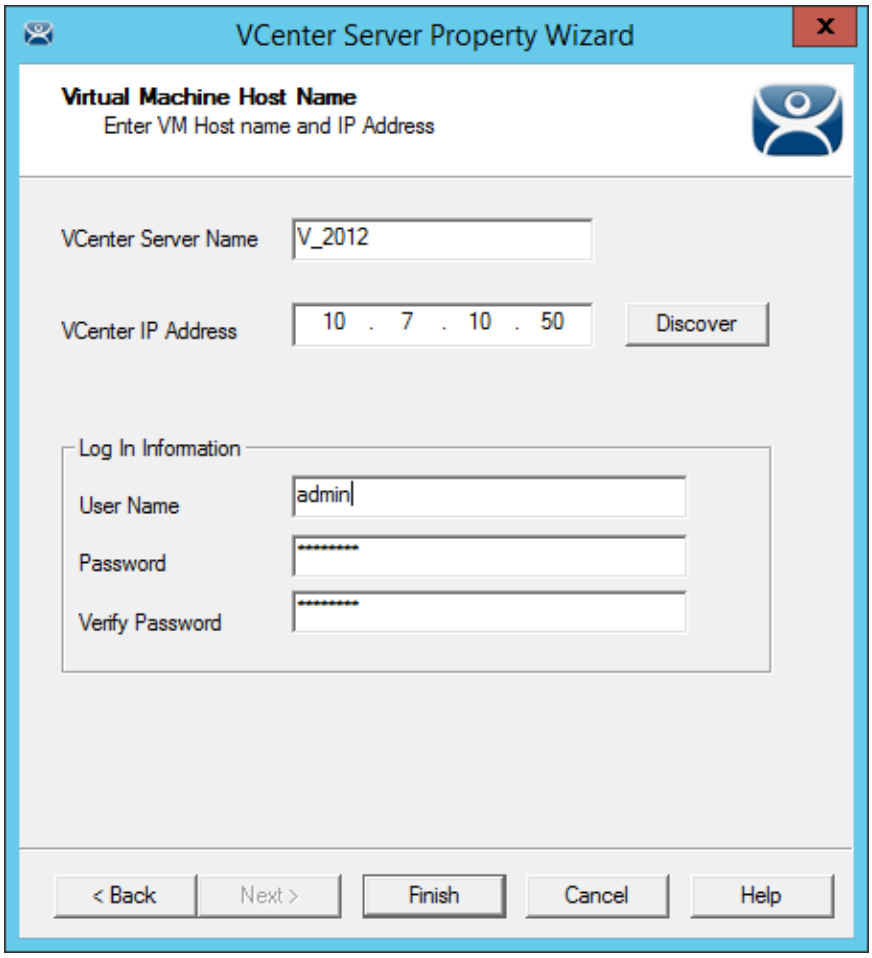
If you use VMware's ESXi you can connect using the ThinManager interface to access several of the management features provided by VMware's VCenter.

Select the **VCenter** icon on the ThinManager tree to open the **VCenter Server** tree.



VCenter Server Tree

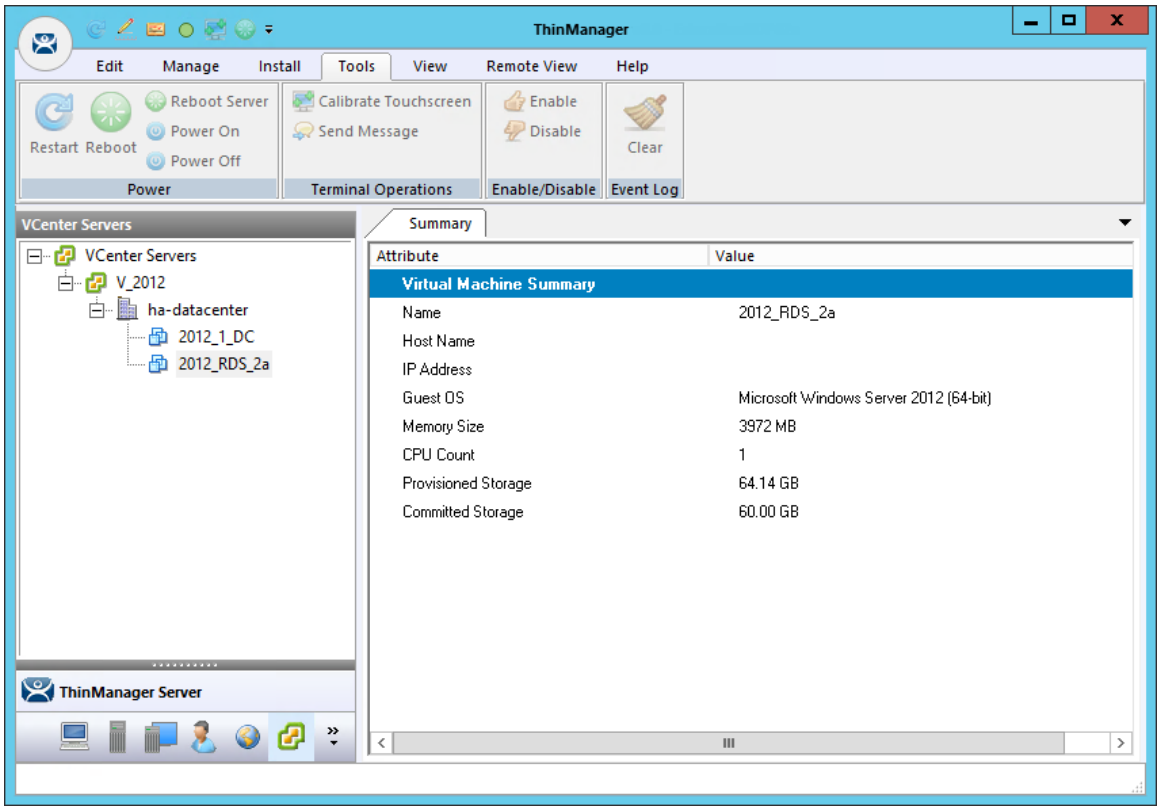
Right click on the **VCenter Server** branch and select Add ***VCenter Server*** to open the VCenter Server wizard.



VCenter Server Wizard

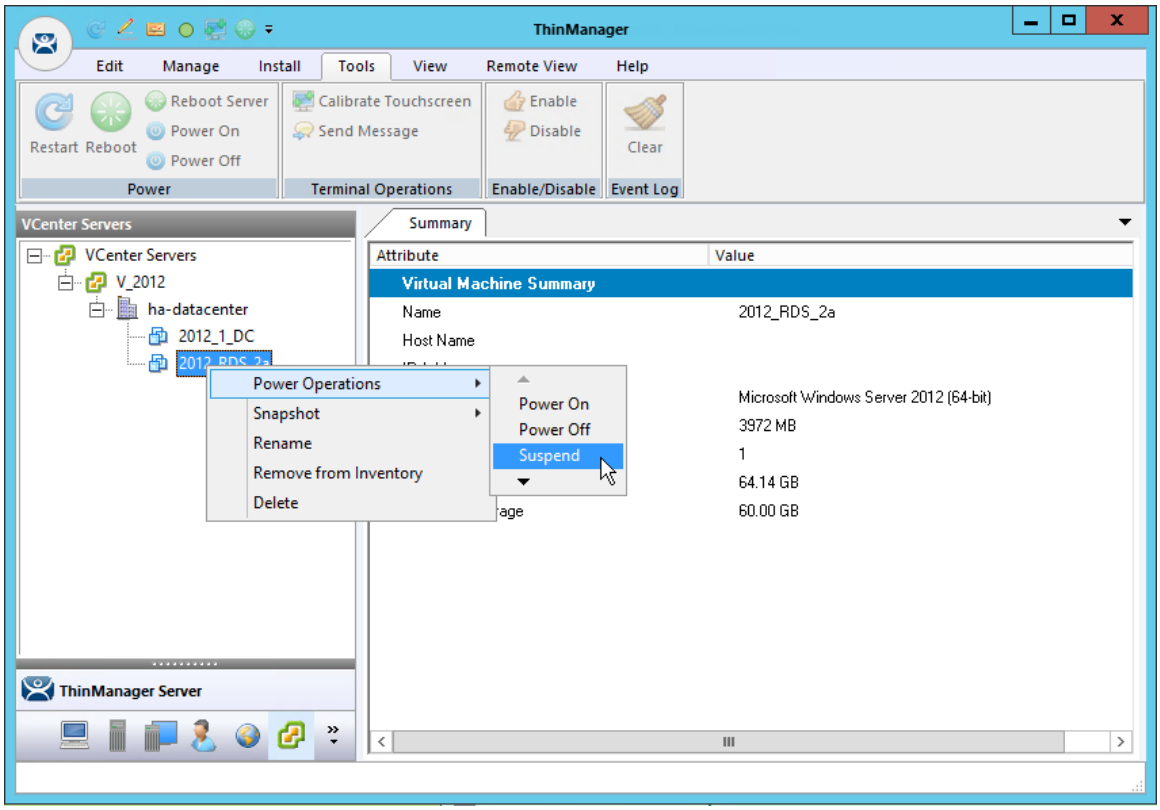
Enter a name and the IP address for your ESXi server.

Enter the administrative account in the ***Log In Information*** fields and select ***Finish*** to accept the changes and close the wizard.



Populated VCenter Server Tree in ThinManager

It will take a few minutes to connect and populate once you select finish. You can highlight the VCenter Server to see the connection status in the **Summary** tab.



VCenter Server Functions

Once the VCenter Server tree has populated you can right click on a virtual machine and do the following:

Power Operations:

- **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.

Snapshot:

- **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.

Rename – Allows the virtual machine to be renamed.

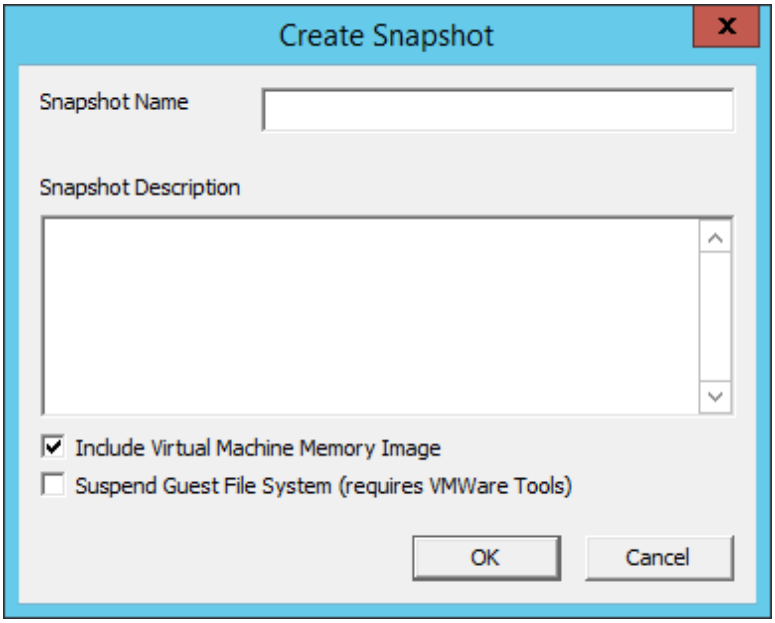
Remove from Inventory – Removes the virtual machine from the tree WITHOUT deleting the files.

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

12.1. Snapshots

Snapshots save the state of the virtual machine in a file. Snapshots allow you to preserve a working status before applying new applications, programs or updates. If the changes fail or are undesired, then the snapshot can be restored allowing the virtual machine to return to the pre-change state.

Right-clicking on the virtual machine and selecting ***Snapshot>Take Snapshot*** will launch the **Create Snapshot** window.



Create Snapshot Window

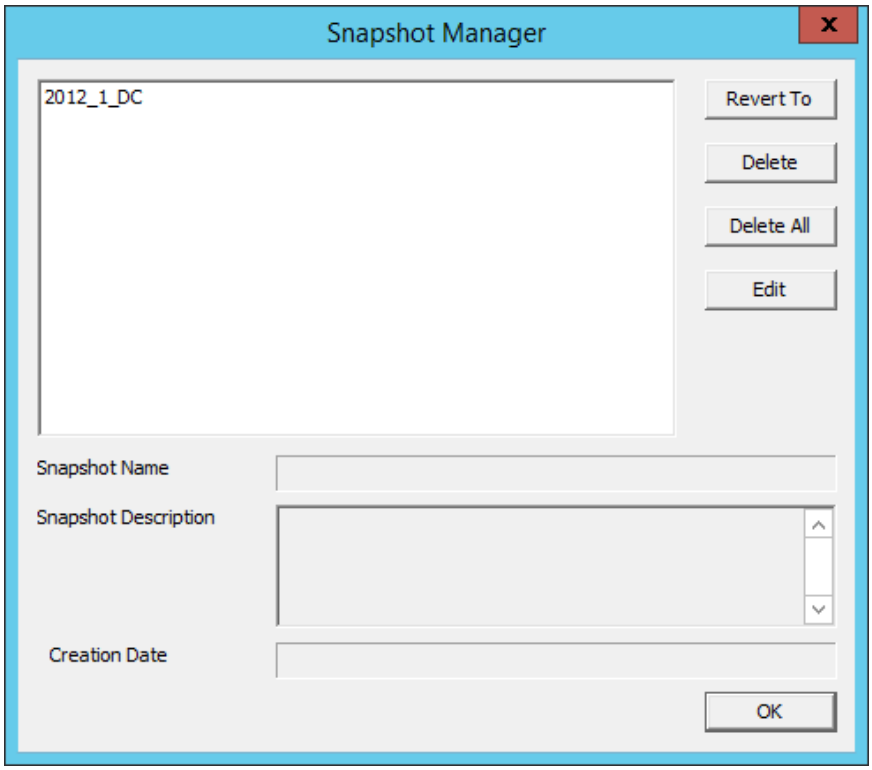
The **Create Snapshot** window allows you to name the snapshot and enter a description.

Select ***OK*** to save the snapshot or ***Cancel*** to close without saving.

Multiple snapshots of a virtual machine can be taken.

Right-clicking on the virtual machine and selecting ***Snapshot>Revert to Current Snapshot*** will apply the last snapshot taken.

Right-clicking on the virtual machine and selecting ***Snapshot>Snapshot Manager*** will launch the **Snapshot Manager** window.



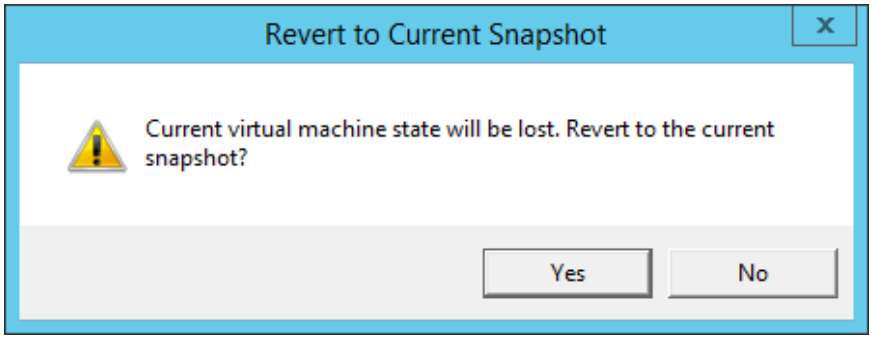
Snapshot Manager

The **Snapshot Manager** window shows all saved snapshots for the selected virtual machine. The **Snapshot Manager** window shows the name, description, and creation date of a highlighted snapshot.

The buttons on the Snapshot Manager include:

- ***Revert To*** **–** This applies the selected saved snapshot.
- ***Delete*** **–** This deletes a highlighted snapshot.
- ***Delete All*** **–** This deletes all saved snapshots.
- ***Edit*** **–** Opens the **Create Snapshot** window to allow changes to the name and description.
- ***OK*** **–** Closes the **Snapshot Manager**.

A dialog box will require confirmation before changes are made.



Revert to Snapshot Warning

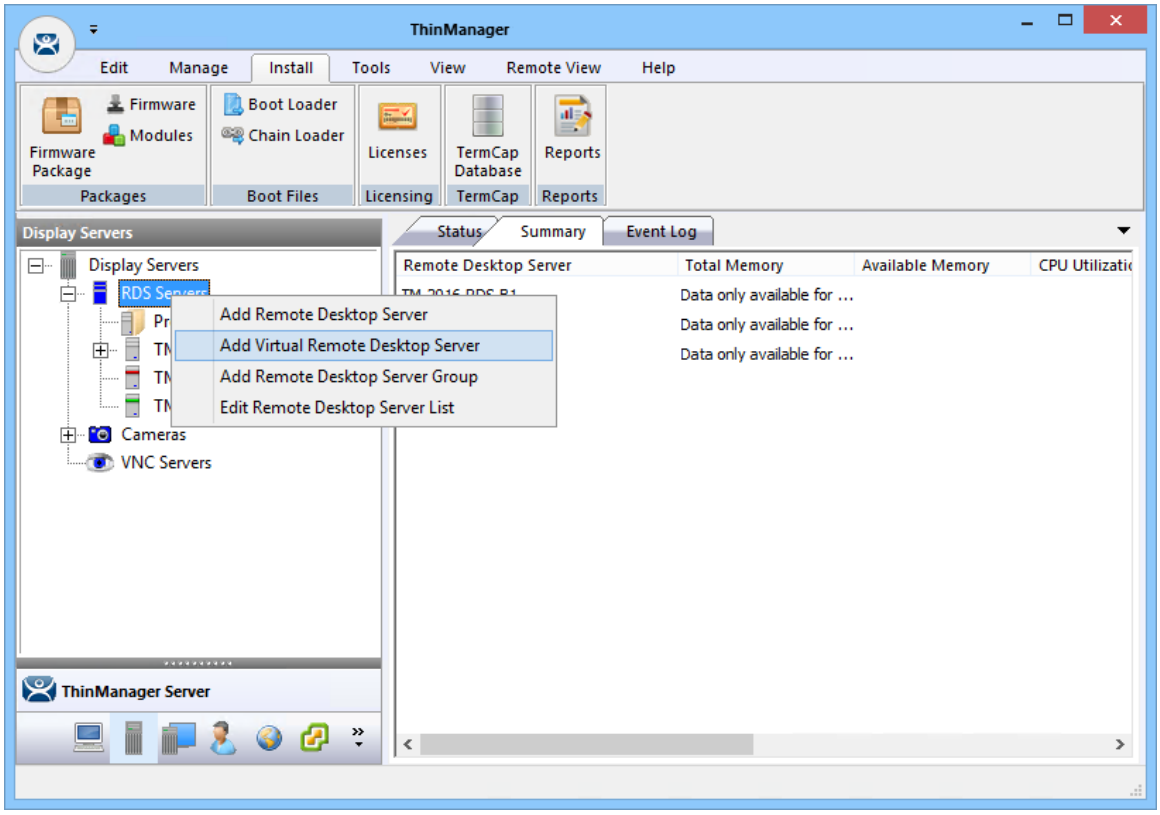
You will receive a warning when you initiate a snapshot restoration.

12.2. Adding a Virtual Server

Virtual Remote Desktop Servers that reside on a VCenter Server can be defined using a wizard.

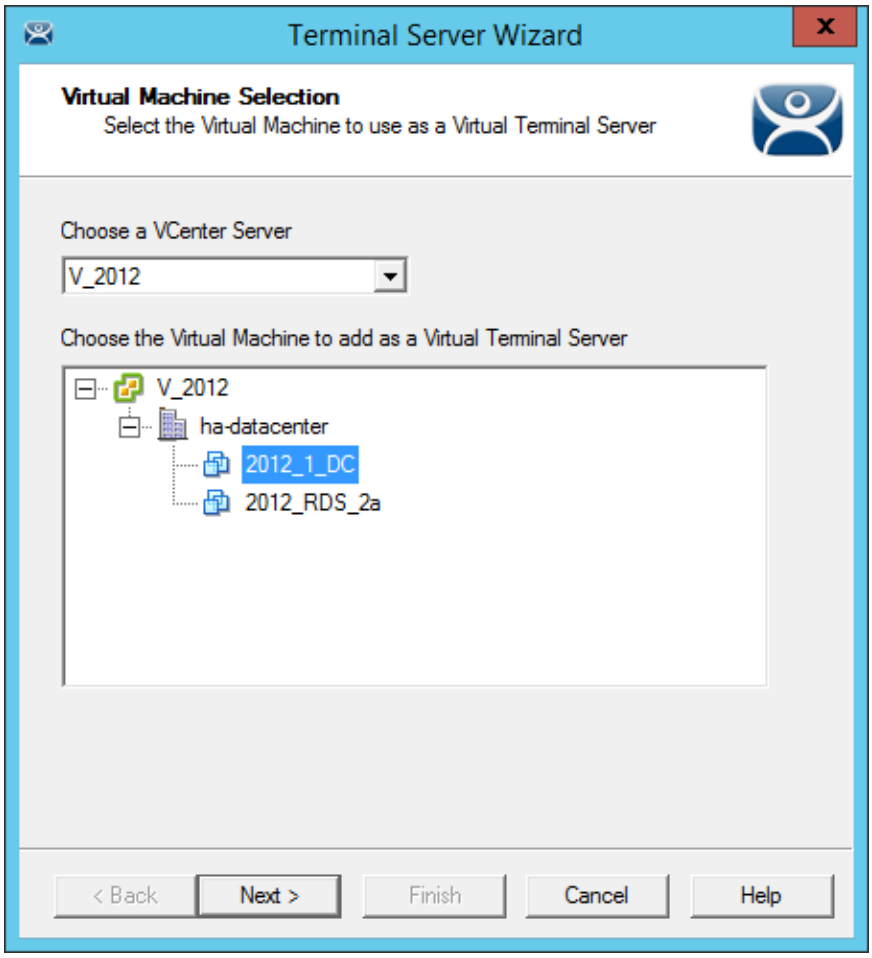
Select the **Remote Desktop Server** icon on the ThinManager tree to open the **Remote Desktop Server** tree.

Right click on the Remote Desktop Servers branch and select ***Add Virtual Remote Desktop Server.***



Remote Desktop Server Tree

Selecting the ***Add Virtual Remote Desktop Server*** command launches the Remote Desktop Server Wizard.



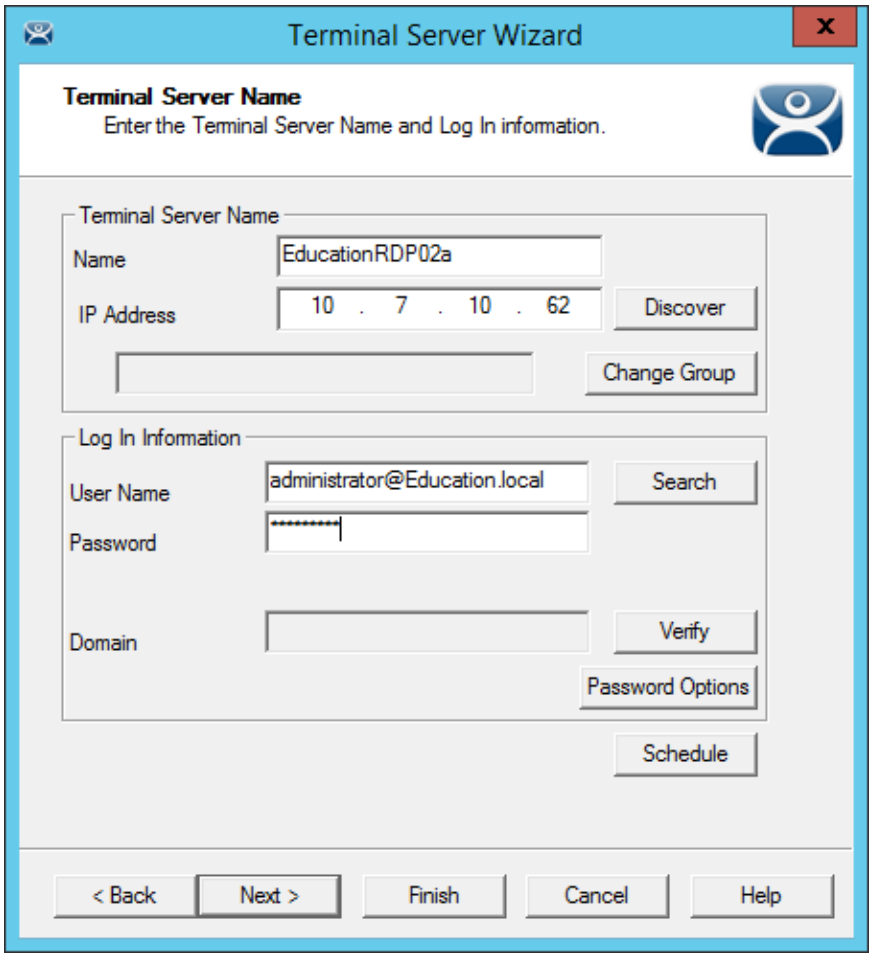
Virtual Machine Selection Page

The Remote Desktop Server Configuration Wizard shows an additional page when you select the ***Add Virtual Remote Desktop Server*** command.

Select your VCenter Server in the drop-down if you have multiples defined.

The VCenter Server tree will populate the selection box.

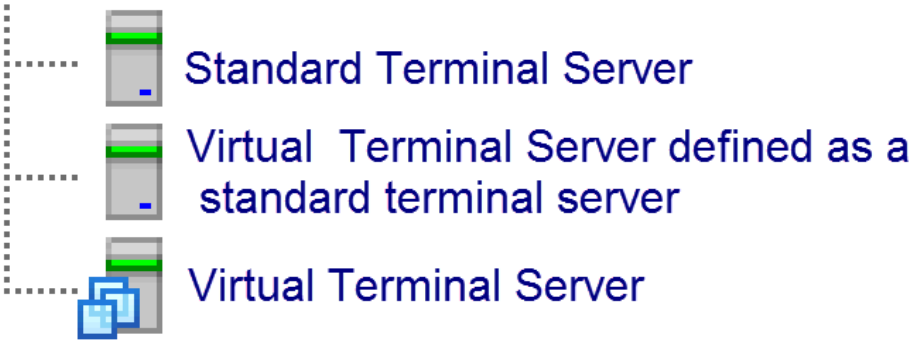
Select the virtual Remote Desktop Server you want and select the ***Next*** button.



Remote Desktop Server Name Page

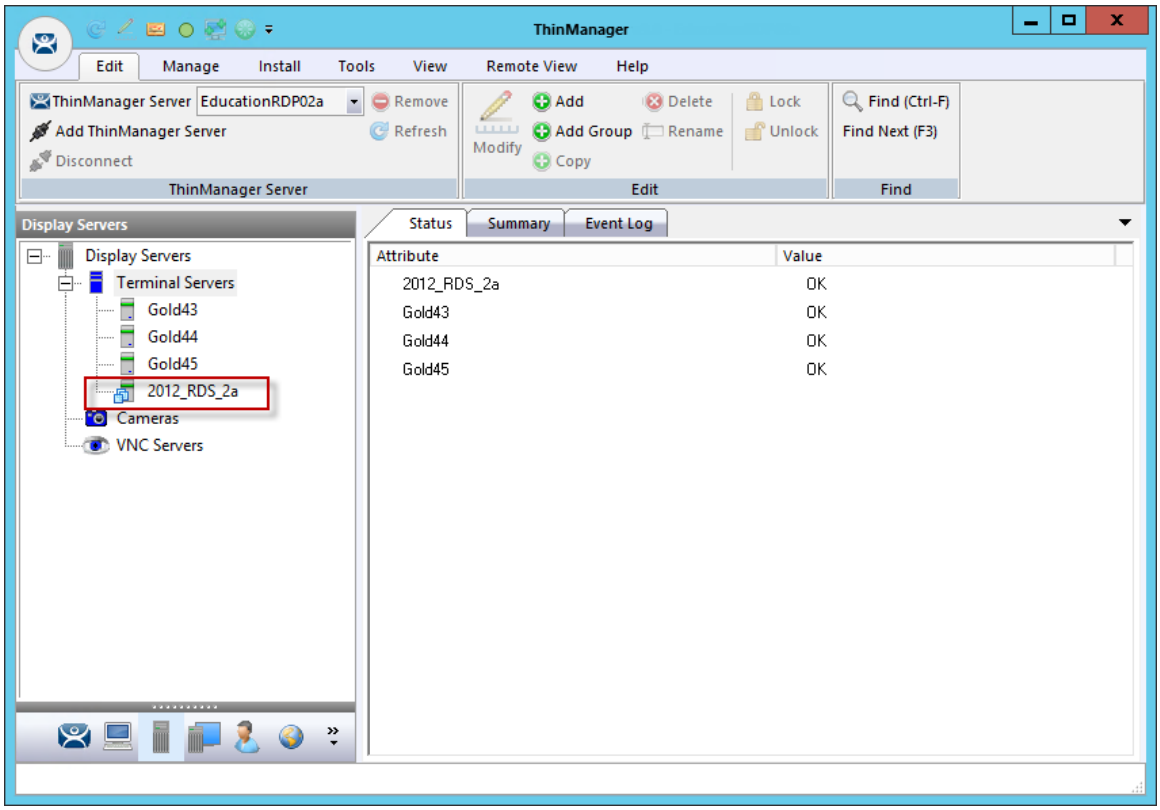
Finish the configuration as you do other Remote Desktop Servers by adding the administrative account in the ***Log In Information*** fields. The IP address should fill automatically.

Finish the wizard as you would regular Remote Desktop Servers by clicking ***Finish*** or by clicking ***Next*** and checking the SmartSession load balancing checkbox.



Remote Desktop Server Icons

The tree will show a different icon for a Remote Desktop Server configured as a virtual Remote Desktop Server. A virtual Remote Desktop Server created as a physical Remote Desktop Server will show the same icon as a physical Remote Desktop Server.



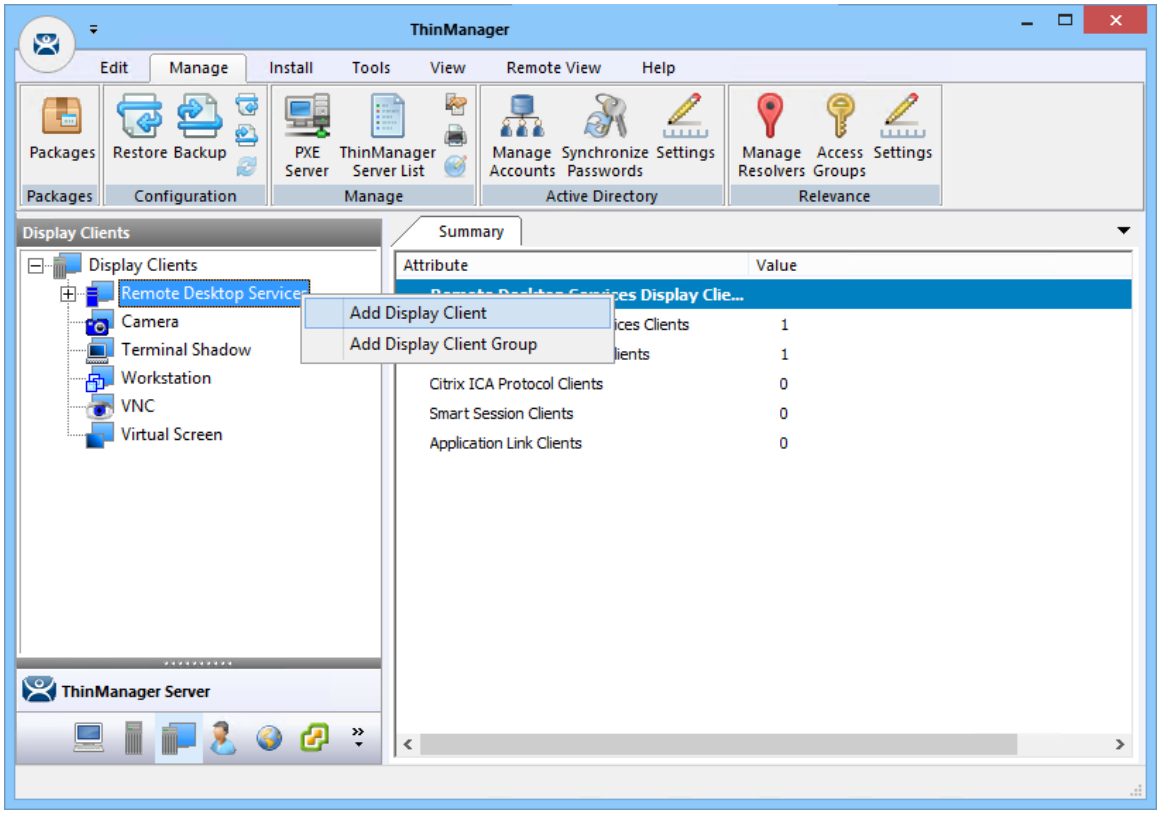
Display Server Tree

Virtual Remote Desktop Servers can be used in display clients just like physical Remote Desktop Servers.

13. Content – Remote Desktop Services Display Client

Content is sent to devices through Display Clients. The most common content sent to a device is a Windows application. These are sent as Remote Desktop Services display clients. You can either give a person a full desktop or limit them to a specific application with AppLink.

ThinManager allows you to deploy several applications to a device at once using MultiSession.

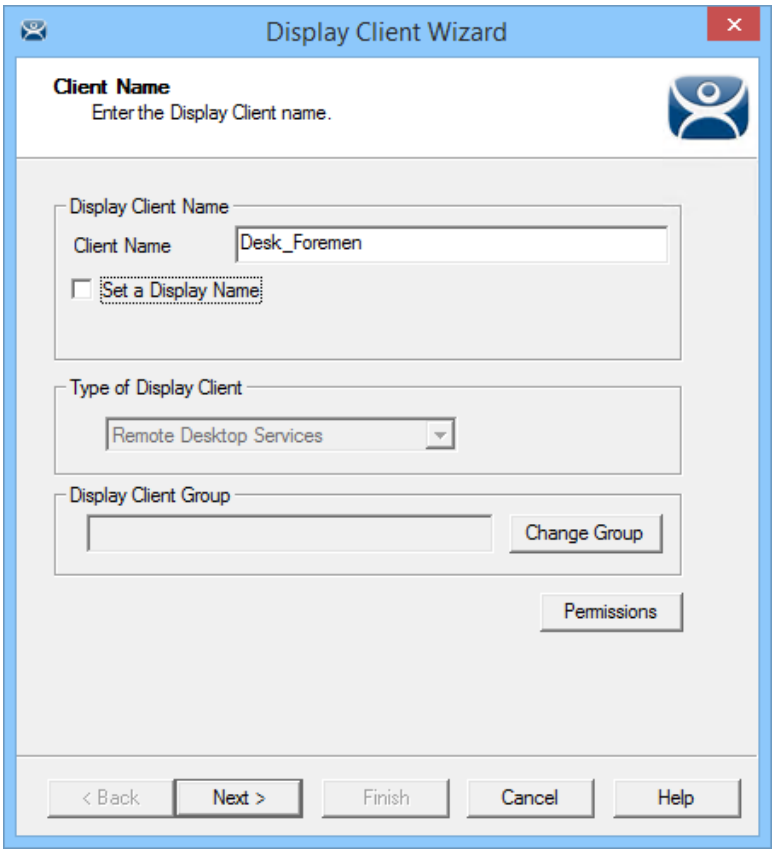


Launch the Display Client Configuration Wizard

Applications are defined using the **Display Client Configuration Wizard**. It is launched by selecting the **Display Client icon** at the bottom of the ThinManager tree, right clicking on the **Remote Desktop Services** branch, and selecting ***Add Display Client***.

13.1. Desktop

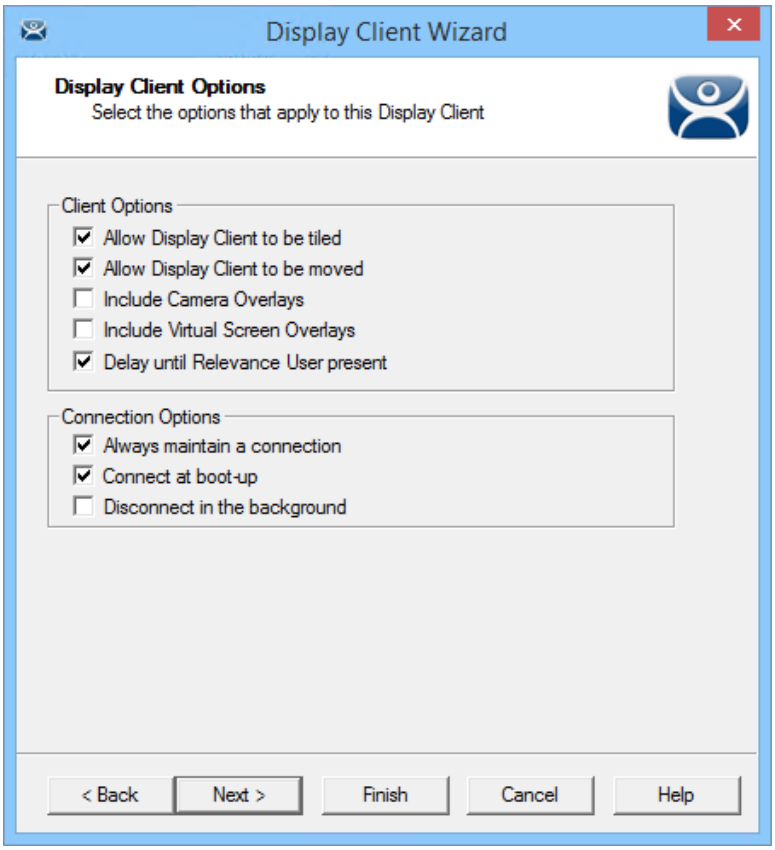
You can present a desktop to a Terminal for the user. The device can automatically login with the Terminal account or you can allow the user to login manually so that they receive the desktop that is associated with their user account.



Client Name Page of the Display Client Wizard

Enter a name for the display client in the ***Client Name*** field.

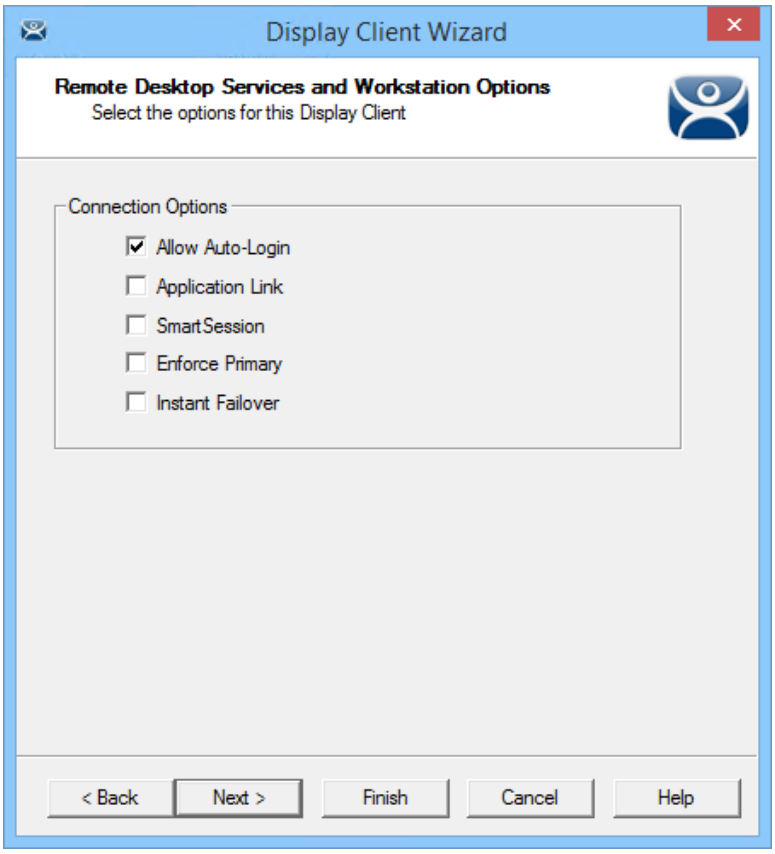
The ***Type of Display Client*** is automatically filled if you right click on the Remote Desktop Services branch. If you right click on the top level Display Clients branch then you will have to select the type of display client you want.



Display Client Options Page of the Display Client Wizard

The checkbox settings are:

- ***Allow group to be tiled*** – This allows the display client to be tiled when checked.
- ***Allow Group to be moved (MultiMonitor)*** – This allows the display client to be moved from screen to screen when using MultiMonitor. A display client that allows it to be moved can be anchored with a setting on the **Screen Options** page of the **Terminal Configuration Wizard**.
- **Include IP Camera Overlays** –This allows an IP Camera overlay to be added to this display client.
- **Include Virtual Screen Overlays** –This allows a display client overlay to be added to this display client. See Content – Virtual Screens on page 195 for details.
- **Delay until Relevance User present** - This will hide the Display Client until a Relevance User logs in. When the Display Client launches it will use the credentials of the Relevance User to start the session.
- ***Always maintain a connection*** – This keeps a session active, reconnecting and restarting if it is closed. If unchecked, the user can close a session and another session won't start automatically.
- ***Connect at boot-up*** – This starts a session for this display client at boot up. Otherwise a user action is required to start the session if unchecked.
- ***Disconnect in background*** – If checked, a display client being used in a MultiSession configuration will disconnect once it is moved into the background. This could be done to require fewer resources.



Remote Desktop Services and Workstation Options Page of the Display Client Wizard

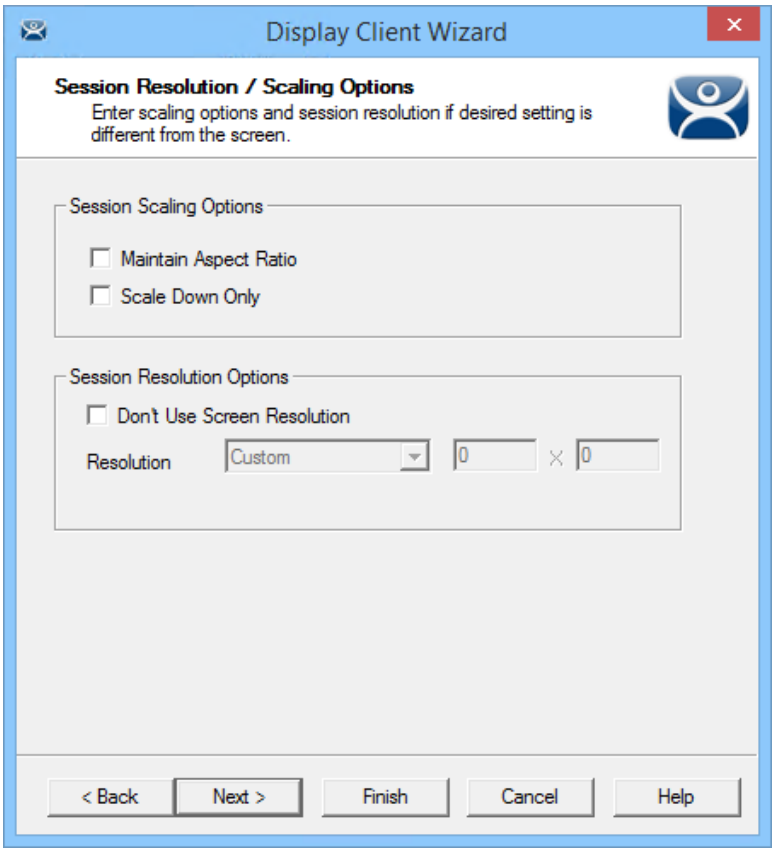
The **Remote Desktop Services and Workstation Options** page of the Display Client Wizard is the key page in Display Client configuration. These settings control how Remote Desktop Server content is deployed to the Terminal.

- ✓ **Leave the Application Link checkbox uncheck to deploy a desktop.**
- ✓ **Uncheck "Allow Auto-Login" if you want to provide the login prompt and force manual login.**

These are the configurations that this page controls:

- ***Allow Auto-Login*** – This automatically logs into the session if a user account is applied to the Terminal.
  Unchecking this shows the login window and forces a manual login. This is useful to provide a user with a login based on their group policy.
- ***Application Link*** – AppLink launches a single application instead of a desktop. The session lacks the Explorer shell and does not show desktop icons or the Start menu. Closing the AppLink program will kill the session and re-spawn a new session with the application running. This allows the administrator to control content to the user in a simple manner without needing to use group policies.
- ***SmartSession*** – This adds SmartSession to the display client which provides load balancing between member Remote Desktop Servers.
  SmartSession uses CPU availability, memory, and the number of sessions on the member Remote Desktop Servers to determine the load on the servers. Thin clients connect to the Remote Desktop Server with the most available resources.
- ***Enforce Primary*** – This setting tells a thin client to reconnect to its original Remote Desktop Server if that Remote Desktop Server has failed and recovered. This is not available if SmartSession is selected.

- ***Instant Failover*** – This activates Instant Failover. In Instant Failover you specify at least two Remote Desktop Servers. On boot the Terminal will connect and start sessions on two Remote Desktop Servers but will only display one session. If the first Remote Desktop Server fails, the session of the second Remote Desktop Server session is immediately displayed, eliminating any downtime due to Remote Desktop Server failure.
  An Instant Failover display client will want to have two active sessions so if one Remote Desktop Server fails the display client will start a session on a third Remote Desktop Server if you have one in the server list.



Session Resolution/Scaling Options Page

The **Session Resolution/Scaling Options** page sets the ability of the display client to scale the session. This page has parameters that can be configured:

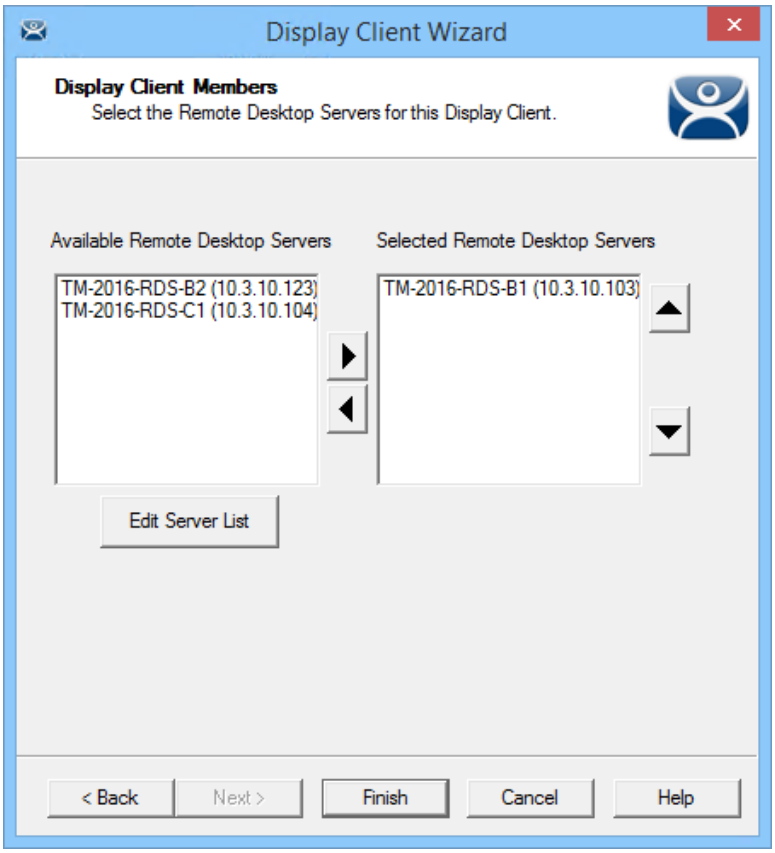
Session Scaling Options:

- ***Maintain Aspect Ratio –*** This keeps the aspect ratio of the session constant when scaling. If unchecked the session will fit the available display size.
- ***Scale Down Only –*** This will allow a session to be shrunk for a thumbnail but won't expand it beyond the original size designation.

Screen Resolution Options:

- ***Don't Use Screen Resolution* –** This allows you to override the session resolution and set a new resolution for the display.
- ***Resolution* –** These drop-downs allow you to select a new resolution for the display if the ***Don't Use Screen Resolution*** checkbox is selected.

Select ***Next*** to continue the wizard.



Display Client Members Page of the Display Client Wizard

The **Display Client Members** page of **the Display Client Wizard** allows the selection of Remote Desktop Servers that you want the application to run on.

Move the Remote Desktop Servers you want to use from the ***Available Remote Desktop Server*** list to the ***Selected Remote Desktop Server*** list by highlighting the desired server and using the Left or Right arrow.

Note: If your defined Remote Desktop Servers do not show in the list then you probably selected ***SmartSession*** on the previous page without checking the ***"Available for Display Clients using SmartSession"*** on the **Remote Desktop Server Capability** page of the Remote Desktop Server Wizard.

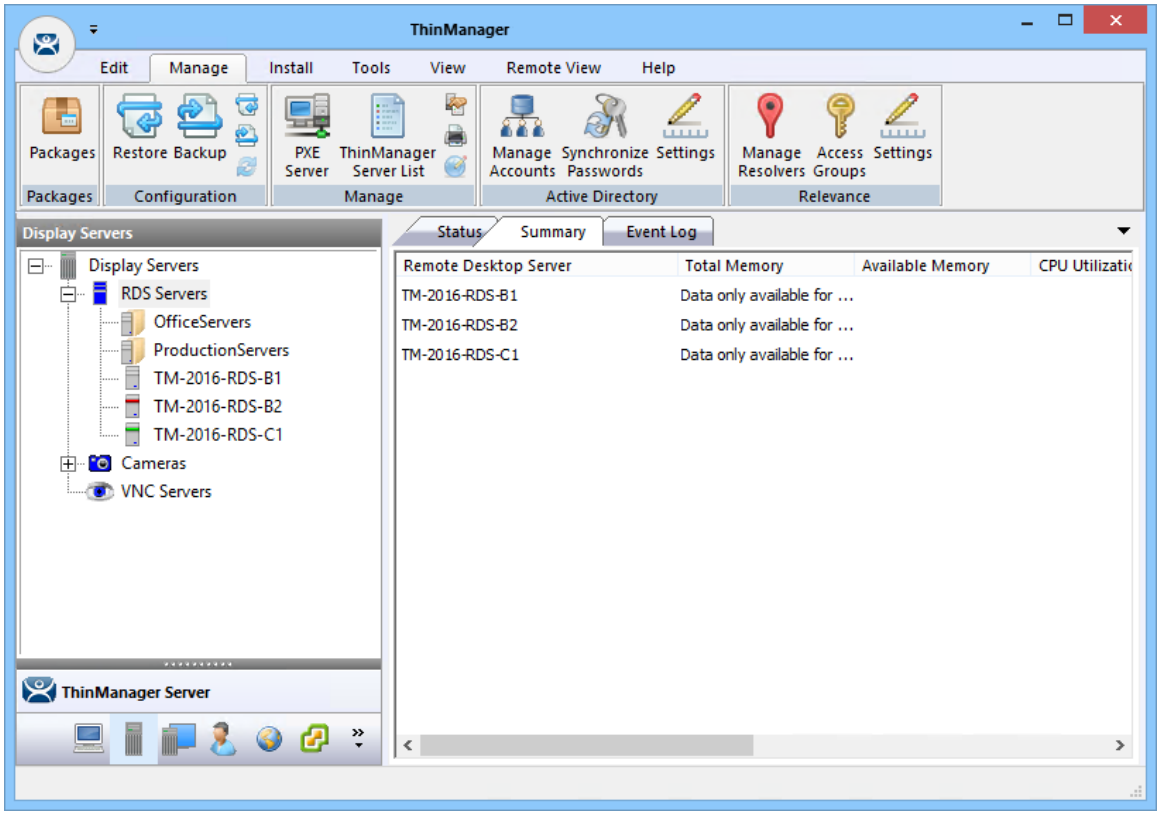
You can click the ***Edit Server List*** button to open the **Remote Desktop Server List Wizard** to open each Remote Desktop Server wizard to check the needed checkbox.

Adding two Remote Desktop Servers to the ***Selected Remote Desktop Server*** list will provide failover. In normal failover the Terminal will connect to the first Remote Desktop Server. If it fails it will connect to the second.

SmartSession load balancing does not follow the list order but instead goes to the Remote Desktop Server with the lightest load.

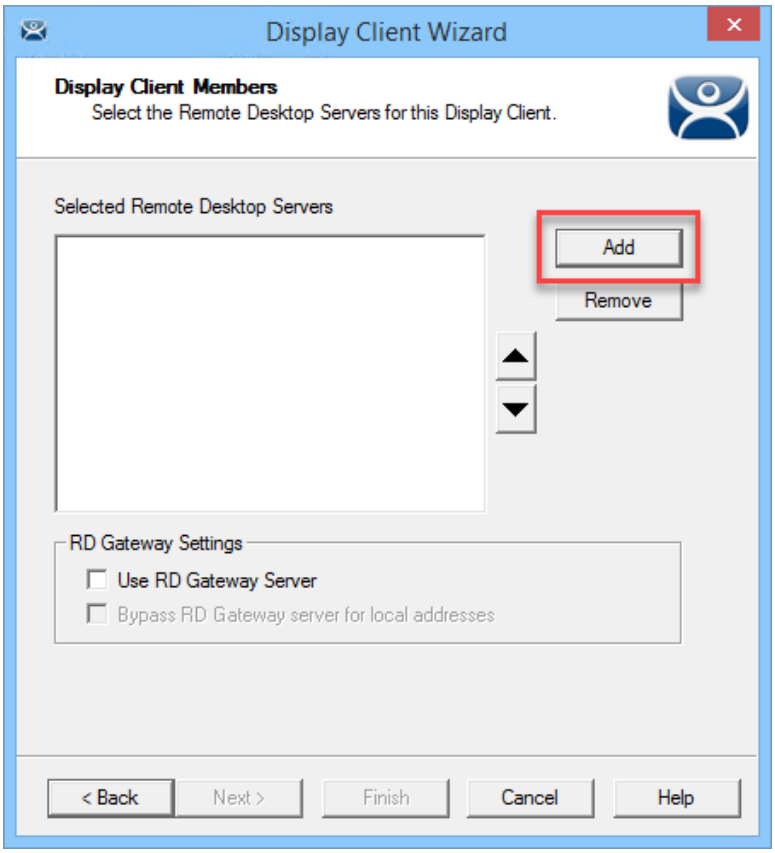
13.1.1. Display Client Using Remote Desktop Server Groups

The Display Client Configuration wizard will take a different appearance if Remote Desktop Server Groups are used to speed selection of Remote Desktop Servers.



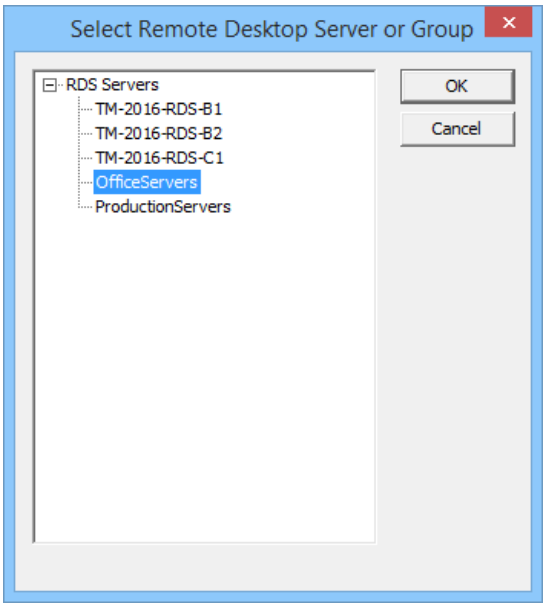
Remote Desktop Server Groups Defined in the RDS Servers Tree

This example has two RDS Groups, *OfficeServers* and *ProductionServers*.



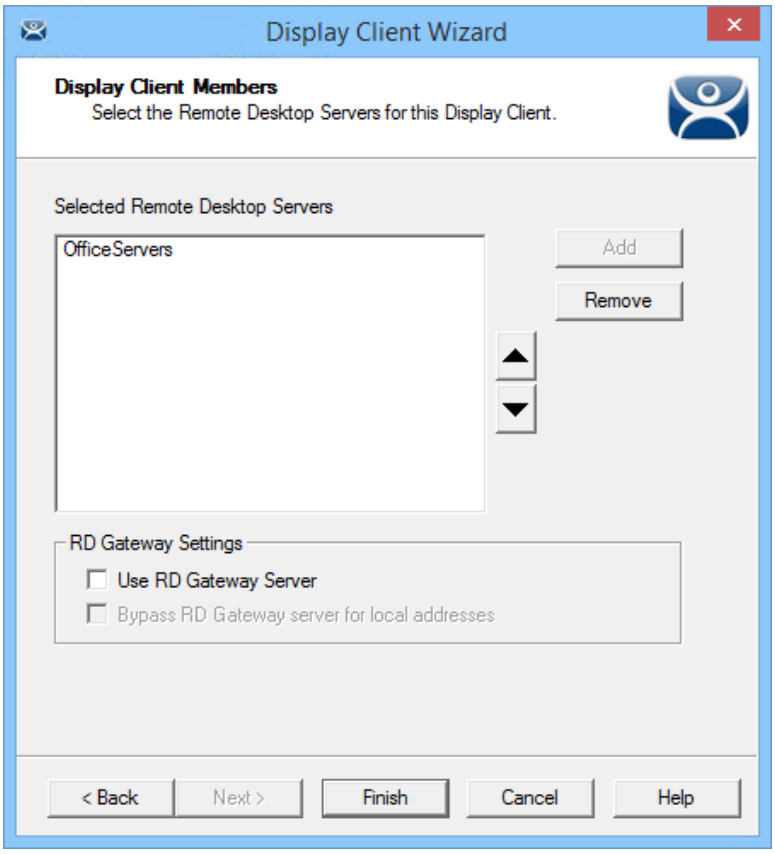
Display Client Members Page with RDS Server Groups

The **Display Client Mem**bers page has a different format to select the Remote Desktop Servers. Select the *Add* button to launch the **Select Remote Desktop Server or Group** window.



Select Remote Desktop Server or Group Window

Highlight the desired RDS group and select the **OK** button.



Display Client Members Page with RDS Server Groups

Two checkboxes will be displayed to control the use of the Microsoft RDP Gateway.:

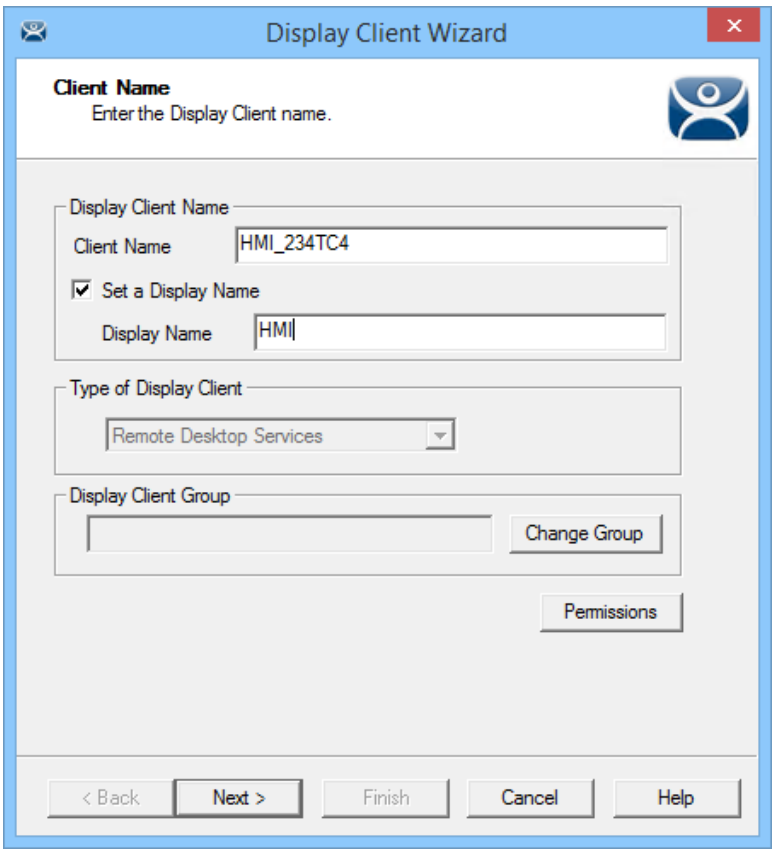
- **Use RD Gateway Server** – This checkbox, if selected, prompts the Display Client to use the Microsoft RD Gateway. See Remote Desktop Server Group on page 64.
- **Bypass RD Gateway server for local address** – This checkbox, if selected, allows the Display Client to use a Remote Desktop Server without going through the RD Gateway if the Terminal and Remote Desktop Server are on the same subnet.

13.2. Single Application Deployment with AppLink

ThinManager uses its AppLink function to launch a single application instead of a desktop. This allows you to control what the user can see and interact with.

The application is launched instead of the Windows Explorer desktop. Closing the application will cause the Terminal to disconnect and re-launch a new connection to the server with the application running.

To create a single application display client launch the **Display Client Configuration Wizard** by selecting the **Display Client icon** at the bottom of the ThinManager tree, right clicking on the **Remote Desktop Services** branch, and selecting ***Add Display Client***.

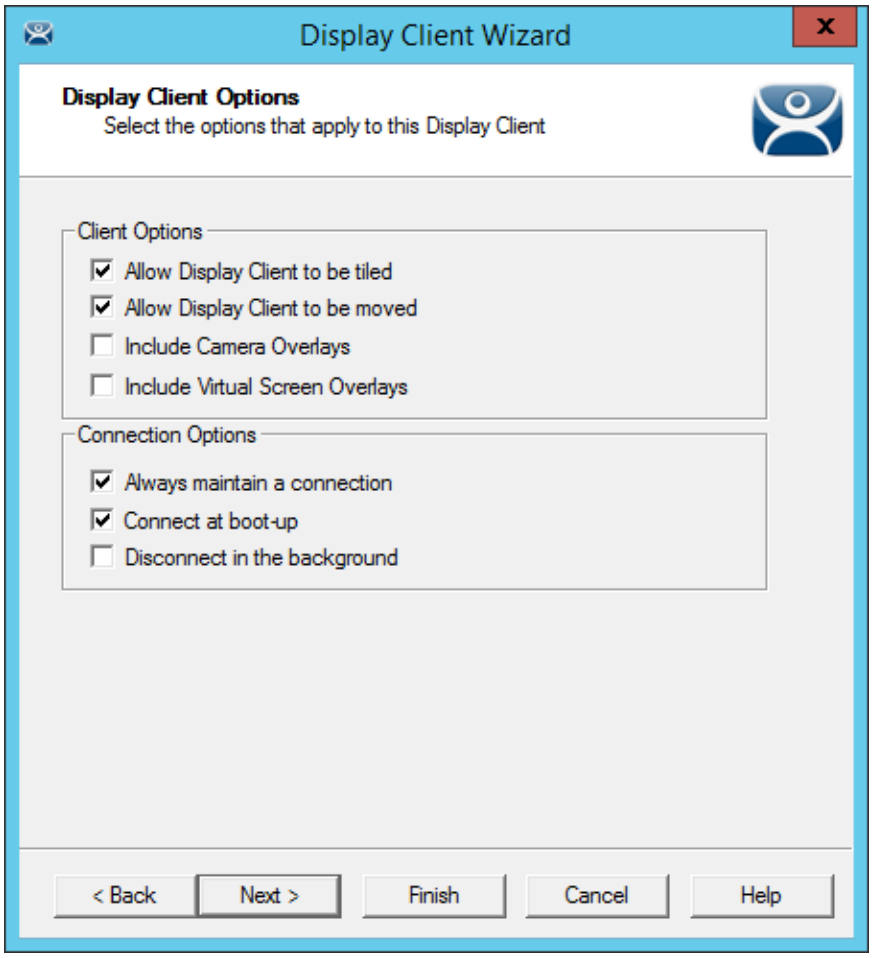


Client Name Page of the Display Client Wizard

Enter a name for the display client in the ***Client Name*** field.

The ***Type of Display Client*** is automatically filled if you right click on the Remote Desktop Services branch. If you right click on the top level Display Clients branch then you will have to select the type of display client you want.

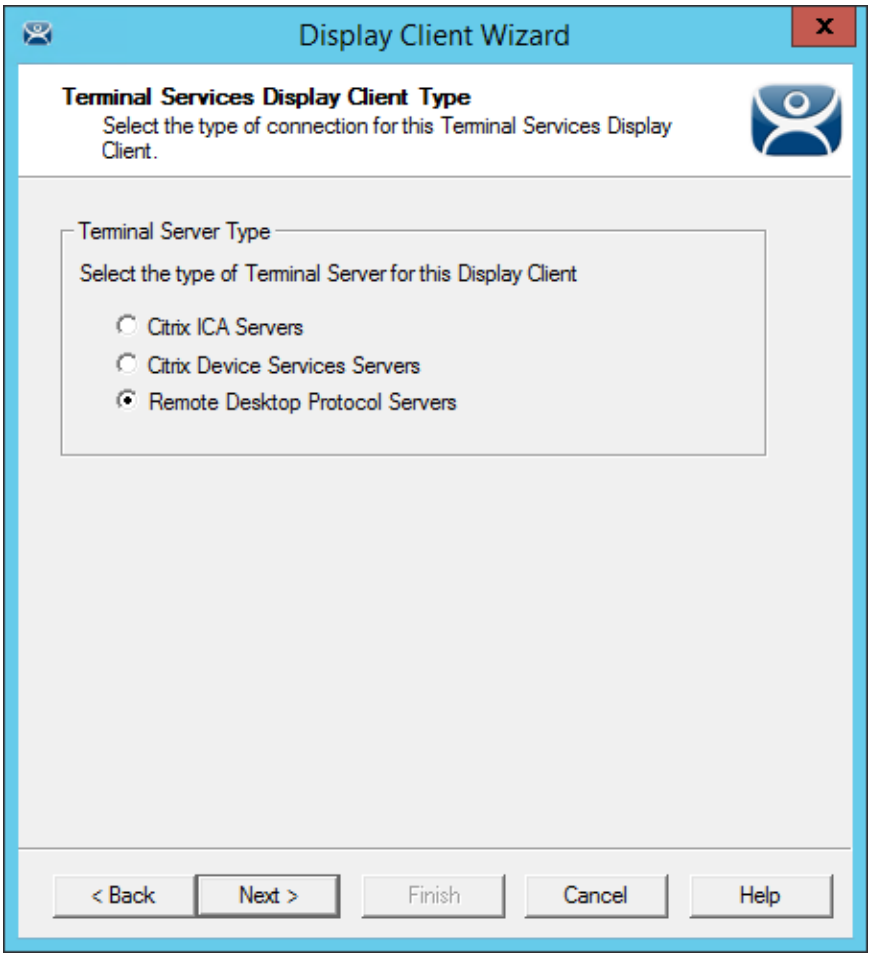
The ***Set a Display Name*** will allow you to simplify the Display Client name in the tree.



Display Client Options Page of the Display Client Wizard

The checkbox settings are:

- ***Allow group to be tiled*** – This allows the display client to be tiled when checked.
- ***Allow Group to be moved (MultiMonitor)*** – This allows the display client to be moved from screen to screen when using MultiMonitor. A display client that allows it to be moved can be anchored with a setting on the **Screen Options** page of the **Terminal Configuration Wizard**.
- **Include IP Camera Overlays** –This allows an IP Camera overlay to be added to this display client.
- **Include Virtual Screen Overlays** –This allows a display client overlay to be added to this display client. See Content – Virtual Screens on page 195 for details.
- ***Always maintain a connection*** – This keeps a session active, reconnecting and restarting if it is closed. If unchecked, the user can close a session and another session won't start automatically.
- ***Connect at boot-up*** – This starts a session for this display client at boot up. Otherwise a user action is required to start the session if unchecked.
- ***Disconnect in background*** – If checked, a display client being used in a MultiSession configuration will disconnect once it is moved into the background. This could be done to require fewer resources.

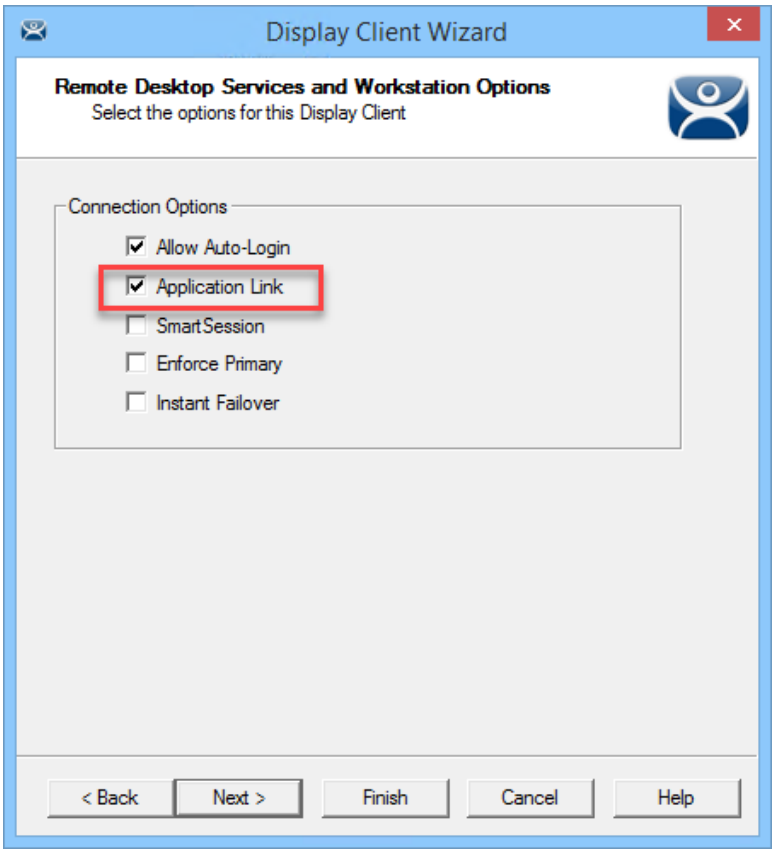


Remote Desktop Services Display Client Type Page of the Display Client Wizard

ThinManager thin clients can use the default **Microsoft RDP (Remote Desktop Protocol)** or the **Citrix ICA (Independent Computing Architecture)**.

Select the protocol you wish to use with the display client and select the ***Next*** button to continue.

Note: This page will not be shown unless you are upgrading from a system with ICA checked or you have added the registry entry as shown in Citrix Servers on page 56.



Remote Desktop Services and Workstation Options Page of the Display Client Wizard

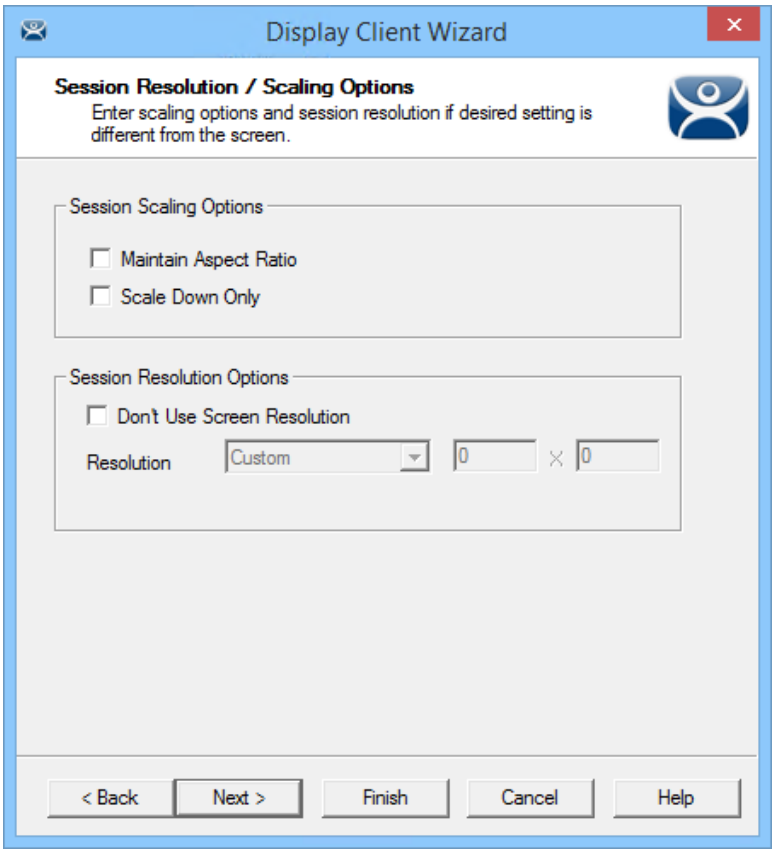
The **Remote Desktop Services and Workstation Options** page of the Display Client Wizard is the key page in Display Client configuration. These settings control how Remote Desktop Server content is deployed to the Terminal.

- ✓ **Check the "Application Link" checkbox to deploy a single AppLink application.**
- ✓ **Uncheck "Allow Auto-Login" if you want to provide the login prompt and force manual login.**

These are the configurations that this page controls:

- ***Allow Auto-Login*** – This automatically logs into the session if a user account is applied to the Terminal. This is the normal setting.
  Unchecking this shows the login window and forces a manual login. This is useful to provide a user with a login based on their group policy.
- ***Application Link*** – AppLink launches a single application instead of a desktop. The session lacks the Explorer shell and does not show desktop icons or the Start menu. Closing the AppLink program will kill the session and re-spawn a new session with the application running. This allows the administrator to control content to the user in a simple manner without needing to use group policies.
- ***SmartSession*** – This adds SmartSession to the display client which provides load balancing between member Remote Desktop Servers.
  SmartSession uses CPU availability, memory, and the number of sessions on the member Remote Desktop Servers to determine the load on the servers. Thin clients connect to the Remote Desktop Server with the most available resources.
- ***Enforce Primary*** – This setting tells a thin client to reconnect to its original Remote Desktop Server if that Remote Desktop Server has failed and recovered. This is not available if SmartSession is selected.

- ***Instant Failover*** – This activates Instant Failover. In Instant Failover you specify at least two Remote Desktop Servers. On boot the Terminal will connect and start sessions on two Remote Desktop Servers but will only display one session. If the first Remote Desktop Server fails, the session of the second Remote Desktop Server session is immediately displayed, eliminating any downtime due to Remote Desktop Server failure.
  An Instant Failover display client will want to have two active sessions so if one Remote Desktop Server fails the display client will start a session on a third Remote Desktop Server if you have one in the server list.
  Instant Failover is free for ThinManager but will probably require a second application license as you have two active sessions running the application.



Session Resolution/Scaling Options Page

The **Session Resolution/Scaling Options** page sets the ability of the display client to scale the session. This page has parameters that can be configured:

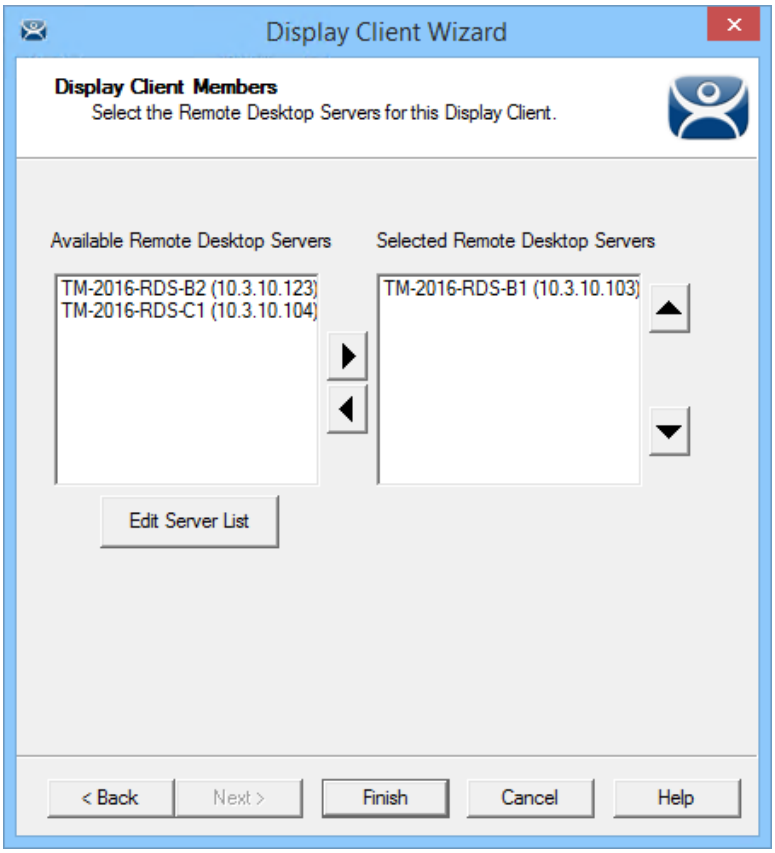
Session Scaling Options:

- ***Maintain Aspect Ratio –*** This keeps the aspect ratio of the session constant when scaling. If unchecked the session will fit the available display size.
- ***Scale Down Only –*** This will allow a session to be shrunk for a thumbnail but won't expand it beyond the original size designation.

Screen Resolution Options:

- ***Don't Use Screen Resolution* –** This allows you to override the session resolution and set a new resolution for the display.
- ***Resolution* –** These drop-downs allow you to select a new resolution for the display if the ***Don't Use Screen Resolution*** checkbox is selected.

Select ***Next*** to continue the wizard.



Display Client Members Page of the Display Client Wizard

The **Display Client Members** page of **the Display Client Wizard** allows the selection of Remote Desktop Servers that you want the application to run on.

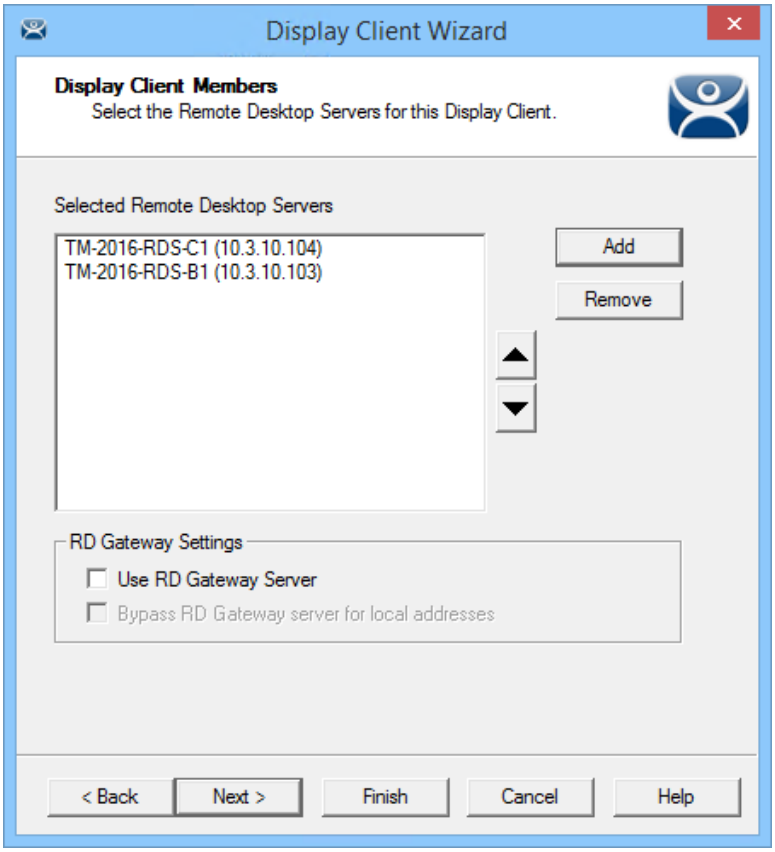
Move the Remote Desktop Servers you want to use from the ***Available Remote Desktop Server*** list to the ***Selected Remote Desktop Server*** list by highlighting the desired server and using the Left or Right arrow.

Note: If your defined Remote Desktop Servers do not show in the list then you probably selected ***SmartSession*** on the previous page without checking the ***"Available for Display Clients using SmartSession"*** on the **Remote Desktop Server Capability** page of the Remote Desktop Server Wizard.

You can click the ***Edit Server List*** button to open the **Remote Desktop Server List Wizard** to open each Remote Desktop Server wizard to check the needed checkbox.

Adding two Remote Desktop Servers to the ***Selected Remote Desktop Server*** list will provide failover. In normal failover the Terminal will connect to the first Remote Desktop Server. If it fails it will connect to the second.

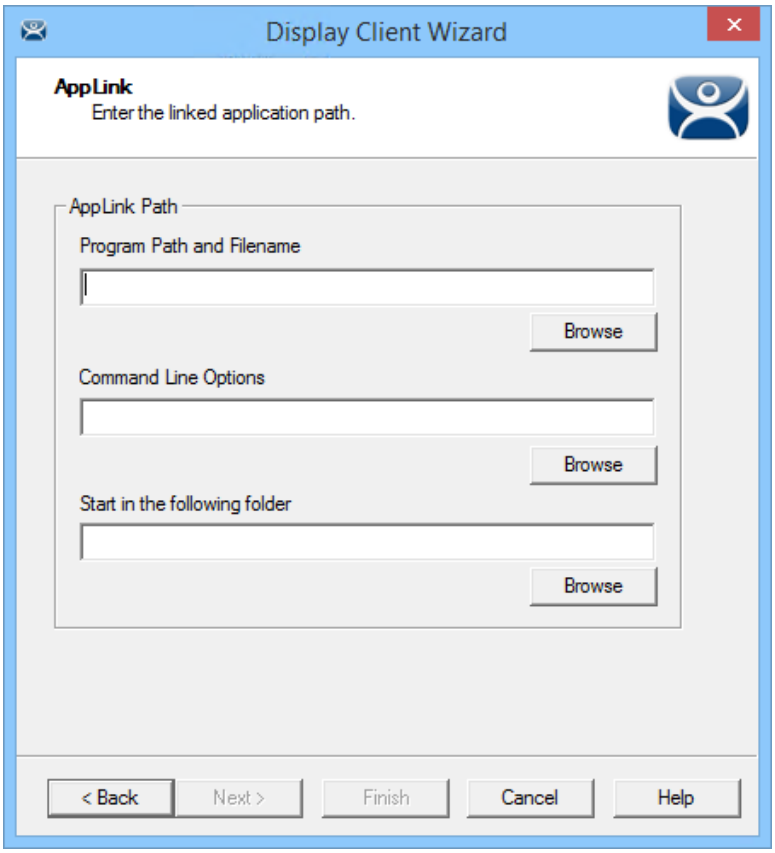
SmartSession load balancing does not follow the list order but instead goes to the Remote Desktop Server with the lightest load.



Display Client Members Page of the Display Client Wizard

If Remote Desktop Server Groups are used to speed the selection of Remote Desktop Servers then the Display Client Members page will show a single window instead of a pair of columns.

Use the Add button to launch the window that lets you select the Remote Desktop Servers or Remote Desktop Server group.

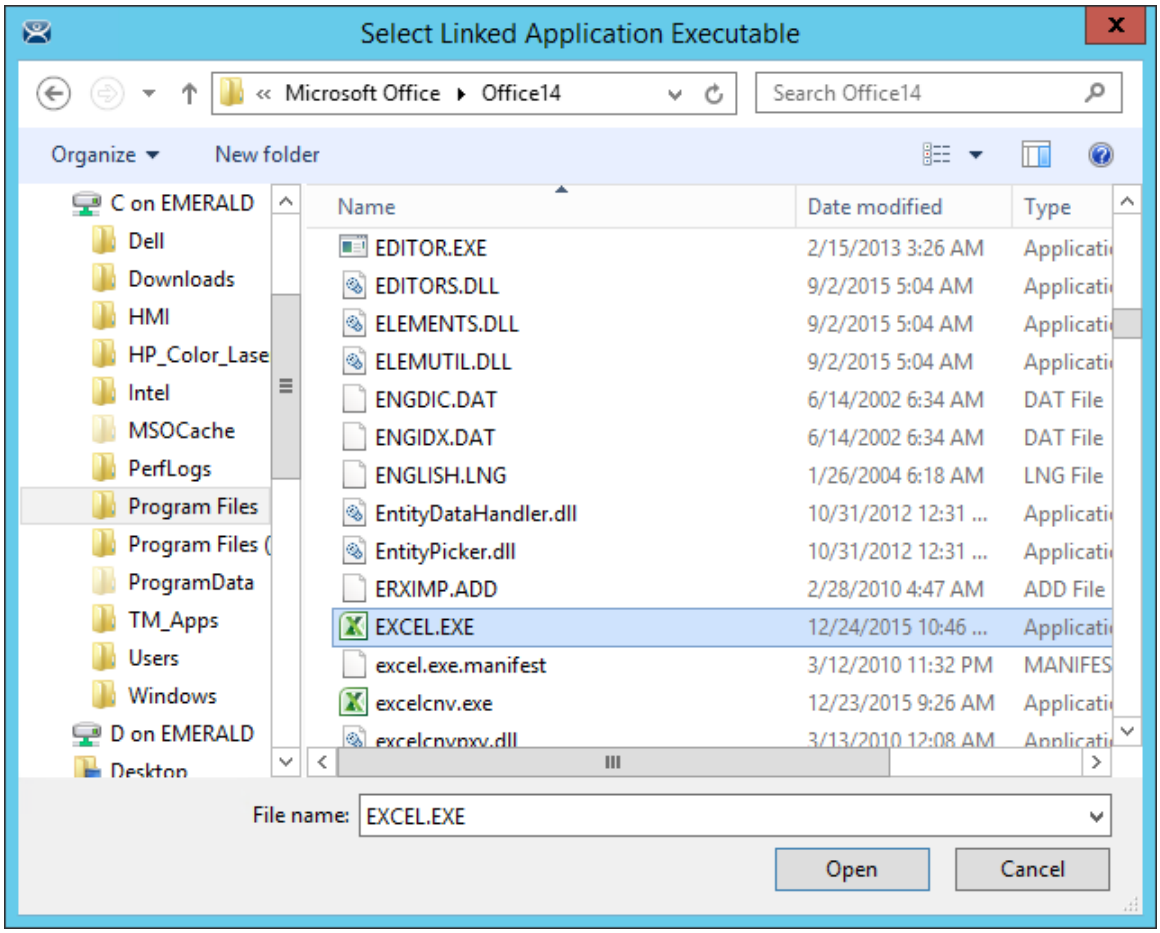


AppLink Page of the Display Client Wizard

The **AppLink Page** of the Display Client wizard has a field for the path to the executable to launch the desired application.

- ✓ **Enter the path to the application in the "*Program Path and Filename*" field.**

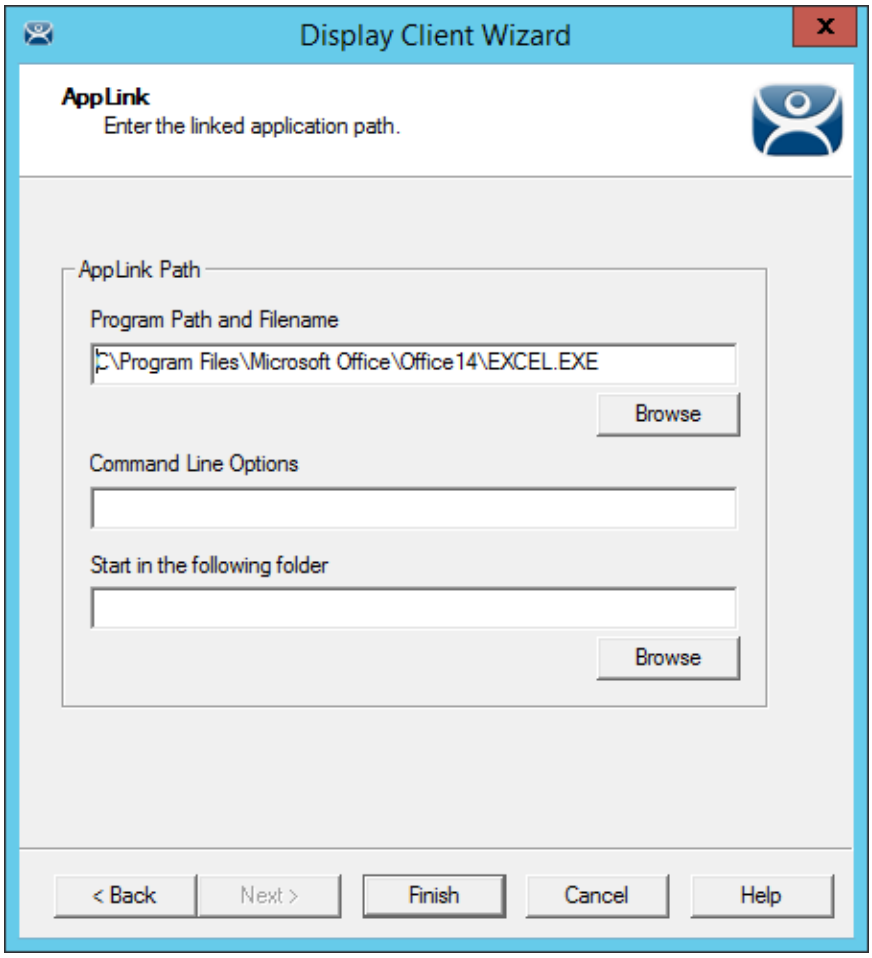
There is a ***Browse*** button that launches a file browser to allow you to select the executable file.



File Browser

Select the ***Browse*** button to open the file browser. Navigate to the executable file, highlight it, and select the ***Open*** button.

This will populate the ***Program Path and Filename*** field.



*Filled **Program Path and Filename** Field*

Select the ***Finish*** button to complete the wizard and save the configuration.

There are a few factors to consider when entering the application in the ***Program Path and Filename*** field:

- The file browser is on the **ThinManager Server** and not the Remote Desktop Server unless you installed ThinManager on your Remote Desktop Server.
- The path to the application needs to be the same on each Remote Desktop Server.
- If the file is different on different servers you may need to use a batch file to launch the application using different paths.

A batch file is created and put in the same location on each Remote Desktop Server.

The batch file can be as simple as 3 lines:

```
CD "C:\Program Files\Microsoft Office\Office14"

Start EXCEL.EXE

CD \
```

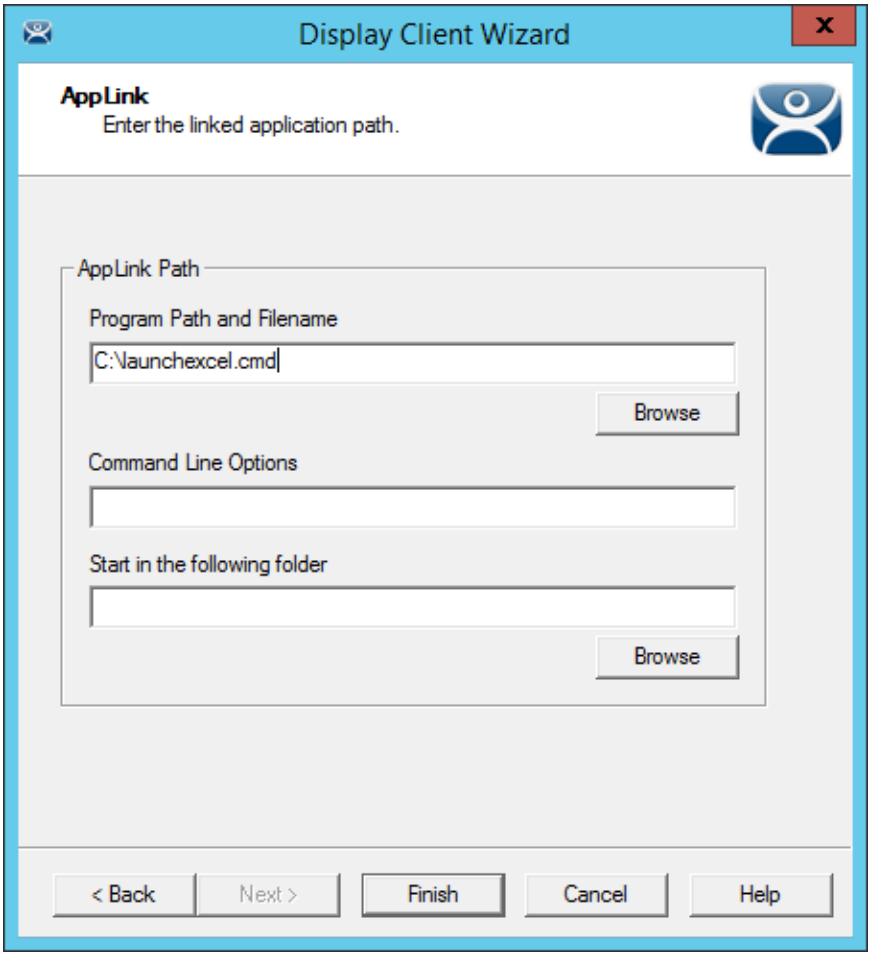
The batch file may need different paths on different servers. The first line is changed to reflect the location on that particular Remote Desktop Server.

```
CD "C:\Program Files (x86)\Microsoft Office\Office14"

Start EXCEL.EXE

CD \
```

This first line uses the **Program Files (x86)** instead of **Program Files** to reflect the location on that particular Remote Desktop Server.

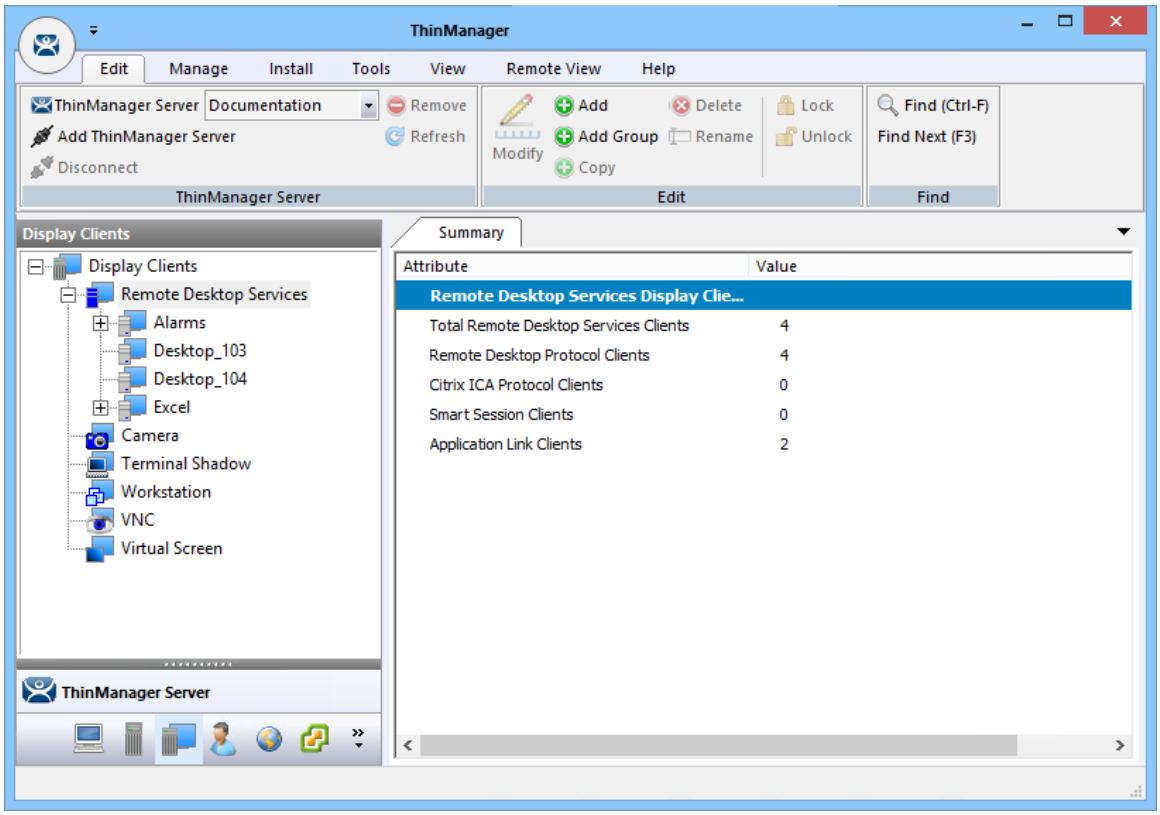
When a Terminal connects to a Remote Desktop Server it will be directed to the batch file.

The batch file will direct the Terminal to the right location.



Batch File as the Program Path

The batch file needs to be in a consistent location when using multiple Remote Desktop Servers.

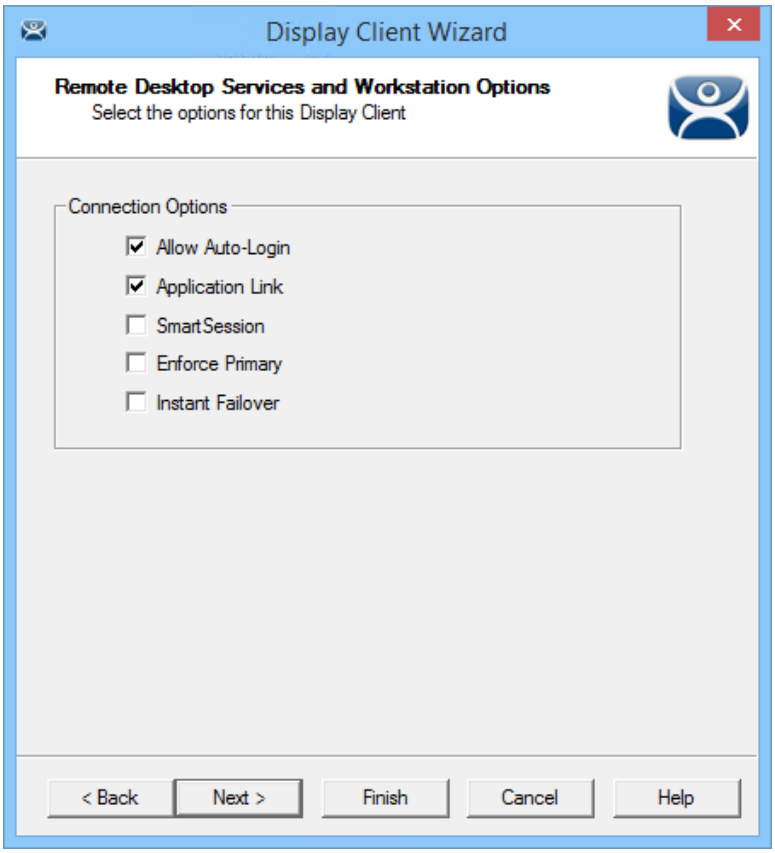


Created Display Clients in ThinManager Tree

Once you have created a display client it will show in the Display Client branch of the ThinManager tree.

13.3. Deployment Options

Remote Desktop Services Display Clients have a variety of deployment options. These are controlled on the **Remote Desktop Services and Workstation Option** page of the **Display Client Wizard**.



Remote Desktop Services and Workstation Option page of the Display Client Wizard

Which checkbox you select changes the way applications are deployed.

13.4. Allow Auto-Login

Allow Auto-Login – This automatically logs into the session if a user account is applied to the Terminal.

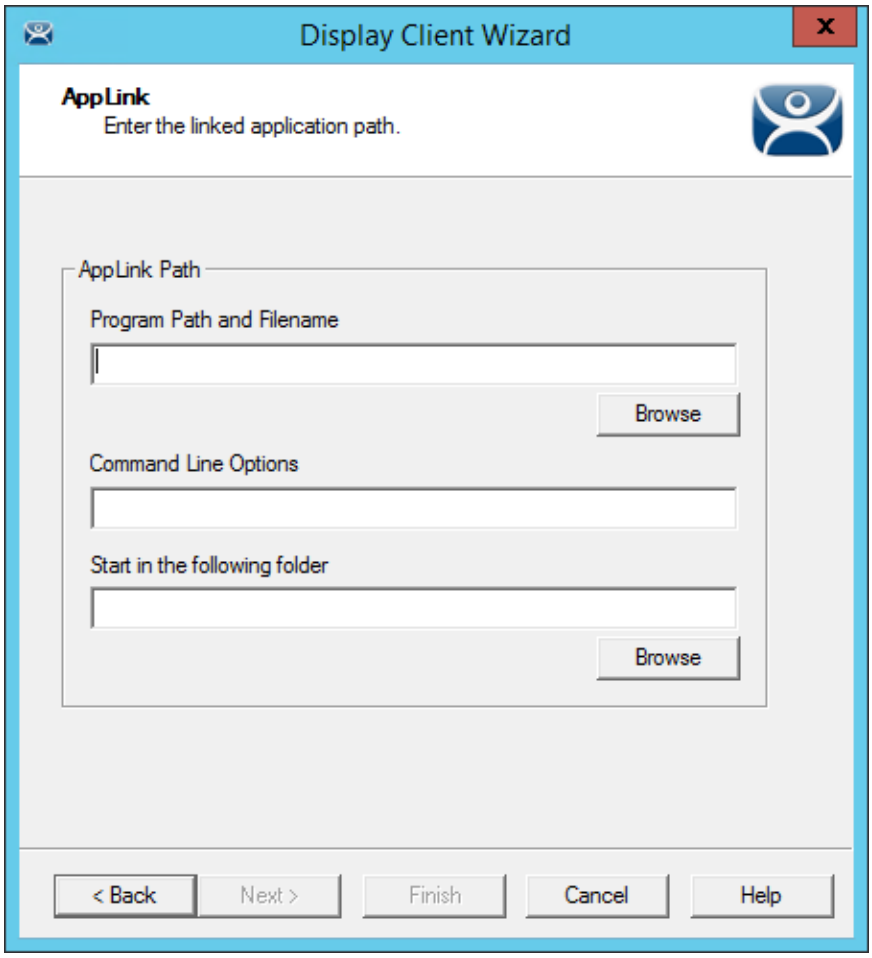
- ✓ **Check the "Allow Auto-Login" checkbox to allow the session to start without needing user interaction if a user account is assigned to the Terminal.**

Using Auto-Login is the default setting. It is important for instant failover so that the backup session is immediately displayed without user intervention.

Unchecking this shows the login window and forces a manual login. This is useful to provide a user with a login based on their group policy, like when desktops are deployed.

13.5. Application Link

Application Link – AppLink launches a single application instead of a desktop. This allows you to control a user's access. If the Display Client uses AppLink the user will not get a desktop or icons but will be limited to the application specified. Closing it will re-launch the program, assuring that it is always running. This allows the administrator to control content to the user in a simple manner without needing to use group policies.



AppLink Page of the Display Client Wizard

The AppLink Page has three fields.

- **Program Path and Filename** - Enter the path to the desired application in the field.

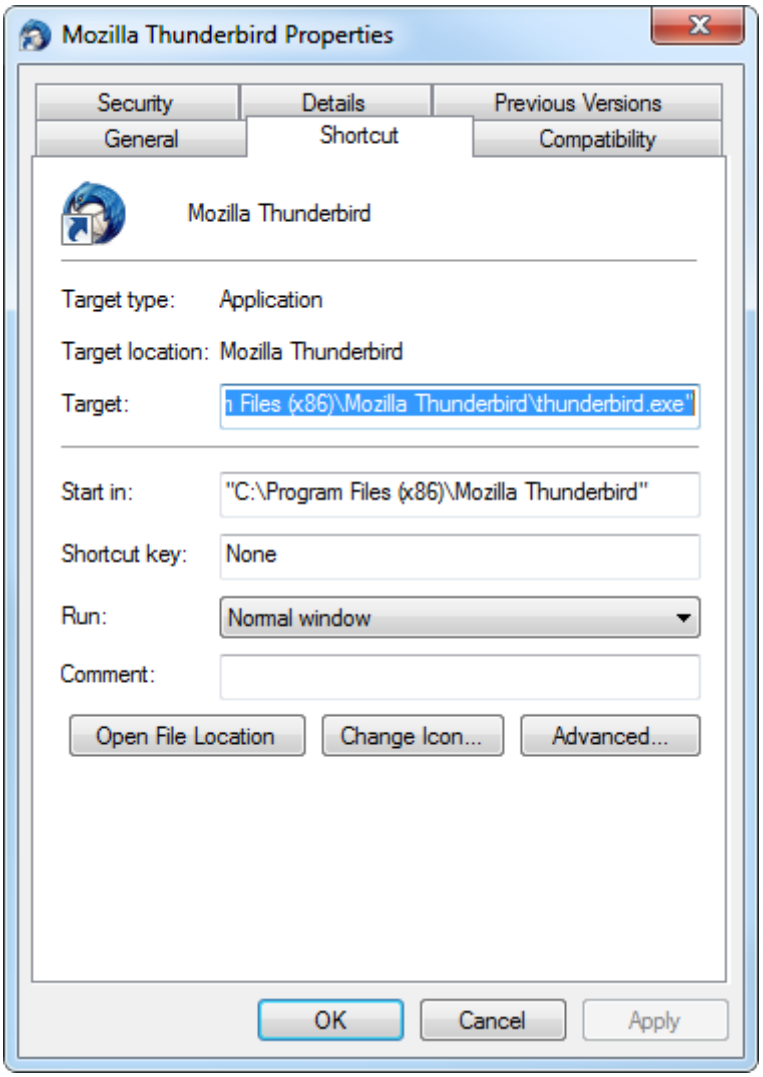
Note: Quotation marks may be needed when there is a space in the path.

- **Command Line Options** – This field provides a space for command line options and switches. This field may not be required.
- **Start in the following folder** - This field is provided in case you need to specify the working directory for the program when using a relative path for the initial program. This field may not be required.

It has one button:

- **Browse** – The Browse button will allow you to select the executable file using a file browser. Make sure the path is correct on all Remote Desktop Servers.

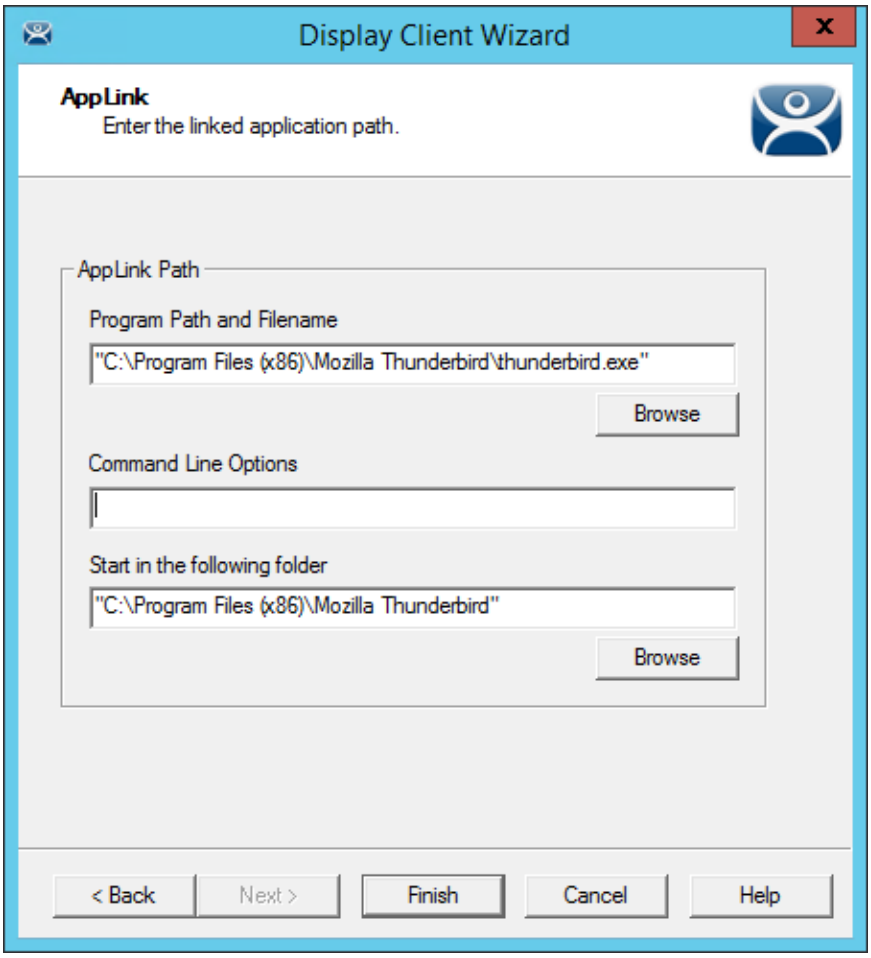
Note: If a Remote Desktop Services Display Client contains several Remote Desktop Servers, the path must be valid on all Remote Desktop Servers. If different Remote Desktop Servers have different paths to the desired program, write a batch file to open the program.



Command Prompt Shortcut Properties

The **AppLink** fields can be explained by looking at the properties of a shortcut.

The Command Prompt shortcut property has a ***Target*** field and a ***Start In*** field. The ***Target*** is the path to the executable. The ***Start In*** field is the home directory for the application.



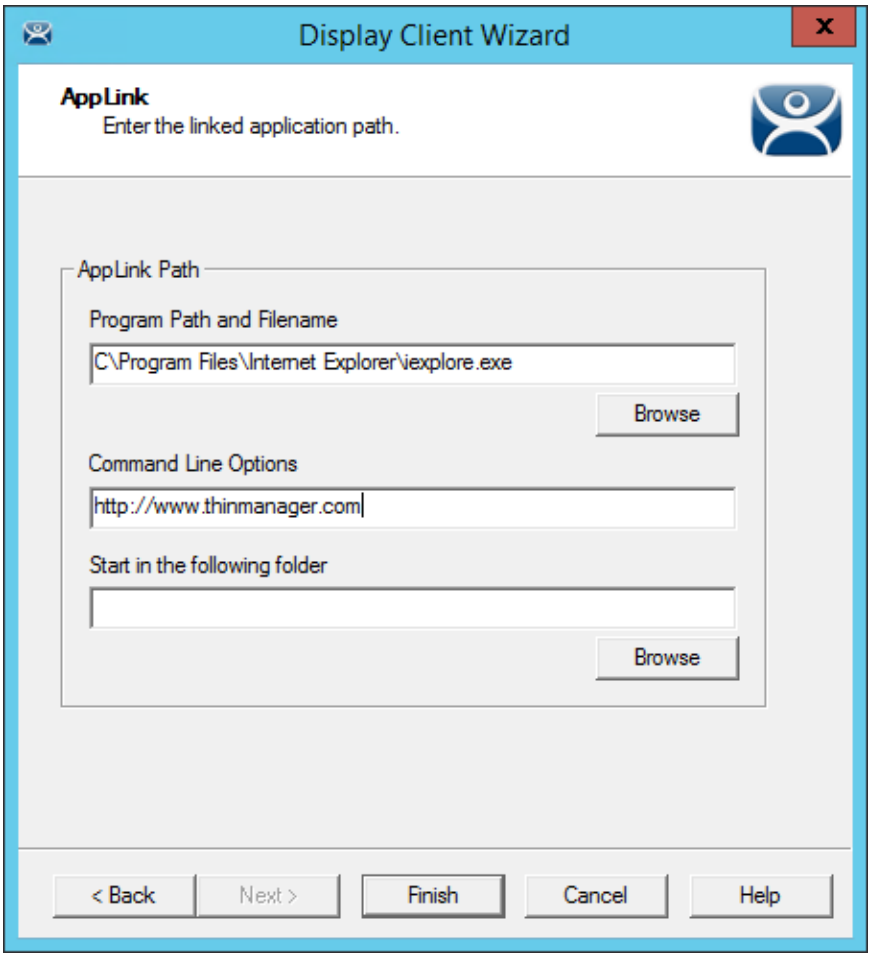
AppLink Paths

This shows how the path data from the shortcut is used in AppLink.

The ***Target*** field is equivalent to the ***Program File and Filename*** field.

The ***Start In*** field is equivalent to the ***Start in the following folder*** field.

Note: The ***Start in the following folder*** is usually not needed.

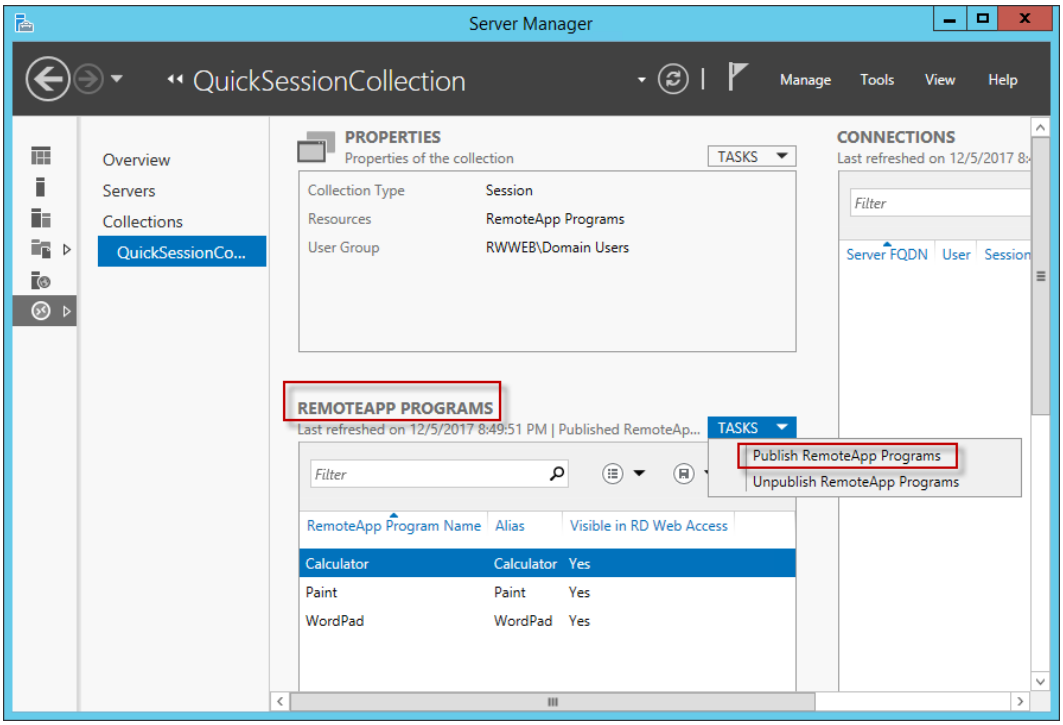


Web Site Deployment

A browser can launch by including the URL of the desired site in the ***Command Line Options*** field.

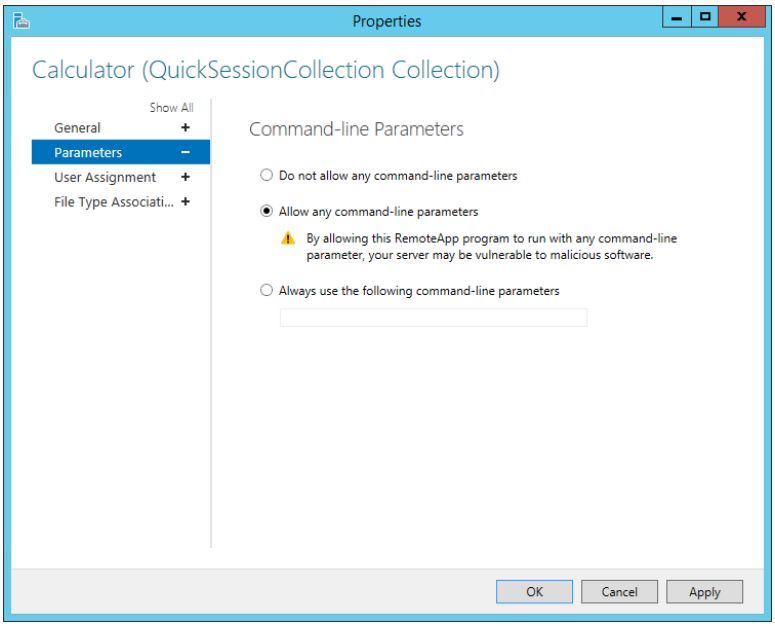
Note: Windows Server 2008, 2012, and 2016 need the AppLink path to be white listed in *the* ***Server Manager > Collections > RemoteApp Programs*** of the Remote Desktop Server.

Alternately the group policy can be configured to allow any initial program. Open the Group Policy, navigate to ***Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Connections*** and set the **Restrict Remote Desktop Services user to a single Remote Desktop Services session** parameter to ***Enabled***



RemoteApp Programs White List

The application is white listed by using the ***Publish RemoteApp Programs*** task.



Allow Any Command-Line Parameters Setting

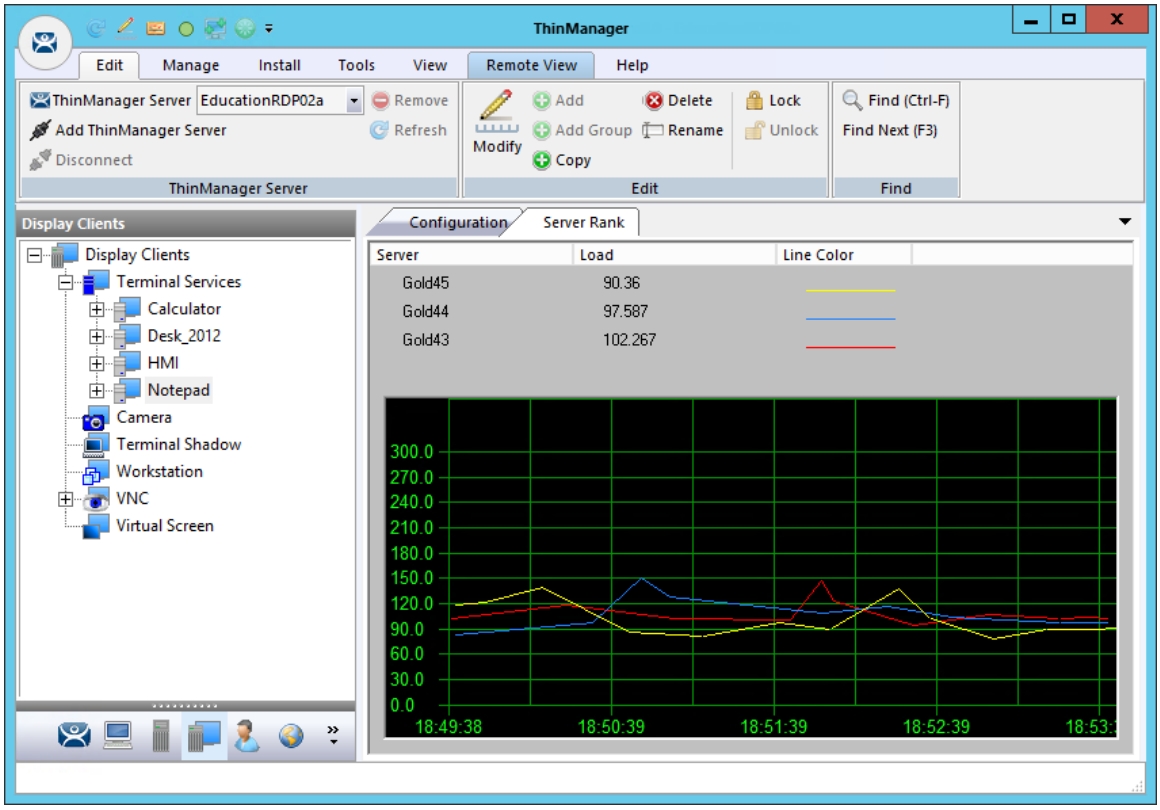
Once the application is published the properties need opened by right clicking the application in the white list.

Set the Command-line Parameters to ***Allow any command-line parameters***. This lets you pass specific files or URLs to the display client.

13.6. SmartSession

SmartSession – This adds SmartSession to the display client which provides load balancing between member Remote Desktop Servers.

SmartSession uses CPU availability, memory, and the number of sessions on the member Remote Desktop Servers to determine the load on the servers. Thin clients connect to the Remote Desktop Server with the most available resources.



SmartSession Load Balancing Graph

The formula that ThinManager uses to calculate SmartSession load balancing is

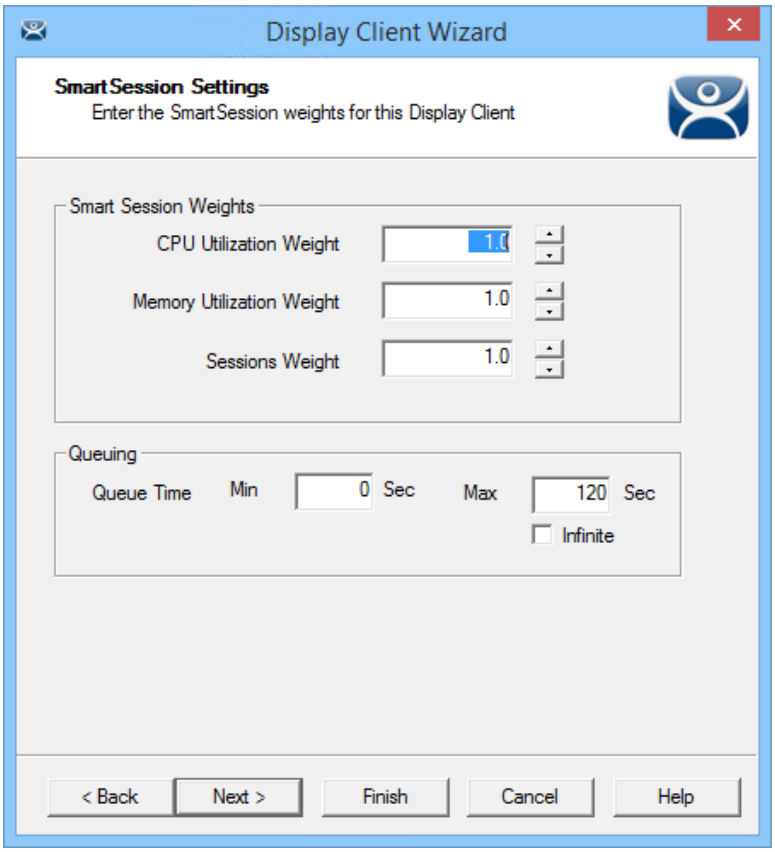
SmartSession Load = (CPUwt X CPU%) + (RAMwt X RAM%) + (SessionWt X Session%)

The load = (CPU weight x the CPU Use %) + (Memory weight x Memory Use %) + (Session weight x Session Number %)

The Weight is configurable in the Display Client Wizard. The % range is configurable in the Remote Desktop Server Wizard.

13.6.1. Weight in SmartSession

If you are concerned with one of the SmartSession measurements, either processor, memory, or sessions, you can increase the weight of that component to make its measurement a bigger factor. This is done on the ***SmartSession Setting*** page of the Display Client Wizard.



SmartSession Settings Page of the Display Client Wizard

Once you have selected the SmartSession checkbox on the Remote Desktop Services and Workstation Options page of the Display Client wizard a SmartSession Settings page will be added before the AppLink page. This allows you to change the weight of each SmartSession load balancing component.

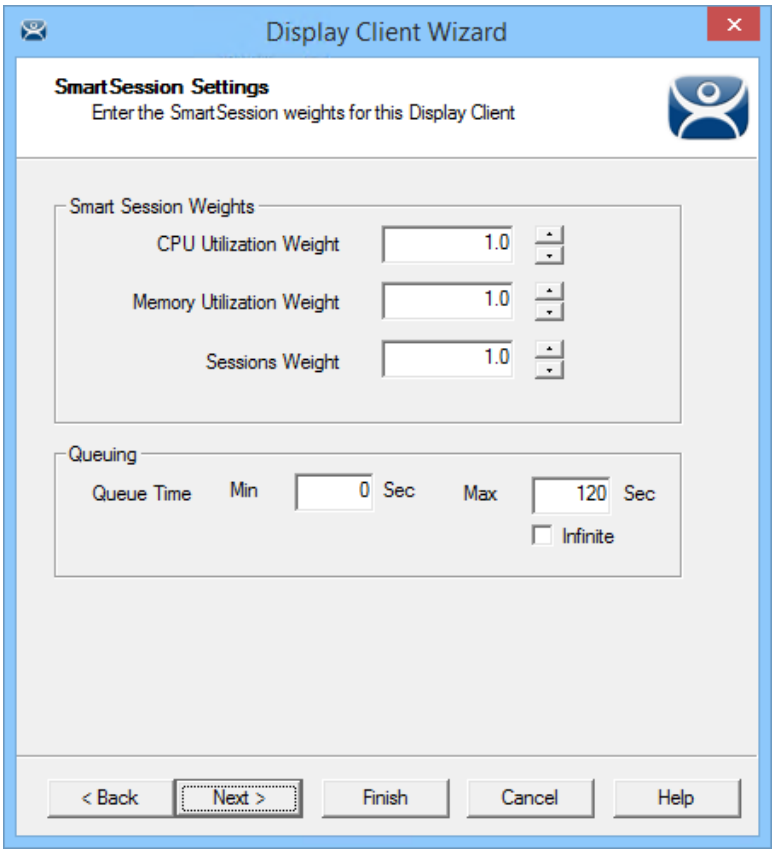
Changing the weight of one of the components will increase its value and make it more sensitive to overload of that resource.

If, for example, you are concerned with the CPU being taxed on the servers you can increase the CPU Utilization Weight to make that value increase the SmartSession load number more.

13.6.2. SmartSession Ranges

Normally ThinManager uses the full range of CPU and RAM to determine the SmartSession load. You can adjust that in the Remote Desktop Server Wizard.

Open the Remote Desktop Server Wizard by double clicking on the desired server on the Remote Desktop Servers branch of the Display Server tree. Navigate to the SmartSession Configuration page.



SmartSession Configuration Page of the Remote Desktop Server Wizard

Each resource that ThinManager measure for SmartSession load balancing has an adjustable range. The ***CPU Utilization*** and the ***Memory Utilization*** uses 0% to 100% as its scale. The ***Sessions*** resource is based on 50 sessions, where 0 sessions is 0%, 25 session sis 50%, and 50 sessions is 100% used.

If you are concerned about using all your resources on a server you can lower the ***Maximum*** setting. Changing the ***Sessions*** maximum to 25 would mean that 25 sessions is 100% utilized and ThinManager will consider the server less available. Likewise, changing the ***CPU Utilization*** maximum to 75% will tell ThinManager that the server is loaded at 75% CPU utilization, leaving some spare CPU available.

These numbers can be left at the default settings, or can be tweaked through trial and error to determine the best performance.

- ✓ **The settings can be left at the defaults unless you notice a performance problem that changing the Weights or Ranges may correct.**

Note: Values are not prevented from exceeding the maximum or minimum. The values represent the levels that 'No Utilization' or 'Full Utilization' is reached.

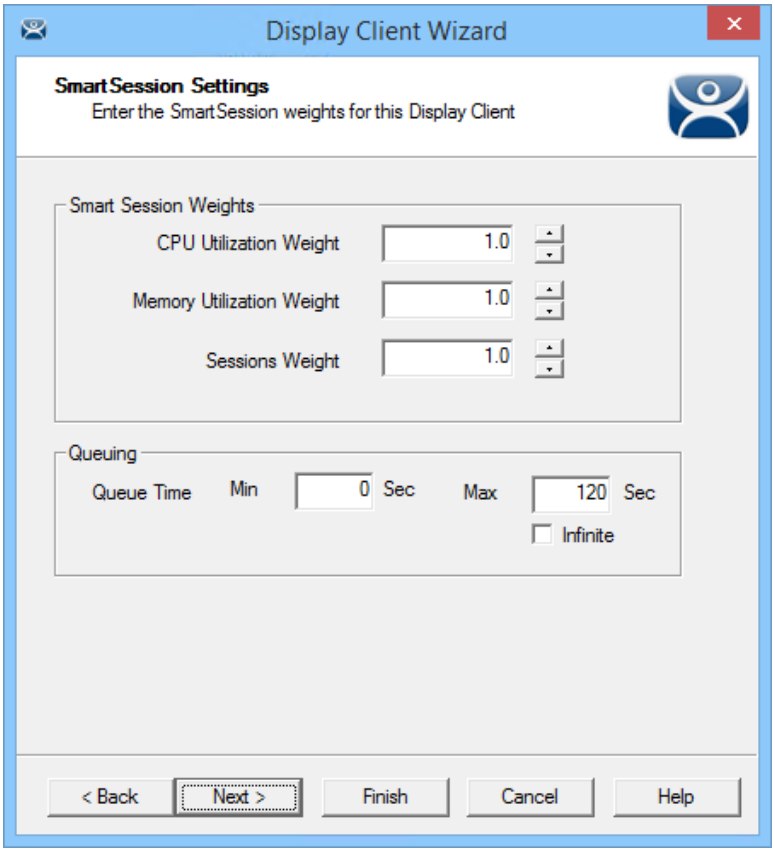
13.6.3. Queuing

Another SmartSession feature is Queuing. This was developed to smooth the transition from one server to another during failover.

A starting session usually takes more resources to initialize than it takes to run. If a server fails and all or its Terminals switch to a backup the many starting sessions may overload and tax the new server. This is especially true with HMIs, SCADAs, and other resource demanding applications.

When a Terminal first starts an application that uses SmartSession ThinManager will check the resources of the member servers and ThinManager will send the Terminal to the server with the lightest load, the one with the most available resources.

Queuing acts like an intelligent bottleneck. When ThinManager sees that if all the servers have maxed out their resources then ThinManager will wait until the loads drop and resources become available before giving the server assignments to the Terminals. Without Queuing the Terminals would switch immediately, taxing the system and greatly slowing performance until all the sessions initialized and reached stable load levels.



SmartSession Settings Page of the Display Client Wizard

The Queuing function is automatically applied to SmartSession Display Clients. The default settings will give a minimum wait of 0 seconds and will let Terminals connect after 120 seconds, even if the load has not lowered.

- ✓ **If the server bogs down with the default settings then try a longer interval.**

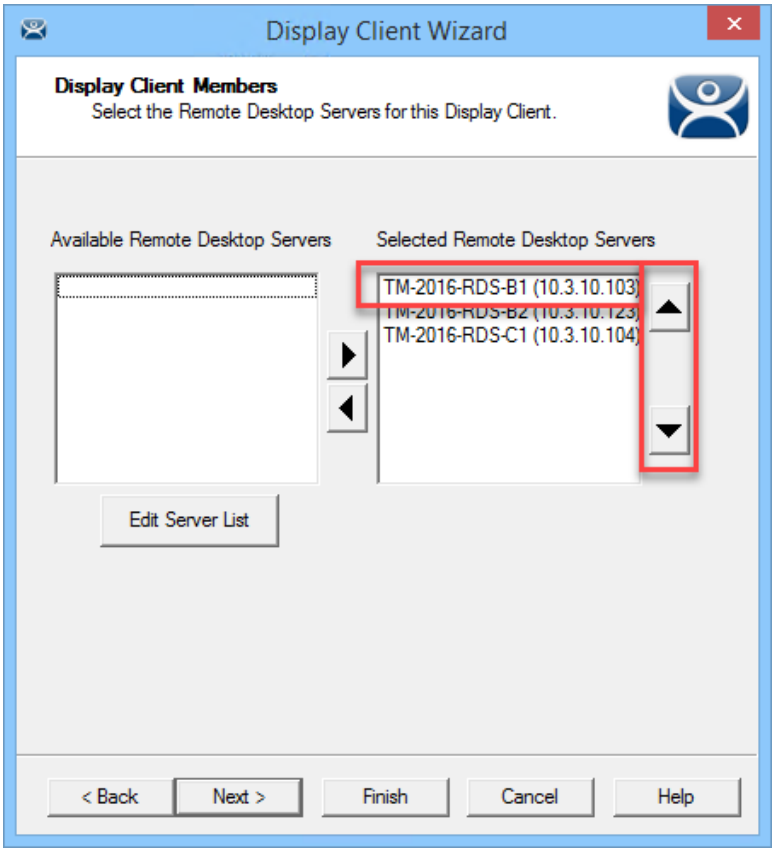
Checking the ***Infinite*** checkbox will keep the Terminal waiting until the load lowers to an acceptable level. However, this may not be a good idea because if the server has problems, like a memory leak, then the resources may never lower enough to allow the Terminals to connect. It would be better to move the ***Max*** field to a higher interval.

- ✓ **SmartSession load balancing and Queuing can be applied to a display client with a single member Remote Desktop Server.**

This allows the single server to have the Terminals connect in an orderly fashion spreading the demand for startup resources instead of all connecting at the same time and overloading the server.

13.7. Enforce Primary

ThinManager uses a list of assigned Remote Desktop Servers that the Terminal can connect to. The top Remote Desktop Server is considered the primary Remote Desktop Server.



Primary Remote Desktop Server

The thin client will connect to the Remote Desktop Servers in order. If the Terminal fails to connect to the first one it will try the second, then third, until it finds a listed server that allows a connection.

With Enforce Primary the top Remote Desktop Server in the list is considered the Primary Remote Desktop Server and the Terminal will always try to connect to this server. If the Terminal is running on the primary server and the server fails then the Terminal will switch to a backup. However, the Terminal will monitor the primary Remote Desktop Server. If the primary Remote Desktop Server becomes available then the Terminal will switch back to its assigned Primary Remote Desktop Server.

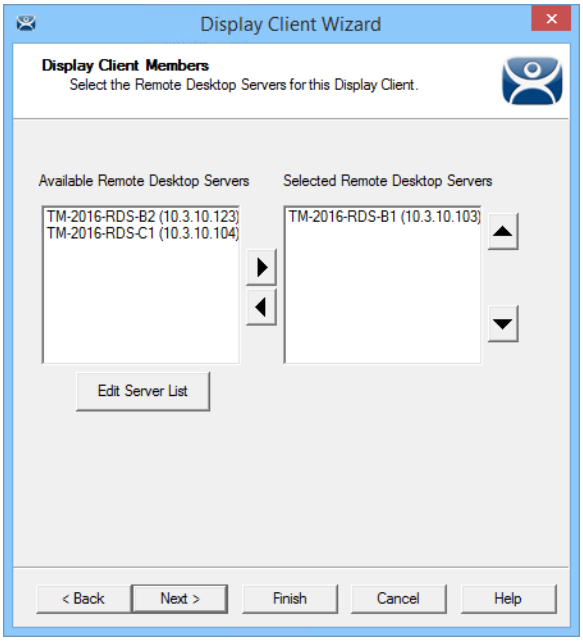
13.8. Failover

ThinManager has a failover feature where you can assign two or more Remote Desktop Servers to a Terminal. If the first server fails the Terminal will detect it and switch to the backup server. This prevents downtime and loss of productivity.

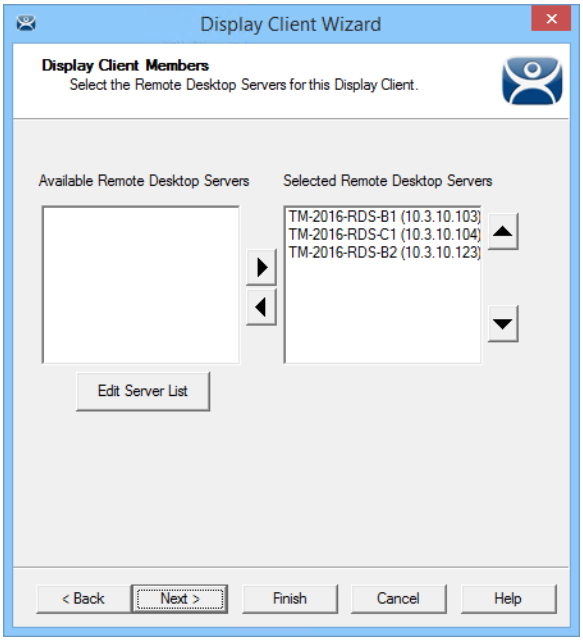
- ✓ **It is a best practice to use Failover in every ThinManager system.**

Failover requires:

- Two or more servers
- The same applications installed with the same path
- The same Windows accounts on each server



Display Client Without Failover



Display Client With Failover

Configuring Failover is a simple as defining multiple Remote Desktop Servers using the **Remote Desktop Server Wizard** and adding two or more servers in the ***Selected Remote Desktop Server*** list on the **Display Client Member** page of the **Display Client Wizard**.

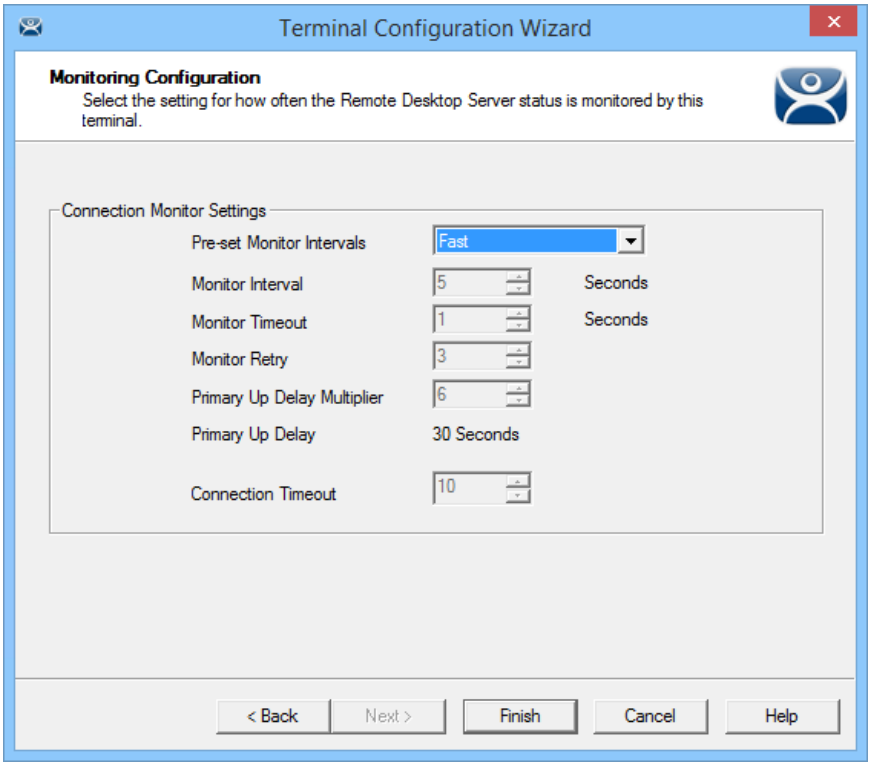
Terminal Connected to First Remote Desktop Server

The Terminal connects to the first Remote Desktop Server in the Selected Remote Desktop Server list.

Terminal Connected to Second Remote Desktop Server

If the first Remote Desktop Server fails the Terminal will detect it, disconnect, and try the next server in the list. It will launch the same display client with the same credentials.

The speed in which server failure is detected can be modified on the **Monitoring Configuration** page of the **Terminal Configuration Wizard**.



Monitoring Connection Page of Terminal Configuration Wizard

When a ThinManager Ready thin client or ThinManager Compatible thin client connects to a Remote Desktop Server and starts a session it forms a secure socket connection with a heartbeat. It the connection is lost the Terminal will try to reconnect. If it fails it will connect to the next Remote Desktop Server in the list.

- The ***Monitor Interval*** is how many seconds the Terminal will wait before attempting to reconnect.
- The ***Monitor Retry*** is the number of times the Terminal will try to reconnect before switching,

- The ***Monitor Timeout*** is the interval between reconnection attempts.

Using the ***Fast*** setting a Terminal will wait five seconds, try, wait a second, try a second time, wait a second, try a third time, then switch to the other server. This takes 10 to 20 seconds in a real world scenario.

There are other settings, including a custom setting but the slower settings are usually not needed with today's fast networks.

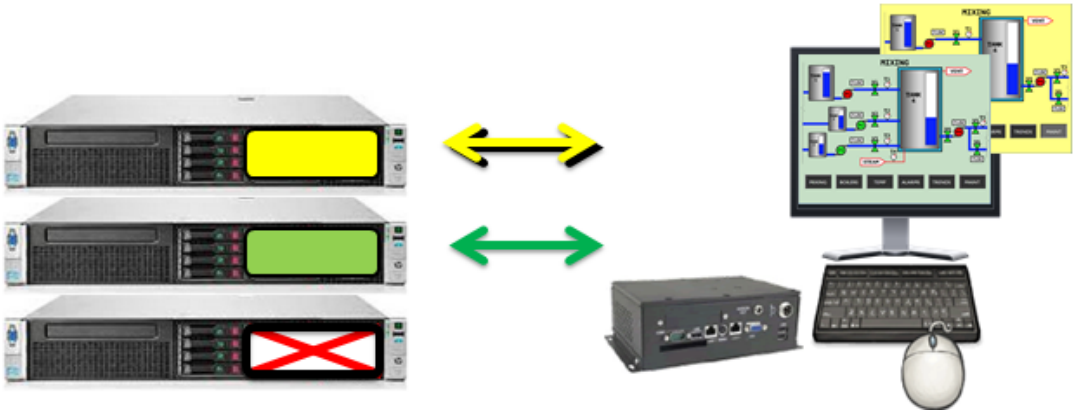
The Terminal can switch to a backup in 10 to 20 seconds but the applications need to load. If you don't want to wait for the application to load you can use Instant Failover.

13.9. Instant Failover

A Display Client configured with the Instant Failover checkbox will send the Terminal to connect to two Remote Desktop Servers at startup, giving it two active sessions.

Instant Failover with Two Active Sessions

If the first Remote Desktop Server fails, the session of the second Remote Desktop Server session is immediately displayed, eliminating any downtime due to Remote Desktop Server failure.



Terminal with Instant Failover and Backup Sessions

An Instant Failover display client will want to have two active sessions so if one Remote Desktop Server fails the display client will start a session on a third Remote Desktop Server if you have one in the server list.

Instant Failover requires:

- ❑ Two or more servers

- ❑ The same applications installed with the same path
- ❑ The same Windows accounts on each server
- ❑ The Display Client needs the ***Instant Failover*** checkbox checked on the Remote Desktop Services and Workstation Options

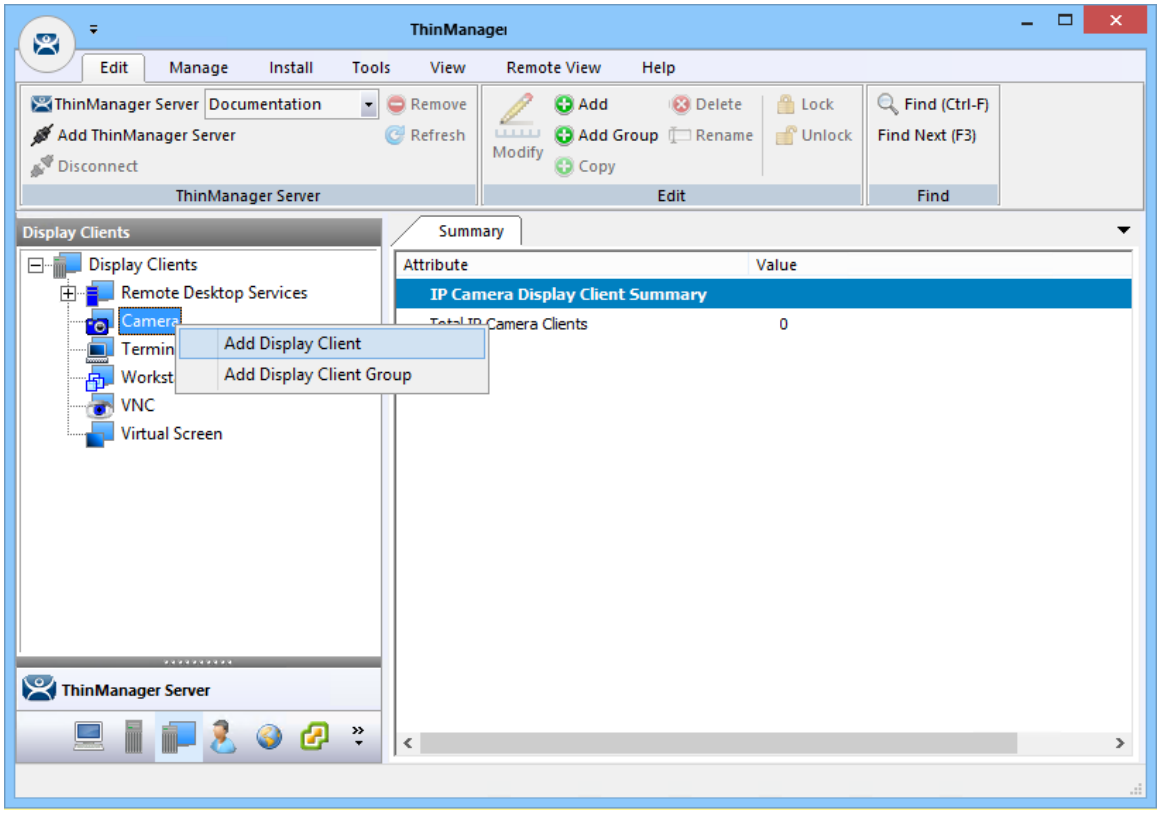
- ✓ **Use the Auto-Login function so switching is automatic and doesn't require a user to login to start the session**
- ✓ **Instant Failover is free from ThinManager but you will probably need a second license from your application vendor.**

14. Content – Camera Display Clients

IP camera video feed can be displayed on ThinManager Ready thin clients and ThinManager Compatible thin clients.

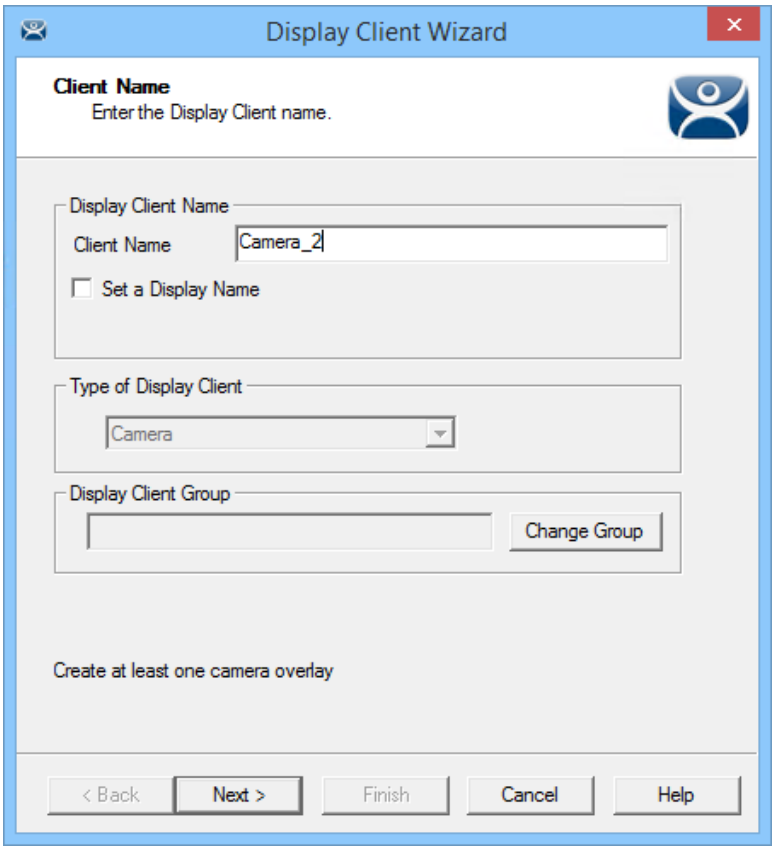
- ❑ Configure the camera device according to the camera vender guidelines and add to your network.
- ❑ Define the camera as a Camera Display Server.
- ❑ Create a Camera Display Client and add camera output as overlays.
  See Content – Camera Display Clients on page 138.
- ❑ Add the Camera Display Client to a Terminal.
  See Terminal Configuration Wizard in ThinManager on page 228.

Camera Display Client applications for the Terminal are defined using the **Display Client Configuration Wizard**



Add Camera Display Client

It is launched by selecting the **Display Client icon** at the bottom of the ThinManager tree, right clicking on the **Camera** branch, and selecting ***Add Display Client***.



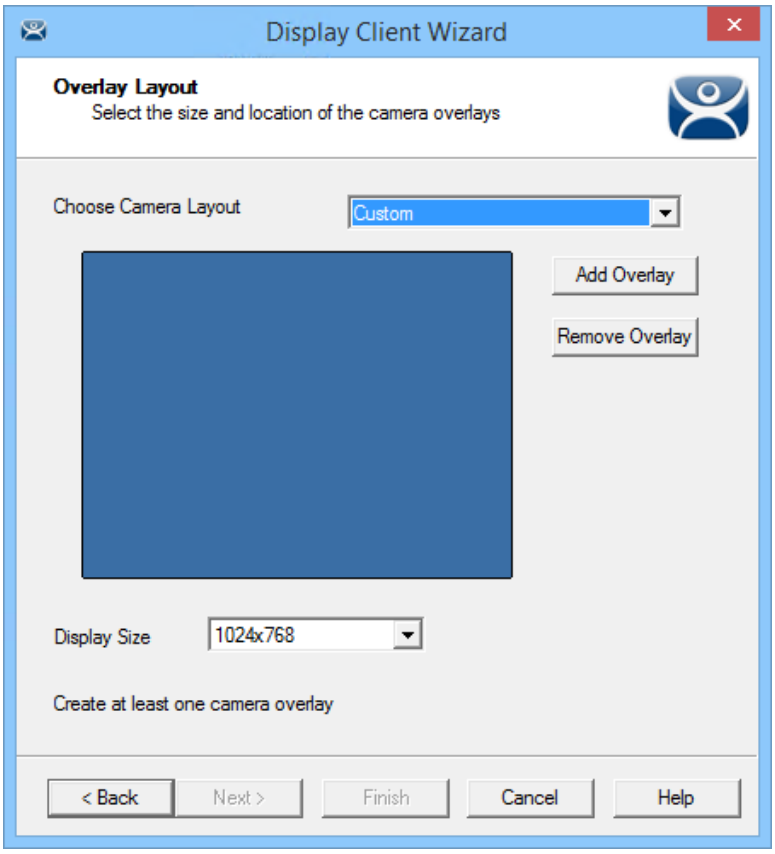
Camera Display Client Name Page of the Display Client Wizard

Name your display client by entering a name in the ***Client Name*** field.

The ***Set a Display Name*** checkbox allows you to assign a different name to be displayed in the ThinManager tree.

The ***Change Group*** button will launch a window that allows you to add this display client to a Display Client Group.

The wizard starts like the **Remote Desktop Services Display Client Wizard** but changes at the **Overlay Outline** page.

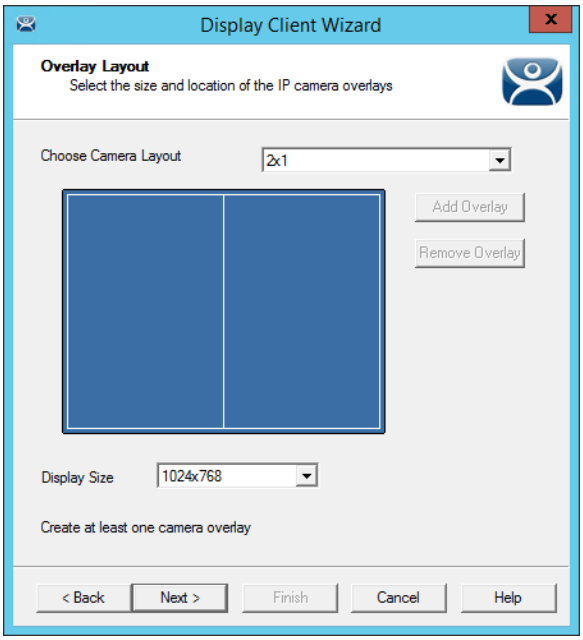


Overlay Layout Page of the Display Client Wizard

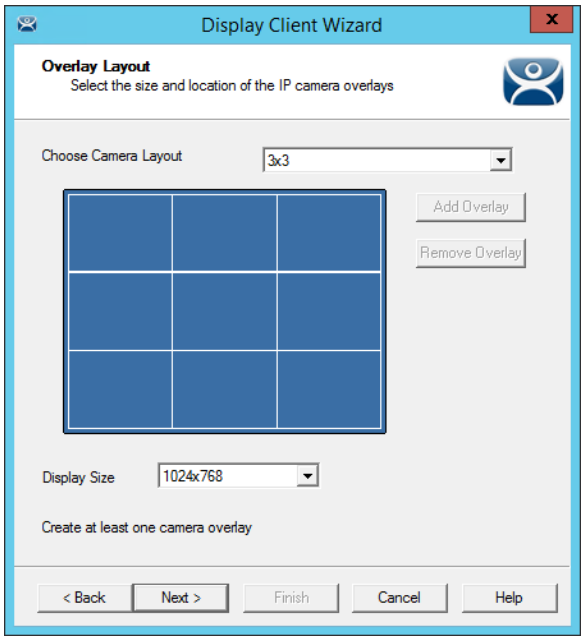
Camera feeds are laid out on the **Overlay Layout** page of the Display Client Wizard. You can either use a camera overlay template or lay out a custom overlay.

14.1. Camera Overlay Template

The wizard has a number of layouts pre-configured. Use the Choose Camera Layout drop-down to select from one to sixteen camera grids. These run from 1x1, through 2x2 and 3x3, to 4x4 cameras.

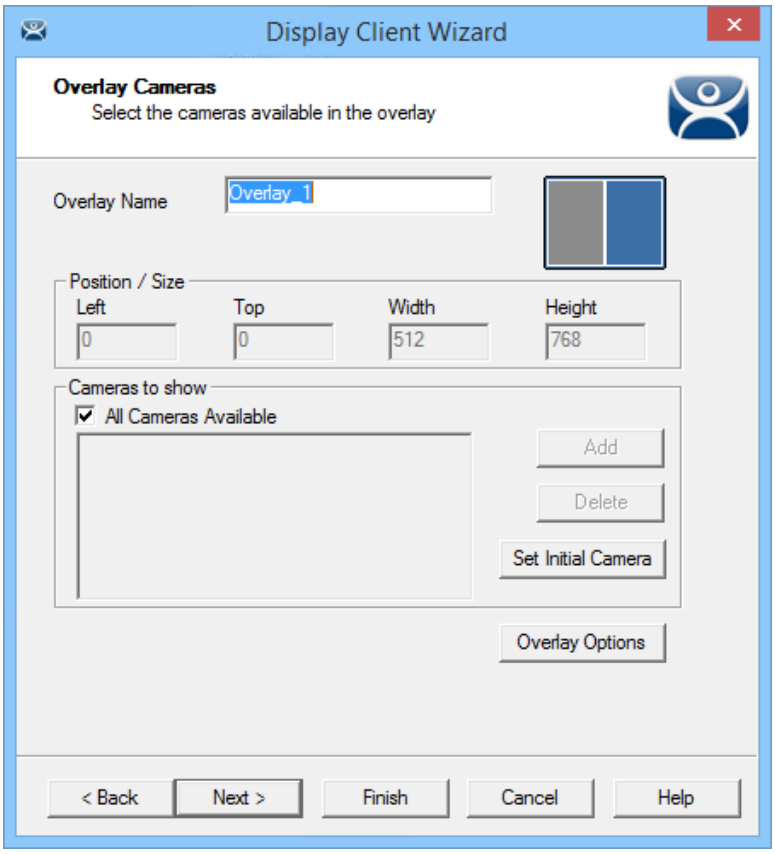


2x1 Grid Template



3x3 Grid Template

One you have selected a template the wizard lets you add a camera per grid.

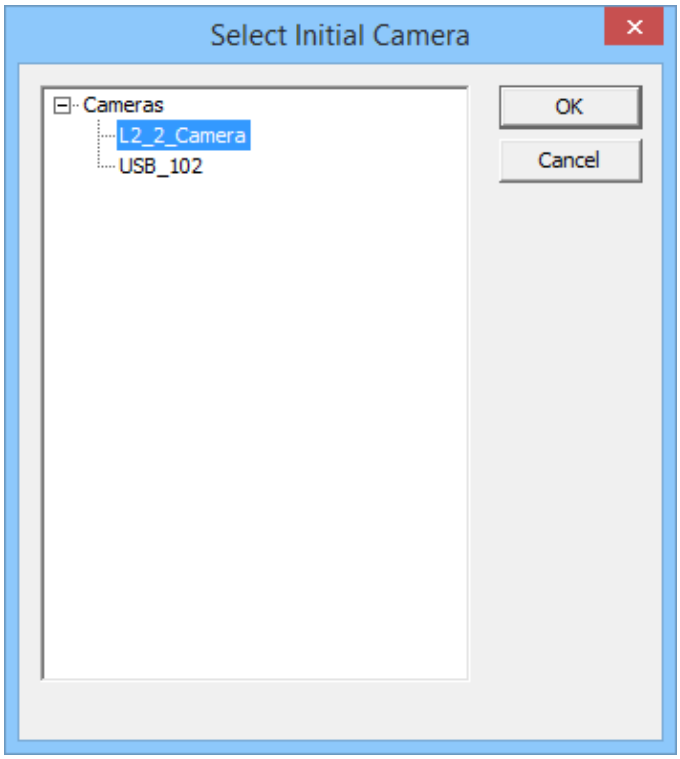


Overlay Cameras Page of the Camera Display Client Wizard

The wizard will show an **Overlay Camera** page for each overlay. The gray overlay is the one you are assigning cameras to.

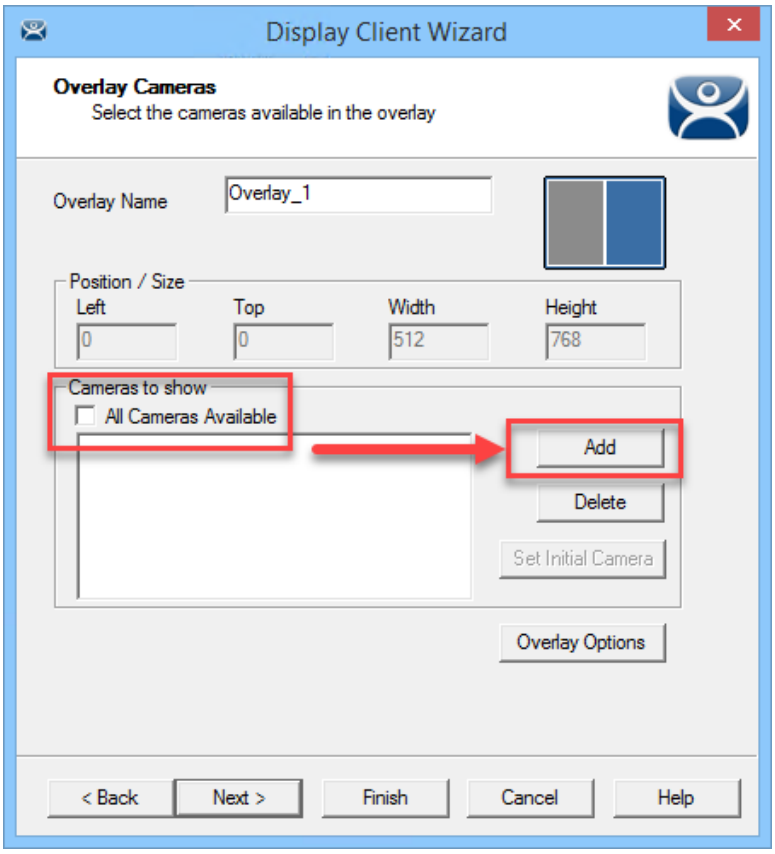
You can leave the default ***All Cameras Available*** checked and all of the cameras are available in that overlay.

The ***Set Initial Camera*** button opens a list of the cameras that lets you select which camera you want to be displayed first.



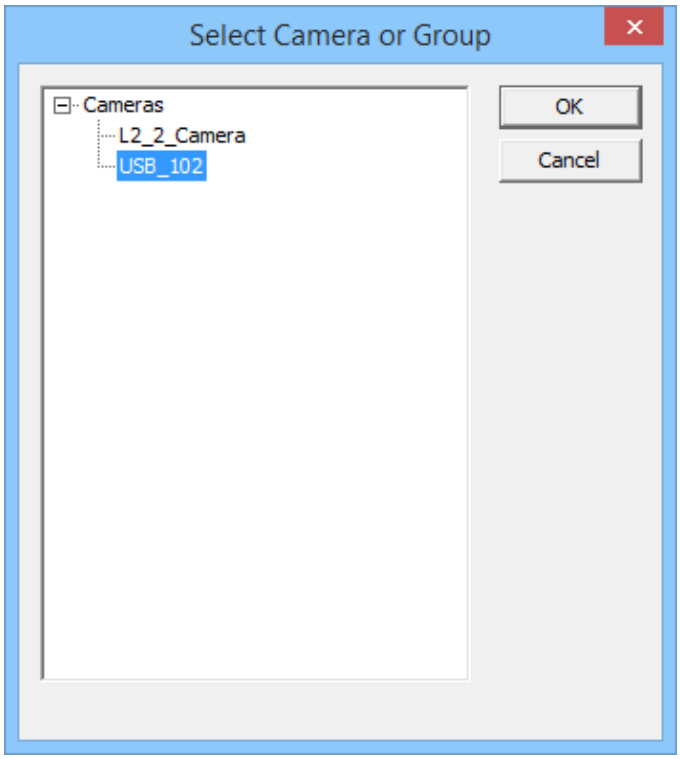
Select Initial Camera Window

The **Select Initial Camera** window shows the cameras in a tree. Select the one you want to be displayed first and select the ***OK*** button to close.



Overlay Cameras Page

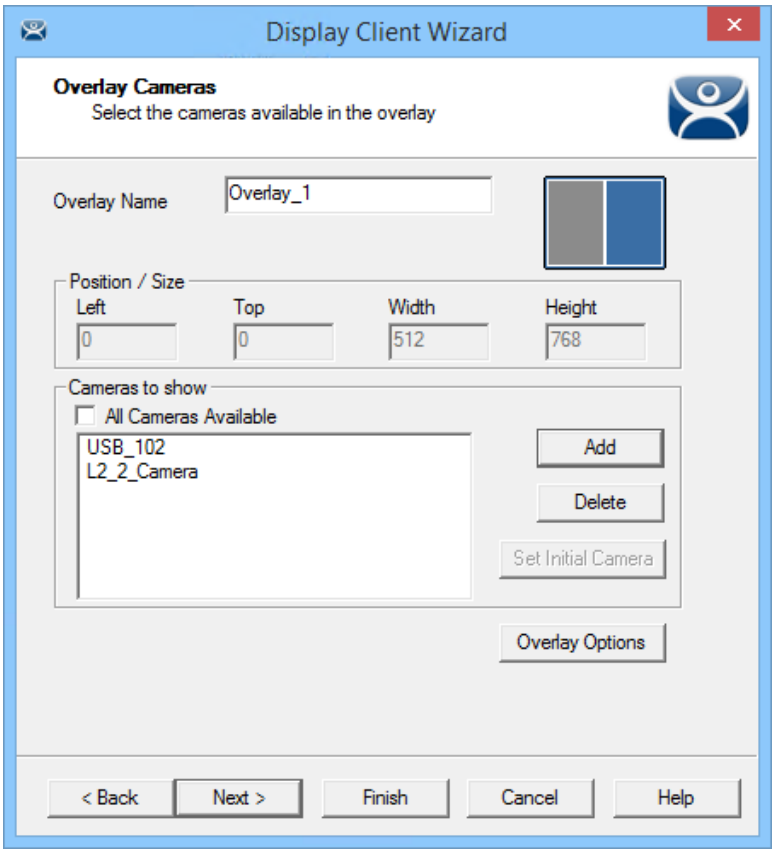
To limit the overlay to a smaller set of cameras you uncheck the ***All Cameras Available*** checkbox and use the ***Add*** button to select the desired camera or cameras.



Select Camera or Group Window

Clicking the ***Add*** button in the **Cameras to Show** frame will launch the **Select Camera or Group** window.

Select a camera and click the ***OK*** button. Repeat until all the desired cameras are selected.



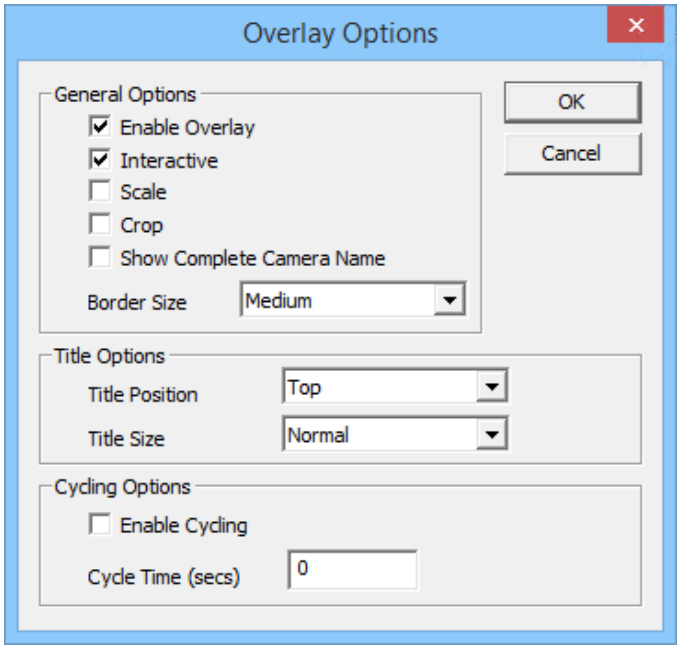
Selected List of Cameras

If you select multiple cameras the top listed camera will be the camera that is shown first.

Select the ***Finish*** button when you have selected cameras for each overlay.

14.1.1. Overlay Options

Once you add a camera or cameras to the overlay you can select the ***Overlay Options*** button to configure the overlay options.



Overlay Options

The **Overlay Options** page has setting to alter the camera display.

General Options:

- **Enable Overlay –** This option allows the overlay to be visible at startup. Unchecking this setting will start the display client with the camera in a disabled non-visible state. The TermMon ActiveX Control can be used by an application to enable the overlay.
- **Interactive –** This option allows the user on the Terminal to interact with the overlay. If the user clicks in the overlay area, he can perform functions such as switching cameras and making the overlay full screen.
- **Scale –** This option will scale camera frames to be to the size of the overlay window. Aspect ratio will be maintained.
- **Crop –** This option will crop the camera frame if it is larger than the camera overlay. This option when combined with the ***Scale*** option will always fill the entire overlay area.
- **Show Complete Camera Name –** Using this option allows the entire path of the camera to be displayed. The path includes any groups of which the camera is a member.
- **Border Size –** This setting determines the size of the overlay outside border.

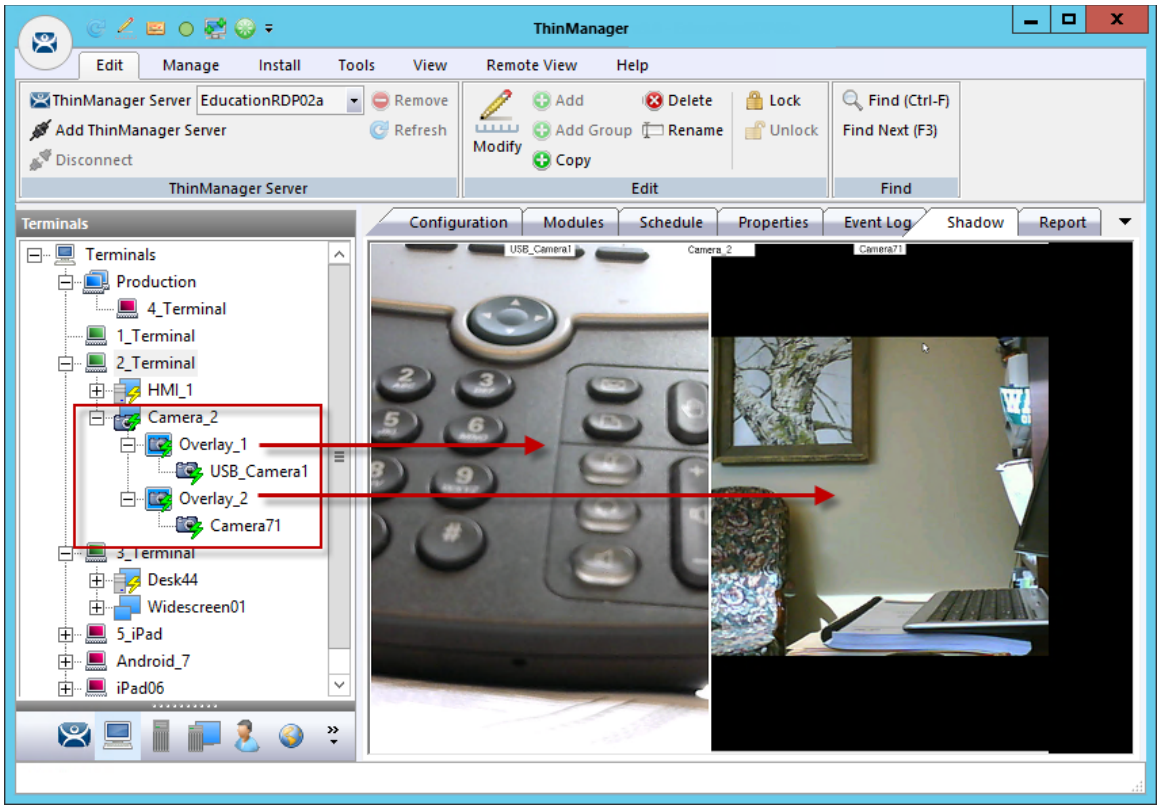
Title Options:

- **Title Position –** This is the position of the camera name within the overlay.
- **Title Size –** This is the size of the camera name when displayed within the overlay. Set this to *Don't' Show Title* if you do not want the camera name displayed.

Cycling Options:

- **Enable Cycling –** Check this setting to cycle between the cameras assigned to the overly.
- **Cycle Time –** This is the time in seconds that the overlay will display each camera before switching to the next camera.

Note: The ***Cycling Options*** are not available if you check the ***All Cameras Available*** checkbox on the **Overlay Cameras** page. You must individually list the cameras in the **Camera to Show** window.



Shadow of a Terminal with a Camera Display Client

Once a Terminal has a Camera Display Client added and is rebooted, the cameras become visible.

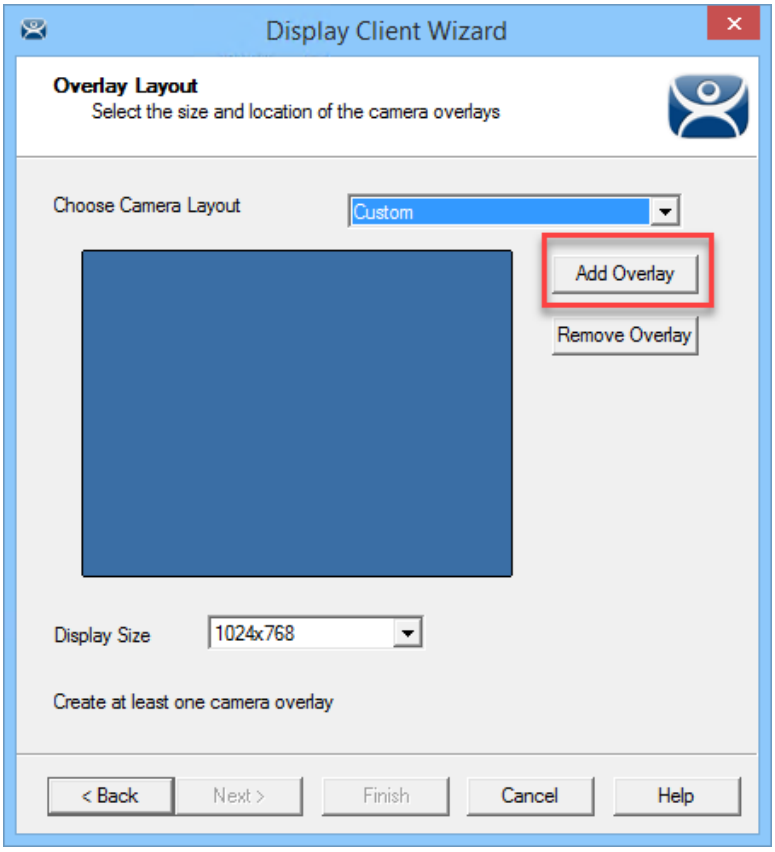
When the Camera Display Client is selected the Terminal will make a connection to the camera and request the feed using the administrative account you entered when you defined the camera as a display server. This connection will only be active if the camera display client is active. If you switch to another display client then the Terminal will drop the connection to the camera.

The overlays and cameras will show green lightning bolts when active and red when inactive.

14.1.2. Custom Overlays

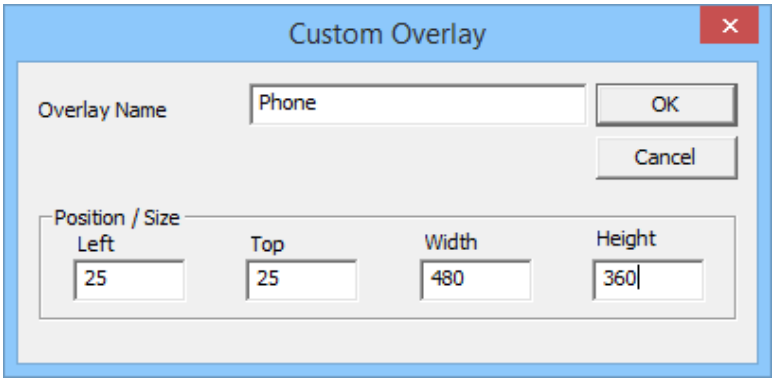
You can create custom overlays instead of using the pre-configured templates.

Create a new Camera Display Client by right clicking on the **Camera** branch of the **Display Client** tree and selecting ***Add Display Client***.



Overlay Layout Page of the Camera Display Client Wizard

Select the ***Add Overlay*** button to open the **Custom Overlay** window.



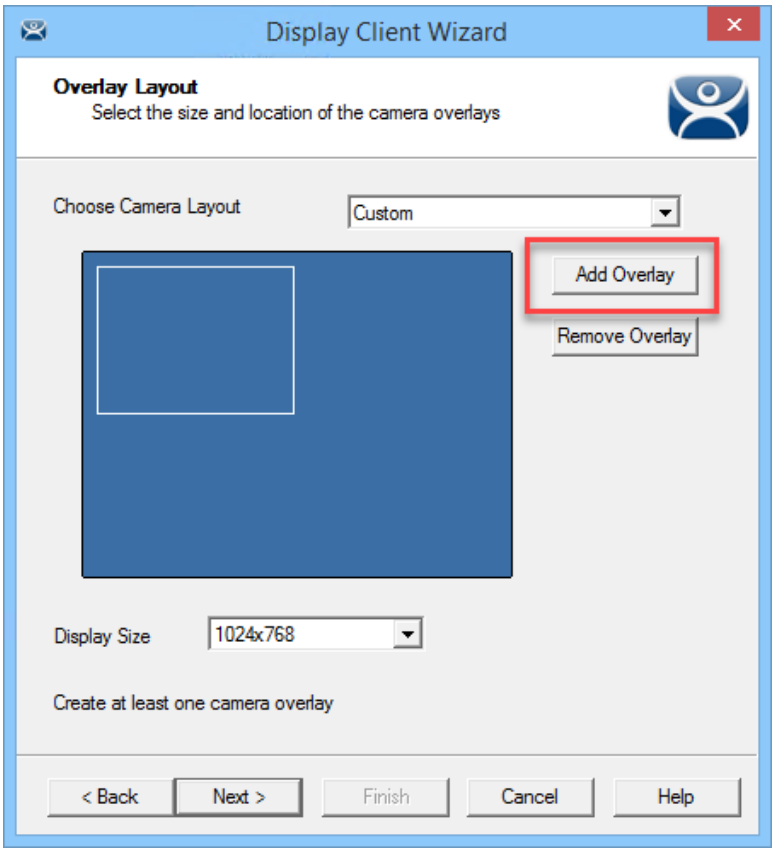
Custom Overlay Window

The **Custom Overlay** window allows you to define the boundaries of the overlay.

Select the position of the overlay in pixels using the ***Left*** and ***Top*** fields.

Define the size of the overlay in pixels in the ***Width*** and ***Height*** fields

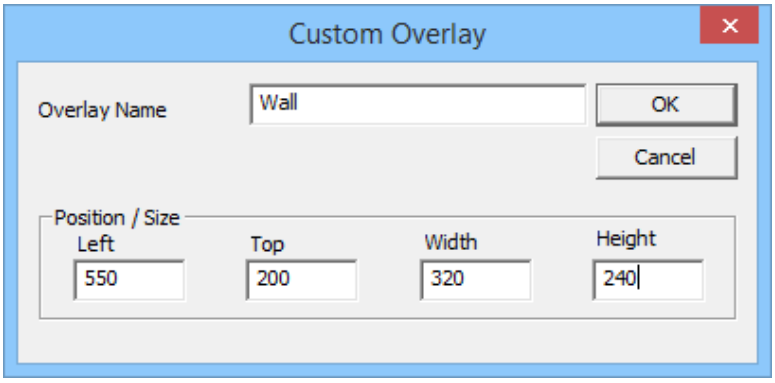
Click the ***OK*** button when done.



Overlay Layout Page of the Camera Display Client Wizard

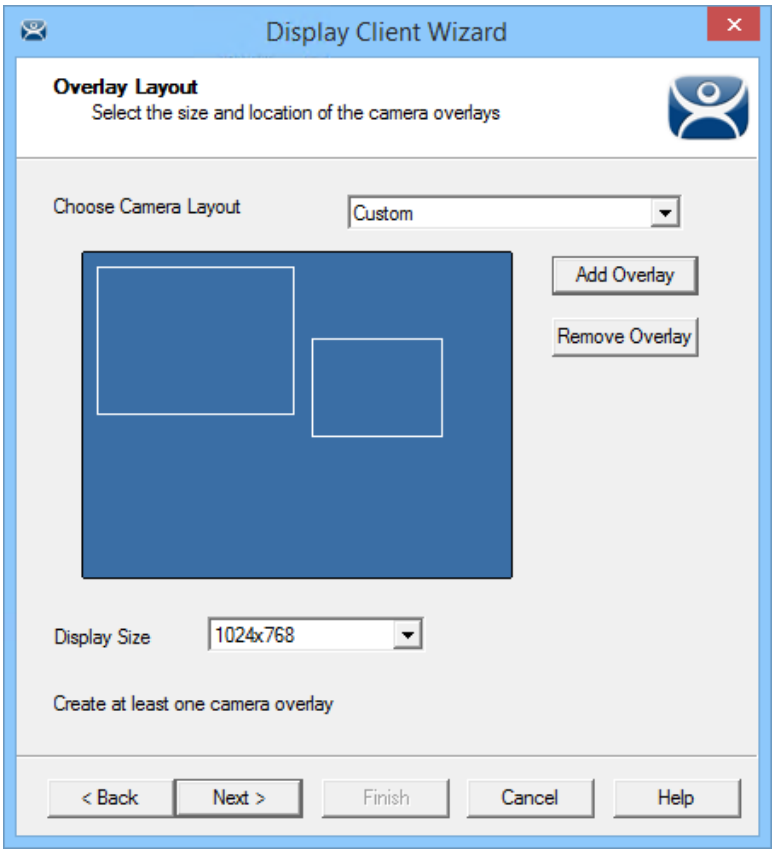
Once the Custom Overlay window is closed the Overlay Layout page will show the boundaries of the custom overlay.

Additional overlays can be added using the ***Add Overlay*** button.



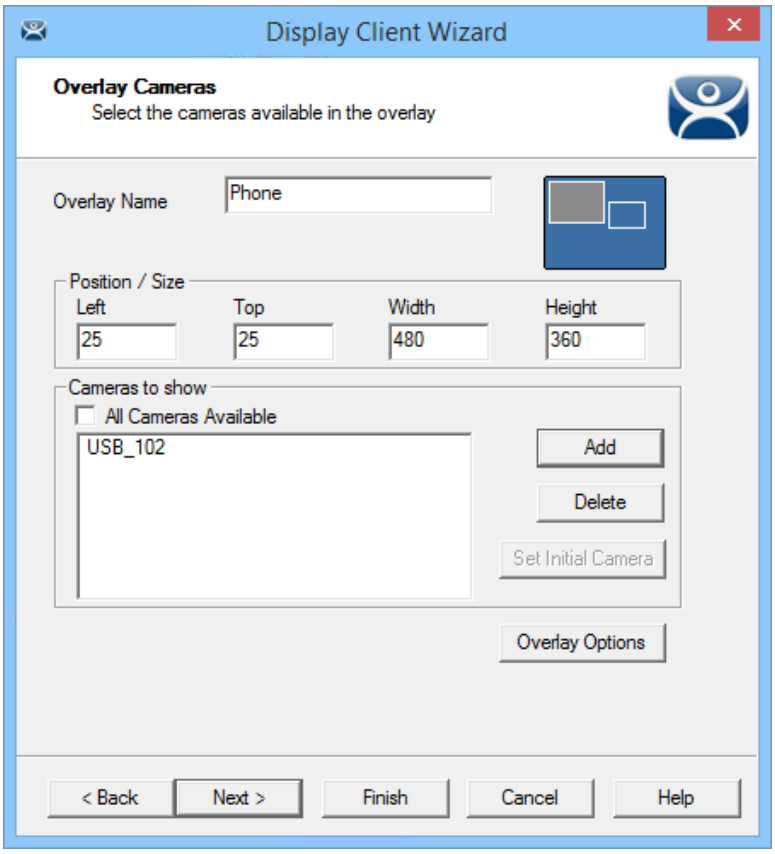
Second Overlay

Additional overlays can be added with the ***Add Overlay*** button.



Overlay Cameras Page

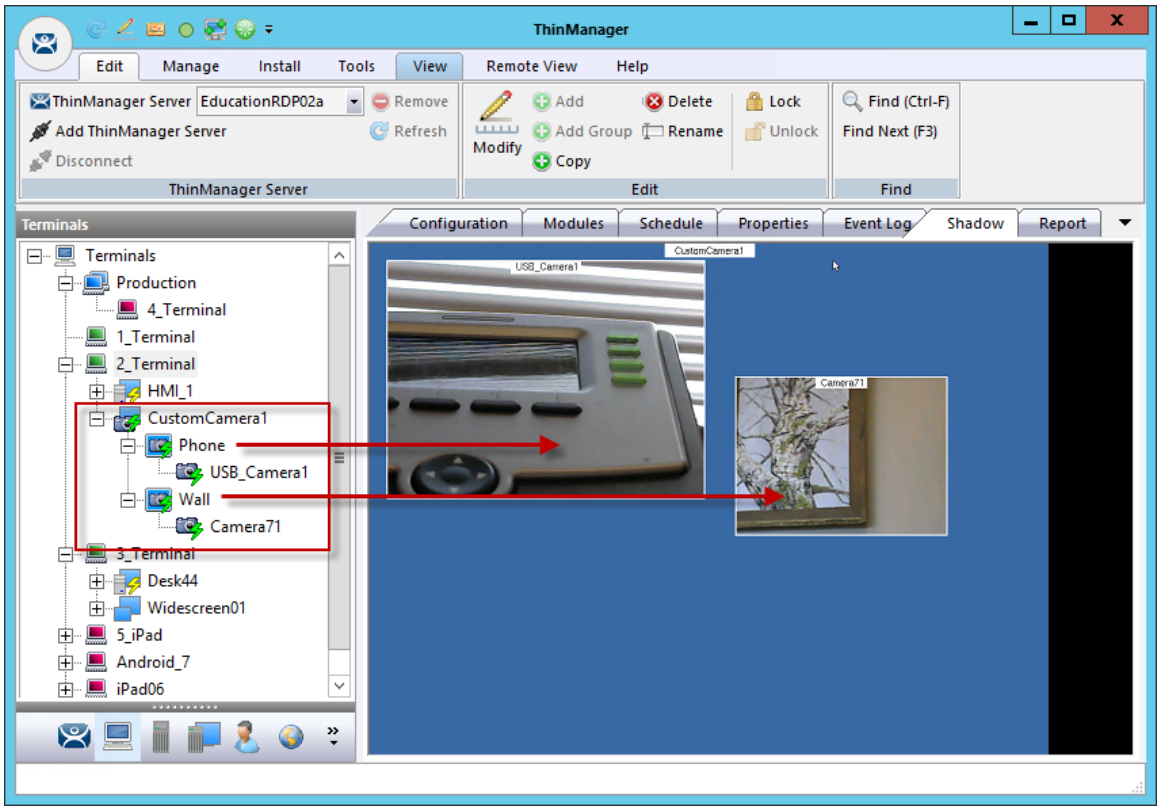
The **Display Client Wizard** will continue to add a camera or cameras to the overlays just like it did for the pre-configured templates.



Multiple Custom Camera Overlays

The wizard will allow you to add cameras to each overlay in turn. The Overlay Camera page also allows you to edit the ***Left*** and ***Top*** positions and the ***Height*** and ***Width***.

Select the ***Finish*** button when done.



Two Custom Overlays in One Display Client

Once the Camera Display Client is assigned to a Terminal and the Terminal is restarted the display client with the custom overlays will be shown on the Terminal.

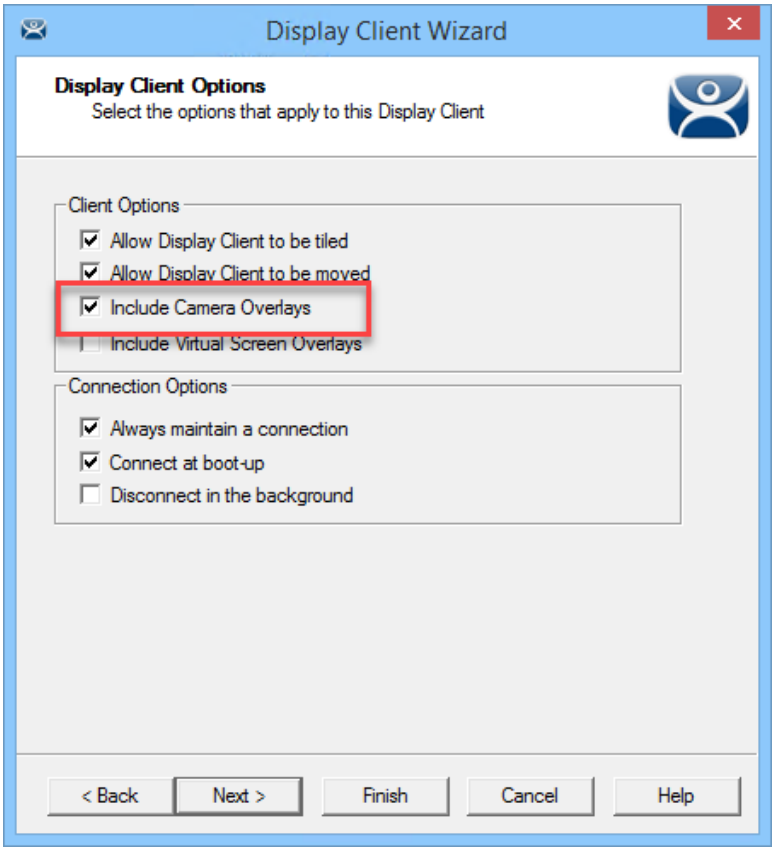
14.1.3. Adding a Camera to an Existing Application

Camera overlays can be added to an application using the Remote Desktop Server Display Client Wizard. It is called an 'Overlay' because it will cover the screen of that display client in the area you define. You can hide and reveal the overlay with the TermMon ActiveX from ThinManager.

- ✓ **Use the TermMon ActiveX to hide and reveal the camera overlay**

See Cameras and the TermMon ActiveX on page 160.

Open a Remote Desktop Server Display Client wizard and navigate to the **Display Client Options** page.

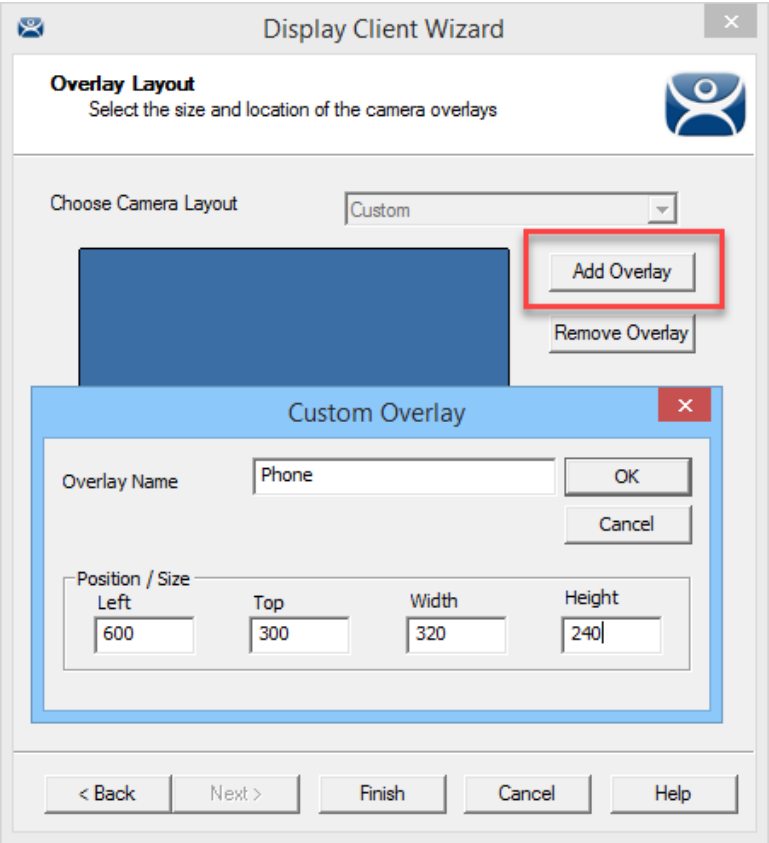


Display Client Options Page of the Remote Desktop Server Display Client Wizard

Check the ***Include IP Camera Overlays*** checkbox.

This will add an ***Overlay Layout*** page to the end of the wizard.

Navigate to the ***Overlay Layout*** page of the wizard.



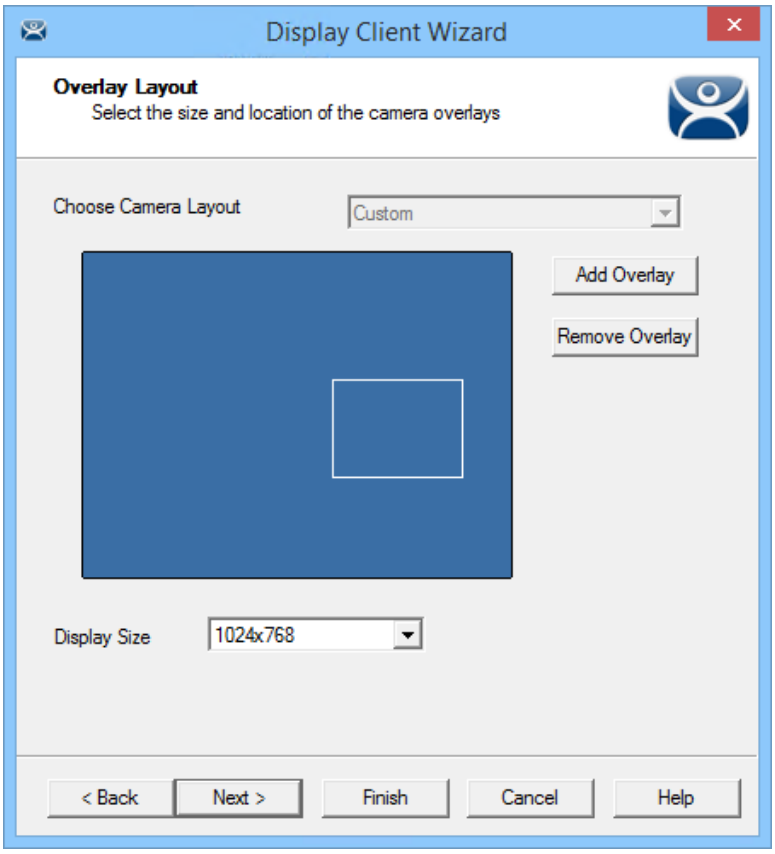
Overlay Layout Page of the Display Client Wizard

Select the ***Add Overlay*** button to launch the **Custom Overlay** window.

Select the position of the overlay in pixels using the ***Left*** and ***Top*** fields.

Define the size of the overlay in pixels in the ***Width*** and ***Height*** fields

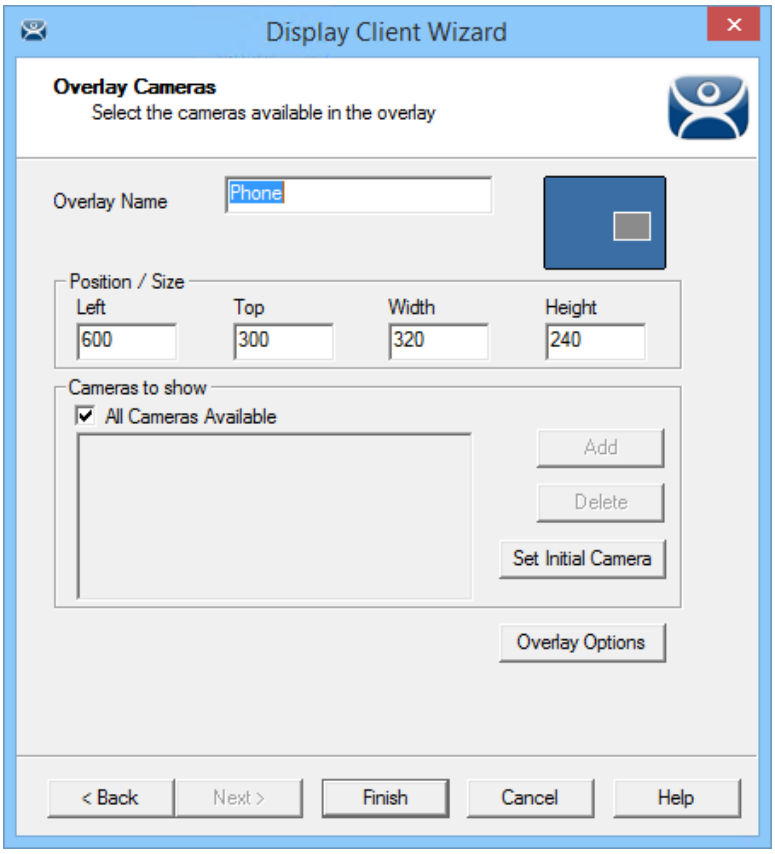
Click the ***OK*** button when done.



Overlay Layout Page of the Remote Desktop Server Display Client Wizard

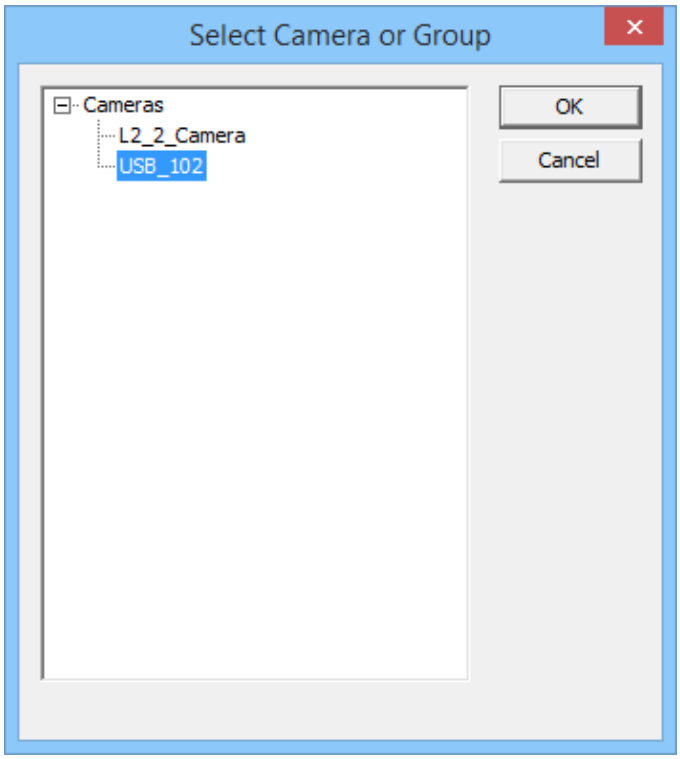
Once the custom overlay is defined and the **Overlay Layout** page is closed you will have the **Overlay Layout** page showing the boundaries of the custom overlay.

Select the ***Next*** button to continue the wizard.



Overlay Cameras Page of the Remote Desktop Server Display Client Wizard

Specify the cameras as before, either using the ***All Cameras Available*** checkbox or the ***Add*** button.

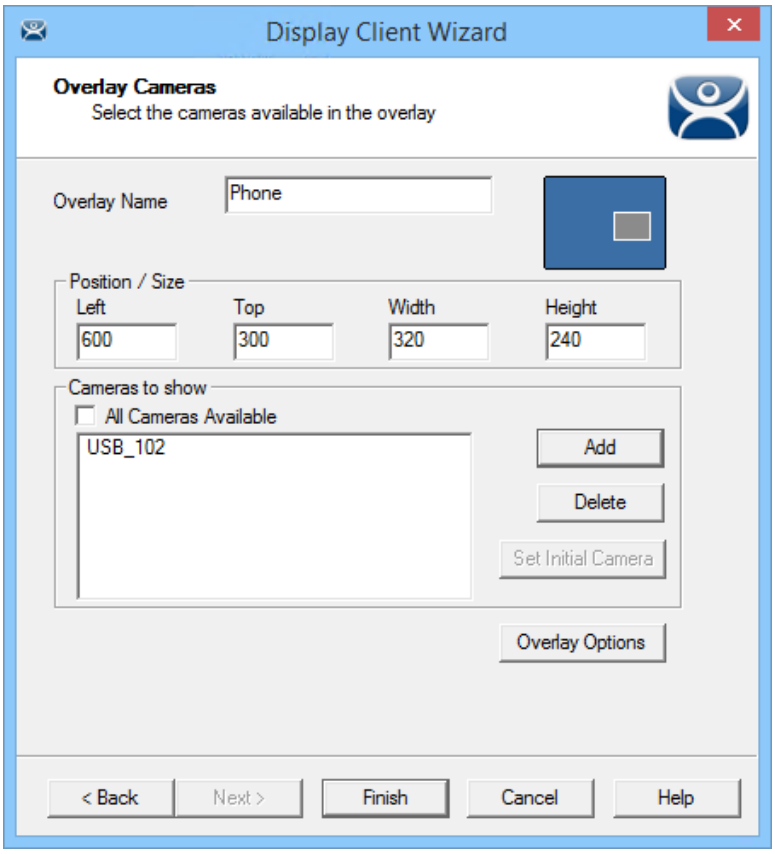


Select Camera or Group Window

The **Select Camera or Group** window is launched from the ***Add*** button and allows you to select a camera for the overlay.

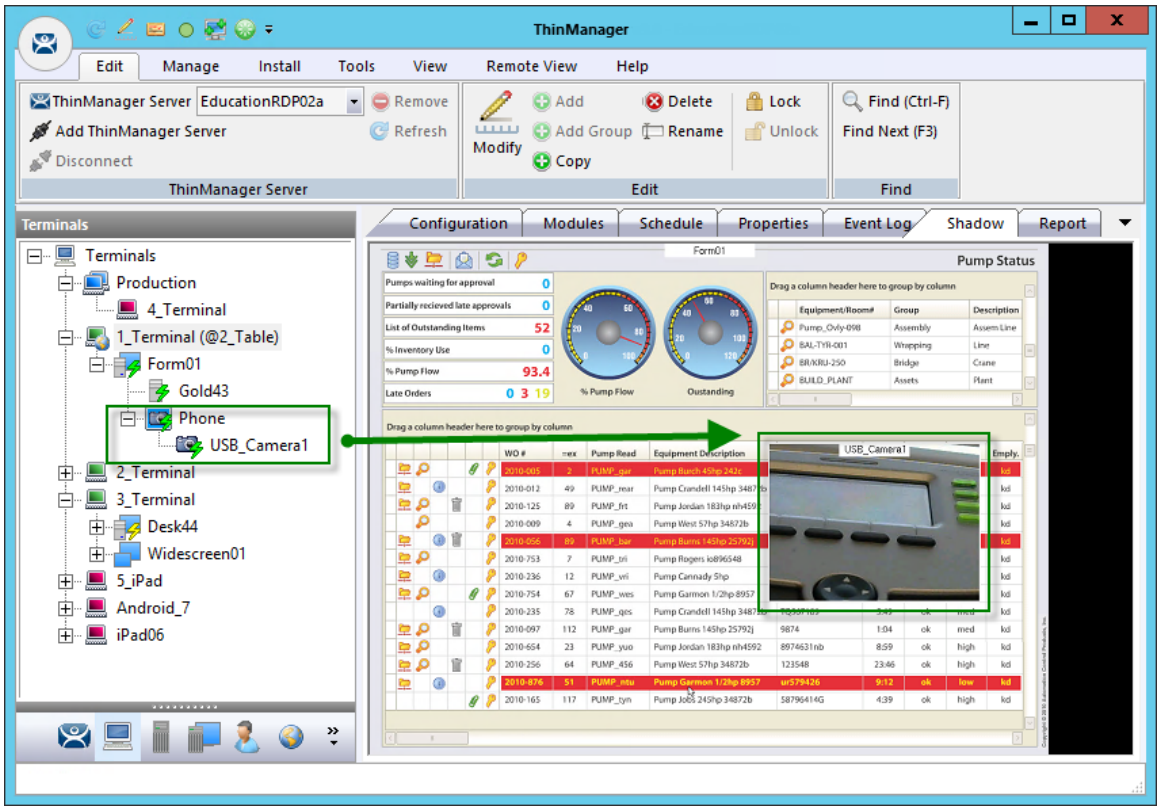
Highlight the desired camera and select the ***OK*** button.

Repeat as needed.



Overlay Cameras Page of the Remote Desktop Server Display Client Wizard

When the cameras are selected and the options configured you can select the ***Finish*** button to close the wizard.



Embedded Camera in Application

The camera will be displayed in the display client when it is added to a Terminal configuration and the Terminal is restarted.

14.1.4. Cameras and the TermMon ActiveX

Camera overlays that are added to an application using the Remote Desktop Server Display Client Wizard will cover the screen of that display client in the area you define. You can hide and reveal the overlay with the TermMon ActiveX from ThinManager.

The TermMon ActiveX Control can be found on the ThinManager CD as **termmon.ocx**. It is also available in the Download section at http://downloads.thinmanager.com/.

The Control must be registered before it can be used. Copy the file **termmon.ocx** to the computer where you want to use it. Register the OCX by executing

regsvr32 <path\termmon.ocx>

Once it is registered it can be added to the application and used to control the camera overlays.

These are the commands available to use with the cameras:

- **CameraOverlayEnable** - This method is used to enable a camera overlay. This method requires two parameters. The first parameter is the name of the Display Client the overlay is on. The second parameter is the name of the overlay.
- **CameraOverlayDisable** - This method is used to disable a camera overlay. This method requires two parameters. The first parameter is the name of the Display Client the overlay is on. The second parameter is the name of the overlay.

- **CameraOverlayCycleStart** - This method is used to start camera cycling for a camera overlay. This method requires two parameters. The first parameter is the name of the Display Client the overlay is on. The second parameter is the name of the overlay.
- **CameraOverlayCycleStop** - This method is used to stop camera cycling for a camera overlay. This method requires two parameters. The first parameter is the name of the Display Client the overlay is on. The second parameter is the name of the overlay.
- **CameraOverlaySwitchNext** - This method is used to switch to the next camera in a camera overlay list. This method requires two parameters. The first parameter is the name of the Display Client the overlay is on. The second parameter is the name of the overlay.
- **CameraOverlaySwitchPrev** - This method is used to switch to the previous camera in a camera overlay list. This method requires two parameters. The first parameter is the name of the Display Client the overlay is on. The second parameter is the name of the overlay.
- **CameraOverlayFullscreenEnter** - This method is used to make the current camera in a camera overlay enter full screen. This method requires two parameters. The first parameter is the name of the Display Client the overlay is on. The second parameter is the name of the overlay.
- **CameraOverlayFullscreenExit** - This method is used to make the current camera in a camera overlay exit full screen. This method requires two parameters. The first parameter is the name of the Display Client the overlay is on. The second parameter is the name of the overlay.
- **CameraOverlaySwitchByName** - This method is used to change cameras in a camera overlay. This method requires three parameters. The first parameter is the name of the Display Client the overlay is on. The second parameter is the name of the overlay. The third parameter is the name of the camera. The camera name must include the full path if the camera is in a camera group.
- **CameraOverlayMove** - This method is used to change the position of a camera overlay. This method requires four parameters. The first parameter is the name of the Display Client the overlay is on. The second parameter is the name of the overlay. The third parameter is the x location. The forth parameter is the y position.
- **CameraOverlayResize** - This method is used to change the size of a camera overlay. This method requires four parameters. The first parameter is the name of the Display Client the overlay is on. The second parameter is the name of the overlay. The third parameter is the width. The forth parameter is the height.
- **CameraOverlayResizeMove** - This method is used to change the size and position of a camera overlay. This method requires six parameters. The first parameter is the name of the Display Client the overlay is on. The second parameter is the name of the overlay. The third parameter is the x position. The forth parameter is the y position. The fifth parameter is the width. The sixth parameter is the height.

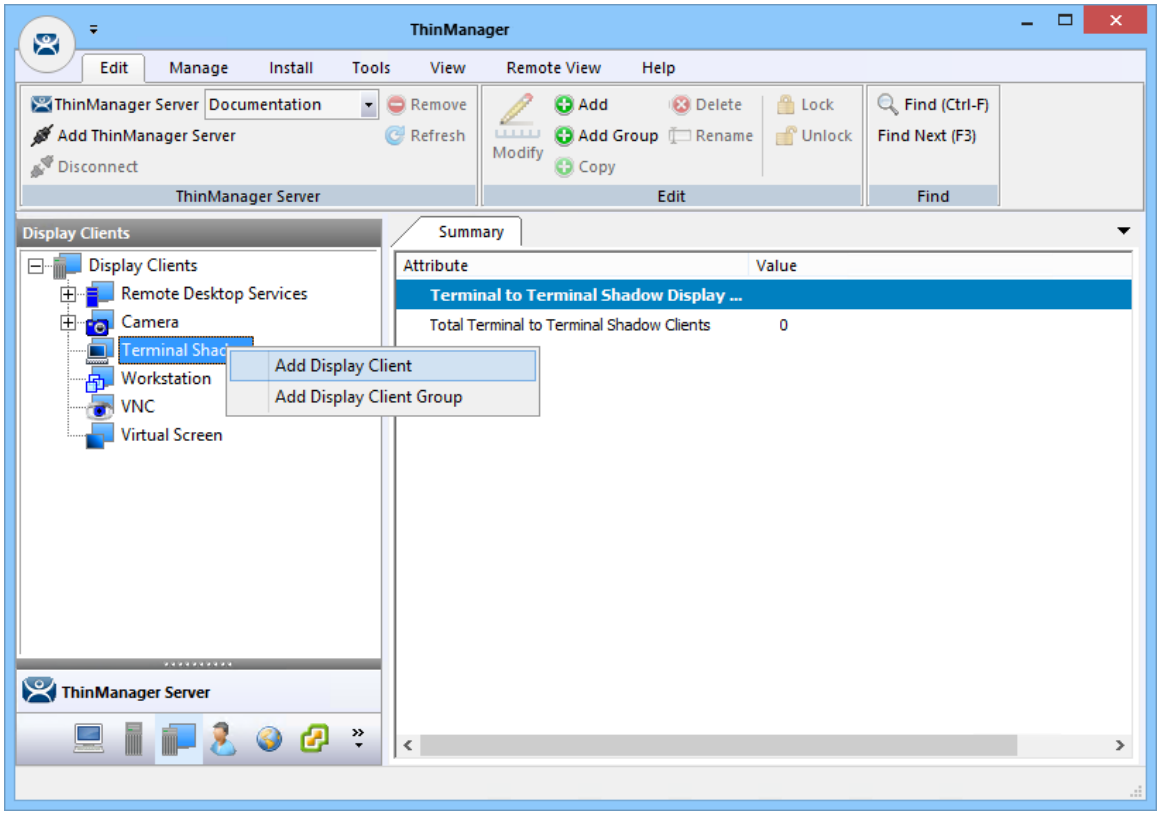
15. Content – Terminal Shadow

The Terminal Shadow display client allows one ThinManager thin client to shadow another. You can shadow one specific thin client or have a menu of Terminals to shadow at will.

Terminal Shadow is valuable because it allows a user to shadow another Terminal without needing to launch ThinManager to use the ThinManager shadow function.

The ThinManager Terminal Shadow sends the screen display from the shadowed Terminal to the shadowed. It doesn't redirect the display from the Remote Desktop Server but sends the images from the actual shadowed Terminal.

Terminal to Terminal shadowing is set up and configured as a Terminal Shadow Display Client.



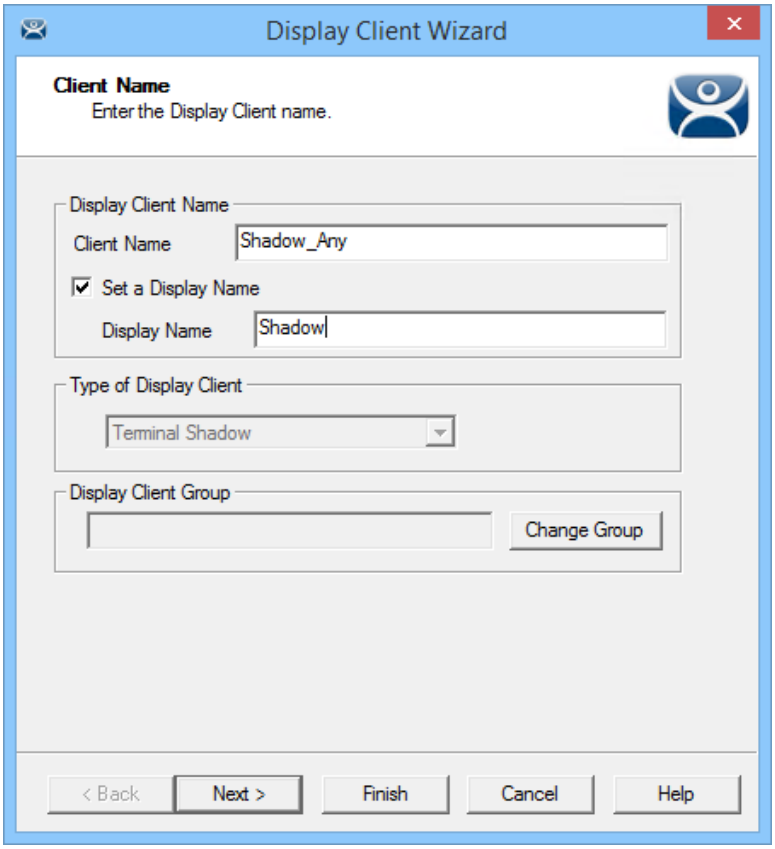
Display Client Tree of ThinManager

Launch the **Display Client Wizard** by right clicking on the **Terminal Shadow branch** of the **Display Clients tree** and selecting ***Add Display Client***.

15.1. Shadow Any Terminal

The Terminal Shadow display client can be created with a list of Terminals that can be shadowed. This is a great troubleshooting tool because a station can be given a chance to view other Terminals to monitor problems or to analyze problems without having to travel to the specific problem area.

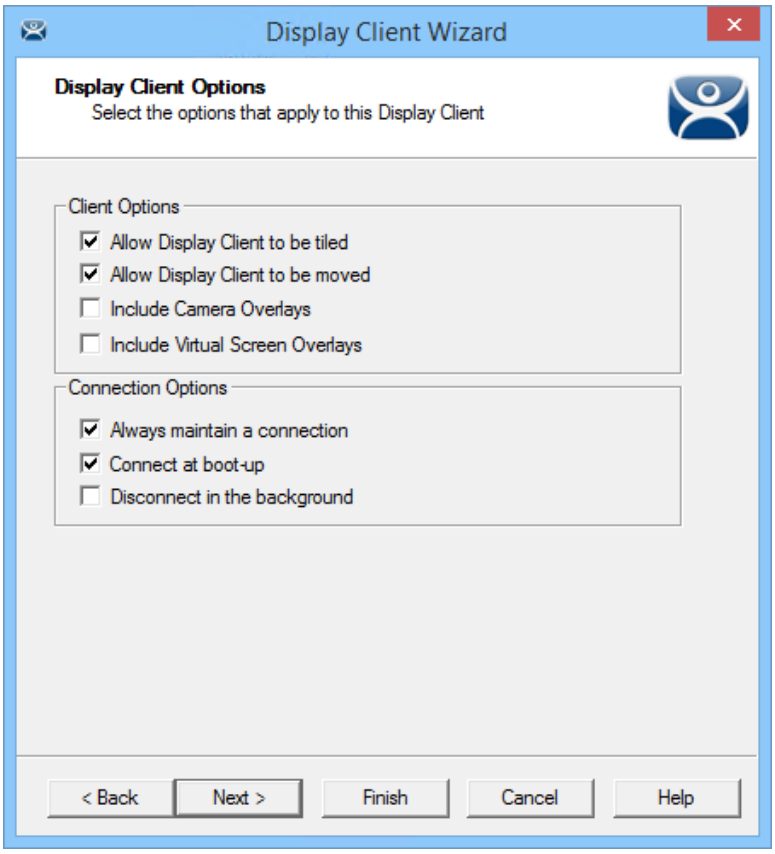
Right clicking on the **Terminal Shadow branch** of the **Display Clients tree** and selecting ***Add Display Client*** will launch the Display Client wizard for Terminal Shadow.



Client Name Page of the Terminal Shadow Display Client Wizard

Enter a name for the Terminal Shadow display client and select ***Next*** to continue.

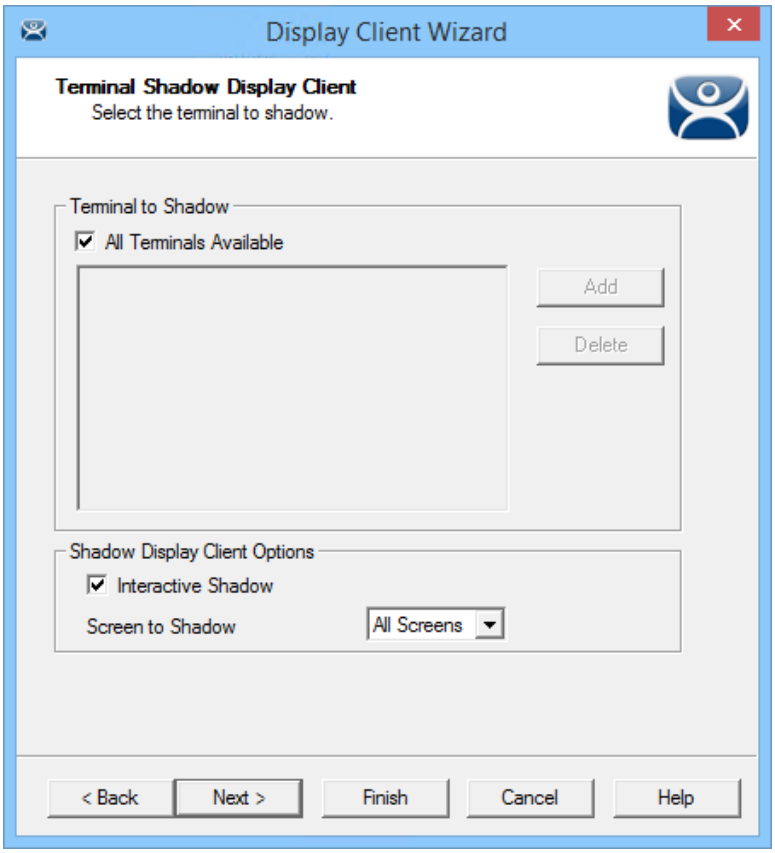
The ***Set a Display Name*** checkbox allows you to configure the display client to display an alternative name in the ThinManager Server tree.



Display Client Options Page of the Terminal Shadow Display Client Wizard

The Display Client Options page of the Terminal Shadow Display Client wizard is the same as the Remote Desktop Server Display Client wizard.

Select ***Next*** to continue.



Terminal Shadow Display Client Page of the Terminal Shadow Display Client Wizard

The Terminal Shadow Display Client page of the Terminal Shadow Display Client wizard is unique.

Leaving the ***All Terminals Available*** checkbox selected will add all of the Terminals to the Shadow menu.

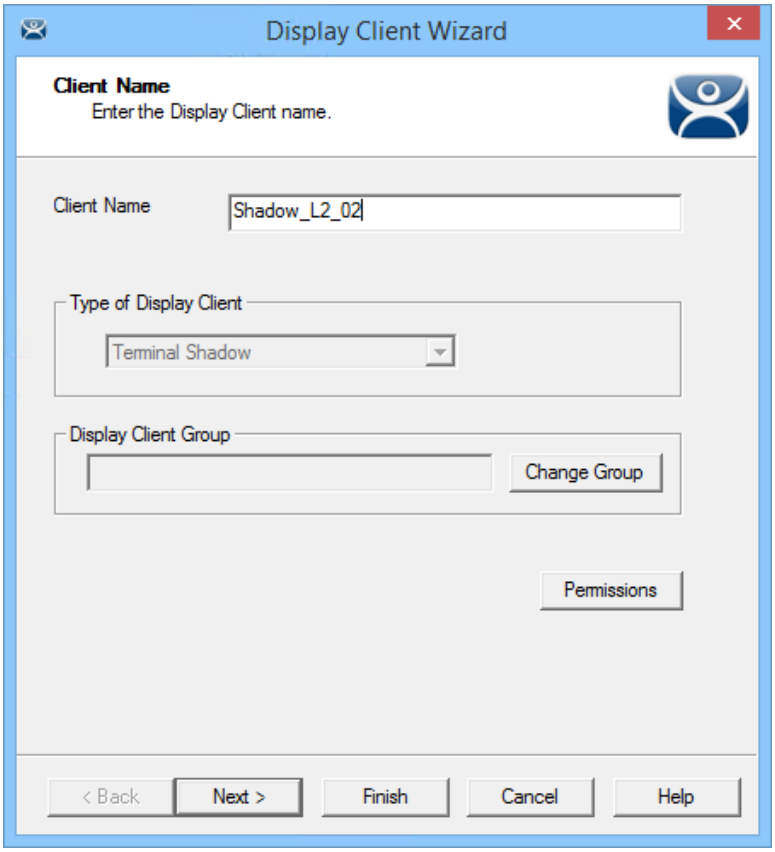
You can unselect the ***All Terminals Available*** checkbox and use the ***Add*** button to launch the **Select Terminal or Group** window to select specific Terminals.

See Shadow a Specific Terminal.

15.2. Shadow a Specific Terminal

You can use the Terminal Shadow Display Client to shadow a specific Terminal, duplicating the display to another thin client. This can be helpful to provide a worker access to his HMI in various places in a large station, like a commercial oven at a baking line.

Launch the Display Client wizard for Terminal Shadow by right clicking on the **Terminal Shadow** branch of the **Display Clients tree** and selecting ***Add Display Client***.

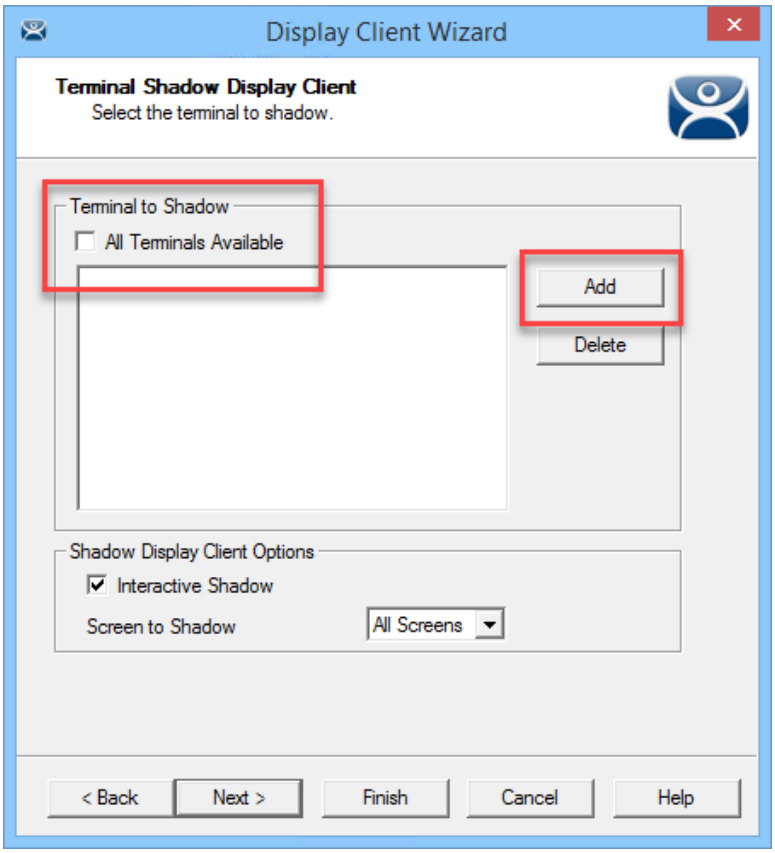


Client Name Page of the Terminal Shadow Display Client Wizard

Enter a name for the display client in the ***Client Name*** field and select the ***Next*** button.

The **Display Client Options** page of the **Terminal Shadow Display Client** wizard is the same as the Remote Desktop Server Display Client wizard.

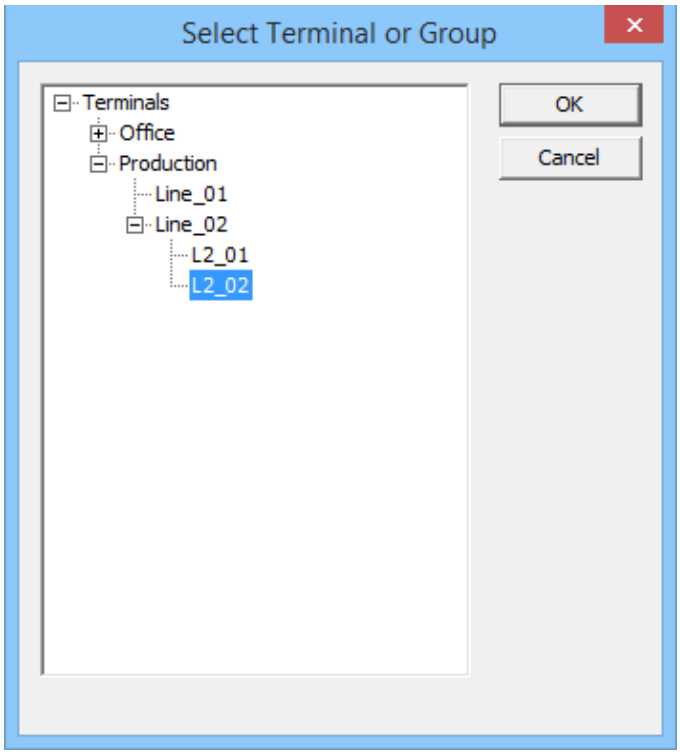
Select ***Next*** to continue.



Terminal Shadow Display Client Page of the Terminal Shadow Display Client Wizard

The **Terminal Shadow Display Client** page of the Terminal Shadow Display Client wizard is unique.

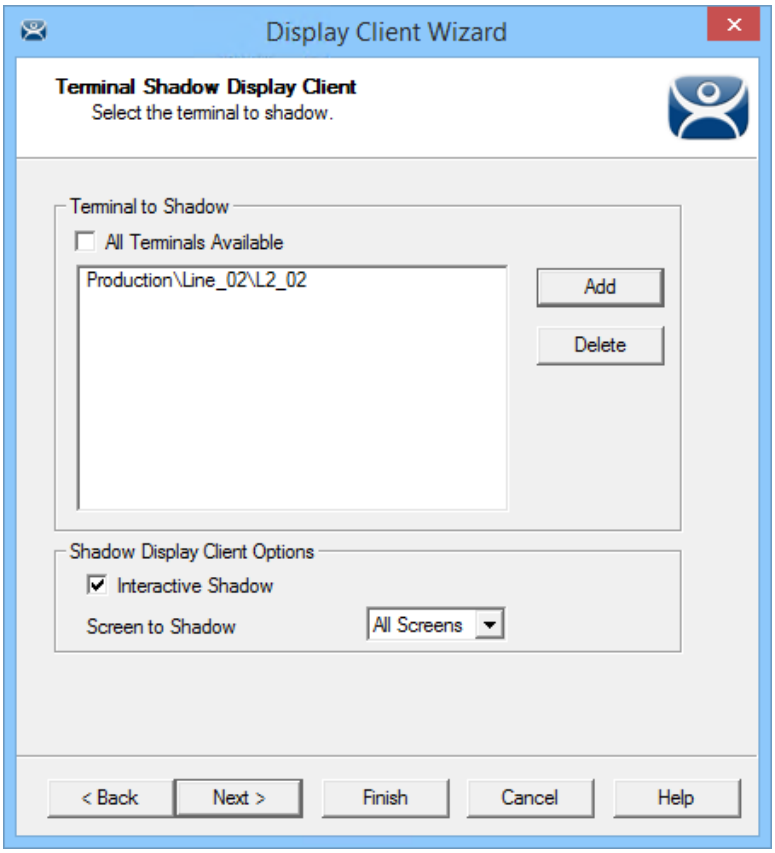
Unselect the ***All Terminals Available*** checkbox and use the ***Add*** button to launch the **Select Terminal or Group** window to add specific Terminals.



Select Terminal or Group Window

The **Select Terminal or Group** window allows you to select a single group or a Terminal and add to the Shadow menu. Highlight your selection and click the ***OK*** button.

If you select a Terminal you can repeat until you have selected all the Terminals you want.



Terminal Shadow Display Client Page of the Terminal Shadow Display Client Wizard

The selected Group or Terminals will be displayed in the Terminal to Shadow frame.

You can allow the shadowing user to interact with the shadowed Terminal by leaving the ***Interactive Shadow*** checkbox selected.

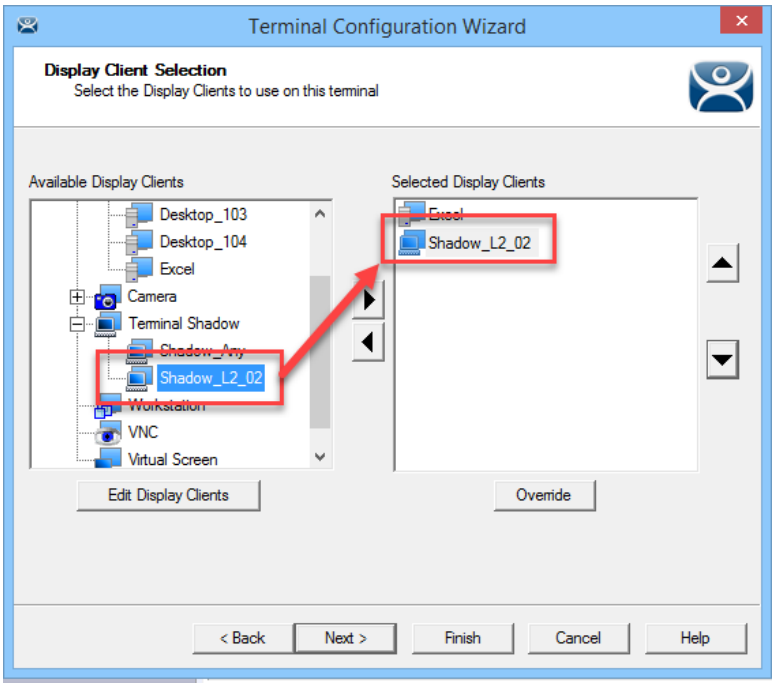
Unchecking the ***Interactive Shadow*** checkbox will allow the shadow user to "look, but not touch."

You can use the Screen to Shadow drop-down to control which screen of a MultiMonitor thin client you shadow.

Click the ***Finish*** button to complete the wizard.

15.3. Shadow of the Terminal

The Terminal Shadow display clients are added to the Terminal like other display clients.

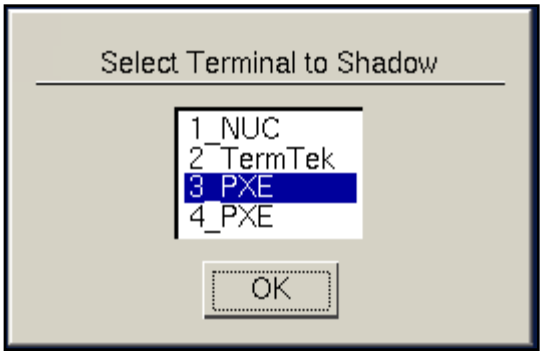


Display Client Selection Page of the Terminal Configuration Wizard

The Terminal Shadow display clients have an icon of a Terminal and a monitor session.

Move the desired Terminal Shadow display clients to the ***Selected Display Clients*** list by double clicking on them or using the arrows on a highlighted display client.

Click the ***Finish*** button to save the configuration and restart the Terminal to send the configuration to the Terminal.



Shadow Menu

A Terminal Shadow Display Client with more than a single Terminal will open with a **Select Terminal to Shadow** menu.

Highlight the Terminal you want to shadow and select the ***OK*** button. You will connect to the Terminal and display the screen from the shadowed thin client.

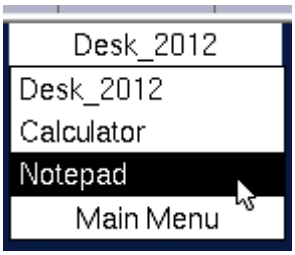
15.3.1. Display Client Group Selector During Shadow

The Terminal Shadow display client will be displayed in the Group Selector Menu of the Terminal it is assigned. The group selector shows the local display clients assigned to the Terminal.

Local Terminal Menu Selector

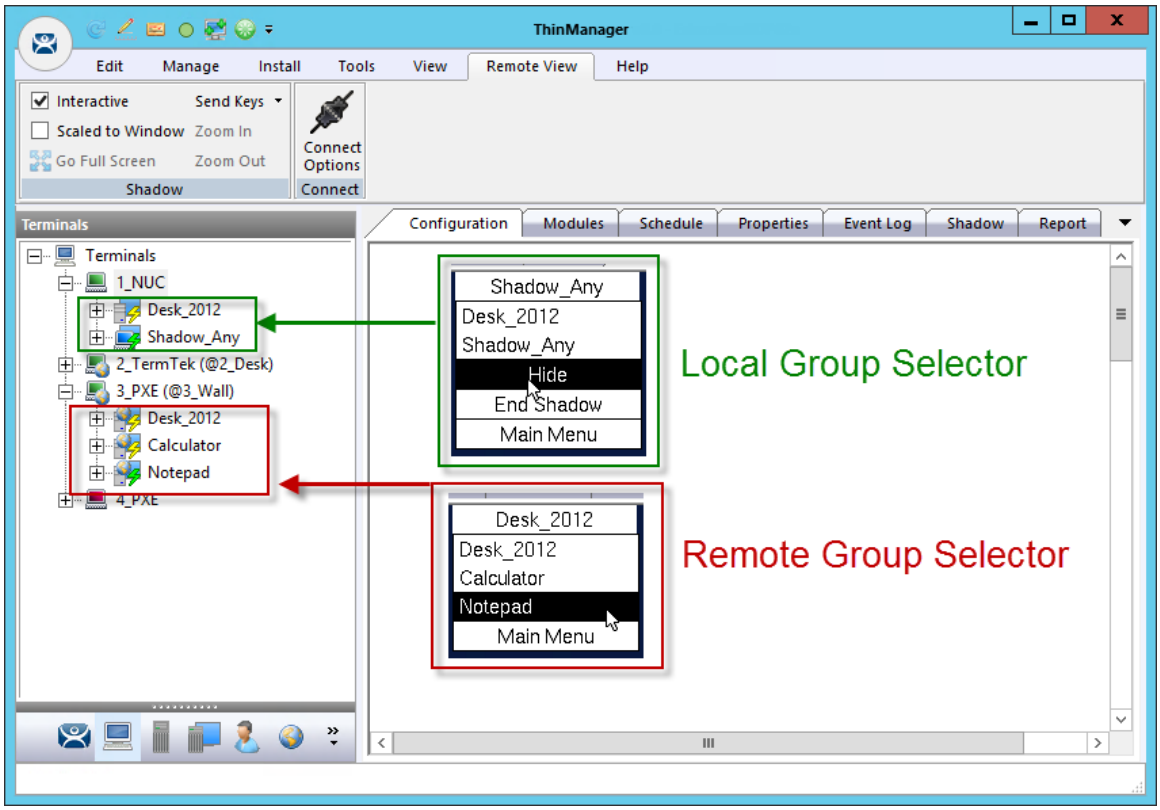
When the local Group Selector menu is shown the Group Selector of the remote Terminal is hidden.

If you want to use the remote Terminal's Group Selector you select ***Hide*** on the local Group Selector. This will hide the local selector and show the remote Group Selector.



Remote Terminal Menu Selector

Once the remote group selector menu is used the local Terminal will revert back to the local group selector.



ThinManager Interface Showing Group Selector Menus

The picture shows the Group Selector for both the local 1_PXE Terminal and the remote 02_Logic Terminals.

16. Content - Workstation Deployment

Microsoft built RDP into their workstation operating systems so that a permitted user can make a connection to a workstation and transfer the desktop session to another computer. This allows ThinManager to capture a session on a Windows XP Pro, Vista Pro, Windows 7, or Windows 10 computer and transfer it to a thin client. This is very helpful. It allows applications that aren't Remote Desktop Services compliant to be run on a workstation but the user can receive the session on a hardened industrial thin client instead of a PC.

Transferring a workstation session to a thin client requires:

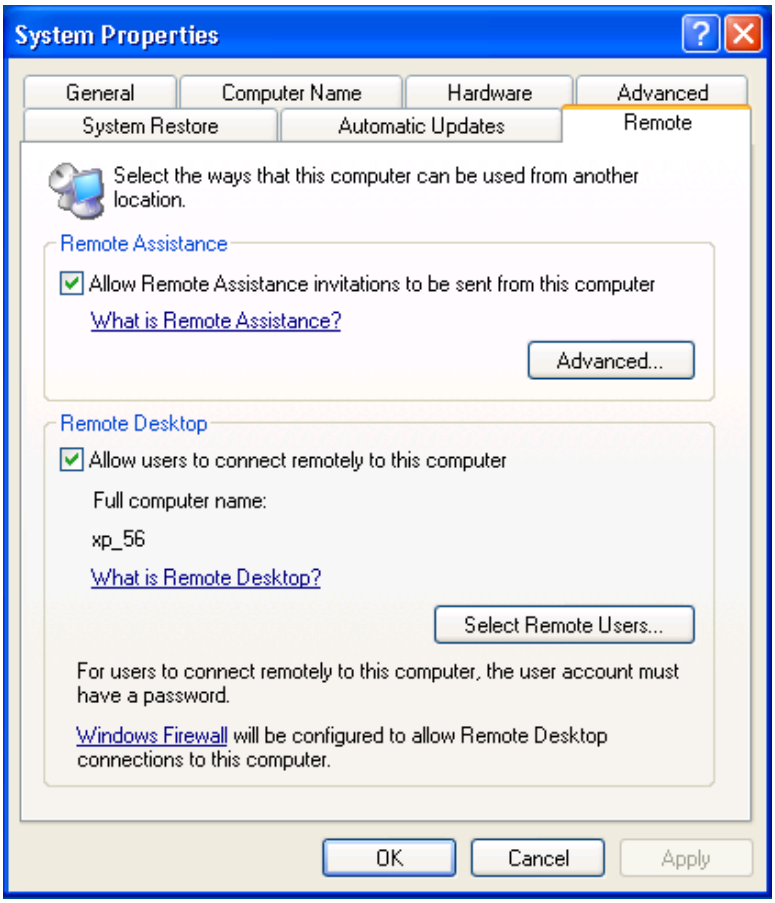
- Turning on the Remote transfer on the PC.
- Creating a Workstation Display Client.
- Applying the Workstation Display Client to a Terminal.

The workstation can be a physical computer or a virtualized desktop.

16.1. Step 1 – On the PC

The workstation needs to have the Remote Desktop function enabled in Systems Properties. This example uses Windows XP. Consult Microsoft instructions for more detail.

Go to the workstation Control Panel and open the **System Properties**. It can also be opened by right clicking on **My Computer** and selecting ***Properties***.



System Properties for XP Workstation

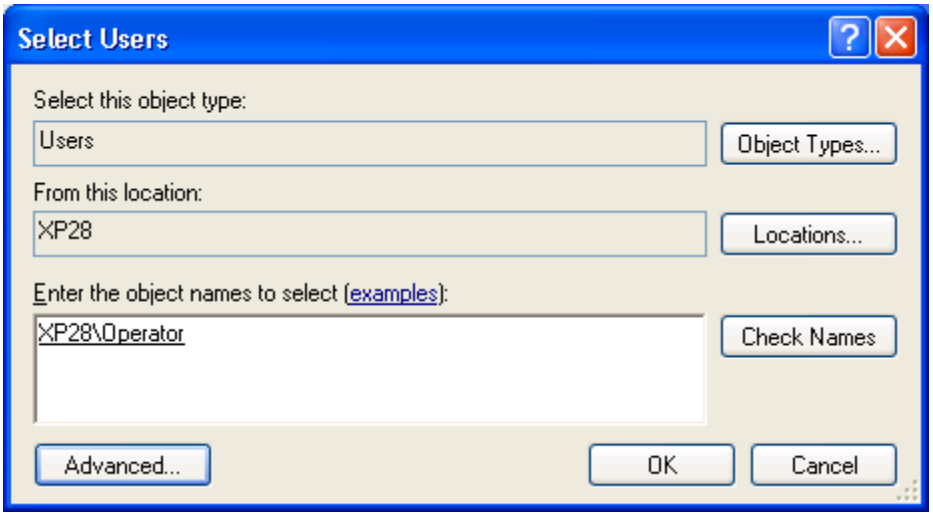
Select the ***Allow users to connect remotely to the computer*** checkbox to enable remote connections.

The ***Select Remote Users…*** button opens a **Remote Desktop Users** window that allows you to specified authorized users.

Remote Desktop Users Window

The **Remote Desktop Users** window shows the users authorized to connect to the computer to transfer the session.

Add users by selecting the ***Add…*** button that opens a **Select Users** window. This window allows you to pick the users to add and authorize.



Select Users Window

Add the desired users to the text box.

Use the ***Check Names*** button to validate.

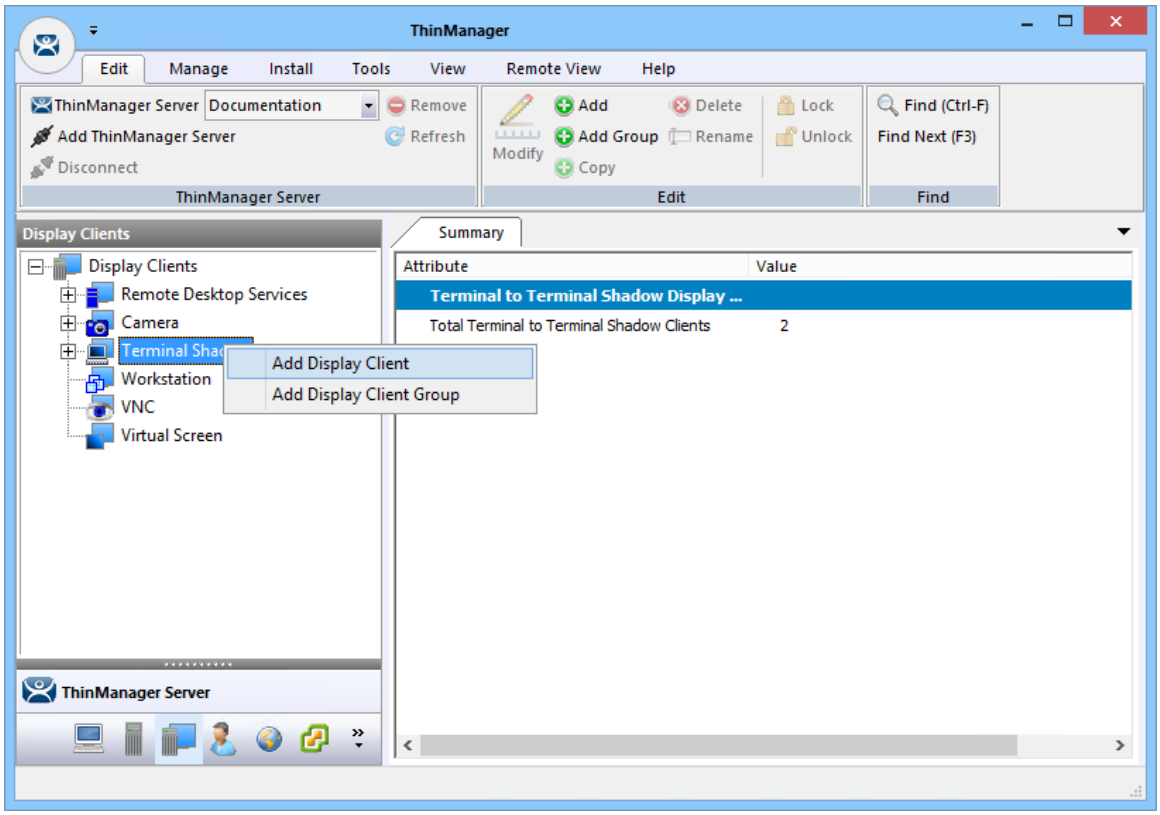
Click ***OK*** to add the user.

Close all the windows to finish the tasks.

16.2. Step 2 – Workstation Display Client

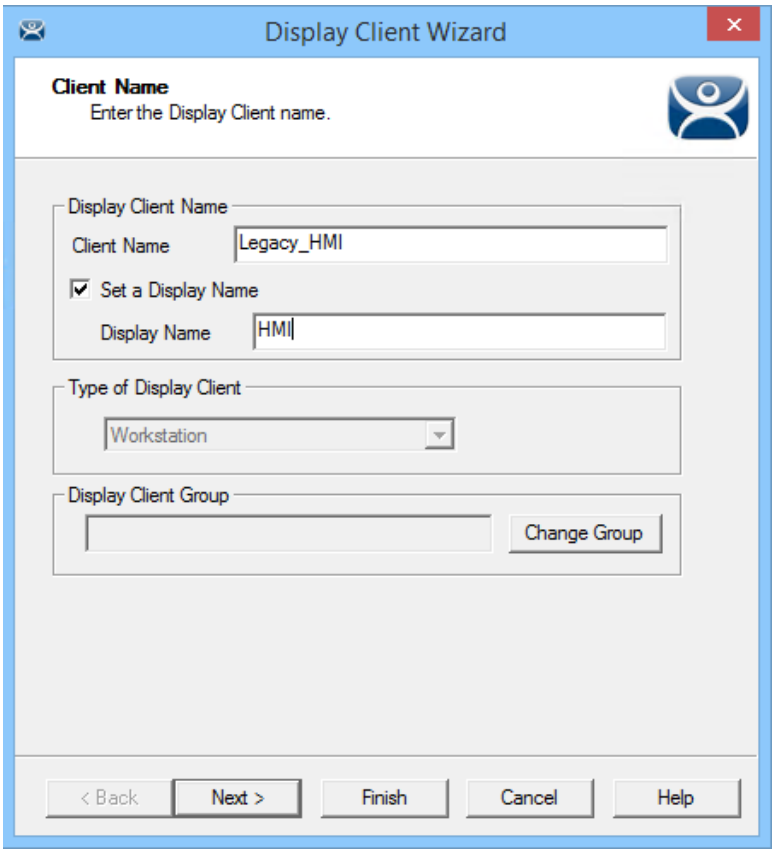
You need to create a **Workstation Display Client** to act as a template for the workstations you want to transfer to a thin client.

Right click on the **Workstation branch** of the Display Clie**nt** branch of the ThinManager tree and select ***Add New Display Client***.



Workstation Display Client Wizard

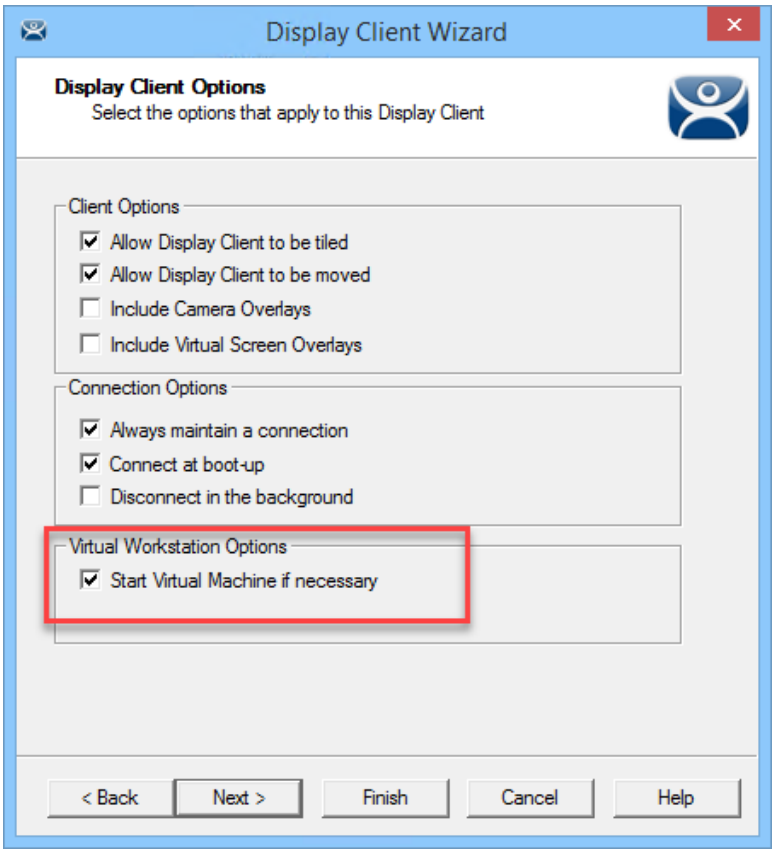
The Workstation Display Client acts as a template for the behavior of the connected workstations.



Client Name Page of the Workstation Display Client Wizard

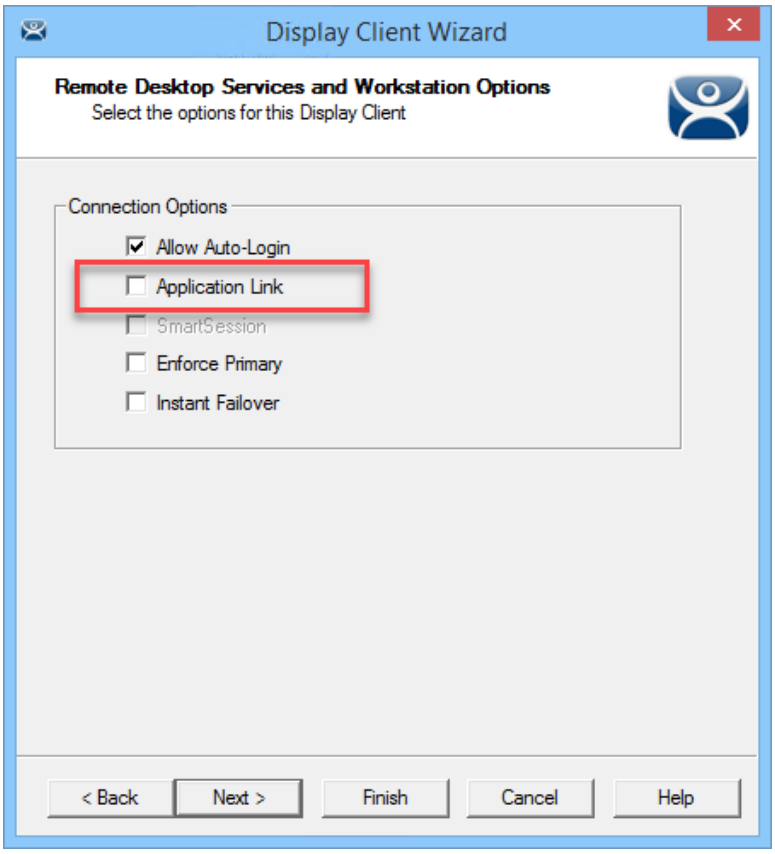
The **Client Name Page** of the **Workstation Display Client** wizard is similar to other **Display Client Option** pages. Enter a unique name and select the ***Next*** button.

The ***Set a Display Name*** allows you to show an alternative name in the ThinManager Server tree.



Display Client Options Page of the Workstation Display Client Wizard

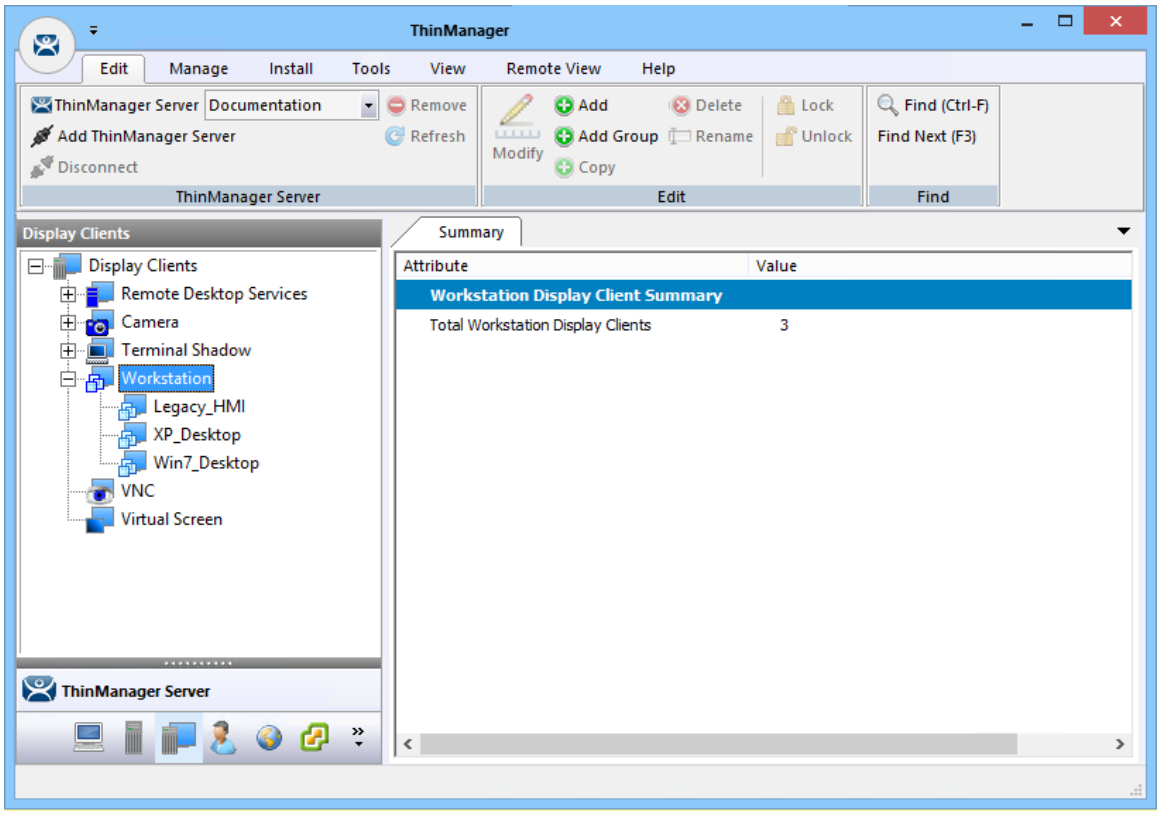
The **Display Client Options Page** of the **Workstation Display Client** wizard is similar to other **Display Client Option** pages except for the ***Start Virtual Machine if necessary*** checkbox. It is a good idea to check this checkbox.



Remote Desktop Services and Workstation Options Page

The **Remote Desktop Services and Workstation Options** page of the Workstation Display Client is similar to other display clients with one exception, ***Application Link***. You must deploy the workstation as a desktop by leaving the ***Application Link*** checkbox unchecked.

Select the ***Finish*** button to close the wizard.



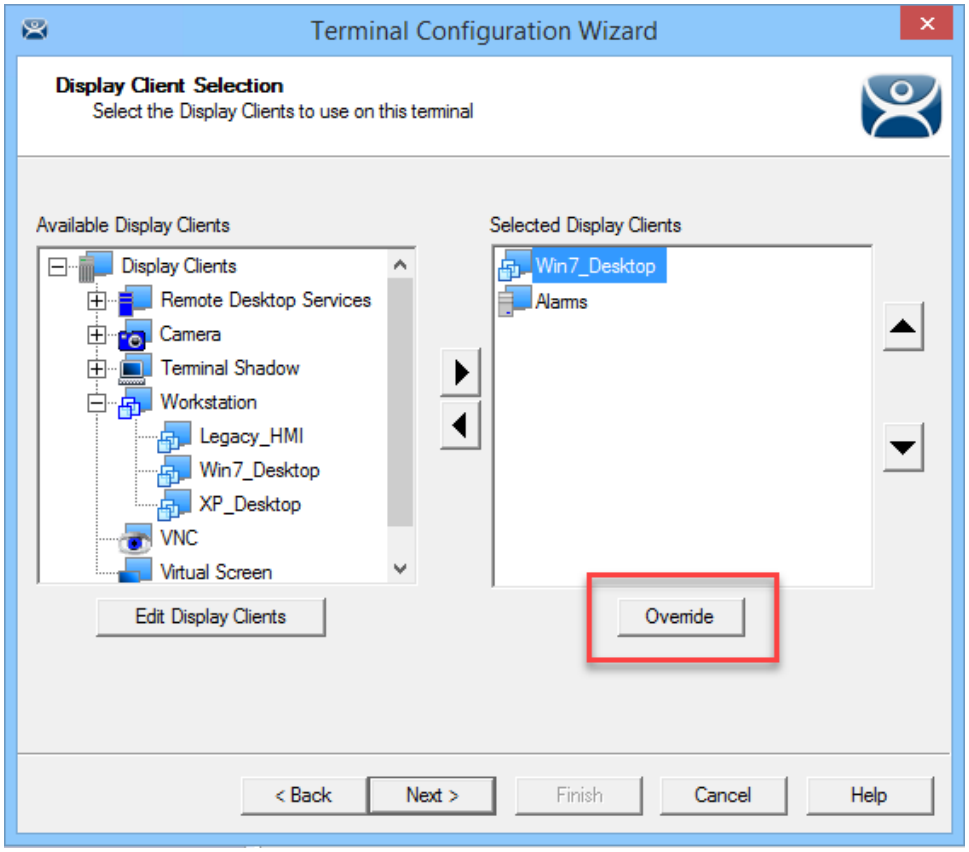
ThinManager with Workstations in the Display Client Tree

The completed display clients will be displayed in the **Workstation** branch of the **Display Client** tree in ThinManager.

16.3. Adding the Workstation Display Client to the Terminal

Open the **Terminal Configuration Wizard** by double clicking on the Terminal in the Terminal branch of the ThinManager tree.

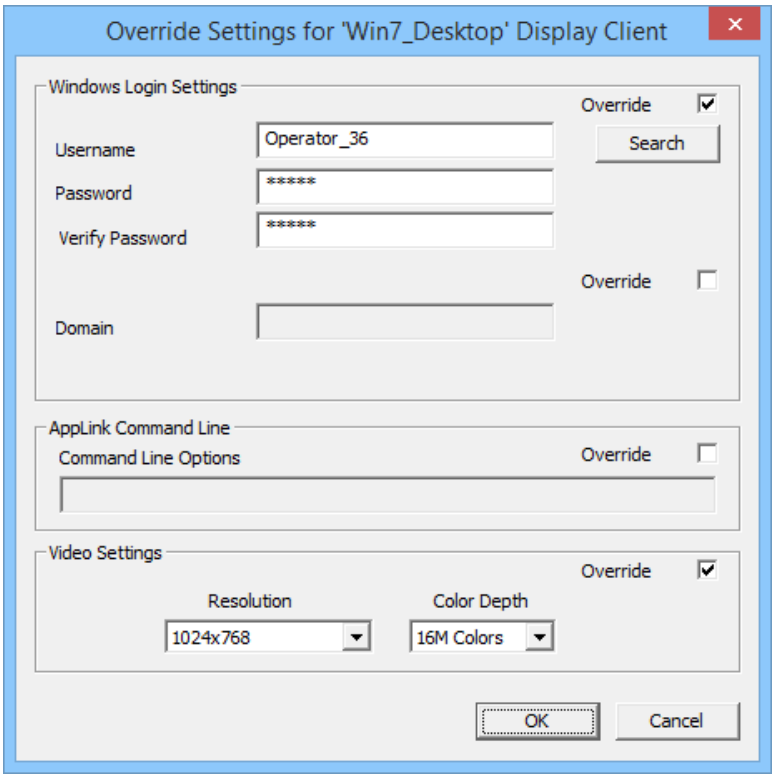
Navigate to the **Display Client Selection** page.



Display Client Selection Page of the Terminal Configuration Wizard

The Workstation display clients can be added like the other display clients by moving them to the ***Selected Display Clients*** list on the **Display Client Selection** page of the Terminal Configuration Wizard.

If the workstation uses a different account then the Terminal use the ***Override*** button to change the Windows account that is used for logging in.



Override Settings

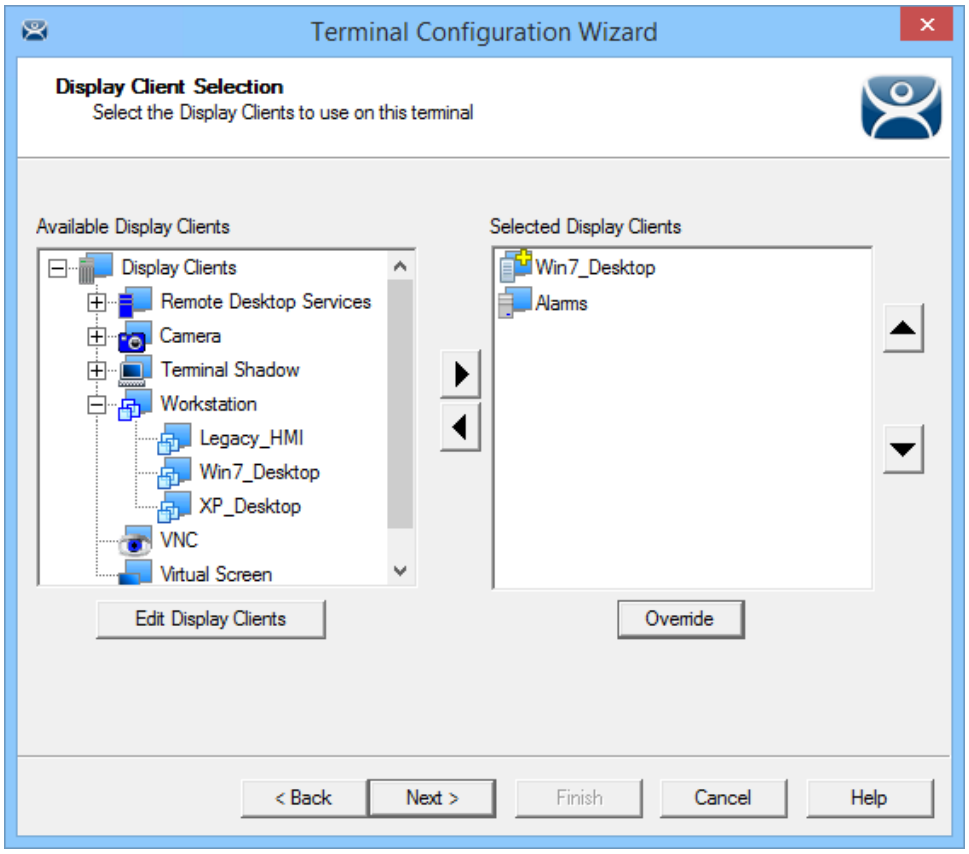
The ***Override*** button on the **Display Client Selection** page will launch the **Override Settings** page.

Check the ***Override*** checkbox in the **Windows Login Settings** frame and add the workstation's correct user account to the ***Username*** and ***Password*** fields.

You may enter a Windows user account manually or use the ***Search*** button to pull a user account from the Active Directory as shown in Domain Member Remote Desktop Server.

You can also change the video resolution that you want displayed with the ***Video Setting*** override.

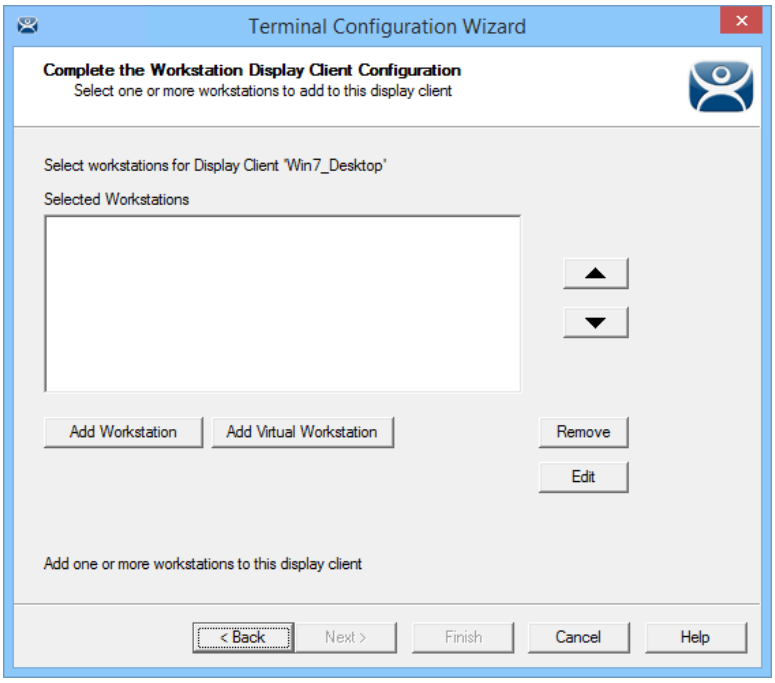
Click ***OK*** to accept.



Override Indicator

Display clients with an override will display a yellow plus sign on their icon.

Select the ***Next*** button to continue.

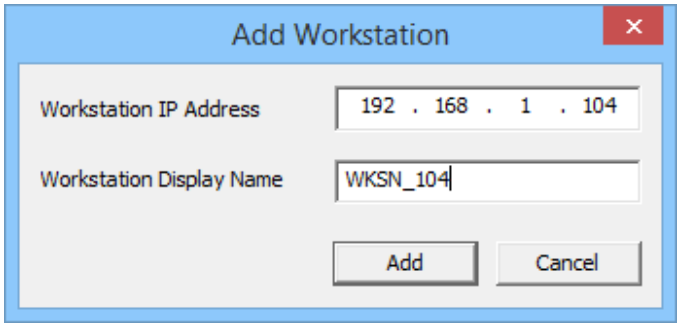


Complete the Workstation Display Client Configuration Page

The Workstation display client will show a new page, the **Complete the Workstation Display Client Configuration** page. This is where you add the workstation you want to transfer to the Terminal.

There are two options, using a physical workstation or a VCenter virtual workstation.

Select the ***Add Workstation*** button to add a physical workstation.



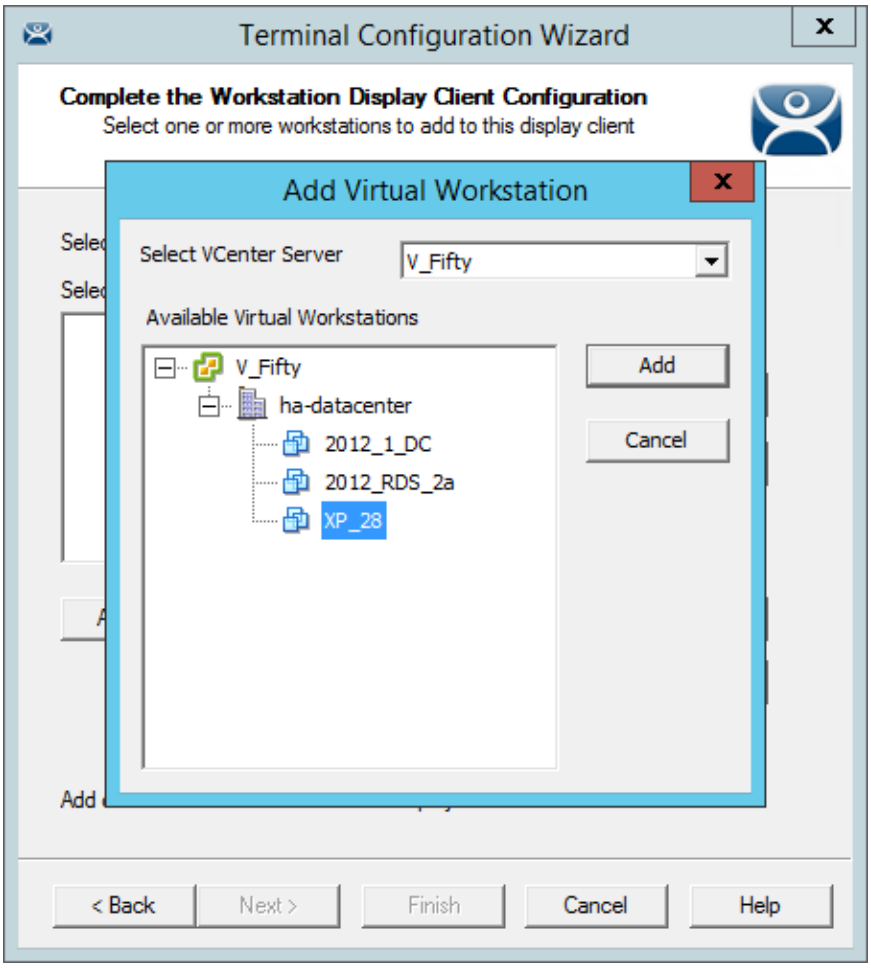
Add Workstation Window

The **Add Workstation** window allows you specify a workstation by IP address and name.

Enter the IP address and name in the ***Workstation IP Address*** field and the ***Workstation Display Name*** field.

You may also use this to point to a virtual workstation. Just add the virtual machine's IP address and name to the ***Workstation IP Address*** field and the ***Workstation Display Name*** field.

If your virtual machines are on a VCenter Server that is defined in ThinManager you can use the ***Add Virtual Workstation*** button.



Add Virtual Machine Window

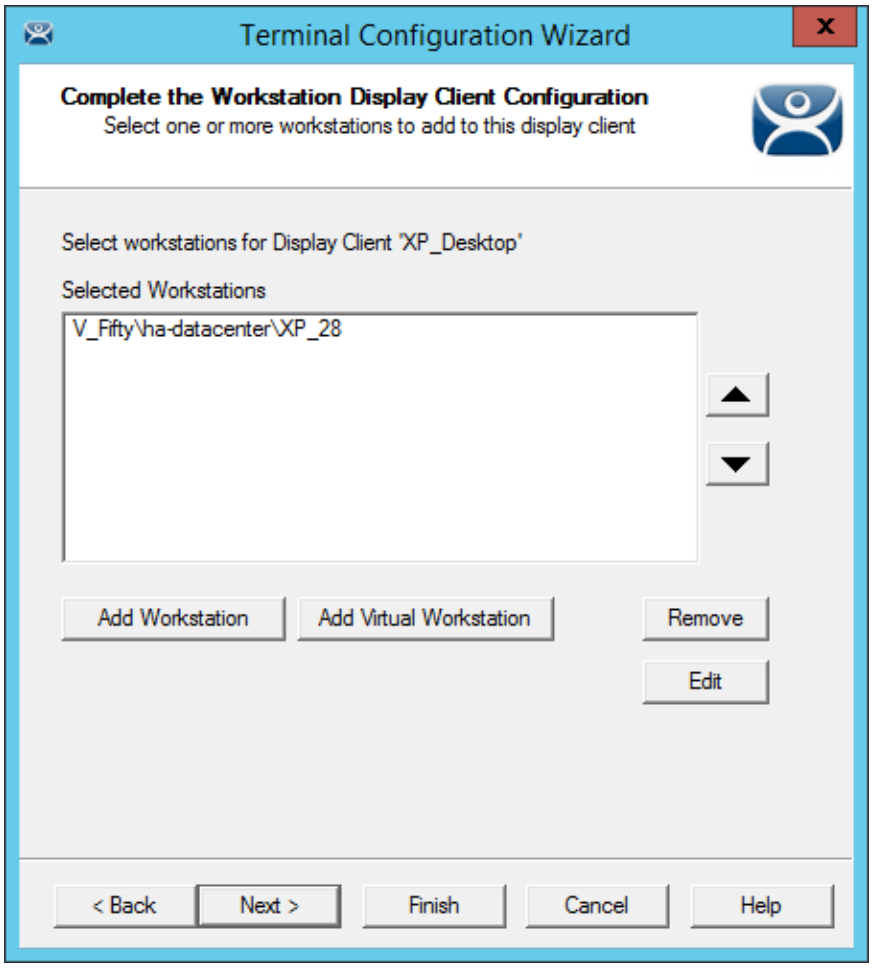
The ***Add Virtual Workstation*** button opens an **Add Virtual Workstation** window that is populated by any VCenter Servers you have defined in ThinManager.

Select the VCenter Server in the ***Select VCenter Server*** drop-down.

Expand the VCenter tree.

Highlight the desired virtual workstation and click the ***Add*** button.

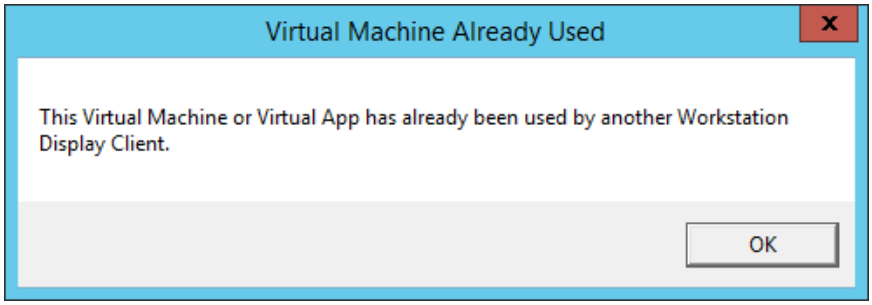
This will select the workstation.



Complete the Workstation Display Client Configuration Page

The workstation will be displayed in the ***Selected Workstations*** textbox on the **Complete the Workstation Display Client Configuration** page.

You can add a second workstation as a backup, if desired.

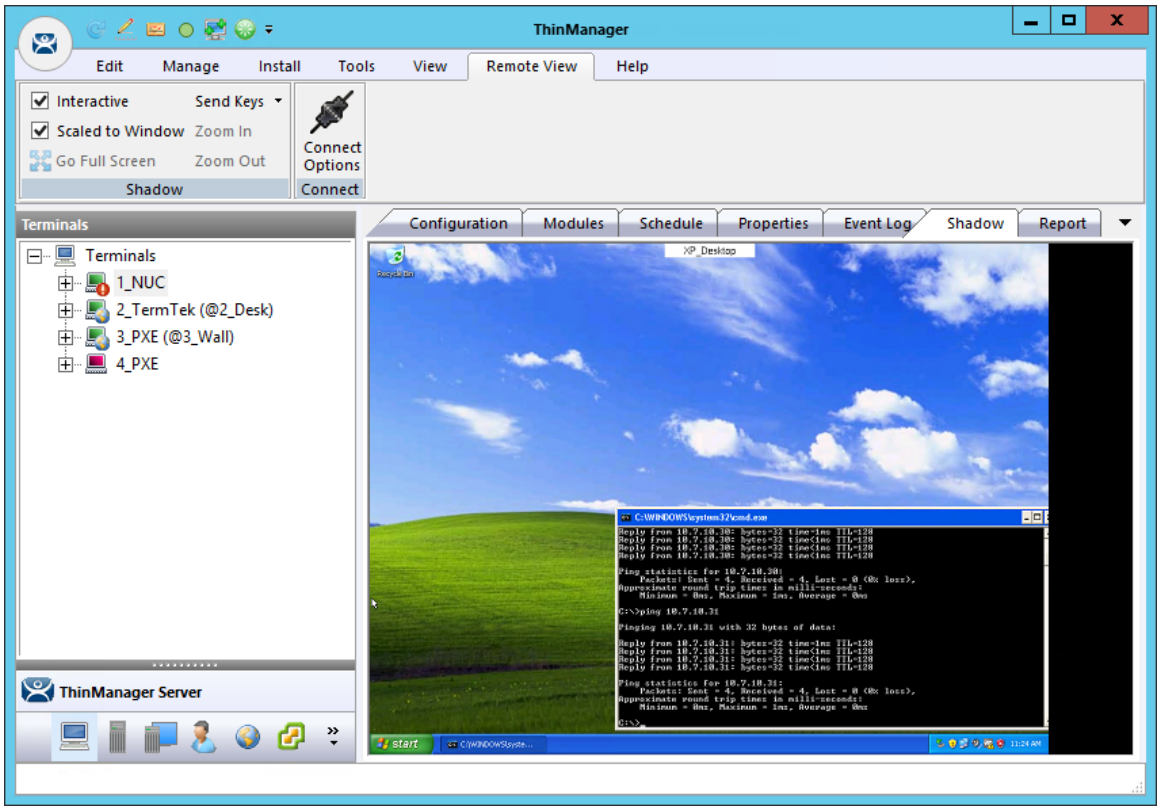


Duplicate Workstation Warning

Workstations can only have one connection to a remote user. They use a one-to-one model instead of the one-to-many model of Remote Desktop Services.

ThinManager has an error check system that prevents a workstation from being deployed twice.

Note: A workstation can be added multiple times as a backup but only once as the primary workstation.



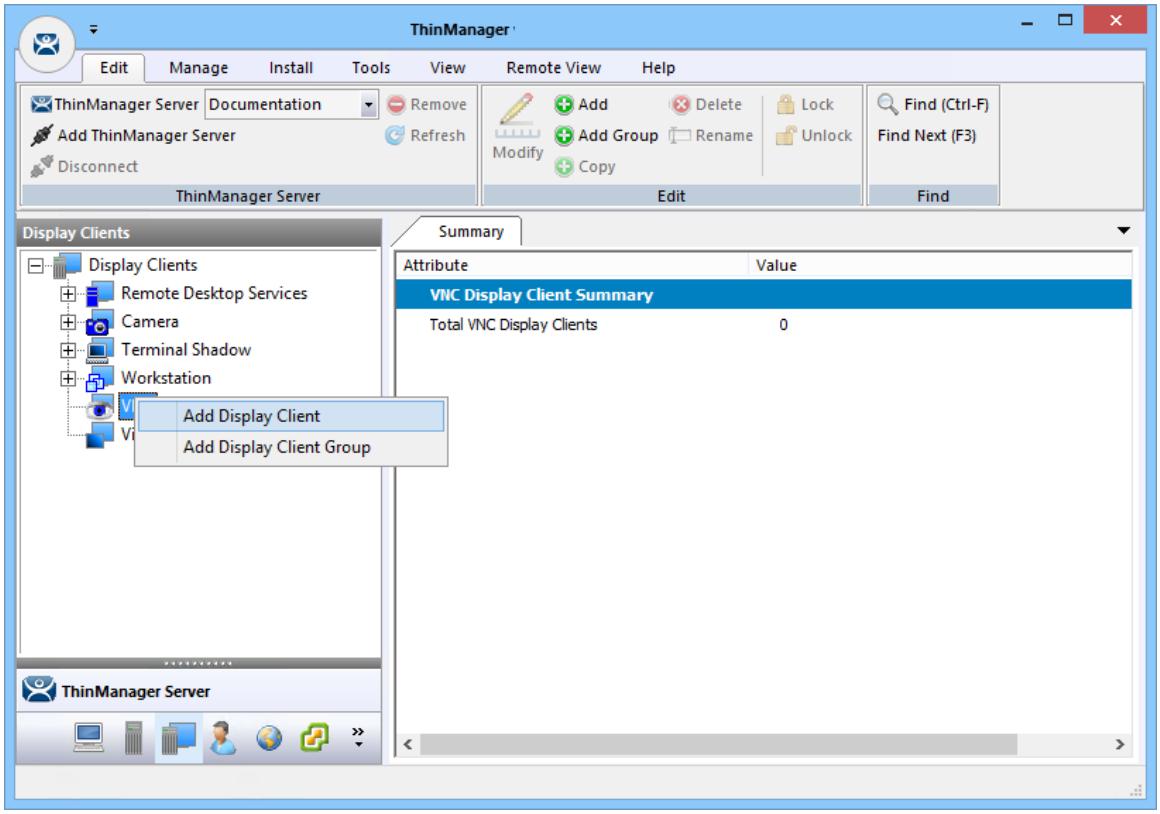
XP Workstation on a Thin Client

Once the Workstation Display Client is added to a Terminal and the Terminal is restarted the Terminal will connect to the workstation and transfer the workstation display to the Terminal.

17. Content – VNC Shadow

ThinManager can connect to a VNC Server and send the VNC shadow to a Terminal as a VNC Display Client. The first step is to define the VNC Server as a Display Server source as shown in Sources – VNC Server on page 87.

The second step is to create a Display Client to deploy the source on a client.

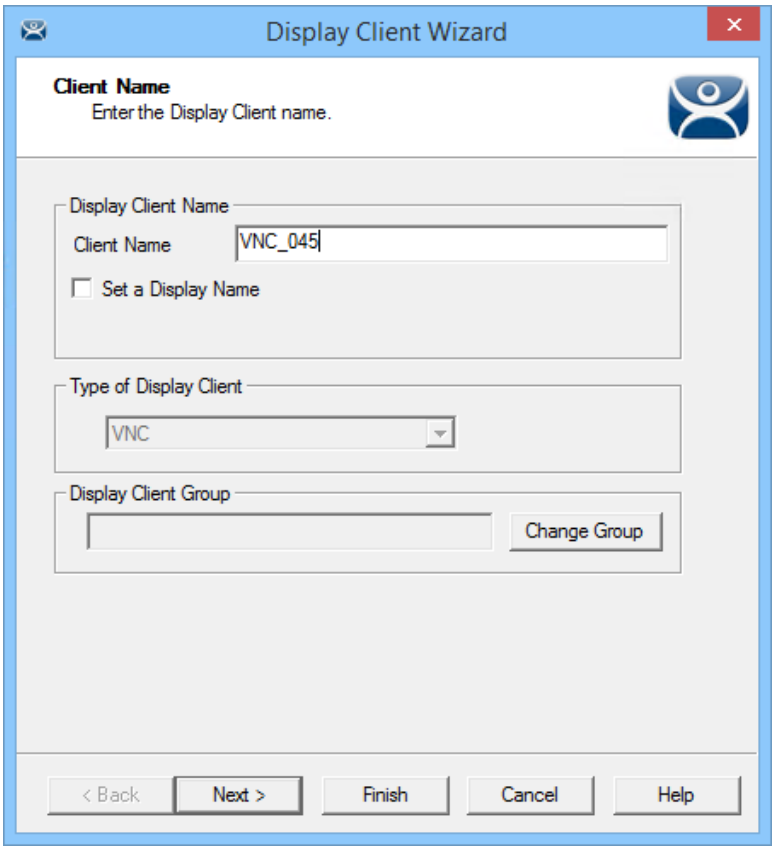


Display Client Tree of ThinManager

Launch the **Display Client Wizard** by right clicking on the **VNC branch** of the **Display Clients tree** and selecting ***Add Display Client***.

17.1. Shadow Any VNC Server

A VNC Display Client can be created that will allow the user to select from a list of all the VNC Servers.



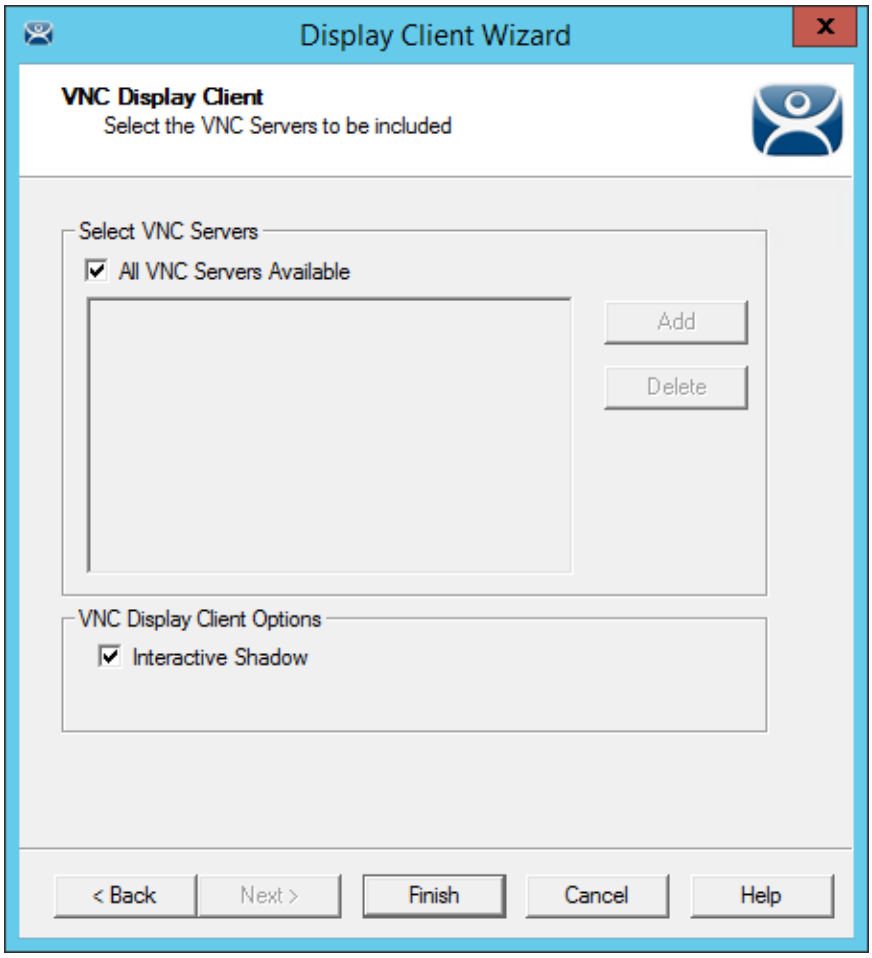
VNC Display Client Configuration Wizard

Right click on the **VNC branch** of the **Display Clients tree** and selecting ***Add Display Client*** will launch the Display Client wizard for Terminal Shadow.

Enter a name and follow the wizard like other display clients.

The ***Set a Display Name*** checkbox allows you to configure the display client to display an alternative name in the ThinManager Server tree.

The main setting is on the **VNC Display Client** page of the wizard.

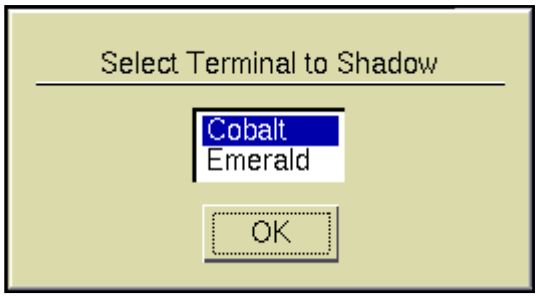


VNC Display Client Page of the Display Client Configuration Wizard

The default setting is to allow all VNC servers available for shadow. The interactive shadow can be turned off by un-selecting the ***Interactive Shadow*** checkbox.

Select the ***Finish*** button to create the display client.

Once the VNC Display Client is added to a Terminal and the Terminal is restarted the VNC Display Client will be available.



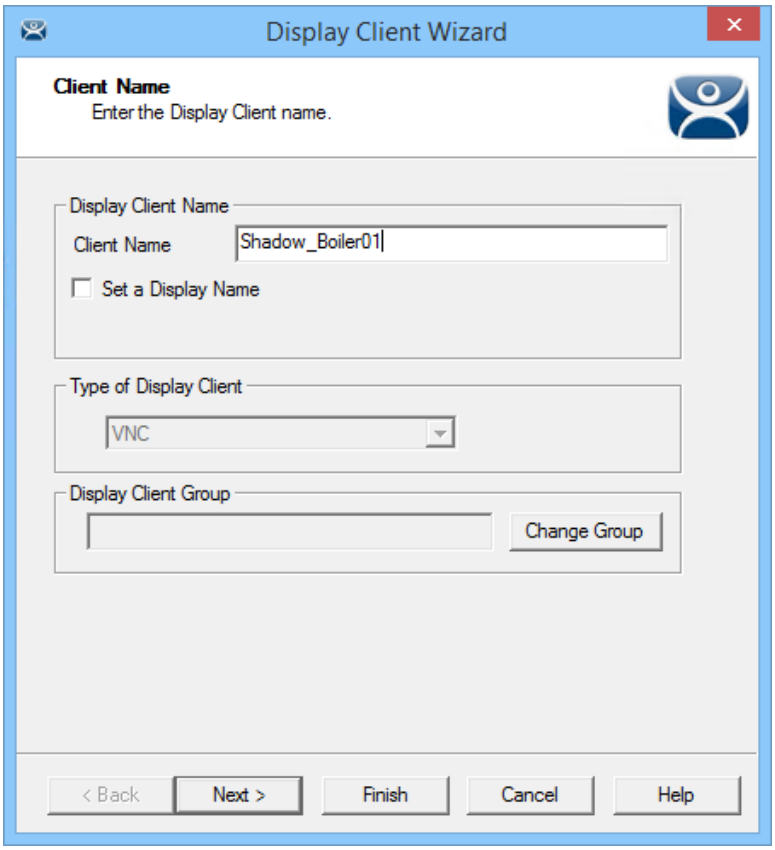
VNC Server Menu

When the user selects a VNC display client with multiple VNC servers add they will be presented with a menu listing all the available VNC servers. Highlight the desired VNC server and select the ***OK*** button.

The selected VNC server will be shadowed.

17.2. Shadow a Specific VNC Server

The VNC Display Client can be configured to show the output from a specific VNC server.



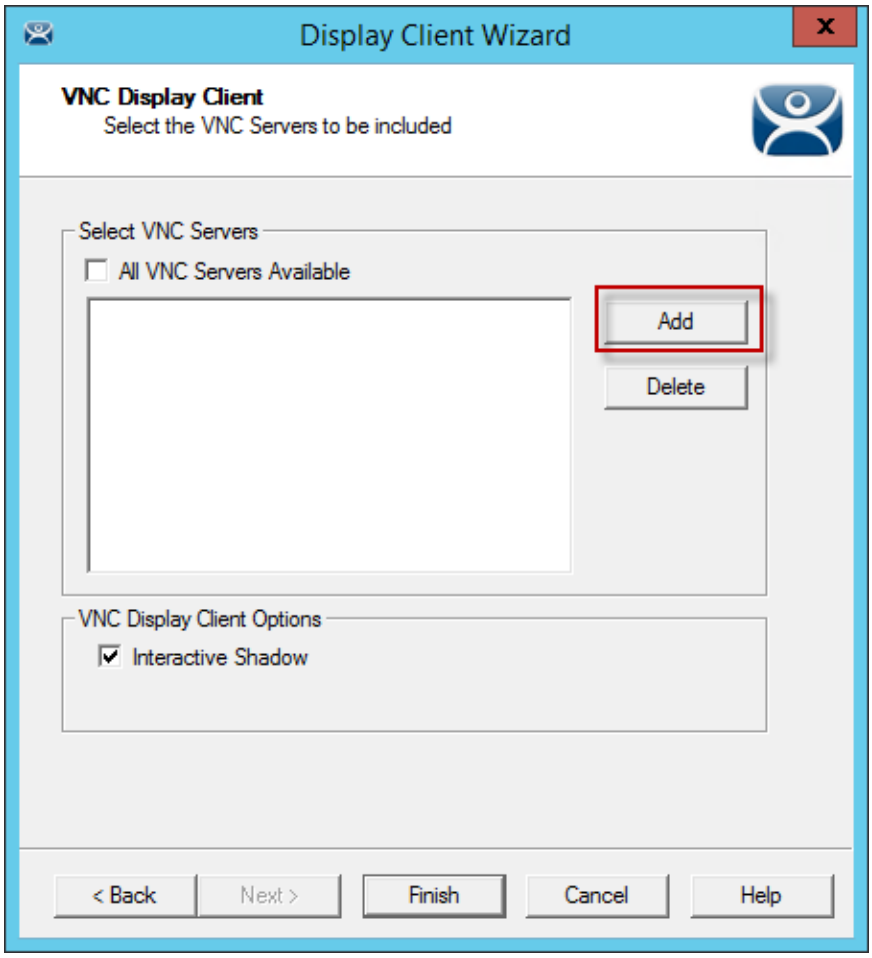
VNC Display Client Configuration Wizard

Right click on the **VNC branch** of the **Display Clients tree** and selecting ***Add Display Client*** will launch the Display Client wizard for Terminal Shadow.

The ***Set a Display Name*** checkbox allows you to configure the display client to display an alternative name in the ThinManager Server tree.

The ***Change Group*** button will allow the display client to be put in a Display Client Group.

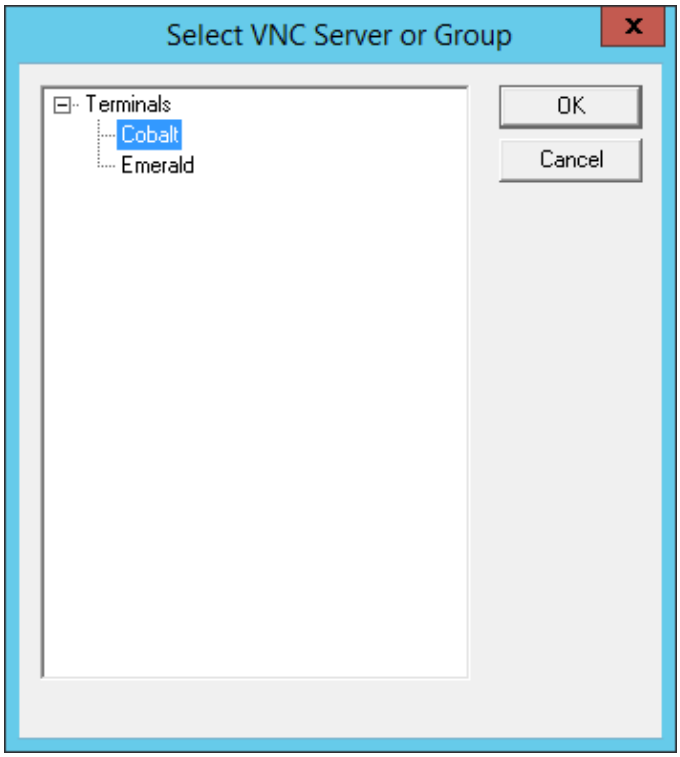
Enter a name and follow the wizard like other display clients.



VNC Display Client Page of the Display Client Configuration Wizard

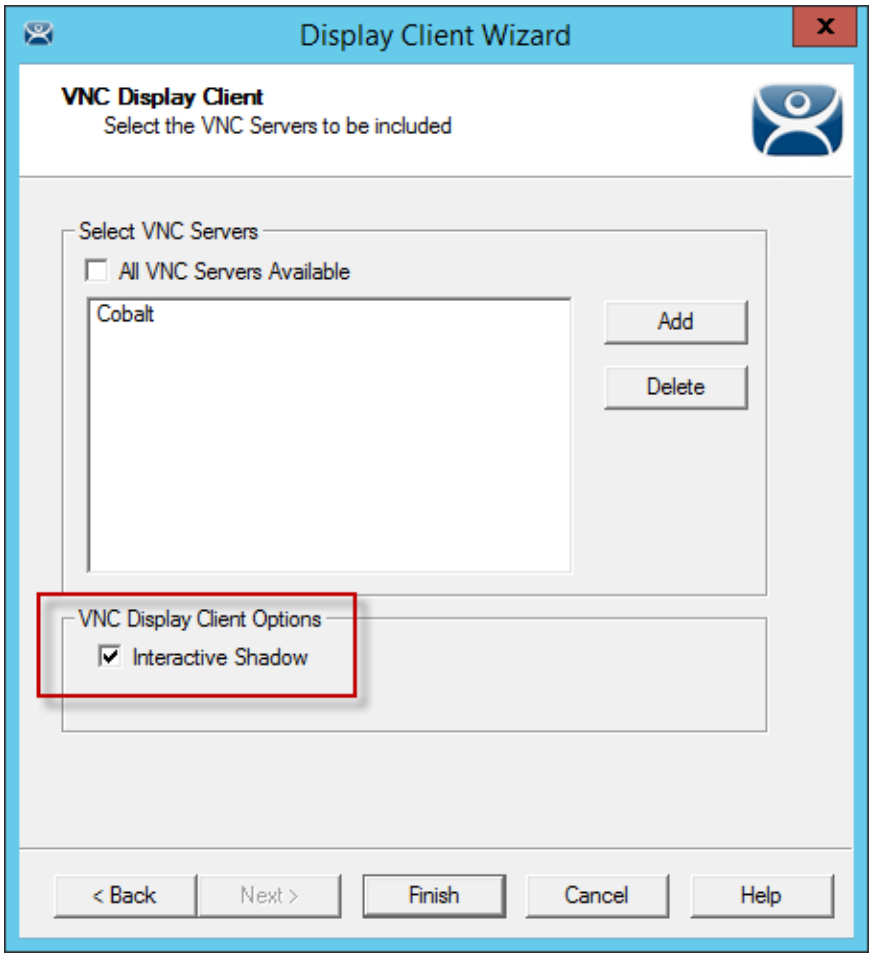
The default setting is to allow all VNC servers available for shadow. To pick a specific VNC server uncheck the ***All VNC Servers Available*** checkbox.

Select the ***Add*** button to launch the **Select VNC Server of Group** window.



Select VNC Server of Group Window

Highlight the VNC server you want to shadow and select the ***OK*** button. This will add the selected VNC server to the field and will close the **Select VNC Server of Group** window.



VNC Display Client Page of the Display Client Configuration Wizard

The VNC server will be added to the list to shadow. You may repeat the process by re-selecting the ***Add*** button and adding other VNC servers.

Select the ***Finish*** button to create the display client when done.

The interactive shadow can be turned off by un-selecting the ***Interactive Shadow*** checkbox. This will put the shadow in a “look but don’t touch” mode.

Once the VNC Display Client is added to a Terminal and the Terminal is restarted the VNC Display Client will be available.

If you have a single VNC server listed the display client will automatically show you that shadow. If you add multiple VNC servers to the list the VNC display client will present the menu with all the listed servers in it.

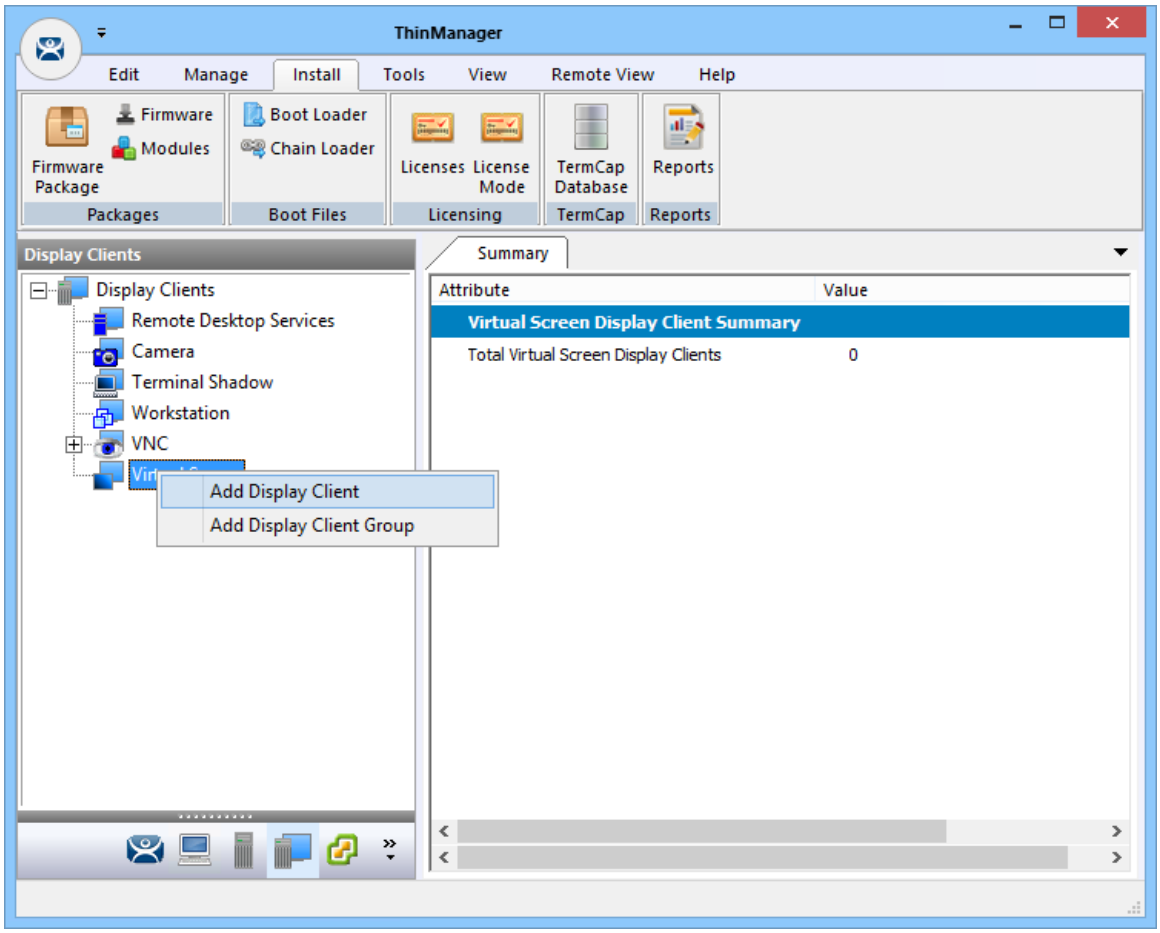
18. Content – Virtual Screens

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.

18.1. Virtual Screen Display Client Wizard

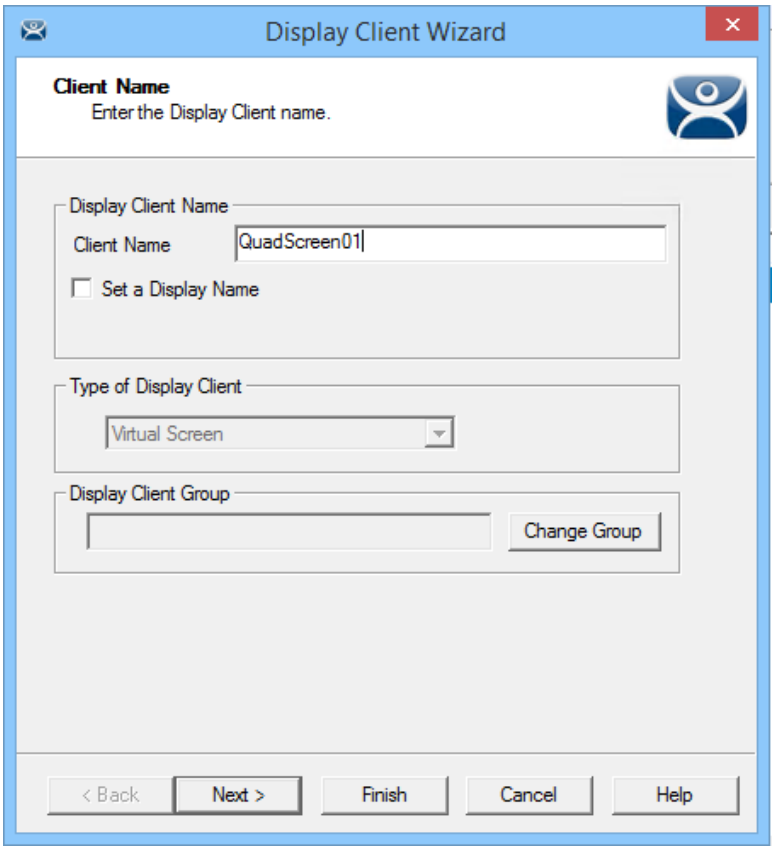
Virtual Screens are defined using the **Display Client Configuration Wizard**. It is launched by selecting the **Display Client icon** at the bottom of the ThinManager tree, right clicking on the **Virtual Screen** branch, and selecting ***Add Display Client***.



Launch the Virtual Screen Wizard

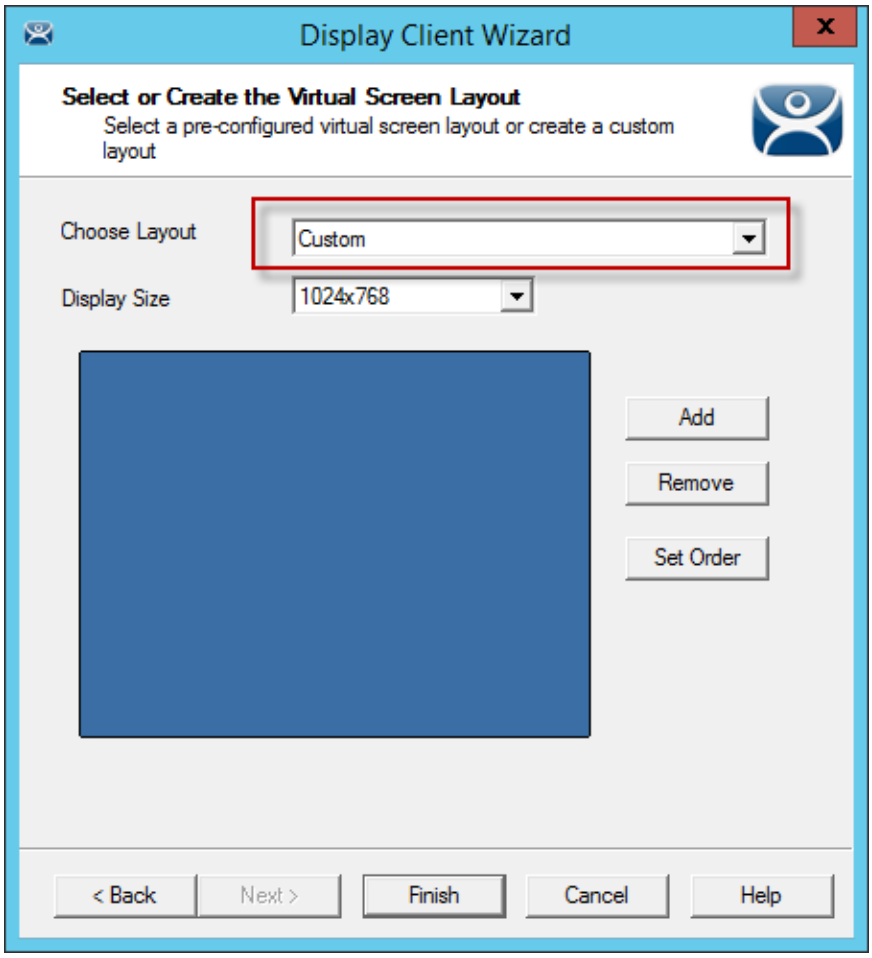
Name your display client by entering a name in the ***Client Name*** field.

Select the ***Next*** button to continue.



Client Name Page of the Display Client Configuration Wizard

The wizard starts like the **Remote Desktop Services Display Client Wizard** but changes at the **Select or Create the Virtual Screen Layout** page.



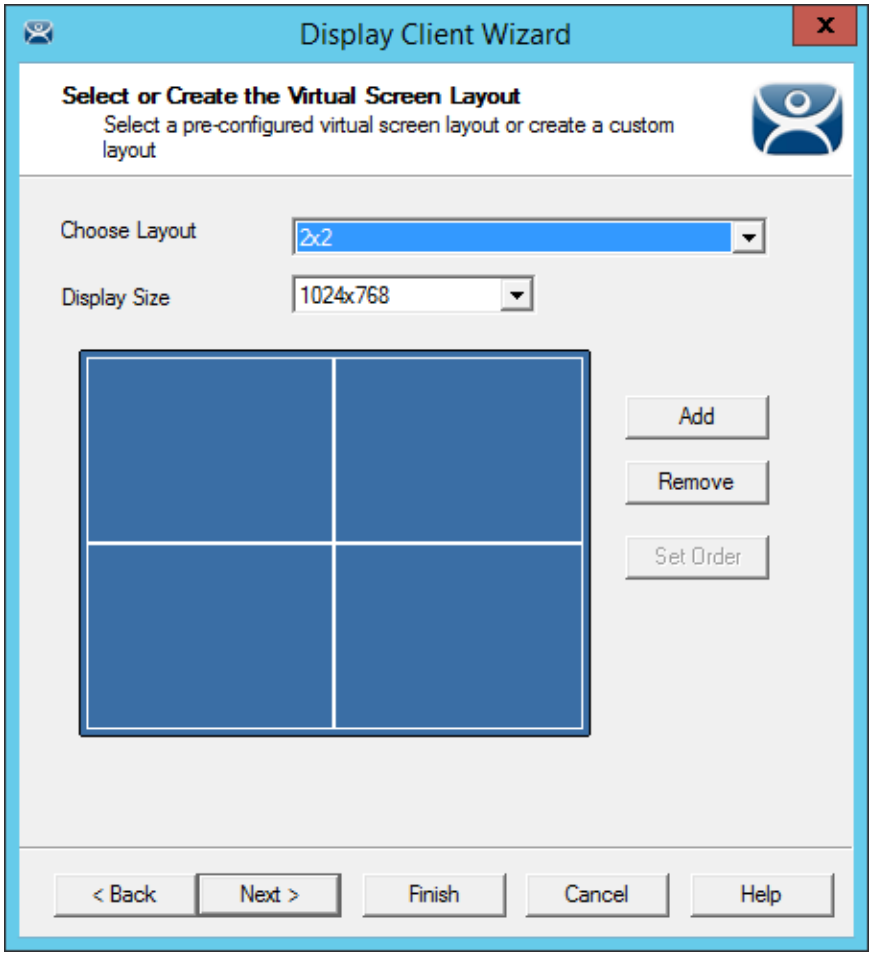
Select or Create the Virtual Screen Layout Page

The **Select or Create the Virtual Screen Layout** page has a ***Choose Layout*** drop-down that allows you to create custom overlays or to use pre-defined templates.

Custom Overlays are covered in Custom Overlays on page 210.

Pre-Defined Templates are covered in Pre-Defined Templates on page 198.

18.2. Pre-Defined Templates



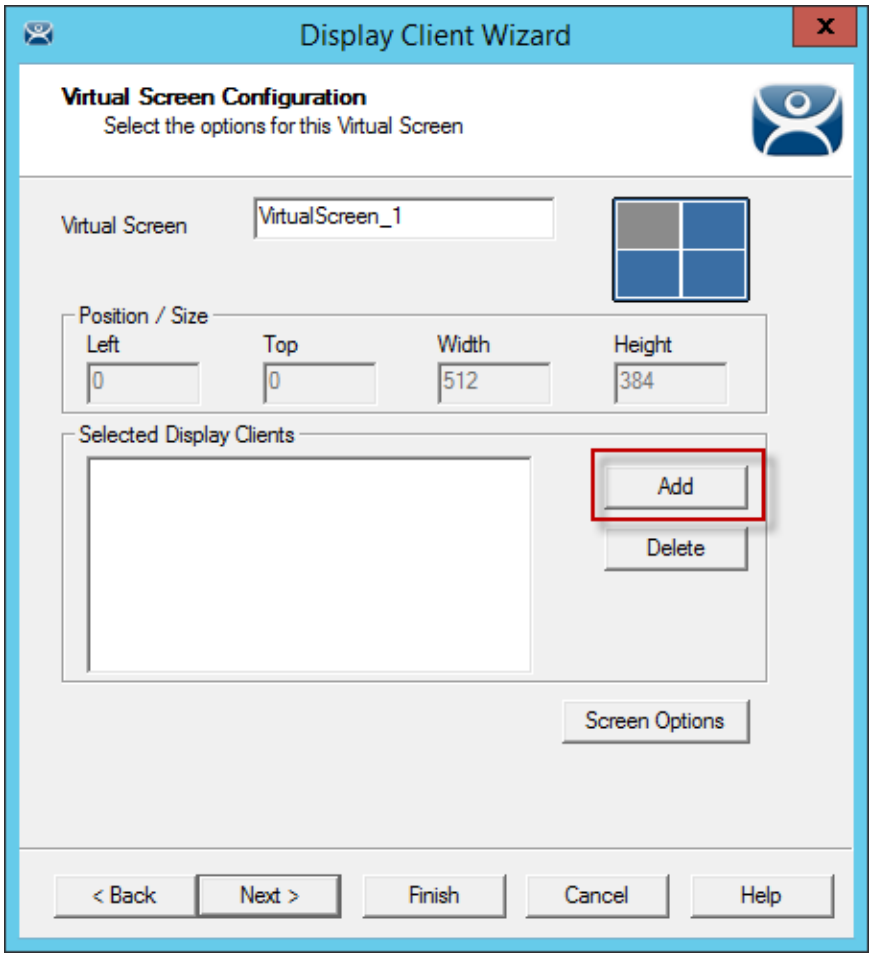
Select or Create the Virtual Screen Layout Page

The ***Choose Layout*** drop-down has a number of pre-defined templates that allow you to add anywhere from one to sixteen virtual screens

Select a pre-defined template from the ***Choose Layout*** drop-down.

Set the desired display resolution in the ***Display Size*** drop-down.

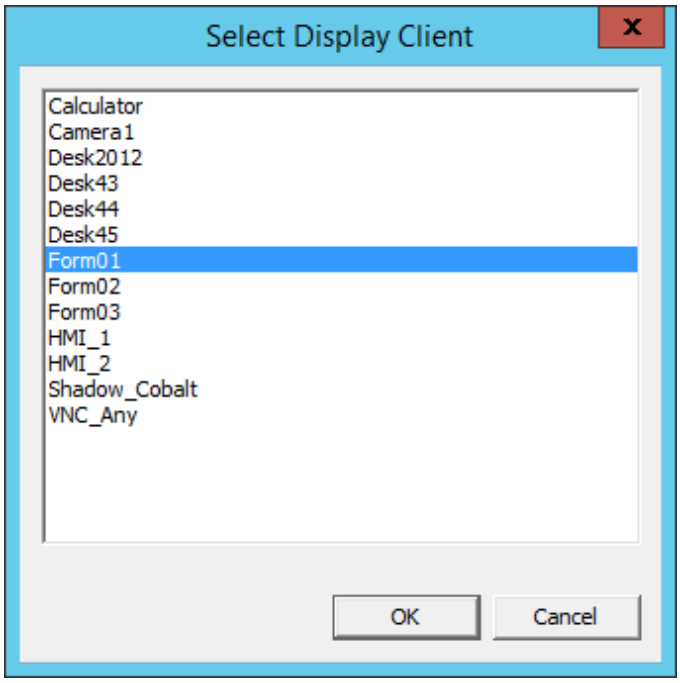
Select the ***Next*** button to continue.



Virtual Screen Configuration Page

The wizard will allow display clients to be added to each overlay just as the Camera Display Client Wizard allows you to add a camera to each overlay.

Select the ***Add*** button to add a Display Client to the overlay.

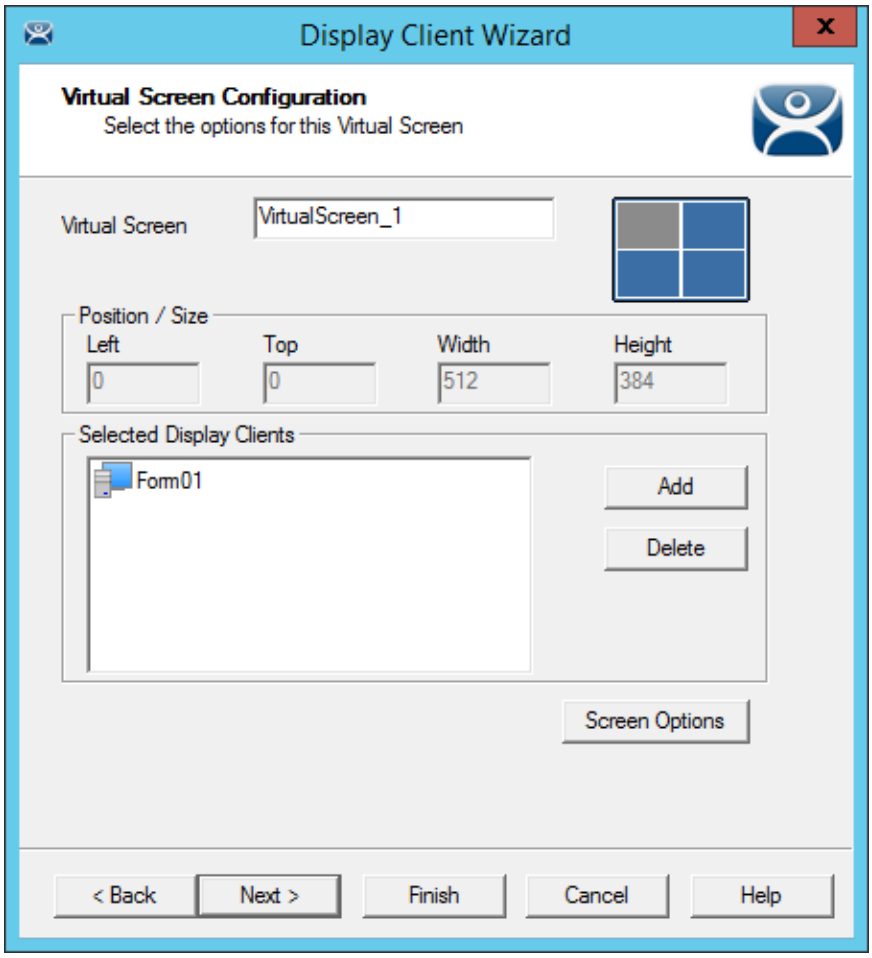


Select Display Client Dialog

A **Select Display Client** dialog will be displayed listing all the display clients.

Highlight the desired Display Client and select the ***OK*** button.

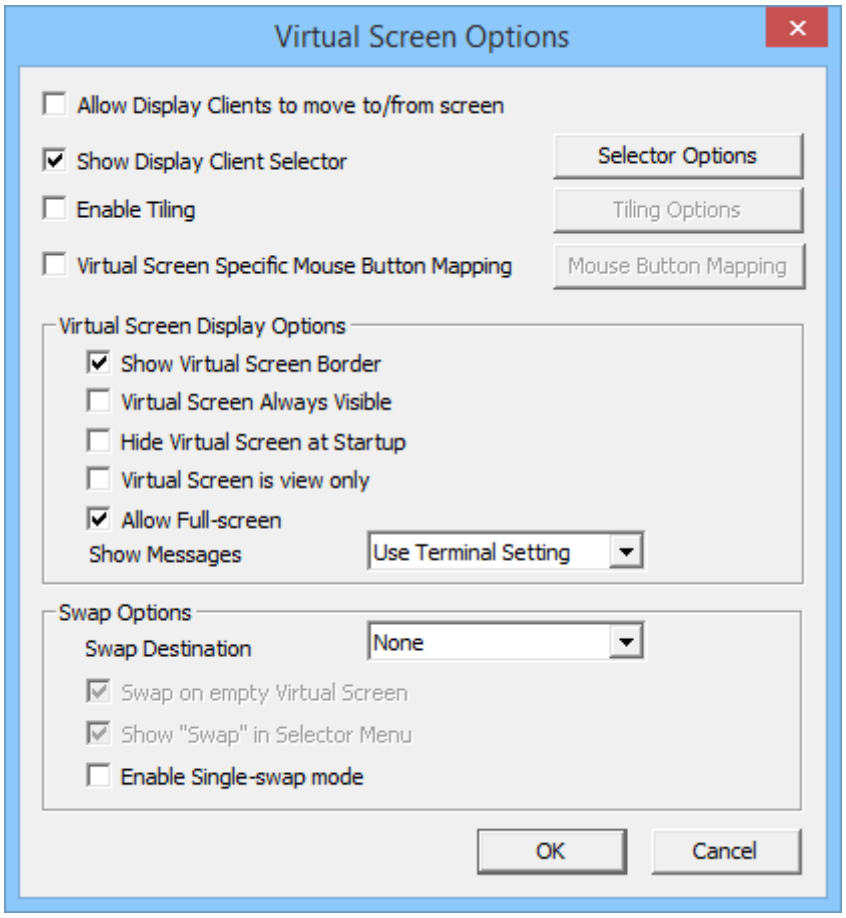
Repeat as needed for that overlay.



Virtual Screen Configuration Showing Applied Display Client

Each overlay may have one or more display clients in the overlay. Select the ***Add*** button to add more display clients.

You may apply virtual screen options by highlighting a display client and selecting the ***Screen Options*** button.



Virtual Screen Options

The Virtual Screen Overlay has several options:

- ***Allow Display Clients to move to/from screen*** – This allows you to move a display client from one overlay to the other much like you can move display clients between monitors on a MultiMonitor thin client.
- ***Show Display Client Selector*** – This shows the drop-down selector at the top of the overlay. It can be configured by clicking the ***Selector Option*** button.
- ***Enable Tiling*** – This will allow tiling of Display Clients within the overlay if you have multiple display clients.
- ***Virtual Screen Specific Mouse Button Mapping*** – This enables the opening of the Mouse Button Mapping window to configure the mouse with use with the Virtual Screens.

Virtual Screen Display Options

- ***Show Virtual Screen Border*** – This will show a border between the overlays.
- ***Virtual Screen Always Visible*** – This will make this specific overlay “always visible’. If the user switches to a different display client this overlay will still be visible even though its display client is hidden.
- ***Hide Virtual Screen at Startup*** – This setting hides the Virtual Screen at start up. It is intended to be used with the TermMon ActiveX that will toggle the overlay visibility.
- ***Virtual Screen is view only*** – This will display the Display Client in the Virtual Screen but make it view only, and not interactive.

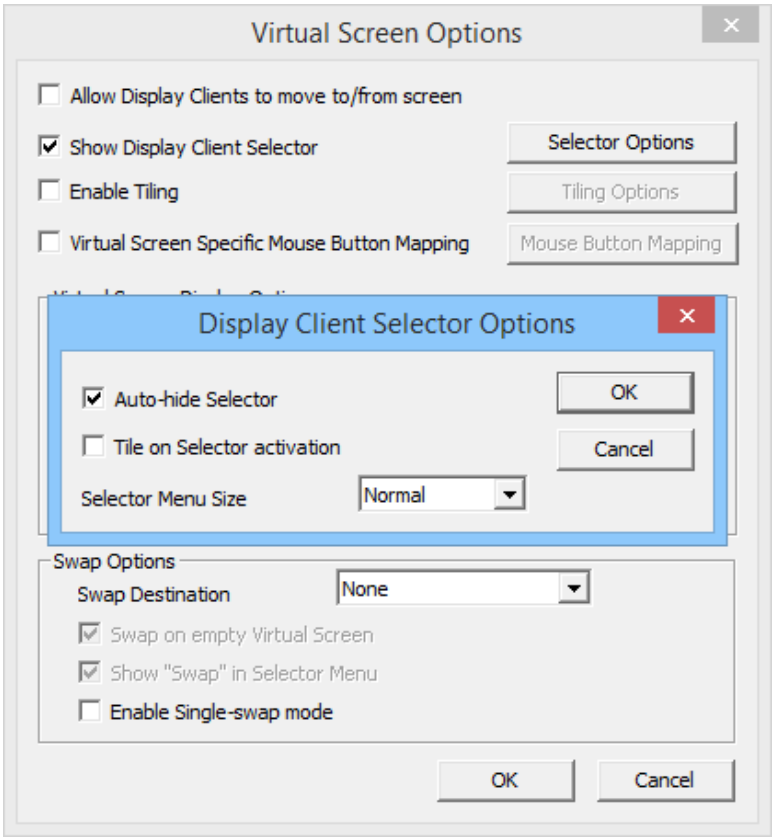
- ***Allow Full-screen*** – This allows a Display Client to go full screen and not show the sidebar Virtual Screens.
- ***Show Messages*** – This drop-down allows you to control the status message shown in the upper left corner of the Terminal display
    - ***Use Terminal Setting*** – This sets the Virtual Screen to follow the configuration of the Terminal.
    - ***Yes*** – This turns on the status messages.
    - ***No*** – This turns off the messages.

Swap Options – This control where the Display Clients will move, or swap, when selected.

- ***Swap Destination*** – This drop-down allows you to specify where you want the Virtual Screen moved during a swap.
- ***Swap on empty Virtual Screen*** – This will move the highlighted Virtual Screen to an empty Virtual Screen when selected from the drop-down Selector..
- ***Show "Swap" in Selector Menu***– This adds the Swap option to the drop-down Selector menu..
- ***Enable Single-swap mode*** – This allows a single mouse click in a Virtual Screen window to initiate the swap..

Select the ***Selector Option*** button to configure the selector options.

Select ***OK*** to accept changes and continue.



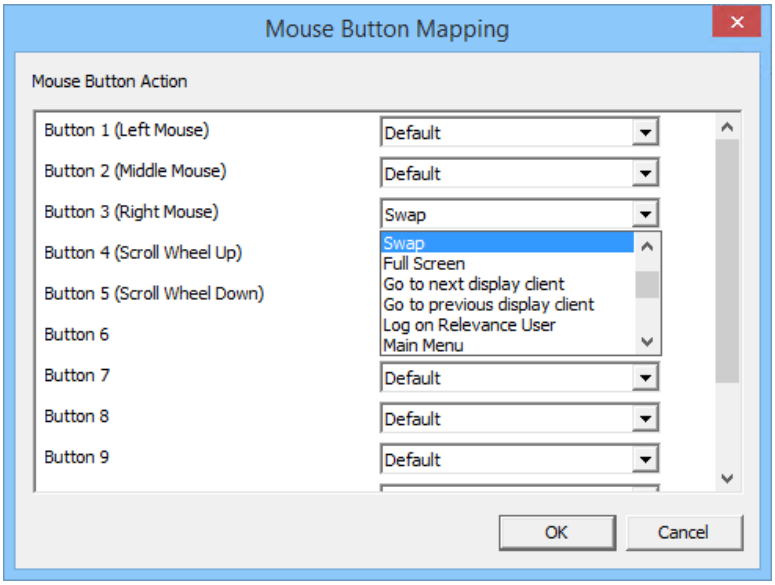
Display Client Selection Options

Selecting the ***Selector Options*** button will open the **Display Client Selector Options** dialog.

- ***Auto-hide Selector*** – This checkbox hides the selector until the mouse is positioned over it. Uncheck this to show the selector at all times.
- ***Tile on Selector activation*** – This checkbox adds the Tiling command to the drop-down menu.
- ***Selector Menu Size*** – This allows you to adjust the font size of the selector.

Select ***OK*** to close the **Display Client Selector Options** dialog.

Selecting the ***Virtual Screen Specific Mouse Button Mapping*** checkbox will activate the ***Mouse Button Mapping*** button.



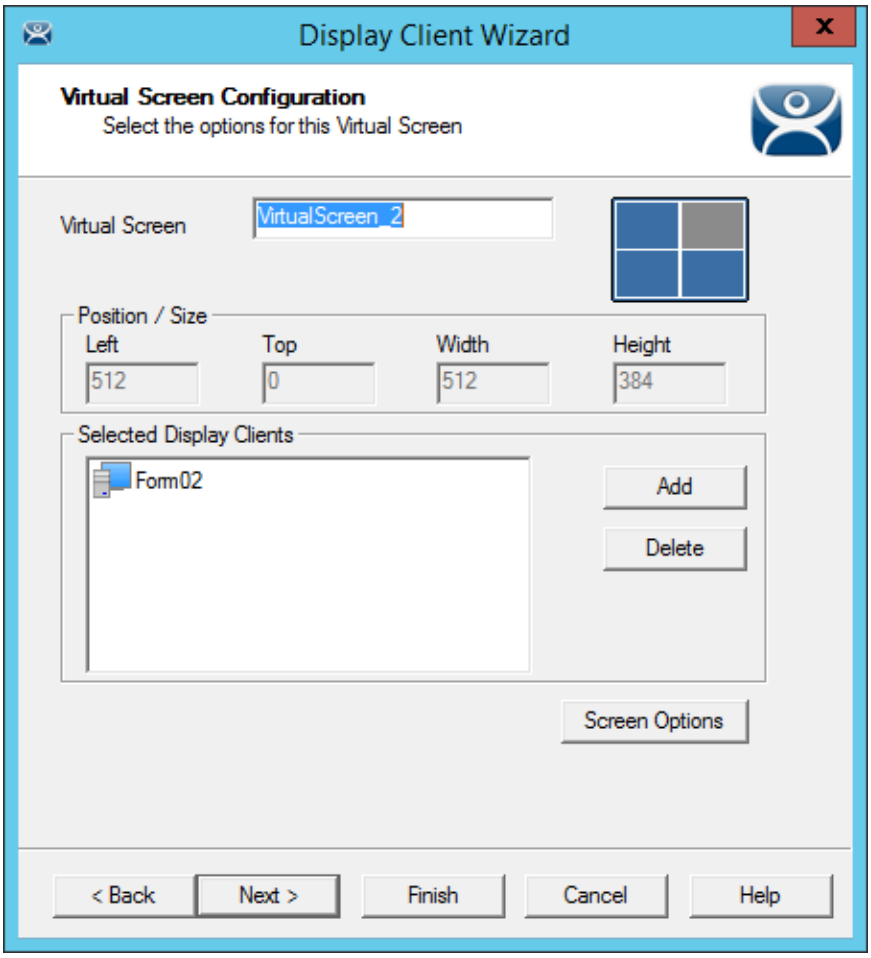
Mouse Button Mapping Window

The Mouse Button Mapping window is opened by selecting the to configure the ***Mouse Button Mapping*** button.

Each mouse button can be configured with a different function Swap is useful to initiate the swapping of Virtual Screens.

Use the ***Button 1 (Left Mouse)*** for touch screens without a mouse.

Select ***Next*** to continue to the next overlay once all the dialog windows are closed.



Virtual Screen Configuration Page

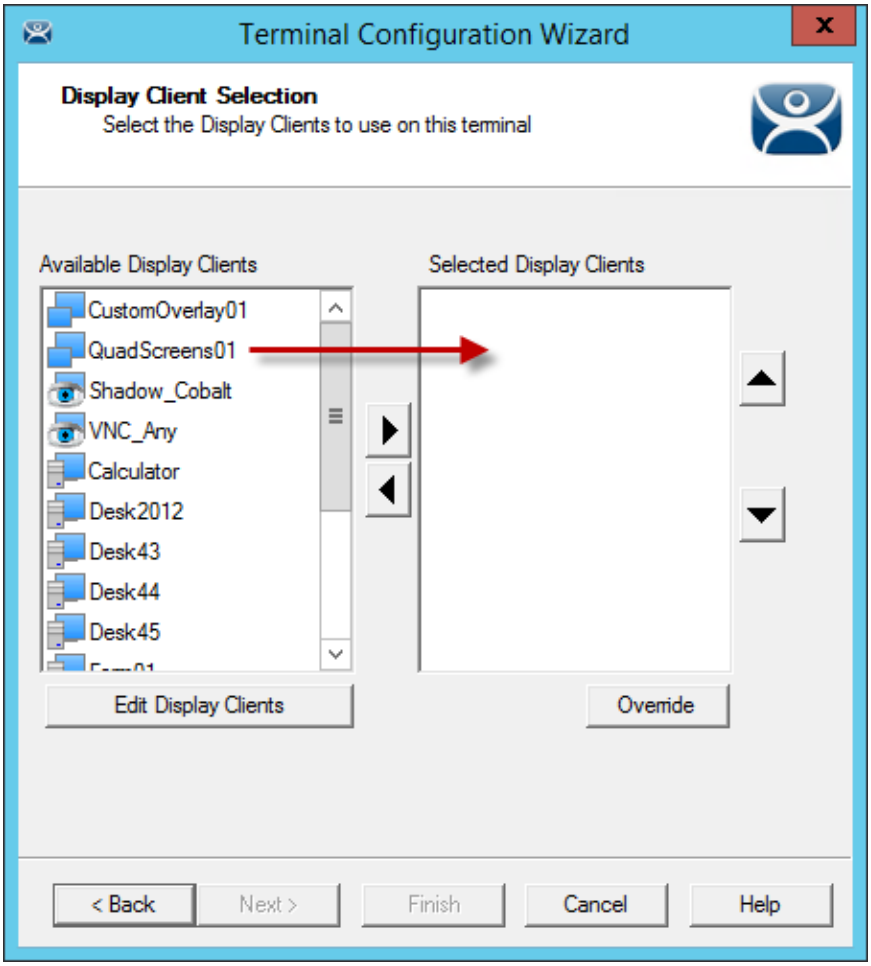
The Display Client wizard will navigate from overlay to overlay allowing you to add display clients to each one.

Select the ***Finish*** button when the configuration is done.

18.3. Adding a Virtual Screen to a Terminal

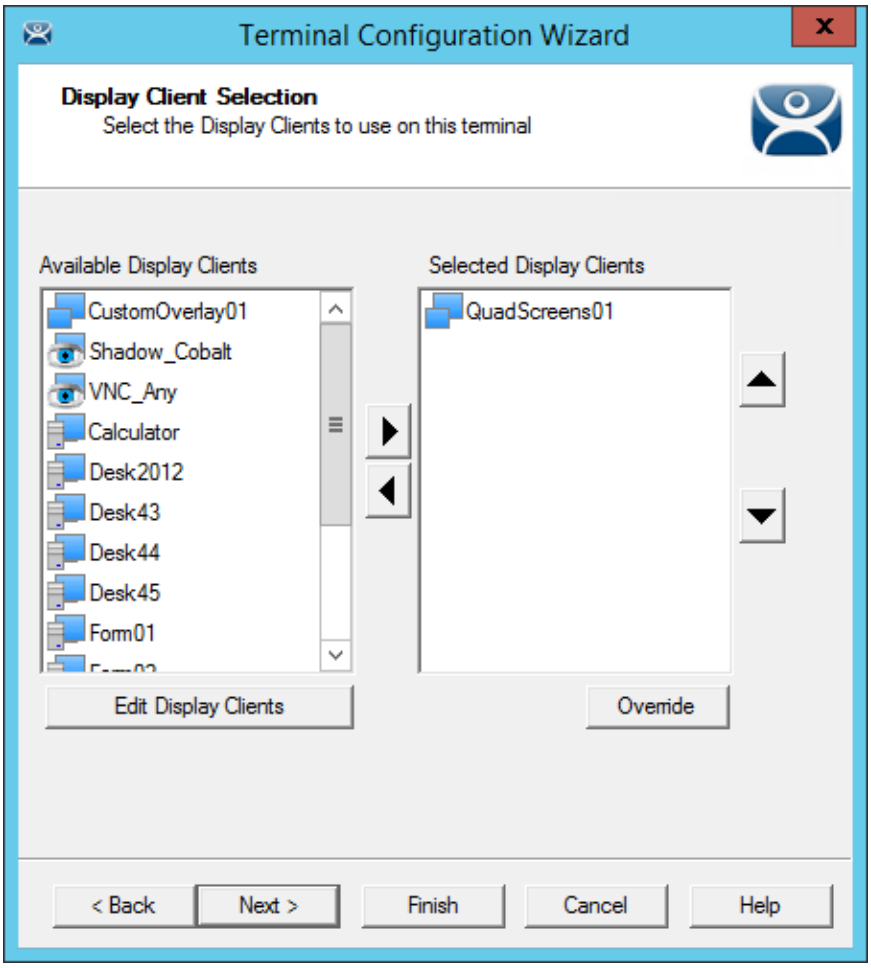
Virtual Screen Display Clients are added to a Terminal the same as any other Display Client.

Open the **Terminal Configuration Wizard** by double clicking on the Terminal in the Terminal tree and navigate to the **Display Client Selection** page.



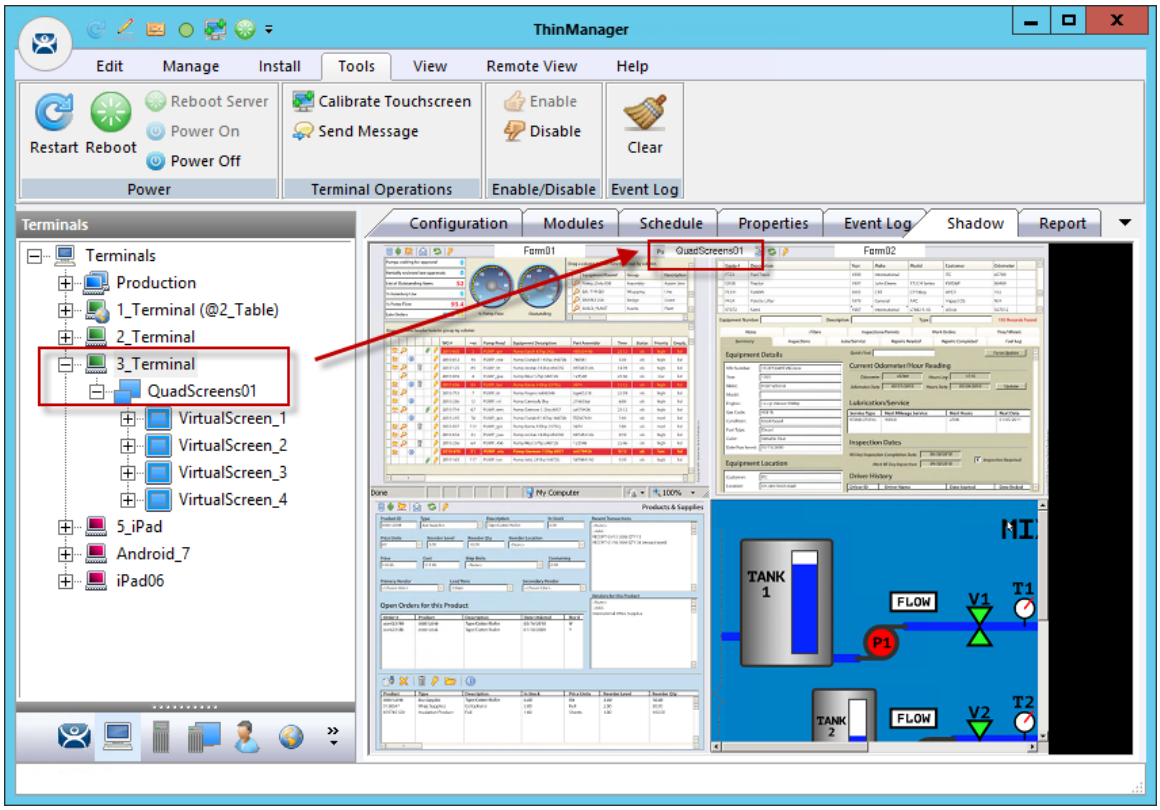
Display Client Selection Page of the Terminal Configuration Wizard

The Virtual Screen display client can be moved to the ***Selected Display Client*** list by double clicking or by highlighting and using the right arrow.



Selected Display Clients

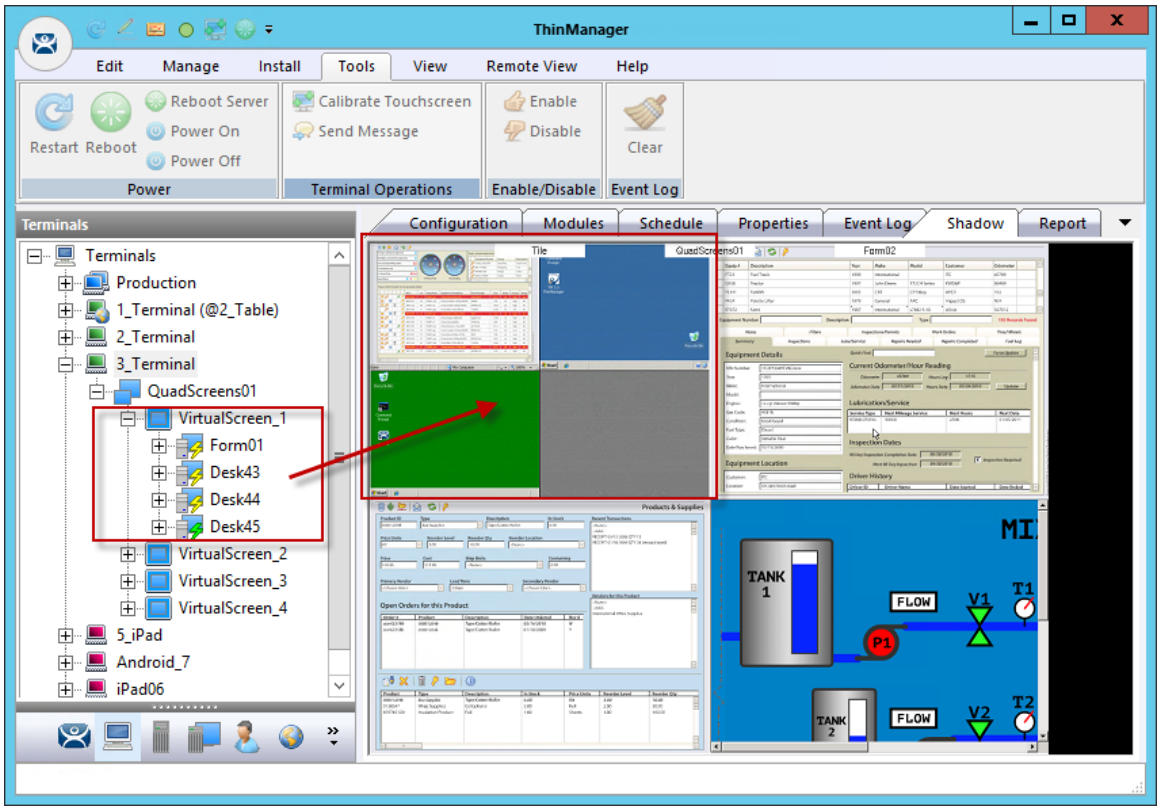
Once the Virtual Screen Display Client is in the ***Selected Display Clients*** list it is added to the Terminal. Select Finish and restart the Terminal to apply the change.



Virtual Screen on the Terminal

This picture shows the QuadScreen01 Virtual Screen Display Client on a Terminal.

The screen has four virtual screens added and showing.



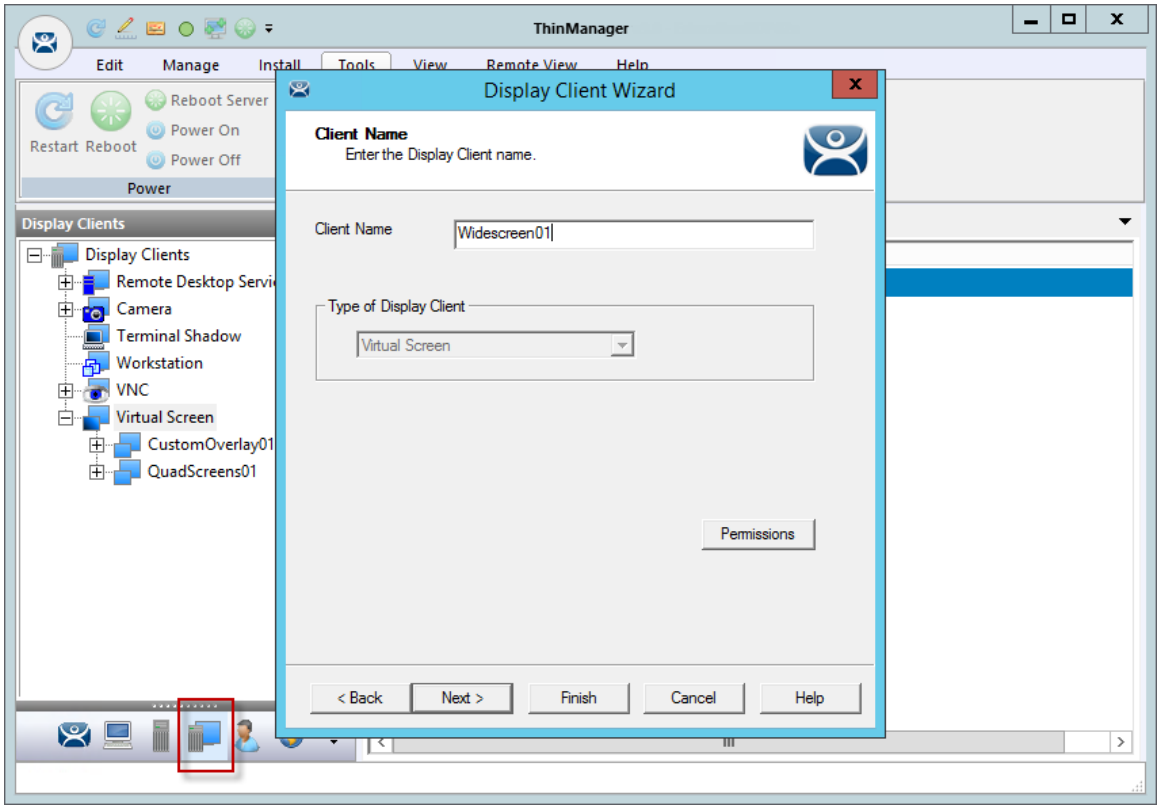
Tiling within an Overlay

If ***Enable Tiling*** is selected on the **Virtual Screen Options** page then the display clients in an overlay will be tiled as shown in this example.

18.4. Custom Overlays

ThinManager provides the option of building and defining custom overlays instead of using the pre-defined templates.

This section will show the example of a custom Virtual Screen display client with 4 custom overlays.

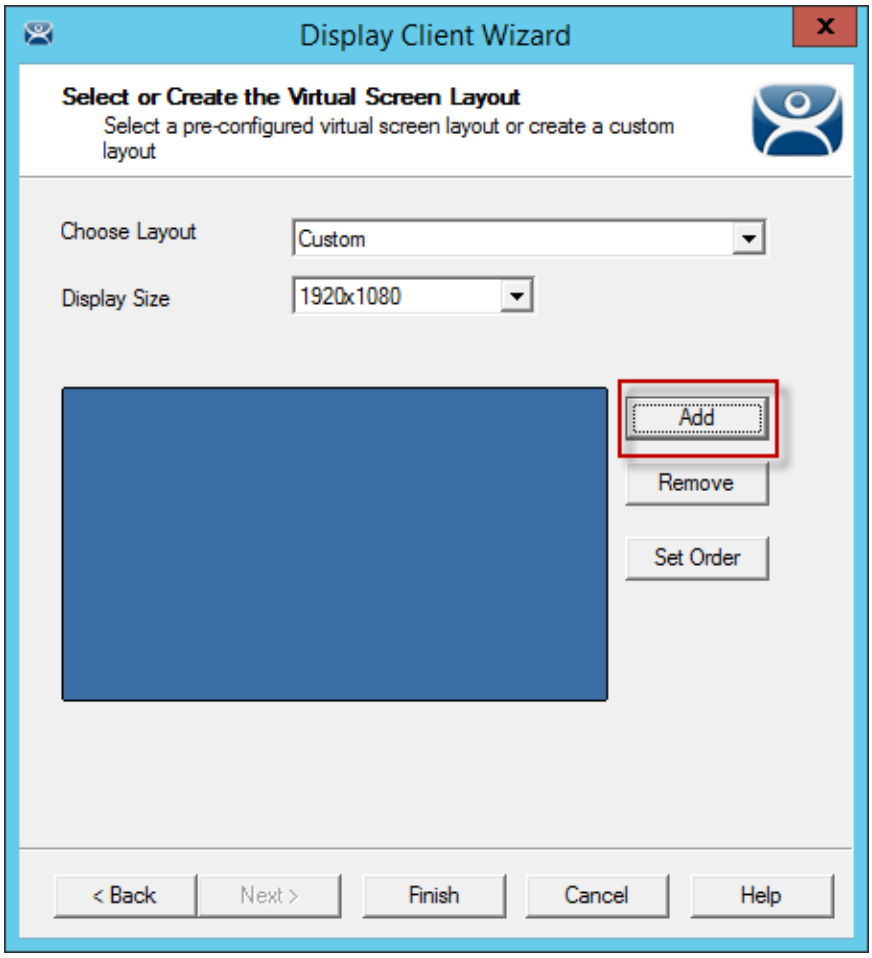


Display Client Wizard for Virtual Screens

Virtual Screens are defined using the **Display Client Configuration Wizard**. It is launched 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***.

Name your display client by entering a name in the ***Client Name*** field.

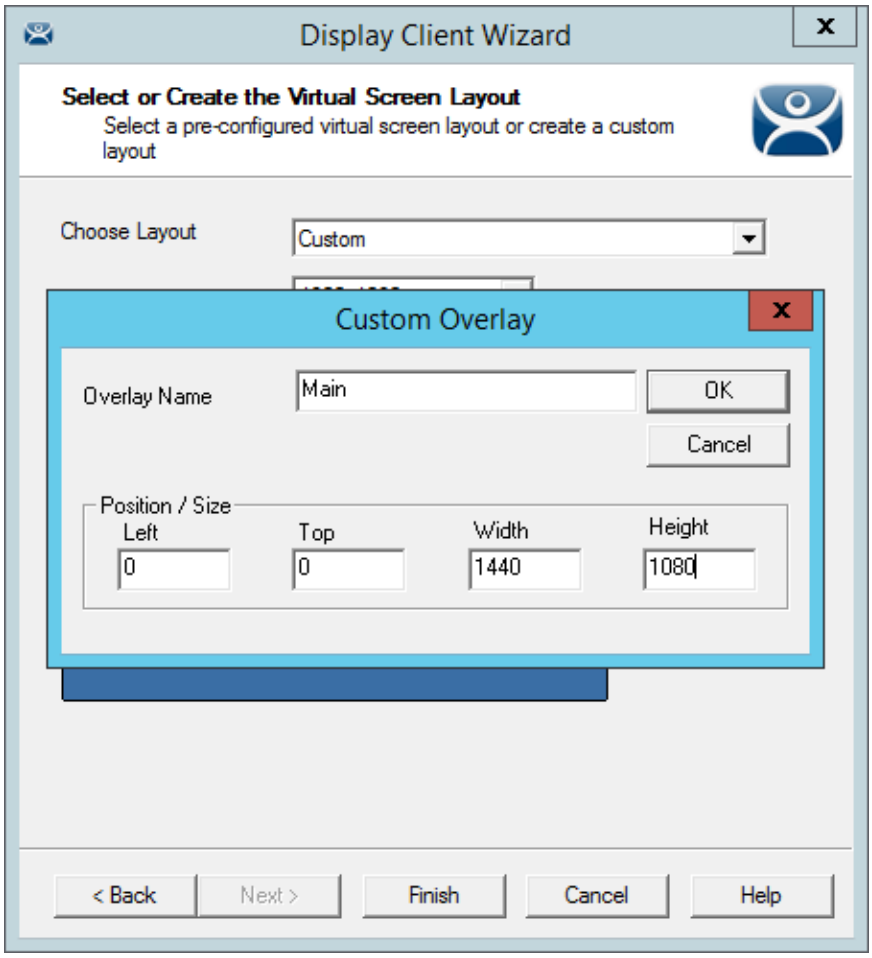
Select the ***Next*** button to continue.



Custom Overlay Layout

The initial Virtual Screen is a blank canvas and needs at least one overlay added.

Select the ***Add*** button to launch the **Custom Overlay** window.



Custom Overlay Layout

The **Custom Overlay** window has a few settings to set the size and location of the custom overlay.

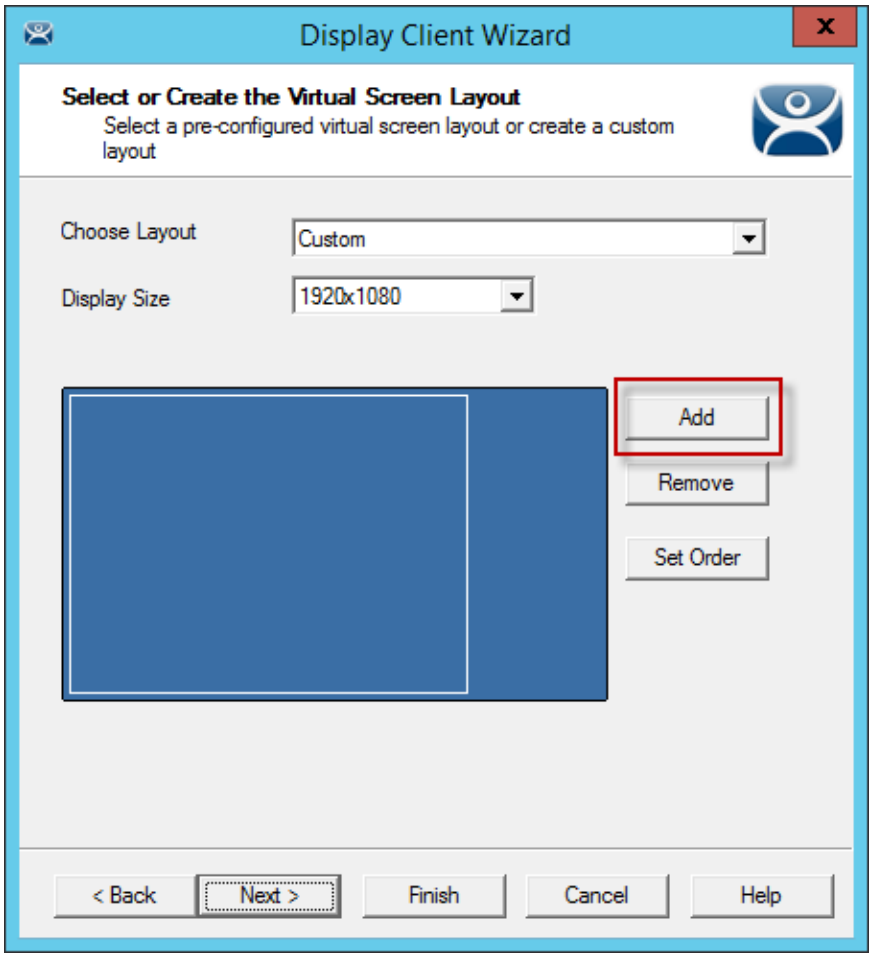
- ***Overlay Name*** – The overlay needs a name in the Overlay Name field.

Position/Size – The overlay needs to have the co-ordinate of its top left corner defined and its size defined. The top left corner of the Virtual Screen is “0,0”.

- ***Left*** – This sets the positon of the left edge of the overlay.
- ***Top*** – This sets the positon of the top edge of the overlay
- ***Width*** – This sets the width of the overlay.
- ***Height*** - This sets the height of the overlay,

This example is creating a 1440x1080 overlay that is touching the upper left corner.

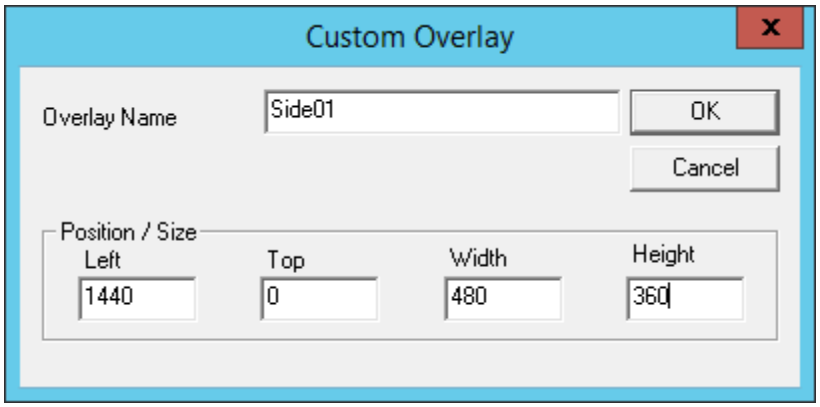
Click the ***OK*** button to accept the settings.



Created Overlay

The created Overlay is shown in **Overlay** window when done.

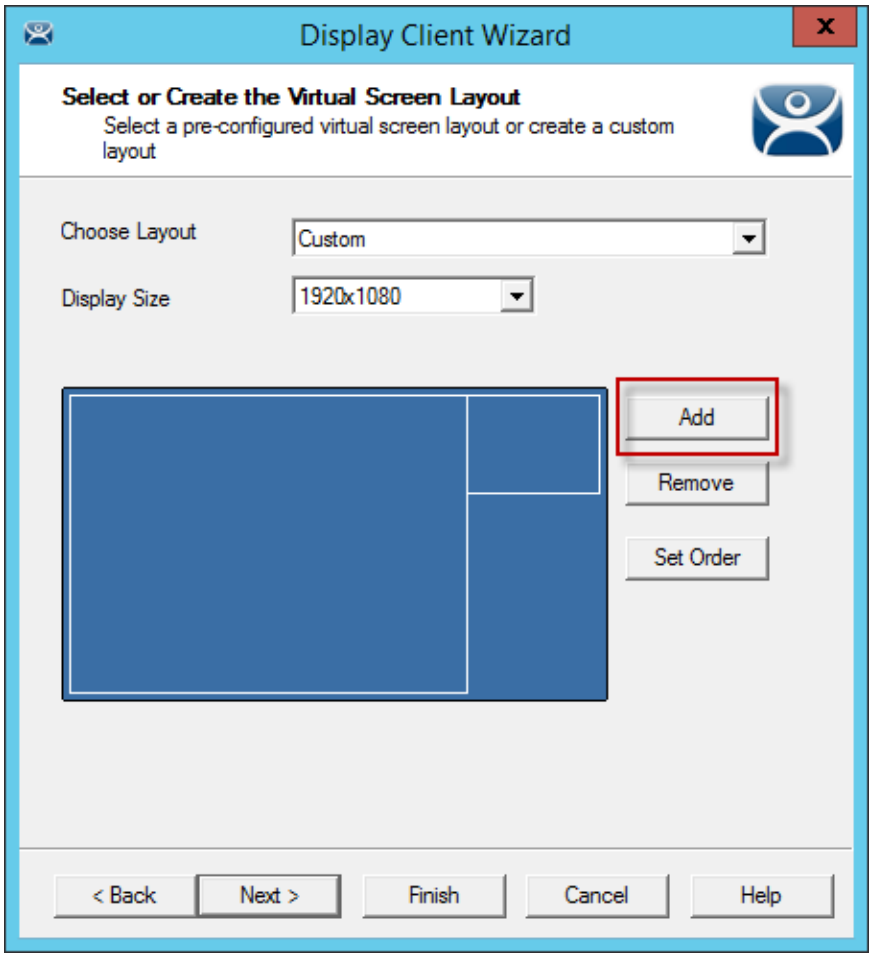
Select the ***Add*** button to launch the **Custom Overlay** window.



Custom Overlay #2

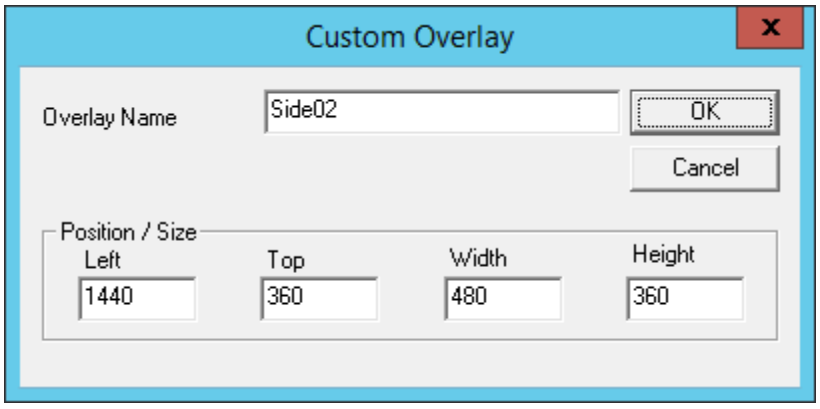
The next example uses an overlay that is 1440 pixels from the left and is 480 x 360.

Click the ***OK*** button to accept the settings.



Display of Created Overlay

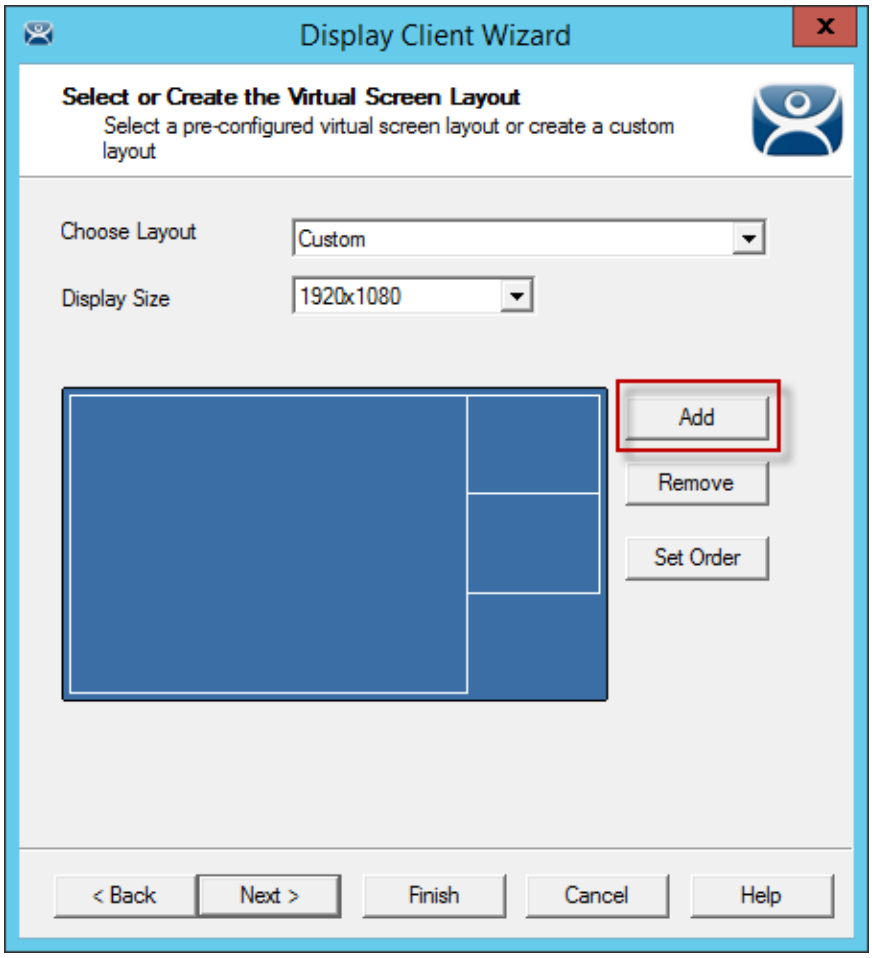
Select the ***Add*** button to launch the **Custom Overlay** window for the next overlay.



Custom Overlay #3

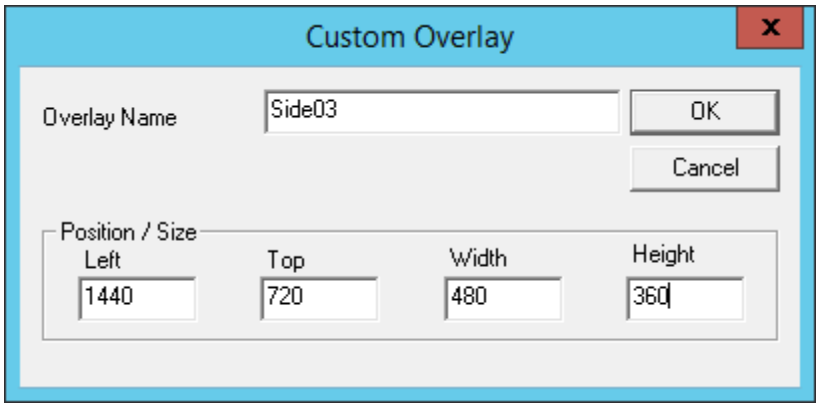
This example uses an overlay that is 1440 pixels from the left, 360 pixels from the top, and is 480 x 360.

Click the ***OK*** button to accept the settings.



Display of Created Overlay

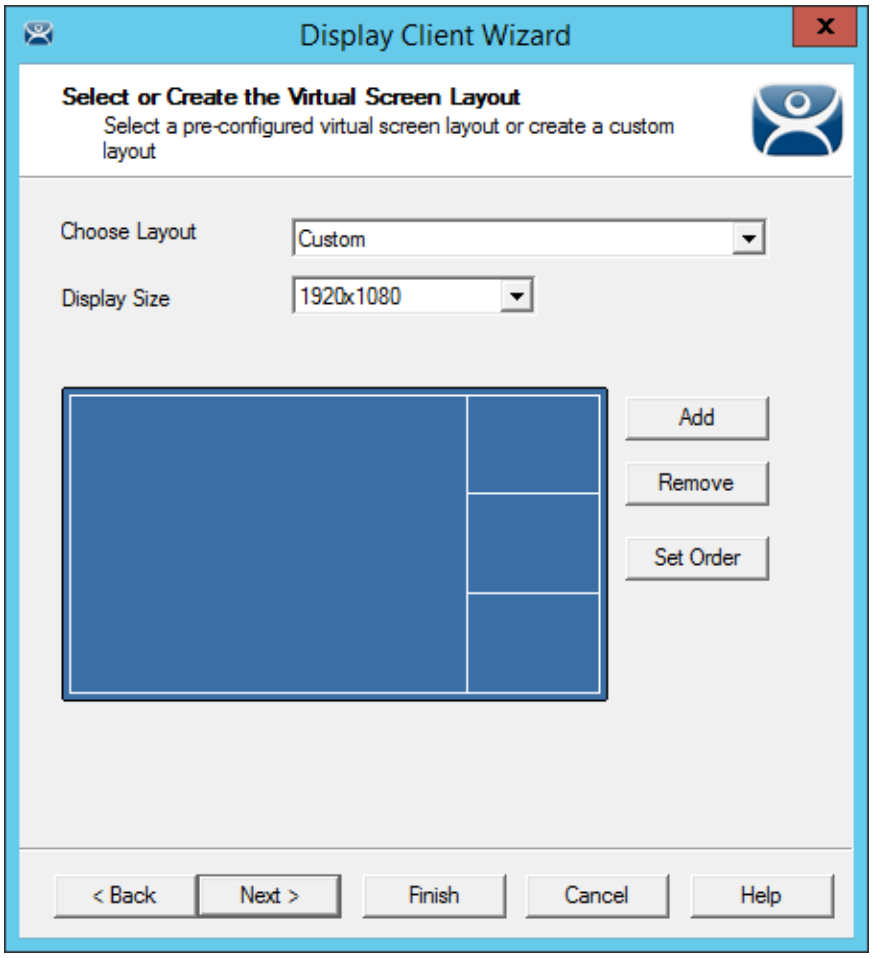
Select the ***Add*** button to launch the **Custom Overlay** window for the next overlay.



Custom Overlay #3

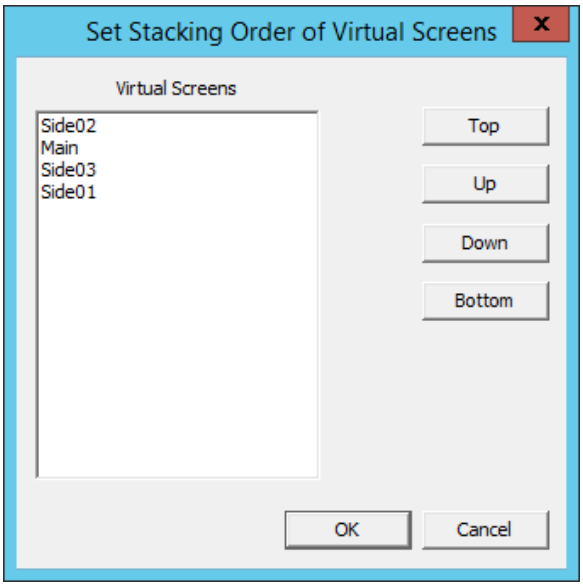
This example uses an overlay that is 1440 pixels from the left, 720 pixels from the top, and is 480 x 360.

Click the ***OK*** button to accept the settings.



Display of Created Overlay

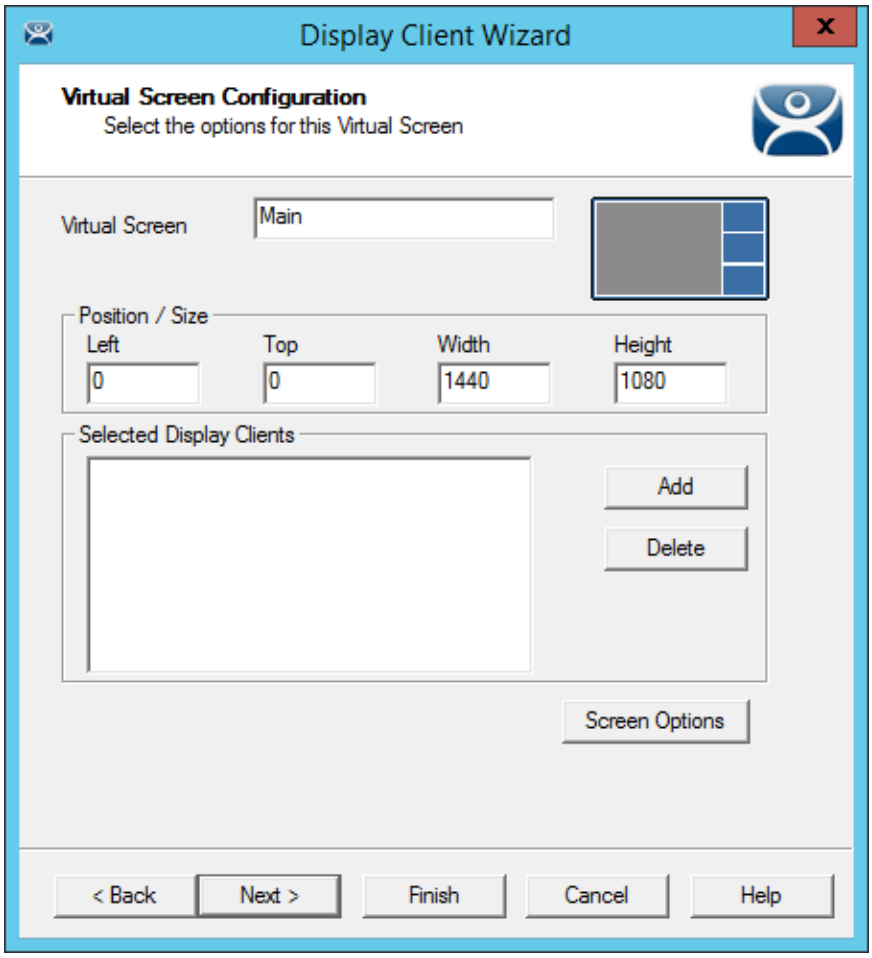
This shows the completed layout of the overlays.



Set Stacking Order of Virtual Screens

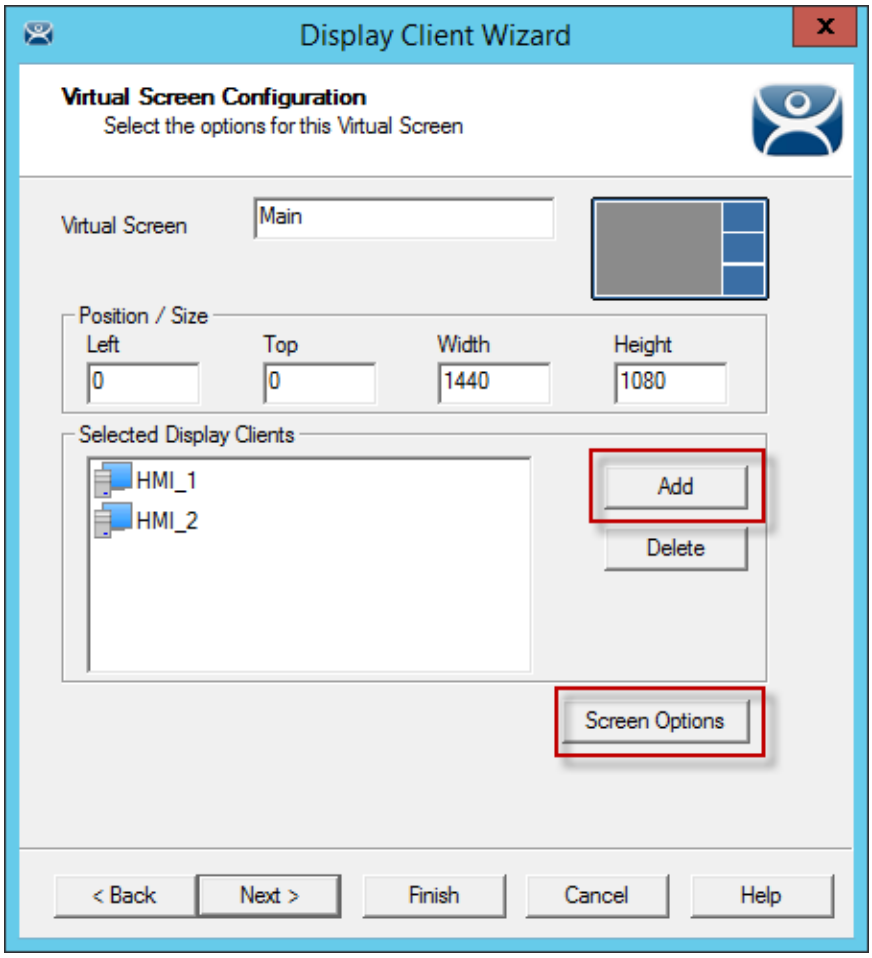
The Set Order button launches the Set Stacking Order of Virtual Screens dialog that lets you change the order that the screens appear. This is important when the overlays overlap.

Select ***Next*** to add display clients to the overlays.



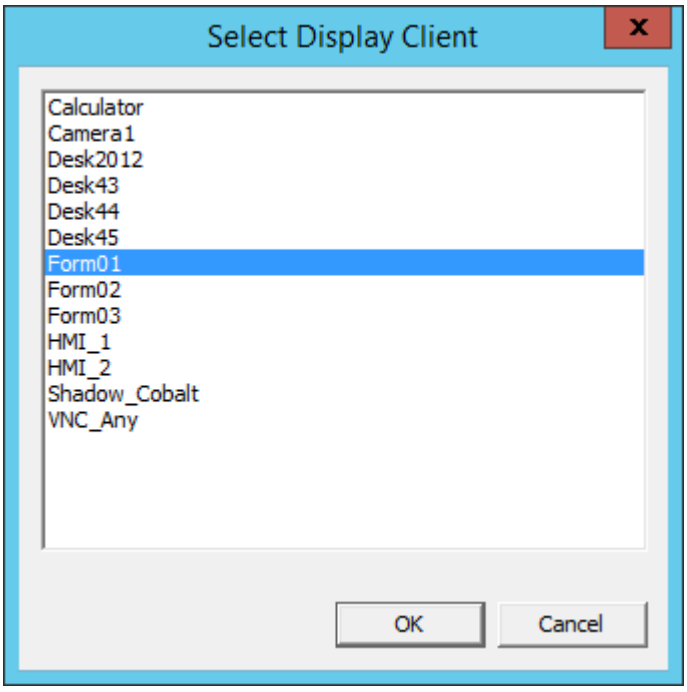
Adding Display Clients to the Virtual Screens

Each custom overlay will need a display client. The wizard shows one overlay at a time and display clients can be added as shown in Pre-Defined Templates on page 198.



Adding Display Clients to the Virtual Screens

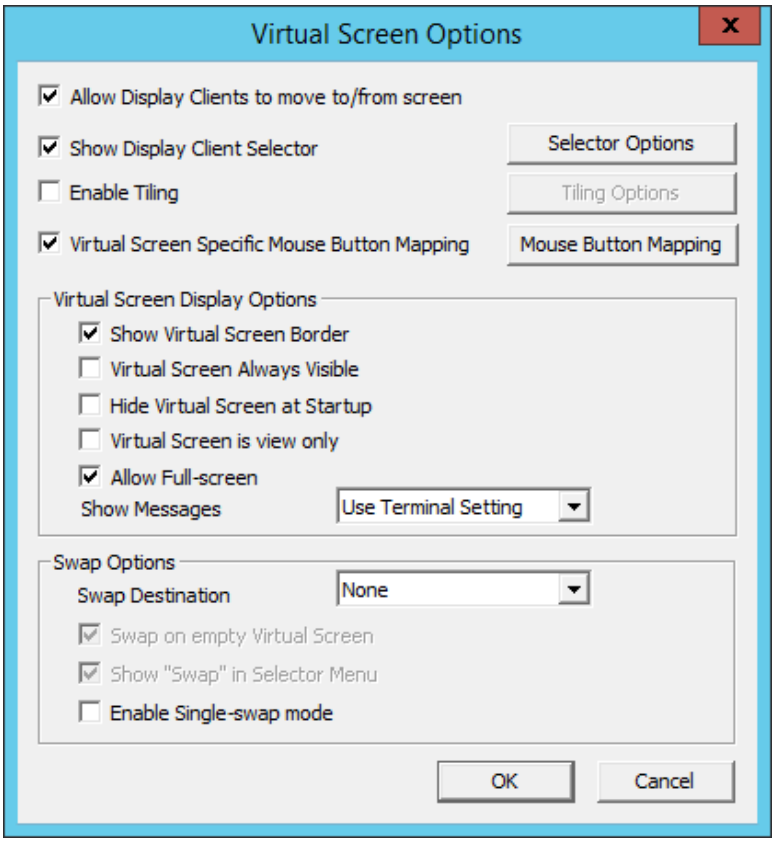
The Add button launches the **Select Display Client** dialog that allows display client selection.



Select Display Client Dialog

A **Select Display Client** dialog will be displayed listing all the display clients.

Highlight the desired Display Client and select the ***OK*** button.



Virtual Screen Options

The Virtual Screen Overlay has several options:

- **Allow Display Clients to move to/from screen** – This allows you to move a display client from one overlay to the other much like you can move display clients between monitors on a MultiMonitor thin client.
- **Show Display Client Selector** – This shows the drop-down selector at the top of the overlay. It can be configured by clicking the Selector Option button.
- **Enable Tiling** – This will allow tiling of Display Clients within the overlay if you have multiple display clients.
- **Virtual Screen Specific Mouse Button Mapping** – This activates the **Mouse Button Mapping** that allows you to assign ThinManager-specific tasks to the mouse buttons.
- **Mouse Button Mapping** – This button launches the **Mouse Button Mapping** window that allows you to assign actions to mouse buttons.

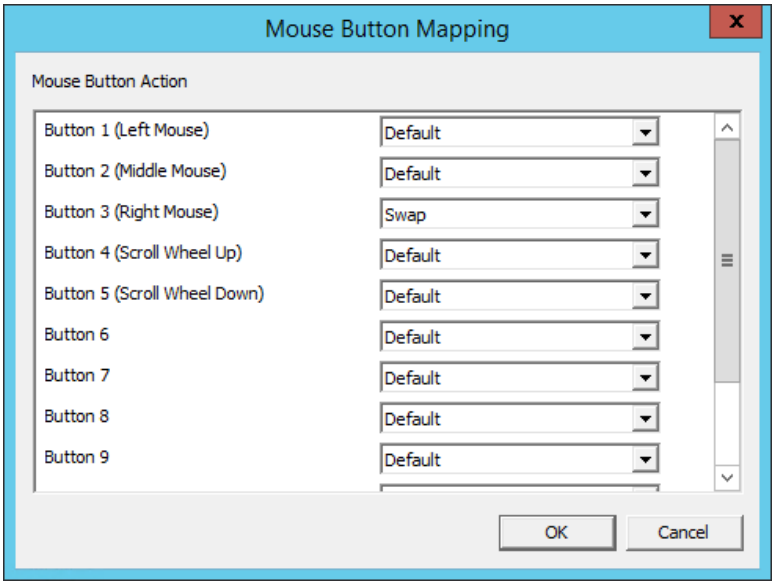
Virtual Screen Display Options

- **Show Virtual Screen Border** – This will show a border between the overlays.
- **Virtual Screen Always Visible** – This will make this specific overlay “always visible’. If the user switches to a different display client this overlay will still be visible even though its display client is hidden.
- **Hide Virtual Screen at Startup** – This setting hides the Virtual Screen at start up. It is intended to be used with the TermMon ActiveX that will toggle the overlay visibility.

- **Show Virtual Screen Border** – This will show a border between the overlays.
- **Virtual Screen is view only** – This makes the display client in the overlay non-interactive.
- **Allow Full-screen** – This will allow the selected overlay to be toggled to full screen

Swap Options

- **Swap on empty Virtual Screen** – This will swap the overlay with an empty overlay.
- **Show "Swap" in the Selector Menu** – This will add the "Swap" command to the dropdown selector.
- **Swap Destination** – This dropdown allows you to assign the swap partner for the overlay.

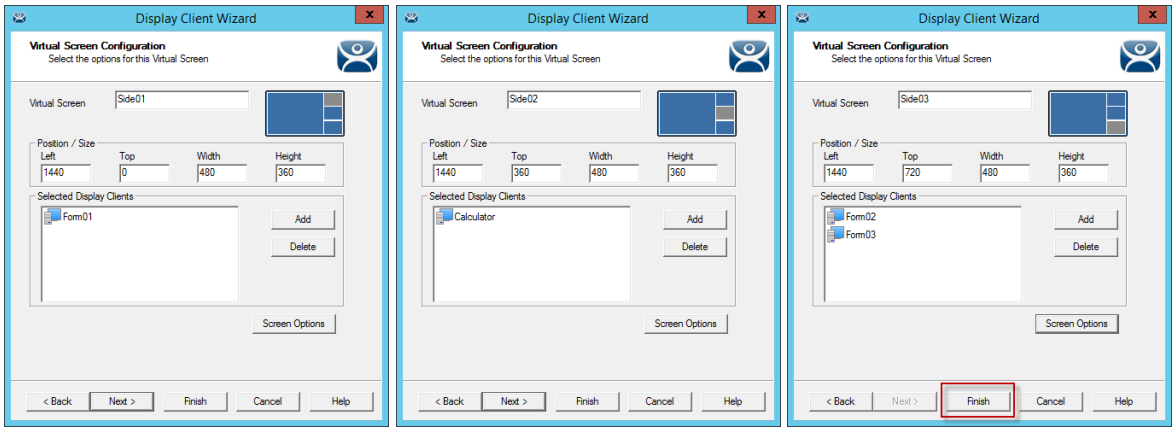


Mouse Button Mapping

The ***Mouse Button Mapping*** button on the **Virtual Screen Option** page will launch the **Mouse Button Mapping** window. This allows you to configure actions for the mouse buttons through drop-down menus.

The Virtual Screen wizard repeats for each overlay.

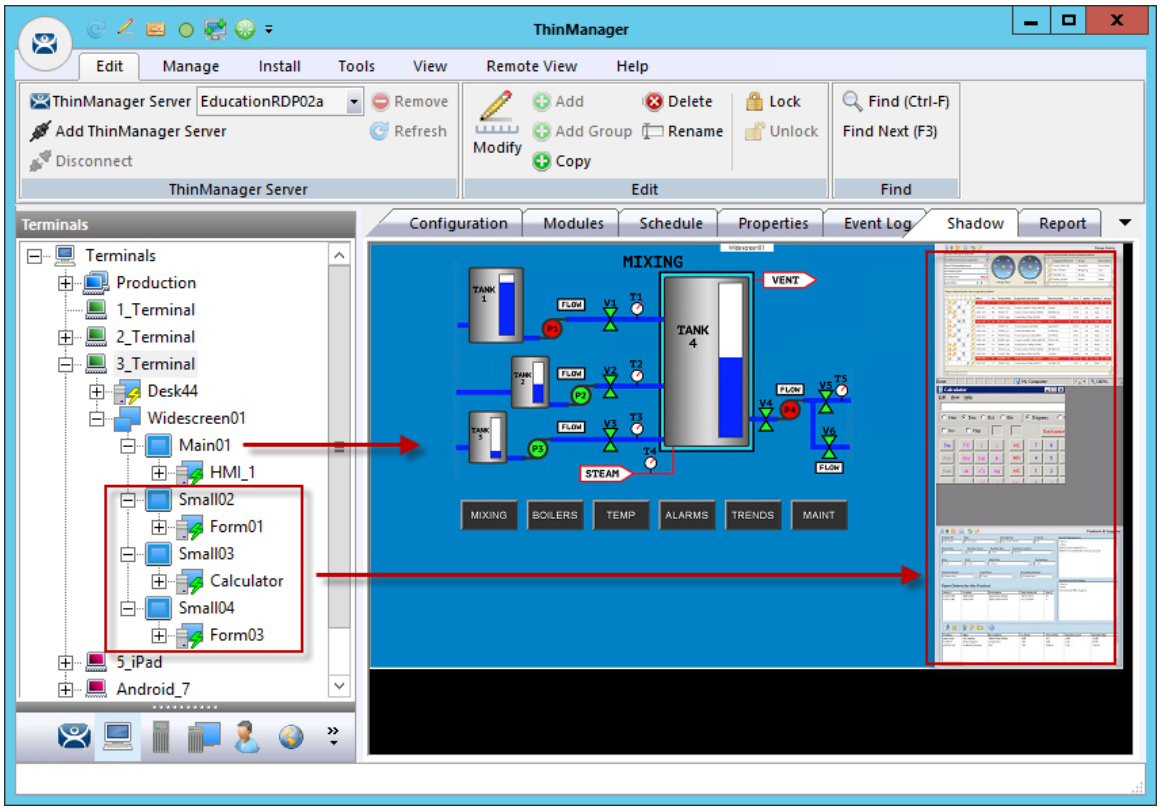
Select the ***Next*** button to go to the next overlay.



Each Overlay Is Configurable

The wizard will navigate to each overlay allowing the selection of display clients and settings.

Select the ***Finish*** button when done.



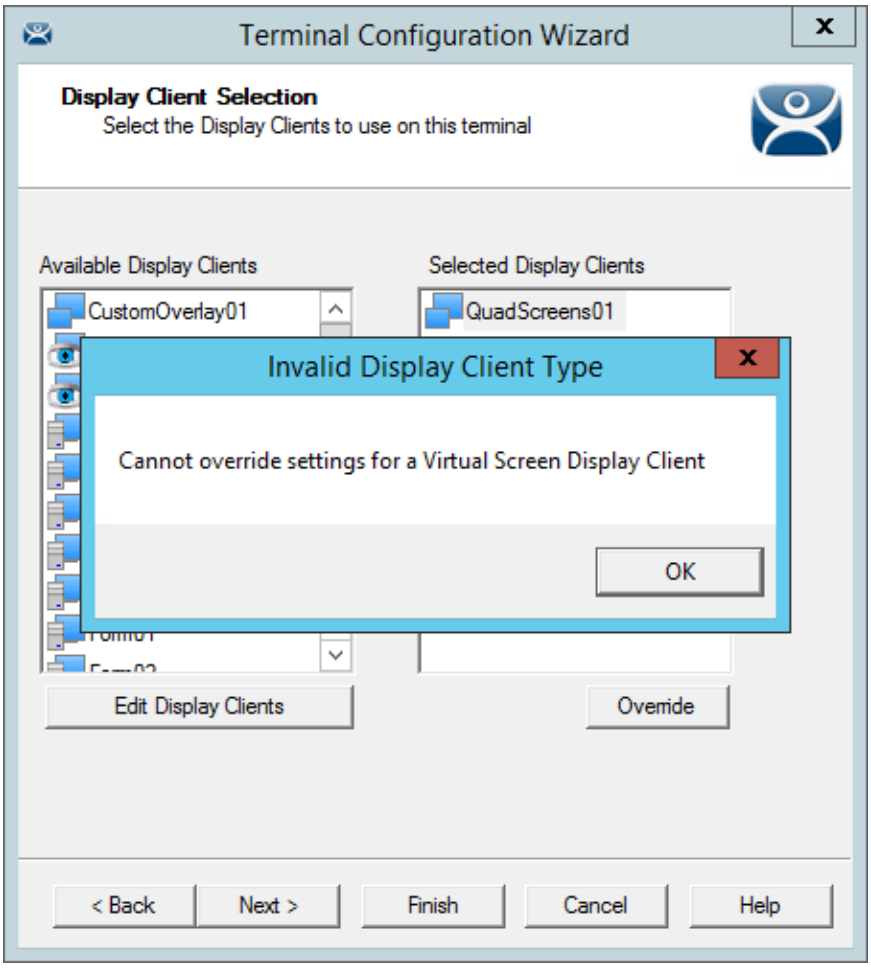
Custom Overlay in Action

Once the Virtual Screen wizard is finished it can be added to a Terminal. The Terminal will show the Virtual Screens once it is restarted.

The example shows the main overlay with an HMI and the three smaller overlays along the side, each with their own display client. These overlays could have multiple display clients and can be tiled if desired.

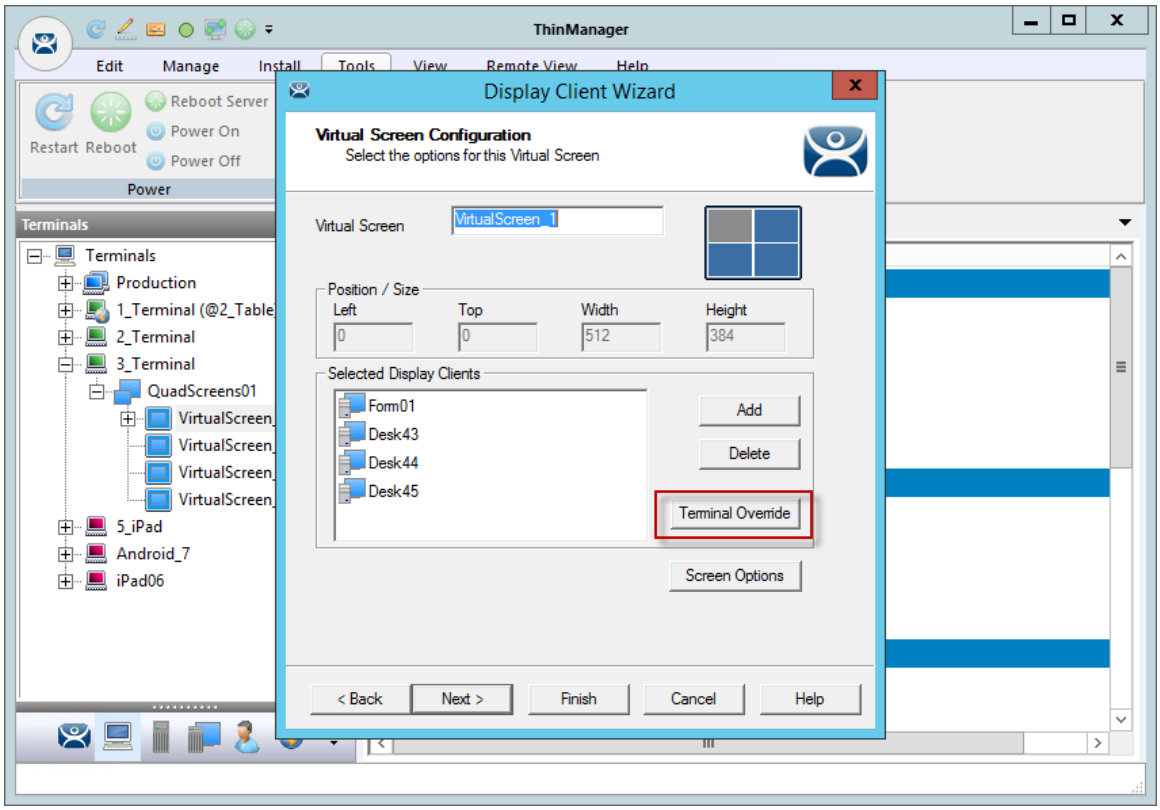
18.5. Display Client Override on Virtual Screens

Virtual Screens do not allow an override in the Terminal Configuration Wizard.



Display Client Selection Page Error

Virtual Screens do not allow an override on the Display Client Selection page of the Terminal Configuration Wizard. It is done from the ThinManager tree instead.

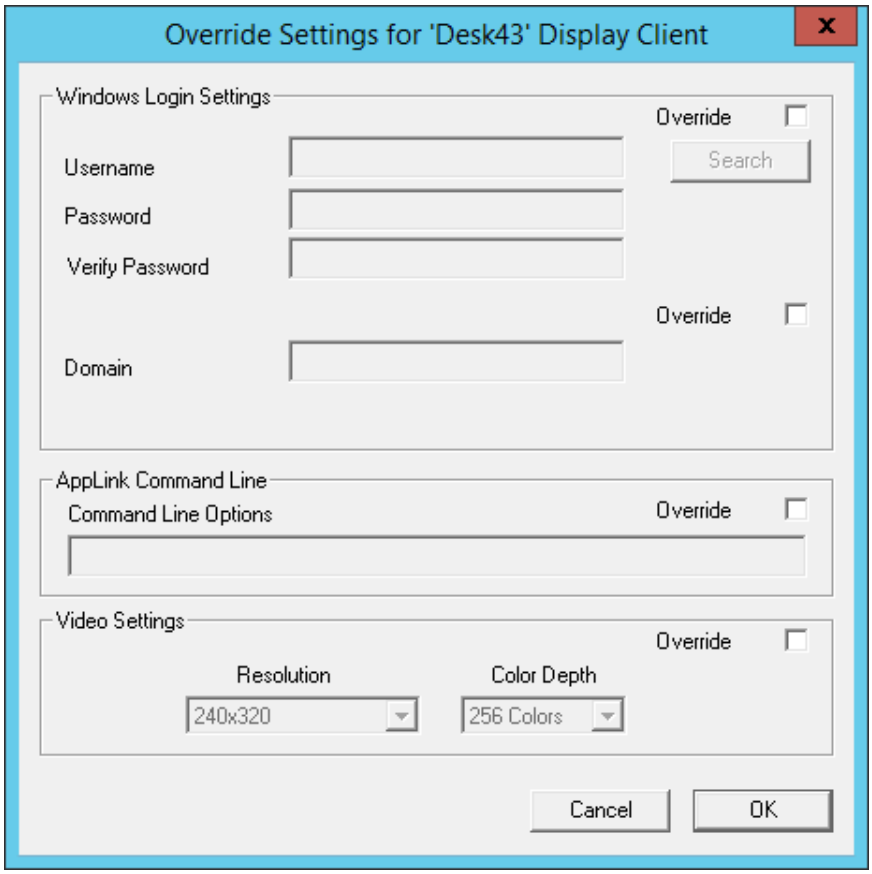


Virtual Screen Configuration Page

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.

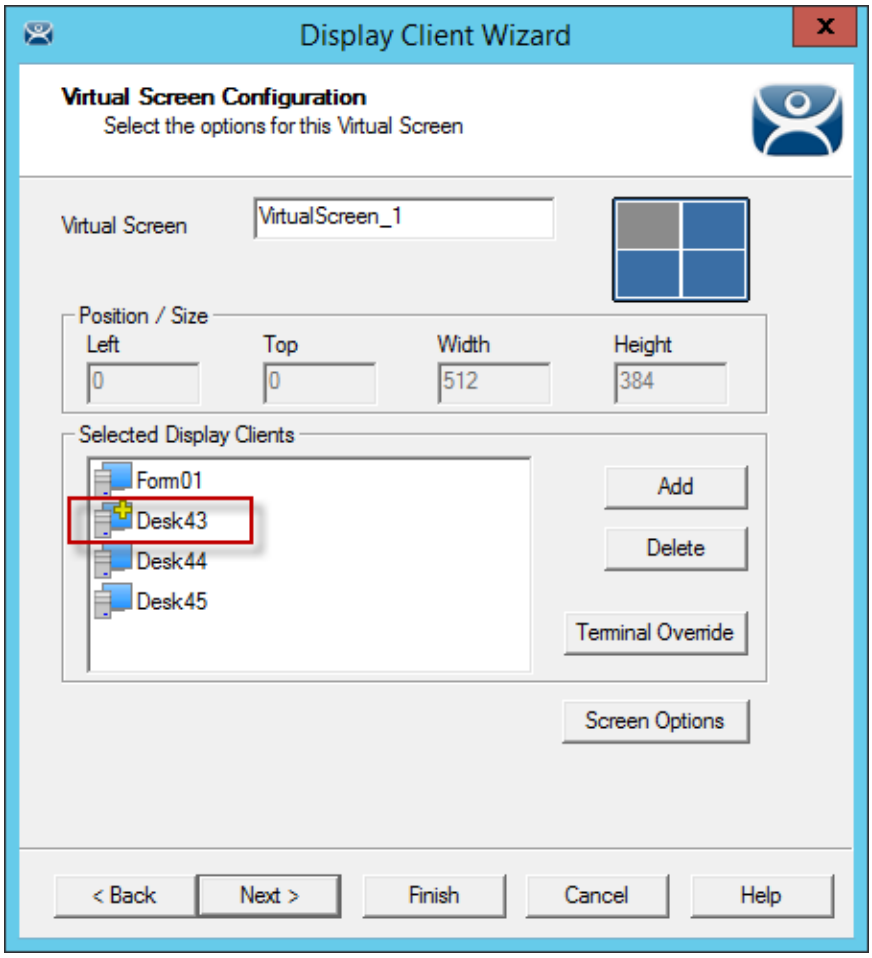
Highlight the display client you want to alter and select the ***Terminal Override*** button.



Override Settings Page

The **Override Settings** page will be displayed that allows the normal display client overrides. See Display Client Selection Page on page 239 for details.

Select the ***Override*** checkbox of your choice to apply the changes to the settings and select the ***OK*** button.



Virtual Screen Configuration Page Showing Override

The Display Client that has overridden settings will display a yellow cross to show that is has a changed setting.

19. Devices – Terminal Configuration

There are five types of Terminals that can be used in a ThinManager system. They are:

- ThinManager Ready thin clients
- ThinManager Compatible thin client
- aTMC for Android Devices
- iTMC client for iOS iPads and iPhones
- WinTMC client for Windows PCs and Surface tablets

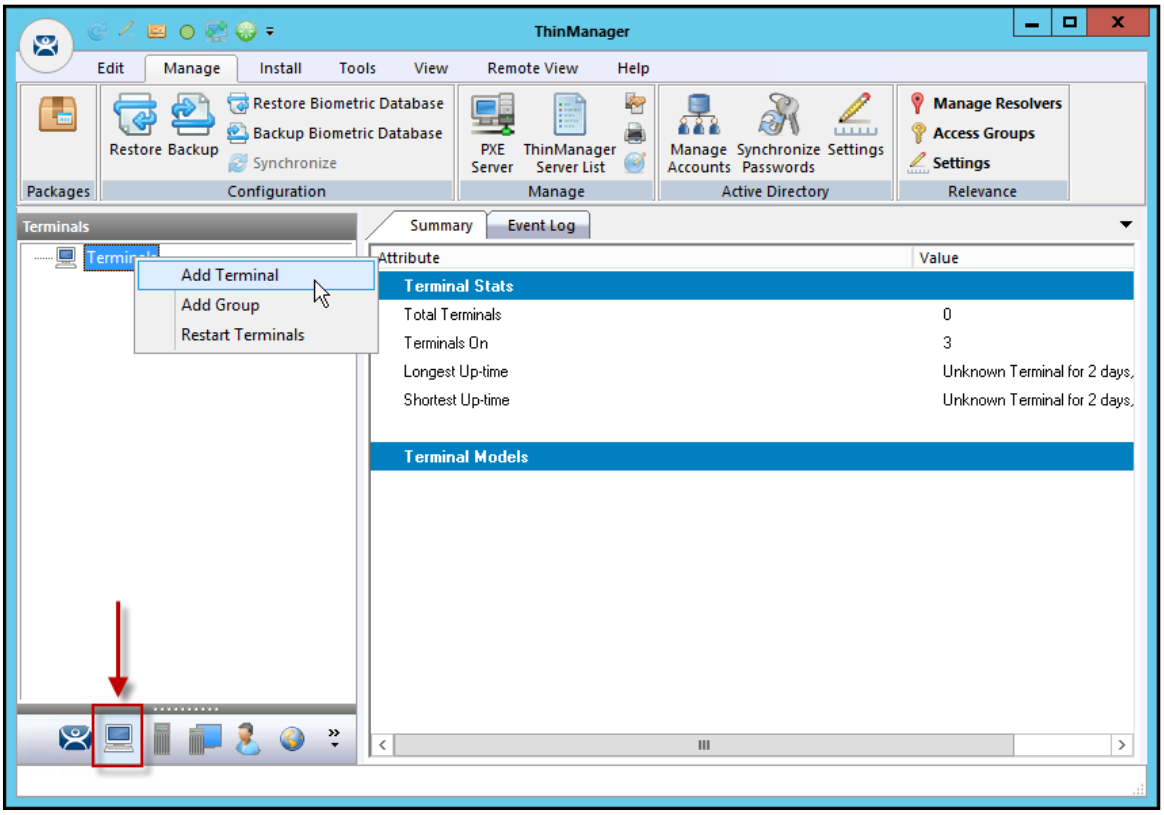
Adding a device is a two-step process. First the device needs to be pointed to the ThinManager Server to receive a configuration. The second step is to have a configuration created in ThinManager for the device to download.

We will cover the configuration of the device in ThinManager first then show how to connect each hardware device to ThinManager second.

19.1. Terminal Configuration Wizard in ThinManager

The **Terminal Configuration Wizard** is launched from the **Terminals** branch of the ThinManager tree.

Open the **Terminals** tree by selecting the **Terminal** icon at the bottom of the ThinManager tree.

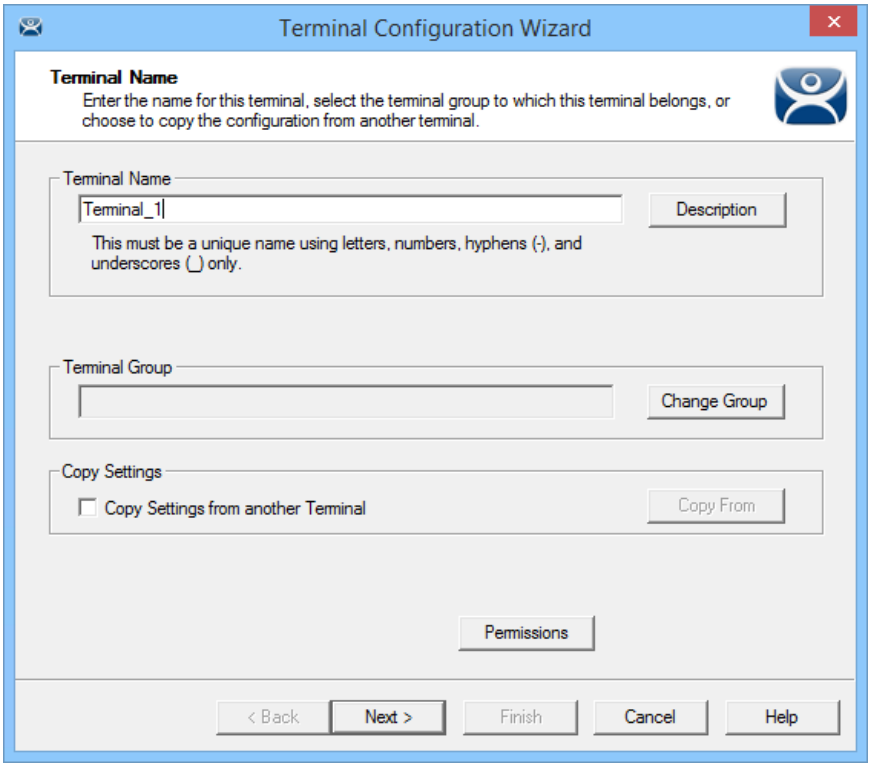


Terminal Branch of the ThinManager Tree

Right click on the Terminals branch and select ***Add Terminal*** to launch the **Terminal Configuration Wizard**.

19.1.1. Terminal Name Page

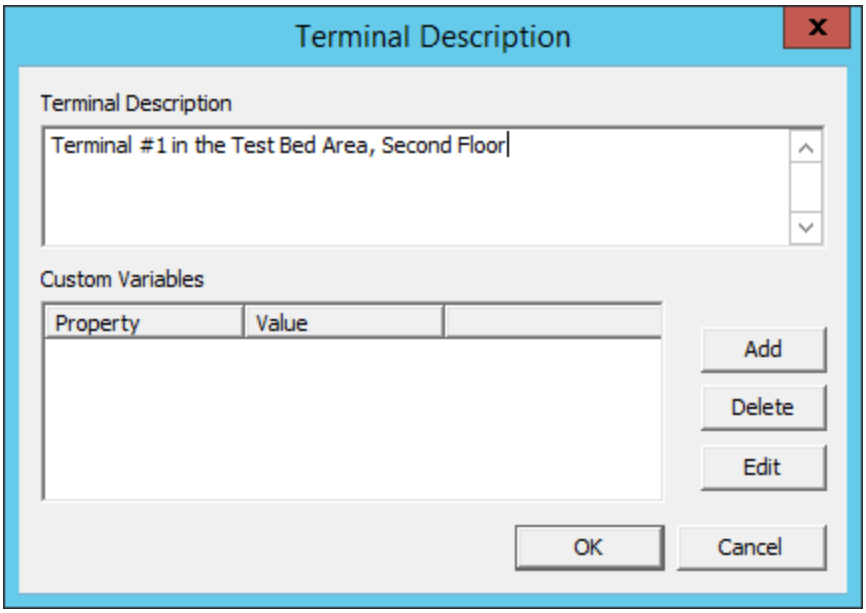
The first page of the Terminal Configuration Wizard is the **Terminal Name** page.



Terminal Name Page of the Terminal Configuration Wizard

Enter a name for the Terminal in the ***Terminal Name*** field. It should be 15 characters or less.

- ***Description*** - The ***Description*** button launches a **Terminal Description** window that allows you to add extra information about the Terminal.
- ***Change Group*** – The ***Change Group*** button allows you to add the Terminal to a Terminal Group. See Using Groups for Organization on page 271 for details.
- ***Copy Settings*** – The ***Copy Settings from another Terminal*** allows you to clone the Terminal configuration. See Copy Settings from another Terminal on page 268 for details.
- ***Permissions*** – The ***Permissions*** button allows you to apply an Access Group to the Terminal. See Permission Deployed Applications in Relevance on page 457 for details.



Terminal Description Window

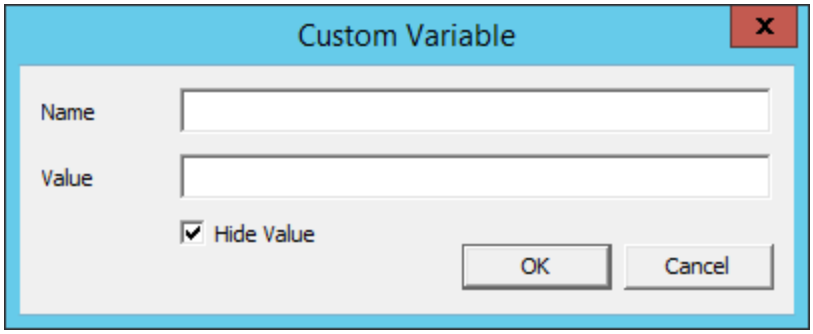
The ***Terminal Description*** field is handy to add extra information when the Terminal names are industrialized, like **USP_MX10_L1_qty** or **Prod_TrayPkgShrkWrp_OIT**.

The Custom Variables allow a variable to be applied for advanced functionality.

- **Terminal Description** – This allows a verbose description to be added to the Terminal.
- **Add** – This opens the **Custom Variable** window for adding a custom variable.

Custom variables allow a single display client can be created with a custom variable as part of the path. Each user, Terminal, or location has specific data in the custom variable to modify the content that the display client delivers, allowing one display client to do the work of many.

Additionally a custom variable can pass specific data to an application through the TermMon ActiveX.

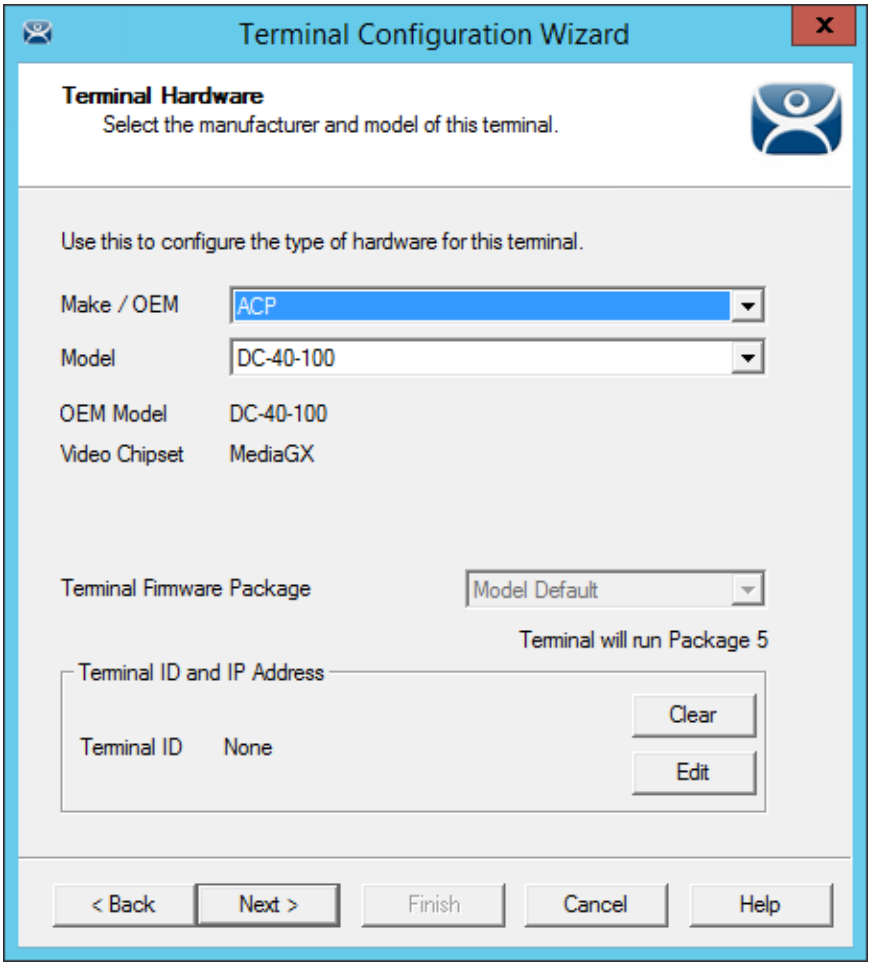


Custom Variable Window

- ***Name*** – This field assigns the name to the custom variable.
- ***Value*** – This field assigns the value or content to the custom variable.
- ***Hide Value*** – This checkbox, if selected, will obscure the custom variable value. If unselected the value is shown.
- **OK** – accepts the changes and closes the window.

19.1.2. Terminal Hardware Page

The Terminal Hardware page allows the type of hardware to be specified.



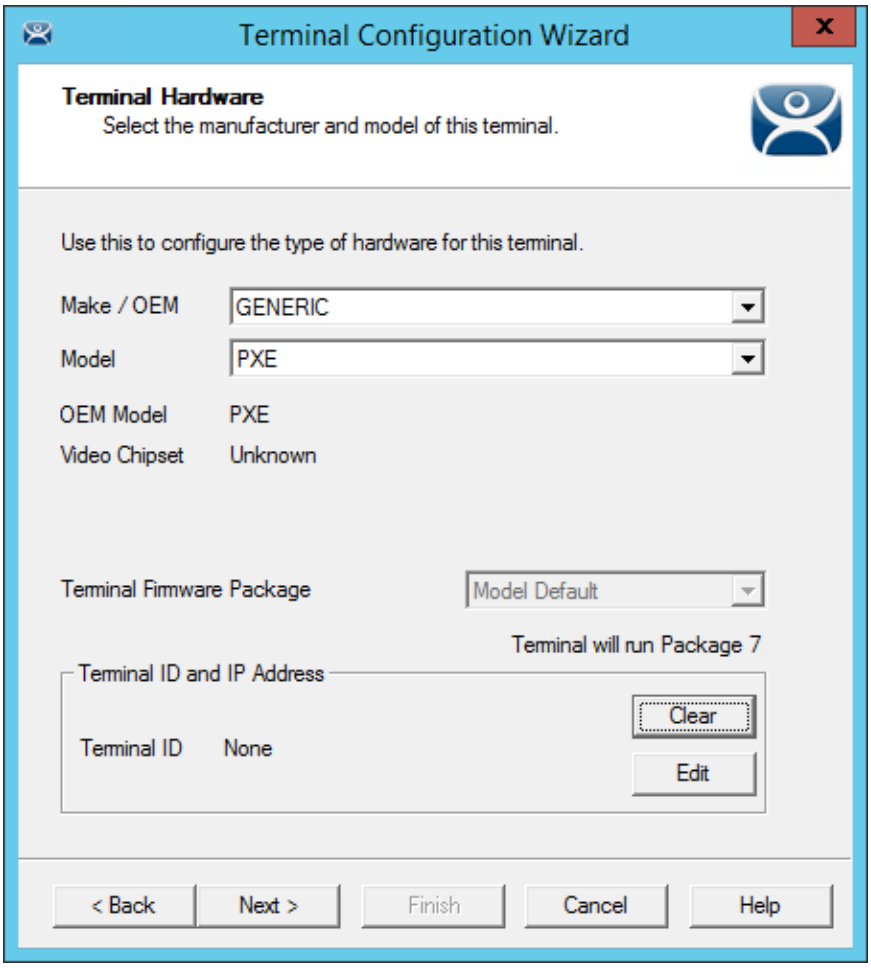
Terminal Hardware Page of the Terminal Configuration Wizard

The **Terminal Hardware** page allows you to specify the make and model of the Terminals you are adding.

Use the correct ***Make*** and ***Model*** if you can. This allows you to configure the Terminal to match the capabilities of the hardware you will be using.

Note: When a Terminal connects to its configuration for the first time ThinManager will adjust the configuration to match the actual hardware used and not the pre-configured hardware selected to prevent errors. ThinManager will "dumb down" the configuration if needed.
The default model, the ACP DC-40-100, is used because it has limited video resolutions that every modern Terminal can use.
If a different model is assigned to this configuration it may end up with the lower video resolutions.

ThinManager uses the MAC address (Media Access Control address) to identify the Terminals. The Terminal ID will be automatically filled when hardware is associated with the configuration.

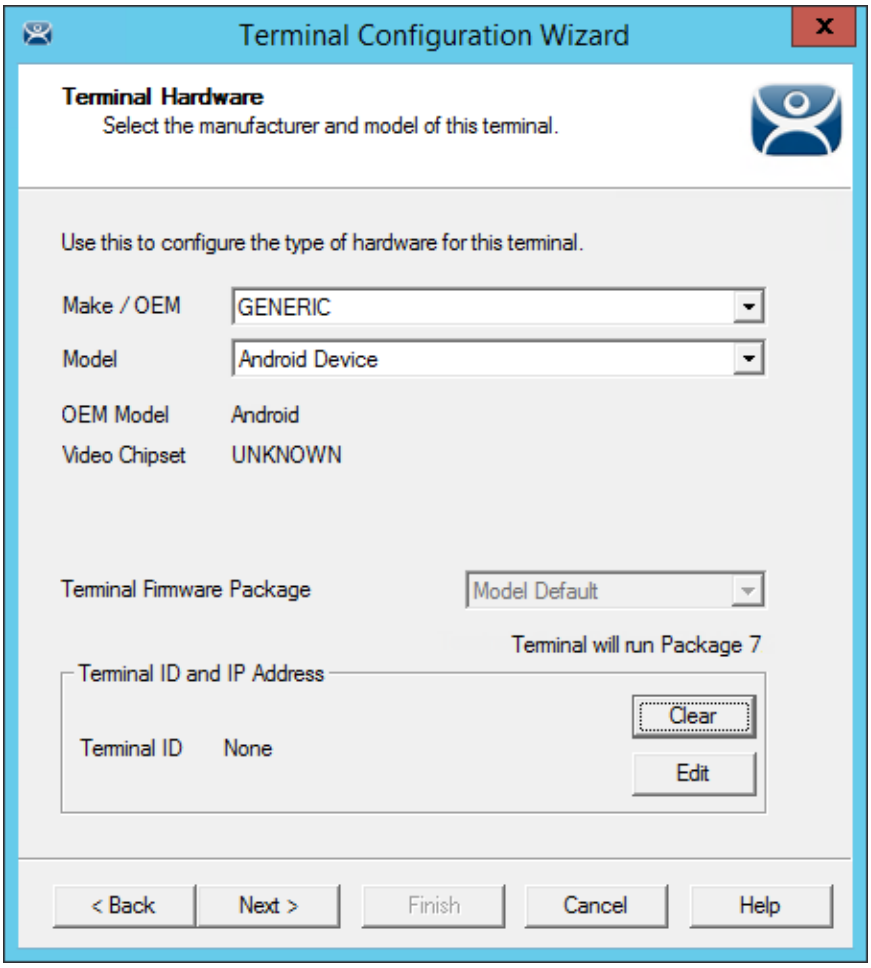


PXE Boot Configuration for ThinManager Compatible Thin Clients

ThinManager Compatible thin clients use PXE boot to download their firmware so they need to be configured at ***Generic / PXE***. You also need to configure the PXE Server in ThinManager by selecting ***Manage > PXE Server***.

See PXE Server and PXE Boot on page 298.

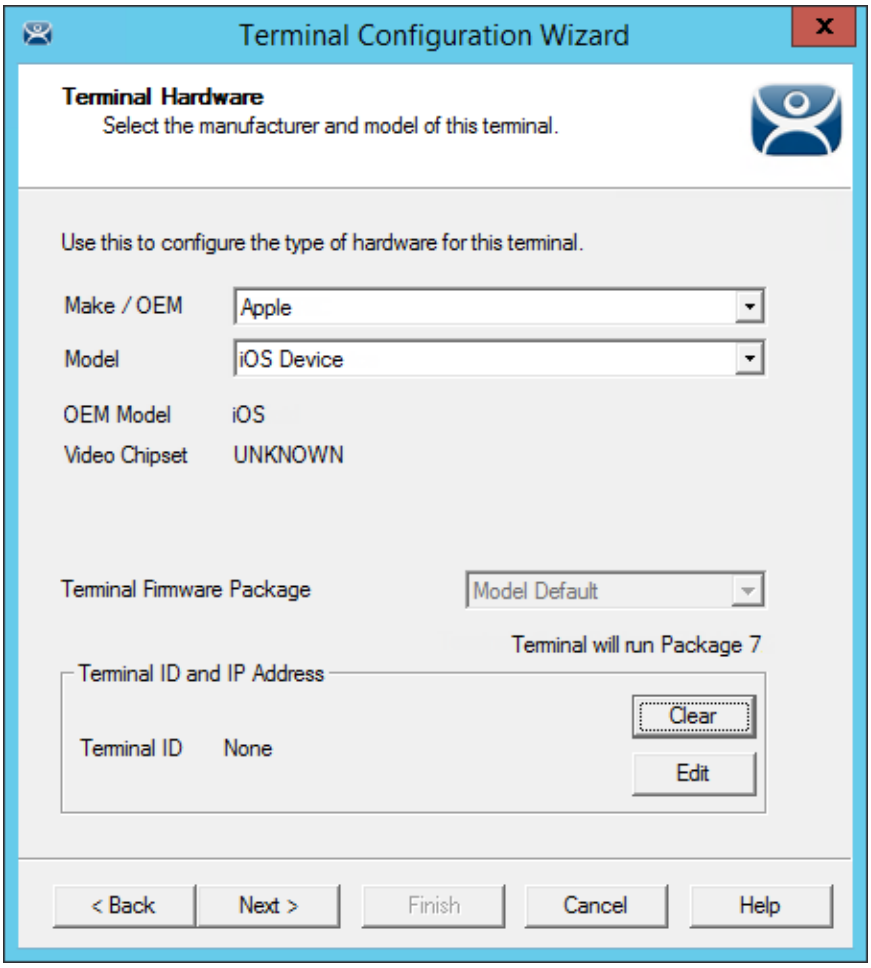
Select ***GENERIC / PXE*** as the ***Make*** and ***Model*** of the client.



Hardware Configuration for Android Devices

ThinManager has an Android application that allows the Android to run an RDP session that is controlled and managed by ThinManager.

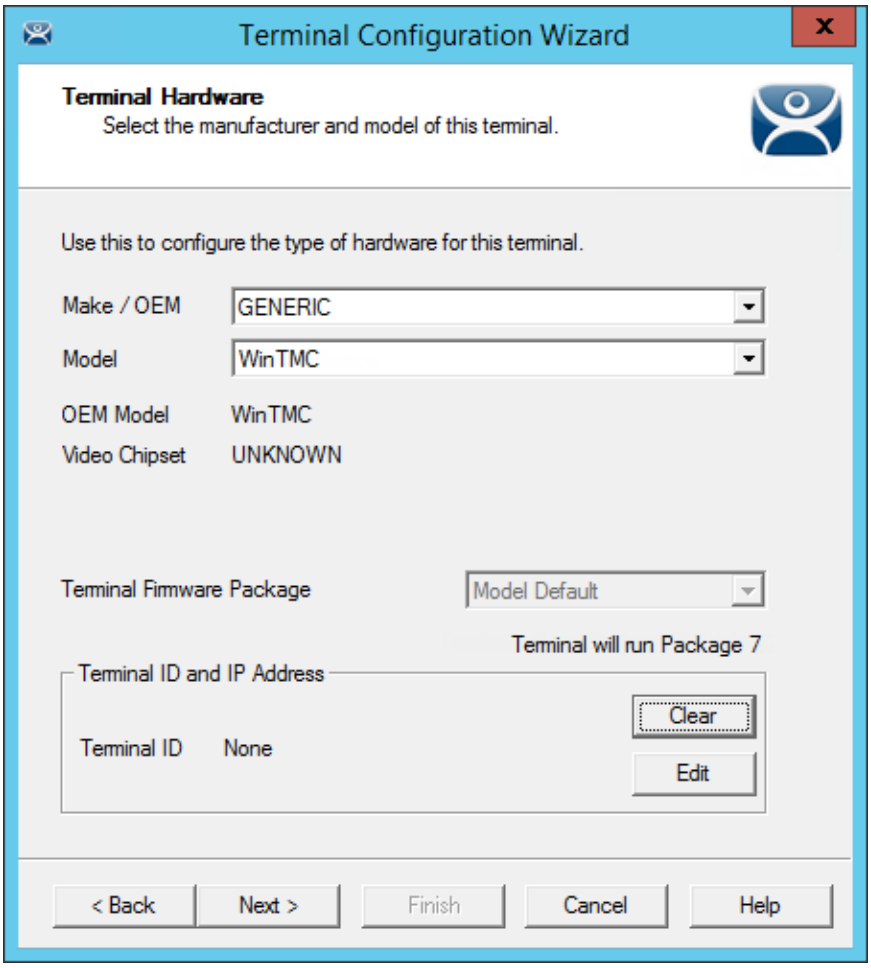
Select ***GENERIC / Android Device*** as the ***Make*** and ***Model*** of the client.



Hardware Configuration for Apple iPad

ThinManager has an iOS application that allows the iPad to run an RDP session that is controlled and managed by ThinManager.

Select ***Apple / iOS Device*** as the ***Make*** and ***Model*** of the client.



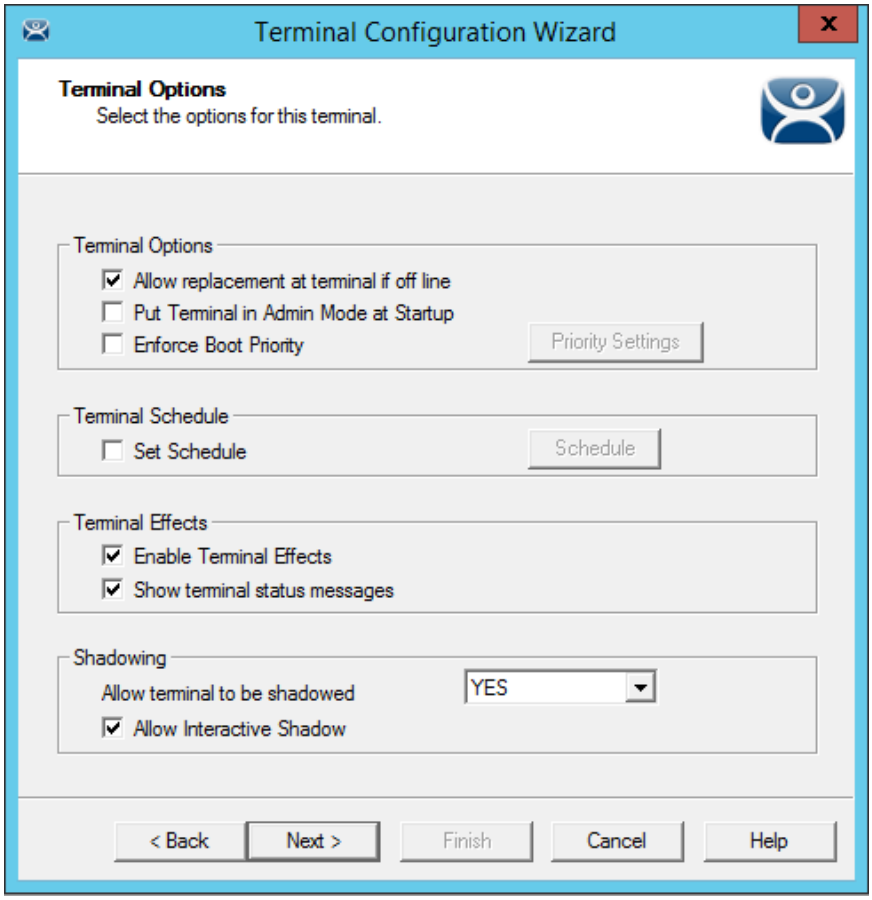
Hardware Configuration for WinTMC Clients

ThinManager has a PC application that allow the PC to run an RDP session that is controlled and managed by ThinManager. Select ***GENERIC / WinTMC*** as the ***Make*** and ***Model*** of the client.

Select the ***Next*** button to configure the configuration.

19.1.3. Terminal Options Page

The **Terminal Options** page starts the configuration process.



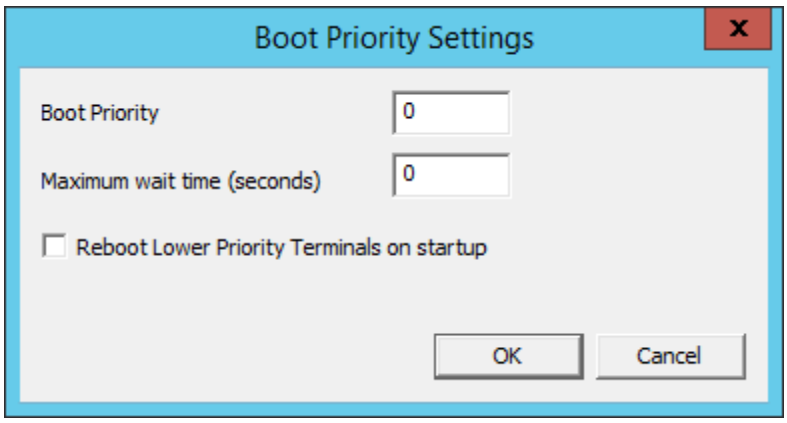
Terminal Options Page of the Terminal Configuration Wizard

The **Terminal Options** page has a few settings of interest.

- ***Allow replacement at Terminal if offline* –** This allows the Terminal to show up in the replacement list during a new Terminal connection
- ***Put Terminal in Admin Mode at Startup* –** This turns the Terminal on without showing the display clients. This is useful to use as the Terminal to register HID cards or registering fingerprint scans.
- ***Enforce Boot Priority*** - This allows you to set an order for the Terminals to boot when many reboot at once.
- ***Set Schedule* –** This will allow the Schedule button to become active.
See Scheduling on page 445.
- ***Enable Terminal Effects* -** This allows the desktops in MultiSession to slide smoothly into the desktop instead of appearing instantaneously.
- ***Show Terminal status messages*** - This allows the Terminal to display status messages in the upper left corner of the screen. Uncheck this to hide the messages from the operator.
- ***Allow Terminal to be shadowed*** – This drop-down sets the Shadowing setting allowing the configuration of Shadowing Options.

- ***No*** – This will prevent the Terminal from being shadowed by anyone.
- ***Ask*** – This will ask the user to allow shadowing. The user will need to say ***Yes*** on a message window before the shadowing is allowed.
- ***Warn*** - Will display a message window alerting the Terminal that it is to be shadowed, but doesn't require user input before the shadowing is allowed.
- ***Yes*** – Will allow shadowing to occur without warning or user input.

- ***Allow Interactive Shadow*** – This allows users with Shadowing permission to interactively shadow the Terminal. Unchecking this will put it into a "Look, but don't Touch" mode.
- ***Priority Settings*** - This button launches the **Boot Priority Settings Window.**



Boot Priority Settings

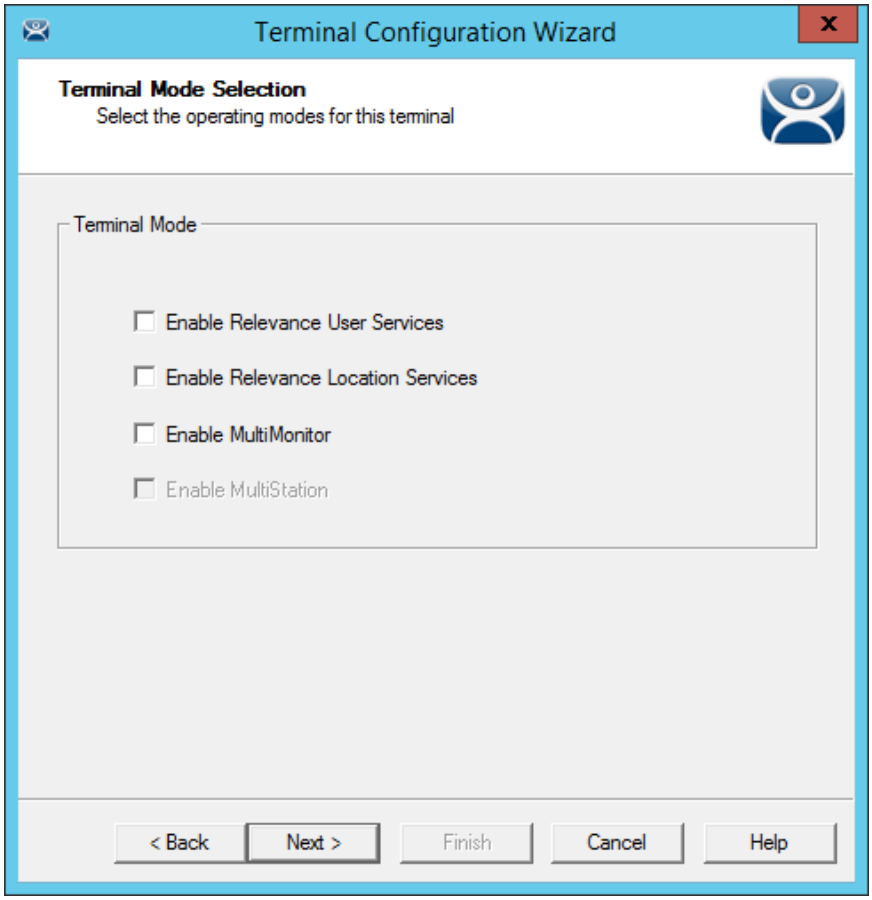
The Boot Priority Settings window is launched by the ***Priority Settings*** button on the **Terminal Options** page.

- ***Boot Priority*** - This sets the priority level, with 1 as the highest and 10 a lower priority.
- ***Maximum wait time (seconds)*** - This sets the maximum interval the Terminal will wait before starting to reboot.
- ***Reboot Lower Priority Terminals on startup*** - This will reboot lower priority (higher number) Terminals when this Terminal reboots. This is useful if the lower priority Terminals are running an application that has a dependency on the higher priority (lower number) Terminal.

Select the ***Next*** button to continue the configuration.

19.1.4. Terminal Mode Selection Page

The **Terminal Mode Selection** page sets the modes used by the Terminal.



Terminal Mode Selection of the Terminal Configuration Wizard

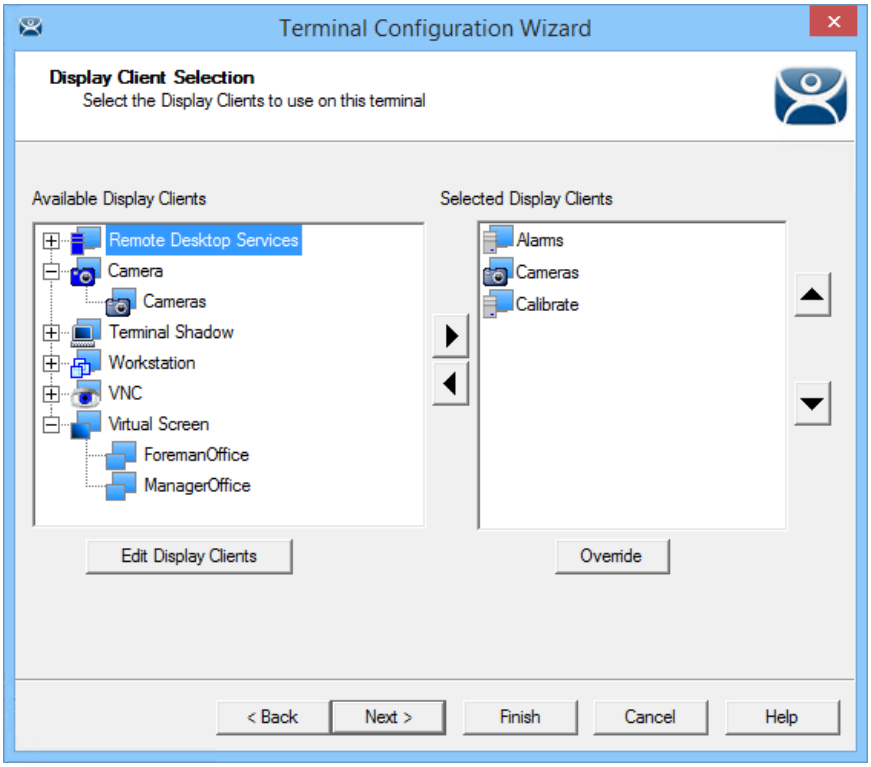
ThinManager uses **Display Clients** to deploy applications. Keeping the ***Use Display Clients*** checkbox allows you to use these. If you uncheck this checkbox you will lose other functions like MultiMonitor, TermSecure, MultiSession, and Instant Failover.

- ***Enable Relevance User Services*** – This uses Permissions and the membership of an Access Group to grant or deny access to applications, Terminals, or locations. .
  See Permission Deployed Applications in Relevance on page 456.
- ***Enable Relevance Location Services*** – This allows the Terminal to be assigned a Location and use the Relevance location features. .
  See Relevance Location Services on page 579.
- ***Enable MultiMonitor*** – This allows you to configure the Terminal to use two to five monitors, depending on the hardware capability.
  See MultiMonitor on page 401.
- ***Enable MultiSession*** – This is an advanced MultiMonitor function that allows multiple users to share a single MultiMonitor Terminal. It isn't active unless MultiMonitor is activated.
  See Hotkey Configuration Page on page 249.

Select the ***Next*** button to configure the configuration.

19.1.5. Display Client Selection Page

The **Display Client Selection** page allows the applications to be assigned to the Terminal.

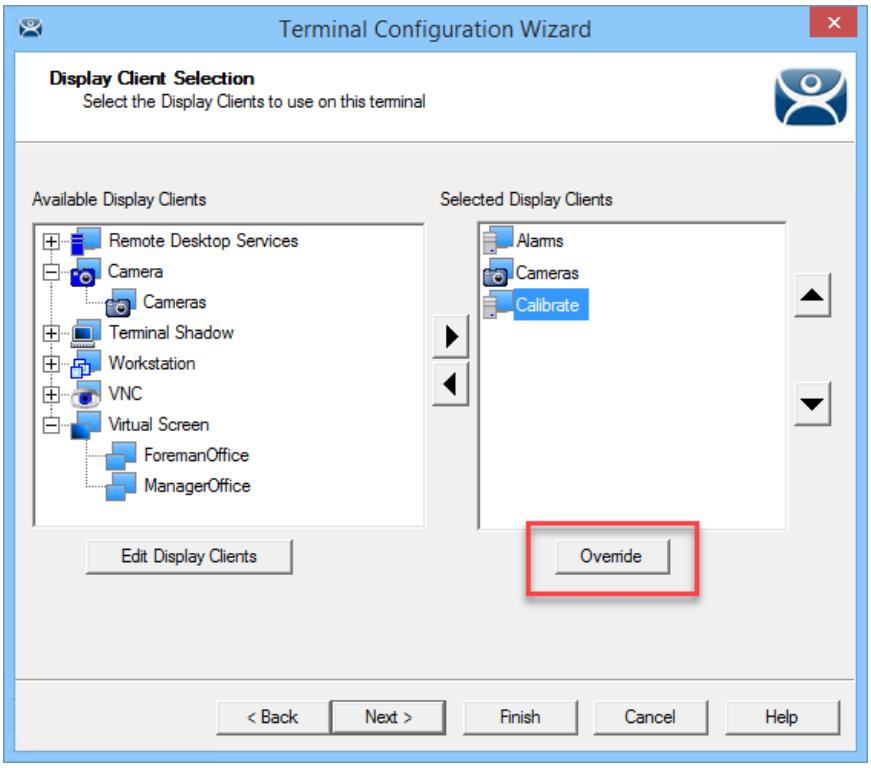


Display Client Selection Page of the Terminal Configuration Wizard

Display Clients are assigned to the Terminal on the **Display Client Selection** page.

The created display clients are in the left hand ***Available Display Clients*** list. Moving them to the right hand ***Selected Display Clients*** list will add the display client to the Terminal configuration.

Select the ***Next*** button to configure the configuration.

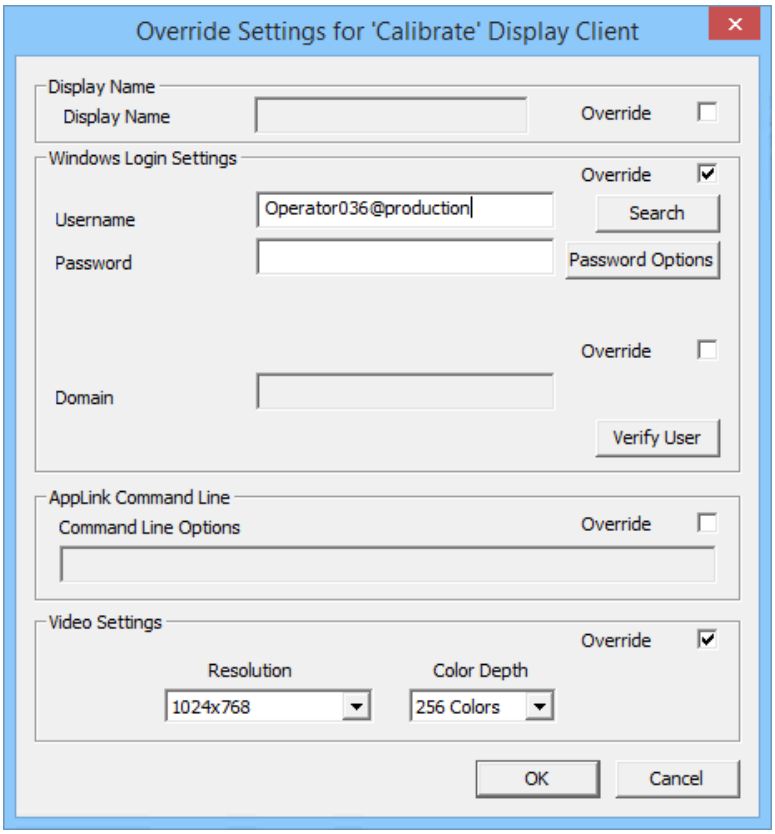


Display Client Selection Page of the Terminal Configuration Wizard

Display clients can be moved by double clicking on them or by highlighting them and using the left and right arrows.

Adding two or more display clients is **MultiSession**. It gives you to ability to deploy applications from different servers with ease.

The ***Override*** button launches the **Override Settings** window that allows you to modify the login settings.



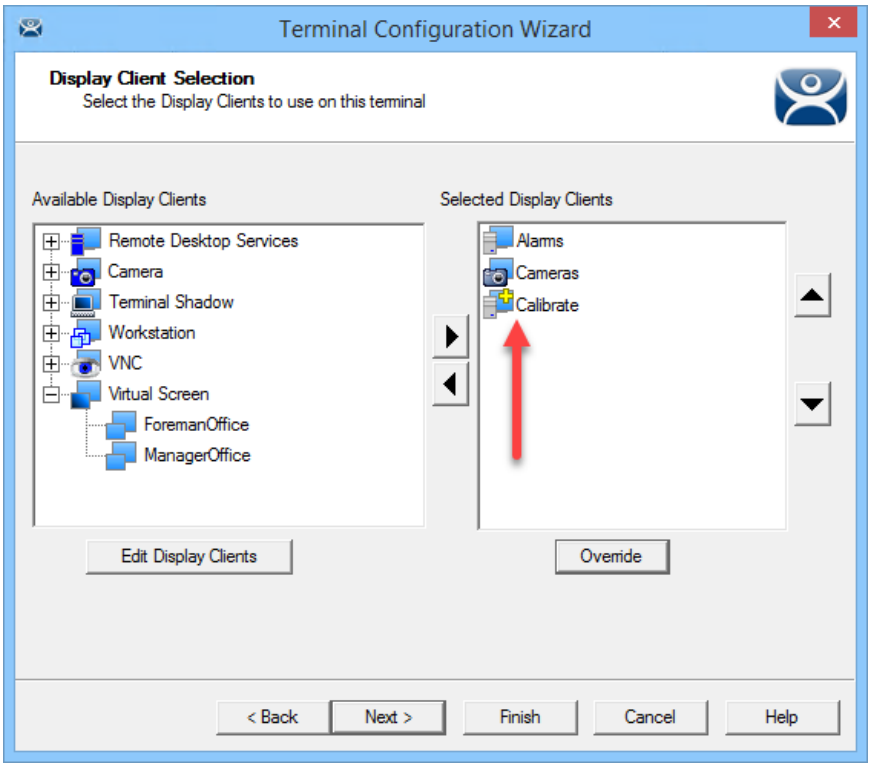
Override Settings Page

The **Override Settings** page allows you to change the user account used for logins, add a command line option, or change the resolution.

If you are in a domain you can use the ***Search*** button to pull a user account from the Active Directory.

See User Accounts in the Terminal Configuration Wizard on page 253.

Select the ***OK*** button to close the **Override Settings** window.



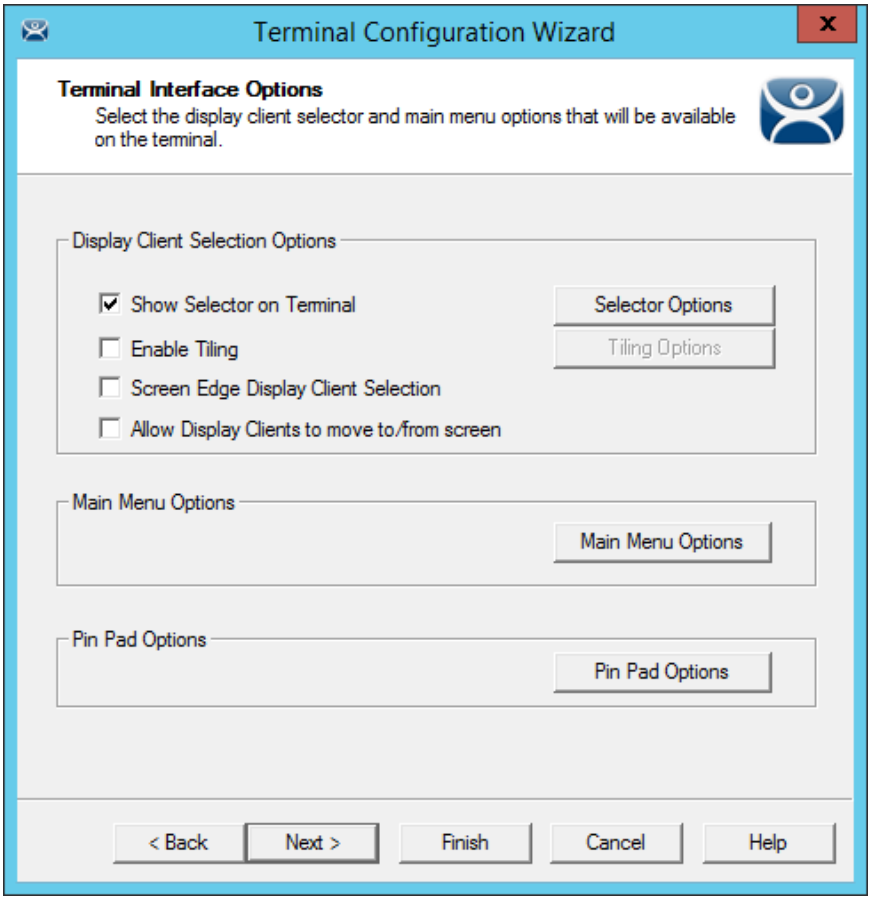
Override Indicator Icon

If a Display Client has a setting overridden then the Display Client will show a **Changed** icon in the ***Selected Display Clients*** list.

Select the ***Next*** button on the **Display Client Selection** page to configure the configuration.

19.1.6. Terminal Interface Options Page

The **Terminal Interface Options** page sets the methods to switch between display clients when using MultiSession.



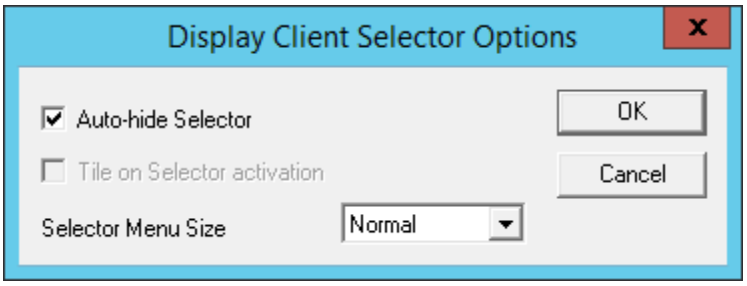
Terminal Interface Options Page of the Terminal Configuration Wizard

A single display client needs no additional navigation on the Terminal. If you have multiple display clients on the Terminal you need to have a method to switch between the sessions. The **Terminal Interface Options** page and **Hotkey Configuration** page allow you to configure switching methods.

The mouse options for switching are:

- ***Show Group Selector on Terminal*** – This checkbox, if selected, will display an on-screen drop-down menu that can be activated by mouse.
- ***Enable Tiling*** – This checkbox, when selected, allows the Display Clients to be tiled on the monitor to provide an overview of all the sessions at once.
- ***Screen Edge Group Selection*** – This checkbox, if selected, will activate a feature that will switch windows if the mouse is moved to the edge of the screen.
- ***Main Menu Options*** – This button is shown when the Relevance User Services is checked on the **Terminal Mode Section** page.
- ***Pin Pad Options*** – This opens the **Pin Pad Options** window that allows you to configure the PIN pad when using a Personal Identification Number instead of a password.

The ***Selector Options*** button launches the **Group Selector Options** window that has the settings for switching between sessions when using MultiSession.



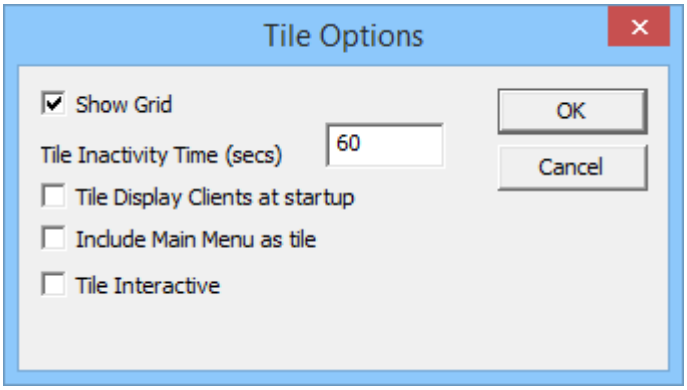
Display Client Selector Options

The **Group Selector** is hidden in the top center of the Terminal screen and can be revealed by moving the mouse to the center of the top edge.

- ***Auto-hide Selector*** - The Group Selector will remain visible if the ***Auto-hide Selector*** checkbox is unchecked.
- ***Tile on Selector activation*** - Checking the ***Tile on Selector activation*** will put the Tile Command on the Group Selector.
- ***Selector Menu Size*** - The Group Selector font size can be adjusted with the ***Selector Menu Size*** drop-down.

Select the ***OK*** button to accept changes or the ***Cancel*** button to close.

The ***Tiling Options*** button launches the **Tile Options** window that has the settings for tiling sessions when using MultiSession.



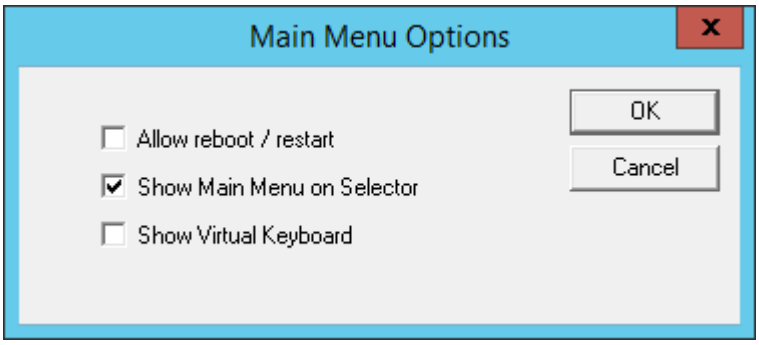
Tiling Options

The **Tile Options** window has several settings.

- ***Show Grid*** – This checkbox, when selected, will show the tiled sessions in a grid with each grid labeled with the session name as while the session is loading.
- ***Tile Inactivity Time*** – This field sets the length of time that the Terminal screen will stay focused on a selected session before reverting back to a tiled state due to inactivity.
- ***Tile Display Clients at startup*** – This checkbox, when selected, will show the sessions tiled when the Terminal first connects to its sessions.
- ***Include Main Menu as tile*** – This checkbox, when selected, will include a session displaying the TermSecure Main Menu.
- ***Tile Interactive*** – This checkbox, when selected, will allow a user to click into a tiled session and control it interactively without switching focus to a single session. To focus on a single session use the Group Selector Drop-down or the tiling hotkey (***CTL + T***), if enabled.

Select the ***OK*** button to accept changes or the ***Cancel*** button to close.

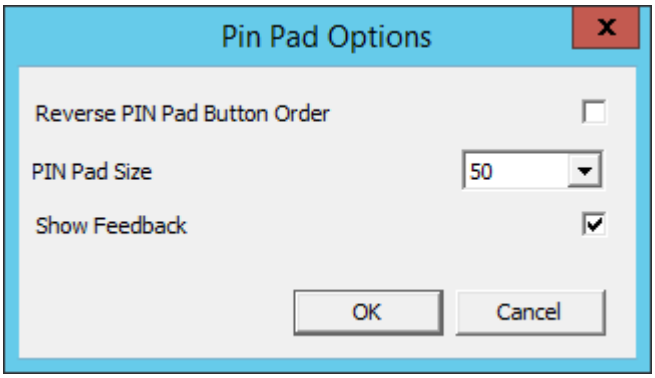
The ***Main Menu Options*** button launches the **Main Options Options** window that has the settings for Main Menu when using Relevance User Services. It is not visible unless Relevance User Services is checked on the **Terminal Mode Selection** page.



Main Menu Options

The **Main Menu Options** window has several settings.

- ***Allow Reboot/Restart*** – This checkbox adds a Restart and Reboot button to the Main Menu on the Terminal so that the Terminal can be rebooted or restarted from the Terminal.
- ***Show Main Menu on Selector*** – This checkbox will list the Main Menu as an option on the Display Client drop-down menu.
- ***Show Virtual Keyboard*** – This checkbox will launch a virtual keyboard the Main Menu is opened so that the operator can manually log in.



Pin Pad Options Window

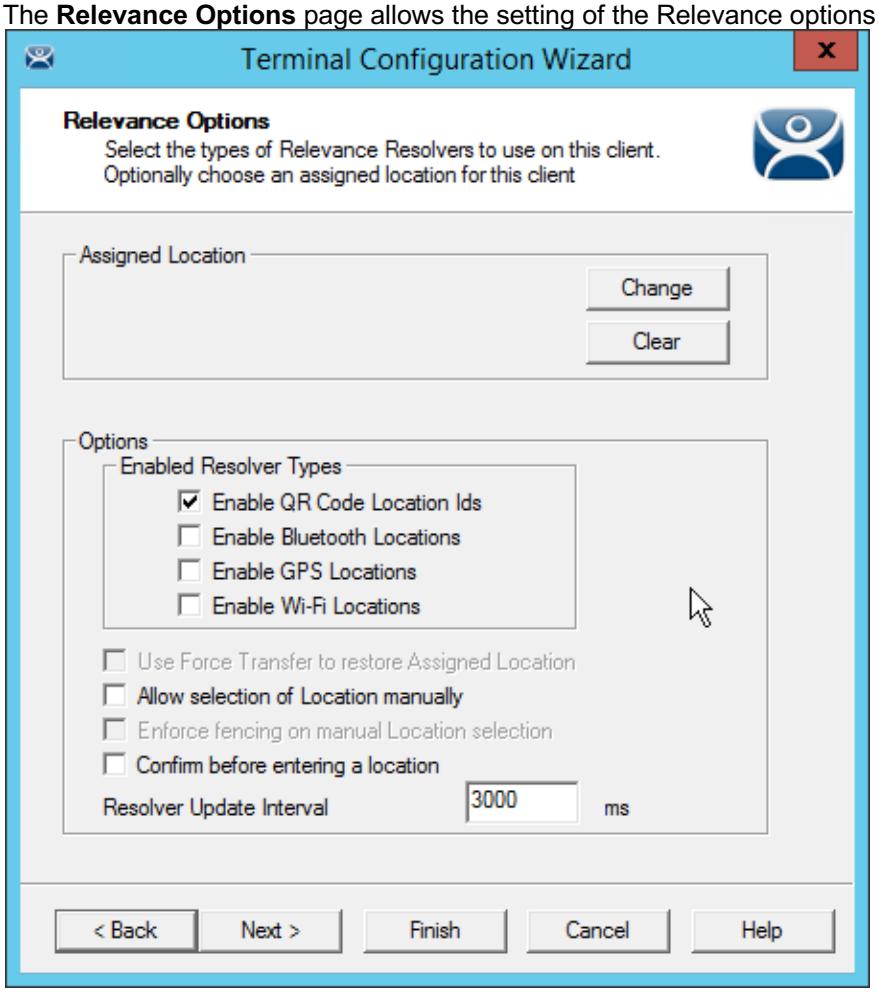
The Pin Pad Options window allows you to configure the PIN pad when using a Personal Identification Number instead of a password.

- ***Reverse Pin Pad Button Order*** – This checkbox changes the pin pad from 1-2-3 on the top row like a phone to 7-8-9 on the top row like a calculator.
- ***Pin Pad Size*** – This sets the size of the pin pad as a percentage of the screen.

Select the ***Next*** button on the **Terminal Interface Options** page to configure the hotkeys.

19.1.7. Relevance Options Page

The **Relevance Options** page allows the setting of the Relevance options.



Relevance Options Page

Select the Options before choosing a location. Once the Location is assigned the Options are locked.

- ✓ **Select the Options before choosing a location. If you need to change an option you can clear the location with the Clear button, change the option, and then re-assign the Location.**

The Options include:

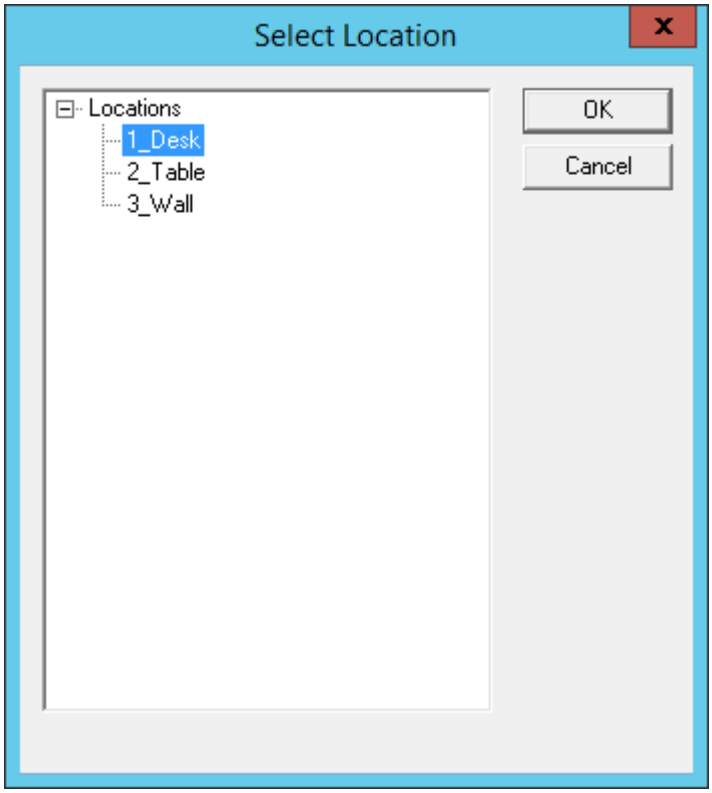
- ***Use Force Transfer to restore Assigned Location*** – This checkbox lets an operator to restore a transferred session without asking permission.
- ***Allow Selection of the Location manually*** – This will let the user select the location manually from a menu on the mobile device. If this is unselected then the user must use a Resolver.
- ***Enforce fencing on a manual Location selection*** – This checkbox, if unselected, allows a manual login anywhere from that Terminal. This might be helpful on a control room Terminal. If selected this will enforce fencing on that Terminal when selecting a location manually.
- ***Confirm before entering a location*** – This checkbox enables a dialog box that will be shown each time a user enters an area.
- ***Resolver Update interval*** – This is the frequency that the resolver updates.

Enable Resolver Types – Relevance has several methods of resolving the location to allow specific applications to get sent to specific locations.

- ***Enable QR Code Location Ids*** – This allows the scanning of a QR code to determine the location.
- ***Enable Bluetooth Locations*** – This allows the use of Bluetooth beacons to determine the location.
- ***Enable GPS Locations***– This allows the Global Positioning System of the mobile device to determine the location.
- ***Enable Wi-Fi Locations*** – This allows the signal strength of Wi-Fi access points to determine the location.

Each method selected will require configuration to associate a location with the Resolver data.

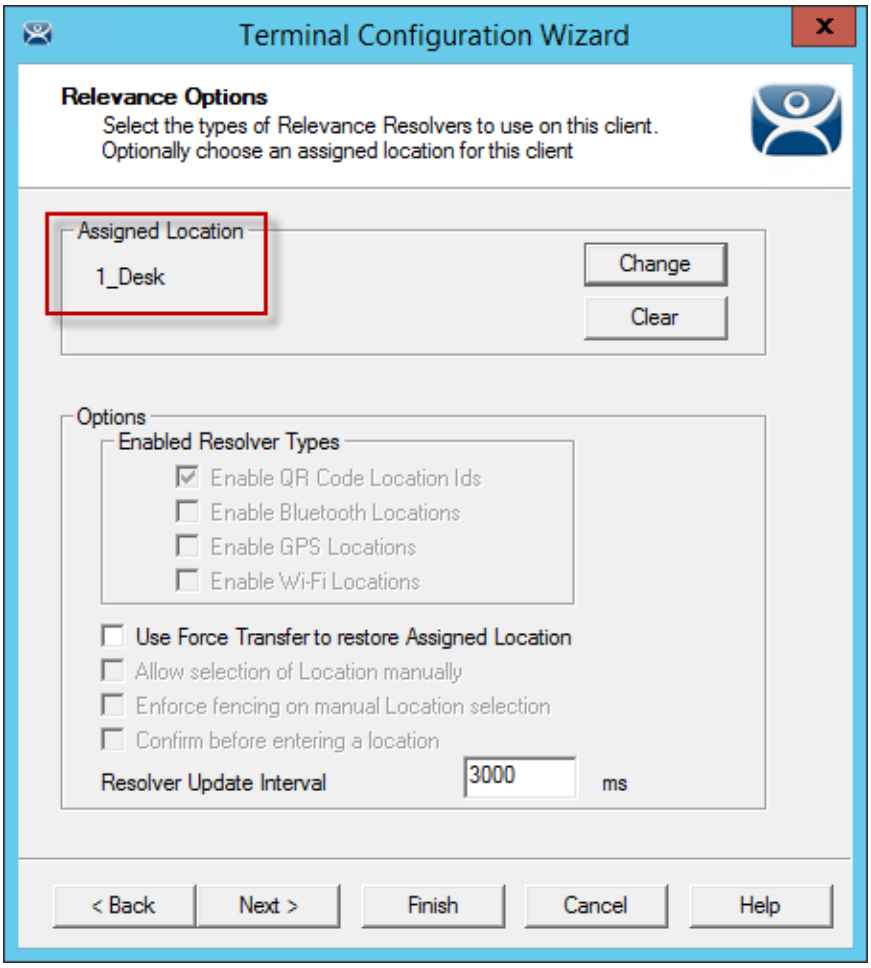
Select the ***Change*** button to open the **Select Location** window.



Select Location Window

The created **Locations** will be displayed in the **Select Location** tree.

Highlight the desired Location and select the ***OK*** button.



Location Assigned

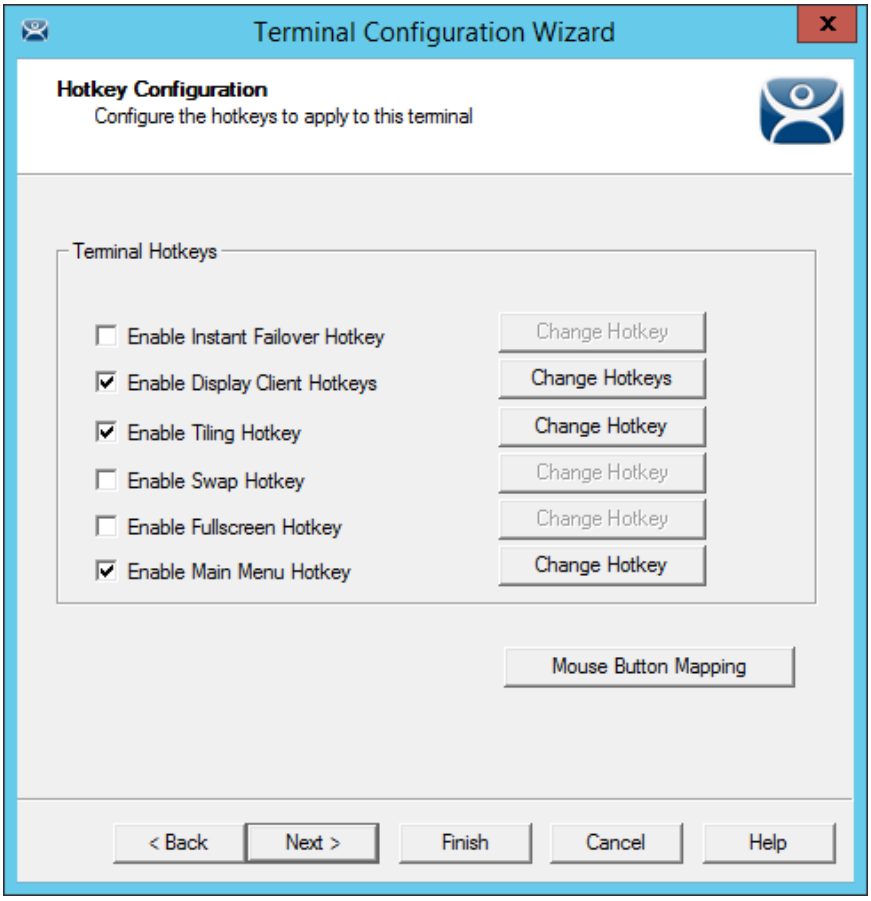
. Once the Location is assigned the Options are locked.

- ✓ **If you need to change an option you can clear the location with the *Clear* button, change the option, and then re-assign the Location.**

Once the location is assigned select ***Next*** and navigate to the **Hotkey Configuration** page.

19.1.8. Hotkey Configuration Page

The **Hotkey Configuration** page allows you to configure hotkeys for display client switching and menu launching.



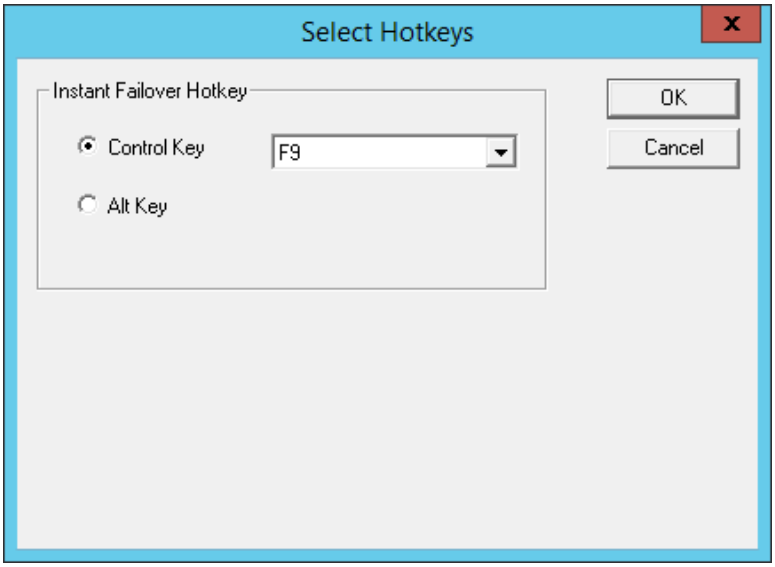
Hotkey Configuration Page of the Terminal Configuration Wizard

Terminal Hotkeys on the **Hotkey Configuration** page allows the selection of keyboard combinations that allow switching between sessions.

- ***Enable Instant Failover Hotkeys*** - This checkbox, if selected, allows the hot key switching between the two active sessions of a Display Client that is using Instant Failover. The Terminal needs to be using a display client with Instant Failover for this to be active.
- ***Enable Display Client Hotkeys*** - This checkbox, if selected, allows the hot key switching between different sessions of a Terminal using MultiSession.
- ***Enable Tiling Hotkey*** – This checkbox, if selected, allows SessionTiling to be activated by a hotkey combination. Tiling has to be selected on the Terminal Interface Options page for this to be active.
- ***Enable Swap Hotkey*** – This checkbox, if selected, allows a hotkey to swap virtual screens instead of a mouse click.
- ***Enable Fullscreen Hotkey*** – This checkbox, if selected, allows the virtual screen to go full sized with a hotkey.
- ***Enable Main Menu Hotkey*** – This checkbox, if selected, allows a hotkey to launch the Main Menu

- ***Mouse Button Mapping -*** – This button opens the **Mouse Mapping Option** window that allows functions to be assigned to mouse buttons.

Selecting the ***Change Hotkeys*** button when ***Enable Instant Failover Hotkeys*** is selected will allow the hotkeys to be changed from the default.

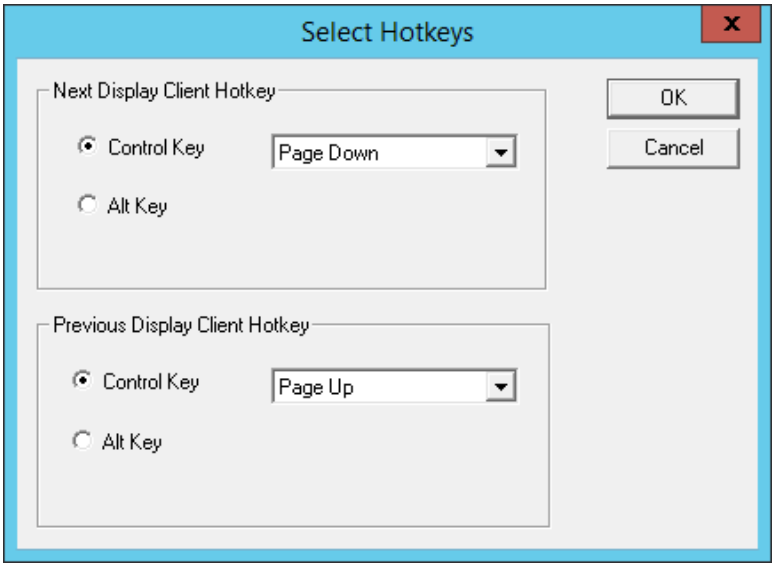


Select Hotkeys for Instant Failover

The default hotkey for Instant Failover switching is set to ***Control+F9***. This can be changed by selecting the ***Alt Key*** radio button or using the drop-down to select another function key.

Select the ***OK*** button to accept changes or the ***Cancel*** button to close.

Selecting the ***Change Hotkeys*** button when ***Enable Group Hotkeys*** is selected will allow the MultiSession switching hotkeys to be changed from the default.

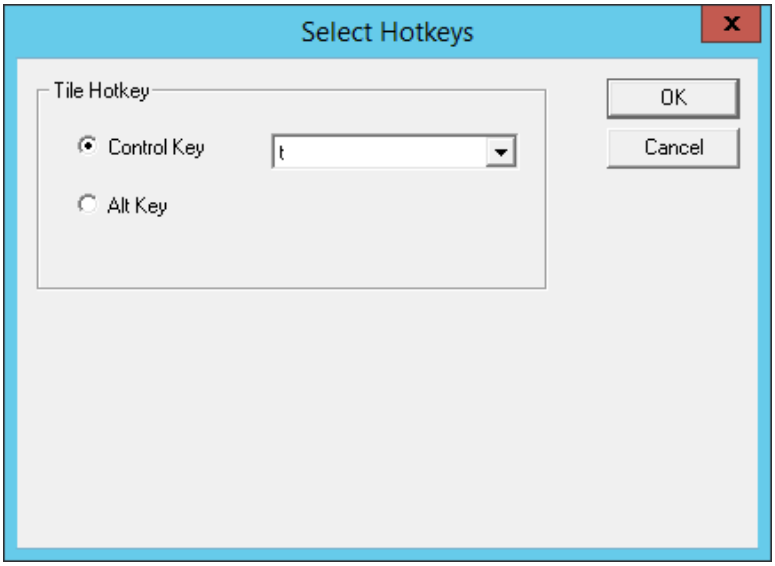


Select MultiSession Switching Hotkeys

The default hotkey for MultiSession switching is set to ***Control+Page Up*** and ***Control+Page Down***. This can be changed by selecting the ***Alt Key*** radio button or using the drop-down to select another hot key.

Select the ***OK*** button to accept changes or the ***Cancel*** button to close.

Selecting the ***Change Hotkeys*** button when ***Enable Tiling Hotkeys*** is selected will allow the hotkeys to be changed from the default.



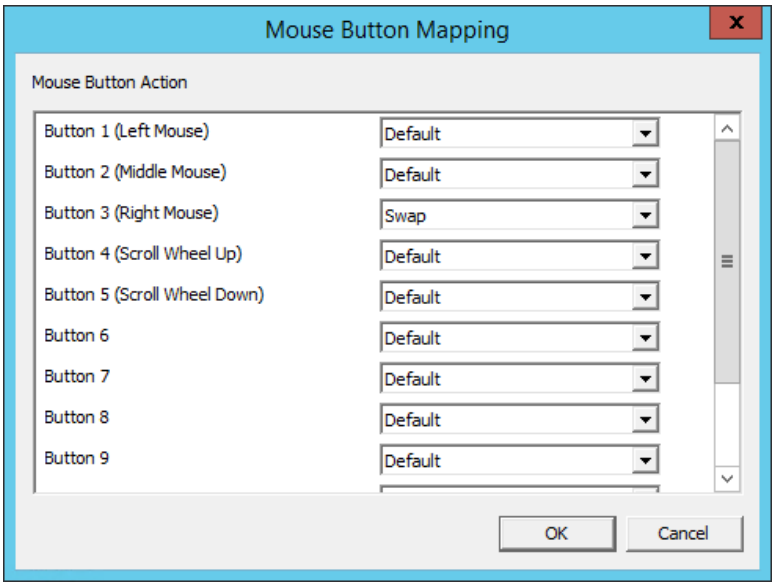
Select SessionTiling Hotkeys

The default hotkey for SessionTiling activation is set to ***Control+t***. This can be changed by selecting the ***Alt Key*** radio button or using the drop-down to select another hot key.

Select the ***OK*** **button** to continue or the ***Cancel*** button to close without accepting changes.

Select the ***Next*** button on the **Hotkey Configuration** page to configure the configuration.

Selecting the ***Mouse Button Mapping*** button will open the ***Mouse Button Mapping*** window.



Mouse Button Mapping

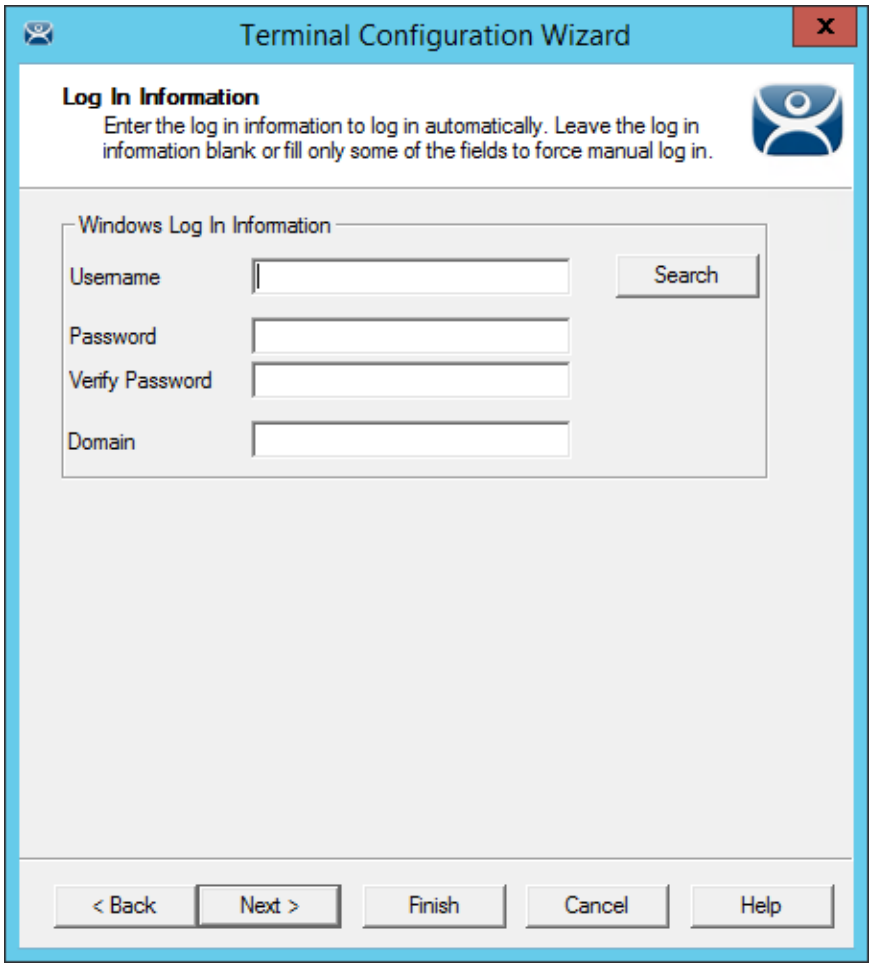
The ***Mouse Button Mapping*** window allows you to configure actions for the mouse buttons through drop-down menus.

Select ***OK*** to accept the setting and close the window.

19.2. User Accounts in the Terminal Configuration Wizard

Each Terminal needs a unique Windows account to start sessions on Windows Remote Desktop Servers.

These Windows accounts can be created locally on each Remote Desktop Server or in an Active Directory for domain accounts using standard Windows procedures. You may apply Microsoft security as desired.

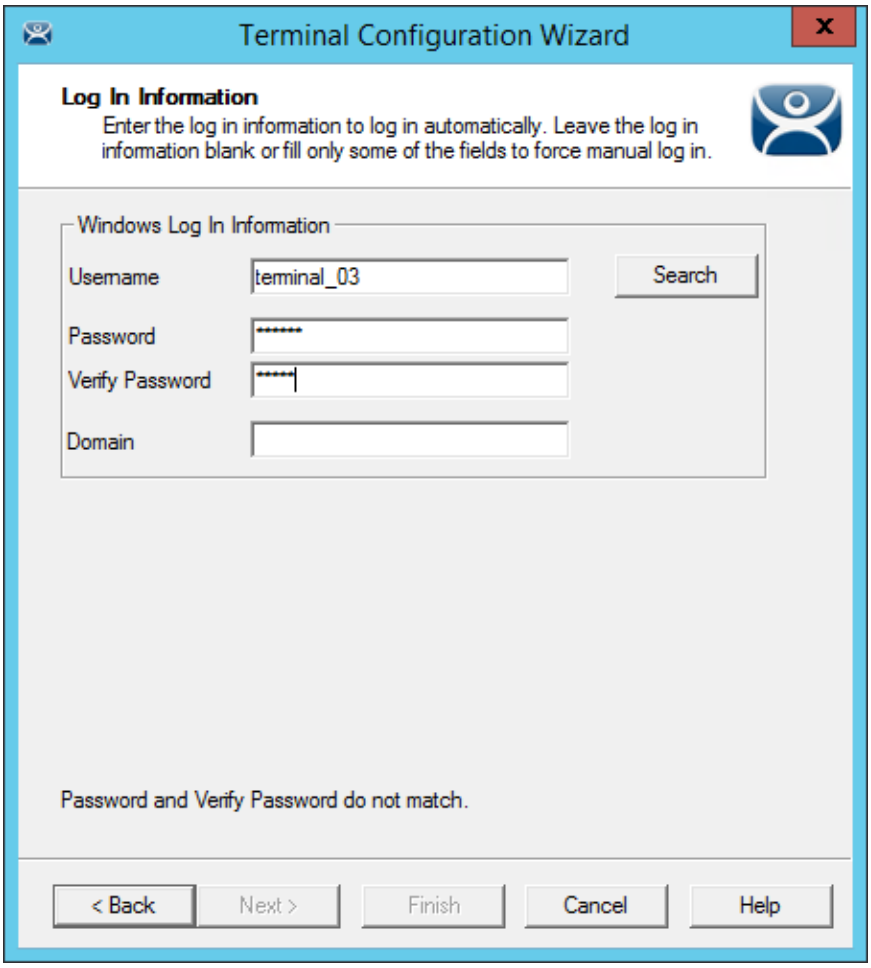


Log In Information Page of the Terminal Configuration Wizard

Leaving the ***Windows Log In Information*** fields blank will force the user to manually log into their sessions. This is useful for office settings or shared Terminals. Each user logs in with their personal account and gets the privileges that the administrator granted them.

19.2.1. Local Windows User Accounts

Filling the ***Windows Log In Information*** fields with an established Windows account allows the Terminal to automatically log in and start sessions without user action. This is useful in industrial settings where the Terminals are public and running 24/7.



Log In Information Page of the Terminal Configuration Wizard

Enter a local Windows account in the ***Username*** field. Enter its password in the ***Password*** and ***Verify Password*** fields if you want to have the Terminal automatically log in.

Leaving these fields blank will require the user to manually logon each time the Terminal connects.

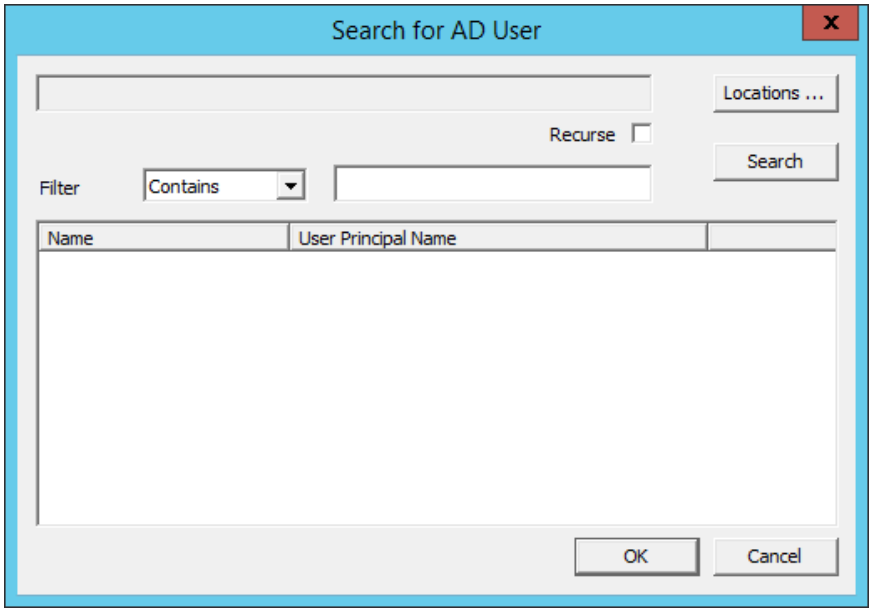
- Individual display clients can be set to require a manual login by unselecting the ***Allow Auto-Login*** checkbox on the **Remote Desktop Services and Workstation Options** page of the **Display Client Wizard**.
- You may use a domain Windows account by adding the domain to the ***Domain*** field.
- Individual display clients can be set to use a different Windows account than the Terminal by using the ***Override*** button on the **Display Client Selection** page of the **Terminal Configuration Wizard**.

Select the ***Next*** button to configure the configuration.

19.2.2. Active Directory User Login Account

A ThinManager Server in a domain may pull an Active Directory account into the ***Username*** field using the ***Search*** button. This launches a series of windows that allow you to select a domain user account for the Terminal login account.

Selecting the ***Search*** button will launch a **Search for AD User** window that allows you to select an Active Directory user.



Search for AD User Window

The **Search for AD User** window has a ***Location*** button that allows you to search the Active Directory locations.

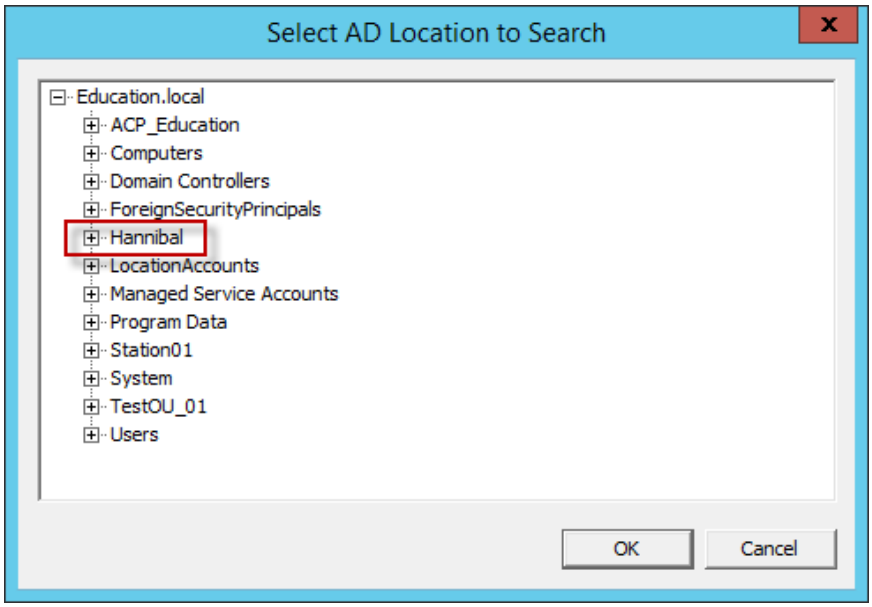
Buttons:

- ***Locations*** – This opens the **Select AD Location to Search** window to select the Organizational Unit (OU) to search.
- ***Search*** – This searches the selected OU and populates the ***Name*** field with the OU members.

Options:

- ***Filter*** – This drop-down will filter the results with either the ***Contains*** or ***Starts With*** function and the entry of the textbox.
- ***Recurse*** – This sets the ***Search*** function to search nested Windows Security Groups when searching a Windows Security Group. The ***Choose AD Synchronization Mode*** needs to be set to **Security Group** on the **Active Directory System Settings** window to work. This window is opened from ***Manage > Active Directory > Settings***.

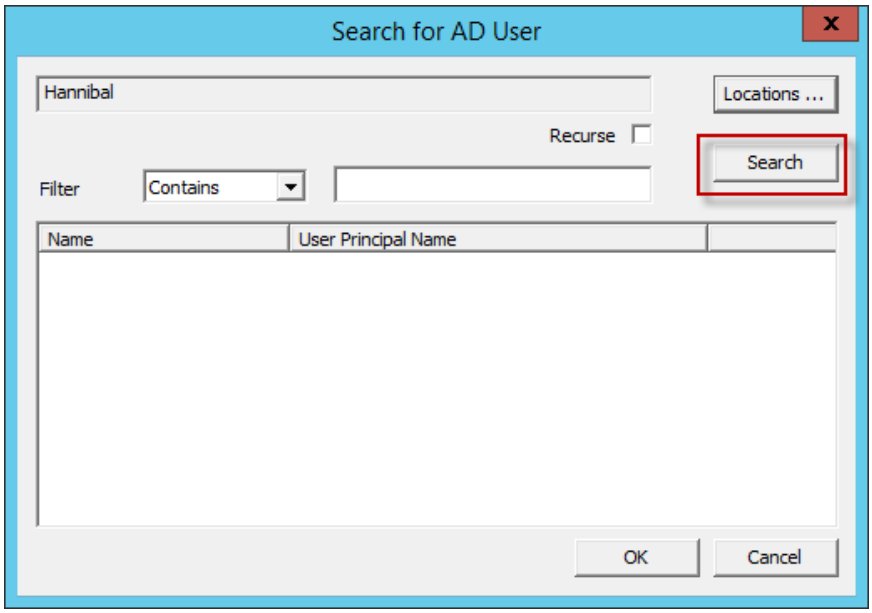
Select the ***Locations…*** button to launch the **Select AD Location to Search** window.



Select AD Location to Search Window

Continue with the wizard by selecting the branch of the Active Directory tree that contains your administrative user account.

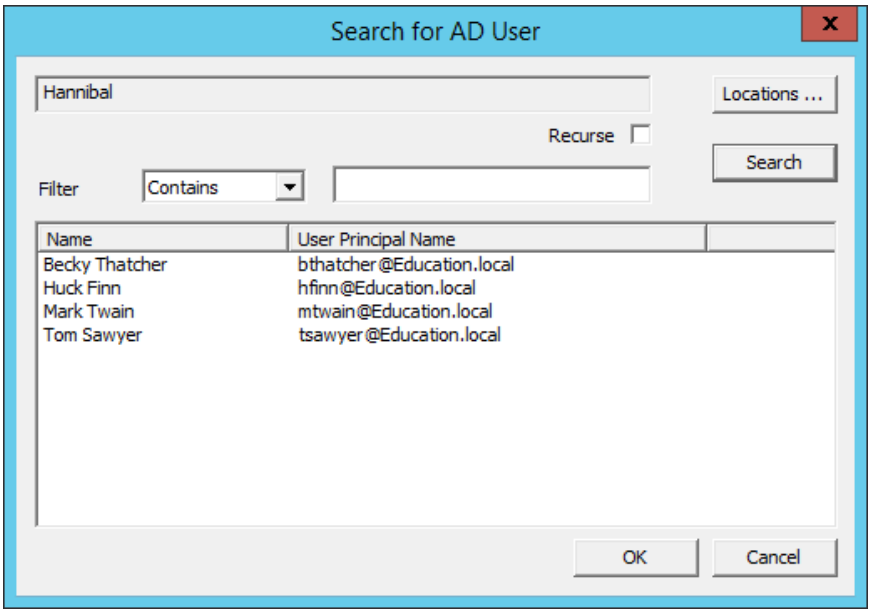
Highlight it and select the ***OK*** button.



Search Organizational Unit

Once you select an organizational unit and select the OK button the OU will be listed as the location.

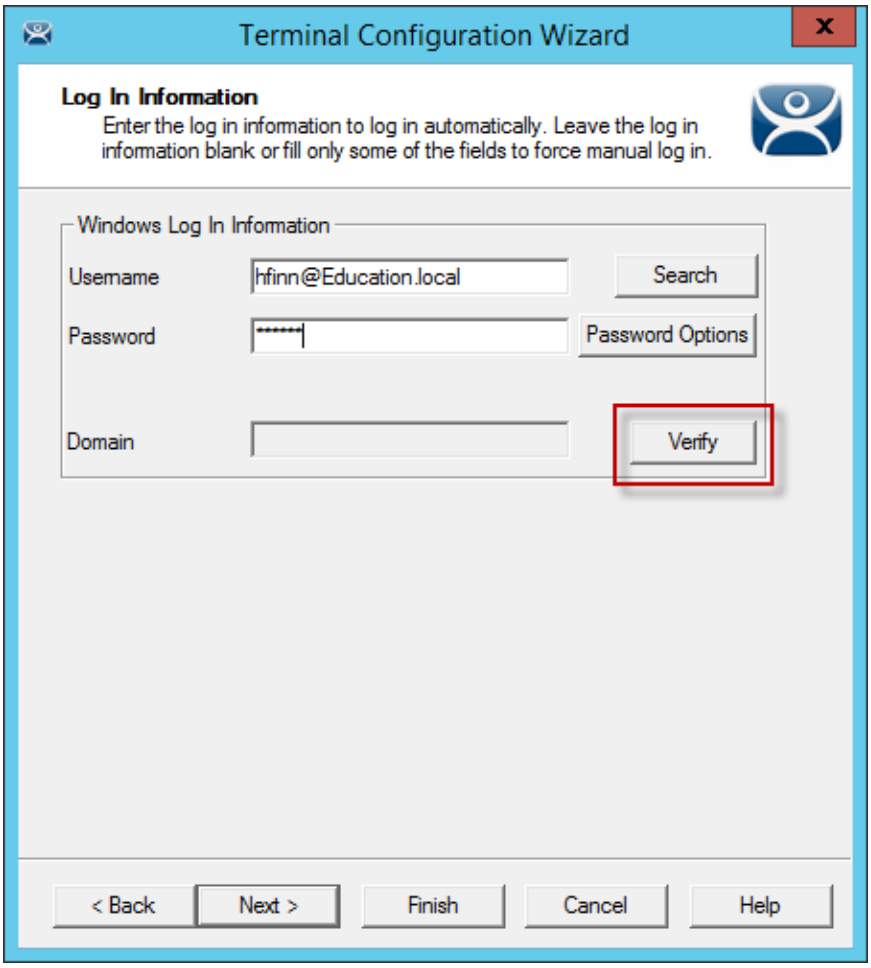
Select the Search button to populate with the users.



Search for AD User Window

Highlighting an Active Directory branch in the **Select AD Location to Search** window and selecting the ***OK*** button will re-open the **Search for AD User** window with the list of domain users from that branch.

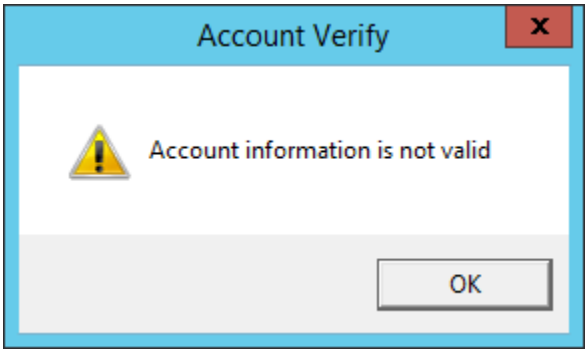
Highlight the desired user and select ***OK***. This will add the domain user to the ***Username*** field of the Terminal Configuration Wizard.



Remote Desktop Server Name - Remote Desktop Server Wizard –Domain

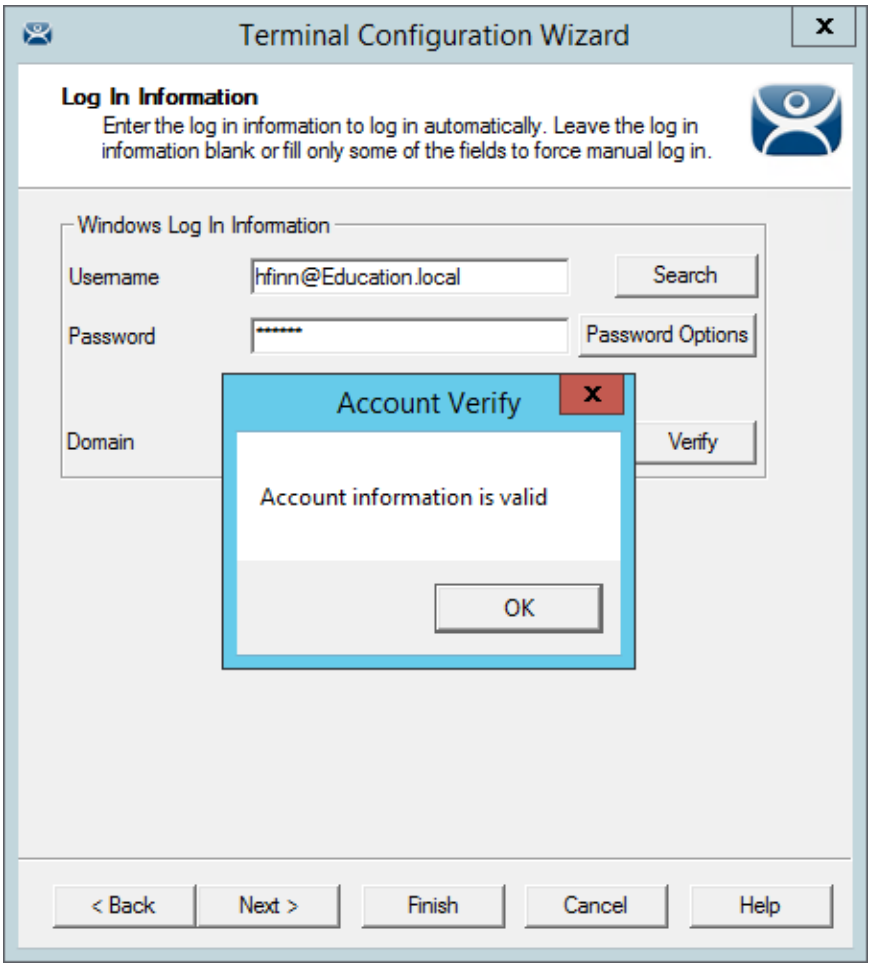
Once the domain user is in the ***User Name*** field of the Terminal Configuration Wizard you need to add the correct password to the ***Password*** field.

The ***Verify*** button will check the entered password and tell you if it is valid or incorrect. Once you have received a positive result select the ***Next*** button to continue with the wizard.



Invalid Account Message

If you receive a message of an invalid account try the correct password.

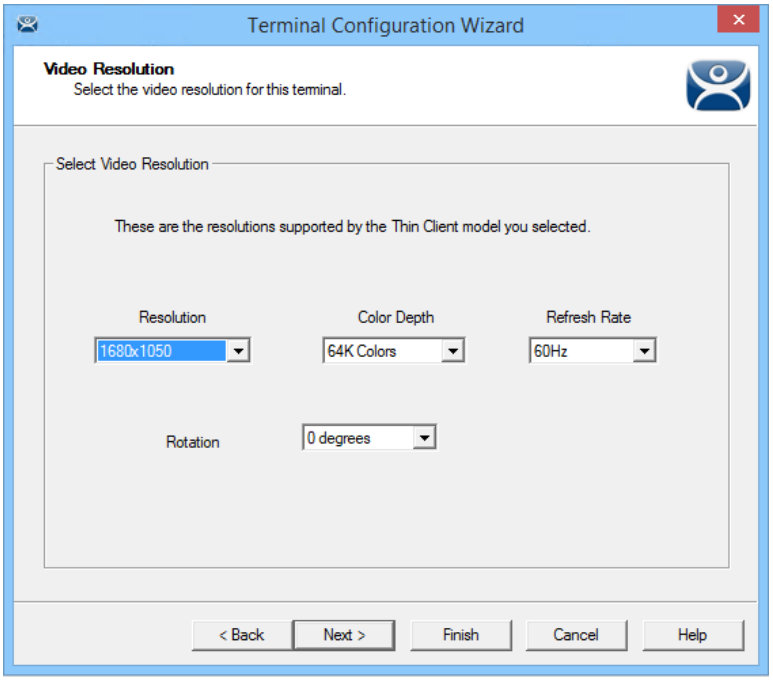


Valid Password Message

Once you have a valid user account select the ***Next*** button to continue the configuration wizard.

19.2.3. Video Resolution Page

The Video Resolution page allows the Terminal resolution to be set.



Video Resolution of the Terminal Configuration Wizard

The Video Resolution page of the Terminal Configuration Wizard lets you choose the ***Resolution***, ***Color Depth***, and ***Refresh Rate*** for your monitor.

The resolutions in the drop-down are dependent on the make and model of hardware used.

A *Rotation* drop-down allows you to configure the monitor in Portrait Mode. The default is *0 degrees* which provides landscape mode.

Selecting an option from the *Rotation* drop-down will change the display. The options are

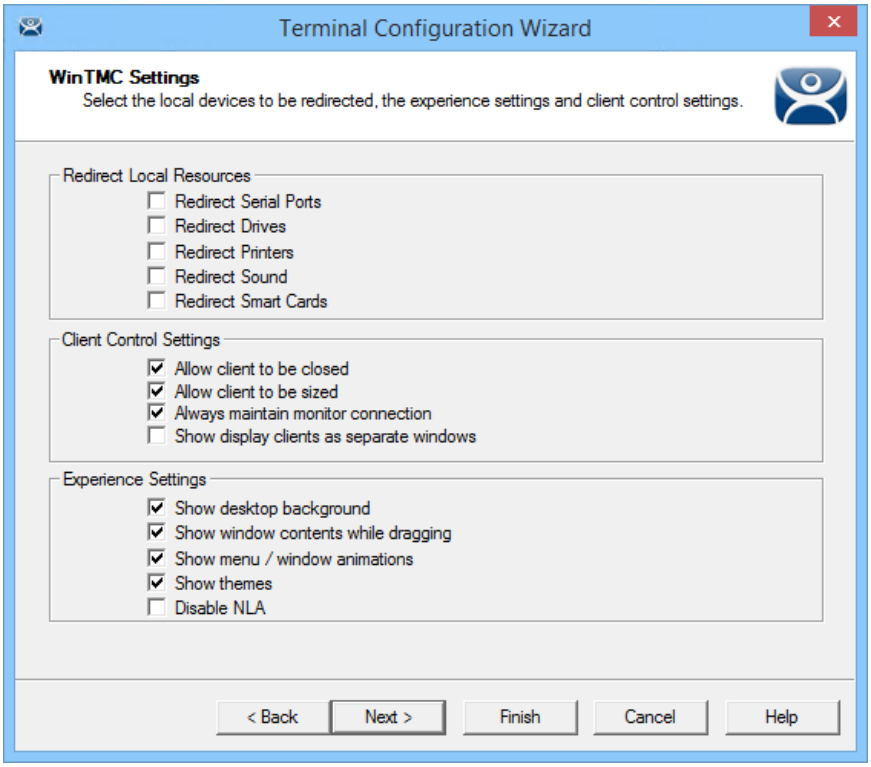
- 0 degrees (default)
- 90 degrees
- 180 degrees
- 270 degrees.

Select the angle which matches the monitor orientation.

Select the ***Next*** button to configure the configuration.

19.2.4. WinTMC Settings

A Terminal configured as a WinTMC Terminal will display a WinTMC Settings page.



WinTMC Settings Page

The **Terminal Configuration Wizard** includes a **WinTMC Settings** page for WinTMC clients. These only apply to connections made by the WinTMC application.

The settings include:

Redirect Local Resources:

- **Redirect Serial Ports** - This checkbox, if selected, will make local serial ports available in a session. Serial Port redirection does not work when you connect to a Remote Desktop Server running Windows 2000 or earlier.
- **Redirect Drives** - This checkbox, if selected, will make local drives available in a session. Drive redirection does not work when you connect to a Remote Desktop Server running Windows 2000 or earlier.
- **Redirect Printers** - This checkbox, if selected, will make your local printer available in a session.
- **Redirect Sound** - This checkbox, if selected, will allow audio played in your session to play locally. Sound redirection does not work when you connect to a Remote Desktop Server running Windows 2000 or earlier.
- **Redirect Smart Cards** - This checkbox, if selected, will make your smart card available in a session. Smart card redirection does not work when you connect to a Remote Desktop Server running Windows 2000 or earlier.

Client Control Settings:

- **Allow Client to be closed -** This checkbox, if selected, will enable your user to close the client (WinTMC program).

- **Allow client to be sized -** This checkbox, if selected, will enable your user to resize the client.
- **Always maintain monitor connection** – Enable this setting to keep the monitoring connection active when WinTMC is closed to allow shadowing. Unselecting this checkbox will release the WinTMC license when the WinTMC program is closed but will deny shadow access.
- **Show groups in separate windows** – This checkbox, if selected, will display multiple Display Clients as separate windows rather than in one window shell.

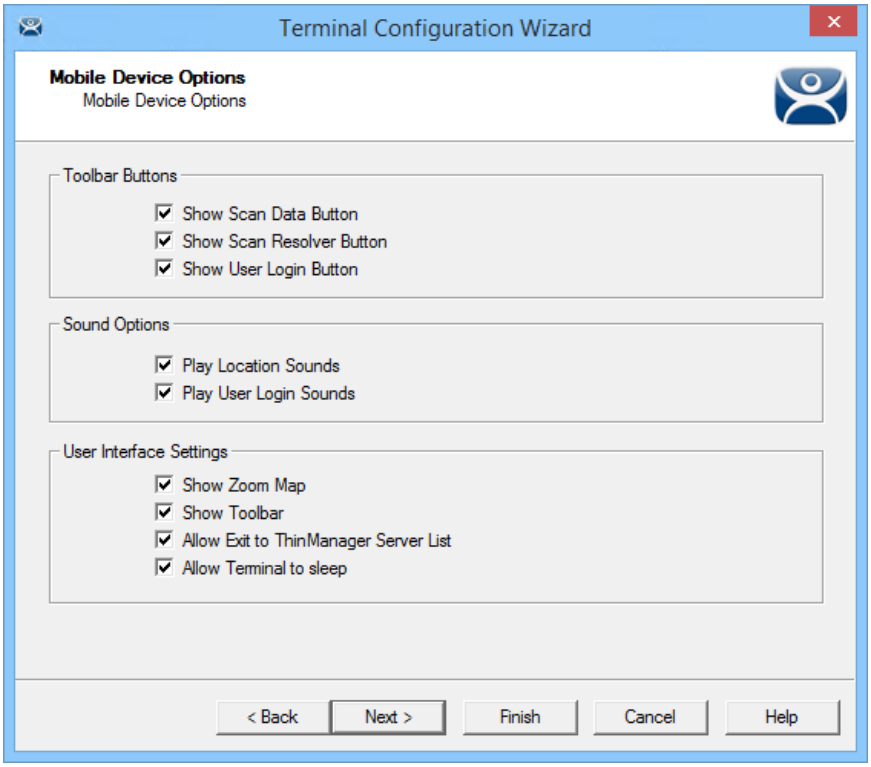
Experience Settings:

- **Show Desktop Background -** This checkbox, if selected, will enable your user to select a Windows Desktop Background. If not selected, the background will be a solid color.
- **Show window contents while dragging -** This checkbox, if selected, will show the window contents to be shown while the window is being dragged.
- **Show menu/window animations -** This checkbox, if selected, will enable menu/window animations on the client.
- **Show Themes -** This checkbox, if selected, will enable your user to select a Windows Theme.

Note: These functions may be denied by user policies or Remote Desktop Server configuration. Check the Microsoft Local Policy, Group Policy, and Remote Desktop Services Configuration.

19.2.5. Mobile Device Settings

A Terminal configured as an Android or Apple iOS Terminal will display a **Mobile Device Options** page.



Mobile Device Options

The **Mobile Device Options** window has several settings that control the user experience on mobile devices. It will only be displayed when configuring an Android or iPad Terminal.

This page allows you to disable features normally displayed in the mobile apps.

Toolbar Buttons

- ***Show Scan Data Button*** – This checkbox, when unselected, will hide the Scan Data button.
- ***Show Scan Resolver Button***– This checkbox, when unselected, will hide the Scan Resolver button.
- ***Show User Login Button***– This checkbox, when unselected, will hide the User Login button.

Sound Options

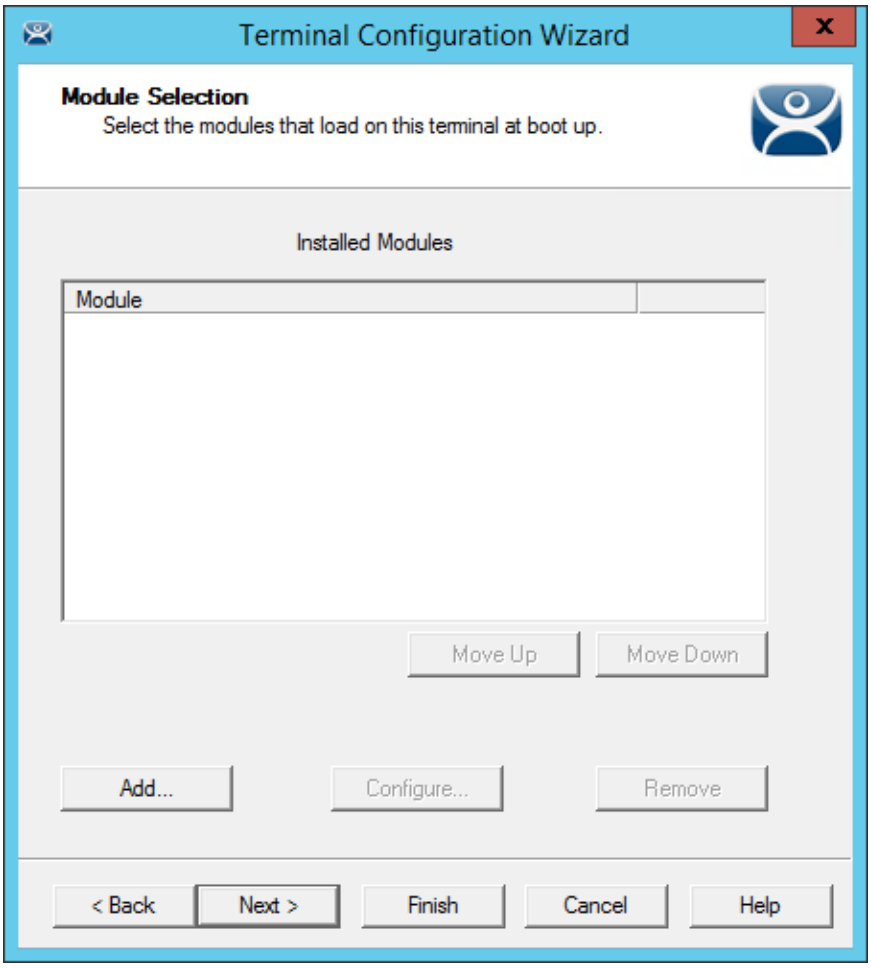
- ***Play Location Sounds*** – This checkbox, when selected, will play a sound when a location is entered.
- ***Play User Login Sounds*** – This checkbox, when selected, will play a sound when the user logs in as a TermSecure or Relevance user.

User Interface Settings

- ***Show Zoom Map*** – This checkbox, when unselected, will hide the screen map while zooming.
- ***Show Toolbar*** – This checkbox, when unselected, will hide the app toolbar.
- ***Allow Exit to ThinManager Server List*** – This checkbox, when unselected, will prevent the user from leaving the app to switch ThinManager Servers.

- ***Allow Terminal to sleep*** – This checkbox, when unselected, will keep a tablet from going into sleep mode.

19.2.1. Module Selection

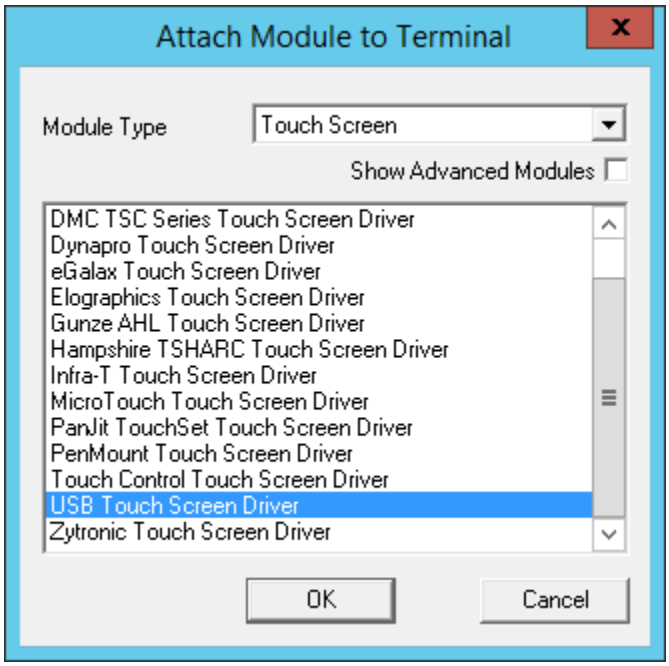


Module Selection Page of the Terminal Configuration Wizard

Modules are components that provide addition functions to a Terminal but aren't required for the running the basic configuration.

Modules include touchscreen drivers, sound drivers, dual Ethernet port modules, USB drives, screen savers and other functions.

The ***Add…*** button launches the **Attach Module to Terminal** window.



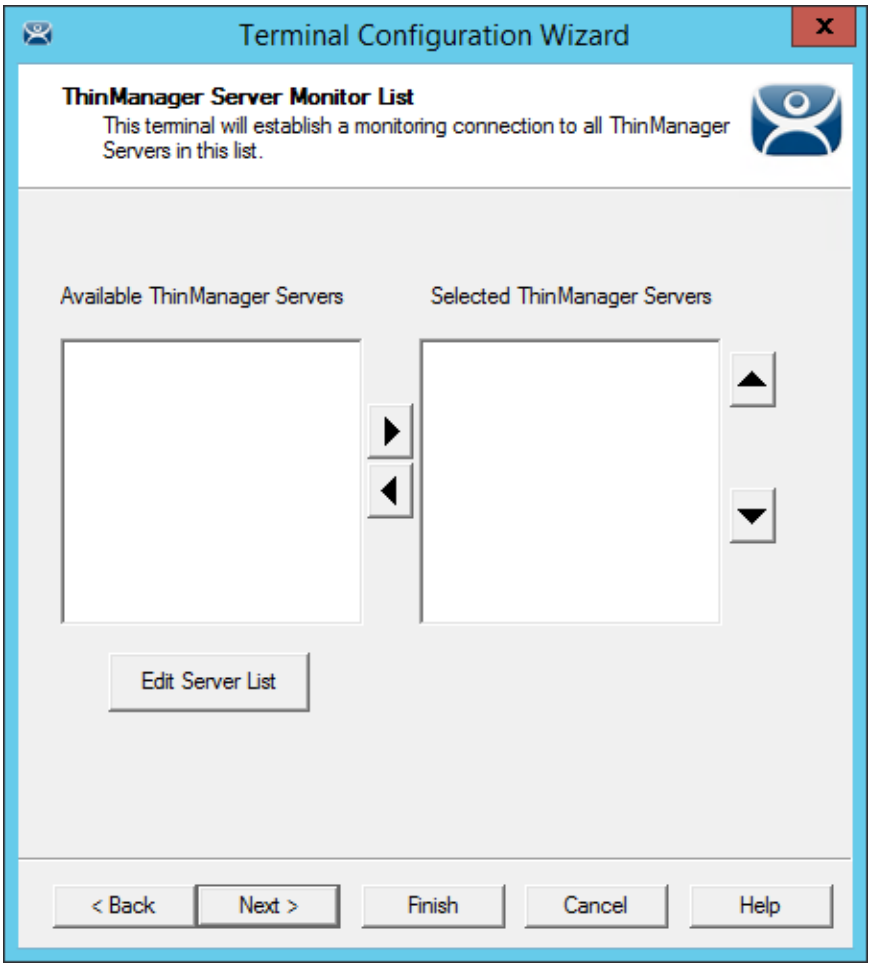
Attach Module to Terminal Window

The **Attach Module to Terminal** window allows you to select a module to add to the Terminal.

The ***OK*** button will add the module and the ***Cancel*** button will close the window without adding the module.

Modules are covered in detail in Modules starting on page 362.

Select the ***Next*** button on the **Module Selection** page to continue the configuration.



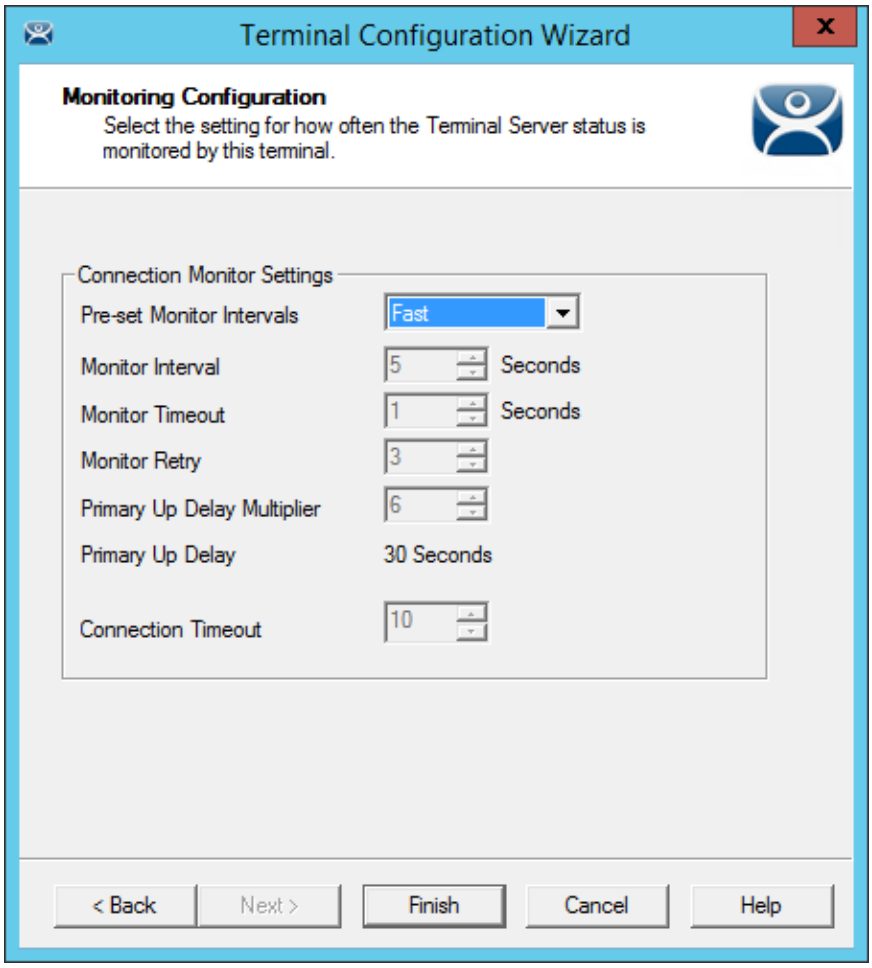
ThinManager Server Monitor List Page

The **ThinManager Server Monitor List** page is a legacy page from early versions of ThinManager and is not used.

This page was used before Auto-Synchronization was added to ThinManager. This page was needed to list the ThinManager Servers for the Terminals. Auto-Synchronization does this automatically so the page will not show if using Auto-Synchronization.

This page was left to prevent problems when upgrading from an old ThinManager system to a modern one.

Select the ***Next*** button to configure the configuration.



Monitoring Connection Page of the Terminal Configuration Wizard

The Monitoring Configuration page sets the speed that failover is detected and initiated. A thin client creates a socket connection to the Remote Desktop Server. If the socket is disconnected the Terminal will try to reconnect and failover based on these settings.

✓ **The "Fast" setting is a good setting to use.**

These are the settings in case you want to tweak your system.

- ***Pre-set Monitor Interval***
  - ***Fast/Medium/Slow*** – These settings have a set rate for the frequency that the Remote Desktop Server status is checked.
  - ***Custom*** – This setting allows the administrator to change the settings from the defaults.
- ***Monitor Interval*** – This is the period of time the Terminal will wait after losing the socket connection before it tries to reconnect.
- ***Monitor Timeout***– This is the period of time the Terminal will wait between tries.
- ***Monitor Retry***- This is the number of times the Terminal will try to reestablish a connection before failing over.
- ***Primary Up Delay Multiplier* -** This is a constant used to generate the Primary Up Delay time.
- ***Primary Up Delay***- This is a delay added (usually set to 30 or 60 seconds) to allow a Remote Desktop Server to get fully booted before the Terminal will try to login. This time period is equal to

the Monitoring Interval times the Primary Up Delay Multiplier.
This prevents a Terminal using Enforce Primary from switching back to its primary Remote Desktop Server before it is ready.

Faster rates will cause a quicker failover but will check on Remote Desktop Server status more often, causing more network traffic. Slowing down the rate will cause less traffic but will slow the failover speed a little.

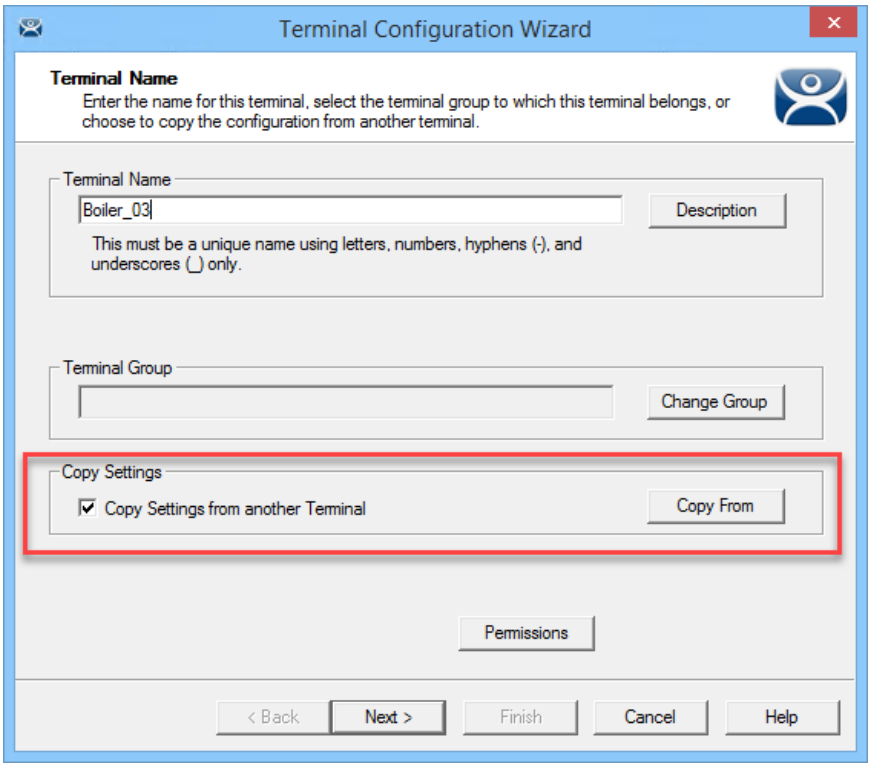
- ***Connection Timeout***– This is the amount of time a Terminal will try to connect to a Remote Desktop Server before giving up and trying the next server.

Select ***Finish*** to save and close or ***Cancel*** to close without saving.

19.3. Copy Settings from another Terminal

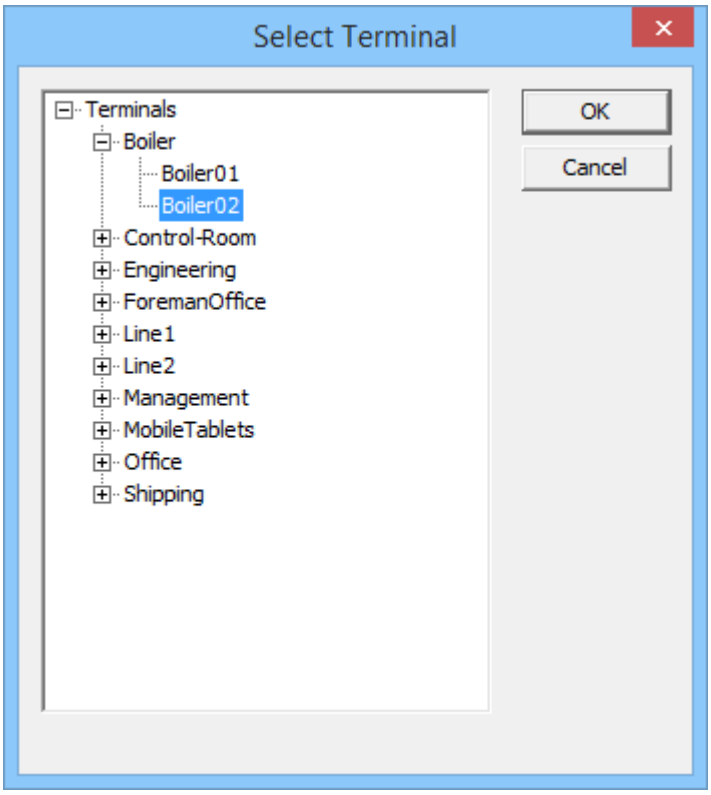
You can copy the settings from one Terminal during the creation process to speed the configuration.

Create a new Terminal by right clicking on the Terminals branch and select ***Add Terminal*** to launch the **Terminal Configuration Wizard**.



Terminal Name Page of Terminal Configuration Wizard

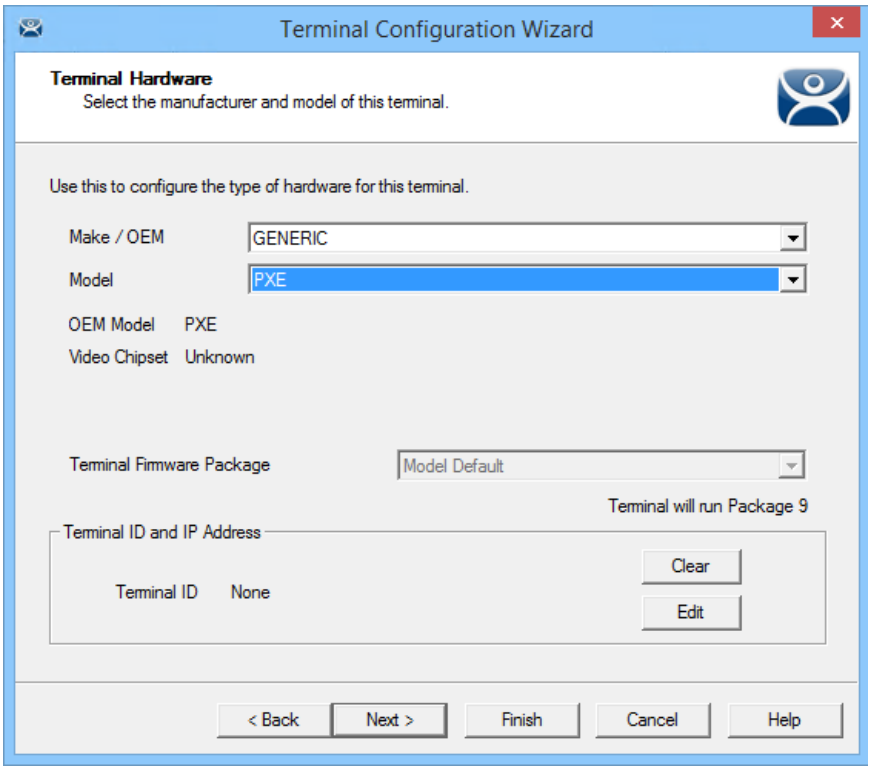
The **Terminal Name** page has a ***Copy Settings from another Terminal*** checkbox. Select this checkbox and click the ***Copy From*** button to launch the **Select Terminal** window.



Select Terminal Window

The **Select Terminal** window will show a tree with all of the created Terminals. Highlight a Terminal and click the ***OK*** button. This will close the window and apply the configuration from the highlighted Terminal to the new Terminal.

Select the ***Next*** button to navigate to the **Terminal Hardware** page.



Terminal Hardware page of the Terminal Configuration Wizard

The new Terminal will need Terminal hardware applied to it.

You will need to select the hardware ***Make*** and ***Model*** before the ***Finish*** button is available.

You should also check the ***Username*** and ***Password*** on the **Login Information** page since every Terminal needs a unique Windows account for logging in.

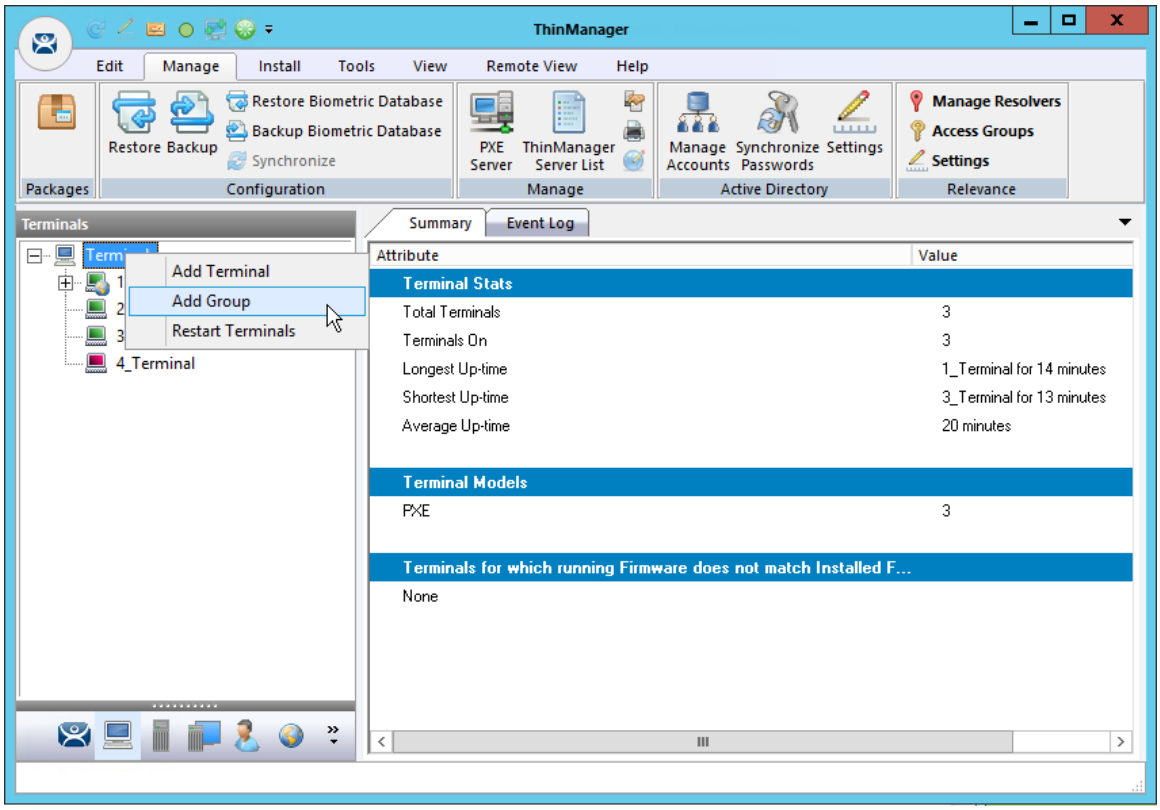
19.4. Using Groups for Organization

ThinManager allows the consolidation of Terminals into Terminal Groups. Groups can be used like folders to organize the Terminals into functional or geographic groups. The ***Group Setting*** checkbox allows settings to be applied to all members of the group to speed configuration and change deployment.

Any group setting is passed down to its members.

The **Group Terminal Configuration Wizard** is launched from the **Terminals** branch of the ThinManager tree.

Open the **Terminals** tree by selecting the **Terminal** icon at the bottom of the ThinManager tree.

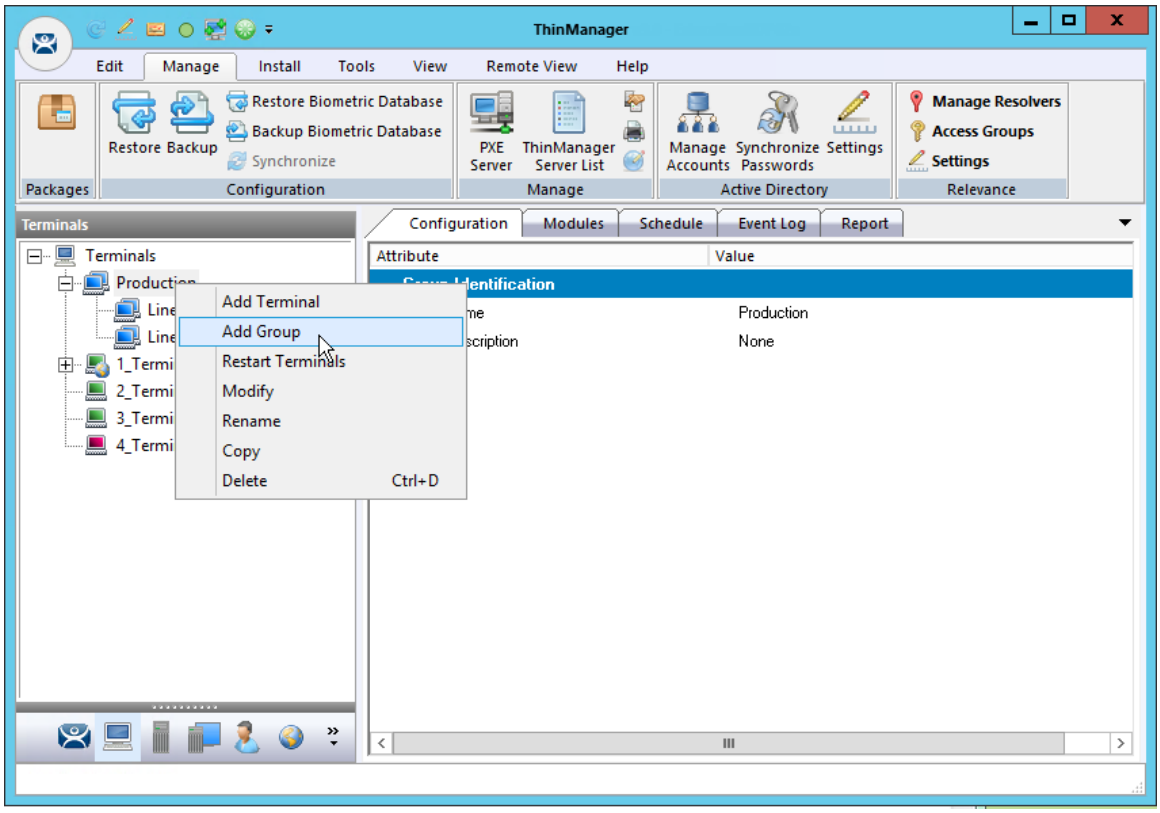


Add Group Command

Right click on the Terminals branch and select ***Add Group*** to launch the **Group Terminal Configuration Wizard**.

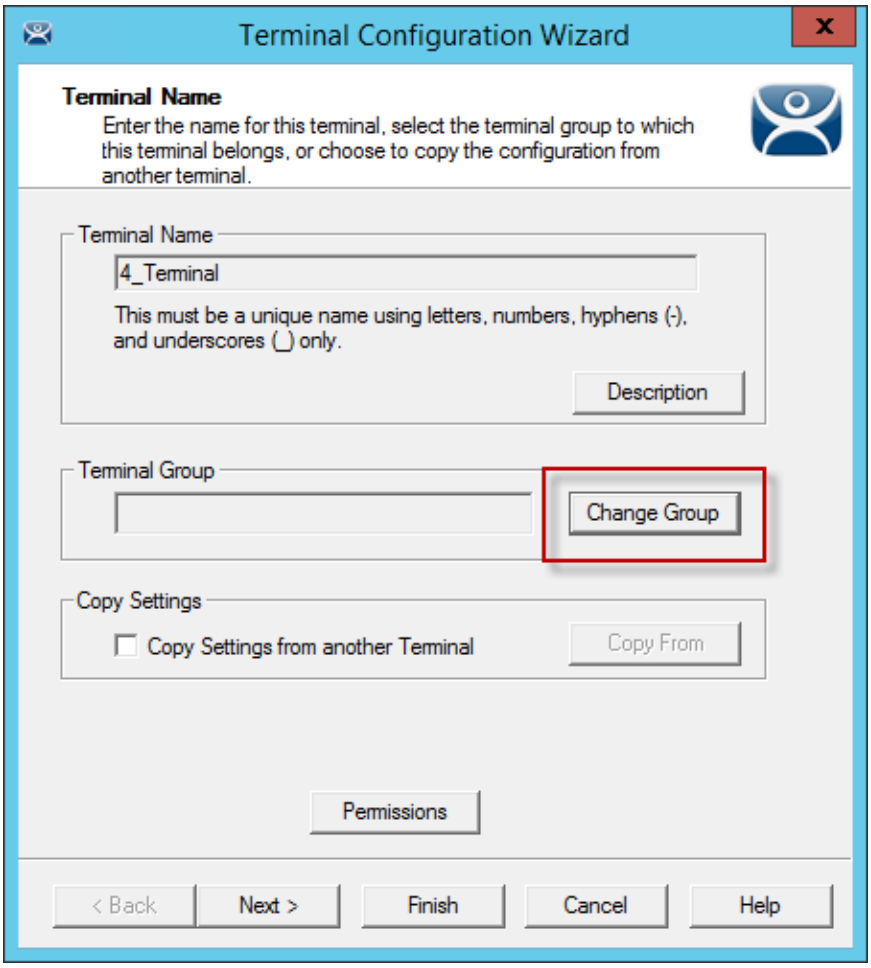
The wizard for the Group parallels the Terminal Configuration Wizard since the group is a collection of Terminals.

A group can be used as a folder to group and organize Terminals.



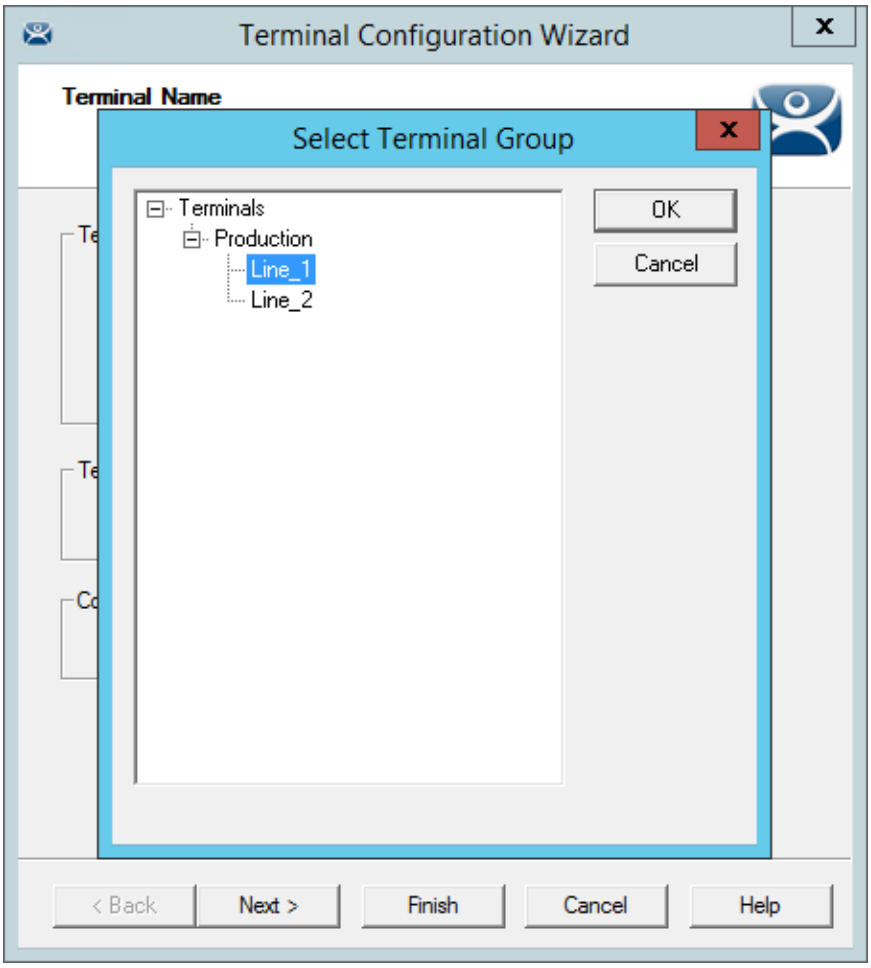
Add Group Menu

You can create sub-groups by highlighting a group, right clicking, and selecting ***Add Group***. It will add a group under the selected group.



Change Group Button

A Terminal can be added to a group by clicking the ***Change Group*** button to launch the **Select Terminal Group** window.

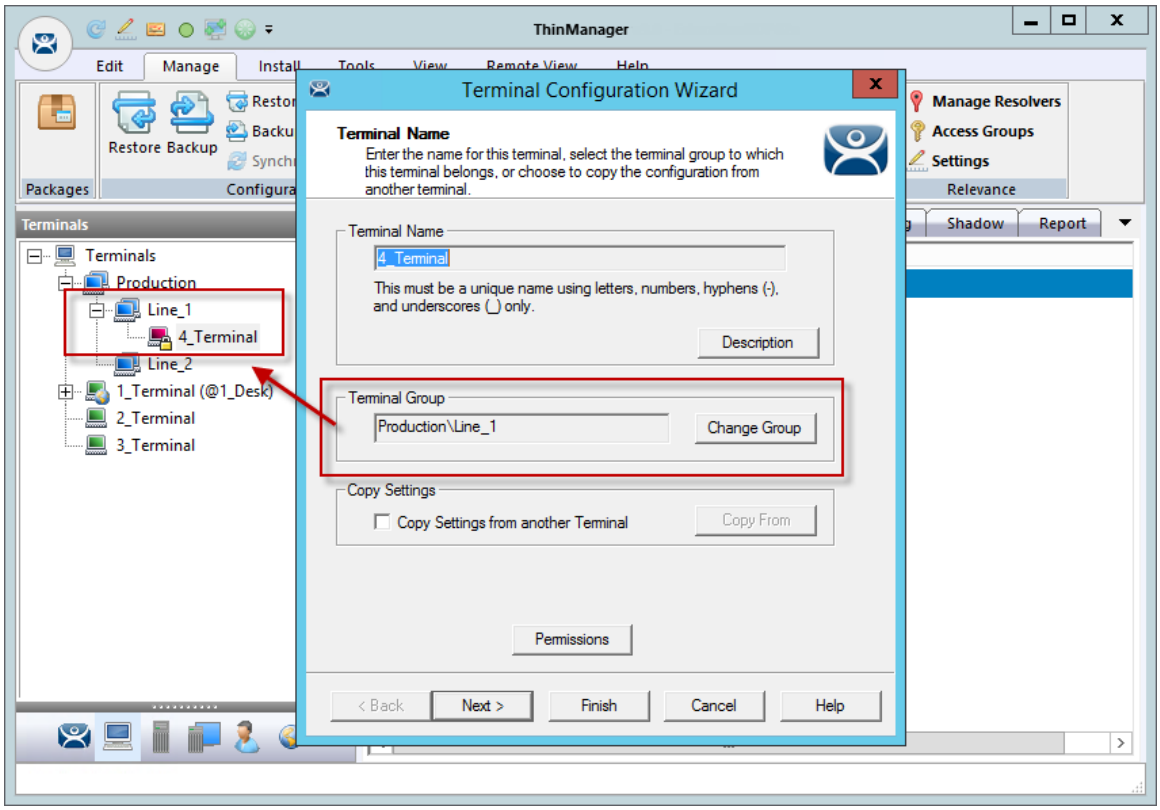


Select Terminal Group Window

The **Select Terminal Group** window will list the groups and subgroups. Expand the tree as needed, highlight the desired group, and select the ***OK*** button.

The Terminal will be assigned to the selected group.

Select the ***Finish*** button to close the wizard and apply the changes before continuing. If you need to adjust the configuration, close the wizard then re-open it.



Group Membership

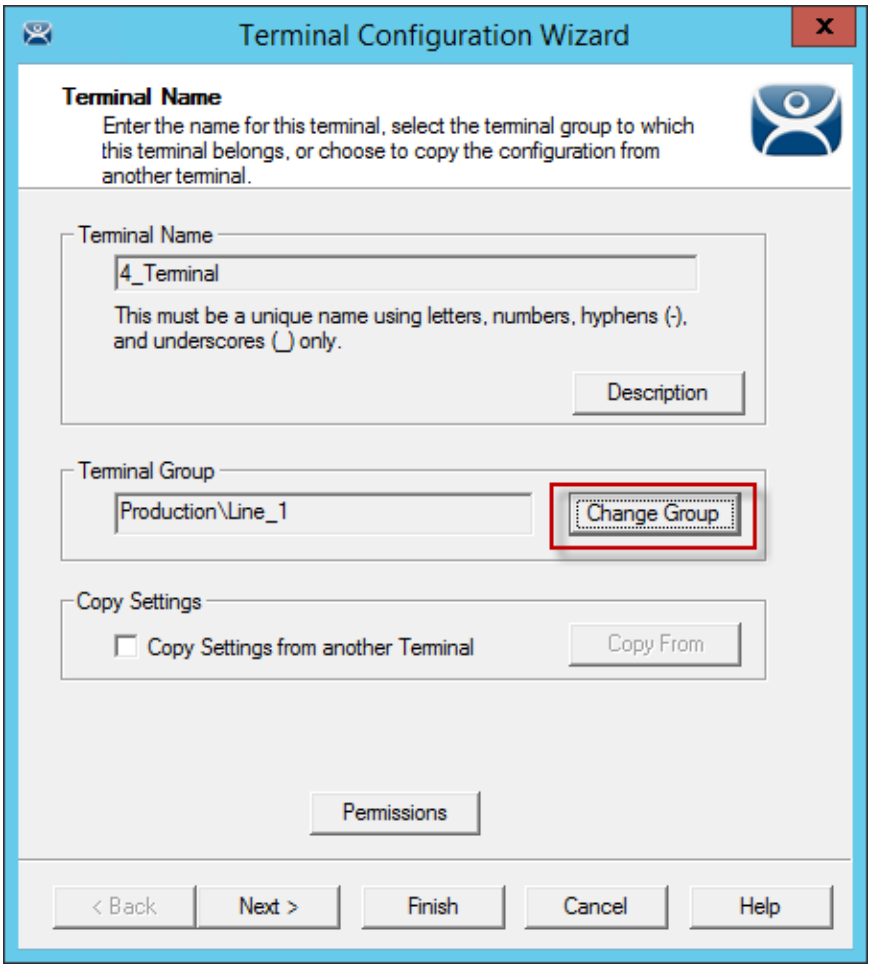
The **Terminal Configuration Wizard** will show the group in the Terminal Group field.

The **Terminals** tree will show the Terminal nested in the group.

19.4.1. Moving Out of a Group

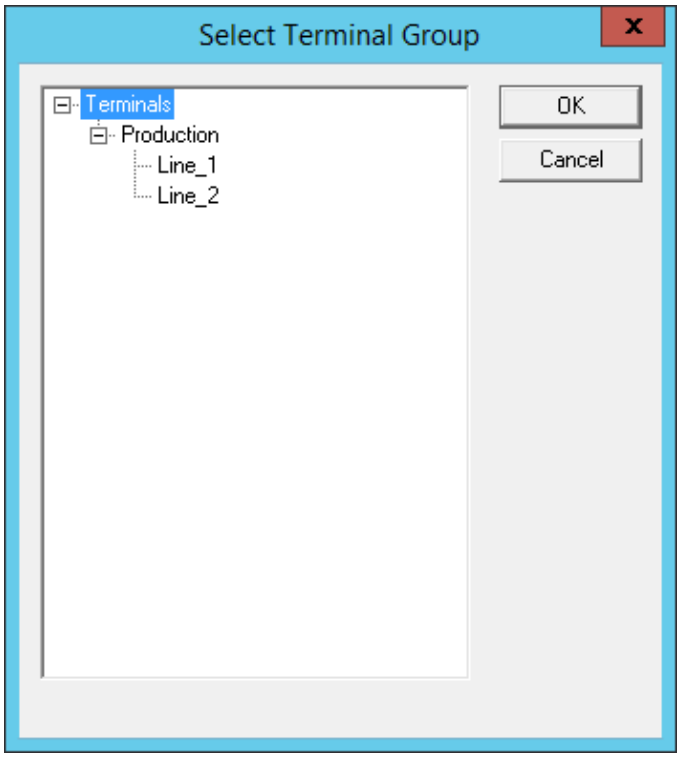
A Terminal can be removed from a group by moving it to the Terminals branch of the **Select Terminal Group** window.

Double click on the Terminal you want to change by double clicking on it in the **Terminals** tree to launch the **Terminal Configuration Wizard**.



Change Group Button on the Terminal Name Page

A Terminal can be removed from a group by clicking the ***Change Group*** button to launch the **Select Terminal Group** window.

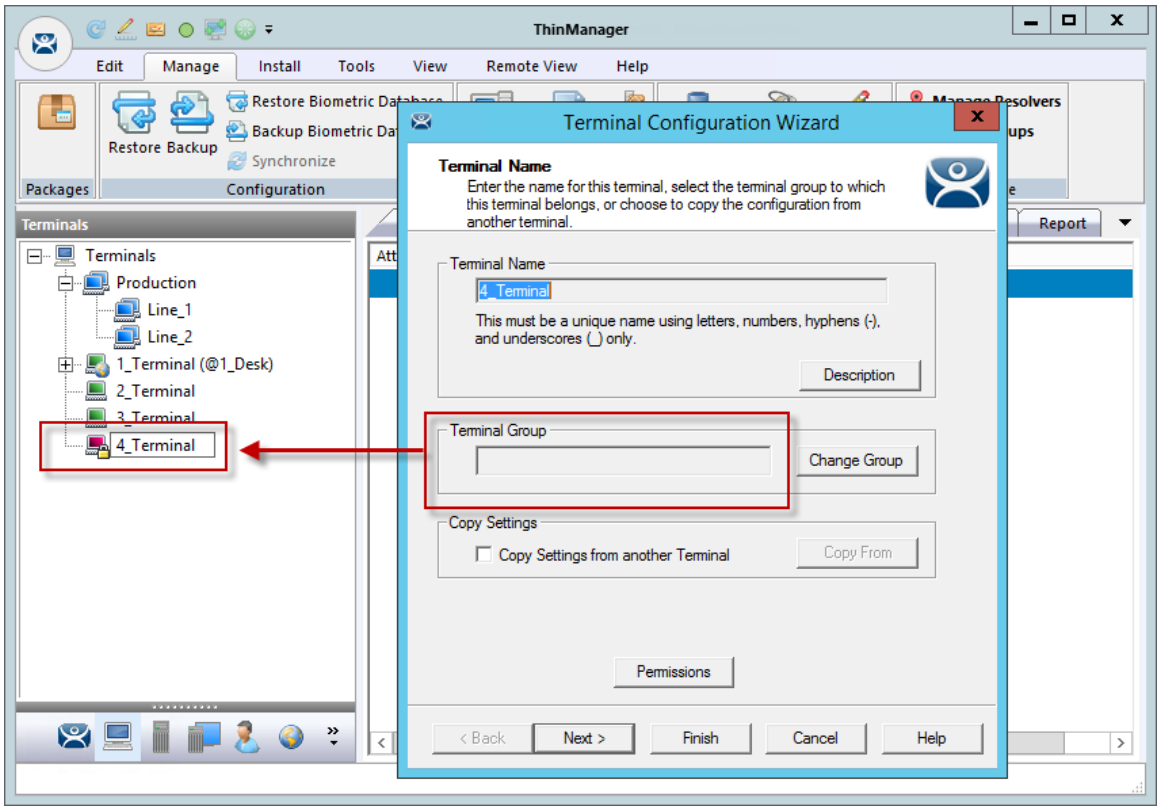


Select Terminal Group Window

Select the top level ***Terminals*** in the Terminal Group tree. This will move the Terminal from a group to the Terminals.

Select the ***OK*** button to finish.

Select the ***Finish*** button to close the **Terminal Configuration Wizar**d and apply the changes before continuing. If you need to adjust the configuration, close the wizard then re-open it.



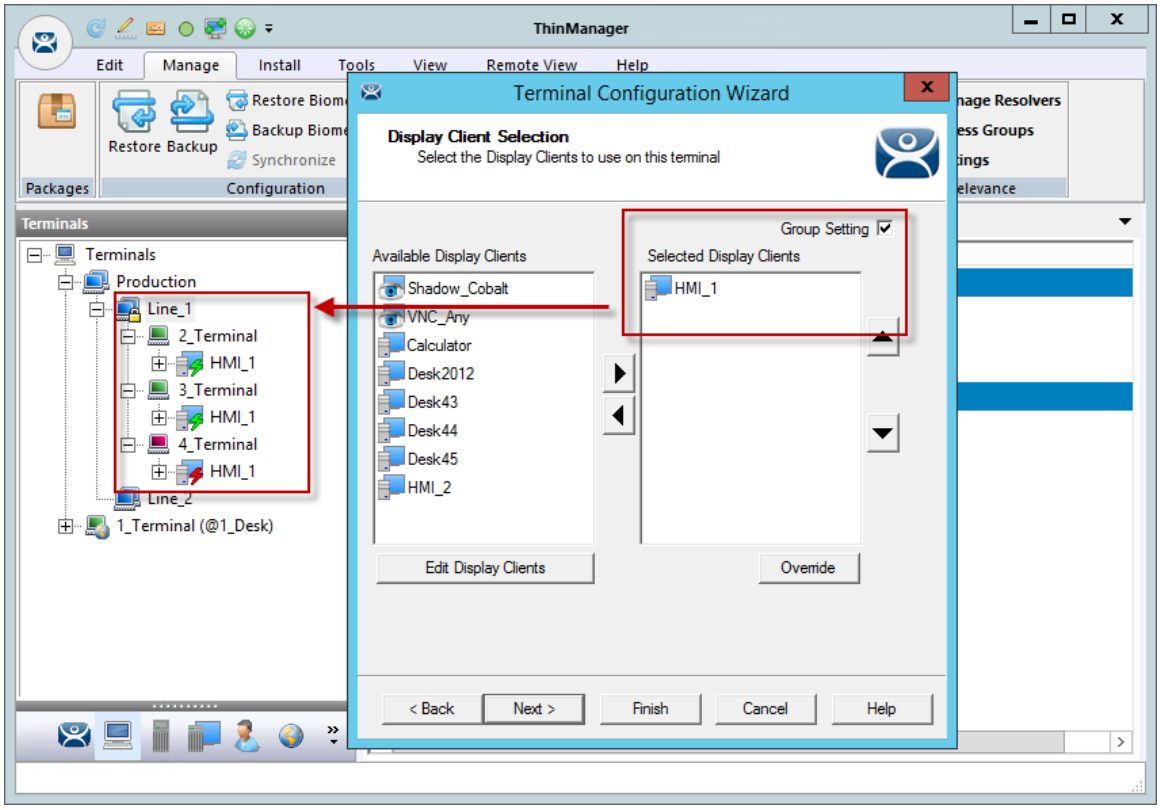
Terminals Tree Showing Ungrouped Terminal

Once the wizard is closed the ThinManager Terminals tree will show the Terminal under the **Terminals** branch and the ***Terminal Group*** field of the **Terminal Name** page will be empty.

19.5. Using Groups for Configuration

ThinManager Terminal Groups can be used for configuration. Every setting in the **Group Configuration Wizard** has a ***Group Setting*** checkbox. If this is checked the setting will be applied to every member of the group.

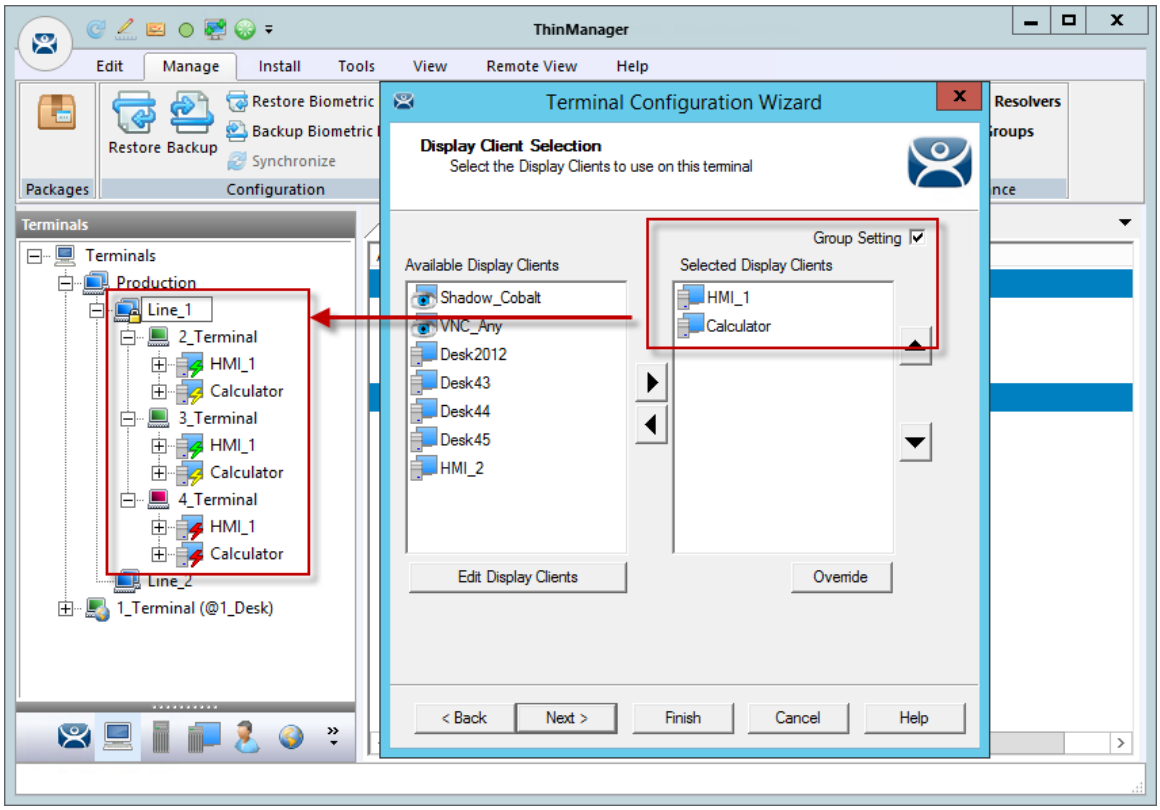
This speeds configuration as you only have to make a configuration change once to have it deployed to all the Terminals in the group.



Display Client Deployed With Group Settings

This picture shows the Line_1 group has three Terminals with a single display clients assigned.

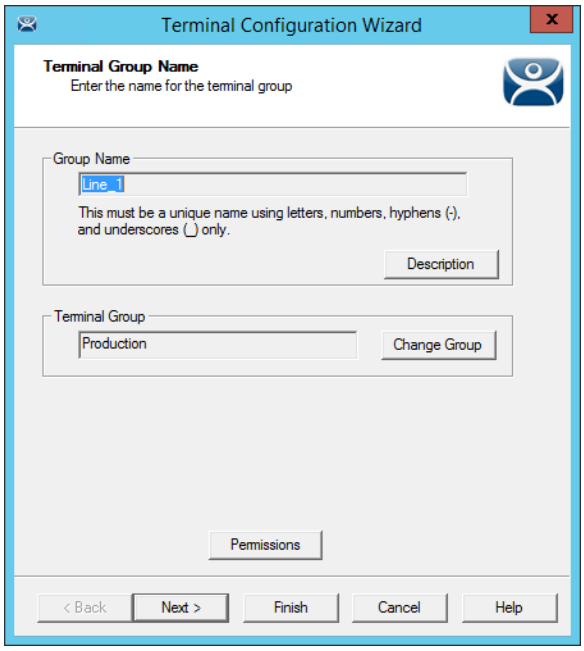
Adding display clients is easy when using ***Group Settings***. You open the **Group Configuration Wizard**, navigate to the **Display Client Selection** page, change the selected display clients, and then restart the Terminals.



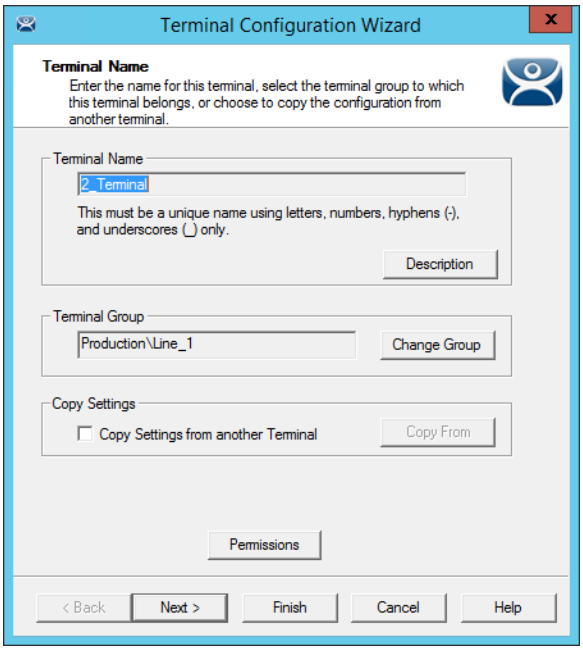
Display Clients Deployed With Group Settings

This picture shows that the Line_1 group had its group display clients changed once and the change was propagated to all of the member Terminals.

The following section will show the **Group Configuration Wizard** on the left and the **Terminal Configuration Wizard** of a member Terminal on the right to show the effects of using the ***Group Setting*** checkbox.



Terminal Group Name

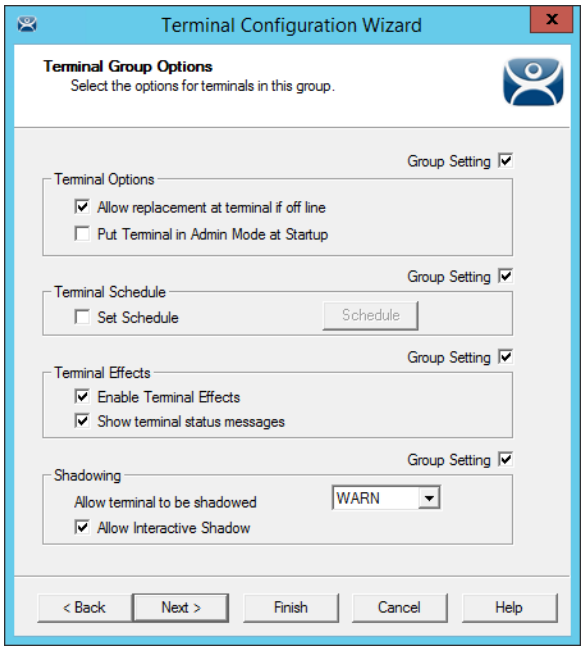


Terminal Name

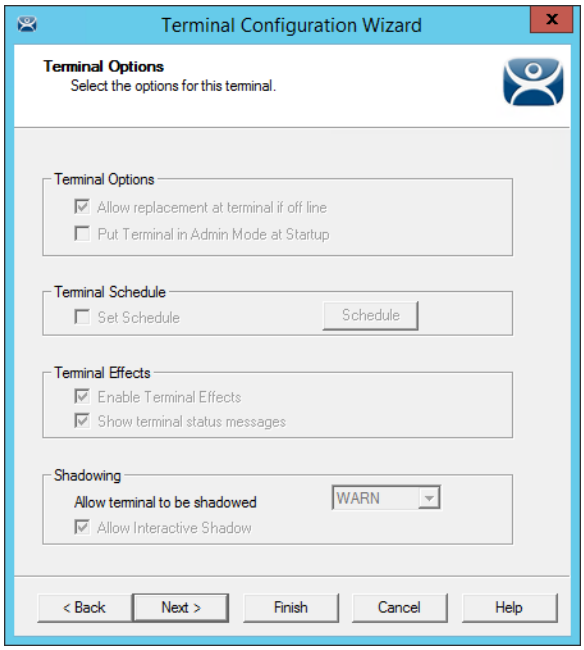
The left shows the opening screen of the **Group Configuration Wizard**.

The right shows the **Terminal Configuration Wizard** of a group member.

The Group will not show the **Terminal Hardware** page since that is an individual selection, not a group selection. The Terminal will show the Terminal Hardware page to allow you to select the hardware for the individual device.



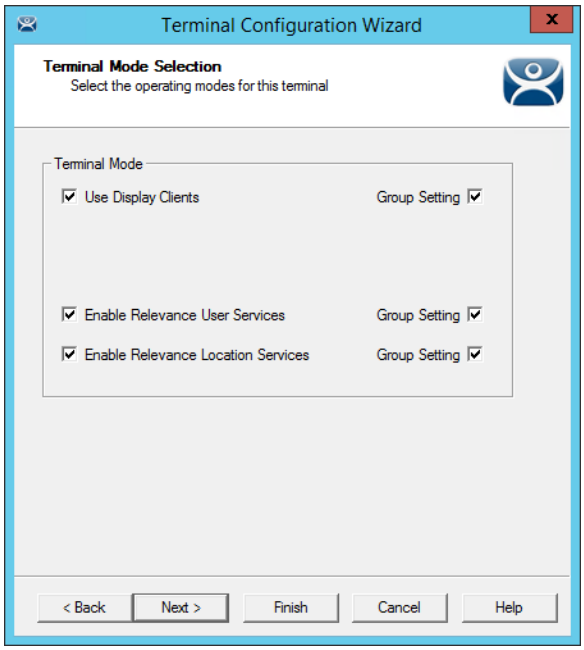
Terminal Group Options



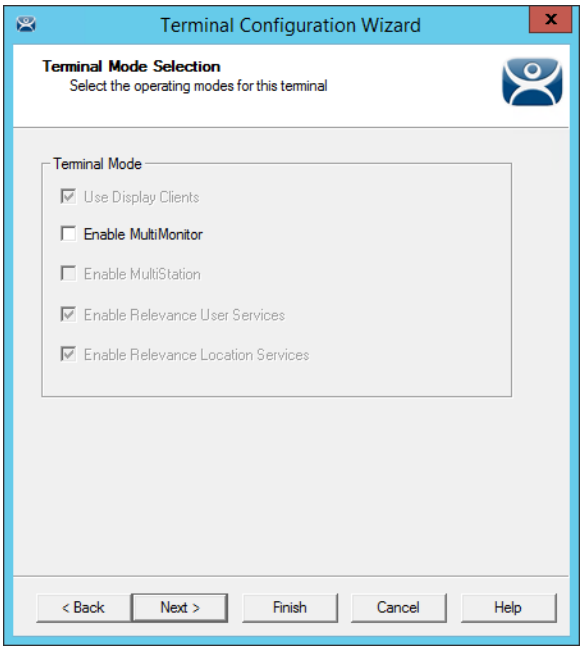
Terminal Options

The **Group Configuration** on the left has had the ***Group Settings*** selected.

The Terminal on the right has the settings grayed out because it is inheriting the ***Group Settings***.

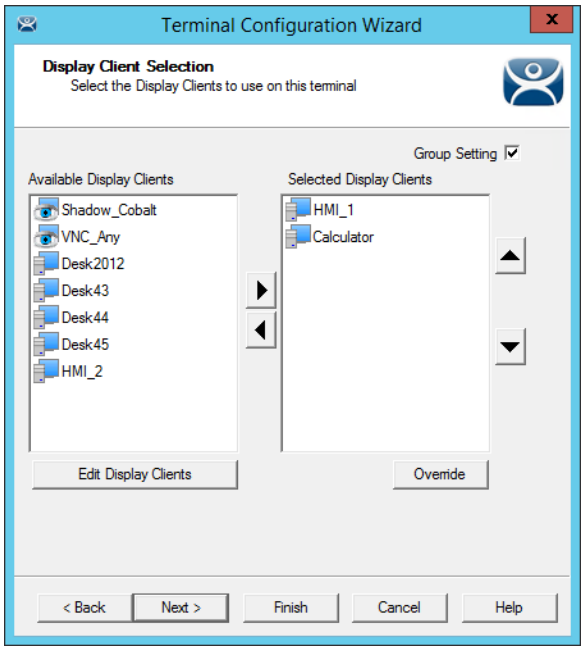


Group Terminal Mode Selection

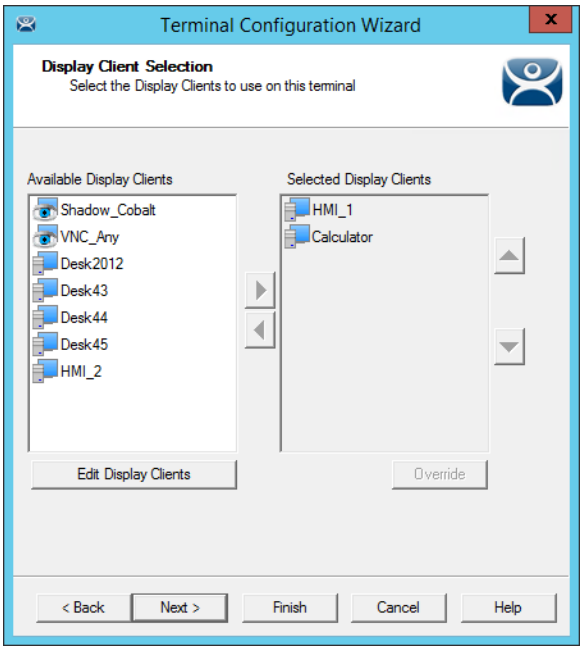


Terminal Mode Selection

Use MultiMonitor is shown on the **Terminal Configuration Wizard** on the right because that is based on the hardware selected and not the group membership.



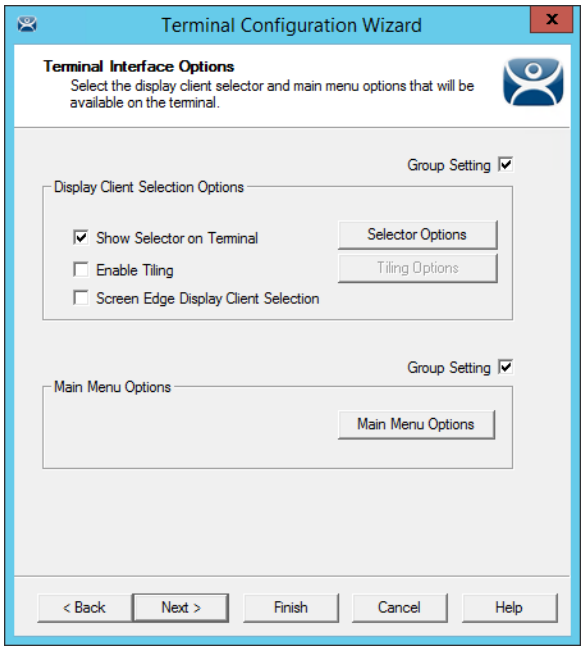
Group Display Client Selection



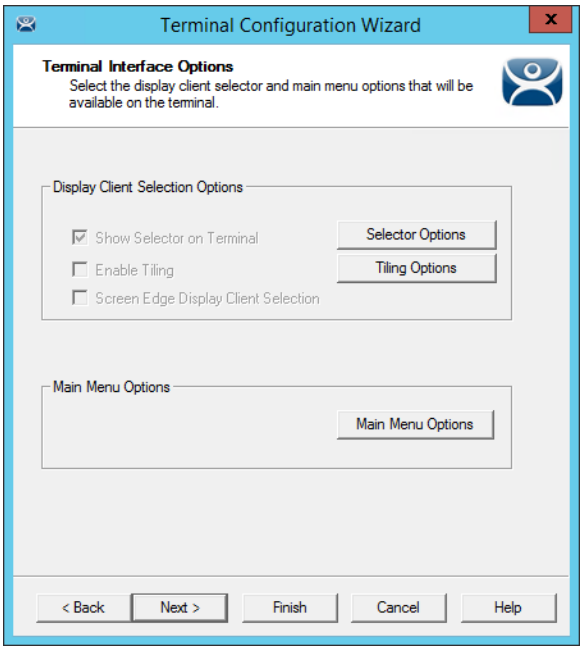
Terminal Display Client Selection

Selecting display clients on the **Group Configuration Wizard** and checking the ***Group Setting*** checkbox will assign those display clients to all member Terminals. You cannot add or subtract from the list on the Terminal.

This is great when all members of a group run the same applications. If they need different applications then leave the ***Group Setting*** unchecked and assign the display clients individually.



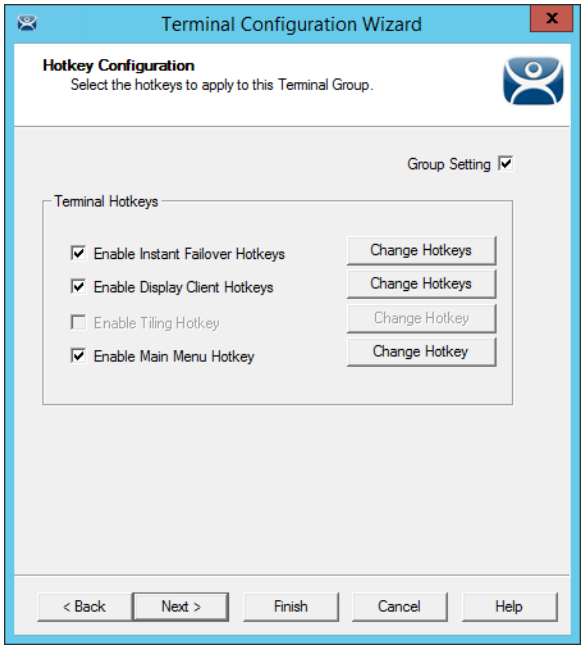
Group Terminal Interface Options



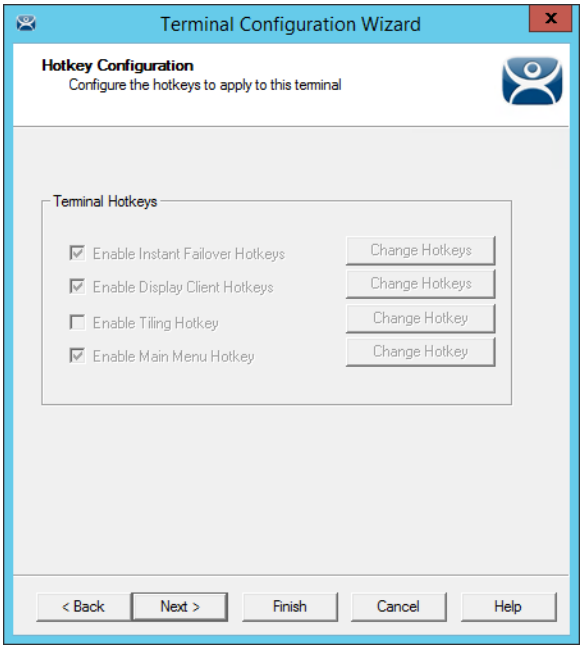
Terminal Interface Options

The **Group Configuration** on the left has had the ***Group Settings*** selected.

The Terminal on the right has the settings grayed out because it is inheriting the ***Group Settings***.



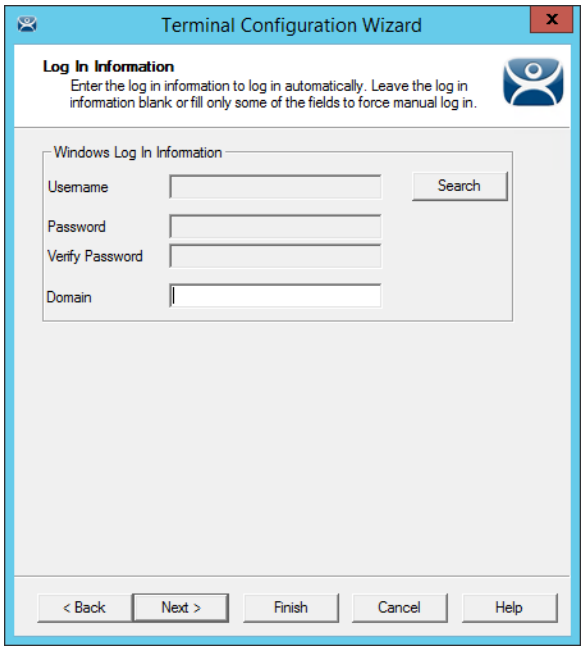
Group Hotkey Configuration



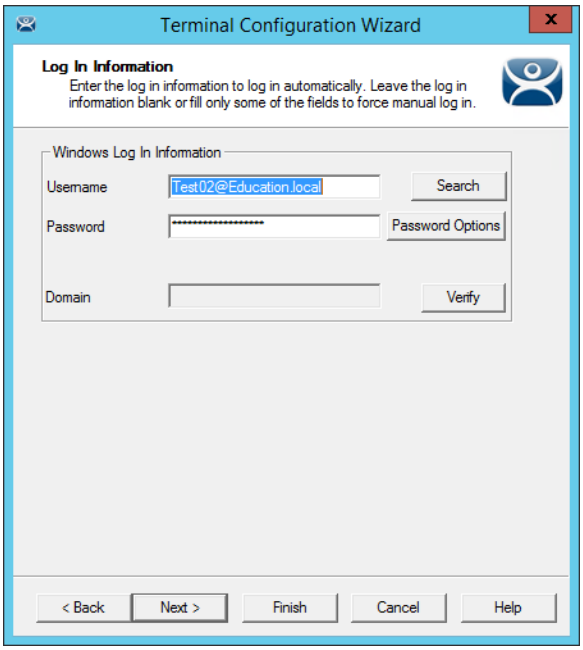
Terminal Hotkey Configuration

The **Group Configuration** on the left has had the ***Group Settings*** selected.

The Terminal on the right has the settings grayed out because it is inheriting the ***Group Settings***.



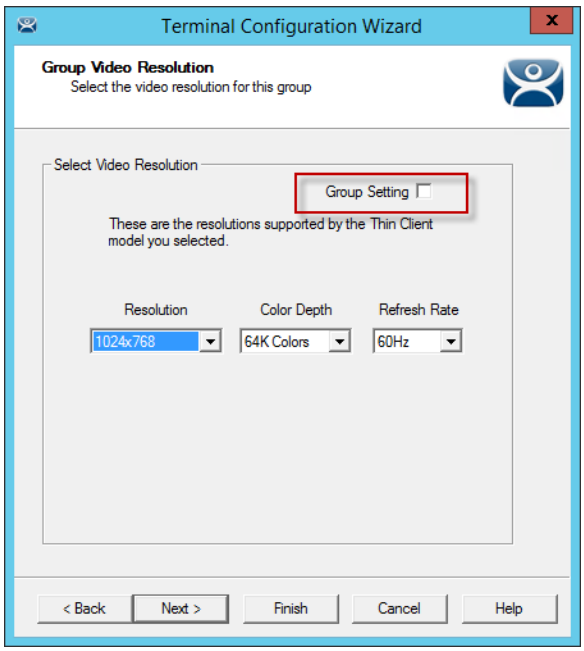
Group Log In Information



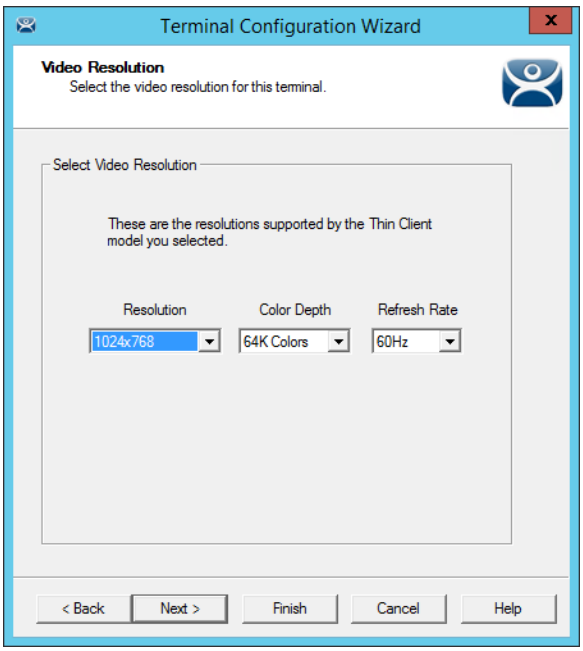
Terminal Log In Information

The **Group Log In Information** page is grayed out and doesn't allow a group user account to be added. This is because each Terminal needs a unique Windows account to log in to Remote Desktop Servers.

✓ **Use a unique Windows account for each Terminal.**



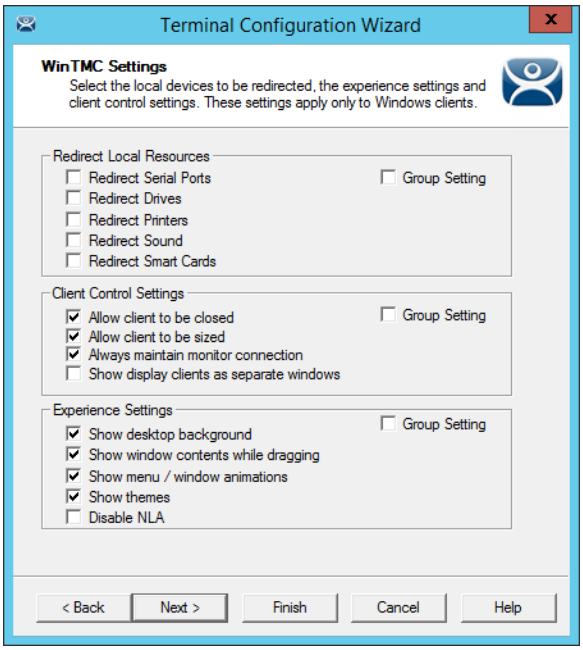
Group Video Resolution



Terminal Video Resolution

The video resolution can be applied to all members of a group. However, if you have to add a different sized monitor in an emergency you would have to uncheck the ***Group Settings*** and apply the resolutions individually.

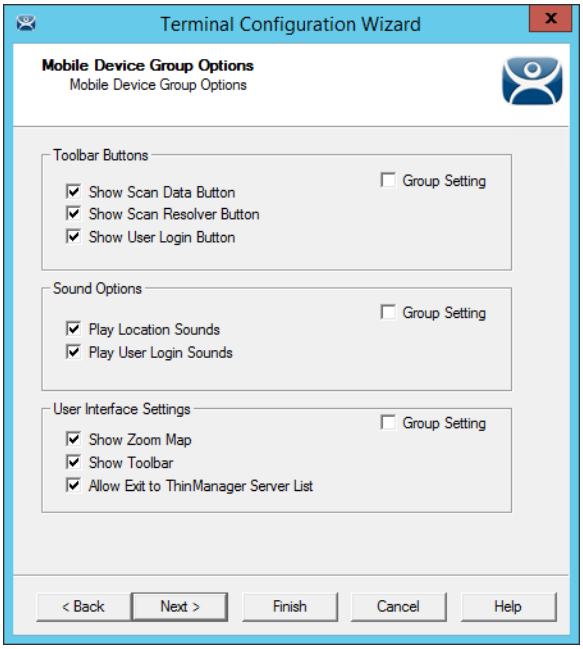
Since switching monitors is a task that almost anyone might be able to do it might be better to set the video resolutions individually.



WinTMC Settings

The **Group Configuration Wizard** will have a **WinTMC Settings** page to allow WinTMC clients to be configured with ***Group Settings***.

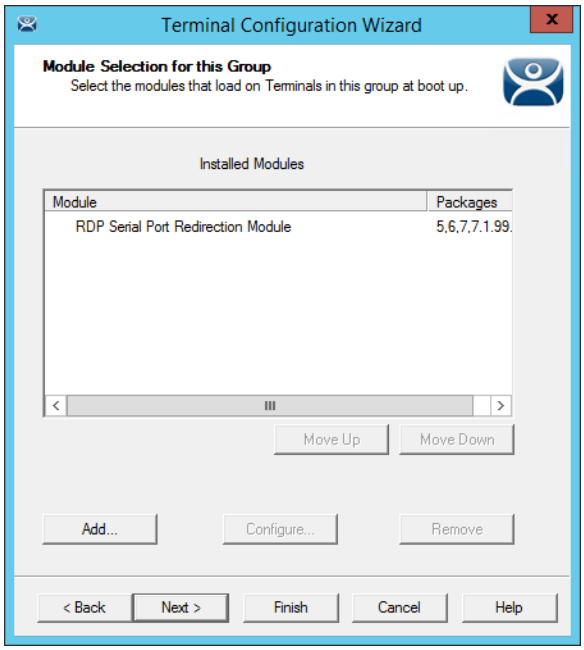
This page will not show up on the **Terminal Configuration Wizard** unless the Terminal had ***GENERIC/WinTMC*** selected as the ***Make*** and ***Model*** on the **Terminal Hardware** page.



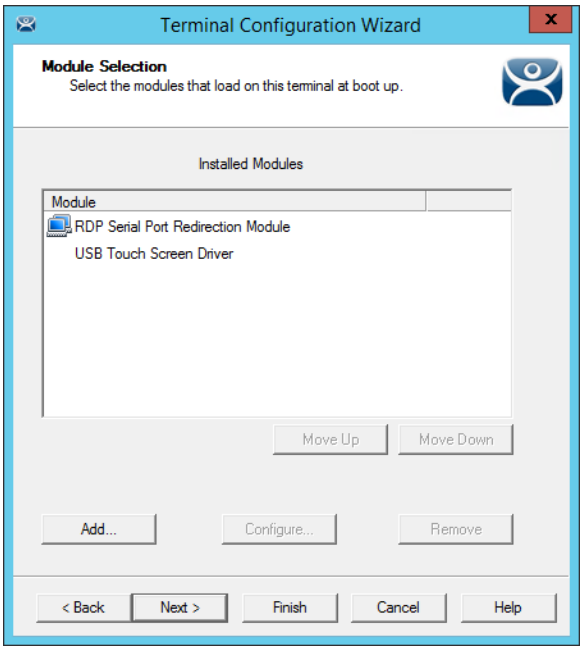
Mobile Device Group Options

The **Group Configuration Wizard** will have a **Mobile Device Group Options** page to allow mobile clients to be configured with ***Group Settings***.

This page will not show up on the **Terminal Configuration Wizard** unless the Terminal has ***GENERIC/Android Device*** *or* ***Apple/iOS*** selected as the ***Make*** and ***Model*** on the **Terminal Hardware** page.



Group Module Selection

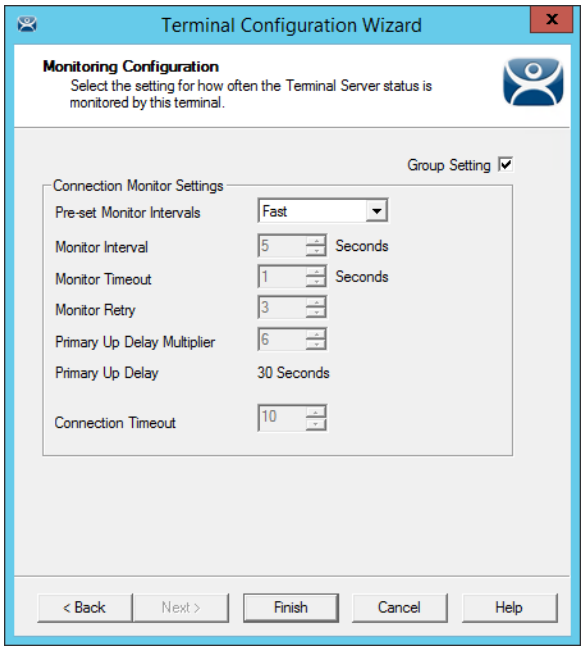


Terminal Module Selection

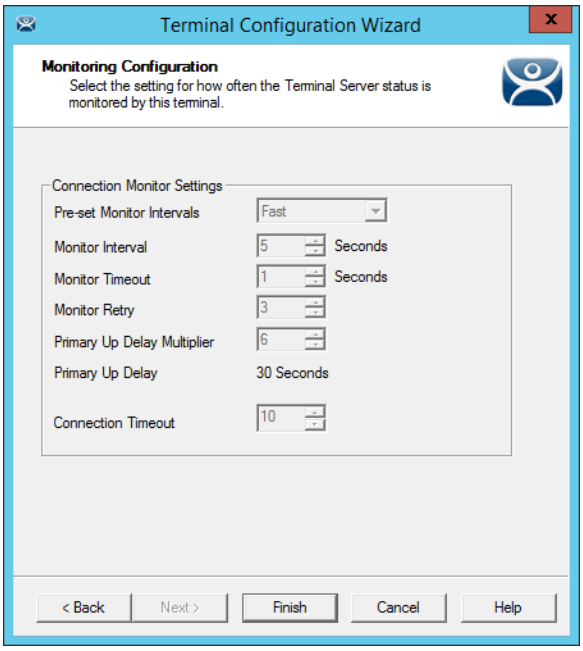
Modules can be added at the group level and at the Terminal level. Modules selected for a group will display a Group icon on the **Module Selection** page of its members.

The picture on the left shows a module added to the group configuration.

The picture on the right shows that module on the Terminal with the Group icon to show where is originated from. The USB touch screen module was added to the Terminal and won't show a group icon.



Terminal Group Name



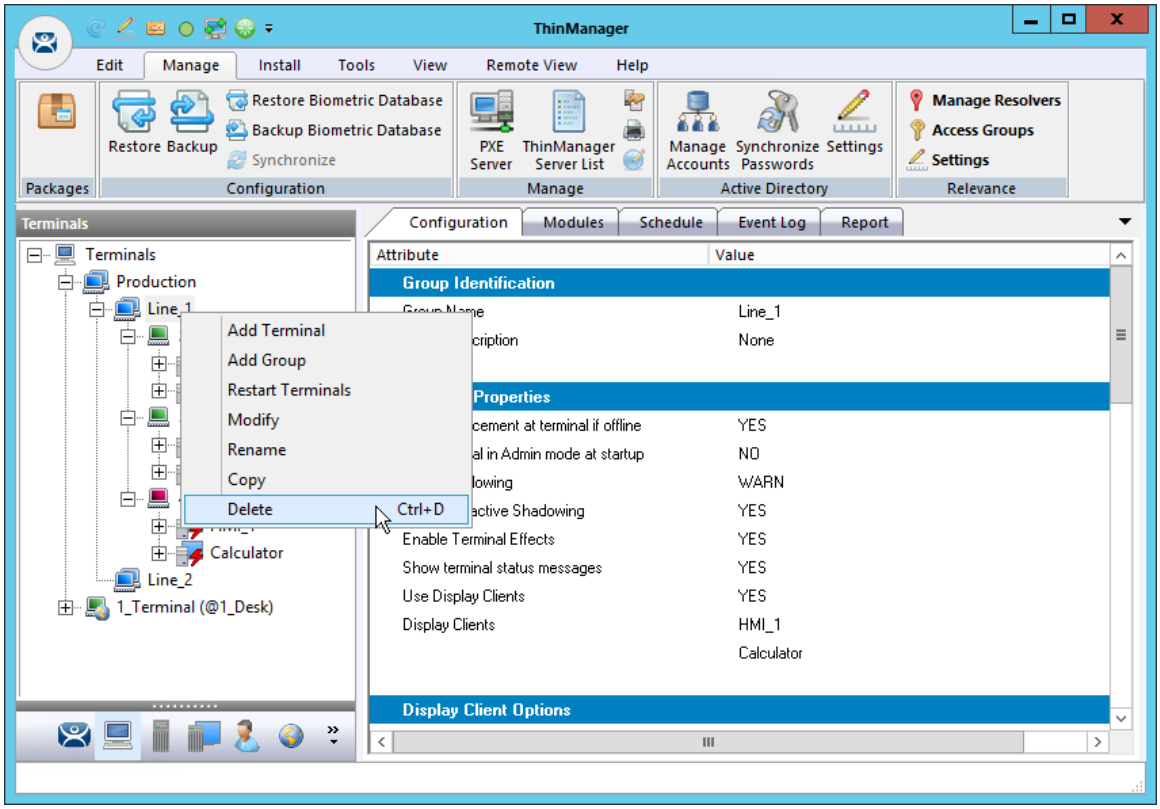
Terminal Name

The **Group Configuration** on the left has had the ***Group Settings*** selected.

The Terminal on the right has the settings grayed out because it is inheriting the ***Group Settings***.

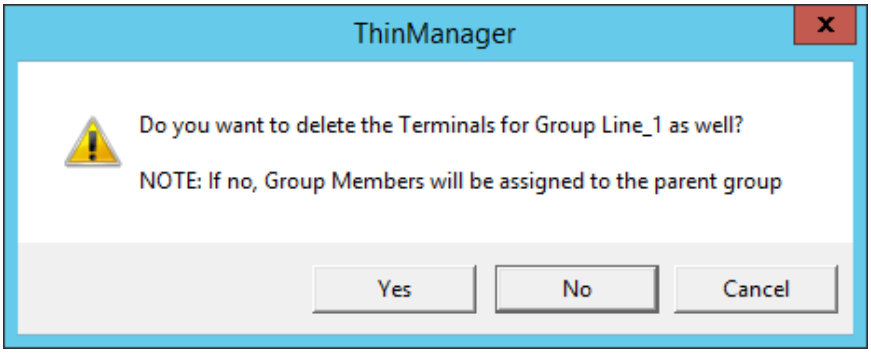
19.5.1. Deleting Old Groups

An unneeded group can be deleted by right clicking on the group and selecting ***Delete***.



Delete Option on Group Right Click Menu

Selecting ***Delete*** will launch a dialog box for deletion.



Delete Dialog Box

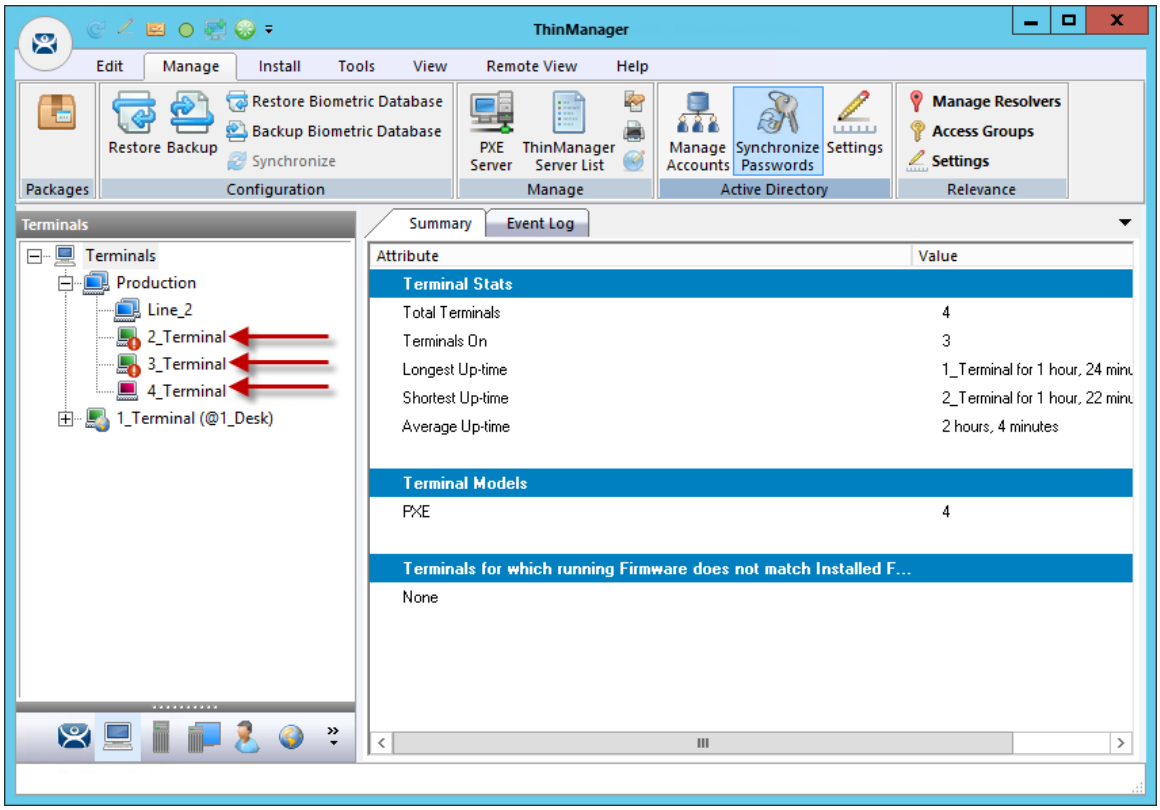
The **Delete dialog** has two options.

Selecting ***Yes*** will delete the group **AND** the member Terminals.

Selecting ***No*** will delete the group but leave the Terminals under the Terminals tree.

Selecting ***Cancel*** will close the dialog without deletion.

- ✓ **Read the dialog box before clicking to prevent the loss of needed Terminals.**



Terminal Tree Showing Terminals without the Group

The Terminals from Line_1 are now nested under the **Production** group in the tree.

Note: The two active Terminals from the **Line_1** group are showing the **Alert** icon indicating that they need to be restarted to load the changed configurations.

---

20. Devices – IP Configuration

There are five types of Terminals that can be used in a ThinManager system. They are:

- ThinManager Ready thin clients
- ThinManager Compatible thin client
- WinTMC client for Windows PCs
- iTMC client for iOS iPads and iPhones
- aTMC client for Android mobile devices

Each has a different method of connecting to ThinManager to receive its configuration.

A **ThinManager Ready thin client** is shipped from the factory with the ThinManager BIOS onboard. A ThinManager Ready thin client requires two things to connect to the ThinManager system:

- An IP Address for the client
- The ThinManager Server Address to retrieve the needed boot file and configuration

A ThinManager Ready thin client can use DHCP or static for the client and ThinManager Server IP address. Its BIOS will instruct it to download the firmware.

A **ThinManager Compatible thin client** is a common off-the-shelf thin client that lacks the ThinManager BIOS. ThinManager Compatible thin clients do not store static IP addresses so each of them require DHCP (Dynamic Host Configuration Protocol) to assign the client IP address. The ThinManager Server IP address and bootfile name can be provided by a DHCP server, or by the ThinManager PXE Server.

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

- PXE Boot enabled in ThinManager
- An IP Address for the client
- The ThinManager Server Address to retrieve the needed boot file

The **WinTMC client** is a ThinManager client that runs on a Windows operating system and provides a centrally managed connection to the Remote Desktop Server.

Each client PC requires two things to connect to the ThinManager system:

- The installation of the WinTMC program
- The IP address of the ThinManager Server

The i**TMC client** is a ThinManager client that runs on an Apple iOS operating system and provides a centrally managed connection to the Remote Desktop Server.

Each iPad requires three things to connect to the ThinManager system:

- The installation of the iTMC program from the Apple App Store
- Membership on the ThinManager Server network
- The IP address of the ThinManager Server

The **AndroidTMC client** is a ThinManager client that runs on the Android operating system and provides a centrally managed connection to the Remote Desktop Server.

Each Android device requires three things to connect to the ThinManager system:

- The installation of the aTMC program from the Google Play Store
- Membership on the ThinManager Server network

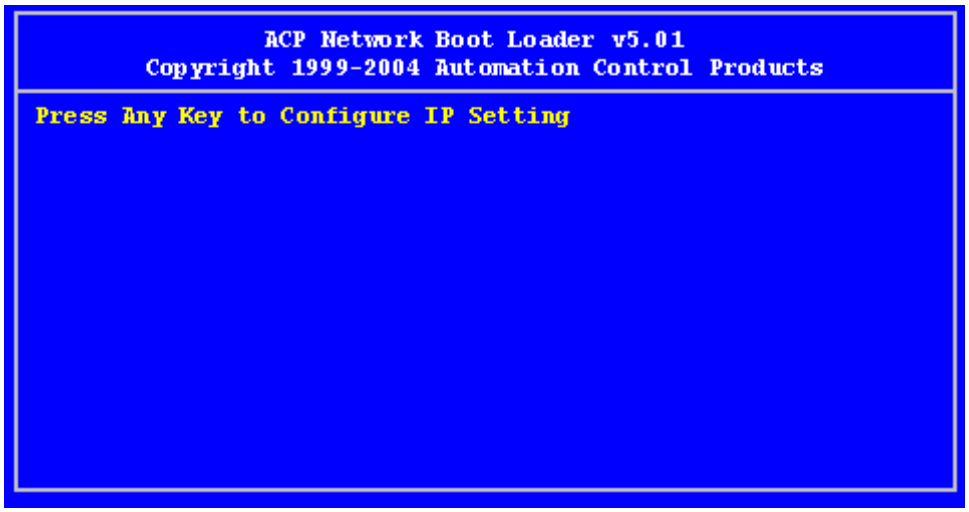
- The IP address of the ThinManager Server

20.1. ThinManager Ready Thin Client IP Configuration

20.1.1. DHCP

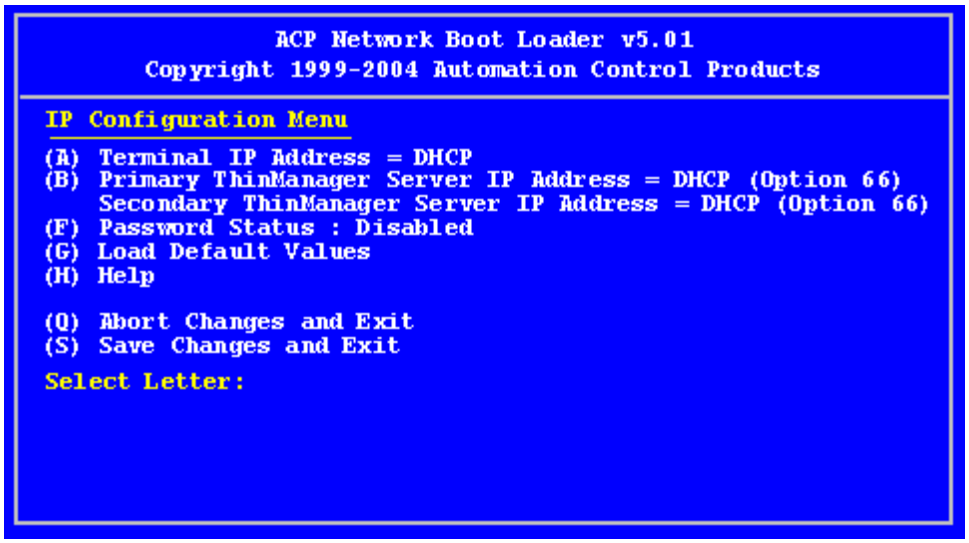
A **ThinManager Ready thin client** is shipped from the factory set to use DHCP (Dynamic Host Configuration Protocol).

When the Terminal is turned on it will display a screen telling you to press any key to enter the IP Configuration menu.



IP Configuration Prompt Page

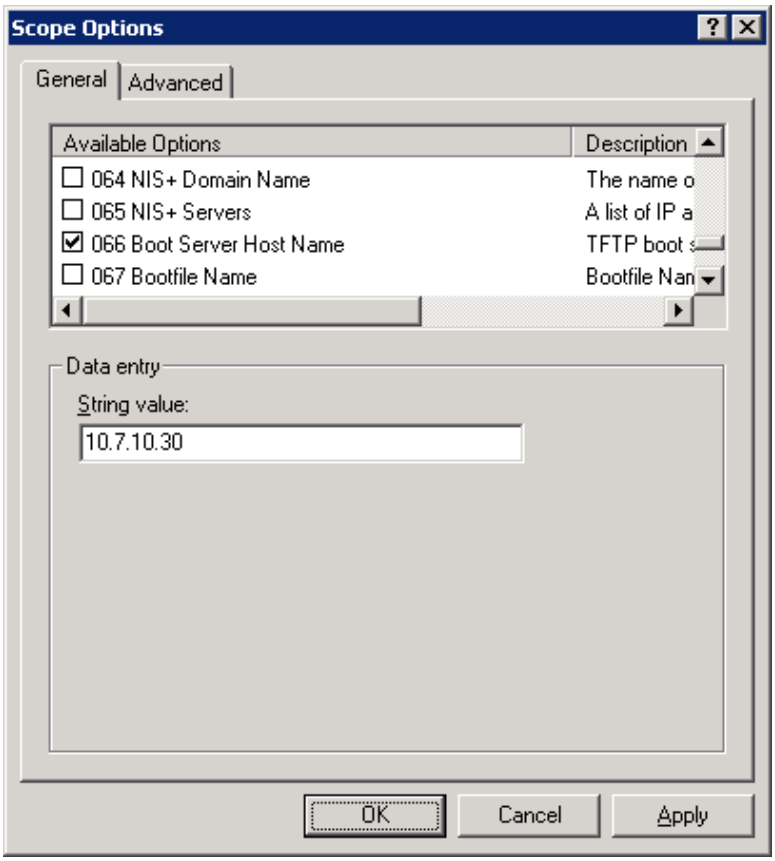
Press the space bar to open the menu.



IP Configuration Menu Page

The ThinManager Ready thin clients uses DHCP out of the box.

DHCP passes out IPaddresses but the thin client also needs the IP address of the ThinManager Server. This can be provided by the DHCP server using ***Option 066, Boot Server Host Name***.



Microsoft DHCP Server

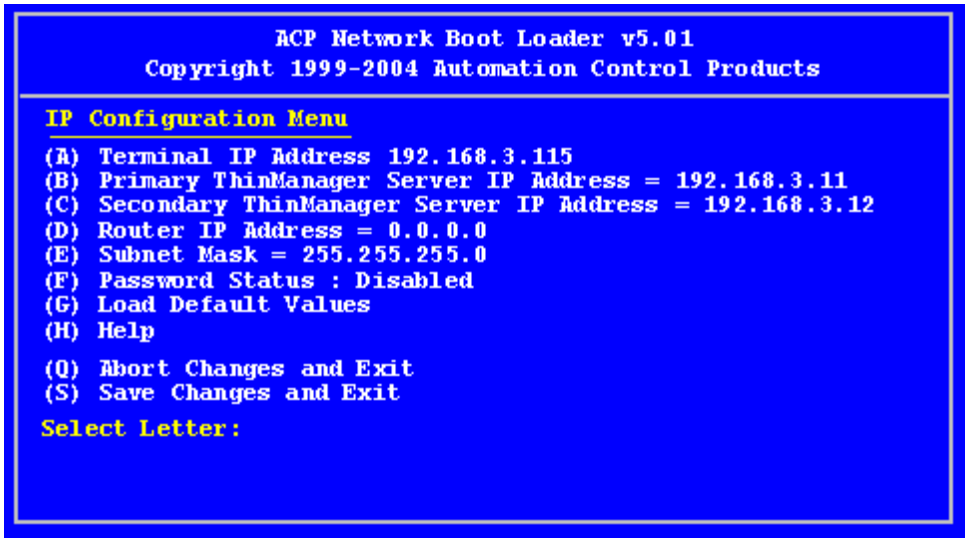
Option 066 provides the ***Boot Server Host Name***. Enter the IP address of the ThinManager Server in the ***Option 066*** field to have the DHCP server send this to the ThinManager Ready thin clients.

PCs and laptops that use DHCP will ignore this setting.

20.1.2. Static IP Addressing

Most models of ThinManager Ready thin clients allow the usage of static IPs. These are set on the **IP Configuration Menu**.

Open the **IP Configuration Menu** by selecting any key at the **IP Configuration Prompt p**age.



IP Configuration Menu – Static IP

Press the ***A*** to allow the client IP to change from DHCP to static by assigning a static IP address to the Terminal.

Type in the static IP address for the client, including the separating periods and press the ***Enter*** key.

Once the Terminal has a static IP assigned, the IP Configuration Menu will be shown to allow the setting of other values.

(A) Terminal IP Address - This should be a unique address for the Terminal.

(B) Primary ThinManager Server IP Address - This should be the unique address for your main ThinManager Server.

(C) Secondary ThinManager Server IP Address - The Secondary ThinManager field allows the Terminal to use two ThinManager Servers. If the Terminal cannot connect to the Primary ThinManager Server, it will connect to the Secondary ThinManager Server to receive its configuration. If you are not using a Secondary ThinManager Server, set the IP address to 0.0.0.0.

(D) Router IP Address - Fill in the IP address of the router or gateway if one is being used. If not this should be set to 0.0.0.0.

(E) Subnet Mask - Set this to your subnet mask. 255.255.255.0 is a standard setting.

(F) Password Status - Allows a password to be set to prevent unauthorized people from changing the configuration.

Note: Forgetting this password is a bad thing.

(G) Load Default Values – This resets the ThinManager Ready thin client to the original IP values.

(H) Help - Will launch a Help to explain the IP Configuration Menu.

(Q) Abort Changes and Exit - This will cancel any setting changes and let the Terminal continue to boot with the old settings.

(S) Save Changes and Exit - This will apply any changes and allow the Terminal to continue to boot with the new settings.

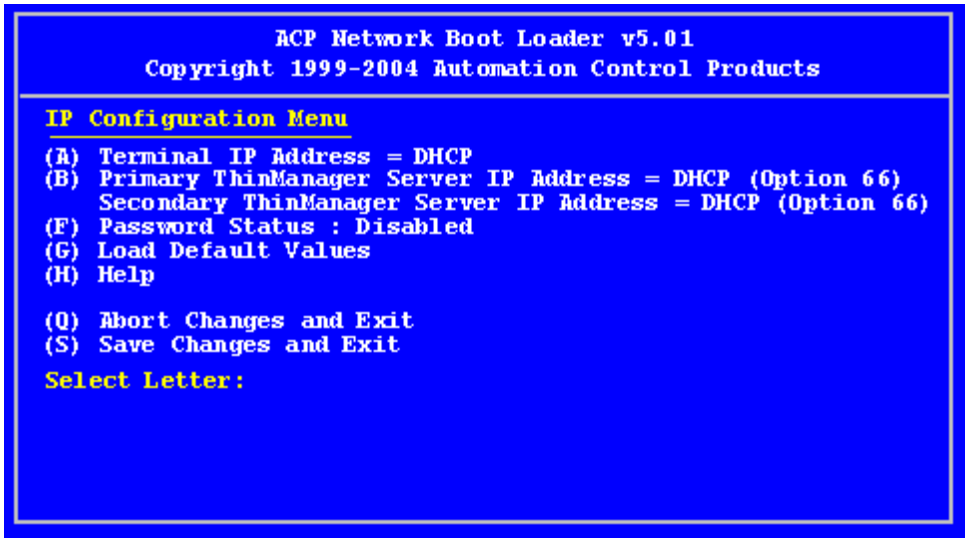
Type the letter of the desired setting and type the IP address, with periods. Press the ***Enter*** key on the keyboard to accept each change.

20.1.3. Hybrid IP Addressing

ThinManager Ready thin clients with Boot Loader 5.01 and later can use DHCP to assign the Terminal IP address, but can assign the ThinManager Server IP address as a static IP in the IP Configuration Menu.

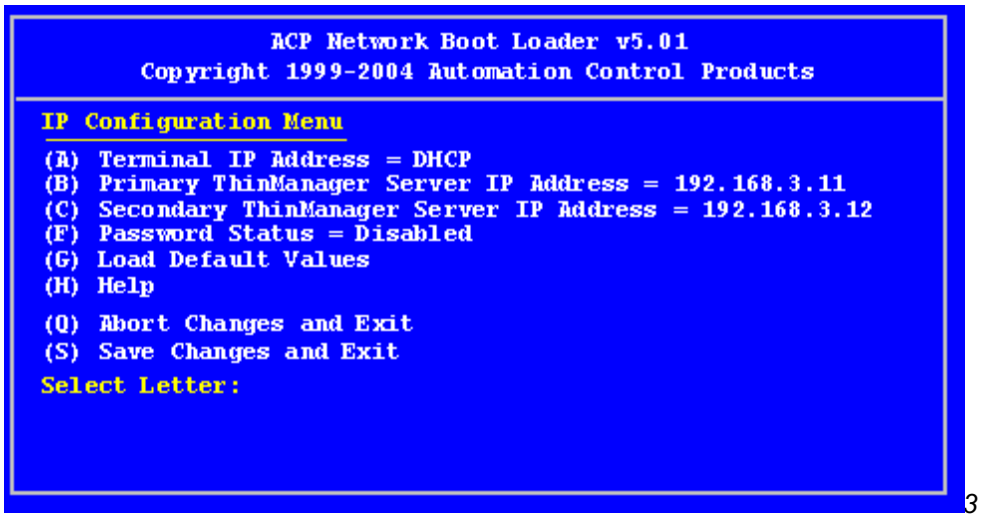
Boot your thin client and press the spacebar when prompted on the IP Configuration Prompt page.

This will open the IP Configuration Menu.



Boot Loader Default Values

Select the **B** key to add a static IP for the ThinManager Server. Type the numbers and periods for the address.



DHCP with Static ThinManager Server

Once a ThinManager Server is assigned, selecting **C** will allow a redundant secondary ThinManager Server to be assigned.

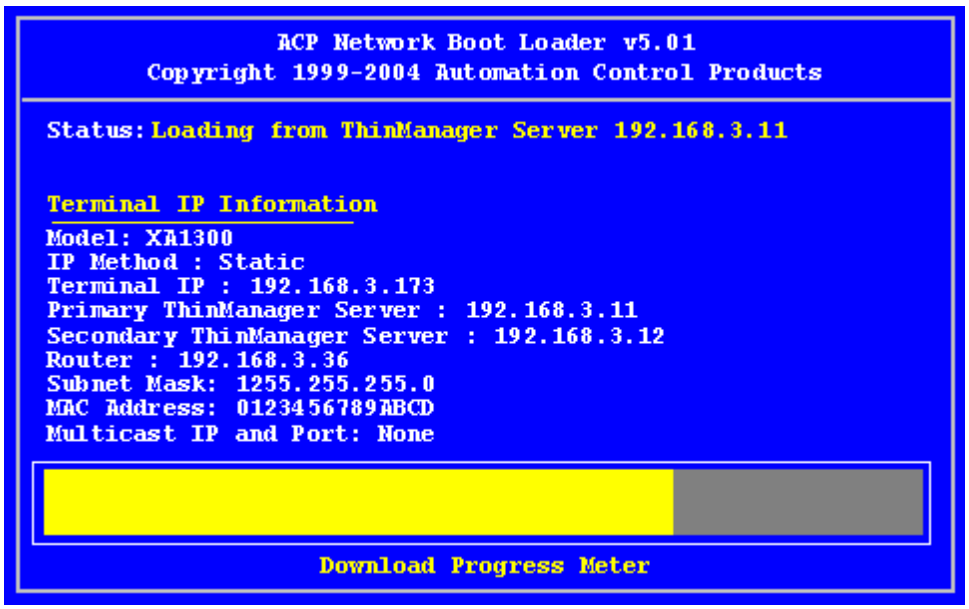
Select **S** to save the changes and allow the connection to the ThinManager Server.

The Terminal will now boot using DHCP.

Note: The ***Escape*** key will let you exit the entry field and return to the **IP Configuration Menu**.

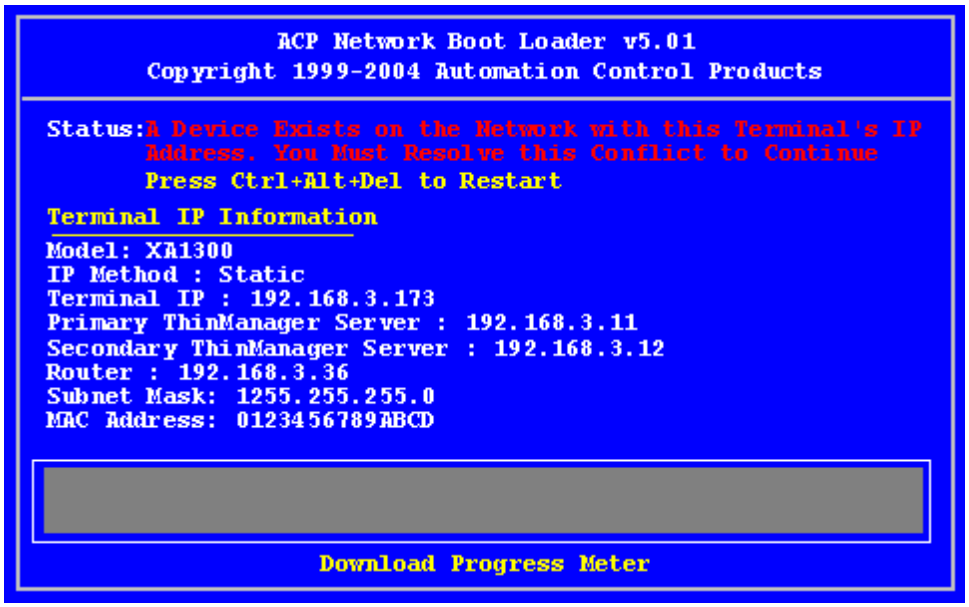
20.1.4. Firmware Download

Once the ThinManager Ready thin client is configured, the Terminal will connect to the ThinManager Server and download the firmware and configuration.



Firmware Download

If the static IP address for the Terminal is a duplicate of another IP address on the network, it will display an error message instead of downloading the firmware.



Duplicate IP Address Error

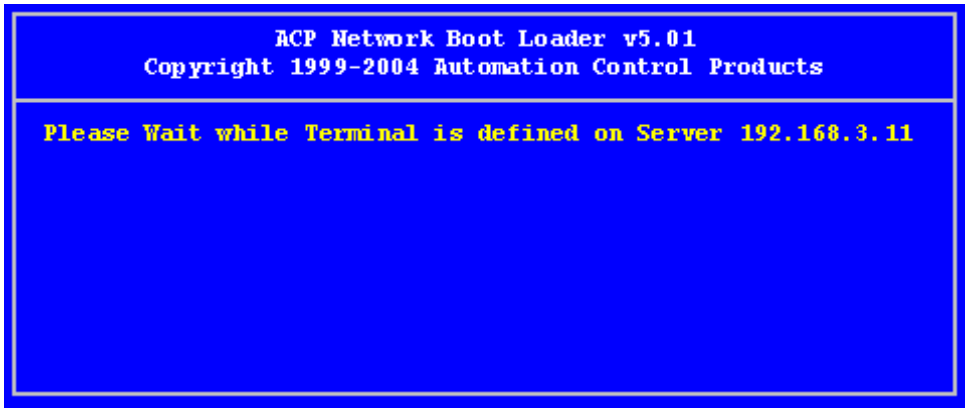
A Terminal with this error message needs to be rebooted and the IP address corrected.

20.2. Adding and Configuring Thin Clients

20.2.1. Connect and Start Wizard

Turning on a Terminal for the first time will initiate the **Create New Terminal** mode if:

- No Terminals are defined in ThinManager, or
- All the defined Terminals are currently connected, or
- All the defined Terminals that are turned off have the ***Allow This Terminal To Be Replaced If Off Line*** check box unselected.

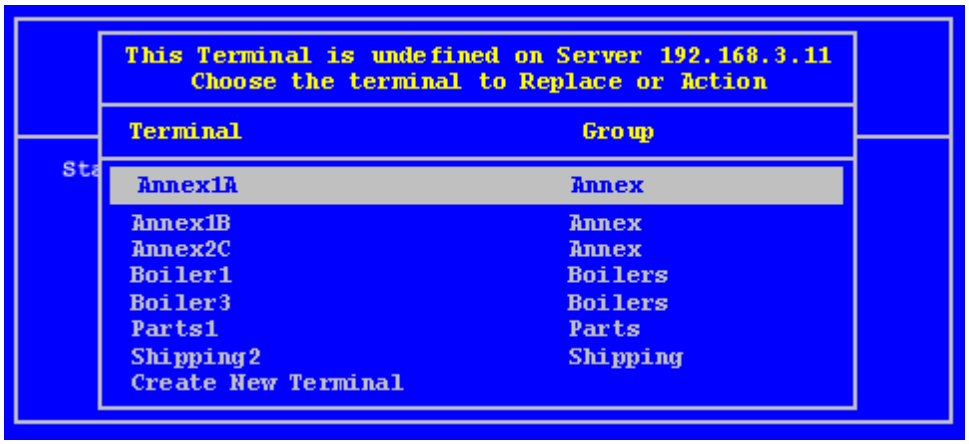


Create New Terminal Mode Screen

When a Terminal enters the **Create New Terminal Mode**, the Terminal will launch the **Terminal Configuration Wizard** on the ThinManager Server. The Terminal will display a screen indicating that it will wait until the configuration is finished before progressing further.

20.2.2. Pre-configure and Select Configuration

Turning on a Terminal for the first time will initiate the ***Replace or Create New Terminal Mode*** if one or more of the defined Terminals are offline and they have the ***Allow This Terminal To Be Replaced If Off Line*** check box selected.



Replace or Create Mode

The screen will display all the offline Terminals that the Terminal can replace. Groups will be displayed, requiring a drill down to the desired Terminal. Highlight the desired Terminal name using the keyboard and press the ***Enter*** button. The Terminal will retrieve the selected configuration and assume its identity.

If a Terminal has previously connected to ThinManager and received its configuration, rebooting it will not give it a choice of configurations, but will apply its normal configuration.

20.3. PXE Server and PXE Boot

A **ThinManager Ready thin client** is shipped from the factory with the ThinManager BIOS onboard. A ThinManager Ready thin client can use DHCP or static for the client IP address and the ThinManager Server IP address. Its BIOS will instruct it to download the firmware.

A **ThinManager Compatible thin client** is a common off-the-shelf thin client that lacks the ThinManager BIOS. ThinManager Compatible thin clients do not store static IP addresses so each of them require DHCP (Dynamic Host Configuration Protocol) to assign the client IP address. The ThinManager Server IP address and bootfile name can be provided by a DHCP server, or by the ThinManager PXE Server.

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

- An IP Address for the device.
- The ThinManager Server Address to retrieve the needed boot file.
- The Boot File name.

20.3.1. PXE Server Modes

There are three modes or methods that a ThinManager Compatible thin client can use to receive this information.

Using standard DHCP server

This mode will allow the client to use an existing DHCP server to provide the client IP address while the ThinManager PXE server will provide the ThinManager IP and boot file name.

Using standard DHCP server on this machine

This mode is required to provide the PXE information when a standard DHCP server is installed on the same computer as the ThinManager Server. Additionally Port UDP-4011 will need to be opened on the computer.

Using standard DHCP server with Boot Options

This mode allows the DHCP server to provide all the information needed. It will use ***Option 066*** to provide the ThinManager IP and will use ***Option 067*** to provide the boot file name in addition to the client IP address.

Not using standard DHCP Server

This gives ThinManager the power to provide all the necessary information, including client IP addresses.

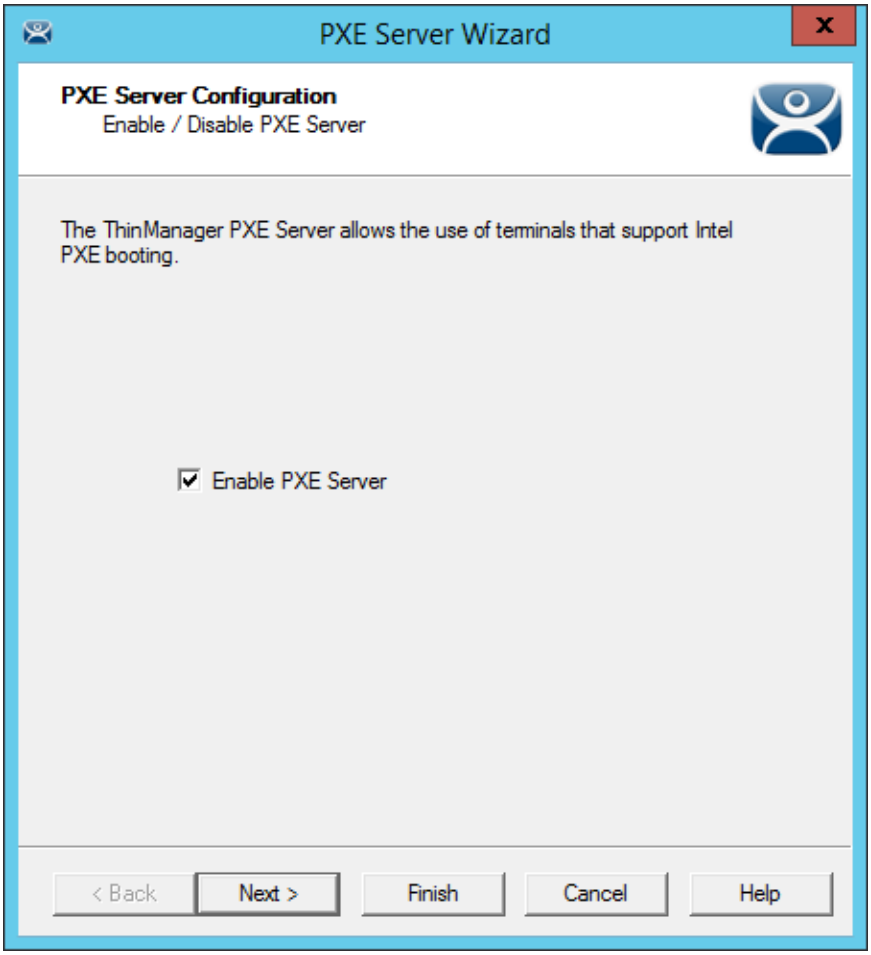
ThinManager Compatible Thin Client IP Sources

	Device IP	ThinManager IP	Boot File Name
Using Standard DHCP	DHCP Server	ThinManager	ThinManager
Using Standard DHCP on machine	DHCP Server	ThinManager	ThinManager
DHCP with Boot Options	DHCP Server	DHCP Option 066	DHCP Option 067
Not Using Standard DHCP	ThinManager	ThinManager	ThinManager

20.3.2. Using Standard DHCP Server

The **Using standard DHCP server** mode is used when you have an existing DHCP server in your system to pass out the IP addresses.

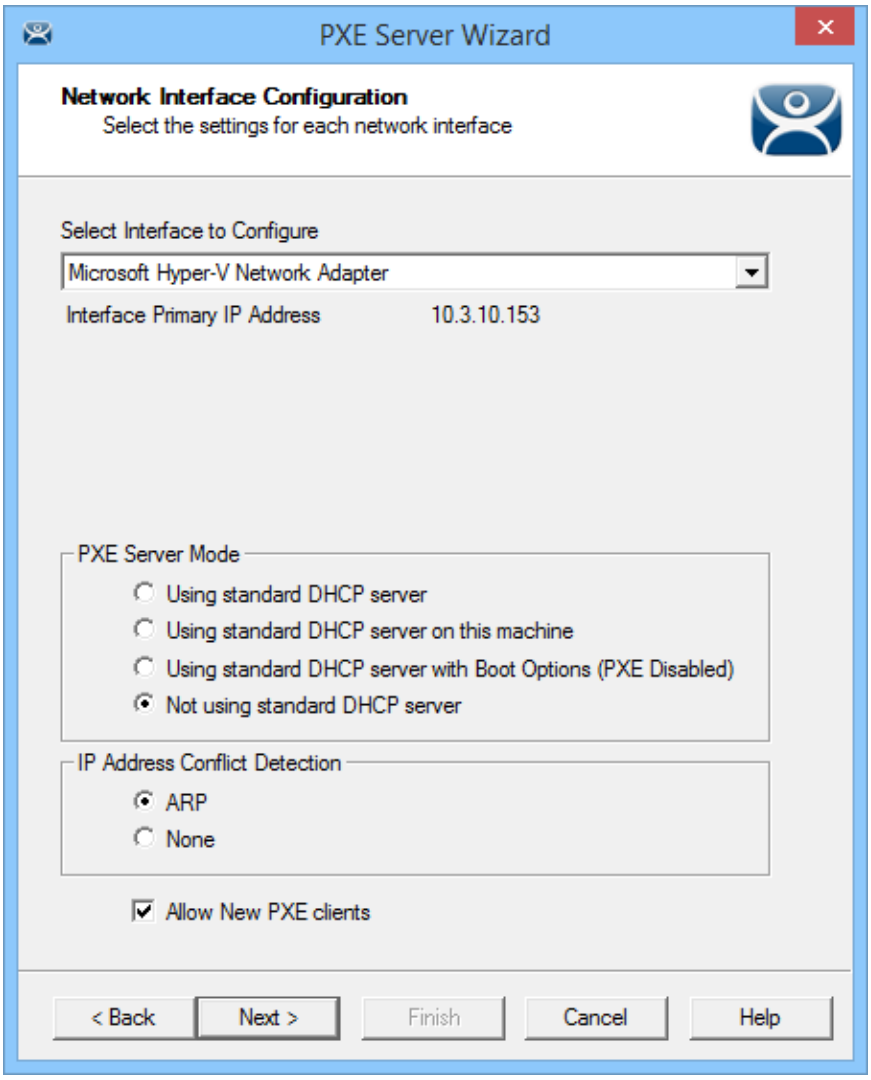
Select ***Manage > PXE Server*** to open the PXE Server Wizard.



PXE Server Configuration Wizard

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

Select ***Next*** to continue with the wizard.



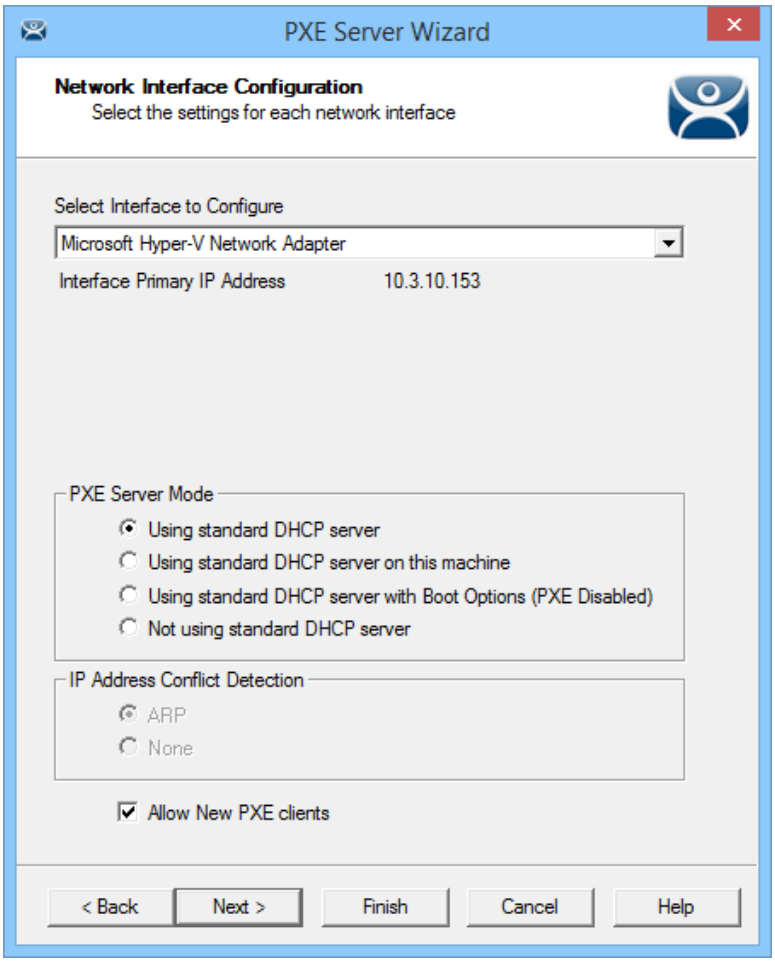
Network Interface Configuration Page of PXE Server Configuration

The **Network Interface Configuration** page allows you to select the network interface if the ThinManager Server has multiple network cards.

The ***PXE Server Mode*** radio buttons allow you to set the PXE mode. This discussion follows.

The ***IP Address Conflict Detection*** will check for conflicts in the Address Resolution Protocol when the ***ARP*** radio button is selected.

The ***Allow New PXE clients*** controls whether ThinManager gives PXE information to new PXE boot ThinManager Compatible thin clients.

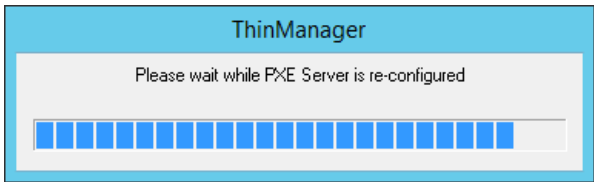


Synchronized Network Interface Configuration Page

A synchronized ThinManager Server will have a drop-down for the network interface on both ThinManager Servers.

The easiest method of PXE boot is if you have an existing DHCP server.

Select the ***Using standard DHCP server*** radio button and click ***Finish***.



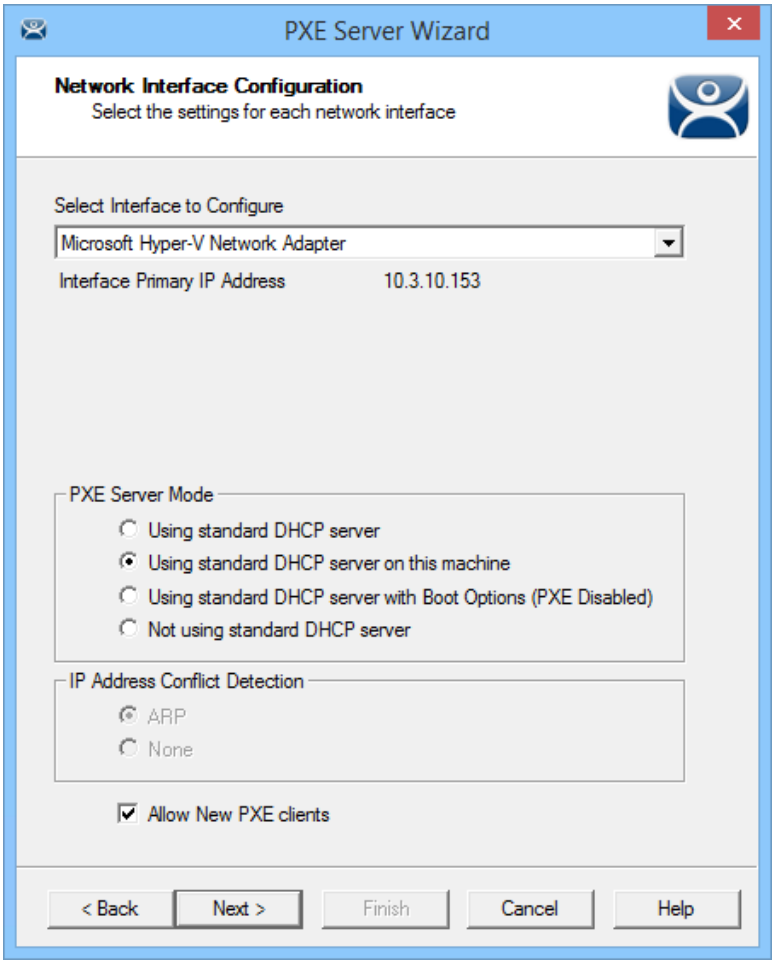
PXE Server Initialization Dialog

The PXE server will initialize and become active.

The ThinManager Compatible thin client will make a request for the DHCP and PXE information when it is turned on. The DHCP server will respond with the client IP address. The ThinManager will respond with the PXE boot information and the thin client will connect to ThinManager.

20.3.3. Using standard DHCP Server on this Machine

The **Using standard DHCP server on this machine** mode is used when you have an existing DHCP server in your system to pass out the IP addresses and it is installed on the ThinManager Server.



Using standard DHCP server on this machine

This mode optimizes the PXE server when the ThinManager Server is installed on the same machine as the DHCP server.

Port UDP-4011 needs to be opened for this setting. The Port UDP-4011 is also required for UEFI boot (Unified Extensible Firmware Interface) PXE clients

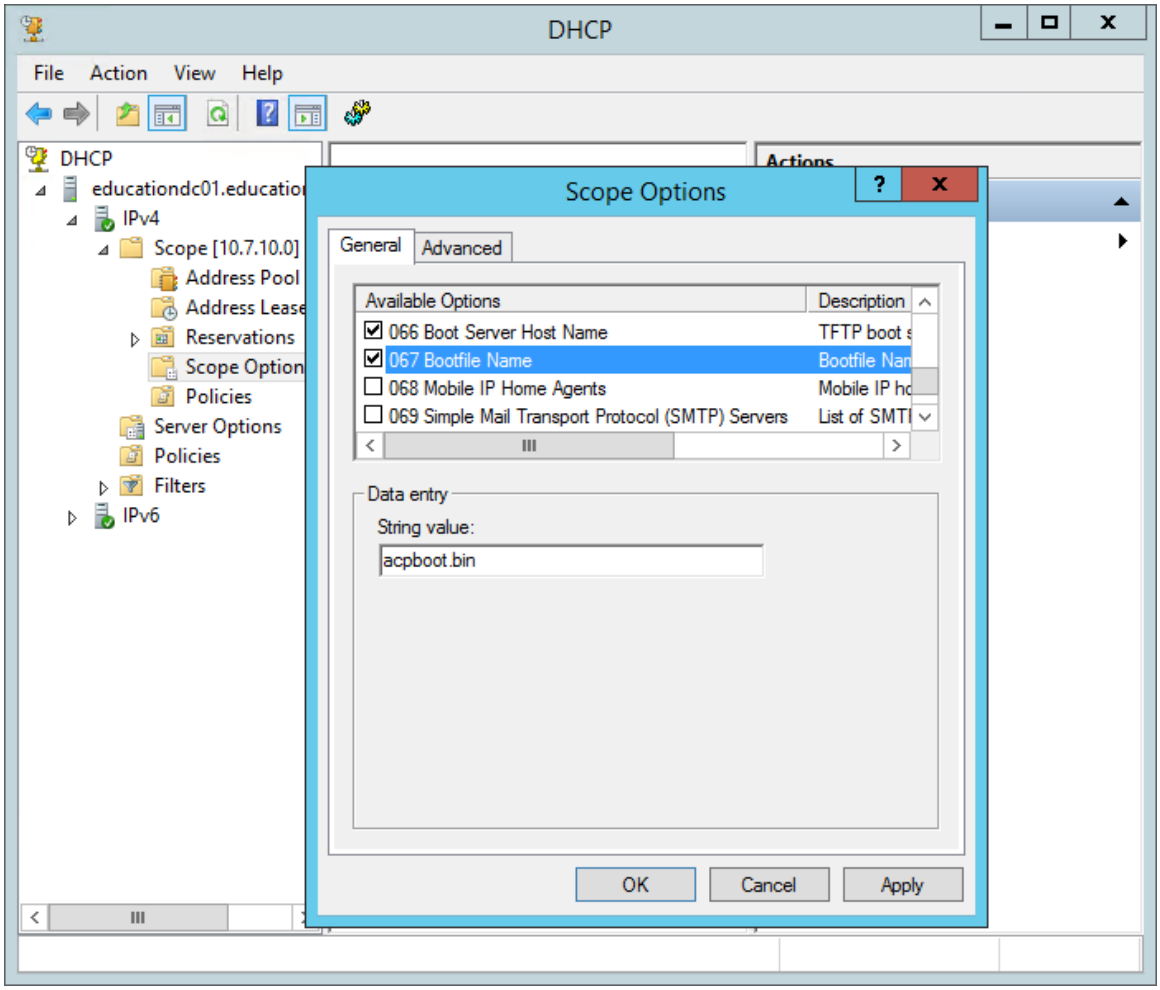
20.3.4. Using standard DHCP server with Boot Options

The **Using standard DHCP server** mode is used when you have an existing DHCP server and want it to provide all the information.

The DHCP server needs to be configured to provide **Option 66, Boot Server Host Name**, and **Option 67, Bootfile Name**.

20.3.4.1. On the DHCP Server

Open the **Microsoft DHCP Service** by selecting ***Start > Administrative Tools > Computer Management*** on your Microsoft DHCP server.



Microsoft 2012 Server DHCP Scope Options

Right click on the ***Scope Options*** in the Scope tree and select ***Configure Options***.

Scroll to ***Option 066 Boot Server Host Name***, check the check box, and enter the IP address of the ThinManager Server in the ***String Value*** field. If you use a redundant pair of ThinManager Servers enter both IP addresses separated by a space.

Scroll to ***Option 067 Bootfile Name***, check the check box, and enter "**acpboot.bin**" in the ***String Value*** field.

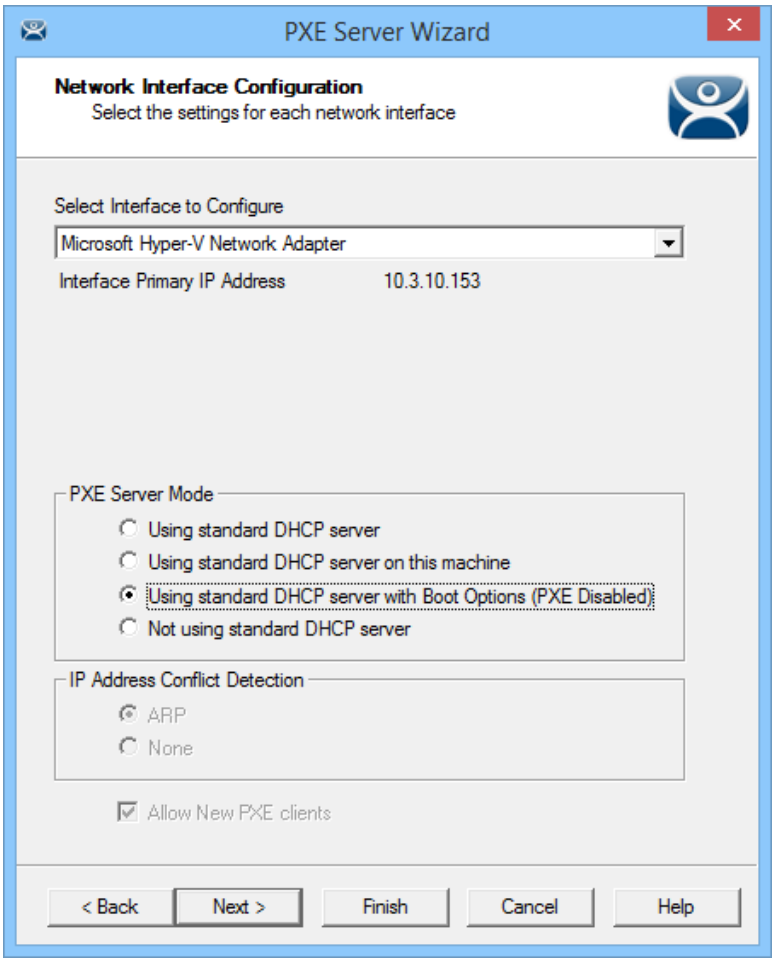
Configuring a DHCP to provide IP addresses, the ThinManager Server IP address as ***Option 066***, and the **acpboot.bin** bootfile as ***Option 067*** will allow the DHCP server to provide the boot information to both ThinManager Ready thin clients using the default DHCP and ThinManager Compatible thin clients using PXE boot.

20.3.4.2. In ThinManager

Select ***Manage > PXE Server*** to open **the PXE Server Wizard**.

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

Select ***Next*** to continue with the wizard.



Network Interface Configuration Page of PXE Server Configuration

Select the ***Using standard DHCP server with Boot Options*** radio button on the **Network Interface Configuration** page.

Select the ***Finish*** button and the PXE server is configured.

The ThinManager Compatible thin client will make a DHCP request when it is turned on. The DHCP server will respond with the client IP address, the ThinManager address, and the name of the bootfile to download. The ThinManager Compatible thin client will connect to ThinManager.

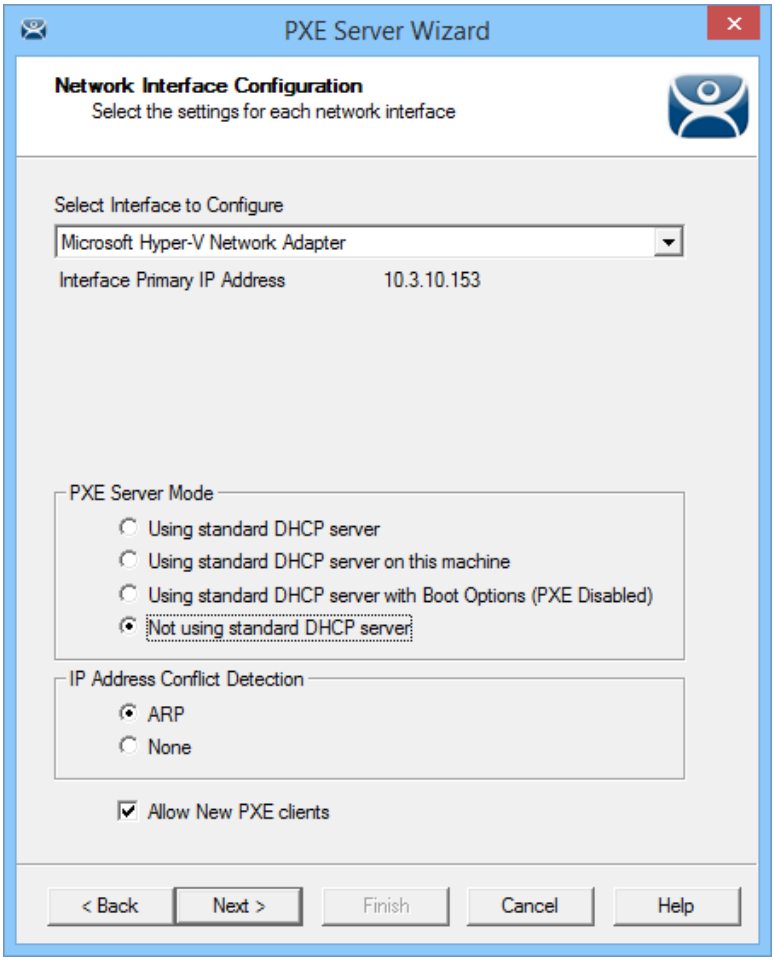
20.3.5. Not using standard DHCP server

The **Not using standard DHCP server** mode is used when you do not have an existing DHCP server. This mode is configured to give ThinManager the ability to pass all the information needed to boot.

ThinManager will only pass IP addresses to terminals making a PXE request. IT will ignore traditional DHCP requests.

Select ***Manage > PXE Server*** to open the PXE Server Wizard.

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



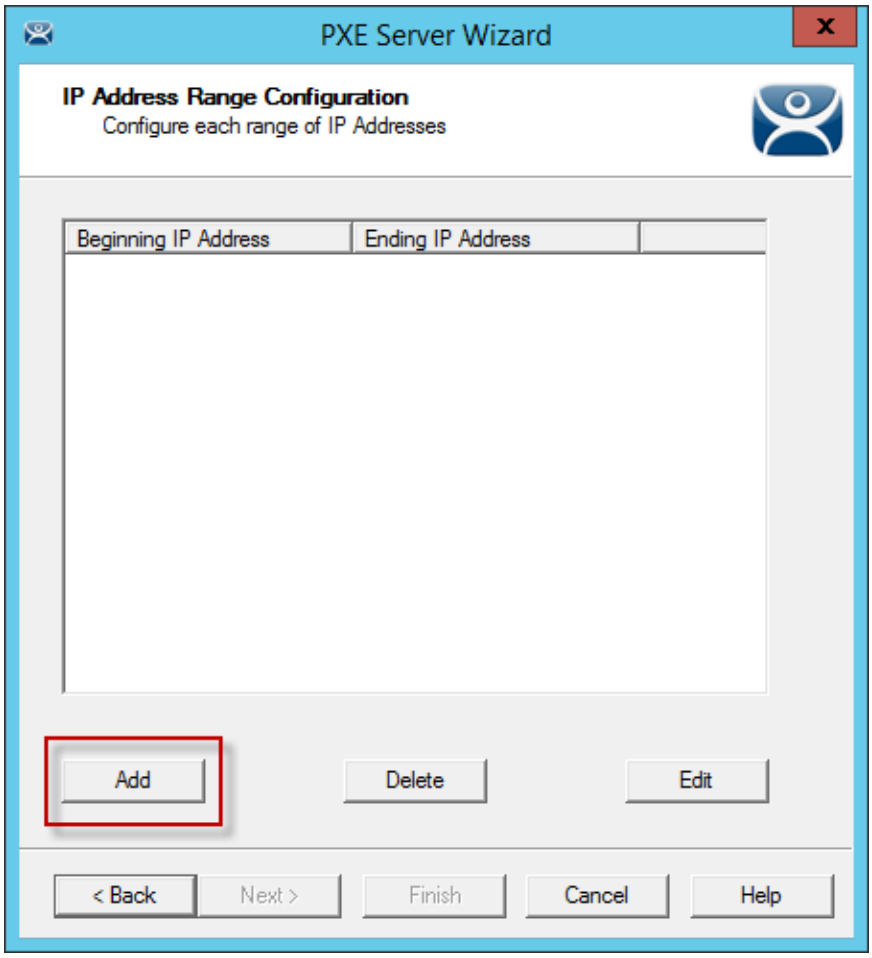
Network Interface Configuration Page of the PXE Server Wizard

Select the ***Not using standard DHCP*** radio button on the **Network Interface Configuration** page.

The ***IP Address Conflict Detection*** will check for conflicts in the Address Resolution Protocol when the ***ARP*** radio button is selected.

The ***Allow New PXE clients*** controls whether ThinManager gives PXE information to new PXE boot ThinManager Compatible thin clients.

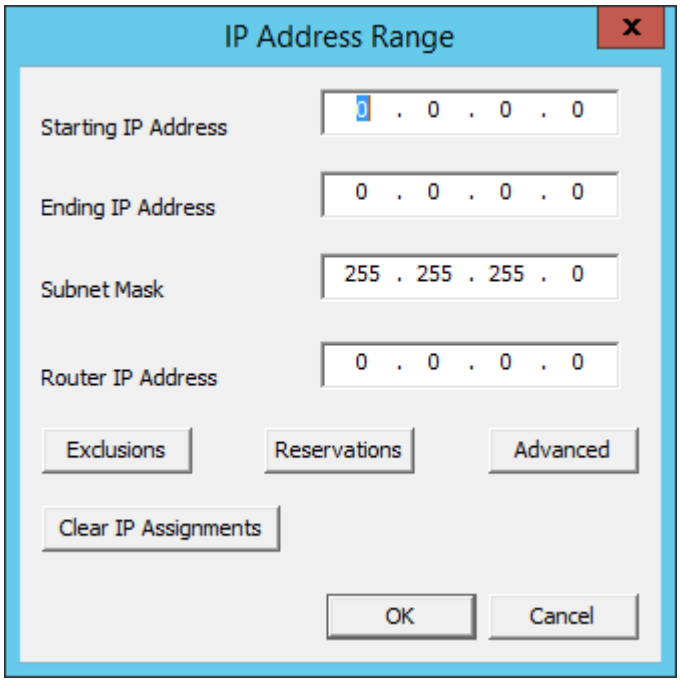
Select the ***Next*** button to navigate to the **IP Address Range Configuration** page.



IP Address Range Configuration Page of the PXE Configuration Wizard

The ThinManager Server needs to have a range of IP addresses added so that it can give the ThinManager Compatible thin client their IP addresses. This is done on the on the **IP Address Range Configuration** page.

Select the ***Add*** button on the **IP Address Range Configuration** page to launch the **IP Address Range** window.



IP Address Range Window

Enter the first IP address of the range in the ***Starting IP Address*** fields.

Enter the last IP address of the range in the ***Ending IP Address*** fields.

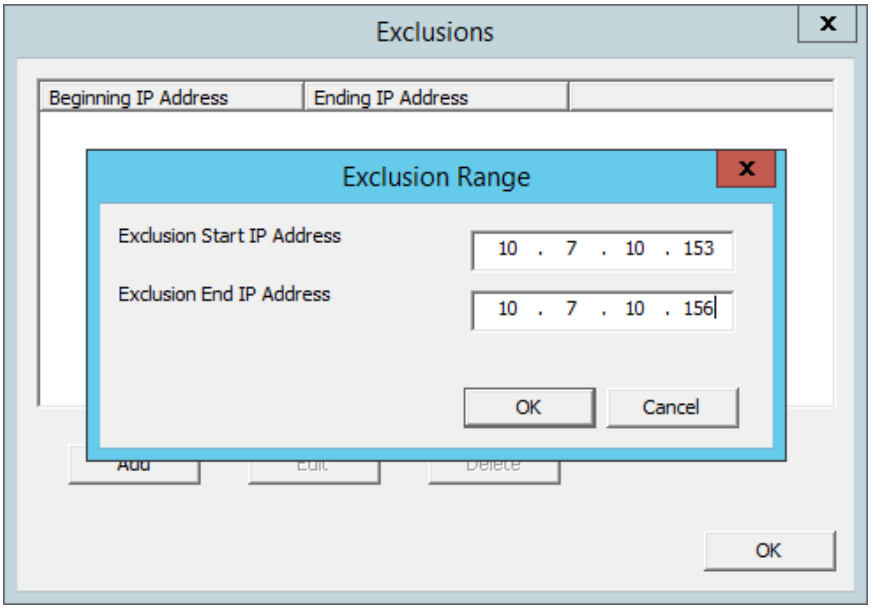
You may also configure the ***Subnet Mask*** and add the IP address for a router.

If you are done select the ***OK*** button to set the range and close the **IP Address Range** window.

If you want to add an **Exclusion** select the ***Exclusion*** button to open the **Exclusions** window.

20.3.6. Exclusions

Exclusions, IP addresses not to be assigned, can be configured by selecting the ***Exclusions*** button to launch the **Exclusions** window.



Exclusions Window and Exclusion Range Window

Select the ***Add*** button on the **IP Address Range Configuration** page to launch the **IP Address Range** window.

Select the ***Exclusions*** button to launch the **Exclusion** window.

Select the ***Add*** button to launch the **Exclusion Range** window.

Enter the range of IP addresses to exclude from assignment by putting the first and last IP address in the ***Exclusion Start IP Address*** and ***Exclusion Stop IP Address*** fields and click the ***OK*** button.

If you are excluding a single IP address then enter it in the ***Exclusion Start IP Address*** field and click the ***OK*** button.

If you are done select the ***OK*** button to set the range and close the **Exclusion** window.

If you want to add a Reservation close the **Exclusion** window and select the ***Reservation*** button to open the **Reservations** window.

20.3.7. Reservations

Reservations allows you to assign a specific IP address to a thin client each time it boots.

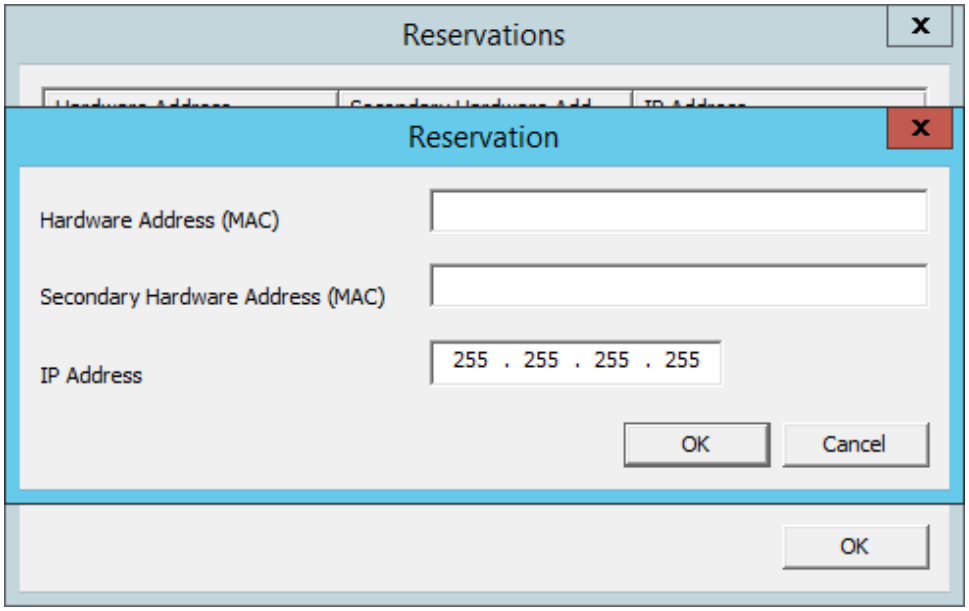
This can be done in the PXE Server or in the Terminal Configuration Wizard.

20.3.8. Reservations in the PXE Server:

Select the ***Add*** button on the **IP Address Range Configuration** page to launch the **IP Address Range** window.

Select the ***Reservations*** button to launch the **Reservations** window.

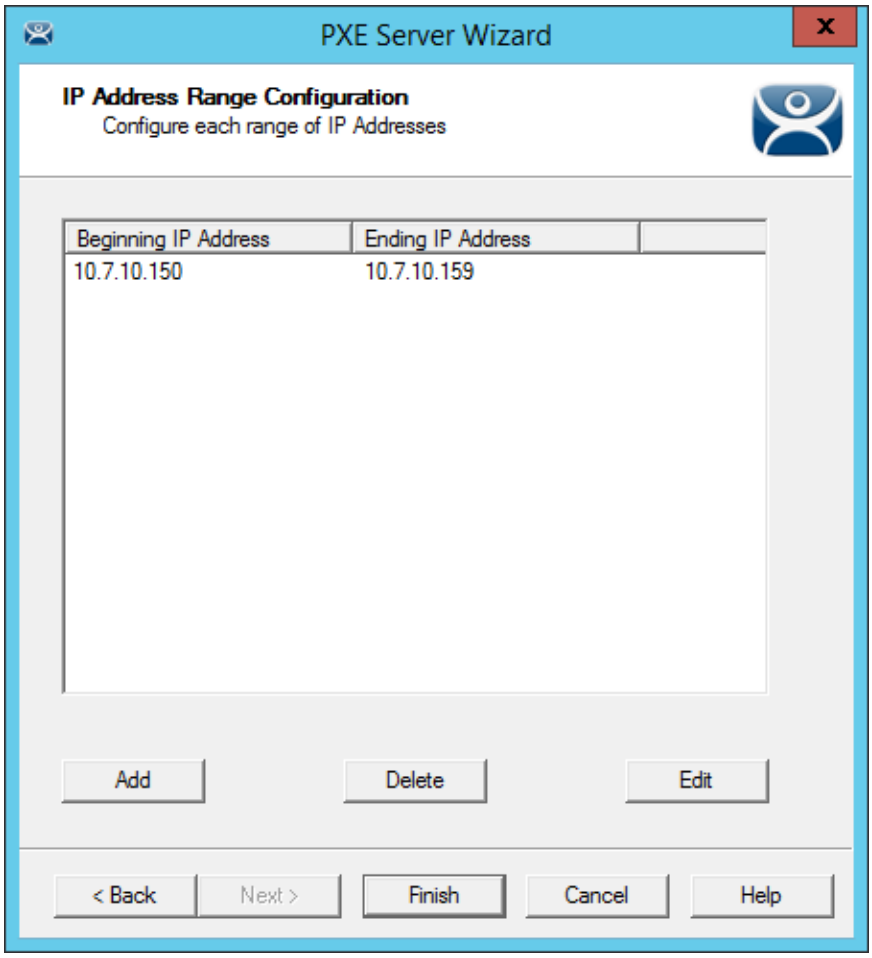
Select the ***Add*** button to launch the **Reservation** window.



Reservation Window in the PXE Server

Enter the MAC address from the ThinManager Compatible thin client in the ***Hardware Address (MAC)*** field. Enter a secondary MAC if it has two NICs. These are often on the serial number label.

Enter the IP address you want to assign to it in the ***IP Address*** fields and click the ***OK*** button.



IP Address Range in PXE Server

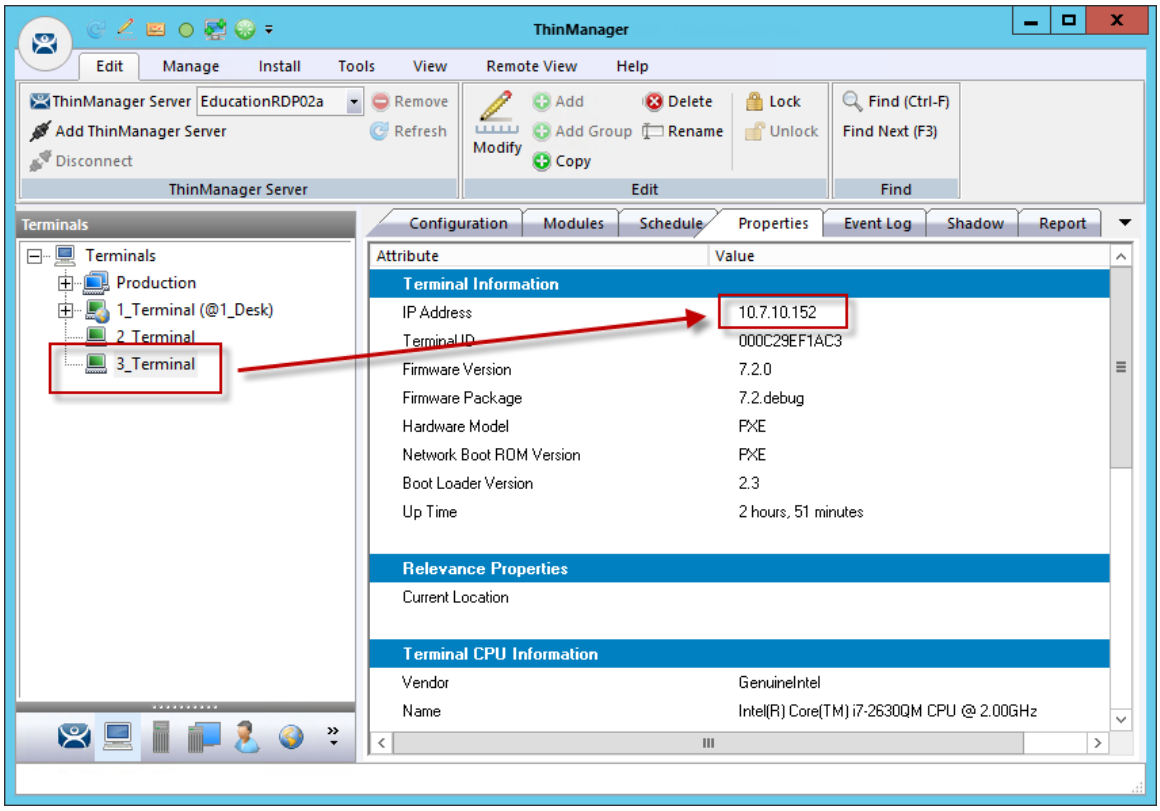
The IP address range will be displayed when you close the IP Address Range window.

Note: The ThinManager PXE server is not a true DHCP server. It will only issue IP addresses to PXE boot devices. It will not assign IP addresses to other computers, laptops, or devices.

20.3.1. Reservations in the Terminal Configuration Wizard

ThinManager has an easy way to reserve IP addresses for PXE boot thin clients.

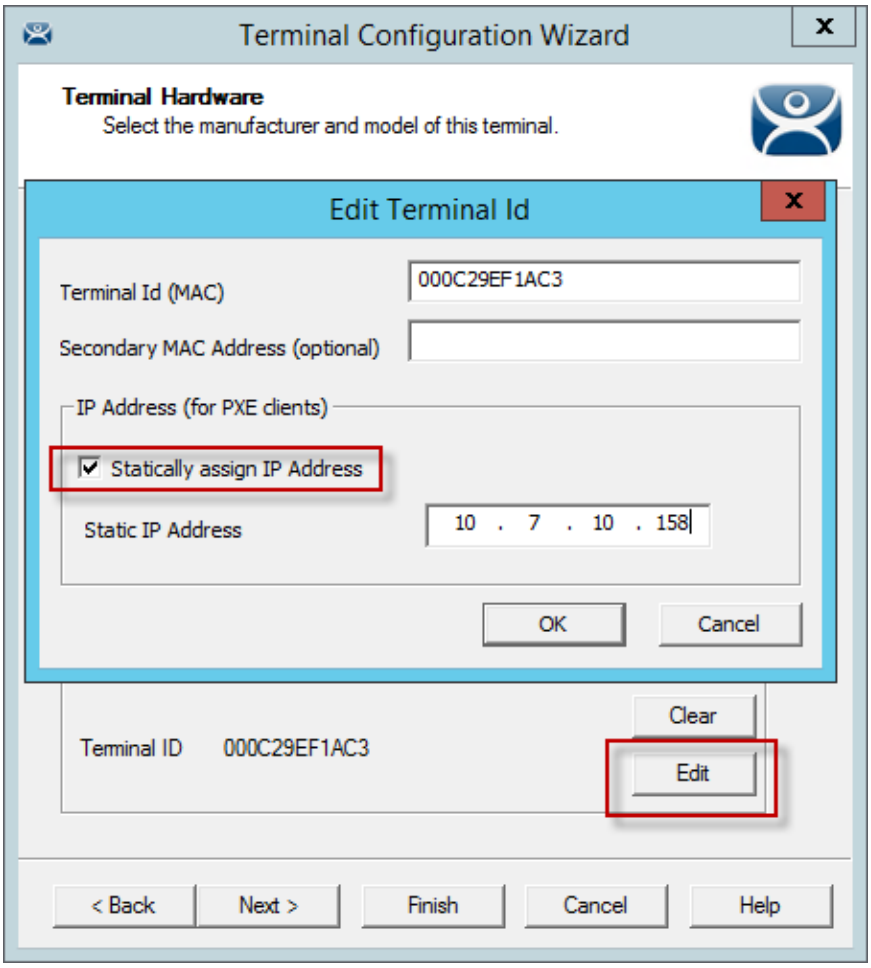
- Turn on the device and associate it with a configuration.
- Turn off the device so the Terminal icon in the tree is red.
- Open the Terminal Configuration Wizard and assign the IP address on the Terminal Hardware page.
- Restart the device.



Original Assigned IP Address

This picture shows the original IP address.

Turn off the device. You cannot change the IP address of a Terminal that is turned on.



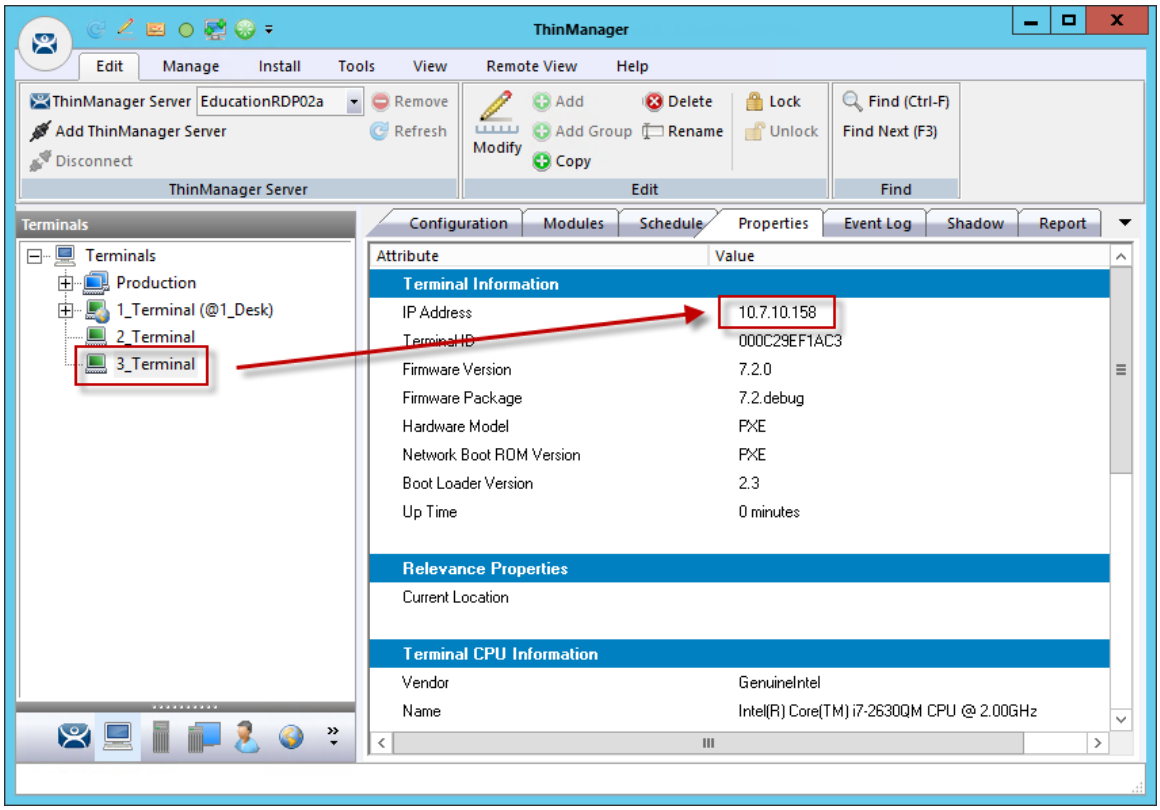
Edit Terminal ID Window

Double click on a turned off Terminal in the ThinManager tree to open the **Terminal Configuration Wizard**.

Navigate to the **Terminal Hardware** page and click the ***Edit*** button to launch the **Edit Terminal ID** page. It will only be active on Terminals that are off.

Check the ***Statically assign IP address*** checkbox. This allows you to set a static IP reservation when assigning addresses with the ThinManager PXE server..

Select ***OK*** to close the **Edit Terminal ID** page and the ***Finish*** button to close the Terminal **Configuration Wizard**.



Newly Assigned IP Address

Restart the Terminal. It will now be assigned the new IP address.

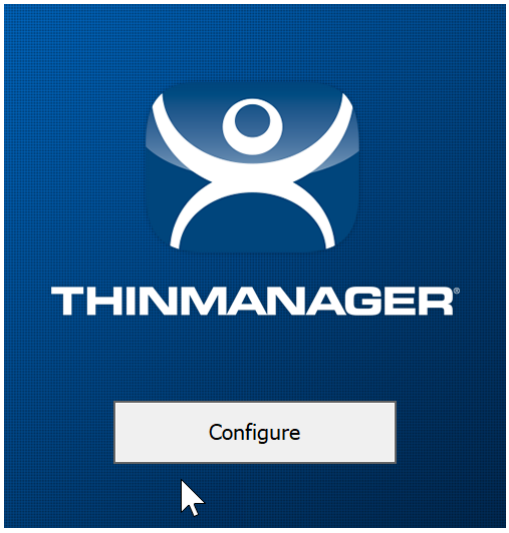
Note: An advantage of using ThinManager to assign IP addresses is that if you do a replacement, the replacement Terminal will be assigned that reserved IP address.

20.4. Local WinTMC Configuration

WinTMC is a PC application that allows ThinManager to manage the RDP connections between the PC and Remote Desktop Servers. It also provides enhanced features lacking in standard RDP connections like failover and Instant Failover.

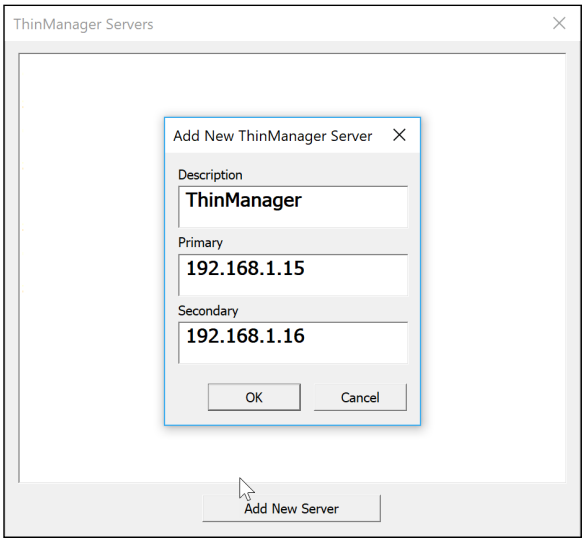
The WinTMC needs installed on the PC then it needs to be configured to point to ThinManager to receive its configuration.

When WinTMC starts, a ***Configure*** button will be displayed on the splash screen.



WinTMC Splash Screen

Click on the **Configure** button to specify the ThinManager Server(s) to use.



WinTMC ThinManager Server List Configuration

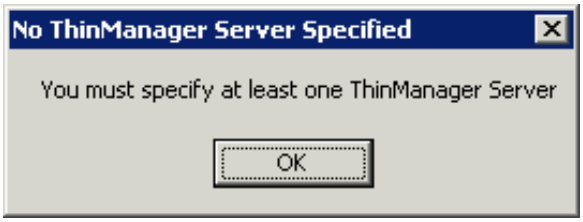
The ThinManager Server List allows the WinTMC to be pointed to one or more ThinManager Servers to retrieve its configuration.

Enter the IP address or name of your ThinManager Servers in the ***Enter new ThinManager Server Name or IP Address*** field and click the ***OK*** button to add them to the Current ThinManager Servers list.

The WinTMC will try to connect to the ThinManager Servers in the order listed, so the order can be changed with the ***Move Up*** and ***Move Down*** buttons.

Unneeded ThinManager Servers can be removed with the ***Delete*** button.

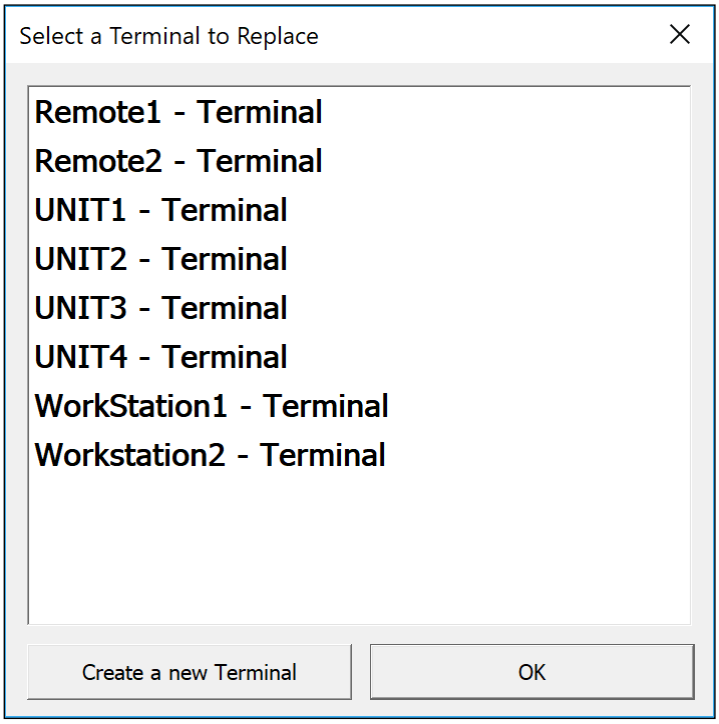
This configuration menu can be password protected by selecting the ***Set Password*** button. Once the password is set, when WinTMC is started and the Configure button is clicked, a password will be required to change the configuration.



No ThinManager Server Specified

If the ***OK*** button is selected without entering a ThinManager Server, an error window will remind you to enter a ThinManager Server address.

Once the local configuration is set, WinTMC will connect to a ThinManager Server and attempt to retrieve its configuration.



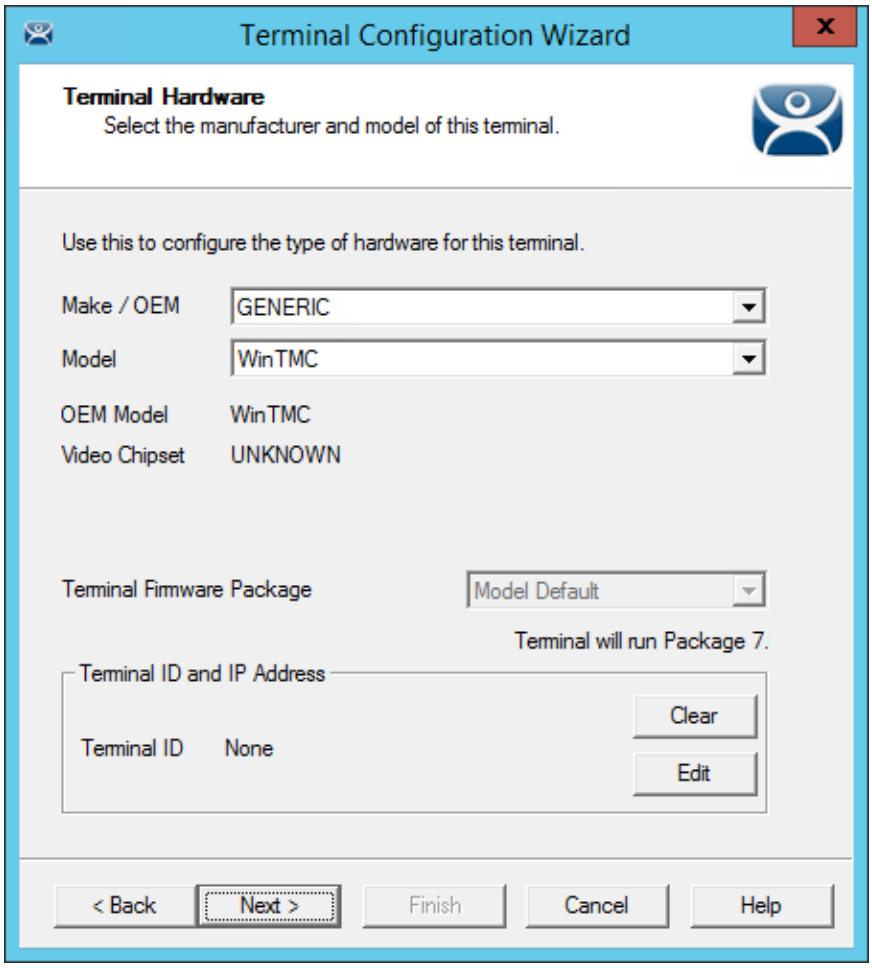
Terminal Replacement Dialog

If the WinTMC PC has not been defined, the user will be prompted with a dialog box to allow for the creating a new configuration or replacing an existing Terminal configuration on the ThinManager Server.

This functionality is similar to that of the create/replacement menu on a Thin Client. Select the thin client configuration you want to assume. Once the WinTMC has been assigned a configuration you will not need to make a selection again.

20.5. WinTMC Configuration in ThinManager

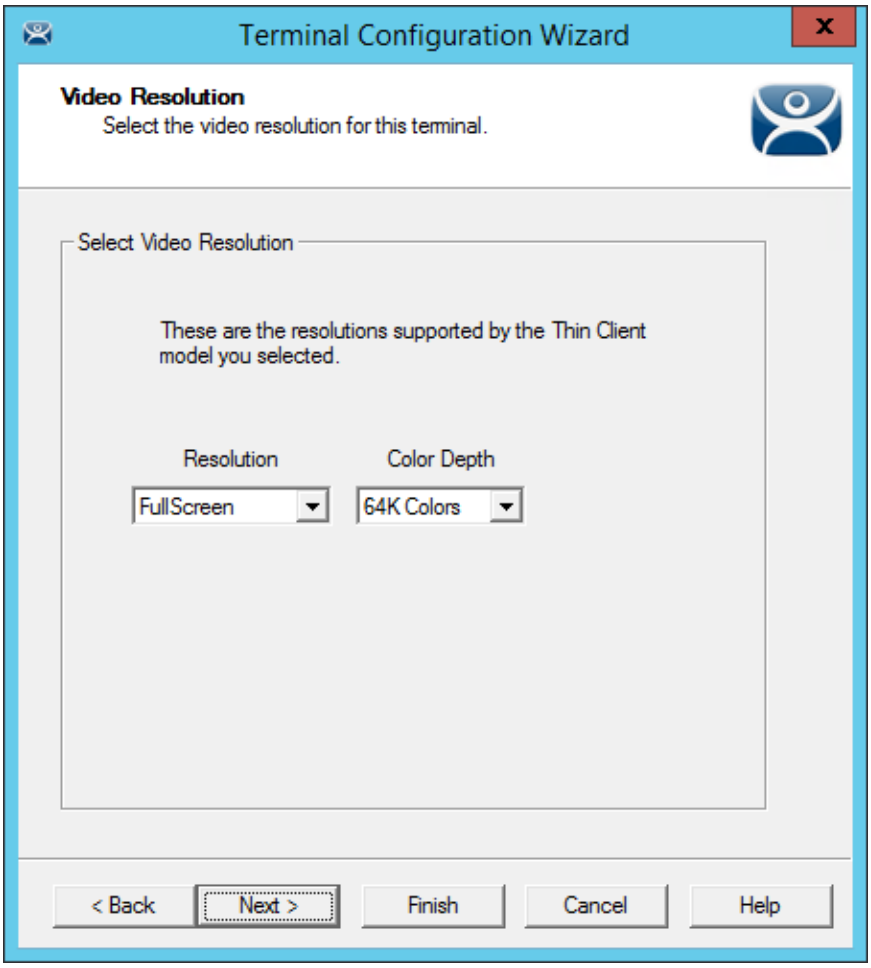
If you want to pre-create a WinTMC client in ThinManager using the Terminal Configuration Wizard, select **GENERIC** for the ***Make/OEM*** and **WinTMC** for the ***Model*** on the **Terminal Hardware** page of the Terminal Configuration Wizard.



WinTMC Settings in Terminal Hardware

The ***Terminal ID*** will fill in with the name of the PC once the WinTMC client is tied to a PC.

The **Terminal Configuration Wizard** for a WinTMC client is the same as for a thin client with a few exceptions. These include the **Video Resolution** page and the **WinTMC Settings** page.

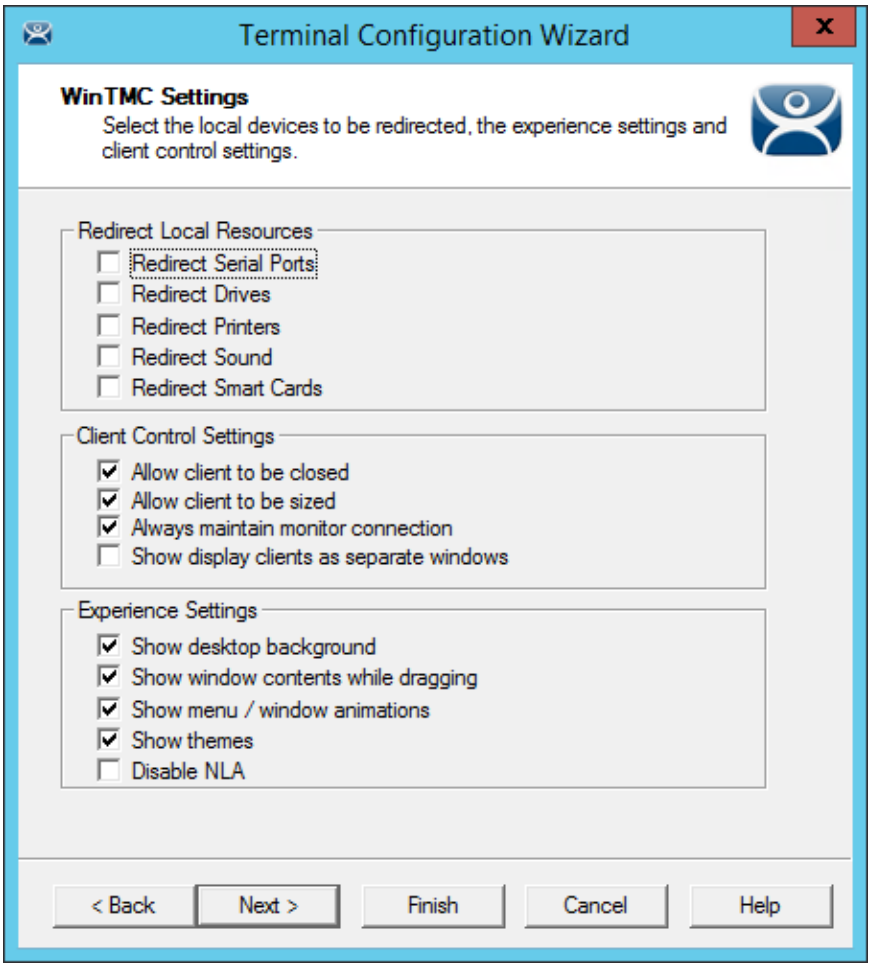


Video Resolution for WinTMC

The **Video Resolution** for WinTMC includes a setting for ***FullScreen***. This will fill whatever resolution the PC client is running.

You may also select from set resolutions.

Note: WinTMC running on computers with multiple monitors can run as MultiMonitor WinTMC clients.



WinTMC Settings

The **Terminal Configuration Wizard** includes a **WinTMC Settings** page for WinTMC clients. These only apply to connections made by the WinTMC application.

The settings include:

Redirect Local Resources:

- **Redirect Serial Ports** - This checkbox, if selected, will make local serial ports available in a session. Serial Port redirection does not work when you connect to a Remote Desktop Server running Windows 2000 or earlier.
- **Redirect Drives** - This checkbox, if selected, will make local drives available in a session. Drive redirection does not work when you connect to a Remote Desktop Server running Windows 2000 or earlier.
- **Redirect Printers** - This checkbox, if selected, will make your local printer available in a session.
- **Redirect Sound** - This checkbox, if selected, will allow audio played in your session to play locally. Sound redirection does not work when you connect to a Remote Desktop Server running Windows 2000 or earlier.
- **Redirect Smart Cards** - This checkbox, if selected, will make your smart card available in a session. Smart card redirection does not work when you connect to a Remote Desktop Server running Windows 2000 or earlier.

Client Control Settings:

- **Allow client to be closed -** This checkbox, if selected, will enable your user to close the client WinTMC program.
- **Allow client to be sized -** This checkbox, if selected, will enable your user to resize the client.
- **Always maintain monitor connection** – Enable this setting to keep the monitoring connection active when WinTMC is closed to allow shadowing. Unselecting this checkbox will release the WinTMC license when the WinTMC program is closed but will deny shadow access.
- **Show groups in separate windows** – This checkbox, if selected, will display multiple Display Clients as separate windows rather than in one window shell.

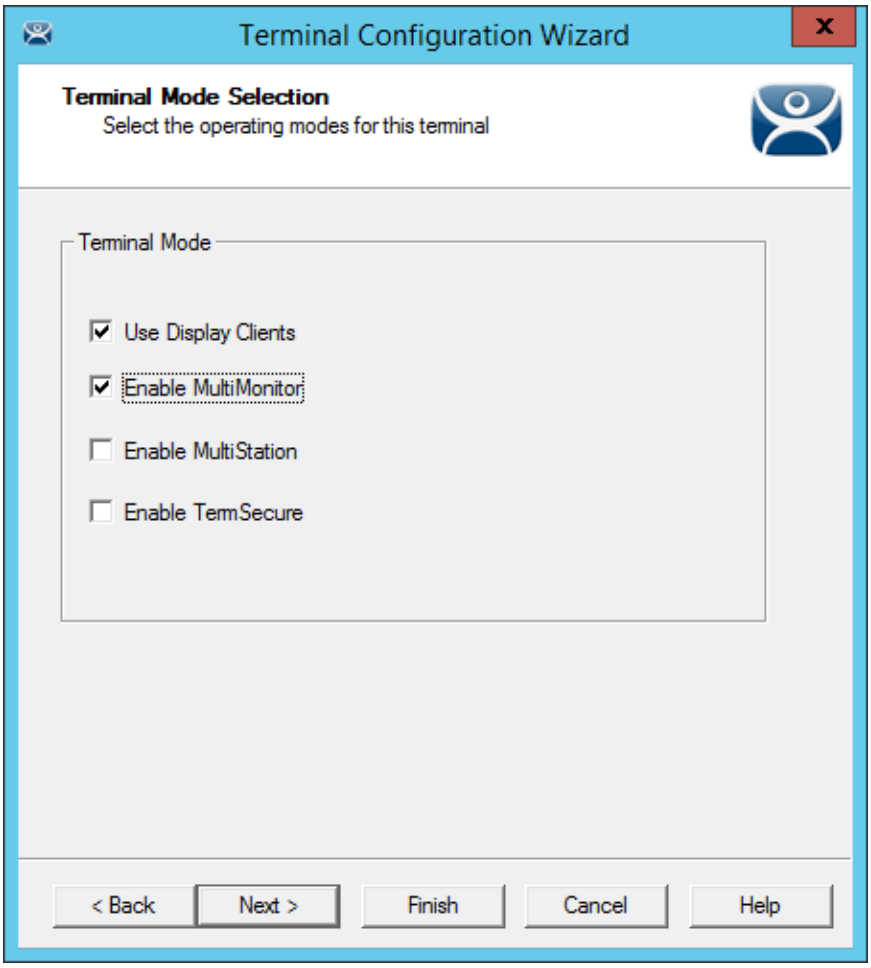
Experience Settings:

- **Show Desktop Background -** This checkbox, if selected, will enable your user to select a Windows Desktop Background. If not selected, the background will be a solid color.
- **Show window contents while dragging -** This checkbox, if selected, will show the window contents to be shown while the window is being dragged.
- **Show menu/window animations -** This checkbox, if selected, will enable menu/window animations on the client.
- **Show Themes -** This checkbox, if selected, will enable your user to select a Windows Theme.
- **Disable NLA -** This checkbox, if selected, will disable the use of Network Level Authentication for the client.

Note: These functions may be denied by user policies or Remote Desktop Server configuration. Check the Microsoft Local Policy, Group Policy, and Remote Desktop Services Configuration.

20.5.1. MultiMonitor WinTMC

ThinManager supports MultiMonitor for WinTMC if the PC has Windows running on multiple video cards. If the PC is successfully running multiple monitors on the host OS then WinTMC can run MultiMonitor using up to five monitors.



MultiMonitor – Enable MultiMonitor

Selecting the ***Enable MultiMonitor*** checkbox on the **Terminal Mode Selection** page will allow you to configure a WinTMC client for MultiMonitor use.

MultiMonitor requires the use of Display Clients. Once the ***Use Display Clients*** checkbox is selected on the **Terminal Mode Selection** page the ***Enable MultiMonitor*** checkbox becomes visible.

Select the ***Use Display Clients*** and the ***Enable MultiMonitor*** checkboxes, and then select the ***Next*** button.

The Terminal Configuration Wizard will display the **MultiMonitor Video Settings** page, **Monitor Layout** page, and **Display Client Selection** page like it does for thin clients.

20.5.2. WinTMC Modules

WinTMC clients cannot use the ThinManager modules because they are running Windows locally. One must install touch drivers, sound drivers, printers, and etc. through the local Windows operating system instead of relying on ThinManager modules.

21. Devices – Mobile Devices

ThinManager supports Microsoft tablets with WinTMC, Apple iPads and iPhones with iTMC, and Android devices with aTMC.

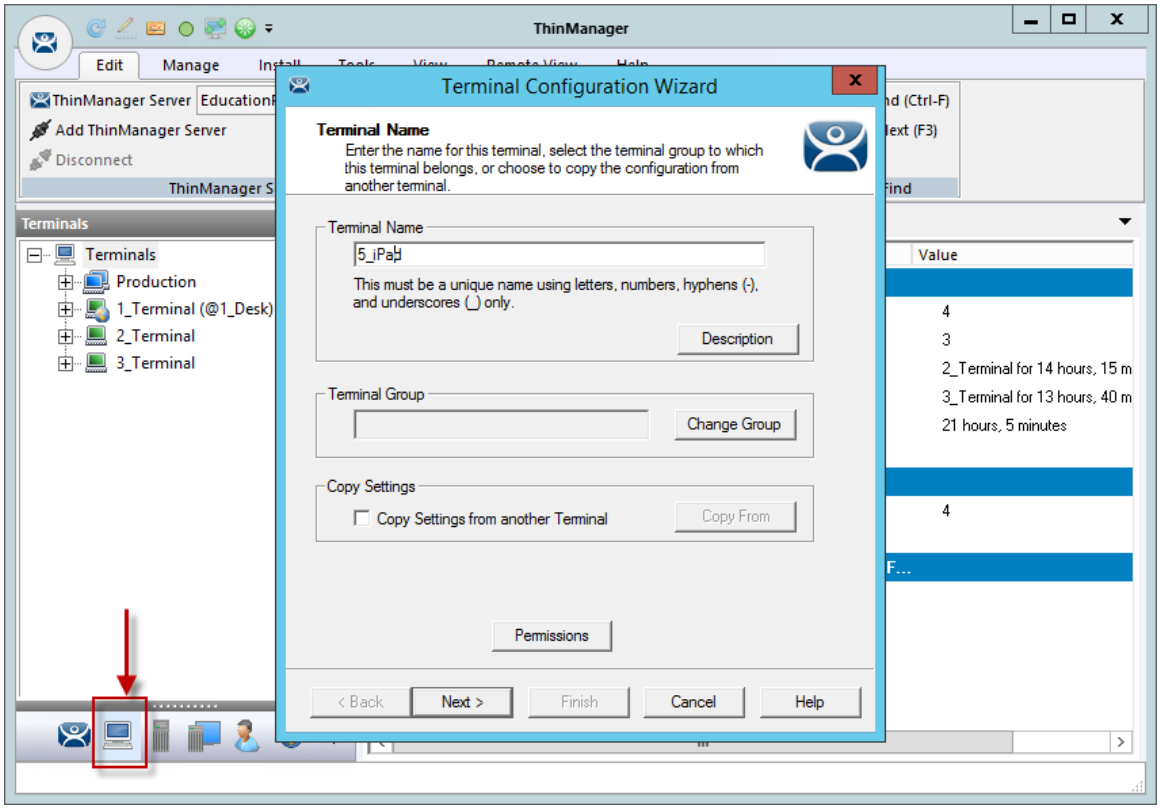
Apple iPad 2 is supported but Bluetooth requires iPad 4.

Currently we support Android 5.0 and higher.

21.1. Configuring an iPad in ThinManager

A configuration needs to be created in ThinManager so that the mobile device can join the system as a Terminal.

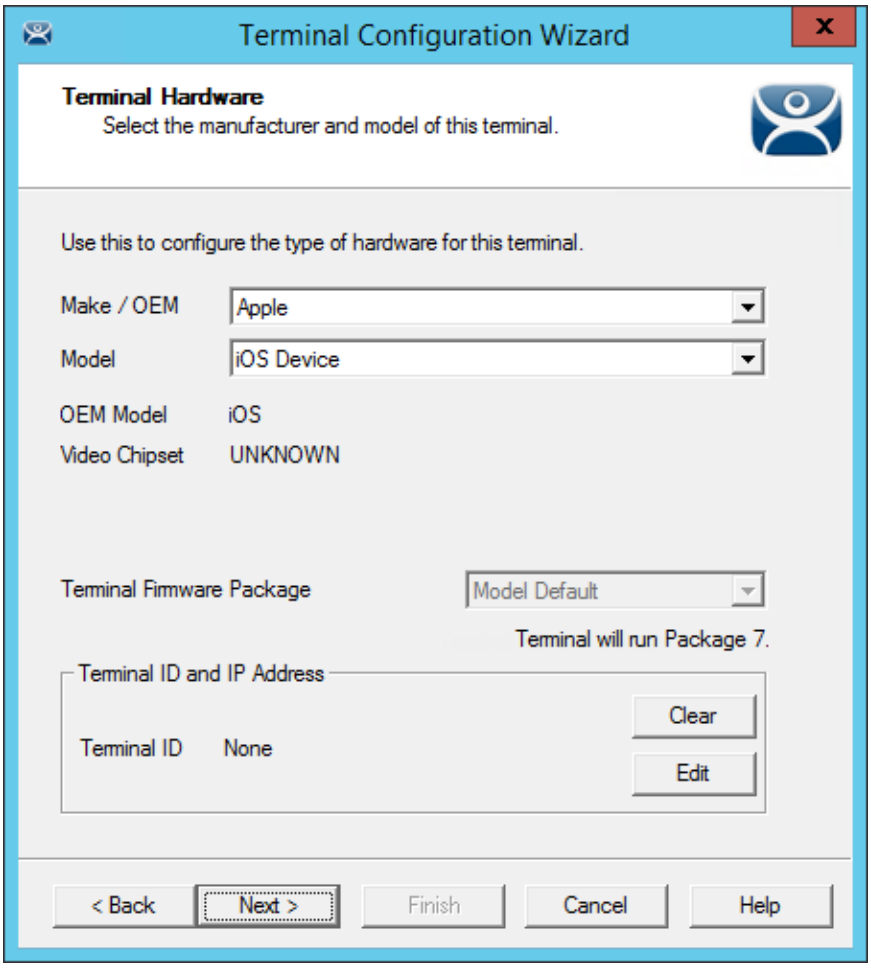
Open ThinManager and select the **Terminal** icon to show the Terminal branch of the tree.



ThinManager Terminal Configuration Wizard

Right click on the Terminals branch and select ***Add Terminal*** to launch the **Terminal Configuration wizard**.

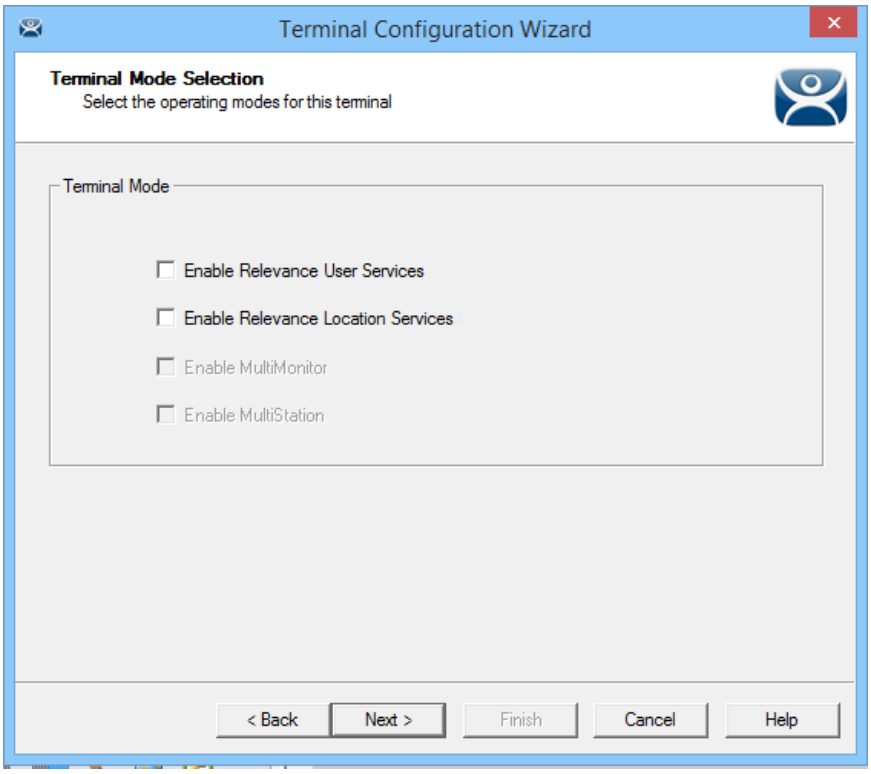
Enter the name for your mobile device and select ***Next***.



Terminal Hardware Page

Select ***Apple / iOS*** for the make and model of hardware.

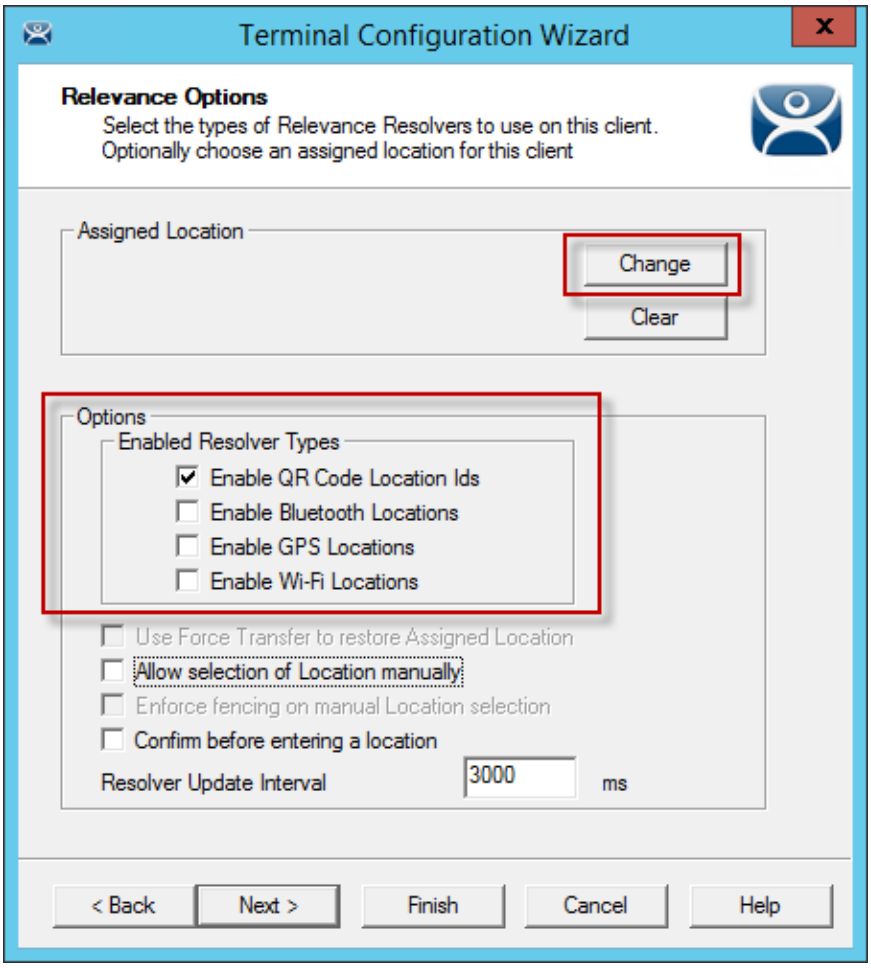
Navigate to the **Terminal Mode Selection** page by clicking ***Next***.



Terminal Mode Selection Page

An iPad can run as a traditional client and have an application sent to it without using Relevance. However you should select the ***Enable Relevance User Services*** and ***Enable Relevance Location Services*** checkboxes if you want to control content by user permission or location.

Navigate to the **Relevance Options** page by clicking ***Next***.



Relevance Options Page

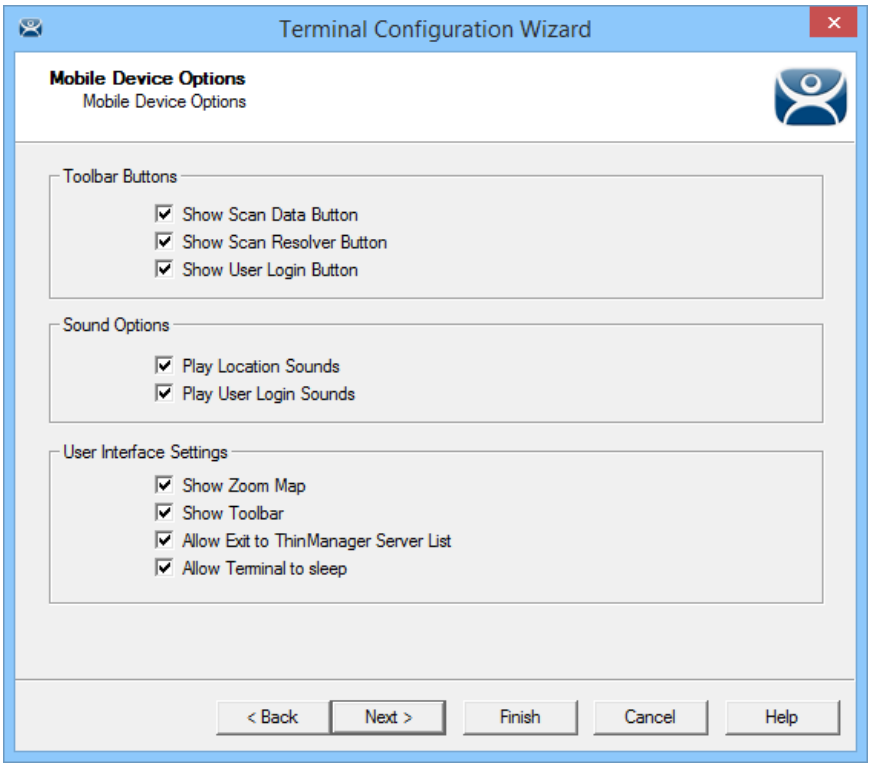
The **Relevance Options** page allows you to assign a location to the iPad. You may not what to assign the iPad to a location but have the iPad interact with different locations.

The **Relevance Options** page allows you to enable various Resolver types. Select the ones you want to use from the iPad.

- ***Enable QR Code Location Ids*** – This allows the scanning of a QR code to determine the location.
- ***Enable Bluetooth Locations*** – This allows the use of Bluetooth beacons to determine the location.
- ***Enable GPS Locations***– This allows the Global Positioning System of the mobile device to determine the location.
- ***Enable Wi-Fi Locations*** – This allows the signal strength of Wi-Fi access points to determine the location.

Each method selected will require configuration to associate a location with the Resolver data.

Navigate to the **Mobile Device Options** page by clicking ***Next***.



Mobile Device Options

The **Mobile Device Options** window has several settings that control the user experience on mobile devices.

This page allows you to disable features normally displayed in the mobile apps.

Toolbar Buttons

- ***Show Scan Data Button*** – This checkbox, when unselected, will hide the Scan Data button.
- ***Show Scan Resolver Button***– This checkbox, when unselected, will hide the Scan Resolver button.
- ***Show User Login Button***– This checkbox, when unselected, will hide the User Login button.

Sound Options

- ***Play Location Sounds*** – This checkbox, when selected, will play a sound when a location is entered.
- ***Play User Login Sounds*** – This checkbox, when selected, will play a sound when the user logs in as a TermSecure or Relevance user.

User Interface Settings

- ***Show Zoom Map*** – This checkbox, when unselected, will hide the screen map while zooming.
- ***Show Toolbar*** – This checkbox, when unselected, will hide the app toolbar.
- ***Allow Exit to ThinManager Server List*** – This checkbox, when unselected, will prevent the user from leaving the app to switch ThinManager Servers.
- ***Allow a Terminal to sleep*** – This check box allows the terminal to sleep and be waken with the ***Tools>Power Off*** and ***Tools>Power*** on commands.

Complete the wizard as you would for any other thin client.

21.1.1. Configuring an iPad for ThinManager

The iPad needs to have the iTMC client installed. The iTMC application can be downloaded from the Apple App Store for free.

Go to the Apple App Store.

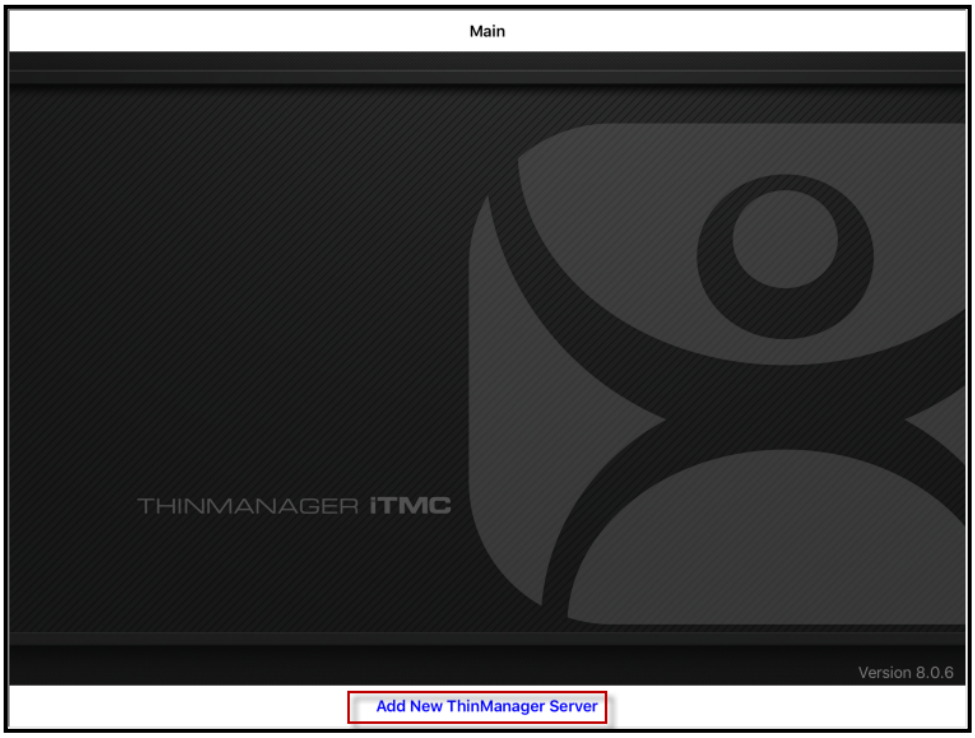
Enter **ThinManager** in the search field.

The version in February 2016 was **iTMC for ThinManager for Platform 8**.

Select the **iTMC** application and select ***Open***. It will download and install on your iPad.

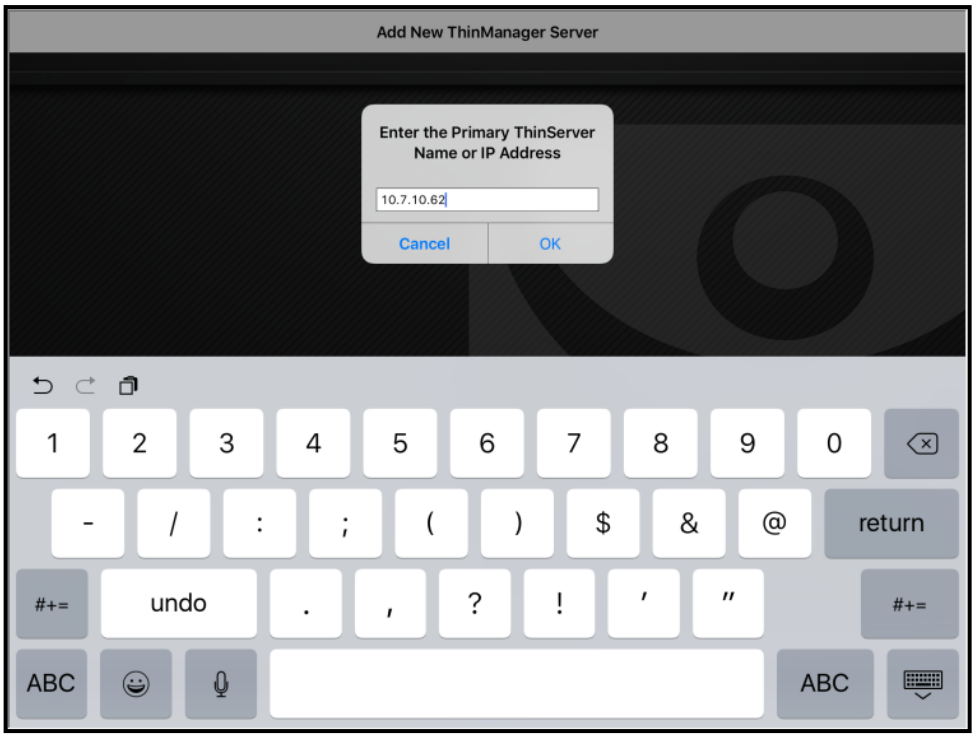
ThinManager iTMC Icon on iPad

The iTMC icon launches the iTMC program.



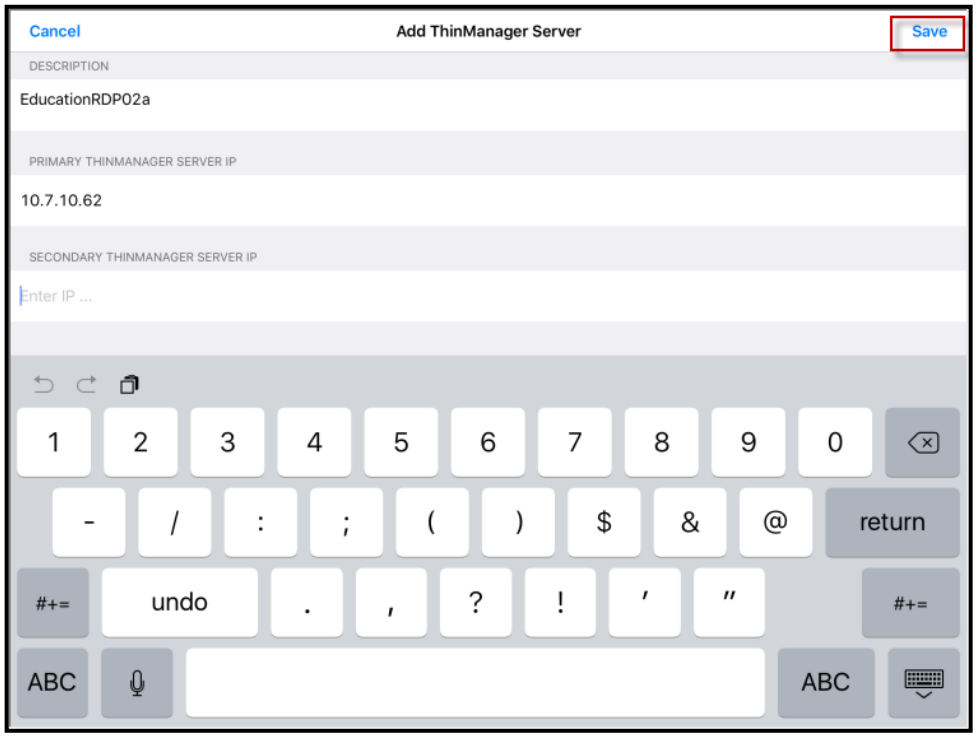
ThinManager iTMC Configuration Screen

Select the ***Add New ThinManager Server*** button at the bottom to add a ThinManager Server connection.



ThinManager Server Name Dialog

A dialog will be displayed. Enter the IP address of your primary ThinManager Server. Select the ***OK*** button when finished.



Add ThinManager Server Page

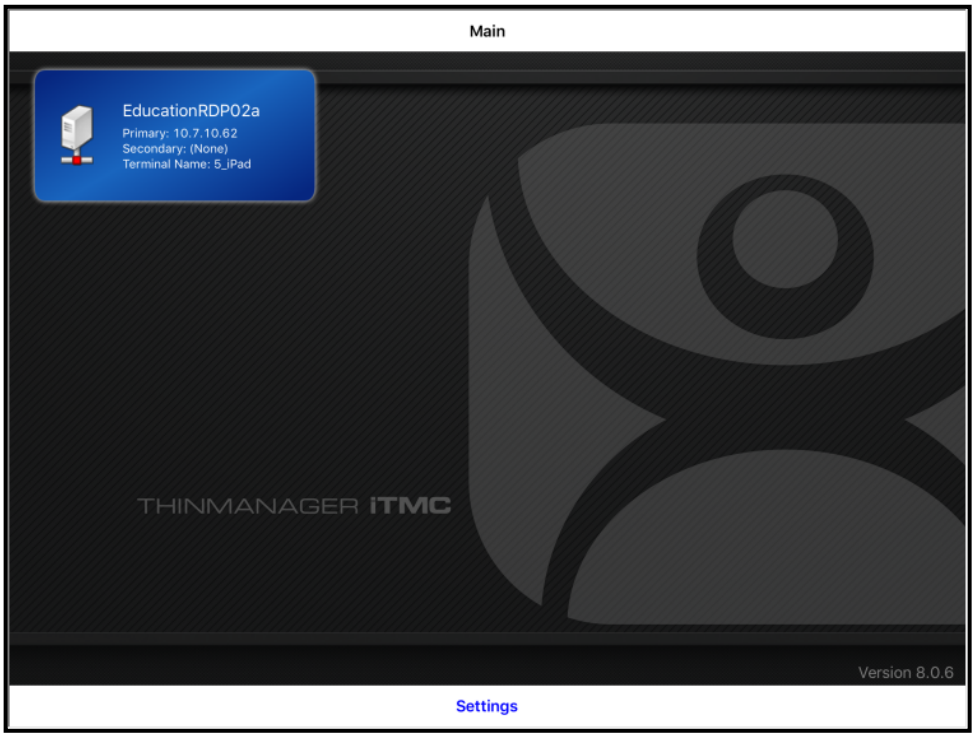
Enter the name of the primary ThinManager Server in the ***Description*** field.

Enter the IP address of a secondary ThinManager Server, if you have one.

Select the ***Save*** button in the corner. This will return you to the **Main** page.

21.1.2. Associating the iPad to the Configuration

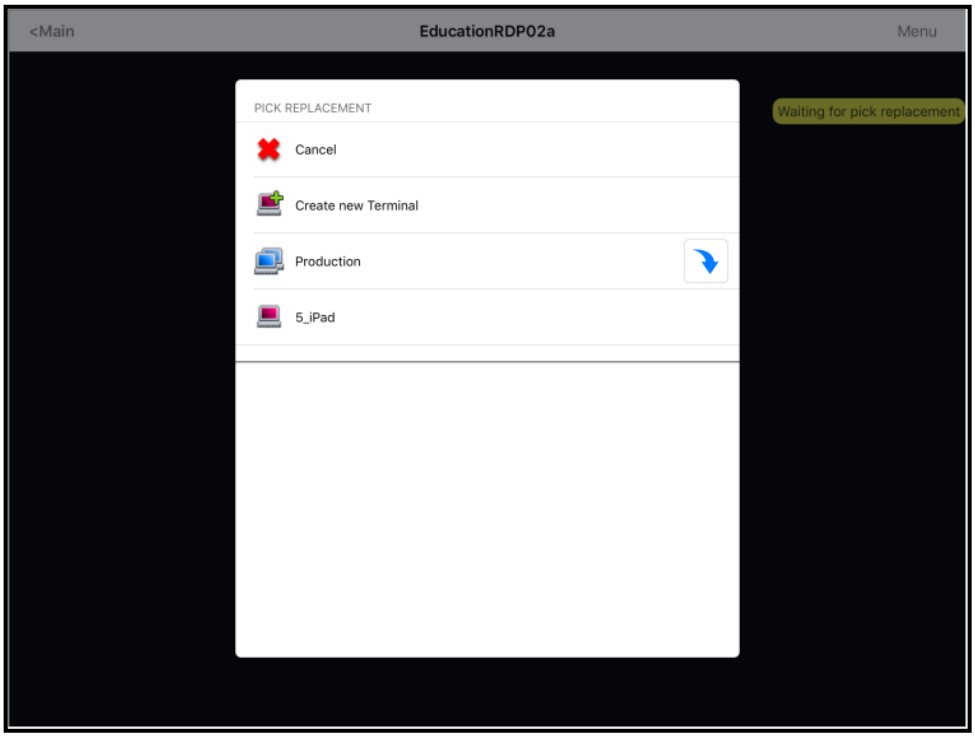
Once the ThinManager Server is defined on the iPad you need to associate the hardware to the iTMC configuration you created.



Main Screen with Defined ThinManager Server

The defined ThinManager Server will be displayed on the ***Main*** screen.

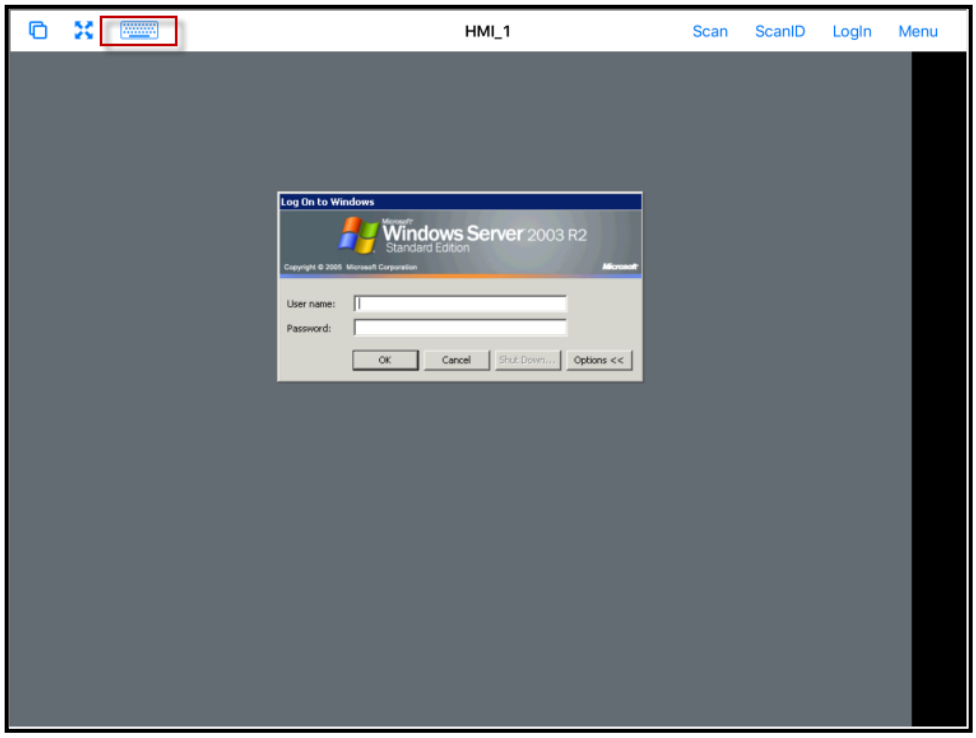
Select the **ThinManager Server**. You will be connected to that ThinManager Server.



Pick Replacement

A **Pick Replacement** window will be shown allowing you to select the newly created Terminal configuration or to launch the Terminal Configuration Wizard by selecting ***Create New Terminal***.

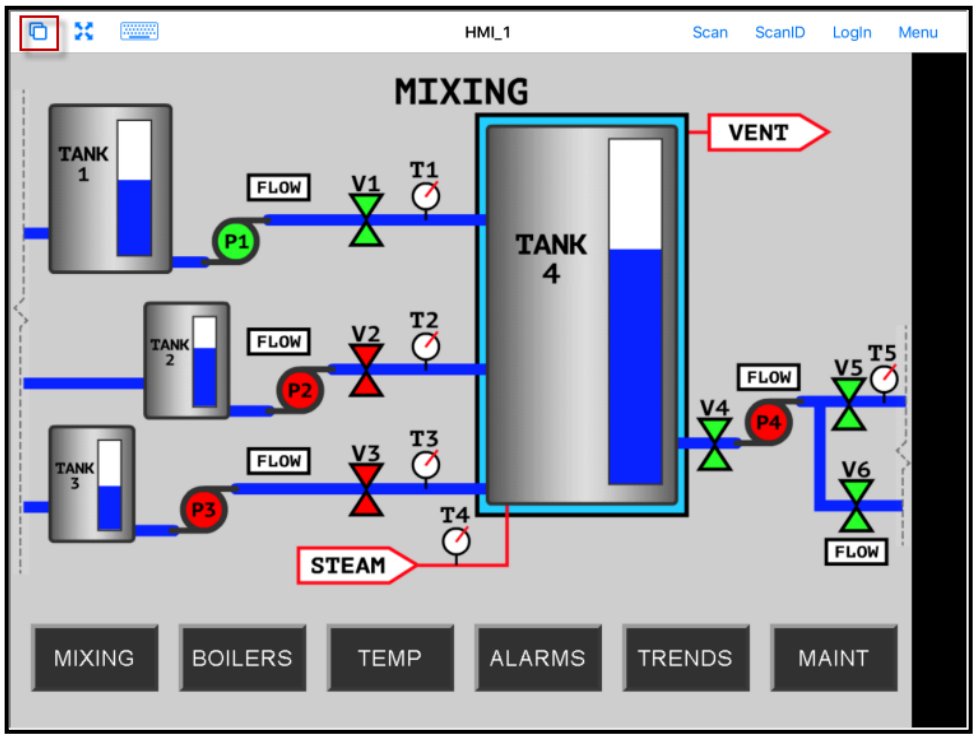
Touch your newly defined Terminal to choose the configuration you created for the iPad.



iTMC Client Session

Once the iTMC client connects it will launch the display client assigned in ThinManager.

The keyboard can be launched by selecting the **Keyboard** icon in the upper left corner.

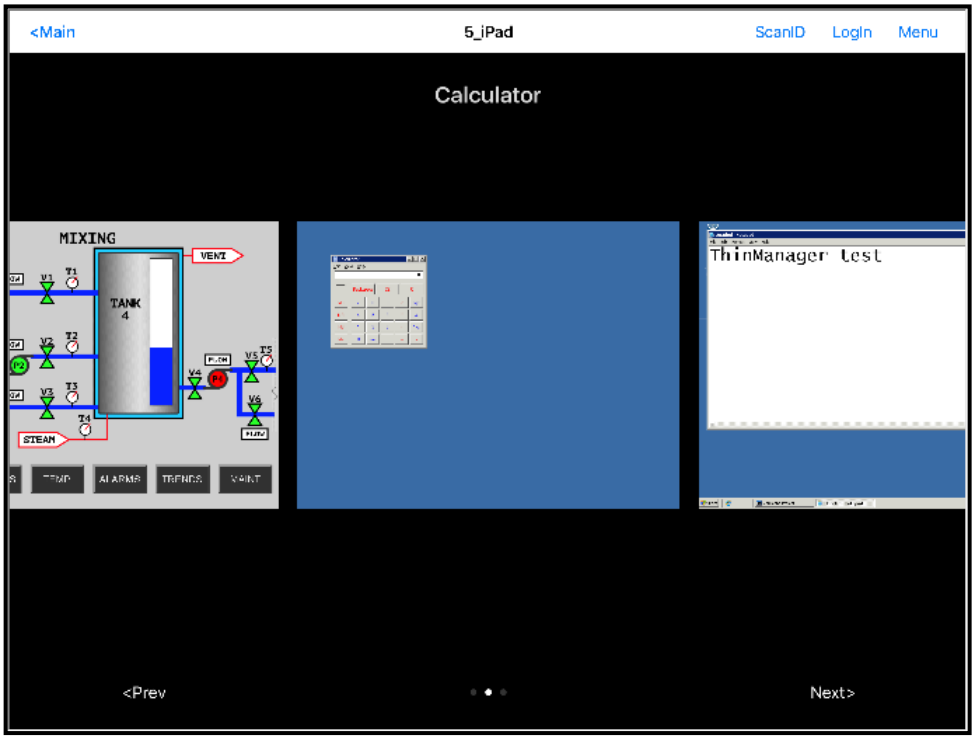


Display Client Session on iPad

The iPad will display one session at a time.

Configurations with MultiSession, using more than one display client will allow you to minimize the display client and switch display clients using a finger swipe.

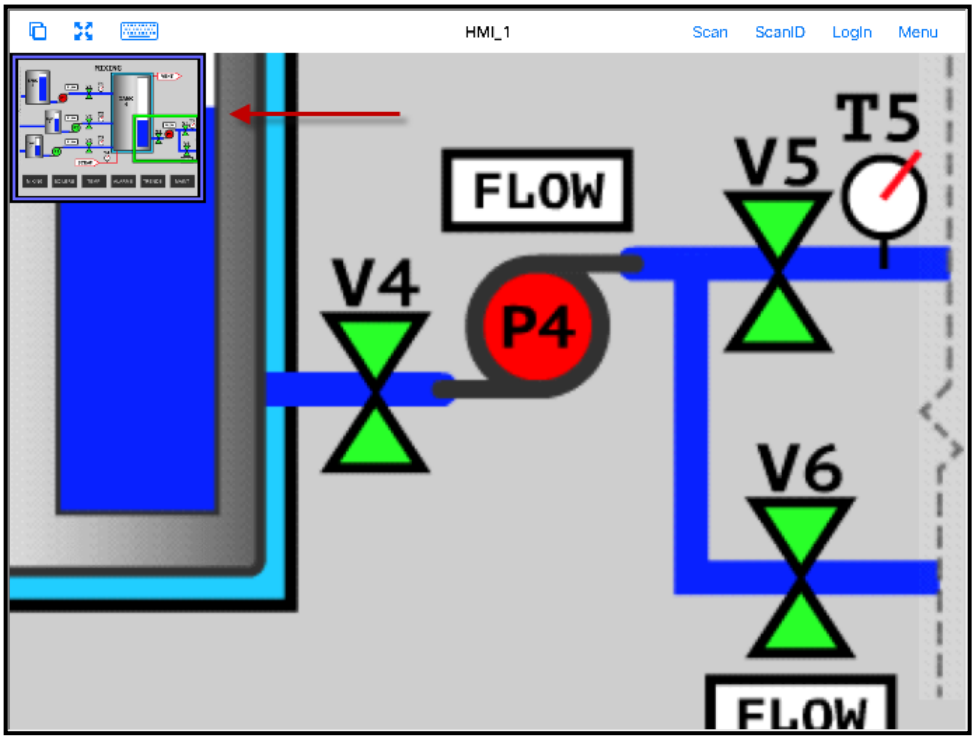
Selecting the **Cascade** icon in the upper right corner will show all the available display clients and allow you to navigate amongst them.



Multiple Display Clients

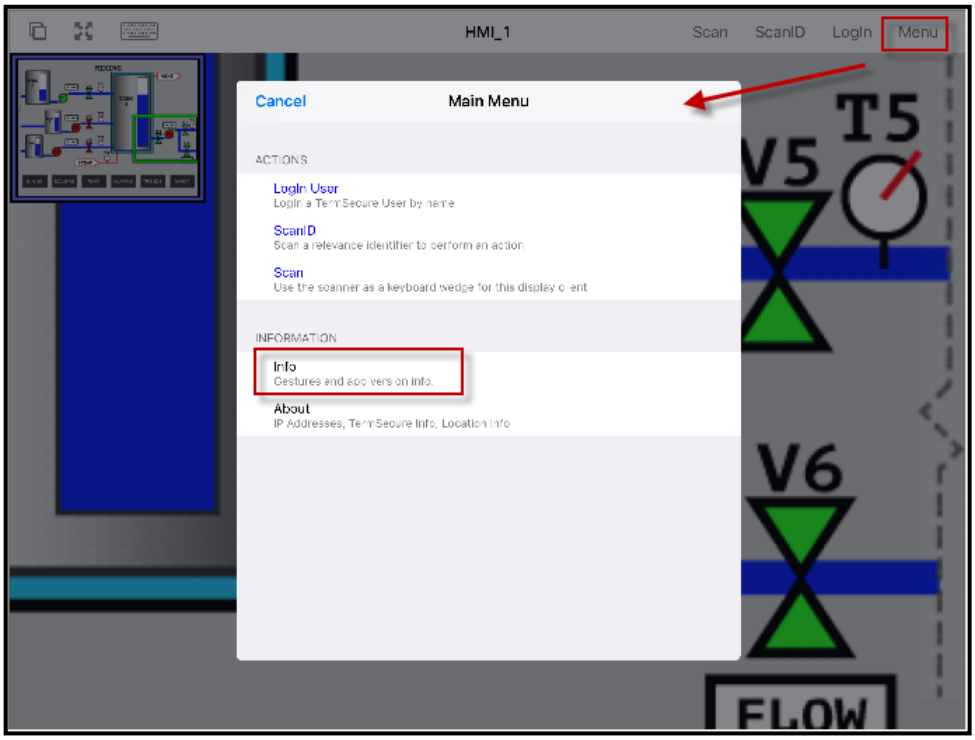
Touching a minimized display client will open it in full screen.

21.1.3. iTMC iPad Gestures



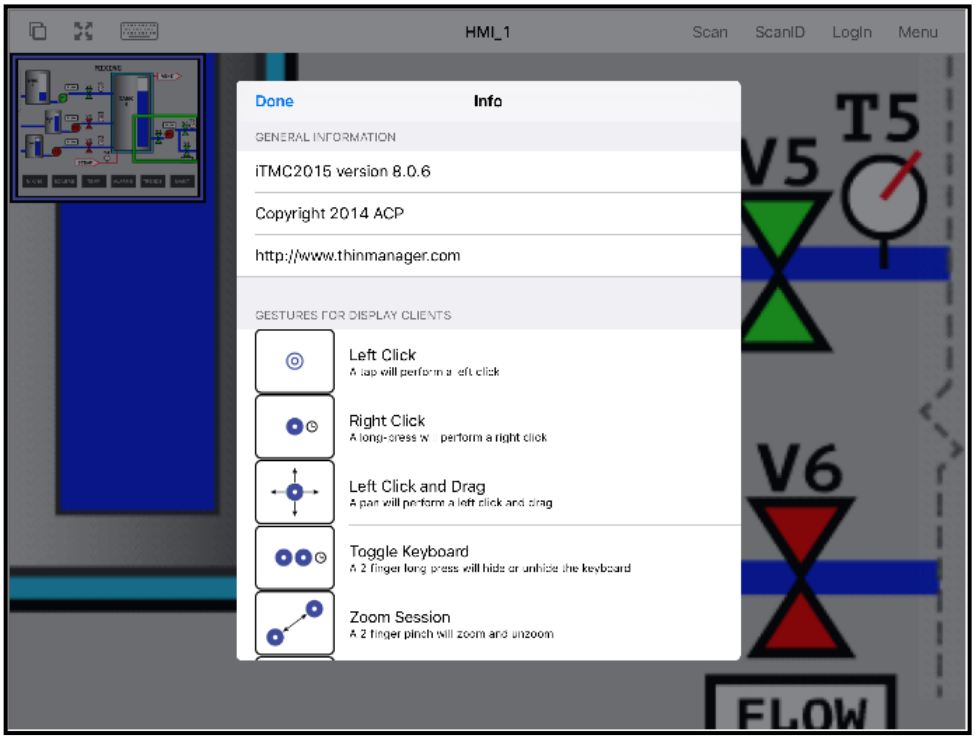
Pinch Zoom Gesture

The iPad program can use multiple figure gestures to control the application. You can zoom in by using two fingers to expand the screen.



Main Menu

The complete list of supported gestures in on the **Info** page. The Info page can be opened by touching the ***Menu*** button in the upper corner to launch the **Main Menu**.



Info Page of the iPad Program

Touching the ***Info*** link on the **Main Menu** will launch the list of gestures.

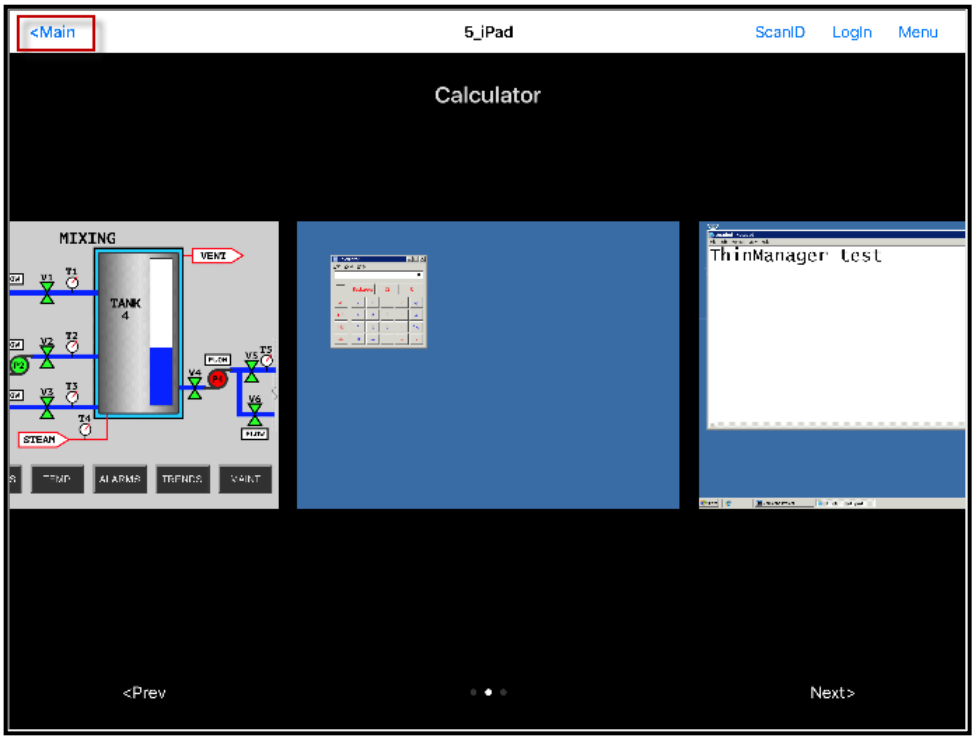
Gestures

- ***Left Click –*** A tap performs a left click.
- ***Right Click –*** A long press performs a right click.
- ***Left Click and Drag –*** This will pan in the session.
- ***Toggle Keyboard –*** A two finger long press will hide or unhide the keyboard.
- ***Zoom Session –*** A two finger pinch will zoom and unzoom.
- ***Pan Session –*** A two finger pan will allow you to pan while zoomed in.
- ***Toggle Menu Bar –*** A three finger long press will hide or unhide the top menu bar.
- ***Next Display Client –*** A three finger swipe left will move you to the next display client.
- ***Previous Display Client –*** A three finger swipe right will move you to the previous display client.

Note: If your three finger commands do not work, go into ***Settings>General>Accessibility*** and turn off the ***Zoom*** feature.

21.1.4. Closing the iTMC App

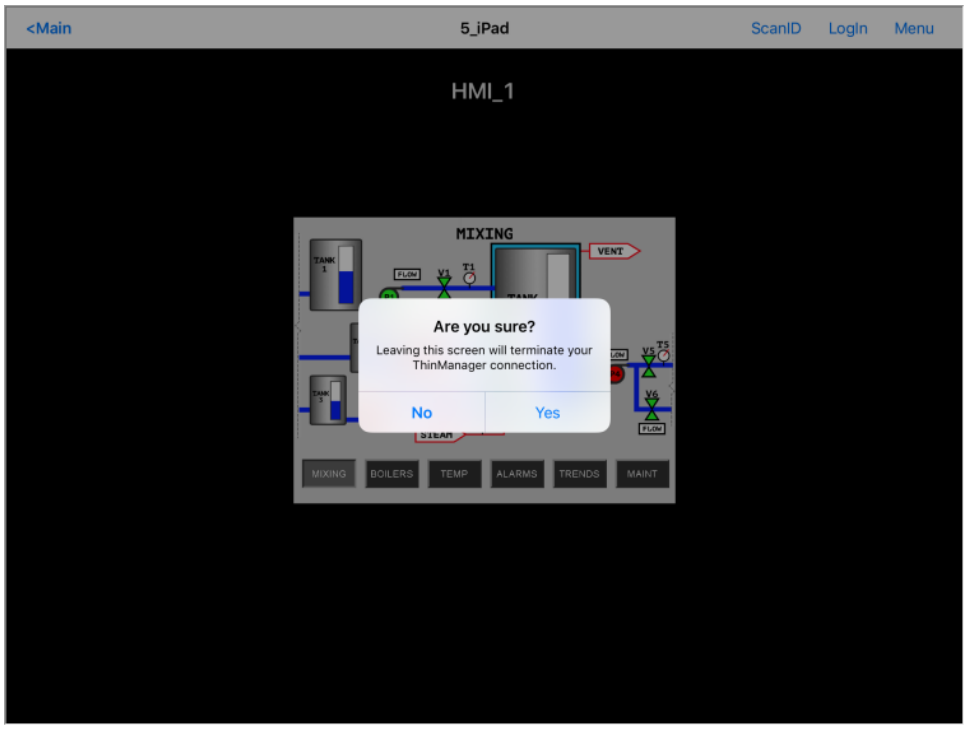
The iTMC app can be closed my double clicking the home button and swiping the app away or by returning to the Main Menu.



Multiple Display Clients

The ***Main*** menu button is displayed when the display clients are minimized.

Touching the ***Main*** button will open a dialog to prompt for closing.



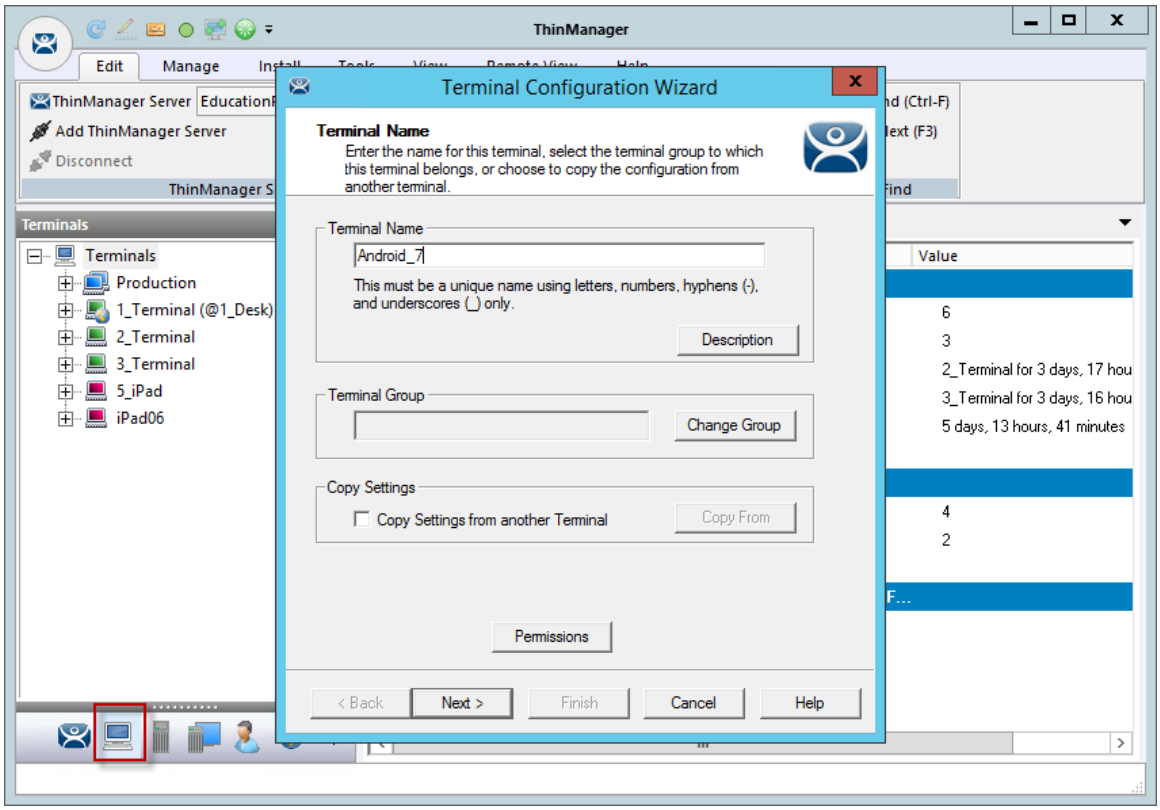
Close Application Dialog

If you select ***Yes*** when prompted the iTMC connection will close and you will return to the **Main Menu** screen.

21.2. Configuring an Android Device in ThinManager

A configuration needs to be created in ThinManager so that the mobile device can join the system as a Terminal.

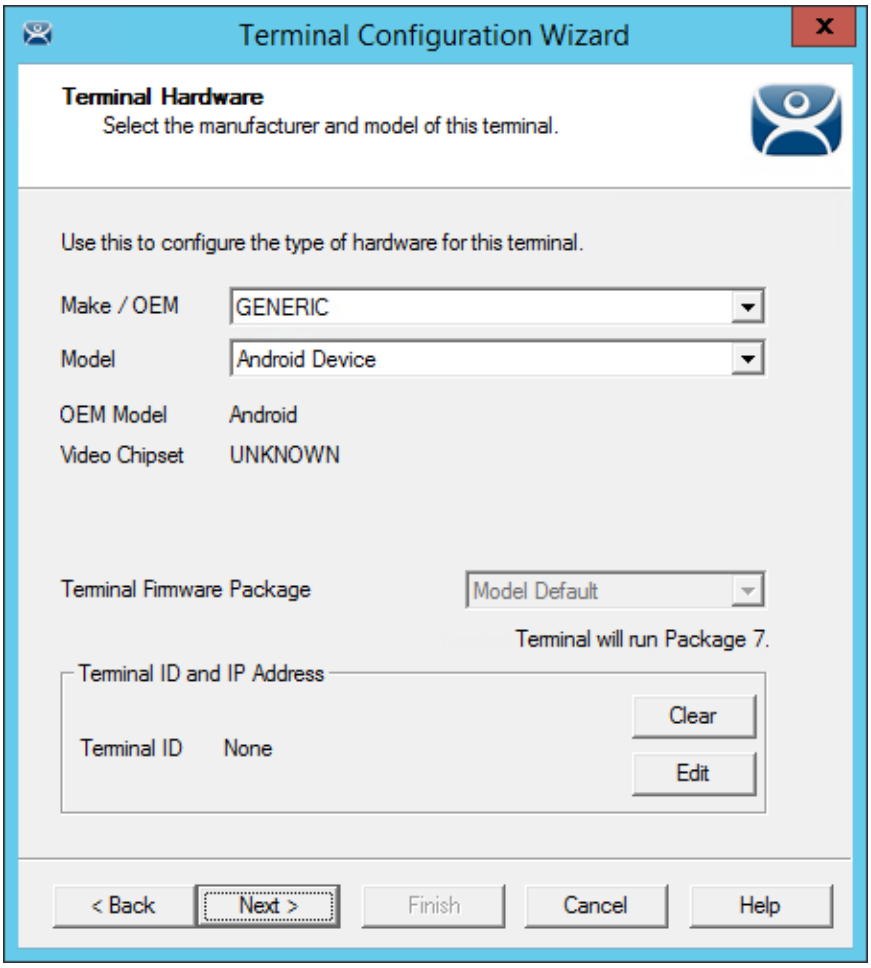
Open ThinManager and select the **Terminal** icon to show the Terminal branch of the tree.



ThinManager Terminal Configuration Wizard

Right click on the Terminals branch and select ***Add Terminal*** to launch the **Terminal Configuration wizard**.

Enter the name for your mobile device and select ***Next***.



Terminal Hardware Page

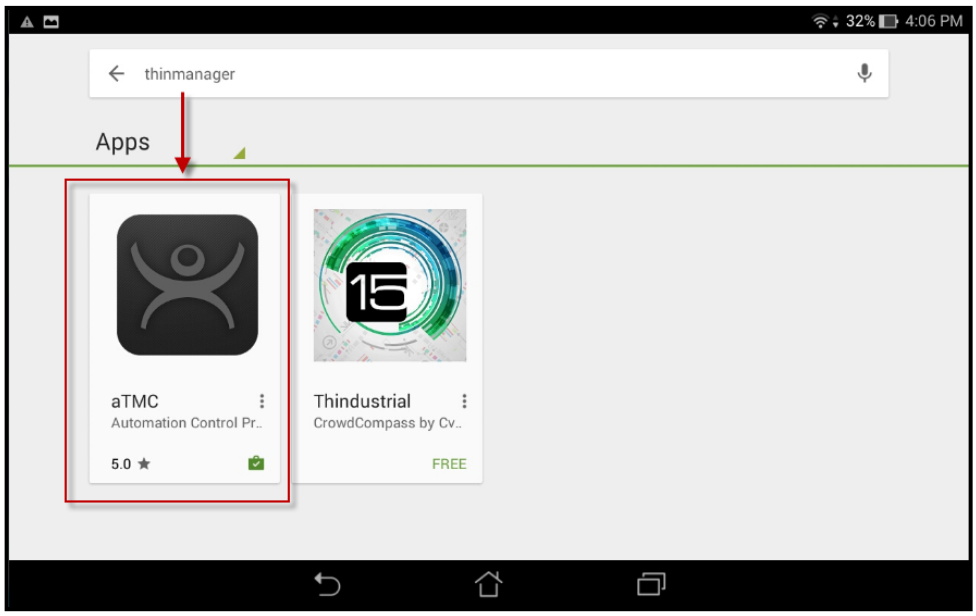
Select ***Generic / Android Device*** for the make and model of hardware.

Navigate to the **Terminal Mode Selection** page by clicking ***Next***.

Complete the wizard as you would for any other thin client.

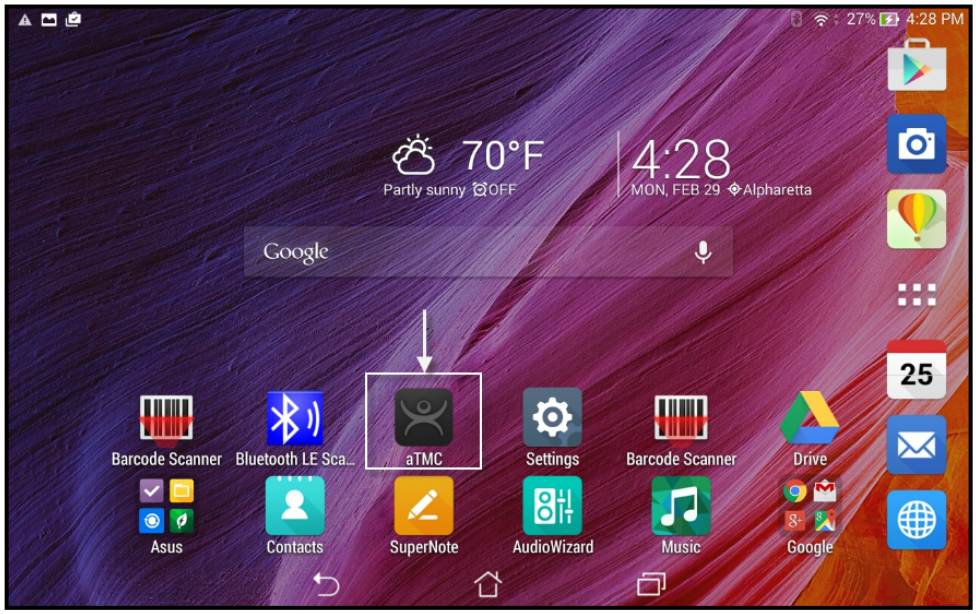
21.2.1. Configuring an Android for ThinManager

The Android device needs to have the aTMC client installed. The aTMC application is a free download from the Google Play store.



aTMC at the Google Play Store

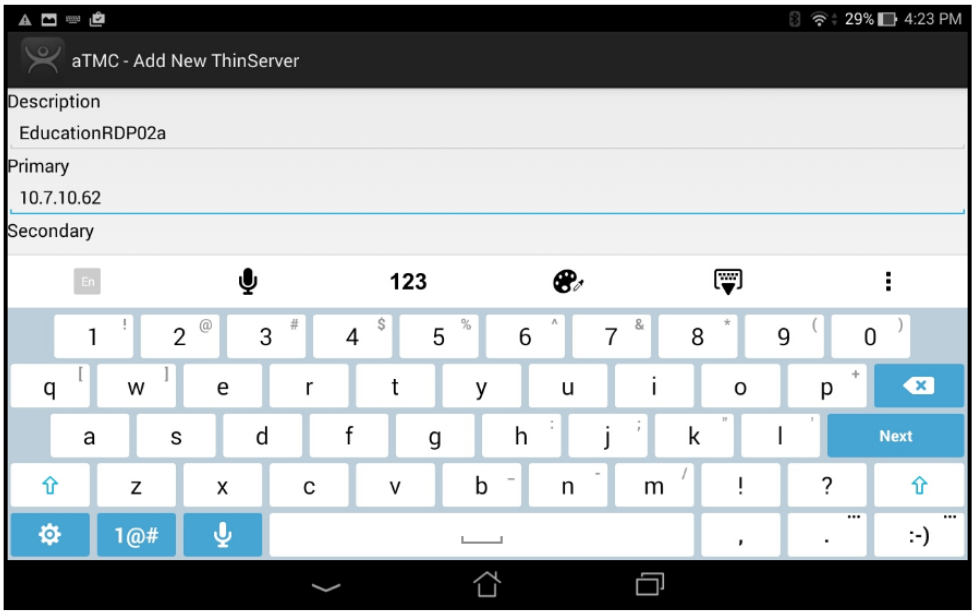
Search for ThinManager and select the aTMC application.



aTMC Application on an Android Desktop

The aTMC program is launched from an icon on the desktop.

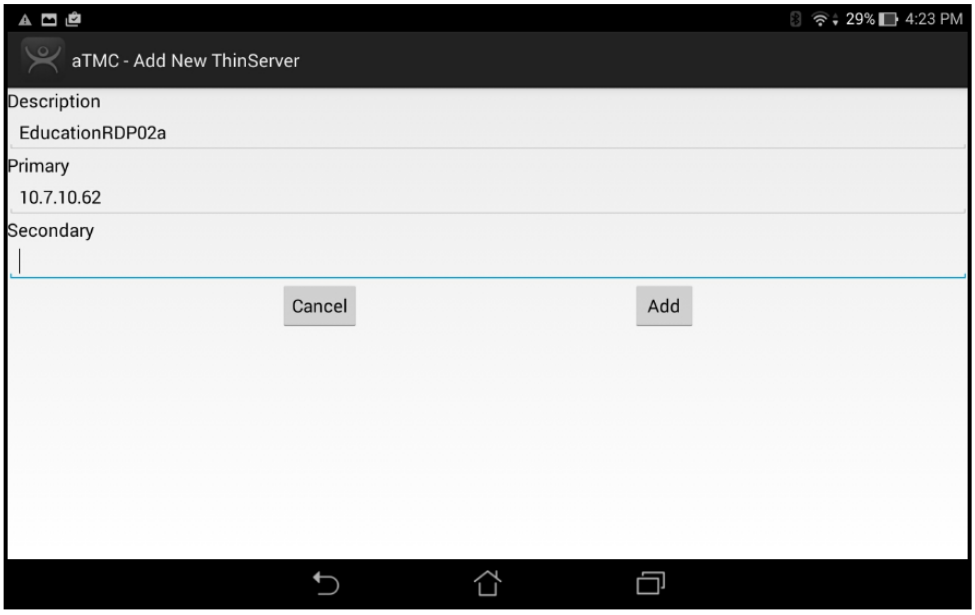
The first action will be to define the ThinManager Server.



Add New ThinServer Window

The **Add New ThinServer** window will launch with fields for the ThinManager Server name and IP address.

Enter the **ThinManager** in the Description field and the IP address of the Primary and Secondary ThinManager Server in the ***Primary*** and ***Secondary*** address field and select ***Done***. If you have only one ThinManager Server you will need to select the ***Next*** button to cycle to the ***Done*** button.

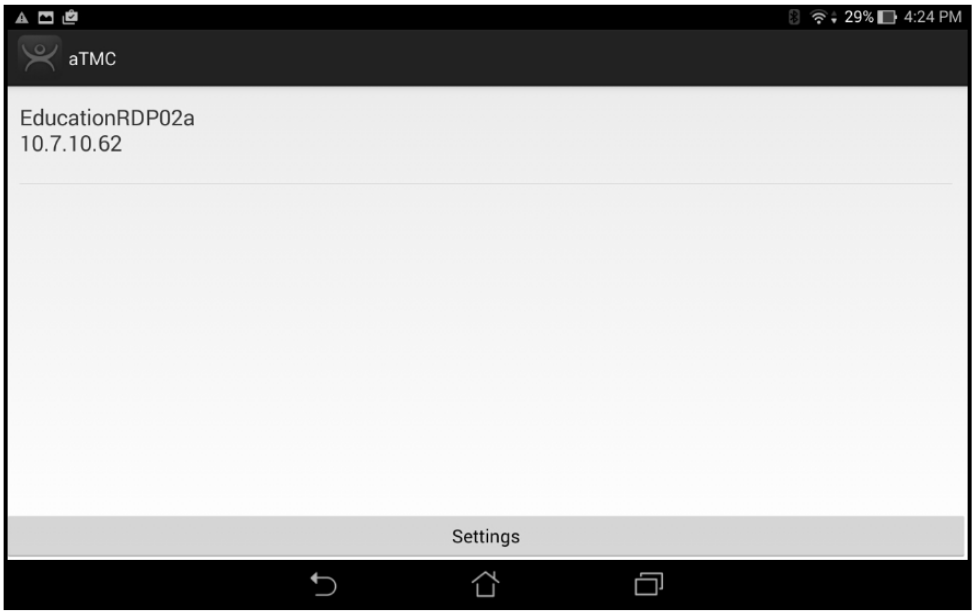


Add ThinManager Server Window

Select the ***Add*** button and the aTMC app has your ThinManager Server listed.

21.2.2. Associating the Android Device to the Configuration

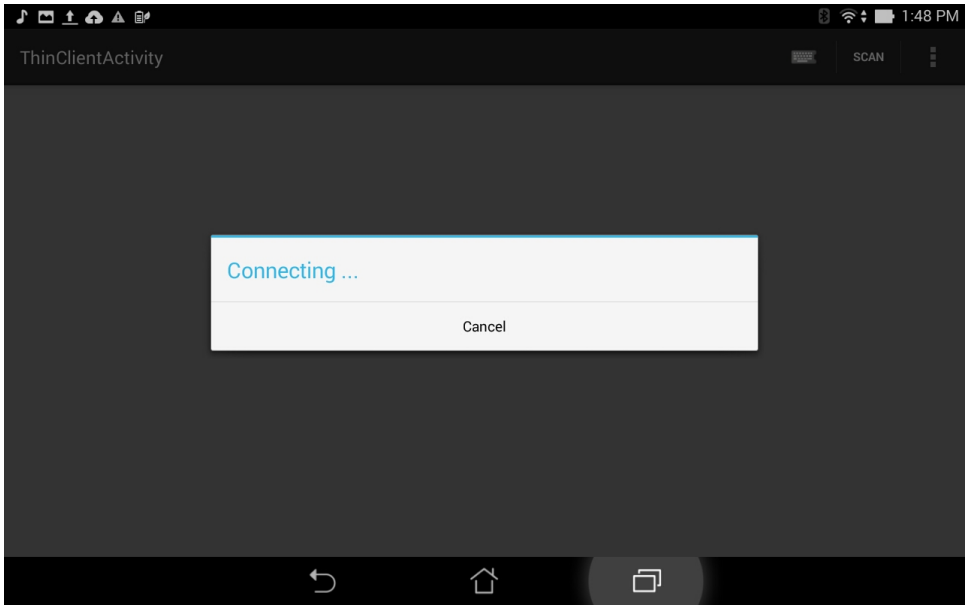
Once the ThinManager Server is defined on the tablet you need to associate the hardware to the aTMC configuration you created.



aTMC Start Screen

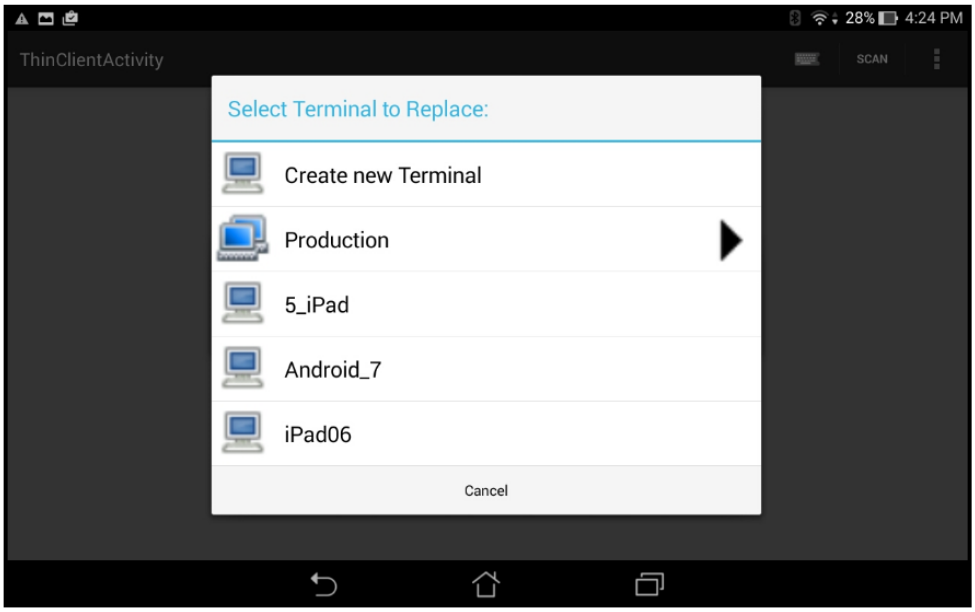
The aTMC Start Screen will show the registered ThinManager Server.

Touch the ThinManager Server to connect.



Connecting Status

The aTMC will connect to the ThinManager Server.

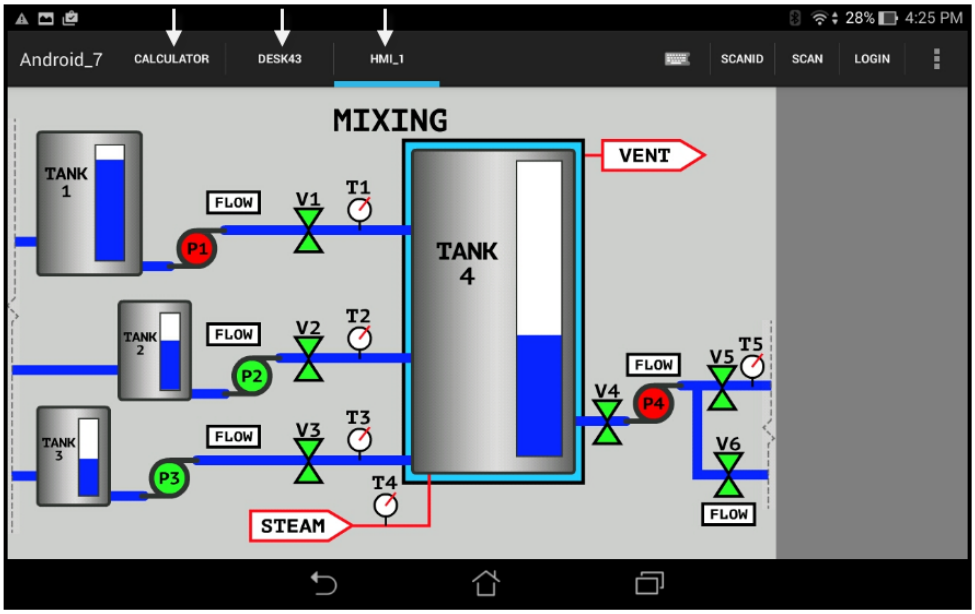


Select a Terminal to Replace

Once the aTMC had connected to the ThinManager Server you will get the **Select a Terminal to Replace** window.

You may choose an existing Terminal configuration or you may choose ***Create New Terminal***.

If you choose ***Create New Terminal*** then a Terminal Configuration Wizard will launch on the ThinManager Server that will let you configure the aTMC as a new Terminal.



aTMC Client

Once connected the Android device will display the applications assigned in ThinManager.

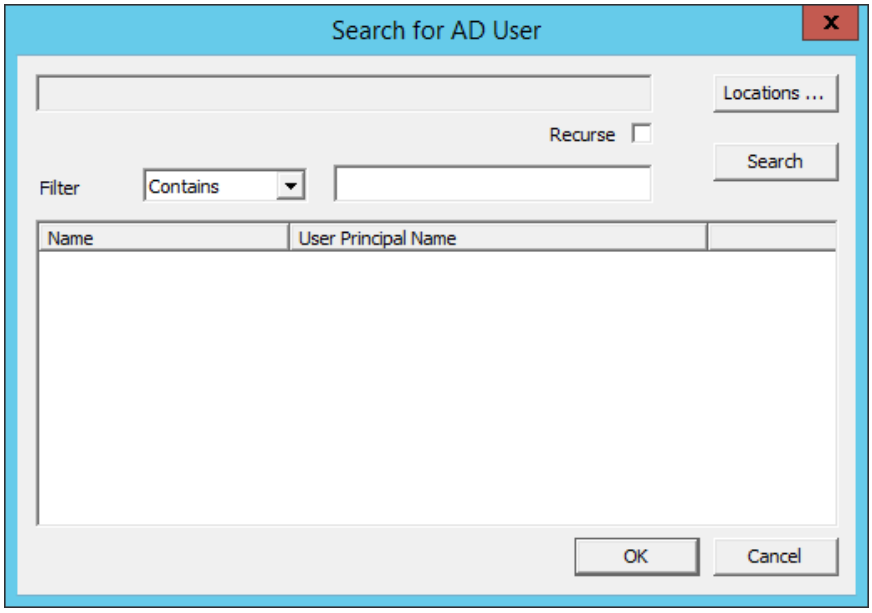
If the Android client is using MultiSession then the display clients will be shown on tabs at the top of the screen.

22. Users - Active Directory User Login Account

A ThinManager Server in a domain may pull an Active Directory account into the ***Username*** field using the ***Search*** button. This launches a series of windows that allow you to select a domain user account for the Terminal login account.

The method is the same on Display Servers, Terminals, and Relevance Users.

Selecting the ***Search*** button will launch a **Search for AD User** window that allows you to select an Active Directory user.



Search for AD User Window

The **Search for AD User** window has a ***Location*** button that allows you to search the Active Directory locations.

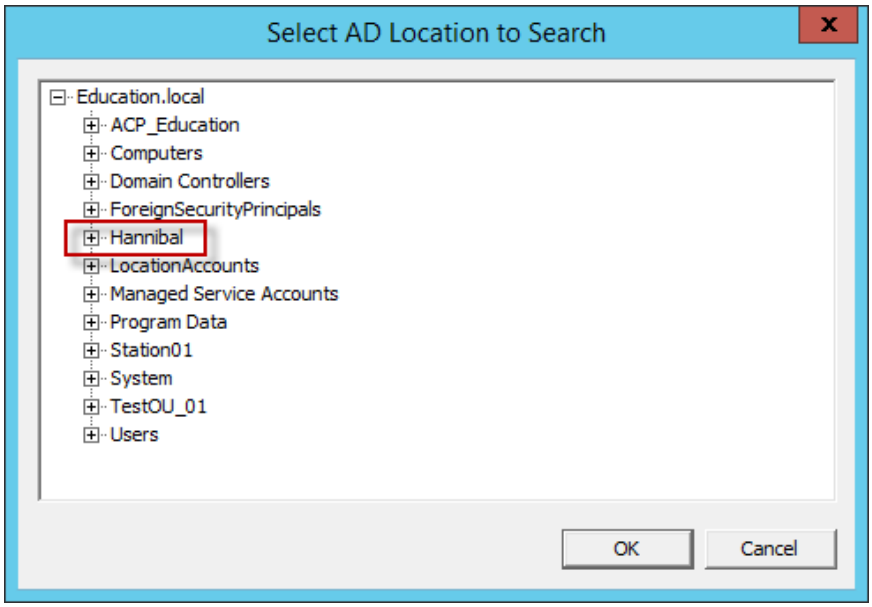
Buttons:

- ***Locations*** – This opens the **Select AD Location to Search** window to select the Organizational Unit (OU) to search.
- ***Search*** – This searches the selected OU and populates the ***Name*** field with the OU members.

Options:

- ***Filter*** – This drop-down will filter the results with either the ***Contains*** or ***Starts With*** function and the entry of the textbox.
- ***Recurse*** – This sets the ***Search*** function to search nested Windows Security Groups when searching a Windows Security Group. The ***Choose AD Synchronization Mode*** needs to be set to **Security Group** on the **Active Directory System Settings** window to work. This window is opened from ***Manage > Active Directory > Settings***.

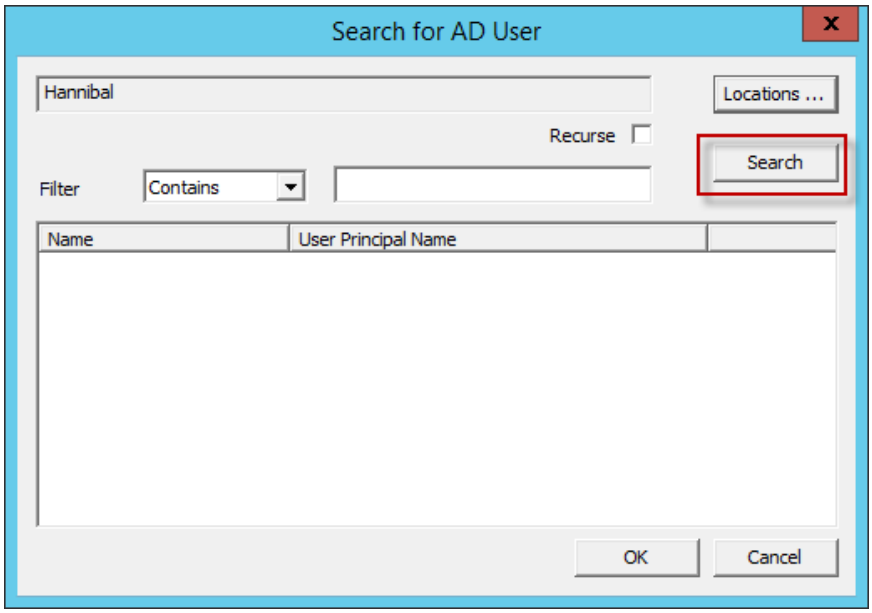
Select the ***Locations…*** button to launch the **Select AD Location to Search** window.



Select AD Location to Search Window

Continue with the wizard by selecting the branch of the Active Directory tree that contains your administrative user account.

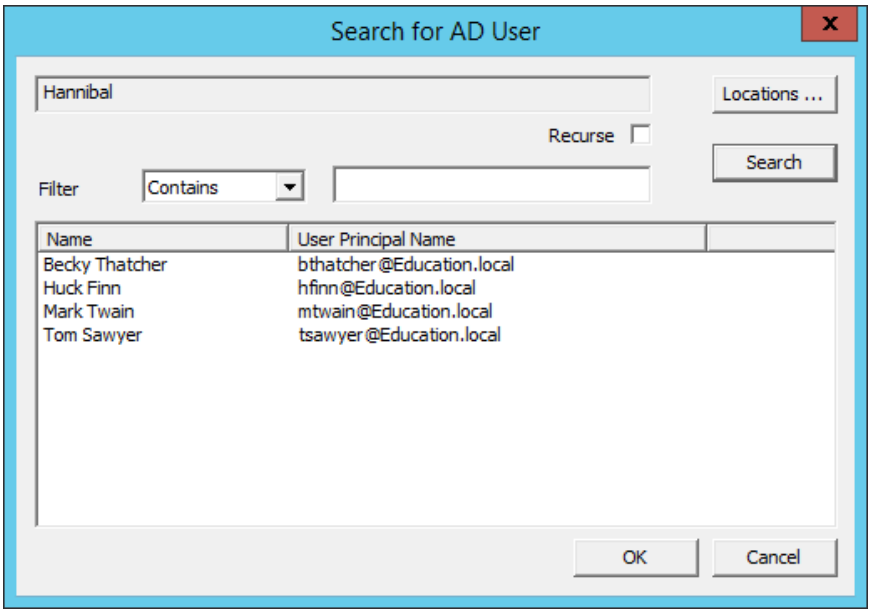
Highlight it and select the ***OK*** button.



Search Organizational Unit

Once you select an organizational unit and select the OK button the OU will be listed as the location.

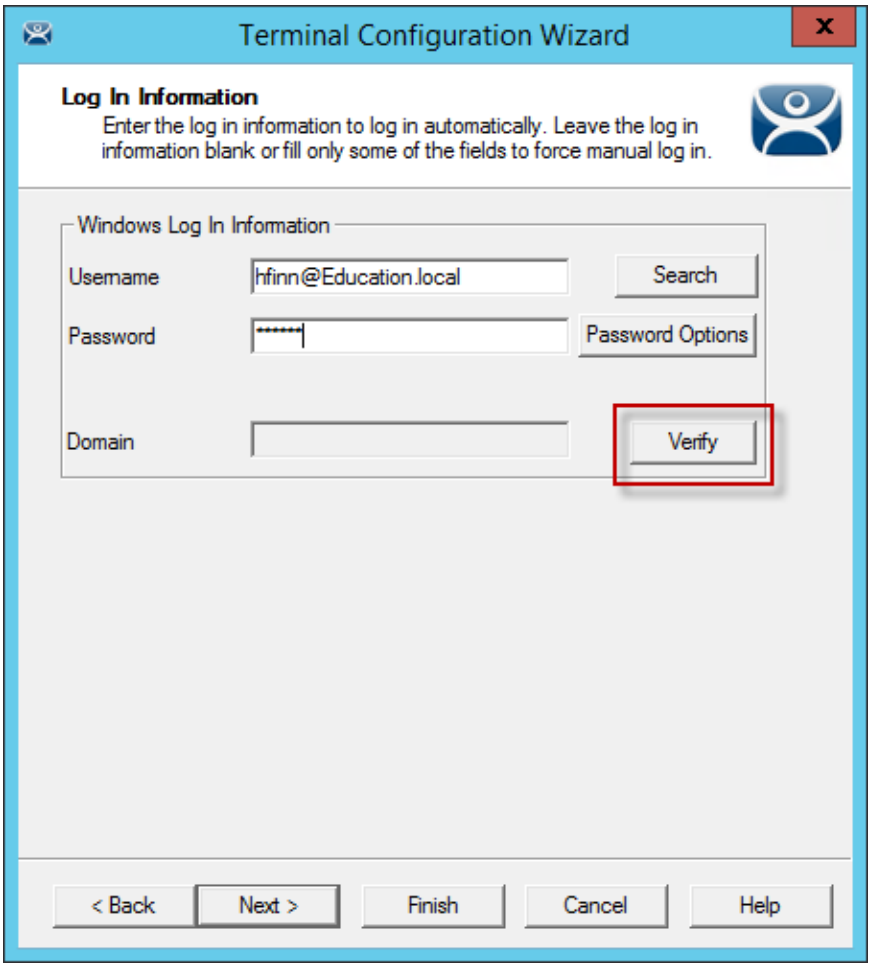
Select the Search button to populate with the users.



Search for AD User Window

Highlighting an Active Directory branch in the **Select AD Location to Search** window and selecting the ***OK*** button will re-open the **Search for AD User** window with the list of domain users from that branch.

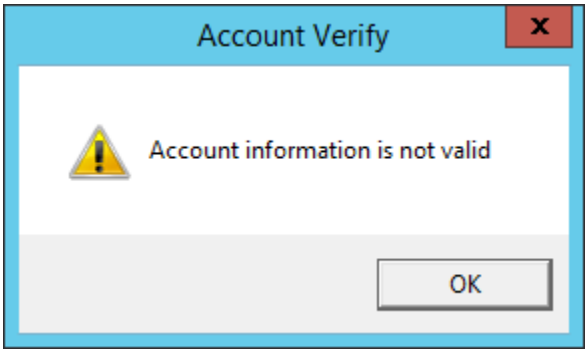
Highlight the desired user and select ***OK***. This will add the domain user to the ***Username*** field of the Terminal Configuration Wizard.



Remote Desktop Server Name - Remote Desktop Server Wizard –Domain

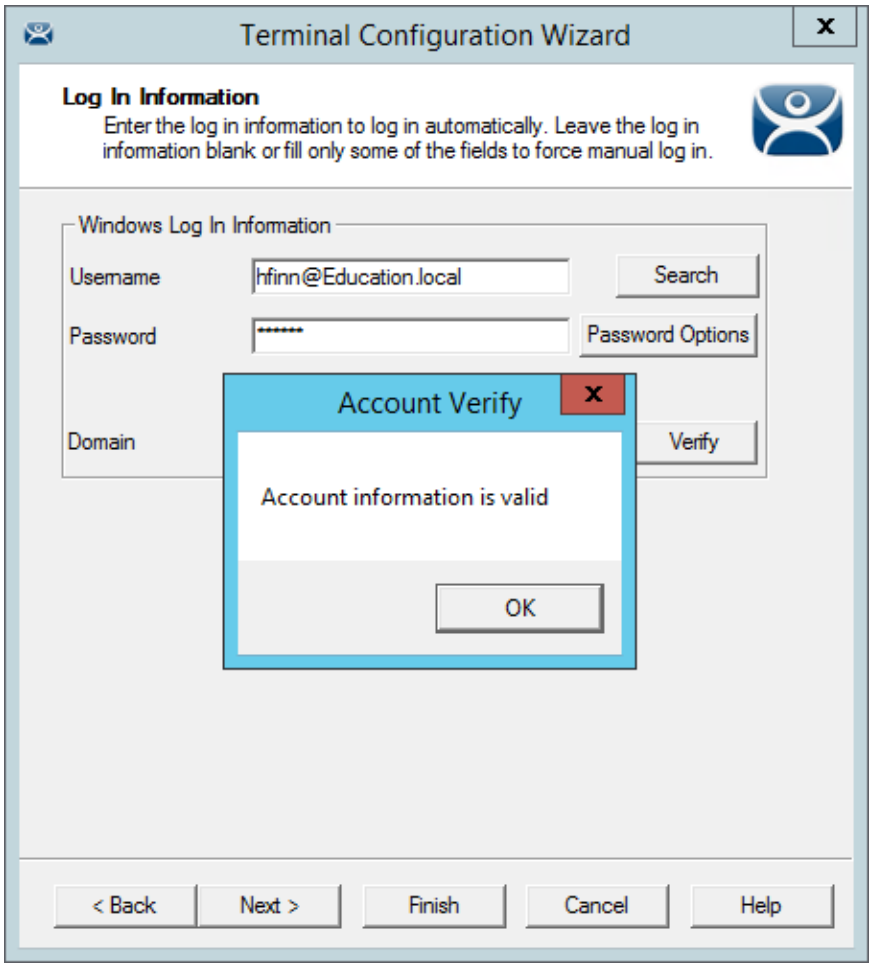
Once the domain user is in the ***User Name*** field you need to add the correct password to the ***Password*** field.

The ***Verify*** button will check the entered password and tell you if it is valid or incorrect. Once you have received a positive result select the ***Next*** button to continue with the wizard.



Invalid Account Message

If you receive a message of an invalid account try the correct password.



Valid Password Message

Once you have a valid user account select the ***Next*** button to continue the configuration wizard.

23. Packages

23.1. Firmware, Packages and Modules

Firmware is the basic operating system that the thin clients run. It is downloaded and expanded into memory where it serves as an operation system.

Modules are additional functions that a thin client may use. These include touch screens, keyboard modules, and sound modules.

Packages contain a version of firmware and the modules that belong with it.

In the past ThinManager made all of the firmware changes backwards compatible so that a 12 year old x86 thin client could run the same firmware as the latest model of thin client. This limited what ThinManager could do to take advantage of new hardware.

ThinManager 6.0 introduced a new approach to firmware and modules called **Packages**. ThinManager has the ability to run different versions of the firmware on different thin clients. Legacy thin clients can run **Package 5** that is equal to the ThinManager 5 firmware while newer thin clients can run **Package 6** and later. As new hardware is released you will be able to run even newer packages to take advantage of new features.

A package, the firmware version and the modules that go with it, can get assigned to by default to a thin client, or you can override the setting and run a different package.

This will be particularly helpful in validated systems. If new hardware is purchased that requires a new firmware you can assign a new package to the new hardware while the existing thin clients can continue to run the original validated package.

Packages, firmware, and modules are included with ThinManager and are registered automatically during ThinManager installation and service package updates. Packages may be updated occasionally and can be downloaded from the ThinManager web site at http://downloads.thinmanager.com/ and applied to ThinManager.

23.1.1. Updating Packages and Files

ThinManager allows the updating of Packages. You can also update just the firmware or specific modules if needed.

Note: These get updated automatically during Service Pack upgrades. This shows how to do it without updating with a Service Pack.

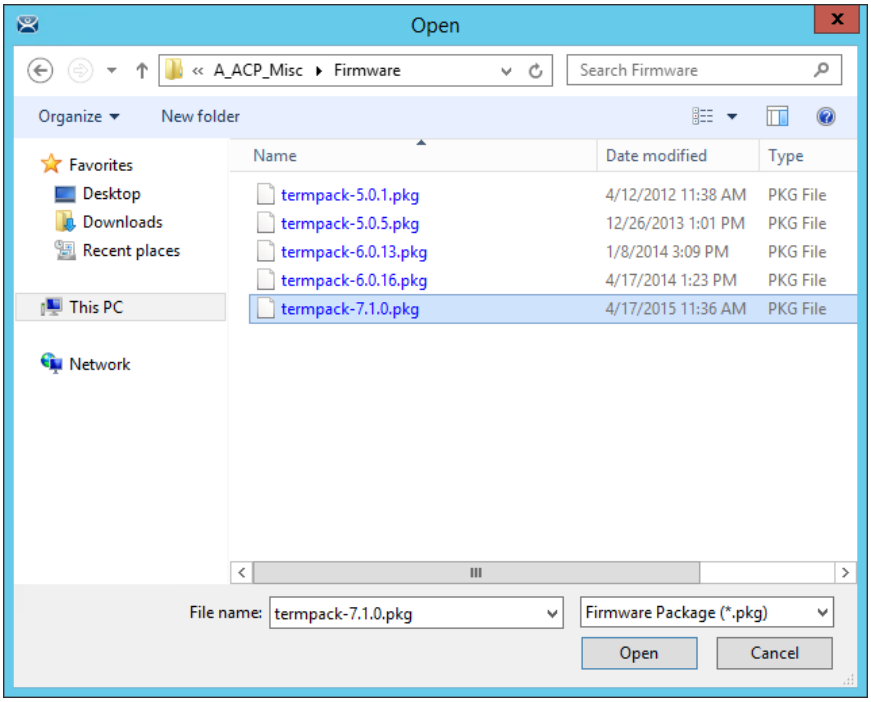
- New components can be downloaded from the ThinManager web site at http://downloads.thinmanager.com/ .
- ***Install > Firmware Package*** will launch a file browser and allow you to install a ***.pkg** file.
- ***Install > Firmware*** will launch a file browser and allow you to install a ***.fw** file. You also use this command to load a new version of the legacy **firmware.acp** firmware file
- ***Install > Module*** will launch a file browser and allow you to install a ***.mod** file.

ThinManager uses a Boot Loader and a Chain Loader during PXE boot.

- ***Install > Boot Loader*** will launch a file browser and allow you to install a ***.bin** file.
- ***Install > Chain Loader*** will launch a file browser and allow you to install a ***.bin** file.

ThinManager uses a Terminal Capabilities Database, or TermCap, to aid in configuring the thin clients.

- ***Install > TermCap Database*** will launch a file browser and allow you to install a ***.db** file.

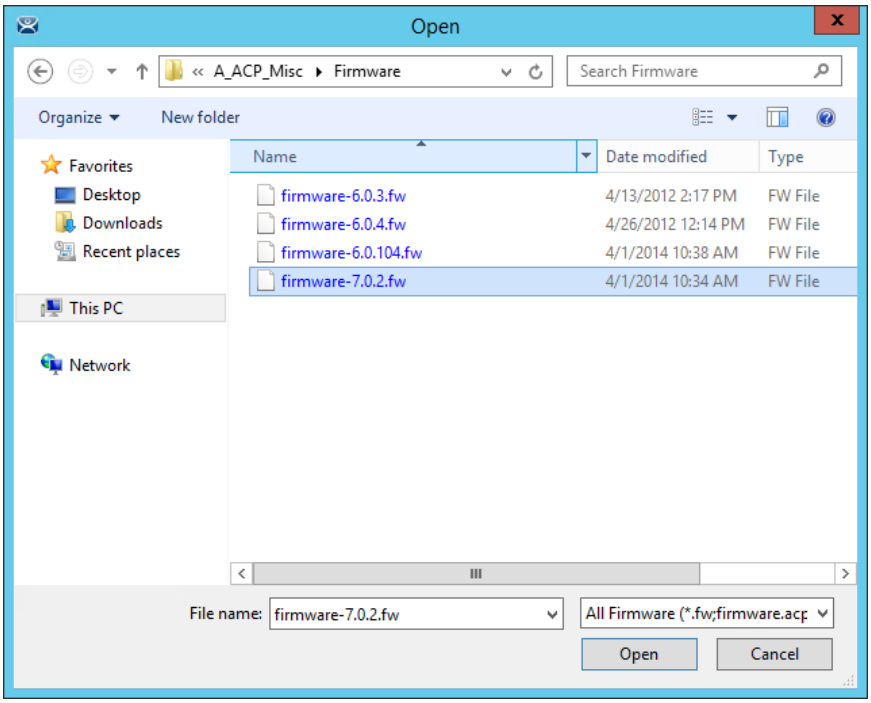


Package Installation

Install > Firmware Package will launch a file browser and allow you to install a ***.pkg** file.

This picture shows a folder with three firmware packages, **v.5**, **v. 6**, and **v 7**.

Highlight the desired firmware package and select the ***Open*** button.

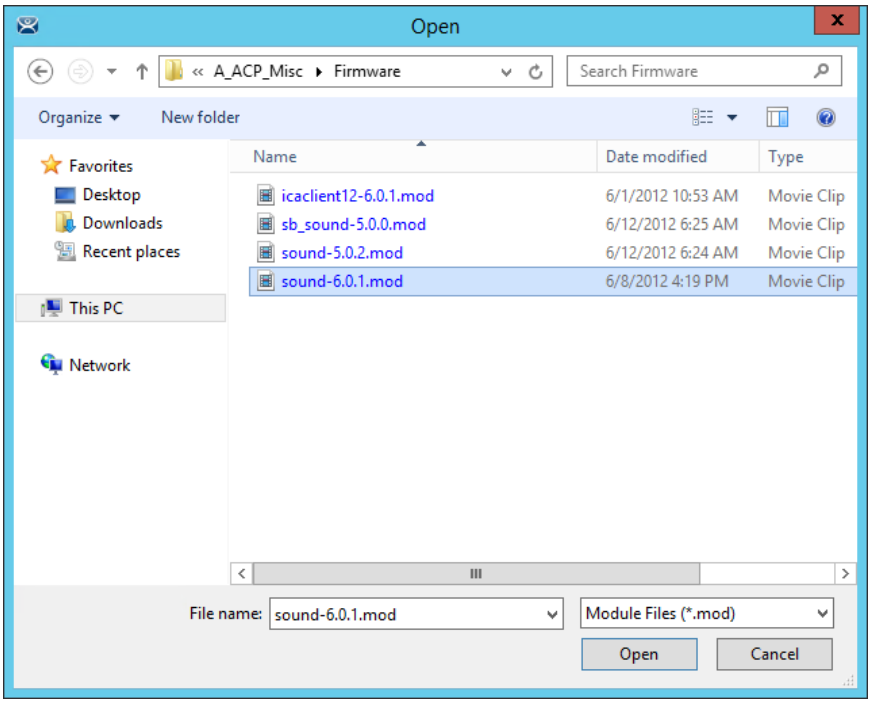


Firmware Installation

Install > Firmware will launch a file browser and allow you to install a ***.fw** file. You also use this command to load a new version of the legacy **firmware.acp** firmware file

This picture shows a folder with several versions of firmware.

Highlight the desired firmware and select the ***Open*** button.



Module Installation

Install > Module will launch a file browser and allow you to install a ***.mod** file.

This picture shows a folder with two sound modules.

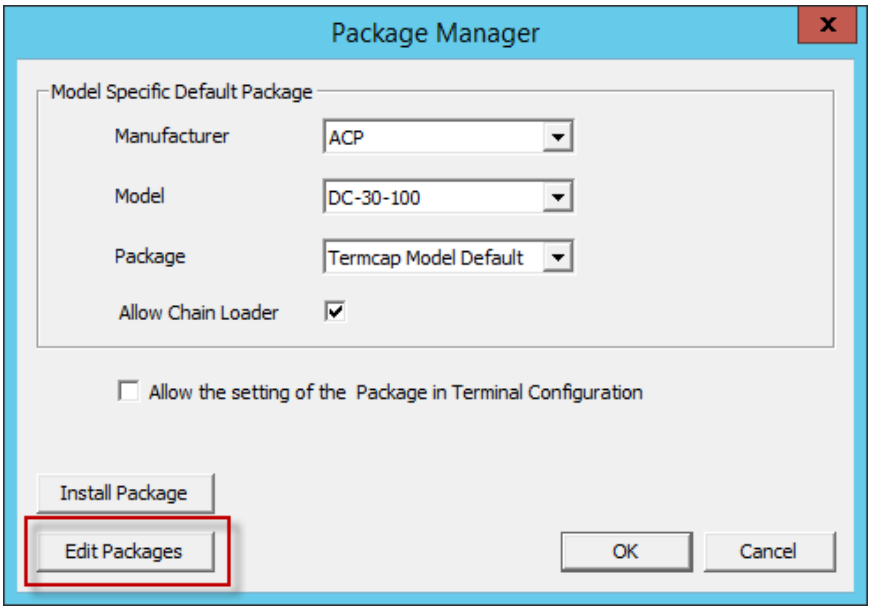
Highlight the desired module and select the ***Open*** button.

23.1.2. Customizing Packages

ThinManager allows you to run different packages on different models or individual Terminals. You can modify a package by copying it and making changes to it.

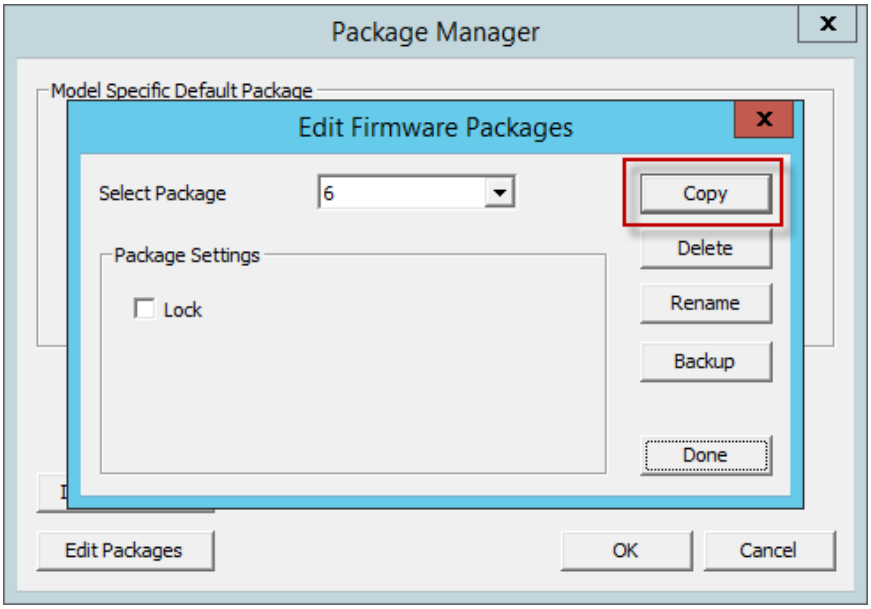
Modules and packages are normally updated with service packs and releases. You can download updated modules at http://downloads.thinmanager.com/ when needed.

Open the **Package Manager** by selecting ***Manage > Packages***.



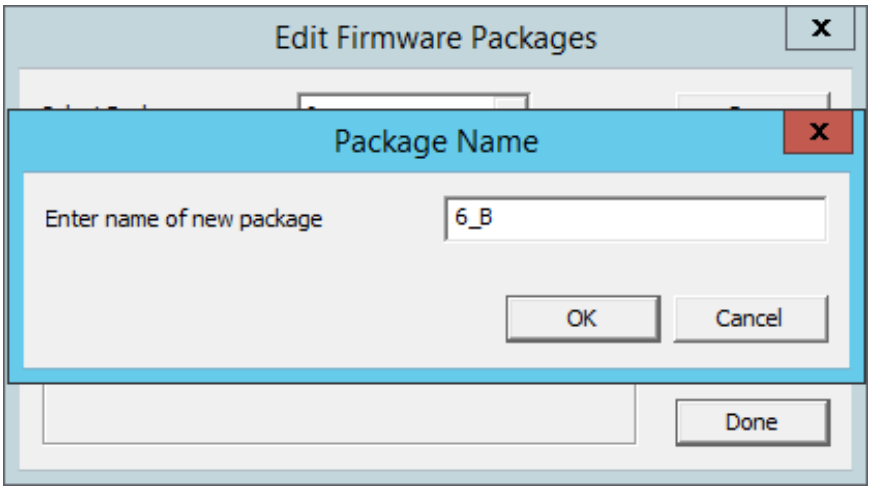
Package Manager Window

Select the ***Edit Packages*** button to launch the **Edit Firmware Package** window.



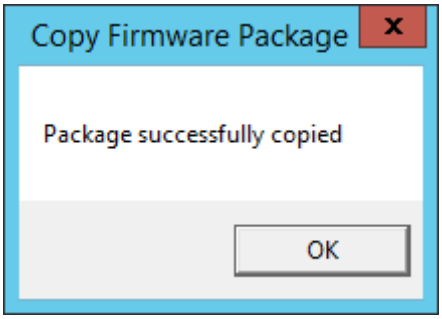
Edit Firmware Packages Window

Select the package you want to modify in the ***Select Package*** window and select the ***Copy*** button to make a copy.



New Package Name Window

Enter a name for the new package in the ***Enter name of new package*** field.

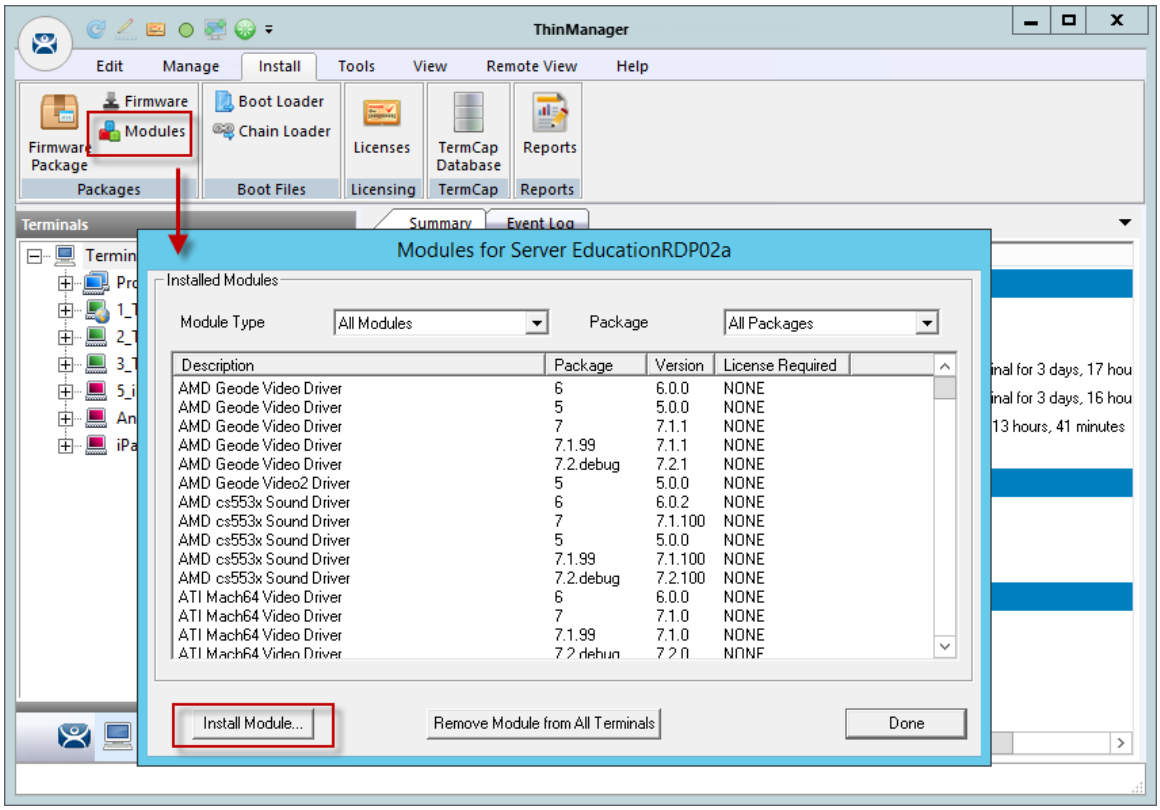


Success Dialog

Success will be confirmed with a dialog.

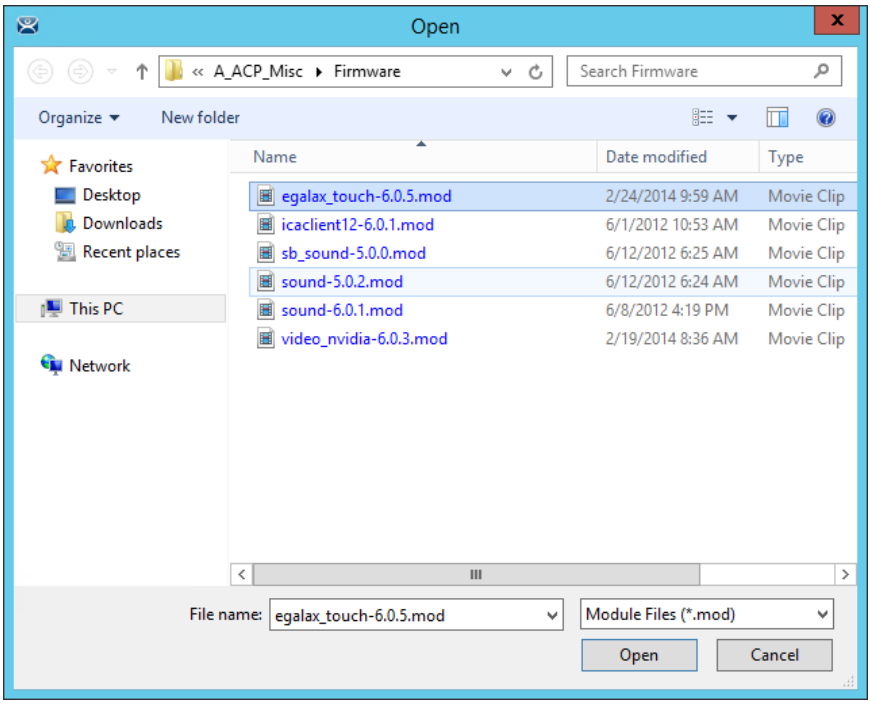
Close the **Edit Firmware Packages** and **Package Manager** windows.

Open the Modules window by selecting ***Install > Modules*** from the ThinManager menu bar.



Modules Window

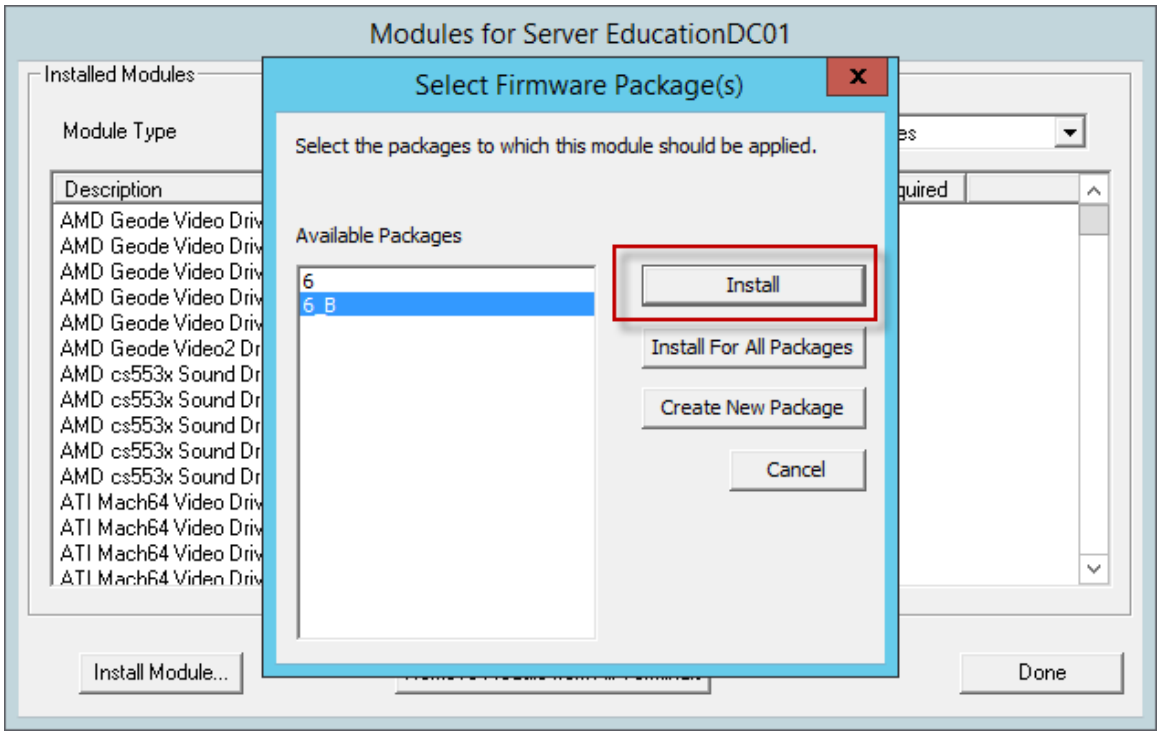
Select the ***Install Modules*** button on the **Modules** window. This will open a file browser.



File Browser

Use the file browser to navigate to your downloaded modules.

Select the needed module and select the ***Open*** button. This will launch a dialog box.

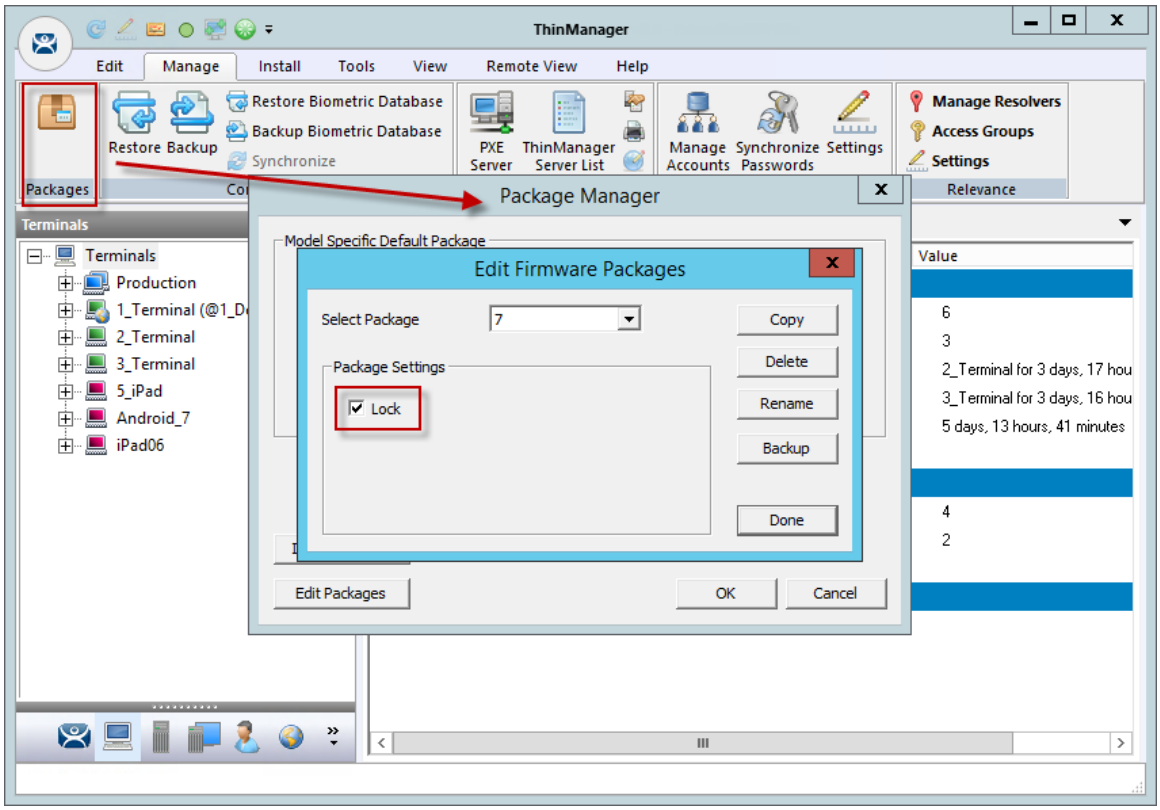


Select Firmware Package Window

A **Select Firmware Package** window will be displayed that allows the selection of which package you want to add the module.

Highlight your copied module and click the ***Selected Packages*** button. This will add the new module to that package.

Close the **Modules** window to finish.



Edit Firmware Packages Window

You can lock a package on the **Edit Firmware Packages** window.

Open the **Package Manager** Window by selecting ***Manage > Packages*** on the ThinManager menu bar.

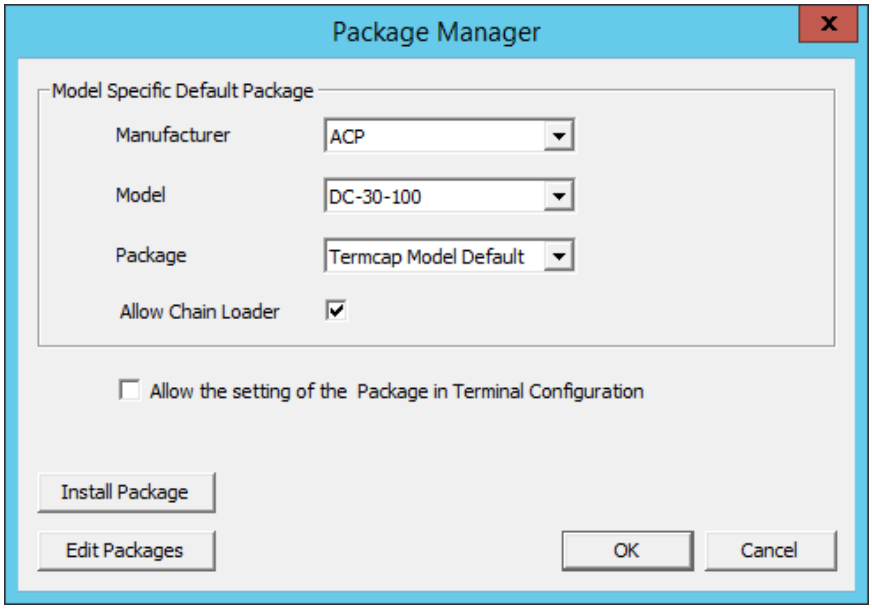
Select the ***Edit Packages*** button on the **Package Manager** window to launch the **Edit Firmware Packages** window.

Highlight the package in the ***Select Package*** drop-down and select the ***Lock*** checkbox. This will lock the package.

23.2. Configuring Packages for a Model of Thin Client

ThinManager allows you to change the package for all units of a make and model.

Select ***Manage > Packages*** to launch the Package Manager window.



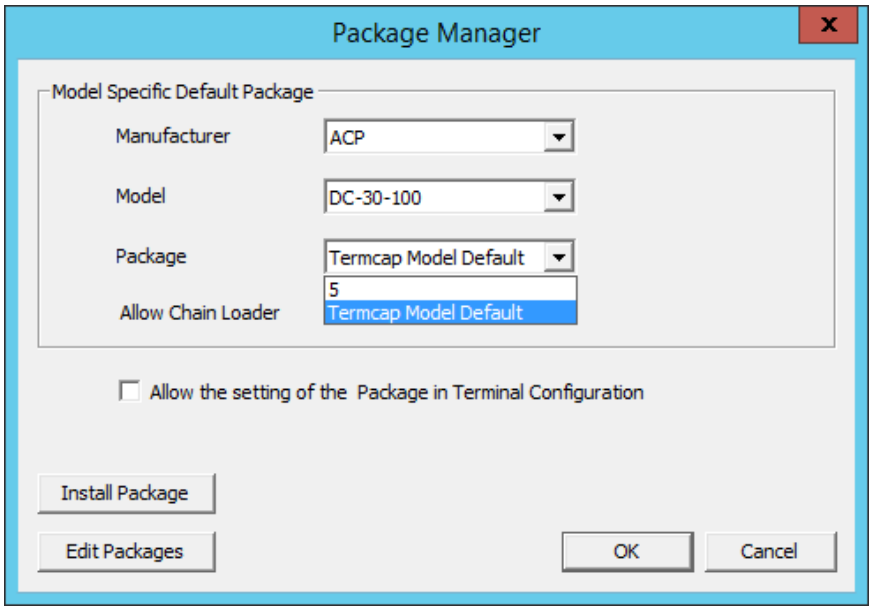
Package Manager

Select your ***Manufacturer*** and ***Model*** in the drop-downs.

Set the package version you want in the ***Package*** drop-down. This becomes the **Model Default.**

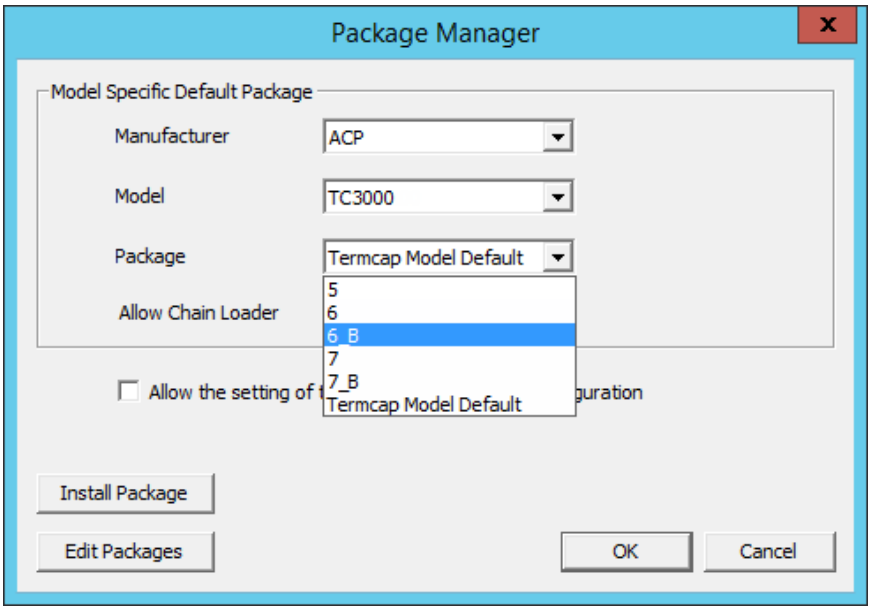
Select ***OK*** to close the **Package Manager** window.

Older Makes and models will have fewer options than newer, more powerful makes and models.



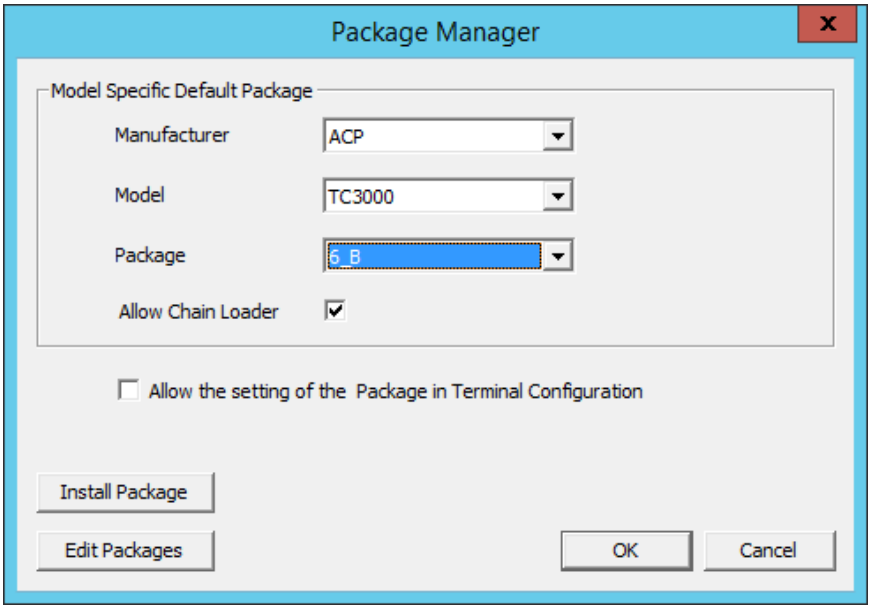
ACP DC-30-100 Firmware

The ancient DC-30-100 can only run package 5. This is set in the TermCap as the default package.



ACP TC3500 Firmware

The more recent ACP TC3000 can run firmware v.5, v.6, v.7, and custom firmware.



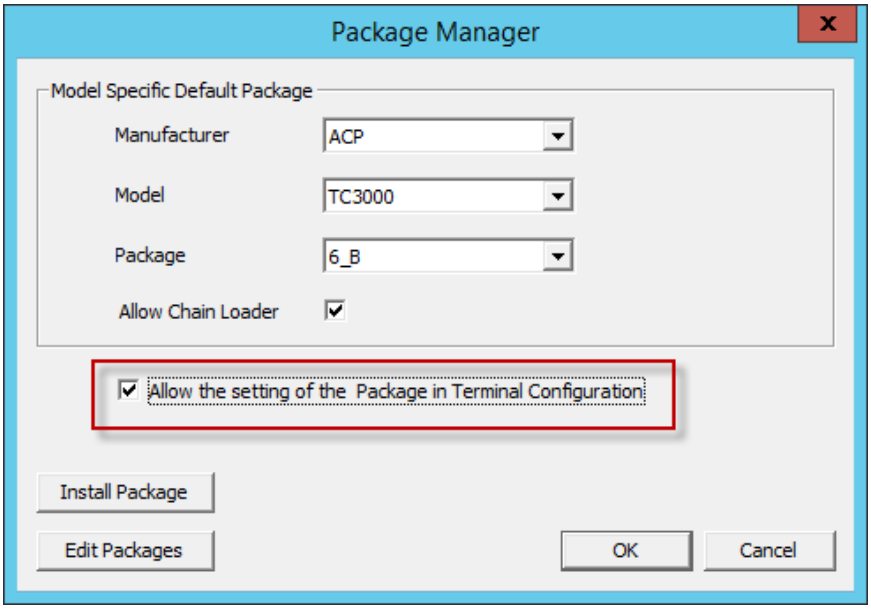
New Default Firmware

Changing the firmware package in the ***Package*** drop-down will set that firmware as the default firmware. Any Terminal of that make and model will run that firmware.

23.3. Configuring Packages for an Individual Thin Client

Packages can be changed for an entire series of thin clients or for an individual thin client. This is done in the **Package Manager** window.

Select ***Manage > Packages*** to launch the **Package Manager** window.



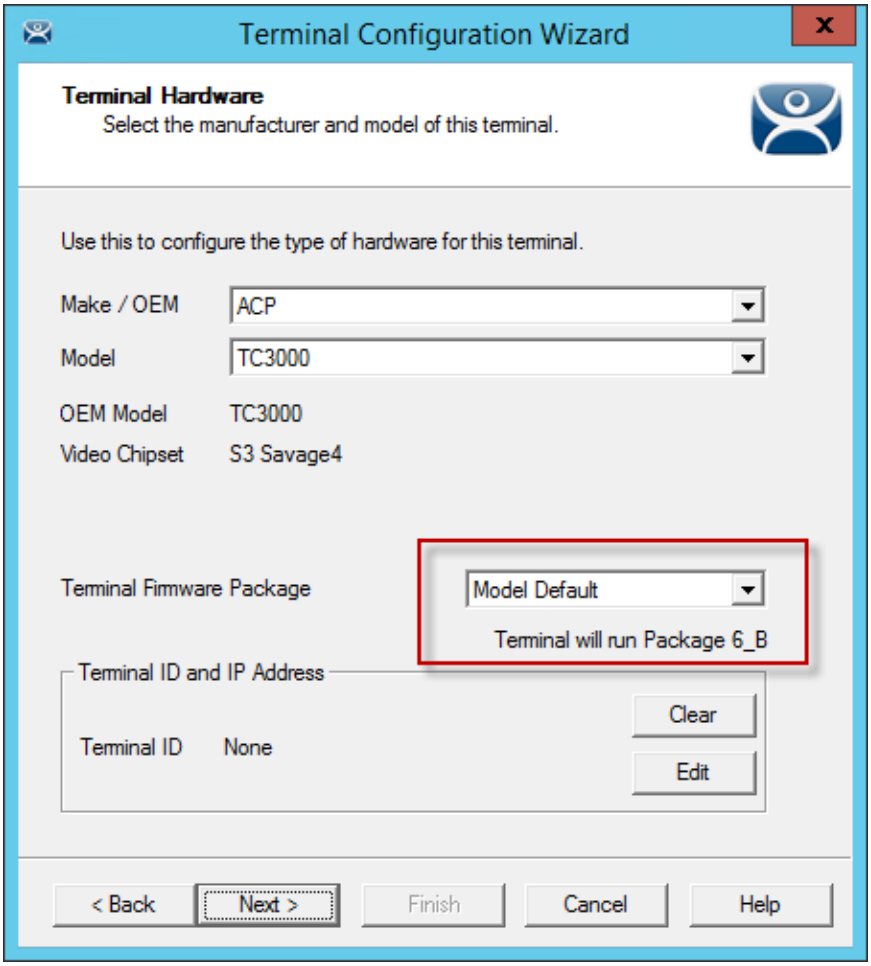
Package Manager

Select the ***Allow the setting of the Package in Terminal Configuration*** checkbox. This allows you to override an individual thin client's package setting.

Select ***OK*** to close the **Package Manager** window.

Open the **Terminal Configuration Wizard** by double clicking on the Terminal in the Terminal branch of the ThinManager tree.

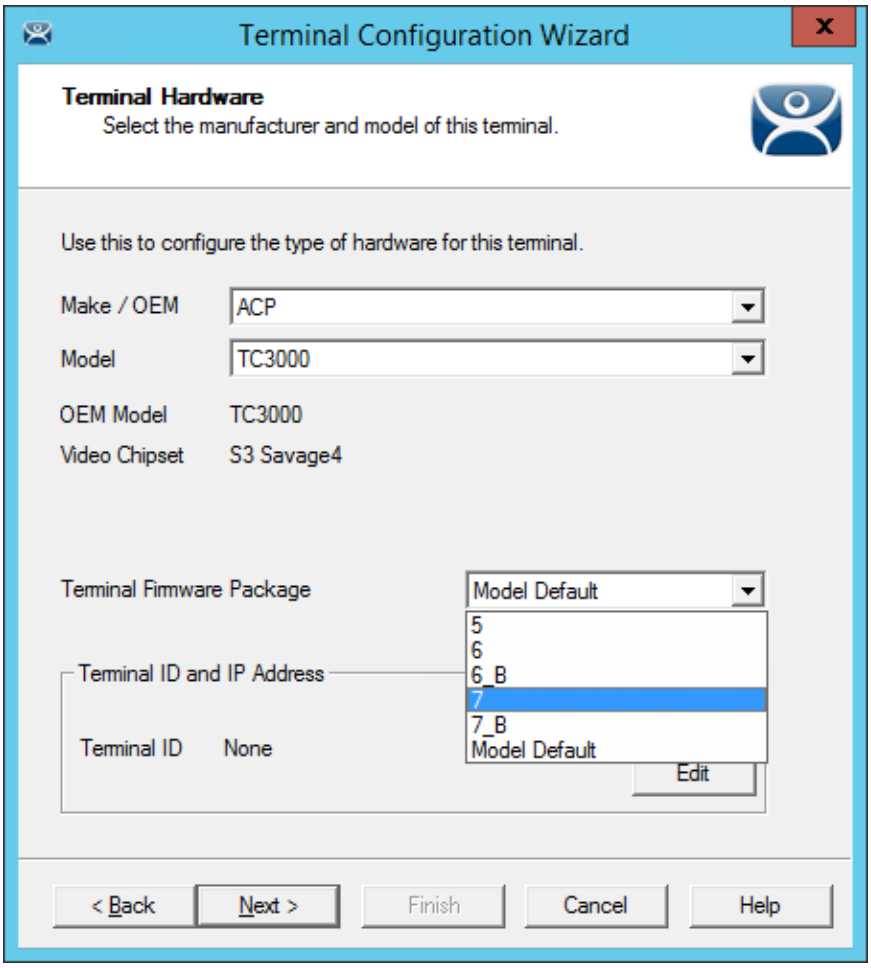
Navigate to the **Terminal Hardware** page.



Terminal Firmware Package Setting

The ***Terminal Firmware Package*** drop-down allows you to pick a different package to run once you allow individual firmware on the Package Manager window.

The current setting shows the **Package 7_b** that was used in the previous example.



New Terminal Firmware Package Setting

Once individual firmware is allowed on the Package Manager window the Terminal Package window the Terminal Firmware Package drop-down becomes active and allows you to select a firmware for that individual Terminal.

Select the ***Terminal Firmware Package*** of your choice.

Select ***Finish*** to close.

Reboot the Terminal by highlighting the Terminal and selecting ***Tools > Reboot*** from the ThinManager Menu.

The Terminal will show the ThinManager splash screen for that firmware during the boot process.

24. Modules

Modules are components and drivers for the Terminals that aren't needed for the basic boot but can be added to enhance the features and functions of the Terminals.

Modules are added to Terminals individually or through Terminal Groups.

ThinManager divides the modules into a number of categories or types to make navigation of the module list easier. Although details on the specific modules will follow, the types and modules include:

Note: Certain modules are used in limited, specific cases and are considered advanced modules. These are marked with a (*). See Advanced Modules for details.

This manual will cover the details of a dozen modules. The first will cover the general steps with the **Key Block Module**. The other modules will cover the individual configuration.

24.1. Module List

ICA - See ICA Modules

- Citrix ICA UseAlternateAddress Module
- Citrix ICA wfclient.ini Extension Module

Keyboard – See Keyboard Modules

- Key Block Module
- Key Block Single Key Module
- Keyboard Configuration Module
- On-Screen Keyboard Configuration Module
- RF Ideas pcProx USB Module
- Share Keyboard and Mouse Master Module
- Share Keyboard and Mouse Slave Module

Language - See Language Modules

- Language Selection Module

Local Storage - See Local Storage Modules

- USB Flash Drive Module
- USB Memory Card Reader Module (Package 5 only)

Miscellaneous - See Miscellaneous Modules

- Add Serial Port
- Bluetooth Module
- Firmware Update Module
- Local Printer Module
- MultiStation Configuration Module
- Redundant Ethernet Module
- Serial to TCP Module
- TermMon ActiveX Configuration
- Time Zone Redirection Module
- TMTerm DLL Configuration Module
- USB to Serial Module
- User Override Module

Mouse - See Mouse Modules

- Locate Pointer Module
- Mouse Configuration
- Serial Mouse Driver
- Share Keyboard and Mouse Master Module
- Share Keyboard and Mouse Slave Module

Network - See Network Modules

- Domain Name System Module
- Second Network Module
- Third Network Module

RDP - See RDP Modules

- RDP Experience Module
- RDP Port Module
- RDP Serial Port Redirection Module
- RDP Session IP Module
- Smart Cart Module

Relevance - See Relevance

- Bluetooth Module
- DigitalPersona UareU Fingerprint Reader
- RF Ideas pcProx Module
- RF Ideas pcProx USB Module
- RF Ideas pcProx Sonar Module
- TermMon ActiveX Configuration Module
- USB Flash Drive Module
- USB ID Reader Module

Screen Saver - See Screen Saver Modules

- MultiSession Screen Saver Module
- Screen Saver Module

Sound - See Sound Modules

- Universal Sound Module

TermSecure - See TermSecure Modules

- Bluetooth Module
- DigitalPersona UareU Fingerprint Reader
- RF Ideas pcProx Module
- RF Ideas pcProx USB Module
- RF Ideas pcProx Sonar Module
- TermMon ActiveX Configuration Module
- USB Flash Drive Module
- USB ID Reader Module

Touch Screen - See Touch Screen Modules

- Arista ARP-16XXXAP-ACP Touch Screen Driver

- CarrollTouch Touch Screen Driver
- Contec Touch Screen Driver (Package 5 only)
- DMC Touch Screen Driver (Package 5 only)
- DMC TSC Series Touch Screen Driver
- Dynapro Touch Screen Driver
- eGalax Touch Screen Driver
- Elographics Touch Screen Driver
- Gunze AHL Touch Screen Driver
- Hampshire TSHARC Touch Screen Driver
- Intra-T Touch Screen Driver
- MicroTouch Touch Screen Driver
- Panjit TouchSet Touch Screen Driver
- PenMount Touch Screen Driver
- Ronics Touch Screen Driver (Package 5 only)
- Touch Control Touch Screen Driver
- Touch International IR Touch Screen Driver (Package 5 only)
- USB Touch Screen Driver
- Xycom 33XX Touch Screen Driver (Package 5 only)
- Zytronic Touch Screen Driver

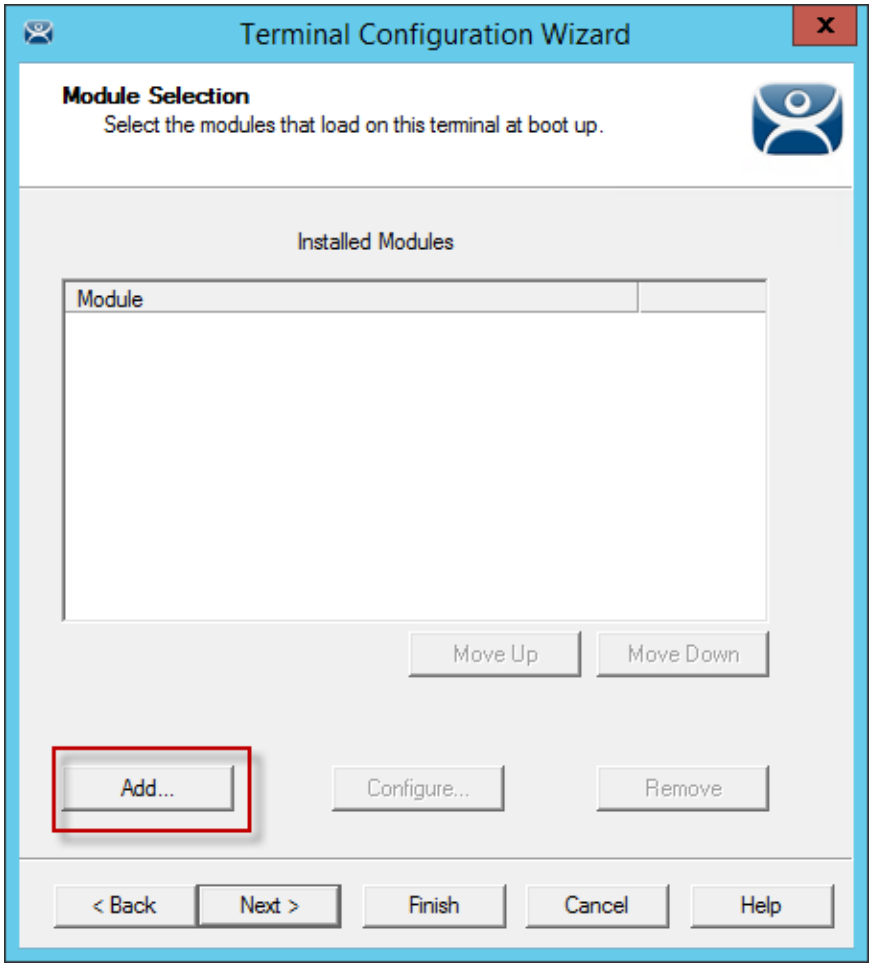
Video Driver - See Video Driver Modules

- Custom Video Mode Module
- Monitor Configuration Module

24.2. Adding a Module (Keyboard > Key Block Module)

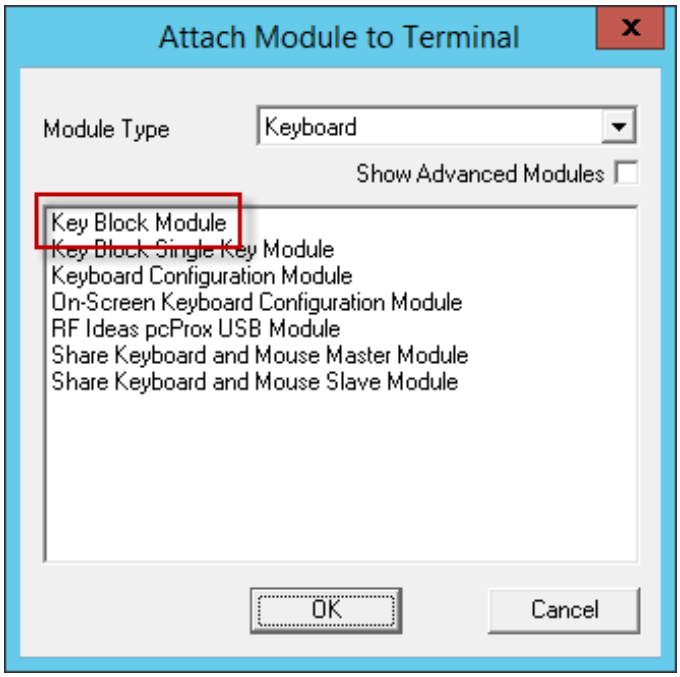
Double click on your Terminal to launch the **Terminal Configuration Wizard**.

Navigate to the **Module Selection** page.



Module Selection Page

Select the ***Add*** button to launch the **Attach Module to Terminal** window.

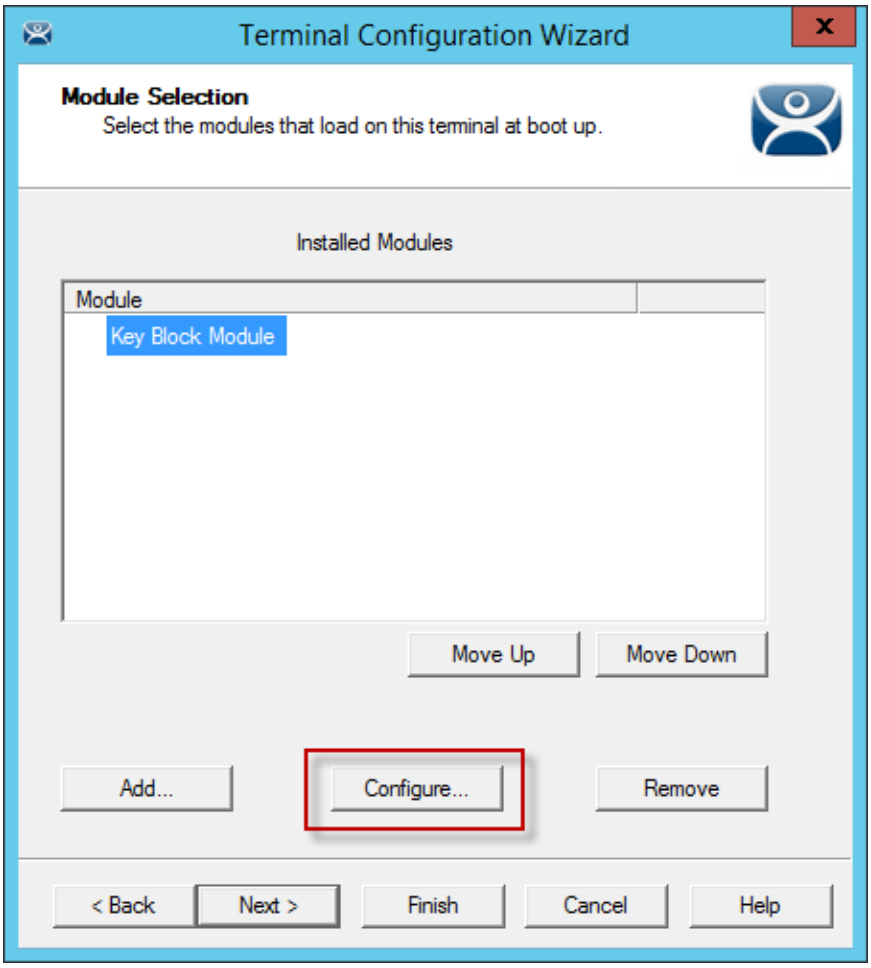


Attach Module to Terminal Window

The **Attach Module to Terminal** window has been organized with a drop-down box. The modules may be viewed by category or as a whole.

Select a module category from the ***Module Type*** drop-down.

Highlight a module and select ***OK***.

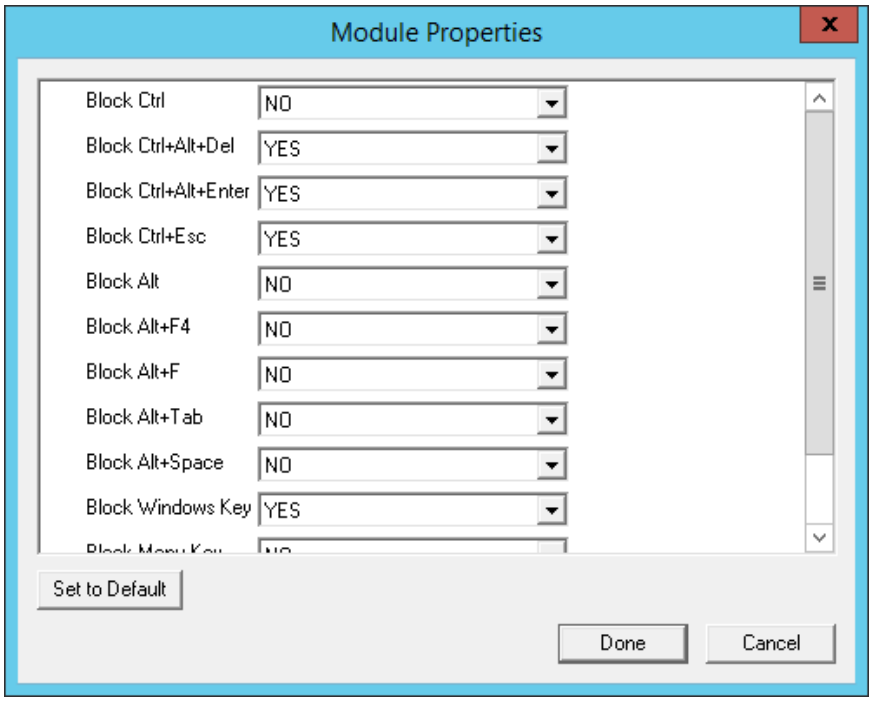


Key Block Module

This picture shows the ***Key Block Module*** in the **Installed Modules** window.

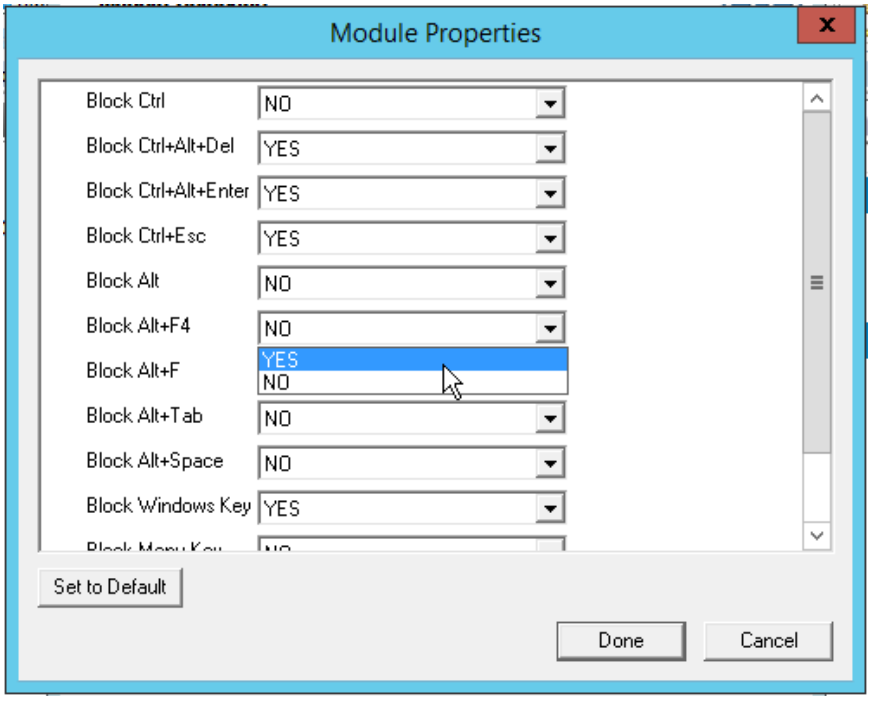
The **Key Block Module** has configurable settings.

Highlight the **Key Block Module** and select the ***Configure*** button to launch the **Modules Properties** window.



Module Properties

The **Module Properties** window shows the settings that can be configured.

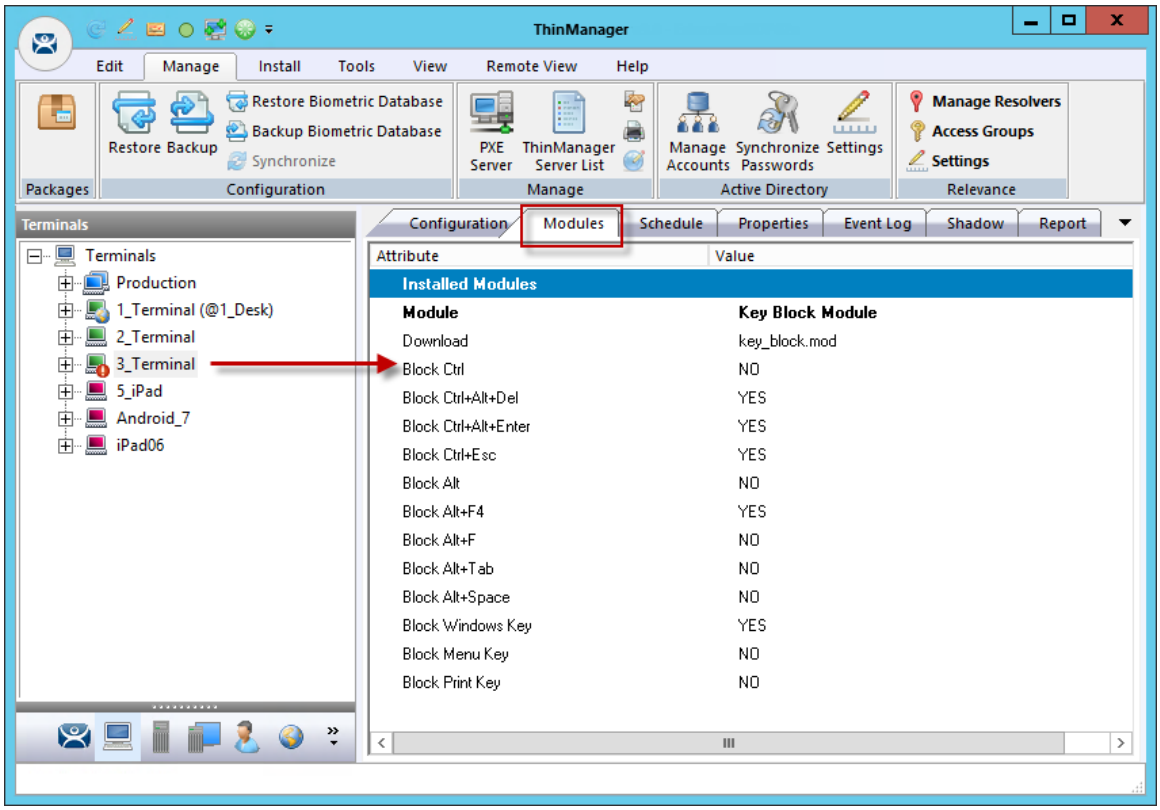


Module Properties

You change a parameter using the drop-down or typing the new setting.

By default ***CTL+ALT+DEL***, ***CTL+ALT+ESC***, and ***CTL+ESC*** are blocked. The other key combinations can be blocked by highlighting the key combination and changing the ***Value*** to ***Yes***.

Select ***Done*** to close the window.



Modules Tab for a Terminal

The module and settings will be displayed on the **Modules** tab when the Terminal is highlighted.

Note: The 3_Terminal shows the red Configuration Indicator icon to show that the configuration changed when the module was added but it hasn't been restarted yet to load the new configuration.

24.3. Individual Module Details

ThinManager divides the modules into a number of categories or types to make navigation of the module list easier. The types and modules include **ICA, Local Storage, Miscellaneous, Mouse, RDP, Screen Saver, Sound, TermSecure, Touch Screen**, and **Video.**

24.4. ICA Modules

The ICA Modules are advanced modules for advanced users of the ICA client communication protocol.

24.4.1. Citrix ICA UseAlternateAddress Module

The **Citrix ICA UseAlternateAddress Module** is used by advance Citrix users to specify connections to Citrix Servers.

Configuration includes **Use Alternate Address**, **Browser Protocol**, and **HttpBrowser Addresses**.

24.4.2. Citrix ICA wfclient.ini Extension Module

The **Citrix ICA wfclient.ini Extension Module** is used by advanced Citrix users. This module allows up to 8 strings of text to be added to the wfclient.exe for passing Citrix parameters.

24.5. Keyboard Modules

The Keyboard Modules are modules used to control or alter keyboard behavior.

24.5.1. Keyboard>Key Block Module

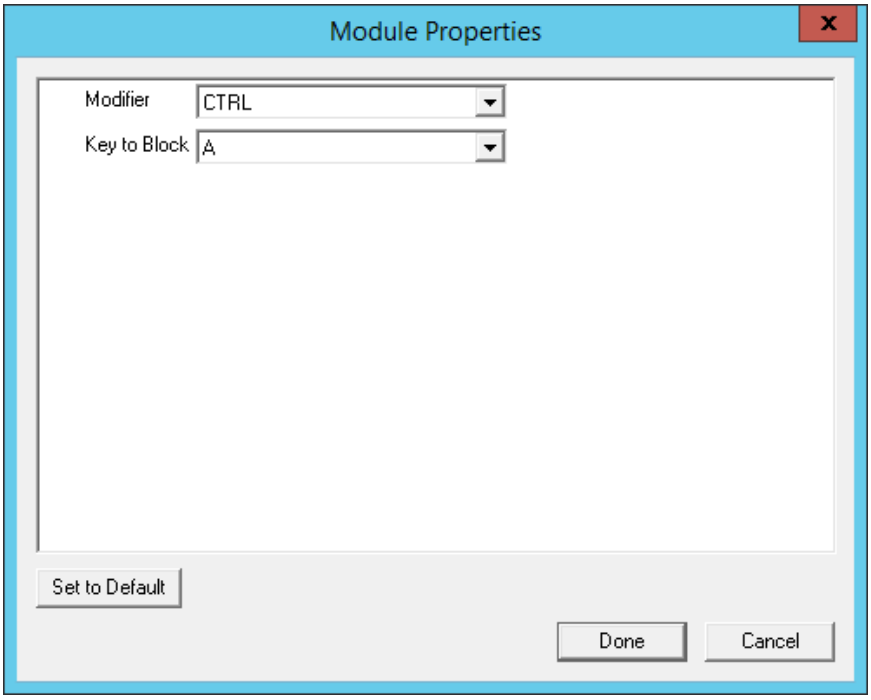
The Key Block module traps certain keystrokes and prevents them from being sent to the Remote Desktop Server for processing.

The key combinations to be blocked can be configured by in the Module Properties. To launch this, highlight the module on the Module Selection page and select the ***Configure*** button. A **Module Properties** dialog box will be displayed. Select the parameter to change in the **Module Properties** window and select the ***Value*** in the drop-down box.

The key combinations that have a value of ***YES*** will be blocked from reaching the Remote Desktop Server.

24.5.2. Keyboard>Key Block Single Key Module

The **Key Block Single Key Module** lets you block a single key combination from being send from the Terminal to the session.



Key Block Single Key Module Properties

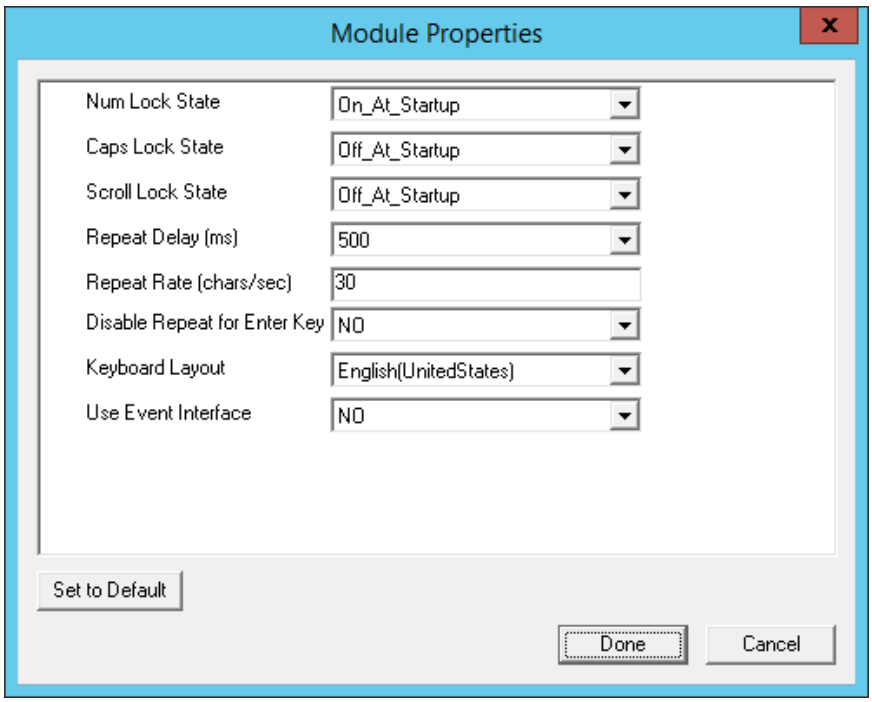
You can block a single set of key combinations by adding and configuring the **Key Block Single Key Module**.

You can set ***ALL***, ***CTL***, ***ALT***, or ***CTL+ALT*** as the modifier key(s) and set ***A-Z***, ***F1-F12***, and ***ESC***, ***Tab***, ***Backspace***, etc. as the key to block.

If you have multiple keys to block add the **Key Block Single Key Module** once for each combination and configure them accordingly.

24.5.3. Keyboard>Keyboard Configuration Module

The Keyboard Configuration Module allows you to set the keyboard language and control the behavior of the Caps lock and Number lock on the Terminal.



Keyboard Configuration Module Properties

The Keyboard Configuration parameters include:

- ***Num Lock State*** – This allows the Number Lock to be set to **On** at startup, **Off** at startup, always **On**, or always **Off**.
- ***Cap Lock State*** – This allows the Caps Lock to be set to **On** at startup, **Off** at startup, always **On**, or always **Off**.
- ***Scroll Lock State*** – This allows the Scroll Lock to be set to **On** at startup, **Off** at startup, always **On**, or always **Off**.
- ***Repeat Delay (ms)*** – This parameter sets the amount of time that a key needs to be held down before it starts repeating the keystroke. If this parameter is set to ***Disable*** a key will only send one keystroke even if the key is held down.
- ***Repeat Rate (char/sec)*** – This parameter sets the number of characters per second that a held down key will send.
- ***Disable Repeat for Enter Key*** – This parameter, when set to ***Yes***, will prevent the **Enter** key from repeating if it is held down.
- ***Keyboard Layout*** – This parameter allows the thin client to use keyboards other than the default English (United States) keyboard map.

24.5.4. On-Screen Keyboard Module

The **On-Screen Keyboard Module** allows you to configure an on-screen keyboard for touch screens. The configuration of the launch of the keyboard through a long touch or hold is done within the Touch

Screen Module. The settings in the on-screen keyboard are configured in the On-Screen Keyboard Module.

- ***Show Keypad***– This parameter adds the keypad to the display.
- ***Show Function Keys***– This parameter adds the function keys to the display.
- ***Show Control Key***– This parameter adds the Control key to the display.
- ***Show Alt Key***– This parameter adds the ALT key to the display.
- ***Num Lock State***– This parameter turns the numbers lock on or off on launch.
- ***Inactivity Timeout (seconds)*** – This parameter sets the duration of the idle time that will close the keyboard.
- ***Keyboard Scale Percentage***– This parameter sets the width of the keyboard, as a percentage of the screen.
- ***Font Size***– This parameter sets the font size of the keys.

24.5.5. RF Ideas pcProx USB Module

The **RF Ideas pcProx USB Module** uses a USB device that allows a Terminal to use RF Ideas pcProx cards as TermSecure ID cards

ThinManager supports the RDR-xx81AKx family of card readers from RFIdeas. This includes the serial RDR-**6081AK2** reader and **RDR-6081AKU** (Package 5, 6, or 7), **RDR-80582AK0** (Package 6 or 7), and **RDR-80081AKU** (Package 7.1.4 and later) USB readers

. The parameters are:

- **Mode –** This allows the device to be used in TermSecure Mode, Wedge, or TermMon mode.
  - The **TermSecure** mode sends data to ThinManager for use with TermSecure.
  - The **Wedge** mode sends data straight to the session as a keyboard wedge.
  - The **TermMon** mode sends data to the TermMon ActiveX that you embed in your application.
- **Allow Manual TermSecure Login** - This, when set to ***Yes***, will allow a Relevance user to log into a Terminal without a TermSecure ID device. If set to ***No***, TermSecure users must use a TermSecure ID device to log in.
- **Prompt for TermSecure Password** - This, when set to Yes, will require a TermSecure to enter their password for access, even if the password is configured in ThinManager.

See Card and Badge Configuration for a Relevance User for details.

24.5.6. Share Keyboard and Mouse Modules

The **Share Keyboard and Mouse** module allows several thin clients to be controlled with a single keyboard and mouse without the need of a KVM switch (Keyboard/Video/Mouse).

The **Share Keyboard and Mouse** has a **Master** module that is added to the controlling Terminal, and a **Slave** module that is added to the dependent Terminals.

The Share Keyboard and Mouse can be used by placing several monitors connected to thin clients, side-by-side or top-to-bottom. The ***Share Keyboard and Mouse Master module*** is loaded on the center thin client. This module is configured by adding the IP addresses of the secondary slave thin clients. The other Terminals receive the ***Share Keyboard and Mouse Slave module***. Once the ***Share Keyboard***

and Mouse Master Module is added to a Terminal, it can be configured by highlighting it in the ***Installed Module*** window and selecting the ***Configure*** button.

- ***Left Terminal IP Address*** - Enter the correct IP address for the Slave Terminal on the left of the master Terminal, if used, and select the ***Set*** button.
- ***Right Terminal IP Address*** - Enter the correct IP address for the Slave Terminal on the right of the master Terminal, if used, and select the ***Set*** button.
- ***Top Terminal IP Address*** - Enter the correct IP address for the Slave Terminal on the top of the master Terminal, if used, and select the ***Set*** button.
- ***Bottom Terminal IP Address*** - Enter the correct IP address for the Slave Terminal on the bottom of the master Terminal, if used, and select the ***Set*** button.
- ***Allow Interactive Shadow of Master*** - Normally a Terminal with the master module loaded is blocked from interactive shadow. If you want to allow interactive shadowing on the master, highlight the ***Allow Interactive Shadow of Master*** parameter, select ***Yes*** from the ***Value*** drop-down, and select the ***Set*** button.

The **Share Keyboard and Mouse Slave module** is loaded on the secondary thin clients using the same methods as other modules are loaded.

- ***Master IP Address*** - This setting allows the slave module to be configured to connect to a specified master by entering the IP address of the master Terminal and selecting the ***Set*** button.

Select the ***Done*** button when finished.

Once the ThinManager Enabled thin clients are booted, the mouse on the master thin client can be moved seamlessly into the other desktops. The keyboard will be active in whatever screen the mouse pointer is on.

This allows an operator to have control of several displays with only one keyboard and mouse. The mouse movement is seamless, allowing access to displays without switching.

Note: A Master Share Keyboard and Mouse session cannot be interactively shadowed in ThinManager unless it is configured to allow it.

The keyboards and mice for the slave thin clients can be left attached but stowed away until a multi-user configuration is needed.

24.1. Language Modules

The Language modules allow different languages to be used by the terminal.

24.1.1. Language>Language Selection Module

The Language Selection Module sets the language on the terminal. You may want to use the Keyboard Configuration module to set the keyboard language and set the language in the session.

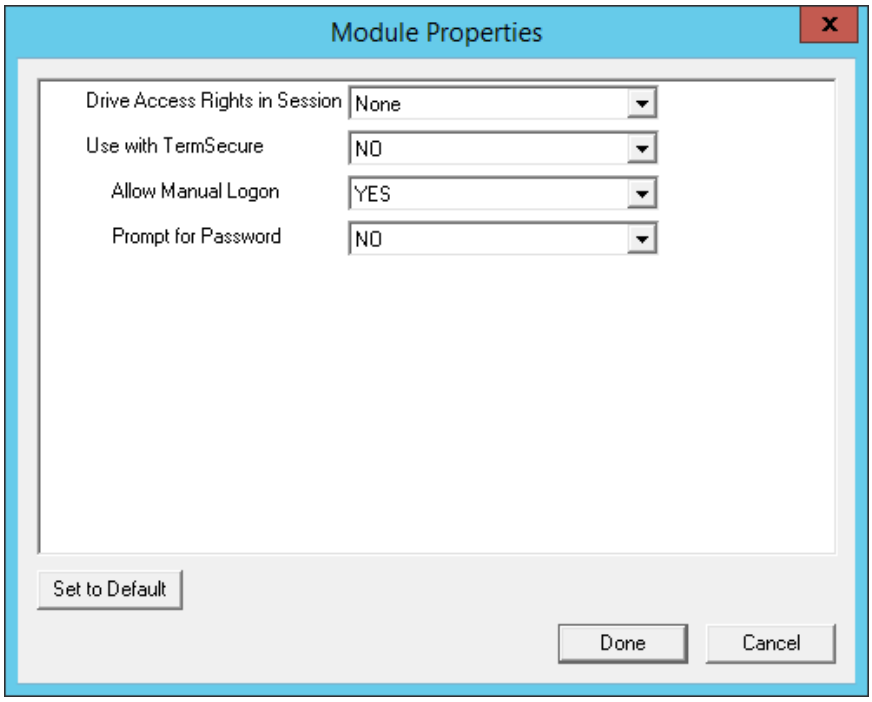
24.2. Local Storage Modules

The Local Storage modules allow the use of USB ports on thin clients. The USB ports are not active by default for security.

24.2.1. Local Storage>USB Flash Drive Module

USB ports are disabled by default in the ThinManager system. You can use the USB ports for keyboards and mice, but not USB drives. You need to allow the port to be used with the **USB Flash Drive Module**.

The USB port will also work with devices that work as a keyboard wedge.



USB Flash Drive Module Properties

The **USB Flash Drive Module** has several parameters.

- ***Drive Access Rights in Session*** - ***ReadWrite*** allows the user to read and write to the flash drive. ***ReadOnly*** allows the user to read data but not write data, and ***None*** sets the flash drive to access only the unique serial number to make it usable as a TermSecure ID device.
- ***Use with TermSecure*** - This needs to be set to ***YES*** to allow the device to be a TermSecure identifier. A ***NO*** setting, in conjunction with a ***ReadWrite*** **Access Rights** setting, will allow the device to be used as a remote storage drive
- ***Allow Manual Login*** - This value, when set to ***Yes***, will allow a Relevance user to log into a Terminal without a TermSecure ID device. If set to No, TermSecure users must use a TermSecure ID device to log in.
- ***Prompt for Password*** - This value, when set to ***Yes***, will require a Relevance User to enter their password for access, even if the password is configured in ThinManager.

Note: USB doesn't map to the session like serial does. If you want to add a USB device that requires a driver installed, like a printer, you can use an IP-to-USB converter that allows you to address the device and mount the drives from the session.

24.2.2. USB Memory Card Reader Module

The **USB Memory Card Reader Module** allows USB card readers to connect to a Terminal. The parameters include:

- **Number of Slots in Reader** - This value sets the number of slots that the card reader uses.
- **Read Only Access** - This value, when set to ***Yes***, will limit the user to reading the card. This value, when set to ***No***, will allow the user to read and write to the card.

24.3. Miscellaneous Modules

These are modules that don't fit in other categories.

24.3.1. Add Serial Port

The **Add Serial Port Module** is only used to configure the serial ports of daughter boards that add additional serial ports to Terminals. Add a module for each additional serial port. Each module will let the user configure one additional port.

- ***Port Number*** - This value is to be set to the port number of the new port.
- ***Port Address*** - This value is to be set to the port address of the new port.
- ***IRQ*** - This value is to be set to the IRQ of the new port.
- ***UART***- This value is set to the chipset type for the new port.

24.3.2. Barcode Configuration Module

This module sets the protocols that a tablet will use to scan barcodes.

24.3.3. Bluetooth Module

This is covered in the Relevance Module section on page 384.

24.3.4. Firmware Update Module

The **Firmware Update module** allows a ThinManager Ready thin client with an embedded firmware to be updated.

ThinManager enables some models of Terminals to store the firmware with Disk On Chip or Compact Flash storage so that the unit doesn't have to download the entire firmware at boot but can boot locally and download just the configuration to save bandwidth. This is most commonly used with units that will connect over low bandwidth networks, like wireless networks or WANs. These units can use the Firmware Update module to download and flash new firmware when the firmware is updated in ThinManager.

The ability to update stored firmware Terminals eliminates the need to send the Terminal back to the manufacturer to update the firmware.

Note: The firmware download can vary, depending on the bandwidth of the connection and the size of the firmware update.
It is recommended that updates be done over a wired LAN instead of over a wireless connection, when possible.

The **Firmware Update** module has two configurable parameters.

Confirm at Terminal - This setting, if set to ***Yes***, will prompt the operator to choose between immediately updating firmware or waiting until the next boot up. If ***Confirm at Terminal*** is set to ***No***, the firmware download will take place immediately.

Force Update - Normally a stored firmware Terminal with the Firmware Update module will check firmware version numbers at boot and only download a new firmware if the versions are different. This setting, if set to ***Yes***, will force the Terminal to always download the firmware for re-flashing.

Disable Update - This prevents the Terminal from downloading and flashing a new firmware if it is installed. This allows the administrator to select the time of update instead of it happening automatically.

Note: The module will download firmware when it detects a different firmware. Since this will only happen at the first reboot after updating the ThinManager firmware, it is safe to leave this module added to Terminals permanently when ***Force Update*** is set to ***No***. It does not need to be added and removed each

time the firmware is updated. However, since it will update when the firmware is different, it will try to update the firmware if you boot it from a ThinManager server with older firmware.

24.3.4.1. Firmware Update Program

Once the new firmware has downloaded, an update program will run on the Terminal to rewrite the new firmware to the storage. The program will display a warning stating that the Terminal must not be reset or powered off during the process, usually around 30 seconds. Ignoring the warning can corrupt the stored firmware, so it is important to leave the Terminal alone for that period of time.

Note: Heed the warning. The Terminal must not be reset or powered off during the brief period that the update program is writing the firmware to the firmware storage device.
It is recommended that updates be done over a wired LAN instead of over a wireless connection, when possible.

24.3.4.2. Stored Firmware Terminal Configuration

A stored firmware Terminal loads the firmware locally before connecting to the ThinManager server. The stored firmware Terminals have a setup program that allows configuration of the connection. Enter the program by selecting any key when ***Select any key*** to configure is displayed during the boot process. A setup screen will be displayed.

The changes may be saved or discarded before the boot process is resumed.

24.3.5. Instant Failover Module

The **Instant Failover Module** is to be used only with Terminal configurations that use the legacy "Individual Remote Desktop Servers" method instead of the preferred Display Clients method.

Since the use of Display Clients is a preferred method of getting Remote Desktop Services sessions over using the legacy "Individual Remote Desktop Servers" the module is hidden from view unless the Show Advanced Modules checkbox is selected.

Instant Failover allows a Terminal to connect to a session on two Remote Desktop Servers. Both sessions are active but only one is displayed. If the first Remote Desktop Server fails, the second session is immediately displayed, eliminating any downtime due to Remote Desktop Server failure. See Instant Failover for details.

Note: The Instant Failover Module is only used with Terminals using Individual Remote Desktop Servers. (See Remote Desktop Server Specification Page).
Terminals using Display Clients use a checkbox to enable Instant Failover. (See Instant Failover with Remote Desktop Services Display Clients).
Do not use this module while using Display Clients.

The Instant Failover function requires an Instant Failover license for each Terminal that uses it.

Instant Failover Configuration When Using Individual Remote Desktop Servers

The thin client cascades both sessions, with the primary in front. You cannot see the secondary session as it is hidden in back. There is an option that allows one to switch between sessions with a hot key.

Hot Key Session Switching - If this parameter is set to ***Enabled***, the hot key combination will allow the toggling between sessions.

- **Hotkey Combination is CTRL+** - The value of the hot key is defaulted to ***CTRL+F9*** but can be assigned to any function key.

24.3.6. Local Print Module

The Local Print Module simplifies printing through the parallel port on thin clients.

There are three steps:

1. Install the print driver on the Remote Desktop Servers that the client will connect to.
2. Add the **Local Print Module** to the thin client as described in Adding a Module to a Group or Terminal.
3. Configure the ***Print Driver Name*** parameter in the module to contain the print driver's name.

- ***Printer Driver Name*** - The Local Print module works when the name of the print driver is entered in the ***Value*** field for the **Printer Driver Name**. The Print Driver name is provided by the properties page for the printer.

The **Printer Property** page for a printer can be launched by selecting ***Start > Settings > Printers*** and selecting the appropriate printer. This will launch the **Printer Queue** window.

Select ***Printer > Properties*** to launch the **Printer Properties** page.

The **Printer Property** page shows the Print Driver name on the ***Advanced*** tab. This is the name that needs to be entered into the Local Print Module.

Note: When printing from the client, the printer will be displayed as **Printer/username/session number**.

24.3.7. MultiStation Configuration Module

The MultiStation Configuration Module allows you to specify how many keyboards and mice are at each station.

The settings include

- **Station Number** – This drop-down specifies the station number to configure.
- **Number of Keyboards** – This sets the number of keyboards at the selected station.
- **Number of Mice** – This sets the number of mice at the selected station.

24.3.8. Redundant Ethernet Module

Adding the **Redundant Ethernet Module** to a Terminal with dual network ports will allow the Terminal to use the second port as a backup. The Terminal will have one IP address but it can have the ports plugged into two switches to have redundant paths to the Remote Desktop Servers.

The **Redundant Ethernet Module** has no configurable settings. Plug each network port into different switches on the same network.

The Terminal will boot from the first available network port and download the configuration. If the first network path fails it will seamless switch to the backup port to prevent interruption of service.

24.3.9. Terminal Shadow Module

This module needs to be installed in ThinManager but is not applied to a Terminal. A Terminal will automatically download this module if it is needed.

24.3.10. TermMon ActiveX Configuration Module

This configures the TermMon ActiveX control that collects Terminal information and can perform Terminal functions. It is listed as both a Miscellaneous Module and a TermSecure Module but is described in the TermSecure section.

See TermMon ActiveX Control for details.

24.3.11. Time Zone Redirection Module

The Time Zone Redirection Module allows a Terminal to display local time when it is connected to a Remote Desktop Server in another time zone.

- ***Time Zone*** - This parameter can be highlighted to activate the ***Value*** drop-down that contains time zones. Select the ***Set*** button to accept the changes.

Windows Remote Desktop Servers need to have time zone redirection allowed in the Group Policy Console.

The Allow Time Zone Redirection policy is found under **Local Computer Policy\Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Client\Server data redirection folder** for Server 2003 or **Local Computer Policy\Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Remote Desktop Server\Device and Resource Redirection** for Server 2008 of the Group Policy.

Please see Microsoft documentation for information on Group Policy.

24.3.12. TMTerm DLL Configuration Module

The TMTerm DLL Configuration module is used to communicate with the Terminal sessions from another Terminal or computer.

- **Allow Connections from** – Selecting ***ANY_IP*** allows you to configure the communication from any computer.
  - ***ANY_IP*** allows you to configure the communication from any computer.
  - ***List*** allows you to limit communication to specified computers.
- **IP Address list (comma separated)** – This allows you to list the IP addresses of computers authorized to retrieve the TermMon data. Separate multiple computer IP addresses with a comma.

24.3.13. USB to Serial Module

The USB to Serial module allows you to map the USB ports to serial ports if you are using a USB-to-Serial device plugged into the Terminal.

24.3.14. User Override Module

The User Override Module is a temporary module that allowed users of ThinManager 3.1 to use the User Override function in Display Clients It is no longer needed in ThinManager 3.2+.

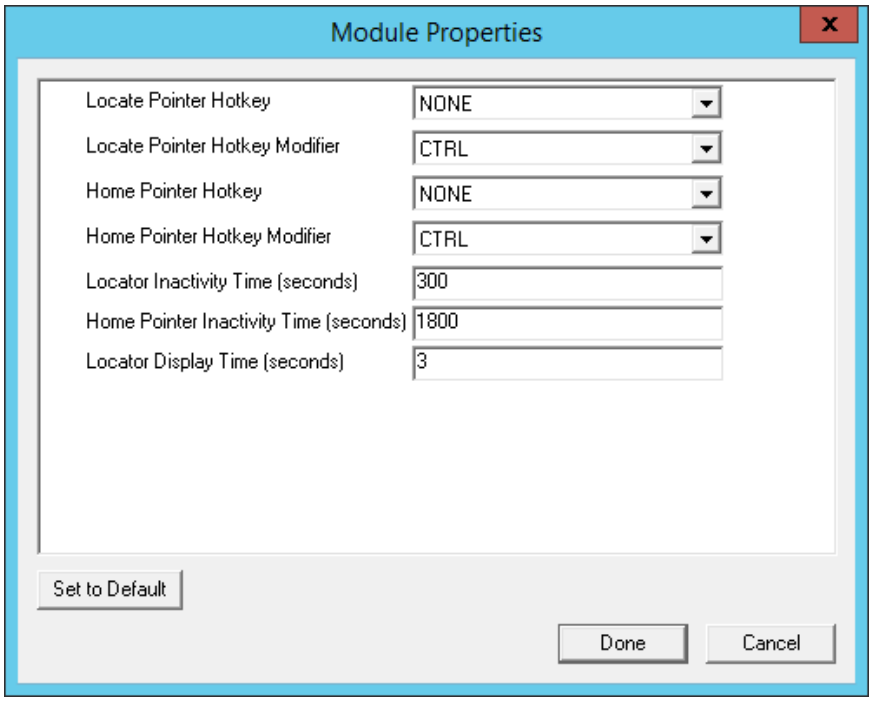
See Display Client Override for the current method of User Override.

24.4. Mouse Modules

Mouse Modules can configure mouse functions in the ThinManager system.

24.4.1. Locate Pointer Module

The **Locate Pointer Module** adds a large crosshair to the cursor when it becomes active after being idle. This allows you to see its location quickly. This is particularly helpful in a MultiMonitor system.



Locate Pointer Module

The settings include

- **Locate Pointer Hotkey** – This allows you to set a hotkey to make the cursor appear.
- **Locate Pointer Hotkey Modifier** – This allows you to set the modifier key to activate the hotkey to show the pointer cursor.
- **Home Pointer Hotkey** – This allows you to set a hotkey that will move the cursor to the center of the main screen.
- **Home Pointer Hotkey Modifier** – This allows you to set the modifier key that will move the cursor to the center of the main screen.
- **Locate Inactivity Time (seconds)** – This sets the length of the idle time before the locate pointer cursor is activated.
- **Home Pointer Inactivity Time (seconds)** – This sets the length of the idle time before the locate pointer cursor is moved to the center of the main screen.
- **Locate Display Time (seconds)** – This is the length of time that the locate pointer crosshair cursor will be displayed when activated.

24.4.2. Mouse Configuration Module

The Mouse Configuration Module allows USB or PS/2 mice to be configured and allows the use of two mice. Mouse configuration settings include:

- ***Primary Mouse Type*** -This setting allows both a PS/2 mouse and USB mouse to be used on a Terminal. This setting will define which mouse is considered the primary mouse.
- ***Mouse Protocol*** - This value allows the selection of different protocols used by the mouse.
- ***Scroll Mouse*** - The value, when set to ***Yes***, allows a scroll mouse to function on a Terminal.
- ***Acceleration Multiplier*** - This value allows the mouse movement to be slowed down or sped up.
- ***Acceleration Threshold (pixels)*** - This value is the number of pixels a mouse must move before the acceleration multiplier takes effect.

- ***Left Button*** – This will disable the left mouse button when set to ***Disabled***.
- ***Right Button*** – This will disable the right mouse button when set to ***Disabled***.
- ***Scroll Button*** – This will disable the scroll button when set to ***Disabled***.
- ***Scroll Wheel*** – This will disable the scroll wheel when set to ***Disabled***.

These parameters can be changed by highlighting the parameter and choosing a new value in the ***Value*** drop-down box. Use the ***Set*** button to accept the new parameter value.

ThinManager supports USB mice. The **Mouse Configuration Module** allows configuration of USB mice.

A thin client can have both a USB and a PS/2 mouse installed. This module allows the selection of the primary mouse when using two mice.

24.4.3. PS/2 Mouse Module

The PS/2 Mouse Module is the forerunner of the Mouse Configuration Module. It allows the changing of PS/2 settings like mouse type, acceleration and threshold. All of these features are now available in the Mouse Configuration Module.

- ***Mouse Type*** -This value allows the selection of PS/2 or USB mouse type.
- ***Scroll Mouse*** - The value, when set to ***Yes***, allows a scroll mouse to function on a Terminal.
- ***Acceleration Multiplier*** - This value allows the mouse movement to be slowed down or sped up.
- ***Acceleration Threshold (pixels)*** - This value is the number of pixels a mouse must move before the acceleration multiplier takes effect.

24.4.4. Serial Mouse Driver

The Serial Mouse Driver allows a serial mouse to be used with thin clients.

Mouse Type - This value defines what type of mouse is used.

Serial Port – Set this value to the serial port number used for the mouse.

24.4.5. Share Keyboard and Mouse Modules

The **Share Keyboard and Mouse** module allows several thin clients to be controlled with a single keyboard and mouse without the need of a KVM switch (Keyboard/Video/Mouse).

The **Share Keyboard and Mouse** has a **Master** module that is added to the controlling Terminal, and a **Slave** module that is added to the dependent Terminals.

The Share Keyboard and Mouse can be used by placing several monitors connected to thin clients, side-by-side or top-to-bottom. The ***Share Keyboard and Mouse Master module*** is loaded on the center thin client. This module is configured by adding the IP addresses of the secondary slave thin clients. The other Terminals receive the ***Share Keyboard and Mouse Slave module***. Once the ***Share Keyboard and Mouse Master Module*** is added to a Terminal, it can be configured by highlighting it in the ***Installed Module*** window and selecting the ***Configure*** button.

- ***Left Terminal IP Address*** - Enter the correct IP address for the Slave Terminal on the left of the master Terminal, if used, and select the ***Set*** button.
- ***Right Terminal IP Address*** - Enter the correct IP address for the Slave Terminal on the right of the master Terminal, if used, and select the ***Set*** button.
- ***Top Terminal IP Address*** - Enter the correct IP address for the Slave Terminal on the top of the master Terminal, if used, and select the ***Set*** button.
- ***Bottom Terminal IP Address*** - Enter the correct IP address for the Slave Terminal on the bottom of the master Terminal, if used, and select the ***Set*** button.
- ***Allow Interactive Shadow of Master*** - Normally a Terminal with the master module loaded is blocked from interactive shadow. If you want to allow interactive shadowing on the master, highlight

the ***Allow Interactive Shadow of Master*** parameter, select ***Yes*** from the ***Value*** drop-down, and select the ***Set*** button.

The **Share Keyboard and Mouse Slave module** is loaded on the secondary thin clients using the same methods as other modules are loaded.

- ***Master IP Address*** - This setting allows the slave module to be configured to connect to a specified master by entering the IP address of the master Terminal and selecting the ***Set*** button.

Select the ***Done*** button when finished.

Once the ThinManager Enabled thin clients are booted, the mouse on the master thin client can be moved seamlessly into the other desktops. The keyboard will be active in whatever screen the mouse pointer is on.

This allows an operator to have control of several displays with only one keyboard and mouse. The mouse movement is seamless, allowing access to displays without switching.

Note: A Master Share Keyboard and Mouse session cannot be interactively shadowed in ThinManager unless it is configured to allow it.

The keyboards and mice for the slave thin clients can be left attached but stowed away until a multi-user configuration is needed.

The ***Share Keyboard and Mouse Master module*** is licensed for each master thin client. The ***Share Keyboard and Mouse Slave module*** is free. Each master module can have 1 to 4 slave units. Future releases will expand the number of slaves that the master can control.

24.5. Network Modules

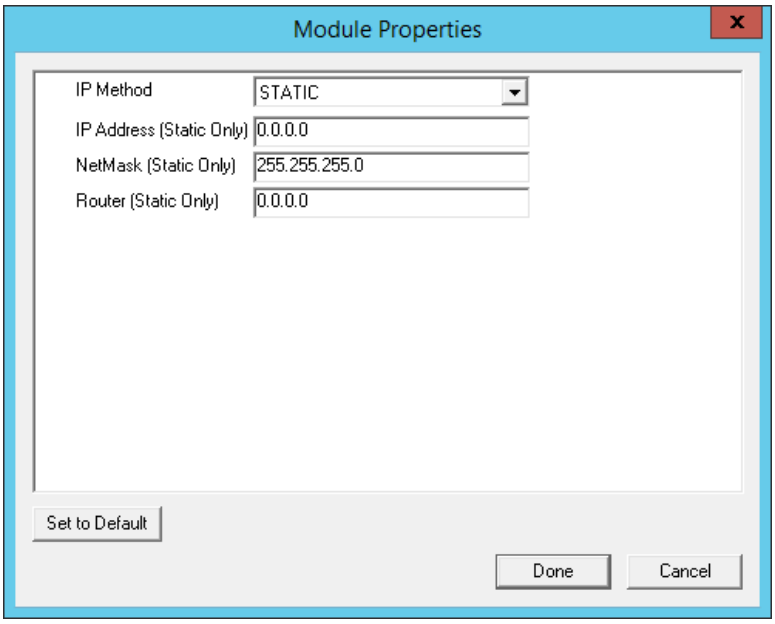
24.5.1. Domain Name System Module

The Domain Name System Module allows you to specify a DNS server for a Terminal without turning on DNS for the entire ThinManager Server system.

24.5.2. Second Network Module

The **Second Network Module** allows you to use the dual network ports on a Terminal on different networks.

Add the **Second Network Module** and configure the second port. The Terminal will always boot from the first port but once booted it will enable the second port and allow communication on both networks. This is useful for separating IP camera bandwidth from the process control network, for example.



Second Network Module

The settings include

- **IP Method** – This allows the second port to use DHCP or a static IP.
- **IP Address (Static Only)** – This allows the second port to be assigned a static IP address.
- **NetMask (Static Only)** – This allows the second port to be assigned a subnet mask.
- **Router (Static Only)** - This allows the second port to be assigned a router.

24.5.3. Third Network Module

The Third Network Module allows you to configure a third network port to connect to a different network than the first network port on Terminals with three network ports..

The Third Network Module parameters are:

- ***IP Method*** – This drop-down allows you to select a static IP or use DHCP.
- ***IP Address (Static Only)*** – This allows you to set a static IP address if Static was the selected IP method.
- ***NetMask (Static Only)*** – This allows you to set a NetMask if Static was the selected IP method.
- ***Router (Static Only)*** – This allows you to set a static IP address for a router if Static was the selected IP method.

24.6. RDP Modules

24.6.1. RDP Experience Module

The RDP Experience Module allows a session connected to a Windows 2003 Remote Desktop Server with RDP to add features to the session.

The **RDP Experience Module** parameters are:

- ***Allow Desktop Background*** - This setting, if set to ***Yes***, will allow a Terminal to show a desktop background.

- ***Show Window Contents While Dragging*** - This setting, if set to ***Yes***, will allow a Terminal to show window contents while dragging.
- ***Allow Menu and Window Animation*** - This setting, if set to ***Yes***, will allow a Terminal to show window and menu animations.
- ***Allow Themes*** - This setting, if set to ***Yes***, will allow a Terminal to show a desktop Theme.
- ***Allow Font Smoothing*** - This setting, if set to ***Yes***, will use the Microsoft font smoothing in the session.
- ***Duplicate Server Connect Delay(seconds)*** - This setting will add a delay when a Terminal is creating multiple connections to a Remote Desktop Server and normally gets a message that the server is busy. Adding a delay can minimize that error message.
- ***Enable Network Level Authentication*** - This setting allows you to tune off NLA (Network Level Authentication) for that Terminal.
- ***Use Hardware Scaling When Available*** - This setting, if set to ***Yes***, will use the local video hardware for scaling.

In order to use these features, the RDP Experience must be enabled by using the **Windows Group Policy Editor**. See Microsoft documentation for details.

24.6.2. RDP Port Module

The **RDP Port Module** allows that port that RDP communicates to the Remote Desktop Server to be changed from the default 3389 to another port.

The RDP Port Module allows the port that RDP uses to be changed from the default 3389.

- ***RDP Server Port Number (decimal)*** - Enter the new port number for RDP in this value.

24.6.3. RDP Serial Port Redirection Module

Using serial ports on a thin client presents a paradox. The session is running on a Remote Desktop Server and not the thin client. If you connect a serial device to the thin client and reference it in the session, the session will look at the local serial ports on the server and not the remote serial ports on the Terminal where the device is attached.

Adding the RDP Serial Port Redirection Module will map the remote ports on the Terminal to the local ports in the session. If the session references COM Port 1it will be sent to the Terminal COM Port 1.

The RDP Serial Port Redirection Module has no configuration, adding it is enough to map the remote COM Ports.

24.6.4. RDP Session IP Module

The **RDP Session IP Module** allows a Terminal to use an alias IP address for a specific Display Client session.

The RDP Session IP module has three settings:

- ***Group Name*** – This specifies the Display Client to use.
- ***Session IP Address*** – This is the IP address to use as the alias.
- ***Session IP Address for Instant Failover*** – This is the IP address to use for a backup session it the Display Client is configured to use Instant Failover.

24.6.5. Smart Card Module

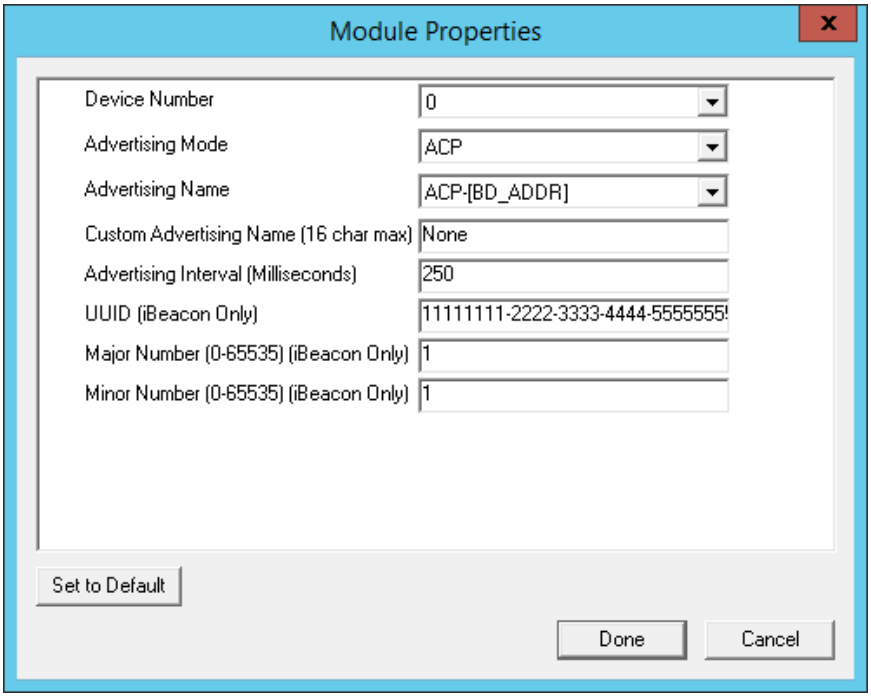
The Smart Card module needs to be added to use a Smart Card Reader and Smart Cards.

Note: Network Level Authentication (NLA) needs to be disabled on the Remote Desktop Servers to use a smart card as a login device.
It can be left enabled if you are using the smart card to send information to the active session.

24.7. Relevance Modules

24.7.1. Bluetooth Module

ThinManager supports Bluetooth 4.0 USB adapters as resolvers for Relevance. A Bluetooth USB adapter can be plugged into a thin client USB port to provide a Bluetooth beacon that doesn't require batteries. The Bluetooth module allows you to configure the USB adapter.



Bluetooth Module

The **Bluetooth Module** has several settings:

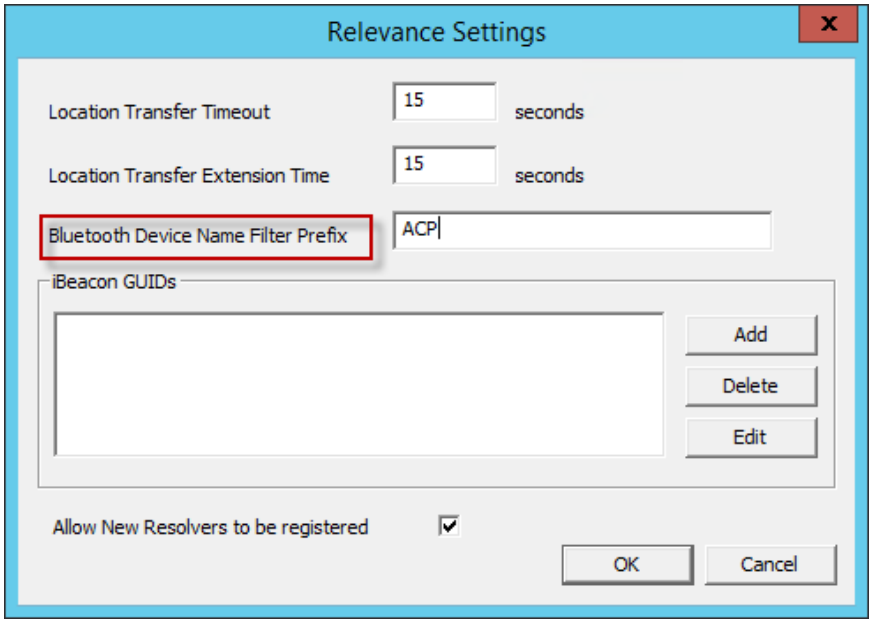
- ***Device Number*** – Add this module for each device added and assign each device a different number. ThinManager will sort out who is who.
- ***Advertising Mode*** – This allows you to set the transmitting mode of the USB adapter.
    - ***ACP*** – This sets the adapter to transmit in the ACP protocol
    - ***iBeacon*** – This sets the adapter to transmit in the iBeacon protocol. You will need to assign a UUID, a major number, and a minor number.
    - ***Disabled*** – This stops the transmission from the adapter.
- ***Advertising Name*** – This allows you to select what naming convention is used to identify the Bluetooth USB adapter.
    - ***ACP-{BD_ADDR}*** – This will transmit the Bluetooth address of the USB adapter with the ***"ACP-"*** prefix.

- ***ACP-{Terminal Name}*** – This will transmit the Terminal name of the client hosting the USB adapter with the ***"ACP-"*** prefix.
- ***BD-Address*** – This will transmit the Bluetooth address of the USB adapter.
- ***Terminal Name*** – This will transmit the Terminal name of the client hosting the USB adapter.
- ***Custom*** – This allows you to set a custom advertising name in the ***Custom Advertising Name (16 char max)*** field.

- ***Custom Advertising Name (16 char max)*** – This field allows you to set a **Custom Advertising Name** if ***Custom*** is selected in the Advertising Name drop-down. You are limited to 16 characters.
- ***Advertising Interval (Milliseconds)*** – This sets the frequency of the Bluetooth signal.
- ***UUID (iBeacon Only)*** – Each iBeacon has a Universally Unique Identifier (UUID). This allows you to associate your iBeacon to the Terminal if **iBeacon** was chosen in the ***Advertising Mode*** drop-down.
- ***Major Number (0-65535) (iBeacon Only)*** – This allows you to add the iBeacon major number for registration.
- ***Minor Number (0-65535) (iBeacon Only)*** – This allows you to add the iBeacon minor number for registration.

Note: iBeacon USB adapters normally have a UUID, a major number, and a minor number assigned to them. These need to be added to the Bluetooth Module in the appropriate fields..

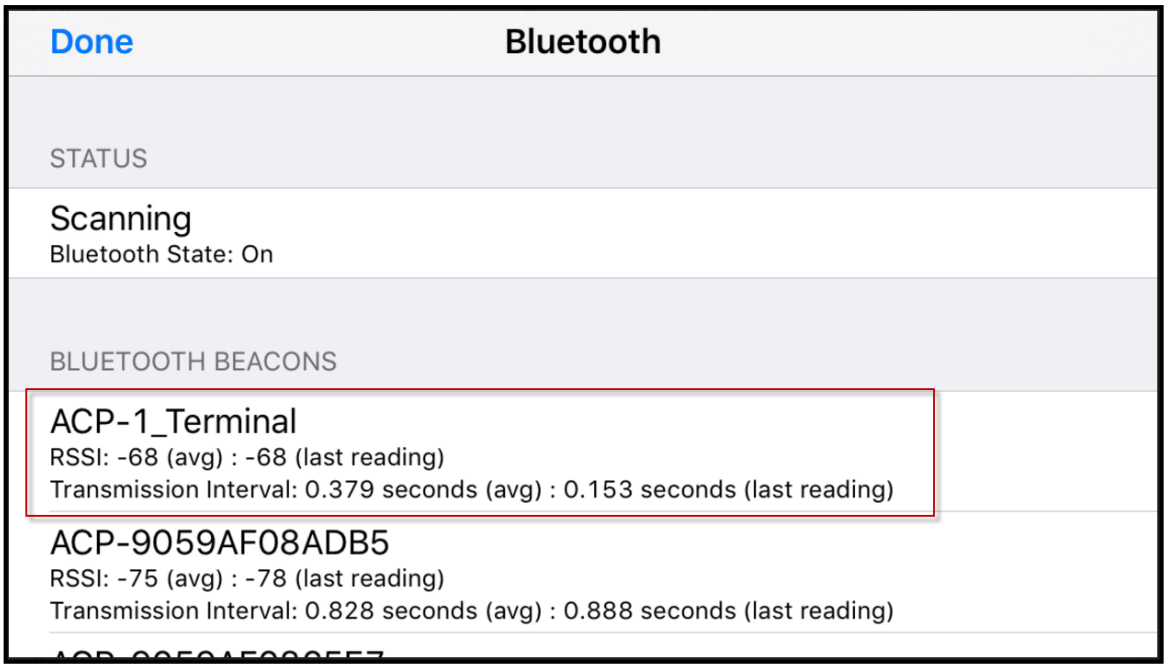
ThinManager® with Relevance® filters Bluetooth adapters by default and will only show Bluetooth beacons with the ACP prefix. If you use the BD-Address, Terminal Name, or Custom advertising names you will need to turn off the ACP filter. This is done on the Relevance Settings window.



Relevance Setting Window

The Relevance Settings Window is launched by selecting ***Manage > Relevance > Settings*** on the ThinManager menu bar.

Clear or change the Bluetooth Device Name Prefix if you use the BD-Address, Terminal Name, or Custom advertising names.



Bluetooth Beacons in iTMC Application

The iTMC application can show the Bluetooth beacons it is receiving.

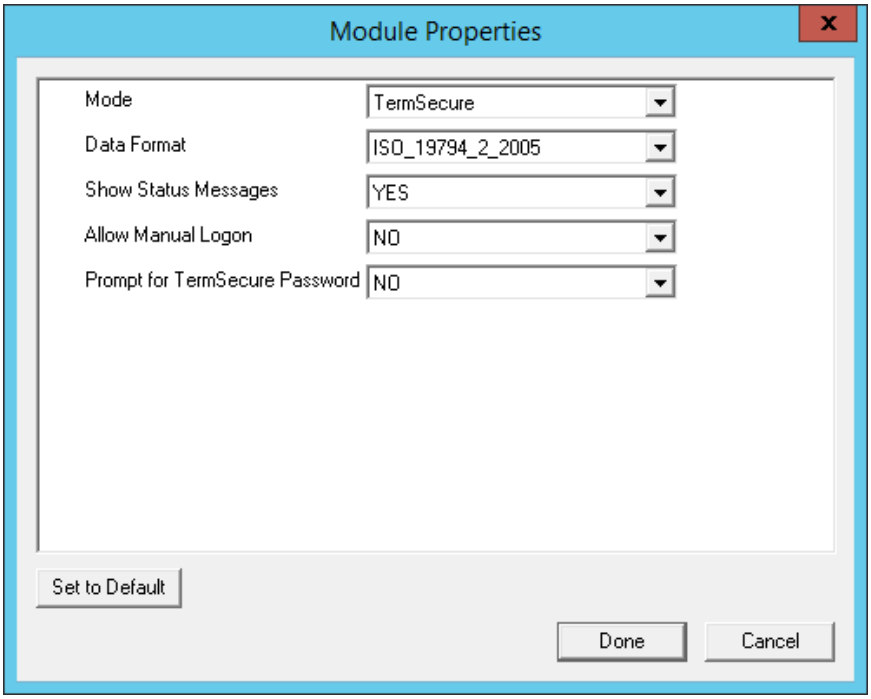
Select Menu in the upper right corner of the iTMC menu bar to launch the Main Menu. Select View Bluetooth Beacons to see the Bluetooth beacons.

This example shows a beacon using the ***ACP-{Terminal Name}*** advertising name.

24.7.2. DigitalPersona UareU Fingerprint Reader

ThinManager supports the DigitalPersona UareU Fingerprint Reader biometric reader from Crossmatch to add another element of security to a ThinManager system.

See Fingerprint Reader on page 568 for more details.



DigitalPersona UareU Fingerprint Reader Module

The **DigitalPersona UareU Module** has several settings:

- ***Mode*** – This allows you to use the reader with TermSecure, the TermMon ActiveX, or as a TermMon Lookup device.
- ***Data Format*** – This allows you to choose the data format used by the biometric reader.
- ***Show Status Messages*** – This will display activity messages in the upper right corner of the Terminal.
- ***Allow Manual Logon*** This can be set to ***No*** to require access only through the biometric device.
- ***Prompt for TermSecure Password*** – This will require a password in addition to finger print scan when set to ***Yes***.

Note: The ability to use a fingerprint scanner needs to be enabled by selecting the ***Support Finger Print Readers*** checkbox on the **Biometric Device Configuration** page of the **ThinManager Server Configuration Wizard**.
The data format is set on the **Biometric Device Configuration** page also.

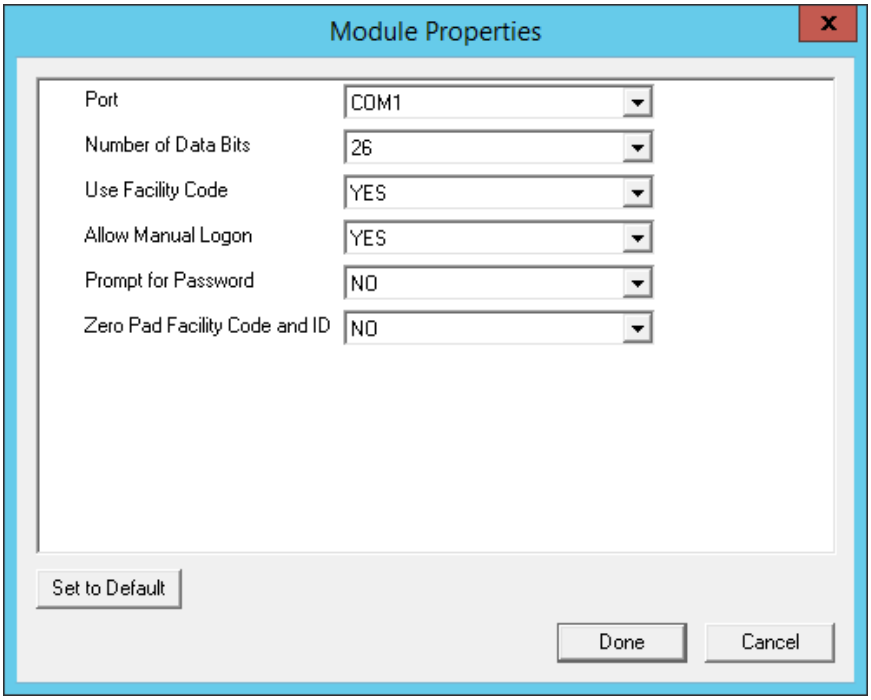
24.7.3. RF Ideas pcProx Modules

ThinManager supports card readers from RF Ideas for use with badges in TermSecure.

There is a serial RF Ideas pcProx Module and a USB RF Ideas pcProx Module.

24.7.3.1. Serial RF Ideas pcProx Module

This module is used with the RFIdeas pcProx Enroll Series 81 readers like RDR-xx81AKx.



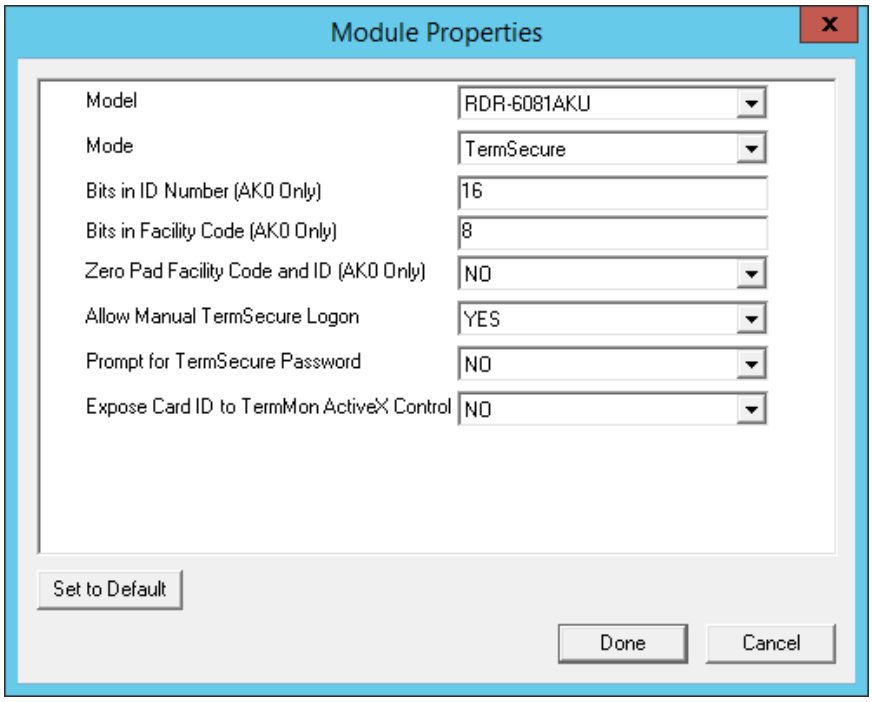
RF Ideas pcProx Module Parameters

The parameters are:

- **Port -** This selects the port that the RF Ideas pcProx card reader is installed.
- **Number of Data Bits –** Different cards use different numbers of data bits in their format. This sets the number of data bits to match that used by the card as an identifier. The choices are ***26***, ***37***, or ***Raw***.
- **Use Facility Code -** This value, when set to ***Yes***, will require the addition of the card's Facility Code to the Card / Badge ID number.
- **Allow Manual Login** - This, when set to ***Yes***, will allow a Relevance user to log into a Terminal without a TermSecure ID device. If set to ***No***, TermSecure users must use a TermSecure ID device to log in.
- **Prompt for Password** - This, when set to Yes, will require a TermSecure to enter their password for access, even if the password is configured in ThinManager.
- **Zero Pad Facility Code and ID** – This will add a zero to the number string. This is rarely needed.

24.7.3.2. USB RF Ideas pcProx USB Module

This module is used with the RDR-6081AKU , RDR-80582AK0, and RDR-80082AK0 USB RFIdeas pcProx readers.



RF Ideas pcProx USB Module

The parameters are:

The **RF Ideas USB pcProx Module** has parameters that can be configured:

- **Model -** This allows you to select between the **RDR-6081AKU**, **RDR-80582AK0**, and **RDR-80082AK0** USB pcProx card reader.
- **Mode –** This allows you to select between **TermSecure**, **Wedge**, and **TermMon** modes.
    - **TermSecure Mode** – This allows the card to be used with TermSecure as a login device.
    - **Wedge Mode** – This allows the data to be sent to the session as a character string.
    - **TermMon Mode** – This allows the data to be sent to the TermMon ActiveX.
- **Bits in ID Number (AK0 Only) –** Different cards use different numbers of data bits in their format. This sets the number of data bits to match that used by the card as an identifier.
- **Bits in Facility Code (AK0 Only) -** Different cards use different numbers of data bits in their format. This sets the number of data bits of the Facility Code.
- **Zero Pad Facility Code and ID (AK0 Only) –** This adds a leading 0 to the Facility Code if needed.
- **Allow Manual TermSecure Login** - This, when set to ***Yes***, will allow a Relevance user to log into a Terminal without a TermSecure ID device. If set to ***No***, TermSecure users must use a TermSecure ID device to log in.
- **Prompt for TermSecure Password** - This, when set to ***Yes***, will require a TermSecure to enter their password for access, even if the password is configured in ThinManager.
- **Expose Card ID to TermMon ActiveX Control –** Allows the card data to be sent to the TermMon ActiveX without using it as a Relevance User identifier.

To configure a parameter:

- Highlight the parameter.

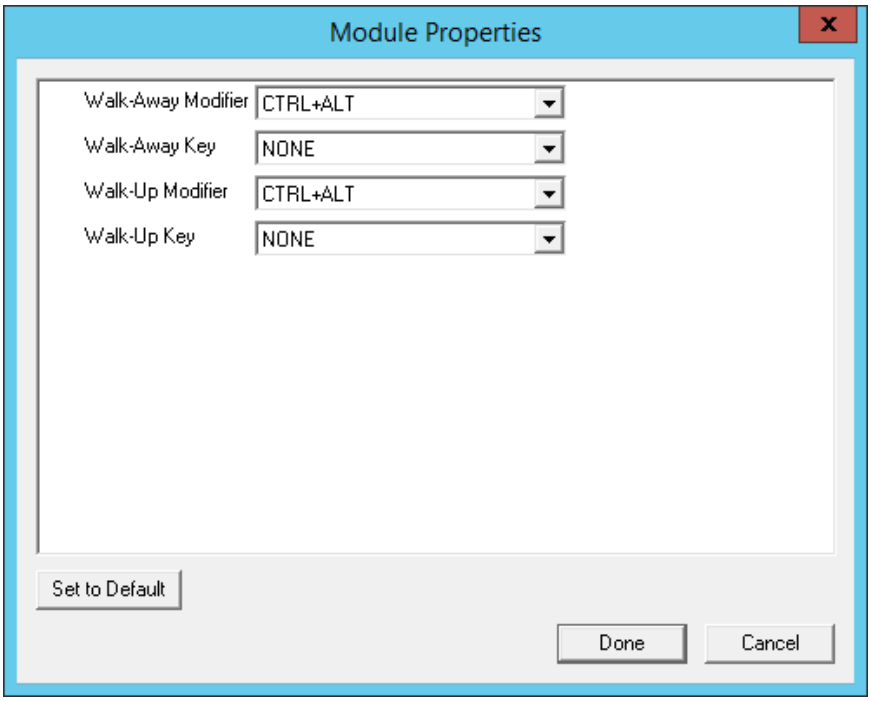
- Change the ***value***.
- Select the ***Set*** button to apply the new value.
- Select ***Done*** to accept the changes.

Once the Terminal has the module added it will need to restart to apply the changes.
Select the *Finish* button to close the Terminal Configuration Wizard.

Right click on the Terminal in the ThinManager tree and select *Restart*.

24.7.3.3. RFIdeas pcProx Sonar Module

RF Ideas has a sonar device that can be pointer to the operator. It becomes active when a Relevance User logs on and measured the time for a sonar echo. If the user walks away without logging off the sonar will detect the absence because of the increase in the time interval of the echo.



RFIdeas pcProx Sonar Module

The ***Walk-Away Modifier*** and ***Walk-Away Key*** allow you to use a key combination to trigger to turn the sonar off.

The ***Walk-Up Modifier*** and ***Walk-Up Key*** allow you to use a key combination to turn the sonar on.

24.7.4. TermMon ActiveX Configuration

This configures the TermMon ActiveX control that collects Terminal information and can perform Terminal functions.

Normally the TermMon ActiveX, when registered on a Remote Desktop Server, allows a Remote Desktop Server session to communicate with its Terminal and act upon it without the need of the TermMon ActiveX module. The TermMon ActiveX module can be added to the Terminal configuration to either deny the default Remote Desktop Server to Terminal access or to allow access to other sessions and PCs.

- ***Allow ActiveX Connections*** - This value, when set to ***Yes***, will allow the ActiveX control to function. Setting this value to ***No*** will prevent any ActiveX communication to the Terminal, including the default Remote Desktop Server to Terminal access.
- ***Only Allow Connections from Session*** - This value, when set to ***Yes***, will allow other Remote Desktop Server sessions and PCs to communicate to the Terminal with the ActiveX functions. If set to ***No,*** the only communication allowed is between the Terminal and a session on the Remote Desktop Server belonging to the Terminal, providing that the ***Allow ActiveX Connections*** is set to ***Yes***.

See TermMon ActiveX Control for details.

24.7.5. USB Flash Drive Module

The USB Flash Drive Module can be used to allow USB flash drives to be used as TermSecure ID devices. It is also listed under Local Storage modules.

See USB Flash Drive Module in the Local Storage Modules for details.

24.7.6. Wavetrend Tag Reader (Package 5 Only)

The **Wavetrend Tag Reader Module** allows a Terminal to use Wavetrend RFID cards as TermSecure ID cards. This allows a user to login through TermSecure when they approach the Terminal and logs them out when they leave the area. The distance required to login and log out are configurable in the module.

The parameters are:

Port - The WaveTrend Tag Reader Module connects to a thin client through the serial port. The ***Port*** setting specifies which COM Port the reader is attached to.

Use Vendor Code - This, if set to ***YES***, includes the vendor code as part of the identifier number.

Allow Manual Login - If set to ***YES***, this allows a Relevance User to use the hotkey to initiate logins, or the device. If set to ***NO***, it will force a Relevance User to use a device to login.

Prompt for Password - ***NO*** allows the device to login without a password. ***YES*** forces every Relevance User to enter a password after using the device.

Entry Signal Strength - The signal strength required to register the card as in range.

Exit Signal Strength - The signal strength required to register the card as out of range.

Entry Sensitivity - The number of reads above the Entry Signal Strength reads that are required to register as “Entered”.

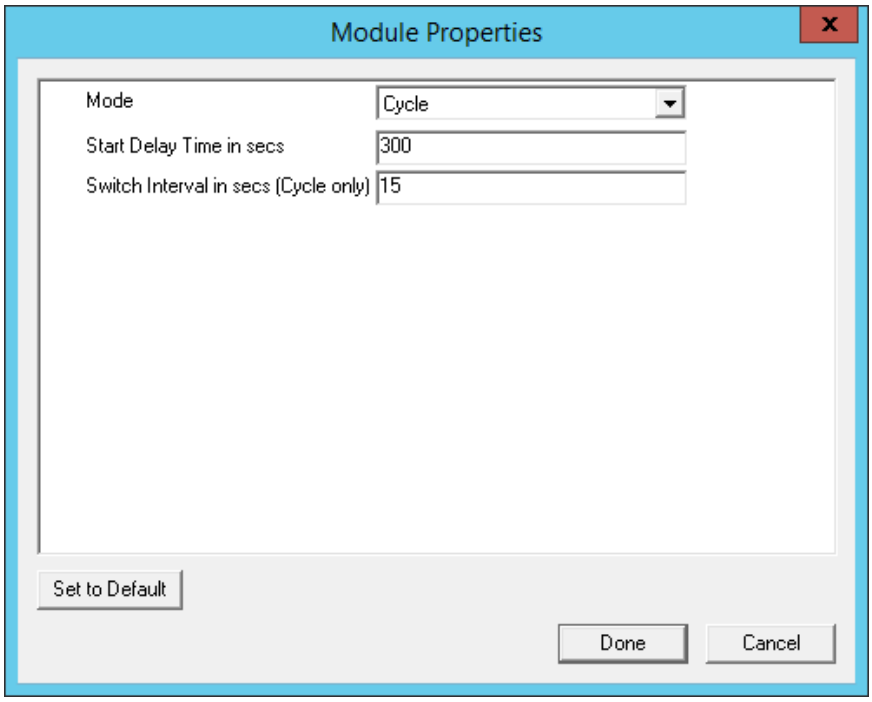
Exit Sensitivity - The number of reads below the Exit Signal Strength that are required to register as “Exited”.

24.8. Screen Saver Modules

It is recommended to use ThinManager Screen Savers because they run on the client. A Microsoft screen saver running in a session can utilize processing power that could be better applied to another session.

24.8.1. MultiSession Screen Saver Module

The **MultiSession Screen Saver Module** is a screen saver that allows a cycling of the different sessions of a MultiSession client.



MultiSession Screen Saver Module

The **MultiSession Screen Saver Module** has two modes. It can be set to cycle through the MultiSession windows when the Terminal is inactive, or it can be set to return to the main MultiSession screen when the Terminal is inactive.

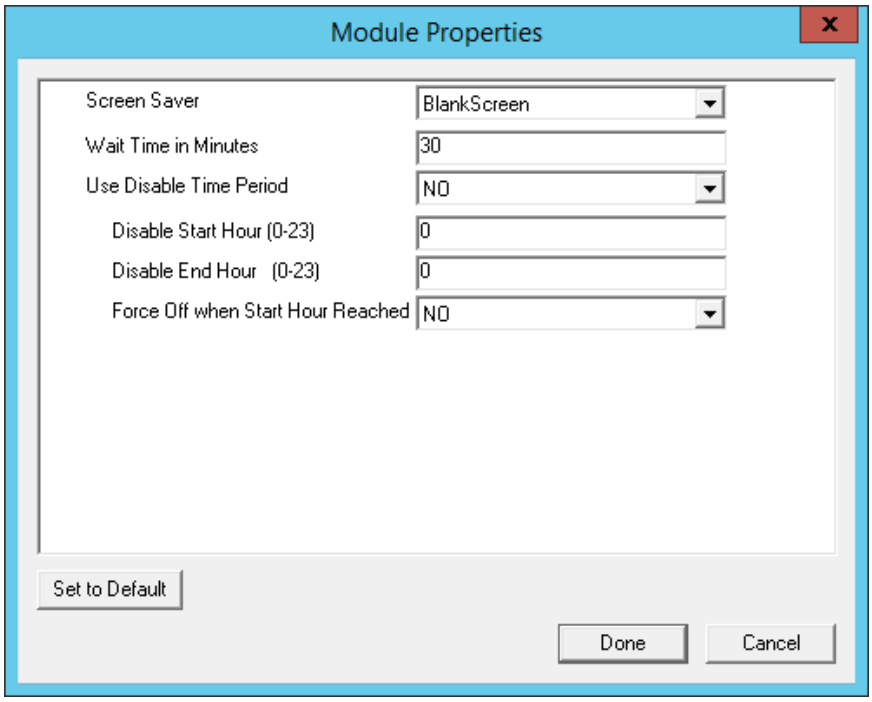
The parameters are:

- **Mode** - The **Cycle** mode will switch between all active sessions on the Terminal. The **GotoFirstGroup** mode will switch the Terminal to the main session when it is inactive.
- **Start Delay Time in secs** - This is the number of seconds of inactivity that the Terminal will allow before starting the screen saver.
- **Switch Interval in secs (Cycle only)** - This is the number of seconds that the Terminal will display each session when using the Cyclic mode.

24.8.2. Screen Saver Module

Screen Saver Module is a module that loads a screen saver on the client. The screen saver will run when the Terminal is idle to protect the monitor. Since the screen saver runs on the client, it saves CPU resources on the Remote Desktop Server.

This module has a Disable Time Period function that will disable the screen saver during working hours so that the screen is visible during the working hours.



Screen Saver Module Parameters

The **Screen Saver Module** configuration includes:

- ***Screen Saver*** - the graphic that is displayed when the screen saver is active.
- ***Wait Time in Minutes*** - the length of time that the Terminal needs to be idle before the screen saver starts.
- ***Use Disable Time Period*** - the screen saver can be set to be disabled or unavailable during a time block. This could be used to prevent the screen saver from running during normal business hours.
    - ***Disable Start Time (0-23)*** - This sets the start of the disabled time block. 0 is Midnight and 23 is 11:00 p.m.
    - ***Disable End Time (0-23)*** - This sets the end of the disabled time block. 0 is Midnight and 23 is 11:00 p.m.
    - ***Force Off when Start Hour is Reached*** - If set to ***Yes***, this will turn the screen saver off when the ***Disable End Time*** is reached.

24.9. Sound Modules

Many ThinManager Ready thin clients and ThinManager Compatible thin clients have audio ports for speakers.

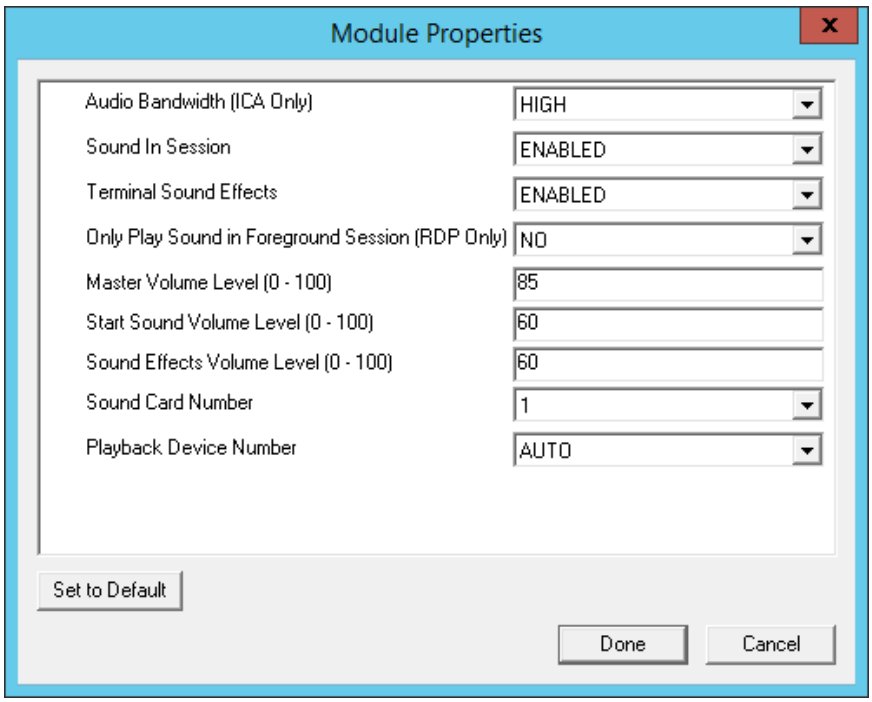
The use of sound from a thin client requires several things:

- Hardware with a Line Out/Speaker plug
- Amplified speaker(s)
- The Universal Sound Driver Module

Plug the speaker(s) into the Line Out plug on the Terminal, add the module, and connect to the Remote Desktop Server.

24.9.1. Universal Sound Driver

The **Universal Sound Driver Module** will activate ThinManager to send the correct sound driver for that Terminal. This module can be added to any thin client that has an audio jack to enable sound.



Universal Sound Driver Properties

The **Universal Sound Module** has several settings:

- ***Audio Bandwidth (ICA Only)*** - This parameter can be set to *Low*, *Medium*, or *High* bandwidth when using Citrix ICA.
- ***Sound in Session*** - This setting, when set to ***Enabled***, will allow sound generated within the session to be played through the Terminal. When this is set to ***Disabled*** the session sounds will be turned off but system sounds will still be generated during TermSecure login for audio feedback during the login process.
- ***Terminal Sound Effects*** - This setting, when set to ***Enabled***, will allow Terminal sound effects like TermSecure login sounds on the Terminal.
- ***Only Play sound in Foreground Session –*** This turns off the sound in background sessions when using MultiSession.
- ***Master Volume Level (0-100) –*** This sets the master volume for the Terminal.
- ***Start Sound Volume Level (0-100) -*** This sets the starting volume for the Terminal.
- ***Sound Effects Volume Level (0-100) –*** This sets the level for sound effects on the Terminal.
- ***Sound Card Number –*** This lets you specify which sound card to use if you have multiple sound cards.
- ***Playback Device Number –*** This lets you pick the playback device output of the sound card.

24.10. TermSecure Modules

There is a legacy category for TermSecure that has been superseded by the Relevance category.

The modules in the TermSecure list are identical to the modules in the Relevance list and can be seen at Relevance Modules on page 384.

The modules are:

- Bluetooth Module
- DigitalPersona UareU Fingerprint Reader
- Serial RF Ideas pcProx Module
- USB RF Ideas pcProx USB Module
- RFIdeas pcProx Sonar Module
- TermMon ActiveX Configuration Module
- USB Flash Drive Module
- USB ID Reader Module
- Wavetrend Tag Reader (Package 5 Only)

24.11. Touch Screen

ThinManager supports over a dozen serial touch screen controllers and a universal USB driver. You need to add the proper driver for the right controller. Some manufacturers are not consistent and use different controllers for different product lines.

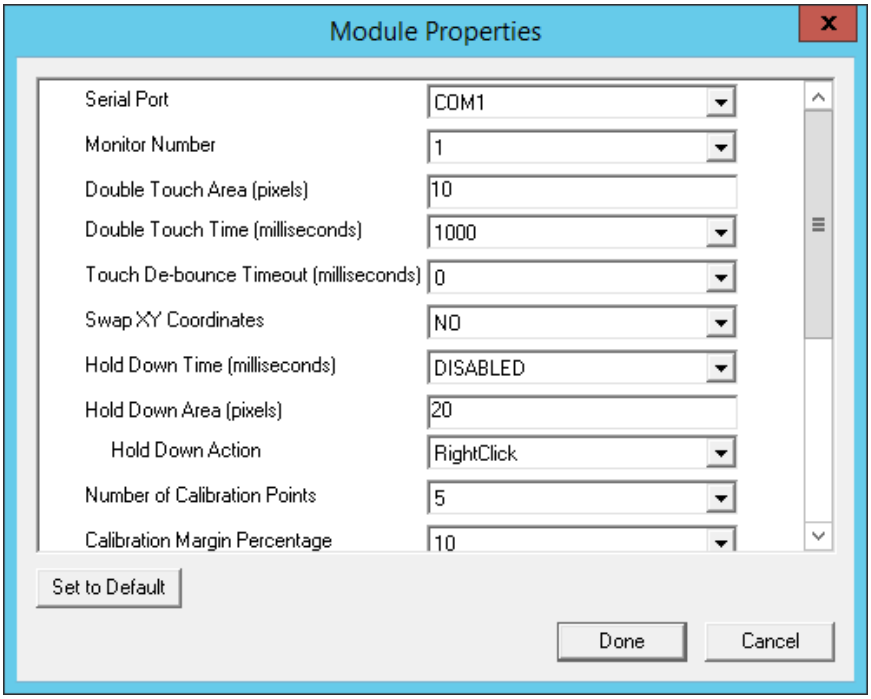
24.11.1. Serial Drivers

Each serial touch screen has a specific touch driver based on the touch controller of the monitor. You need to add the appropriate driver that matches the touch controller. ThinManager supports over a dozen serial touch screen controllers.

- Arista ARP-16XXXAP-ACP Touch Screen Driver
- CarrollTouch Touch Screen Driver
- Contec Touch Screen Driver (Package 5 only)
- DMC Touch Screen Driver (Package 5 only)
- DMC TSC Series Touch Screen Driver
- Dynapro Touch Screen Driver
- Elographics Touch Screen Driver
- Gunze AHL Touch Screen Driver
- Hampshire TSHARC Touch Screen Driver
- MicroTouch Touch Screen Driver
- Panjit TouchSet Touch Screen Driver
- PenMount Touch Screen Driver
- Ronics Touch Screen Driver (Package 5 only)
- Touch Control Touch Screen Driver
- Touch International IR Touch Screen Driver (Package 5 only)
- USB Touch Screen Driver
- Xycom 33XX Touch Screen Driver (Package 5 only)

- Zytronic Touch Driver

Note: The touch controller is the important component. May people make touch screen monitors but fewer make the controller. You need the module that matches the controller.



Serial Touch Screen Driver

Some, but not all, touch screen modules have parameters that can be modified. These may include:

Connection

- ***Serial Port*** – Sets the COM port that a serial touch screen is connected to.
- ***Baud Rate*** - Sets the speed used for communication between the Terminal and the touch screen on some serial touch screens.
- ***Monitor Number*** – Used to specify which monitor in a MultiMonitor scheme will use for the touch screen. MultiMonitor thin clients with multiple touch screens will need a module loaded for each touch screen used.

Touch Settings

- ***Double Touch Area (pixels)*** – This sets the size of the area that a second touch will register as a double touch.
- ***Double Touch Time (milliseconds)*** - The amount of time between touches that qualifies as a double touch.
- ***Touch De-Bounce Timeout*** - a time interval used to prevent a single touch from being registered as multiple touches.
- ***Swap XY Coordinates*** – If X and Y are reversed, this setting will correct the orientation.
- ***Hold Down Time (milliseconds)*** - This setting, when enabled, will initiate the **Hold Down Action** when the touch is held for the configured time

- ***Hold Down Action*** - This sets the action that a long touch will initiate. These include Right Click and OnBoard Keyboard.
- ***Hold Down Area (pixels)*** - This sets the size of the area that a second touch will register as a right click.

Calibration

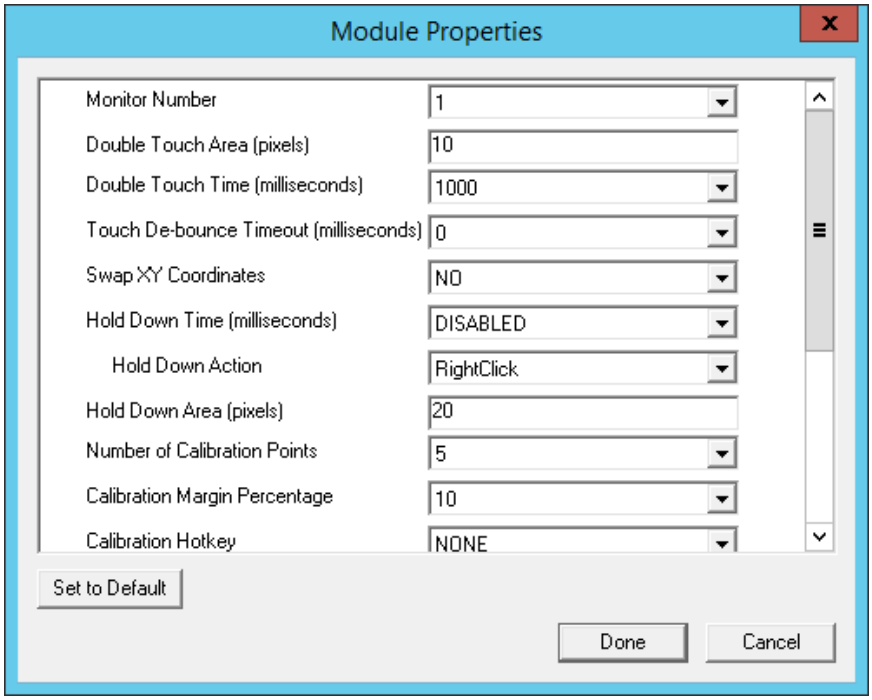
- ***Number of Calibration Points*** – This sets the number of calibration points that the calibration program uses during the calibration process.
- ***Calibration Margin Percentage*** – This sets the distance from the edge of the screen that the calibration points are displayed.
- ***Calibration Hotkey*** – This allows a function key to be set as a hotkey so that the calibration can be launched from a keyboard.
- ***Calibration Hotkey Modifier***– This setting adds ***CTL or ALT*** to the hotkey to launch the calibration from the keyboard, if desired.
- ***Calibration Hold Down Time (seconds)*** – This setting, when enabled, will launch the calibration program when the screen is touched and held for the assigned number of seconds. This cannot be used with the ***Right Click Hold Time***.
- ***Clean Time –*** This sets an idle time before the calibration to allow you to clean and wash a touch screen. The calibration will wait until you are done touching the screen while cleaning.
- ***Calibration (entered automatically)*** – This is set automatically by machine. These are the values set during the calibration process.

Miscellaneous

- ***Hide Mouse Cursor –*** This hides the mouse cursor if a mouse is not present.
- ***Orientation (entered automatically)*** - This is set automatically by machine. Used at the direction of Tech Support in error correction.

24.11.2. USB Touch Screen Driver

USB touch screens are easy to use as they use a standardized format. The USB Touch Screen Driver should work for all USB touch screens.



USB Touch Screen Module

Some, but not all, touch screen modules have parameters that can be modified. These may include:

Connection

- ***Monitor Number*** – Used to specify which monitor in a MultiMonitor scheme will use for the touch screen. MultiMonitor thin clients with multiple touch screens will need a module loaded for each touch screen used.

Touch Settings

- ***Double Touch Area (pixels)*** – This sets the size of the area that a second touch will register as a double touch.
- ***Double Touch Time (milliseconds)*** - The amount of time between touches that qualifies as a double touch.
- ***Touch De-Bounce Timeout*** - a time interval used to prevent a single touch from being registered as multiple touches.
- ***Swap XY Coordinates*** – If X and Y are reversed, this setting will correct the orientation.
- ***Hold Down Time (milliseconds)*** - This setting, when enabled, will initiate the **Hold Down Action** when the touch is held for the configured time
- ***Hold Down Action*** - This sets the action that a long touch will initiate. These include Right Click and OnBoard Keyboard.
- ***Hold Down Area (pixels)*** - This sets the size of the area that a second touch will register as a right click.

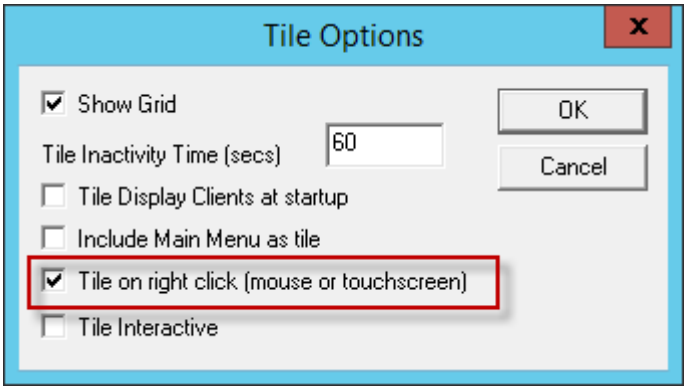
Calibration

- ***Number of Calibration Points*** – This sets the number of calibration points that the calibration program uses during the calibration process.
- ***Calibration Margin Percentage*** – This sets the distance from the edge of the screen that the calibration points are displayed.
- ***Calibration Hotkey*** – This allows a function key to be set as a hotkey so that the calibration can be launched from a keyboard.
- ***Calibration Hotkey Modifier***– This setting adds ***CTL or ALT*** to the hotkey to launch the calibration from the keyboard, if desired.
- ***Calibration Hold Down Time (seconds)*** – This setting, when enabled, will launch the calibration program when the screen is touched and held for the assigned number of seconds. This cannot be used with the ***Right Click Hold Time***.
- ***Clean Time –*** This sets an idle time before the calibration to allow you to clean and wash a touch screen. The calibration will wait until you are done touching the screen while cleaning.
- ***Calibration (entered automatically)*** – This is set automatically by machine. These are the values set during the calibration process.

Miscellaneous

- ***Hide Mouse Cursor –*** This hides the mouse cursor if a mouse is not present.
- ***Orientation (entered automatically)*** - This is set automatically by machine. Used at the direction of Tech Support in error correction.

The ***Right Click Hold Time (milliseconds)*** setting allows you to send a right click to the session. This can be used with the ***Tile on right click setting*** on the **Tile Options** window to allow a user to switch screens on a touch screen without keyboard or mouse.



Tile Options

The **Tile Options** page is found on the **Terminal Interface Options** page of the **Terminal Configuration Wizard**.

24.12. Video Driver Modules

The method of downloading video drivers was changed in ThinManager 3.0. In previous versions all of the video drivers were contained in the firmware and were downloaded at boot. In v3.0 the video was split out of the firmware and each thin client will only download the video driver that it needs.

One does not need to add the video module to the Terminal but only needs to have the video module installed in ThinManager to make it available. As each Terminal connects to ThinManager it will download the correct module.

These modules are normally installed with ThinManager. See Installing a Module to see how to update or add new modules.

24.12.1. Custom Video Mode Module

ThinManager Ready thin clients are designed for use with traditional computer monitors. The TermCap lists the standard resolutions for each Terminal. Some TVs, when used as a monitor, use a different non-traditional mode line. The **Custom Video Mode Module** allows a different set of parameters to be sent to the Terminal with use with the monitor.

This module is normally not needed and is used under direction of the ThinManager technical support staff.

24.12.2. Monitor Configuration Module

The **Monitor Configuration Module** allows the manual configuration of a monitor. This is generally used at the direction of ThinManager tech support as most monitors are supported automatically by ThinManager.

- ***Monitor 1 Connection Type*** – This allows you to select the connection type of your first monitor.
- ***Monitor 2 Connection Type*** – This allows you to select the connection type of your second monitor.
- ***Monitor 3 Connection Type*** – This allows you to select the connection type of your third monitor.
- ***Monitor 4 Connection Type*** – This allows you to select the connection type of your fourth monitor.
- ***Monitor 5 Connection Type*** – This allows you to select the connection type of your fifth monitor.
- ***Enable TwinView for nVidia Adapters*** – This enables TwinView.

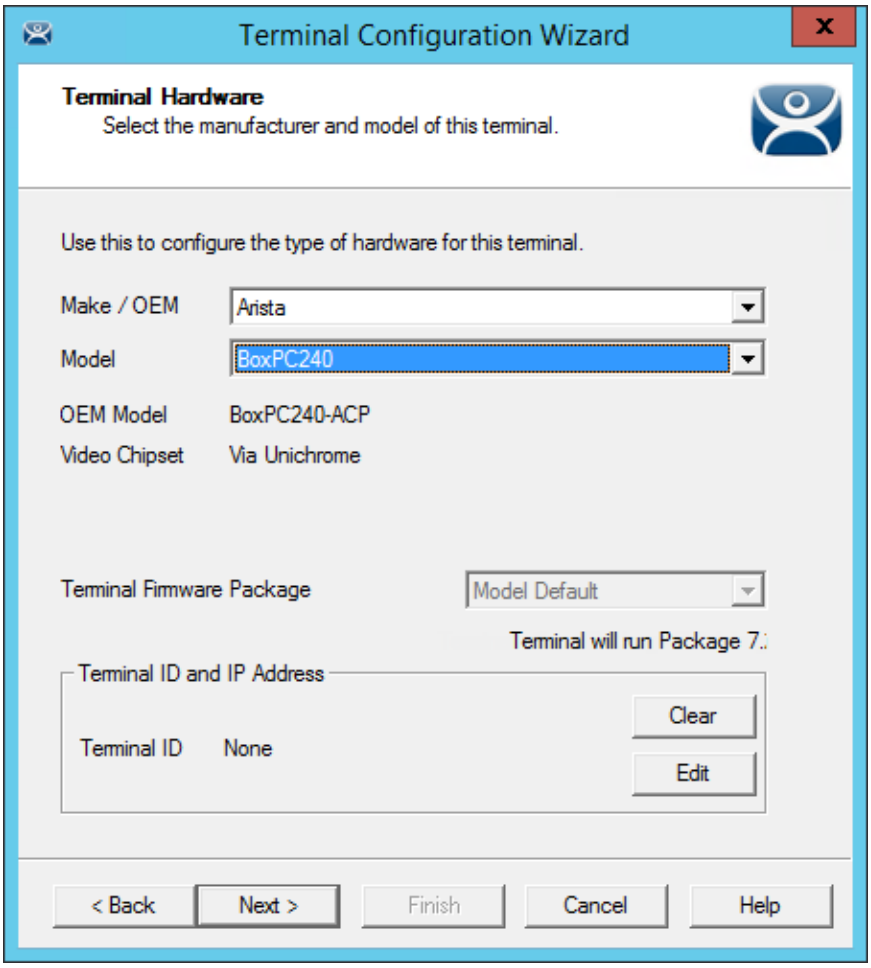
25. MultiMonitor

The **MultiMonitor** method uses specific ThinManager Ready thin clients that have multiple video ports built into the hardware. Each MultiMonitor thin client can have from two to five monitors attached. These monitors can be configured to merge into an expanded desktop (called "**spanned**" by ThinManager) or can display individual desktops (called "screened" by ThinManager), or combinations of "spanned" and "**screened**" sessions.

MultiMonitor Thin Client with Four Monitors

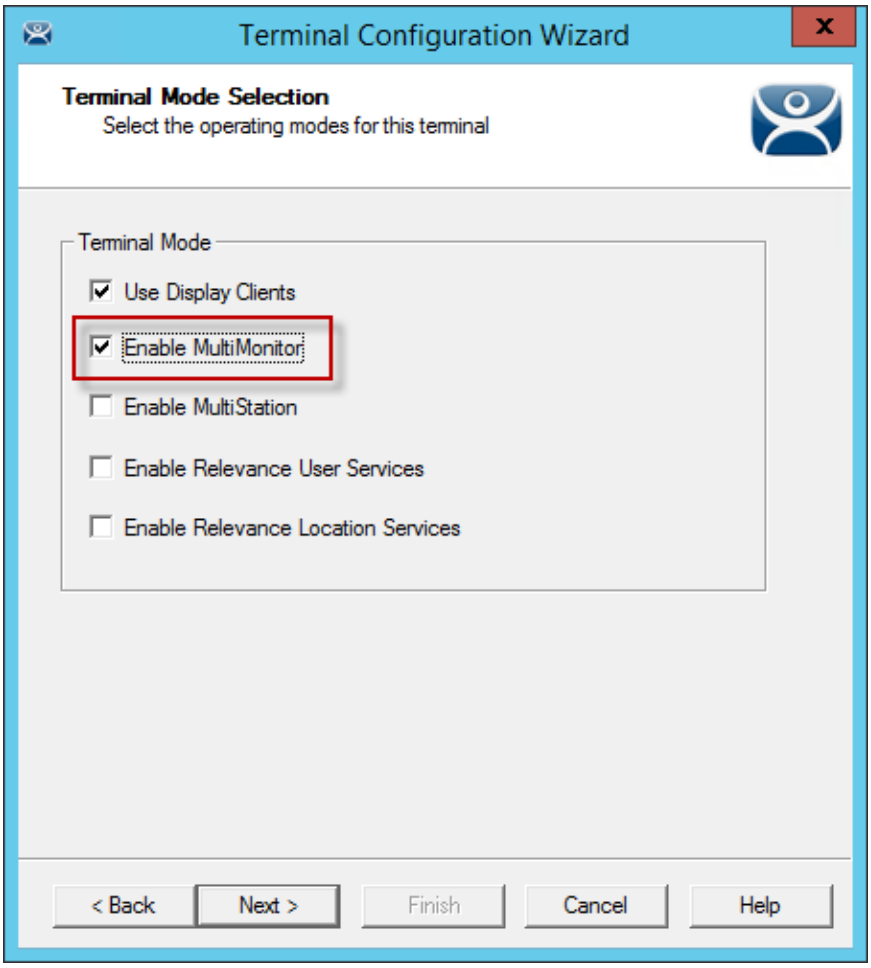
WinTMC supports MultiMonitor sessions on PCs that have Windows running on multiple desktops.

MultiMonitor is configured in the **Terminal Configuration Wizard** or the **Group Configuration Wizard**.



Terminal Hardware

MultiMonitor configuration is initiated in the **Terminal Configuration Wizard** when a MultiMonitor-capable thin client is selected on the **Terminal Hardware** page.



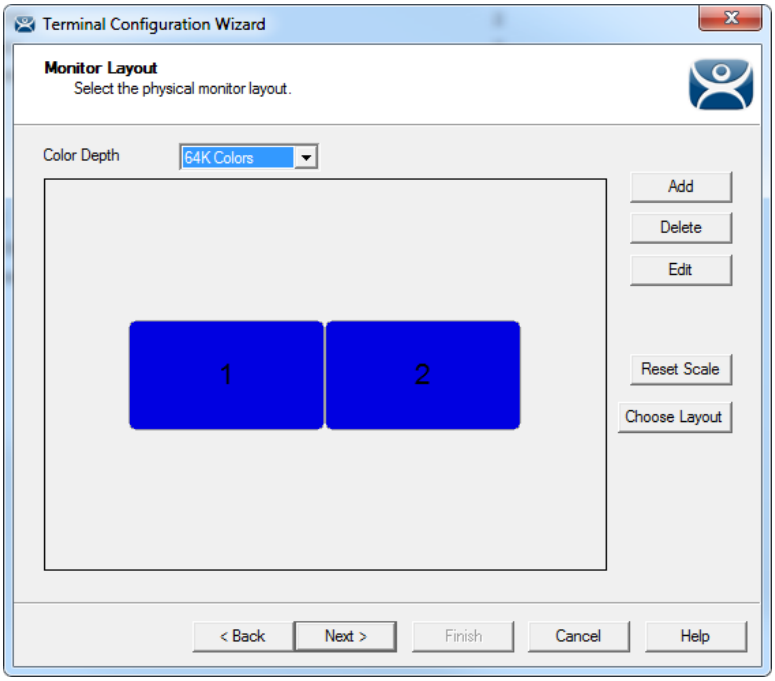
MultiMonitor – Enable MultiMonitors

MultiMonitor requires the use of Display Clients. Once the ***Use Display Clients*** checkbox is selected on the **Terminal Mode Selection** page, the ***Enable MultiMonitor*** checkbox becomes visible.

Select the ***Next*** button to continue to the **MultiMonitor Layout** page.

25.1. MultiMonitor Layout Page

The MultiMonitor configuration process changed in ThinManager 11.1. Additionally, ThinManager 11.2 added Portrait Mode.

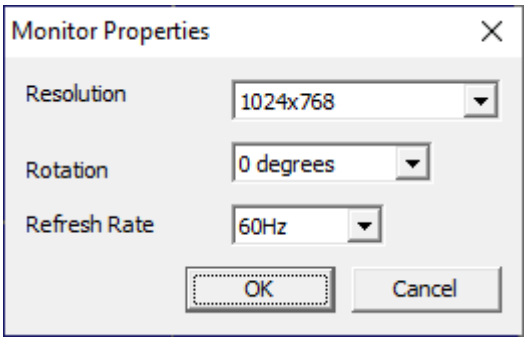


MultiMonitor – Monitor Layout

The default setting shows two monitors. You can add more as needed.

Buttons

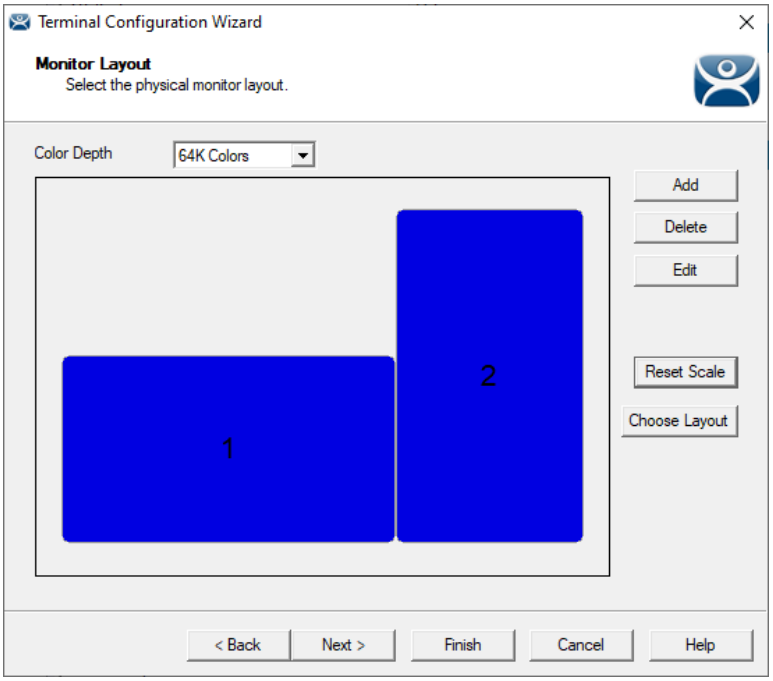
- ***Add*** – This button launches the **Monitor Properties** window and adds a new monitor.
- ***Delete*** – This button will delete a highlighted monitor.
- ***Edit*** – This button will open the **Monitor Properties** window of a highlighted monitor and allow the resolution to be changed.
- ***Reset Scale*** – This button will center the monitors in the configuration wizard. You can also use the scroll wheel of the mouse to zoom in and out.
- ***Choose Layout*** – This button will allow you to select from pre-created layouts. Otherwise you can drag monitors to a location.



Monitor Properties

The resolution of the monitor is set on the **Monitor Properties** dialog. Launching this window from the Add button will create and add another monitor.

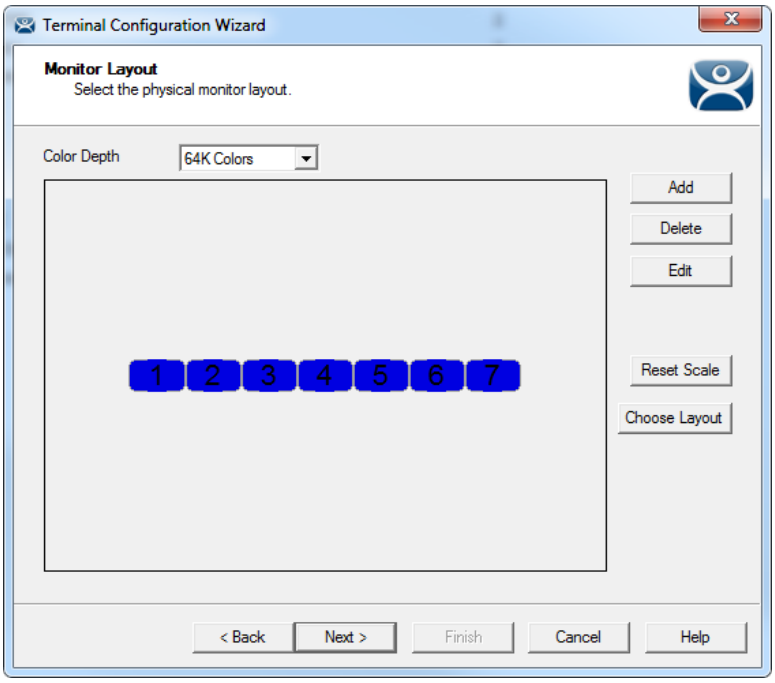
The **Rotation** drop-down allows you to select a rotation angle, setting the monitor to Portrait Mode.



Monitor Layout Page

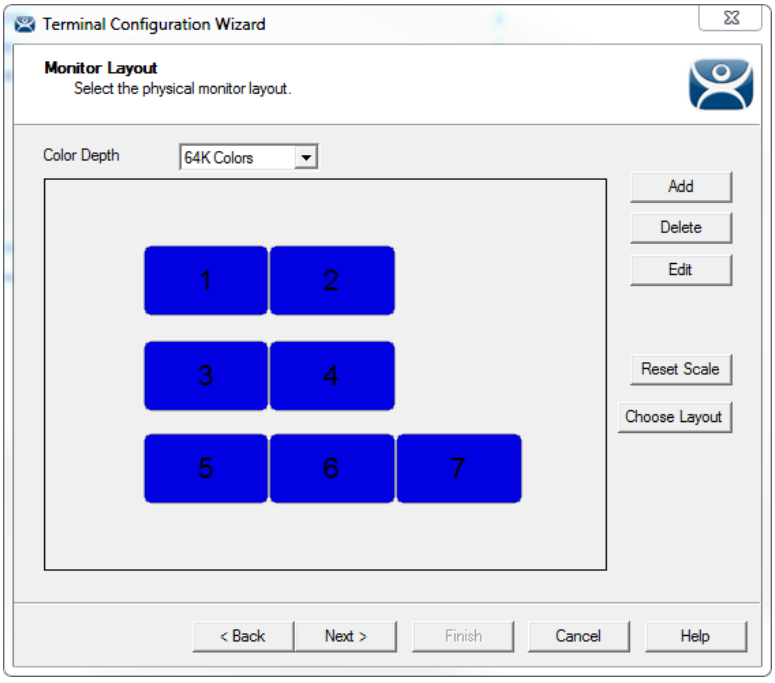
This example shows a dual monitor setup with the second monitor rotated 90 degrees for portrait mode.

Select the ***Next*** button to continue to the **Monitor Layout** page.



Monitor Layout Page

Once the needed number of monitors is added they can be moved by dragging.



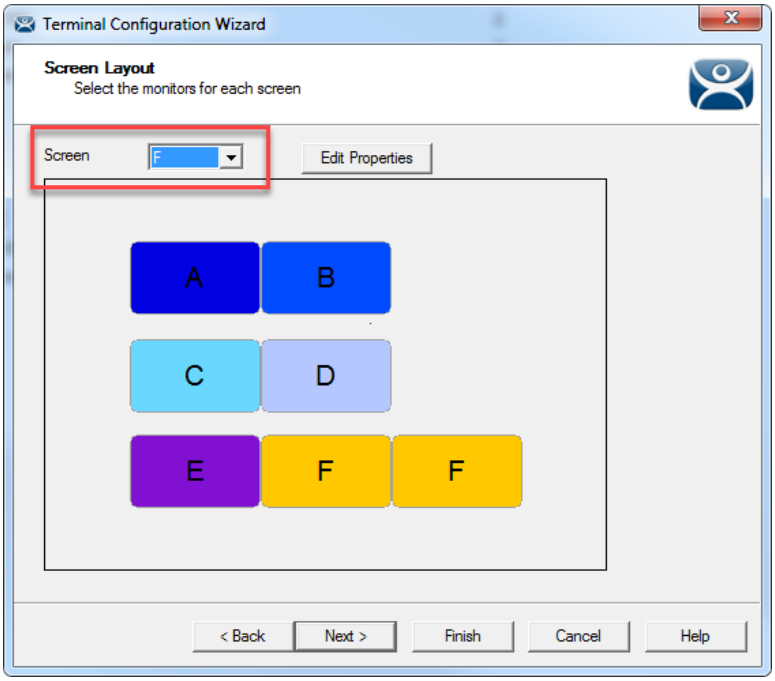
Monitor Layout - Rearranged

The **Screen Layout** page of the **Terminal Configuration Wizard** allows you to set whether a monitor shows a single session or is “spanned” to merge several monitors into one desktop.

Spanned monitors must form a rectangular shape and have the same resolution.

All the monitors will start as **Screen A**.

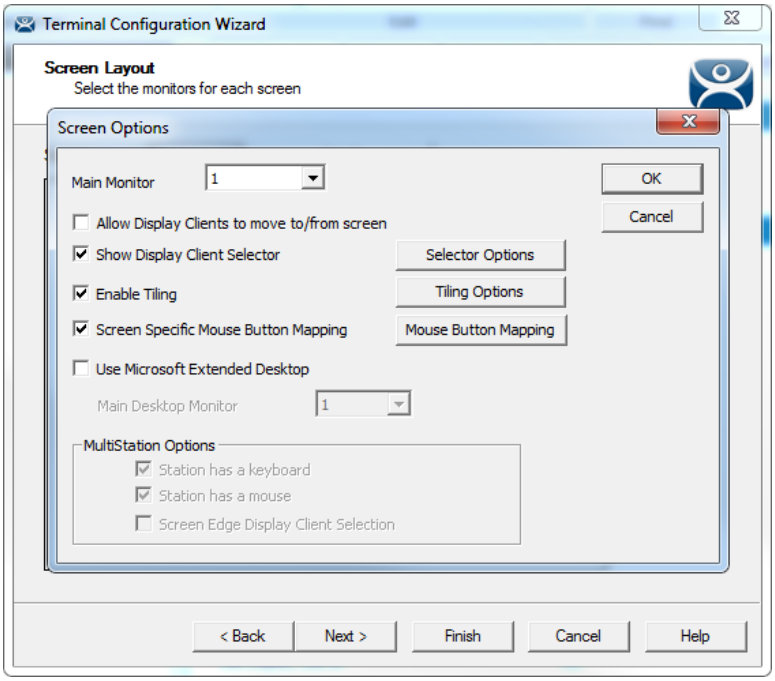
To change a monitor letter designation select the screen letter from the **Screen** drop-down and then select a monitor icon. This will apply the monitor letter to the screen.



Monitor Layout – Screen Letters Assigned

Monitors can share a desktop if they have the same letter designation. They must be the same resolution and form a rectangle; they can't be askew.

The ***Edit Properties*** button will launch the **Screen Options** window to configure the monitor properties.



Screen Options Window

The ***Edit Properties*** button will launch the **Screen Options** window.

The ***Reset Scale*** button will make the monitor configuration easier to see once in order.

- **Main Monitor** – This sets which monitor will have the mouse focus on boot and will display the Relevance Main Menu.
- **Allow Display Clients to move to/from screen** – This checkbox allows you to move Display Clients from monitor to monitor by allowing you to open the Display Client in a different monitor.
- **Show Display Client Selector** – This checkbox will make the drop-down Group Selector present.
    - **Selector Options** – This button opens the **Display Client Selector Options** window.
        - **Auto-hide Selector** – This hides the Group Selector drop-down when checked. Unchecking it will show the Group Selector.
        - **Tile on Selector Activation** – This checkbox, if selected, will tile the sessions when an auto-hid selector is activated.
        - **Select Menu Size** – This drop-down allows you to change the size of the Group Selector.
- **Enable Tiling** – This checkbox will show all Display Clients assigned to a monitor in a tiled mode if selected. Selecting one tile will make it full monitor.
    - **Tile Options** – This button opens the **Tile Options** window that configures tile options.
        - **Show Grid** – This checkbox will display gridlines when it is tiled.
        - **Tile Activity Time (secs)** – This field sets the time before the monitor reverts to tiled mode when a single screen is showing.
        - **Tile Display Clients at start up** – This checkbox configures the monitor to show the display clients in tiled mode at startup.
        - **Include Main Menu as tile** – This checkbox will add a tile with the Main Menu in it. This is handy for terminals with touch screens.
        - **Tile Interactive** – This checkbox changes the behavior of the mouse. Instead of switching from tiled mode to a single display client it allows the use to click into the tiled session and use the session in the tiled mode.
- **Screen Specific Mouse Button Mapping** – This checkbox allows you to assign actions to mouse buttons.
    - **Mouse Button Mapping** – This button opens the **Mouse Button Mapping** window.
        - Each button can be configured with a different action. These include
            - *Calibrate Touch Screen*
            - *Tile*
            - *Swap*
            - *Full Screen*
            - *Go to next display client*
            - *Go to previous display client*
            - *Log on Relevance user*
            - *Main Menu*

- *Left Mouse Button*
- *Right Mouse Button*
- *Middle Mouse Button*
- *Scroll Up*
- *Scroll Down*
- *Virtual Keyboard*
- *Disable Button*

Touch Screen Modules had a Hold Time that can convert a long touch to a right click. Using the Mouse Mapping Button feature allow you to apply any of these actions to the long hold.

- **Use Microsoft Extended Desktop** – This checkbox will apply the Microsoft Extended Desktop to a spanned set of monitors.
  With the Microsoft Extended Desktop an expanded application will stop at the monitor boundary as it does in Windows.
  Without the Microsoft Extended Desktop an expanded application will fill the entire desktop.
- **Main Desktop Monitor** – This checkbox sets which monitor of a spanned set will be the primary desktop.
- MultiStation Options – This applies to MultiStation, a feature where a MultiMonitor thin client can support several users by adding multiple keyboards and mice. It is turned on by selecting the selecting the *Enable MultiStation* checkbox on the **Terminal Mode Selection** page of the **Terminal Configuration Wizard**.
  - **Station has a keyboard** – Use this checkbox if you are using a keyboard with MultiStation.
  - **Station has a mouse** – Use this checkbox if you are using a mouse with MultiStation.
  - **Screen Edge Display Client Selection** – This checkbox allows you to switch between display clients by moving the mouse to either edge of the monitor.

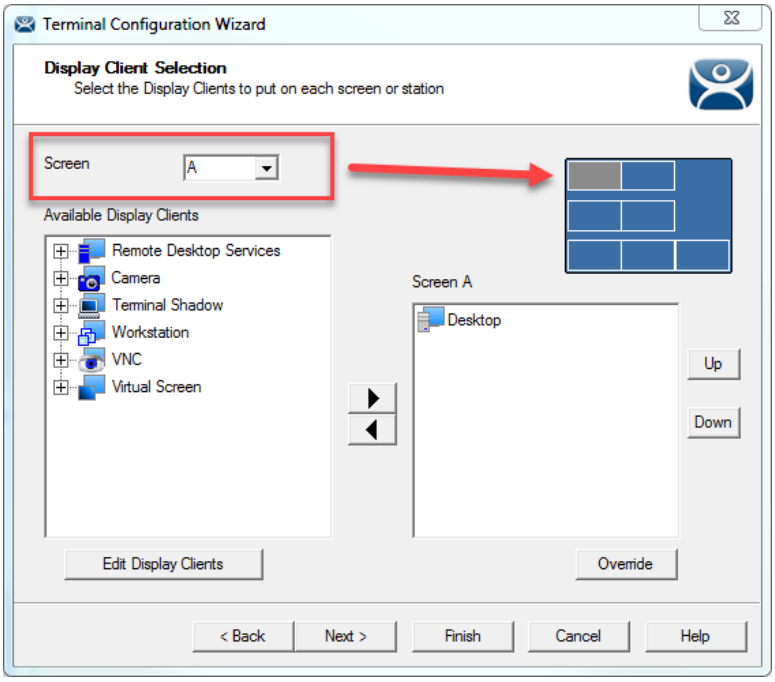
Note: The desktop of a spanned session is limited to **4096x2048** in Server 2008 R2 and earlier. The resolution of a Server 2012 is **8196 x 8196**. The ***Use Session Size Limits*** drop-down on the MultiMonitor Video Setting page allows you to change to this higher resolution.

The selection of monitor resolution on the **MultiMonitor Video Settings** page can affect the number of monitors that you can add to a spanned session.

Select the ***Next*** button to continue.

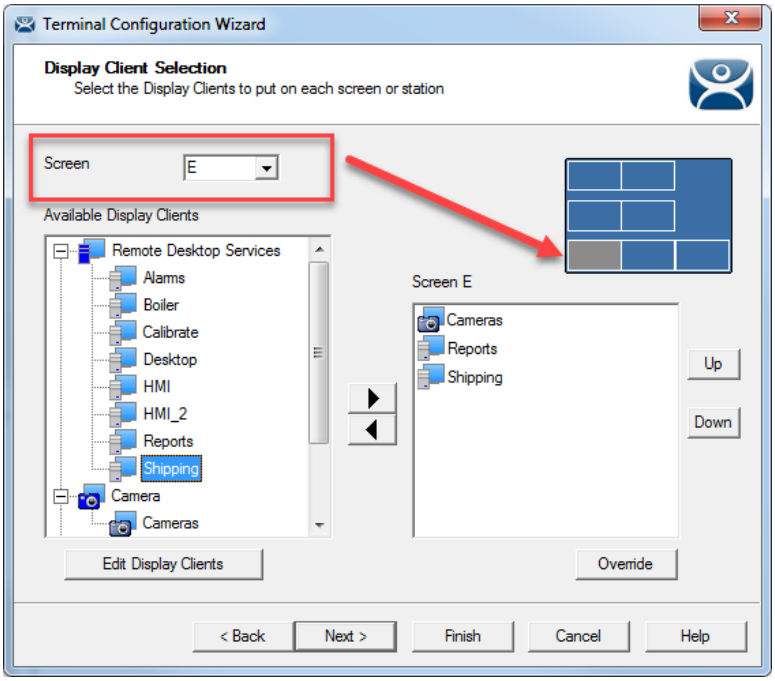
Display Clients are assigned to the screens on the **Display Client Selection** page of the **Terminal Configuration Wizard**.

25.2. MultiMonitor Display Client Selection Page



Display Client Selection

Use the **Screen** drop-down to select the screen and add a display client by moving it into the **Screen "X"** list.



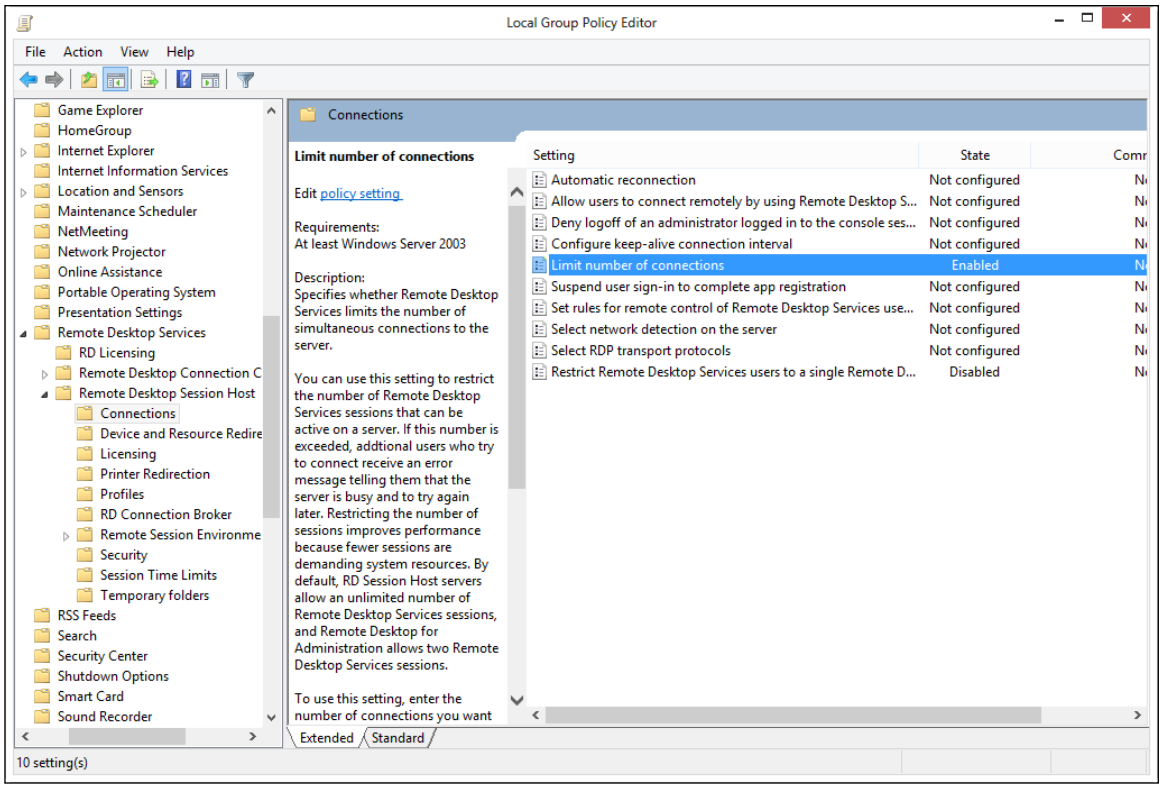
Change the screen letter in the **Screen** drop-down to select a different screen to apply the display client to that screen. The icon of the screen will change colors to show which screen is being edited.

Multiple display clients can be added to each screen.

The *Override* button launches the **Override Settings** window where the display client can have customized settings applied.

25.3. Override Function

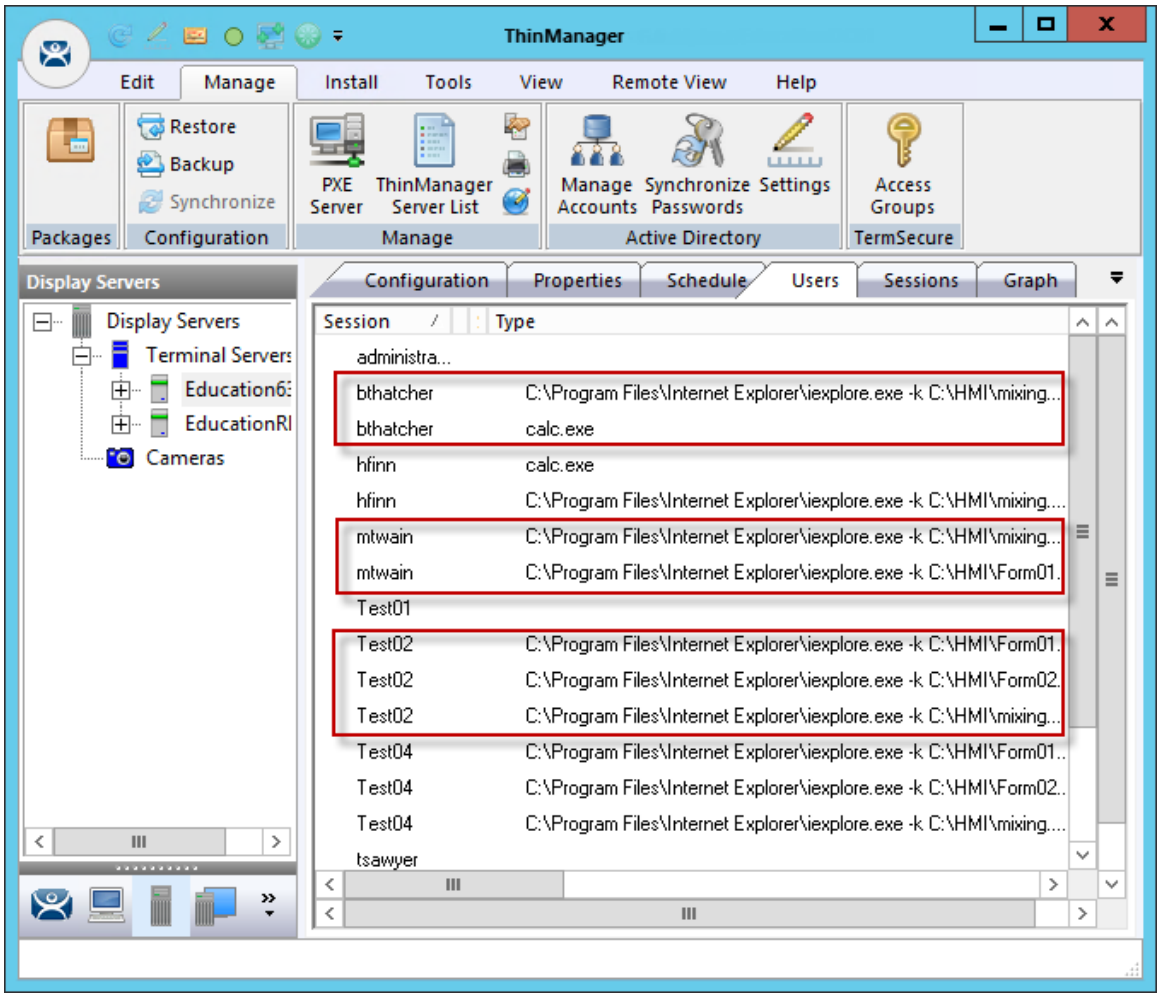
Microsoft restricts each user to a single session on a server by default. It is smart to keep this setting to prevent conflicts. If it is disabled then a user creates multiple sessions consuming licenses and resources and making it more difficult to connect to the proper session.



Limit Number of Sessions

MultiMonitor has an ***Override*** function that allows Display Clients on a MultiMonitor thin client to login with different user accounts or video resolutions. This prevents the monitors from fighting over a single session.

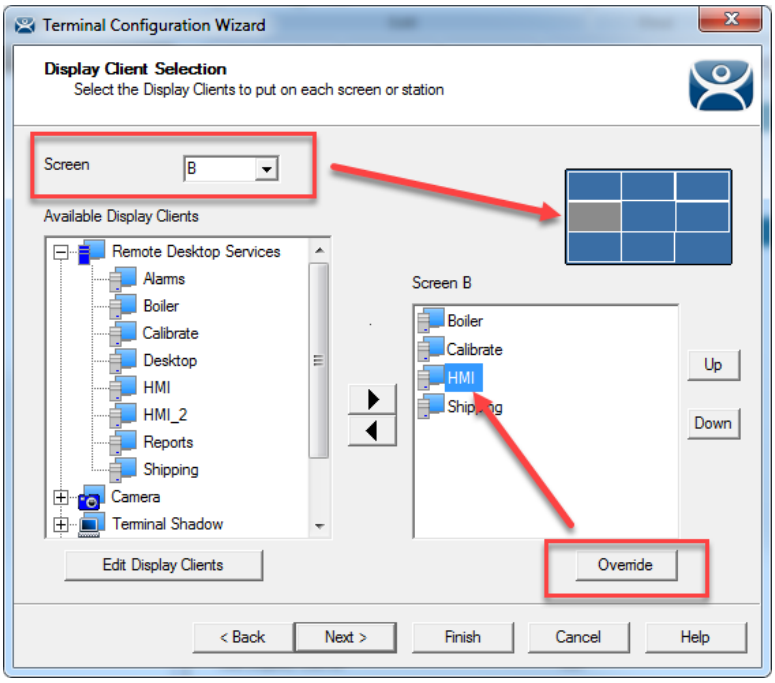
This may be needed to run duplicate copies of a program on the same thin client.



Users on a Remote Desktop Server

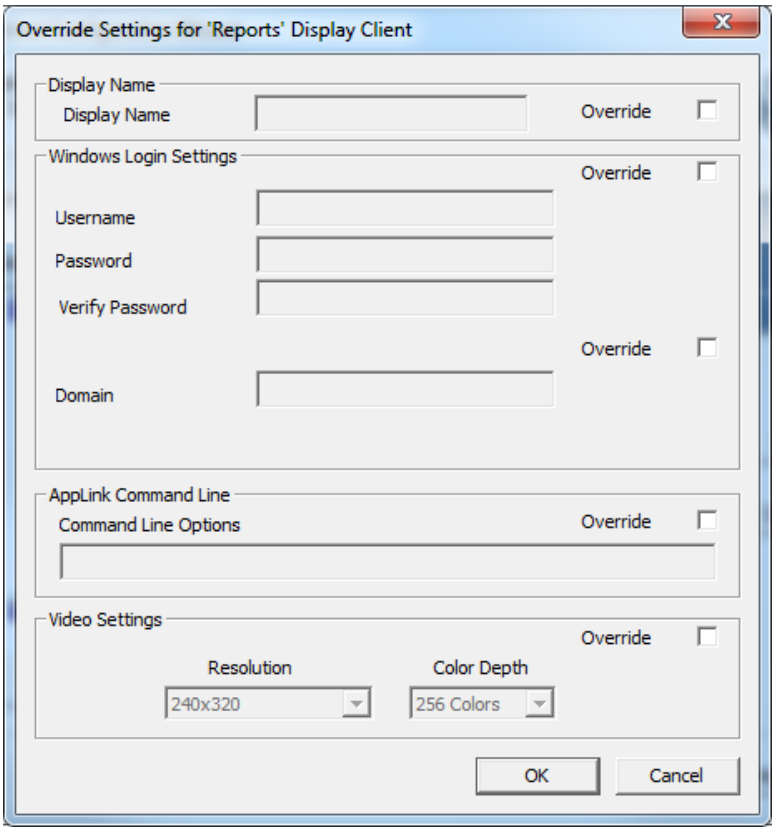
In reality a user can log into a Remote Desktop Server multiple times as long as they are running different applications. Each ***Username/Application*** needs to be unique.

If you want to run the same application twice you will have a problem. This is a common desire on MultiMonitor displays. The ***Override*** function solves this issue.



Override Button on the Display Client Selection Page

Highlight a Display Client assigned to the MultiMonitor thin client on the **Display Client Selection** page. Select the ***Override*** button to launch the **Override Settings** window.

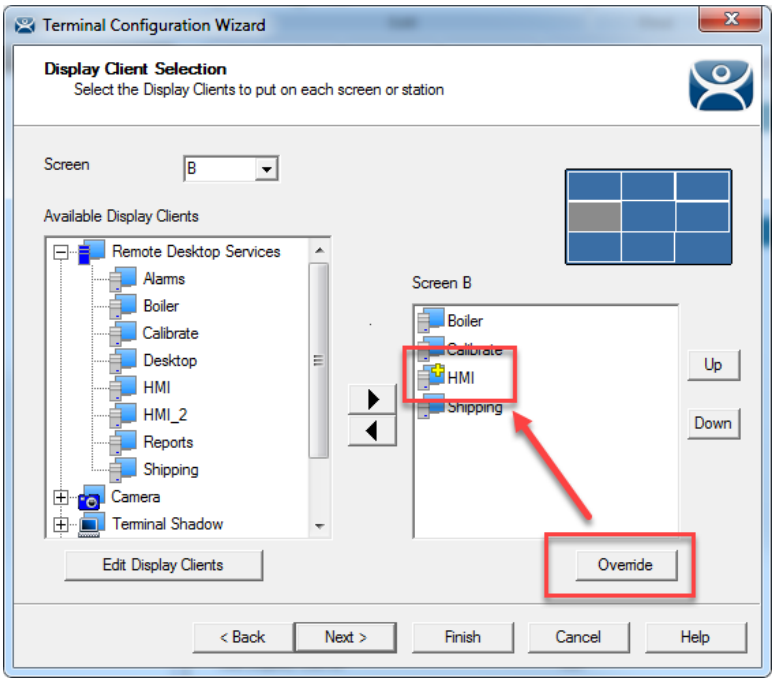


The **Override Settings** window is launched when a display client is highlighted and the *Override* button is selected.

Selecting an **Override** checkbox activates the override setting and allows customization.

- **Display Name** – This allows the display client to show a different name that the one originally listed.
- **Windows Login Settings** – This allows different credentials to be used for the display client.
- **AppLink Command Line** – This field allows different command line parameters to be applied to the program.
- **Video Settings** – This allows the resolution of the display client to be changed from the monitor setting.

Note: Using multiple user accounts on a Terminal doesn't affect the **"Per Device" TS/RDS CAL** count but will require more **"Per User" TS/RDS CALs**.



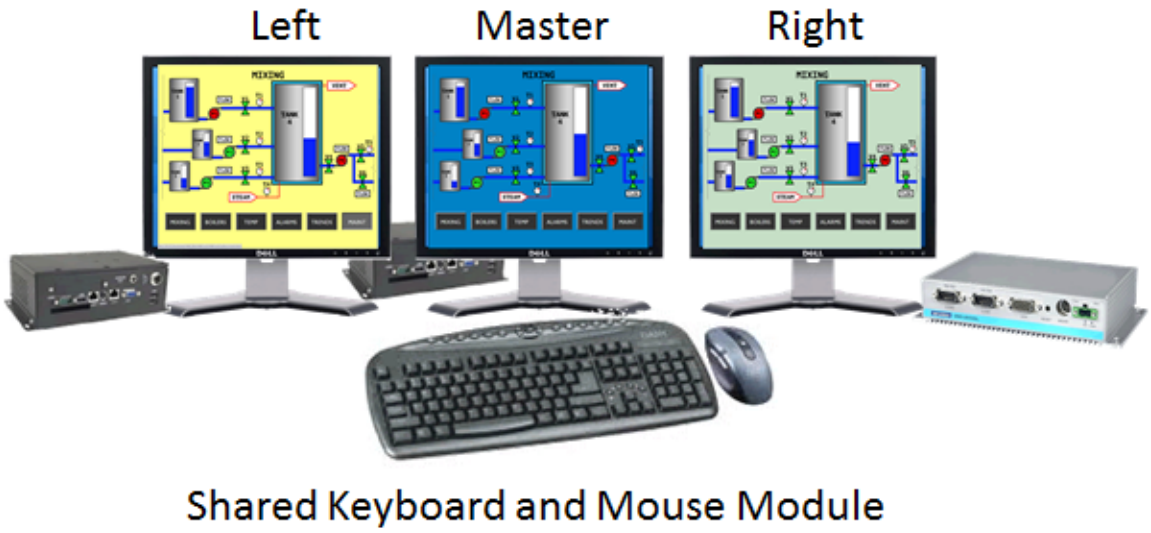
Display Client Selection

This shows the ***Override*** button and the **Plus** icon for a Display Client that has its properties overridden.

Repeat for any display client that requires a different user account.

25.4. Share Keyboard and Mouse Module

The Share Keyboard and Mouse module allows several ThinManager Ready thin clients to be controlled with a single keyboard and mouse without the need of a KVM switch (Keyboard/Video/Mouse).



Shared Keyboard and Mouse Layout

The **Share Keyboard and Mouse** can be used by placing several monitors connected to ThinManager Ready thin clients side-by-side or top-to-bottom. The **Share Keyboard and Mouse Master module** is loaded on the center thin client. This module is configured by adding the IP addresses of the secondary slave thin clients. The other Terminals receive the **Share Keyboard and Mouse Slave module**.

Place three Terminals and their monitors side-by-side.

25.4.1. Master Thin Client Configuration

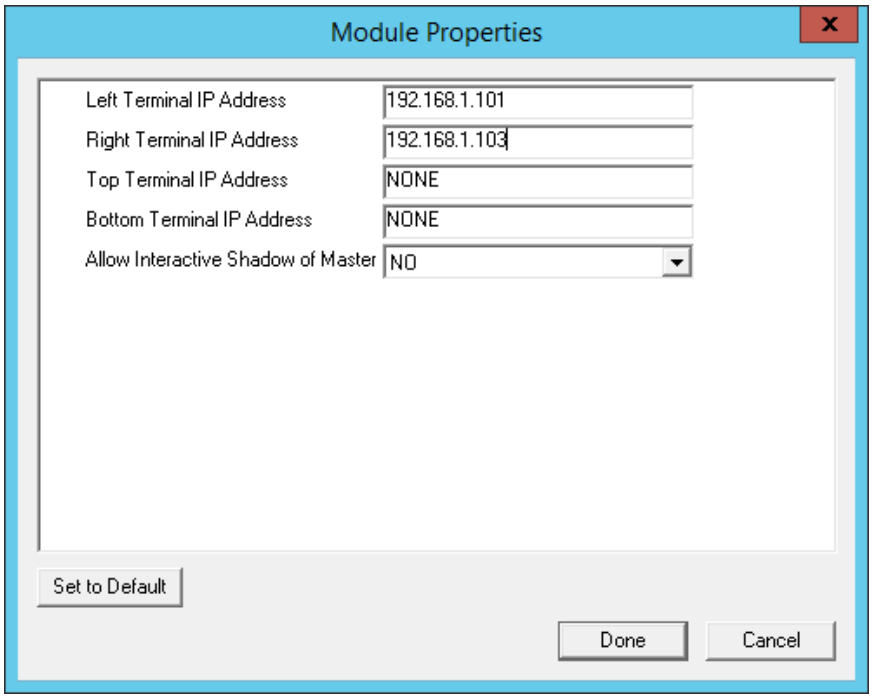
One thin client needs to be configured as the Master. It is the dominant Terminal whose keyboard and mouse will be used to control the grouped Terminals.

Open the **Terminal Configuration Wizard** for the center Terminal by double clicking on it in the ThinManager tree.

Navigate to the **Modules Selection** page by selecting the ***Next*** button.

Select the ***Add*** button and select the **Share Keyboard and Mouse Master module**.

Highlight the **Share Keyboard and Mouse Master module** and select the ***Configure*** button to launch the **Module Properties** window.



Share Keyboard and Mouse Master Module

The Share Keyboard and Mouse Master module has a few settings.

- ***Left Terminal IP Address –*** Enter the IP address of the left Terminal, if present.
- ***Right Terminal IP Address –*** Enter the IP address of the right Terminal, if present.
- ***Top Terminal IP Address –*** Enter the IP address of the top Terminal, if present.
- ***Bottom Terminal IP Address –*** Enter the IP address of the bottom Terminal, if present.
- ***Allow Interactive Shadow of Master -*** This controls whether the master Terminal is allowed to be controlled by a remote user.

Select the **Done** button and restart the ThinManager Ready thin client to apply the changes.

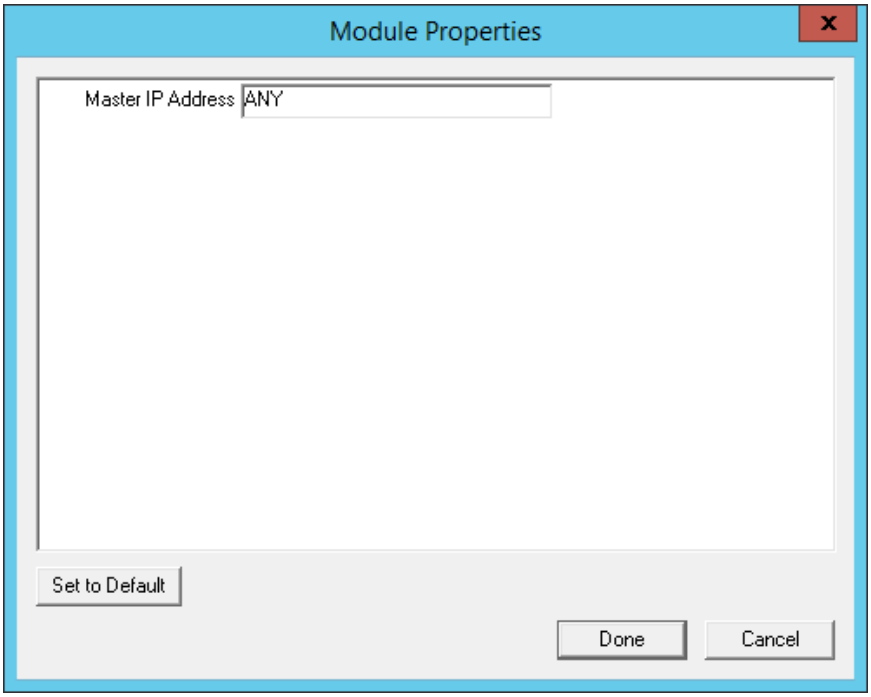
25.4.2. Slave Thin Client Configuration

The other Terminals in the group need the ***Slave*** module.

Open the **Terminal Configuration Wizard** for the each Terminal by double clicking on it in the ThinManager tree.

Navigate to the **Modules Selection** page by selecting the ***Next*** button.

Select the ***Add*** button and select the **Share Keyboard and Mouse Slave** module.



Share Keyboard and Mouse Master Module Properties

The **Share Keyboard and Mouse Slave** module has one parameter that allows the slaves to point to a master.

- ***Master IP Address –*** If set to ANY then this Terminal can be added to several master Terminals and controlled from any. To prevent confusion a single master Terminal can be defined in the field.

Select the ***Done*** button and restart the ThinManager Ready thin client to apply the changes.

Once the ThinManager Enabled thin clients are booted, the mouse on the master thin client can be moved seamlessly into the other desktops. The keyboard will be active in the screen the mouse pointer is on.

This allows an operator to have control of several displays with only one keyboard and mouse. The mouse movement is seamless, allowing access to displays without switching.

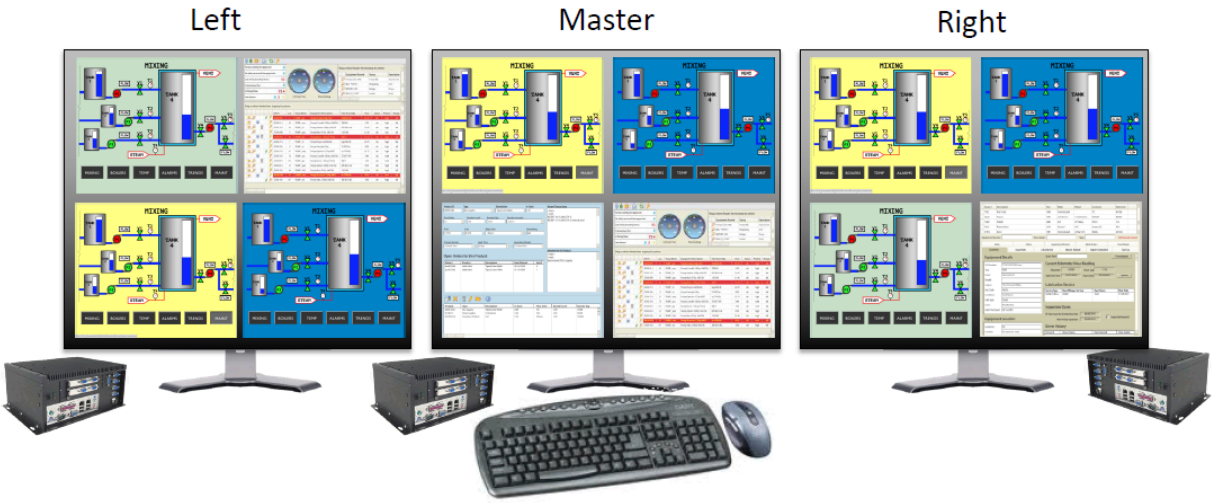
Note: A Master Share Keyboard and Mouse session cannot be interactively shadowed in ThinManager unless that parameter is activated.

The keyboards and mice for the slave thin clients can be left attached, but stowed away until a multi-user configuration is needed.

25.4.3. Shared Keyboard and Mouse with MultiMonitor

Using the Shared Keyboard and Mouse module fell out of favor when the MultiMonitor hardware was introduced. It was easier to use a single MultiMonitor thin client to show multiple displays than using several thin clients and the Shared Keyboard and Mouse module.

The Shared Keyboard and Mouse module made a comeback once people realized they could tie several MultiMonitor thin clients together to provide a wall of monitors in a control room.



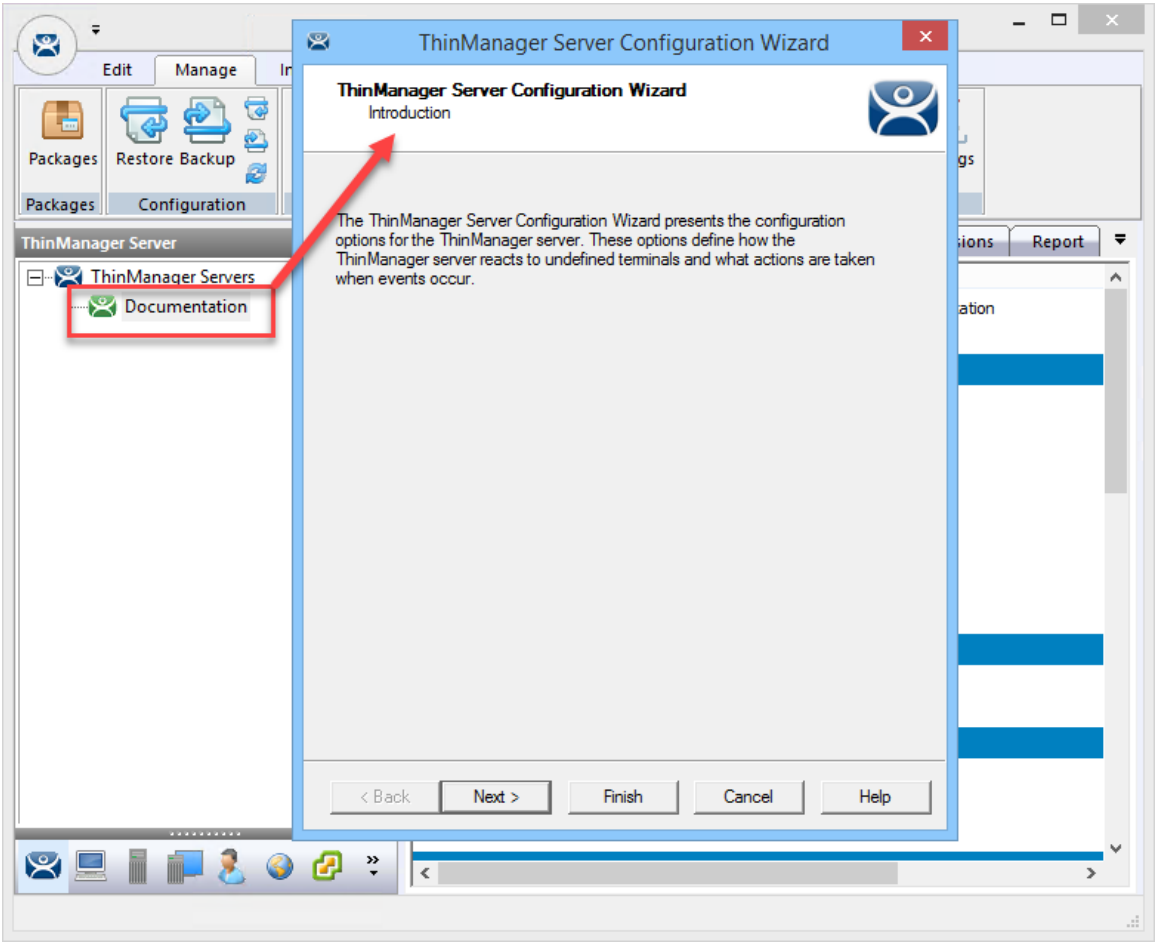
MultiMonitor with Shared Keyboard and Mouse

The configuration of the Slave and Master Shared Keyboard and Mouse modules are the same with MultiMonitor thin clients as they are with single monitor thin clients.

26. ThinManager Server Configuration Wizard

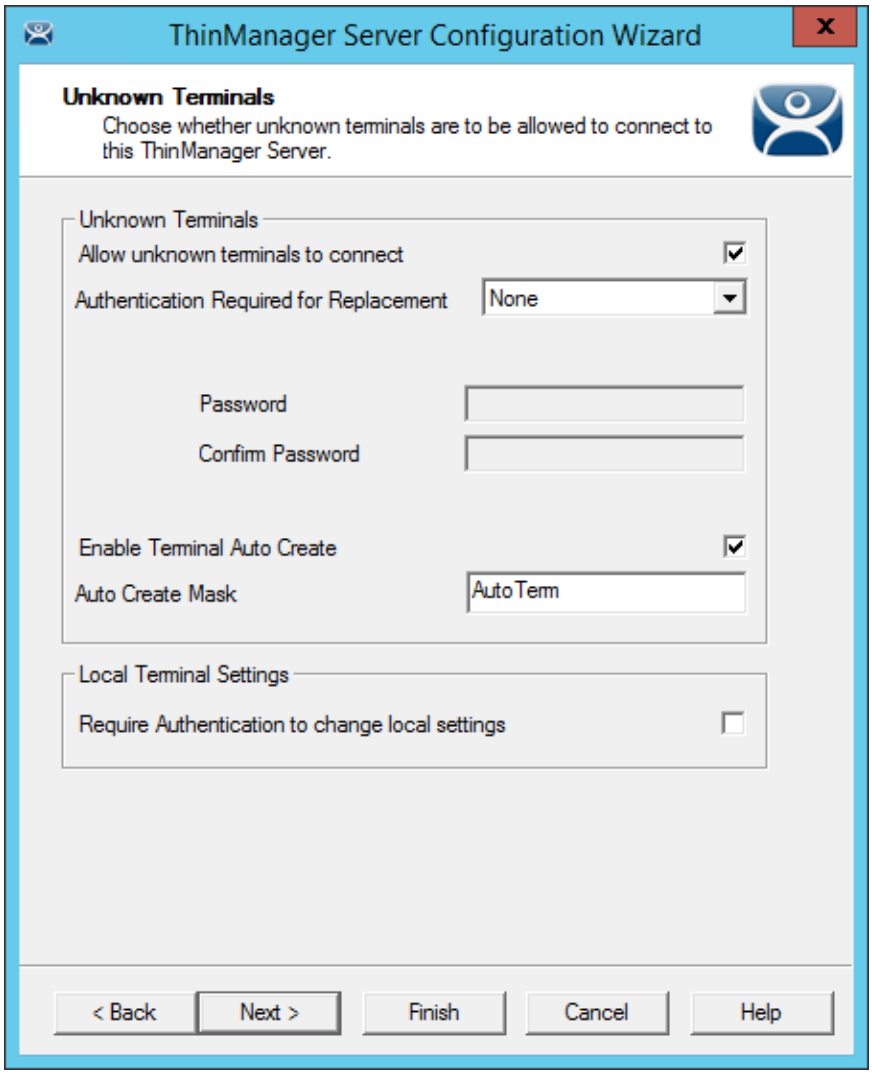
The ThinManager Server Configuration wizard allows the configuration of global ThinManager settings. It can be launched by:

- Selecting ***Edit > Modify*** while the ThinMan icon is highlighted in the ThinManager tree, or
- Double-clicking on the ThinManager icon in the tree, or
- Right clicking the ThinMan icon and selecting ***Modify***.



ThinManager Server Configuration Wizard

Importance of Page: This displays introductory information



Unknown Terminals

Importance of Page: Controls creation and replacement of Terminals through use of passwords and auto-creation.

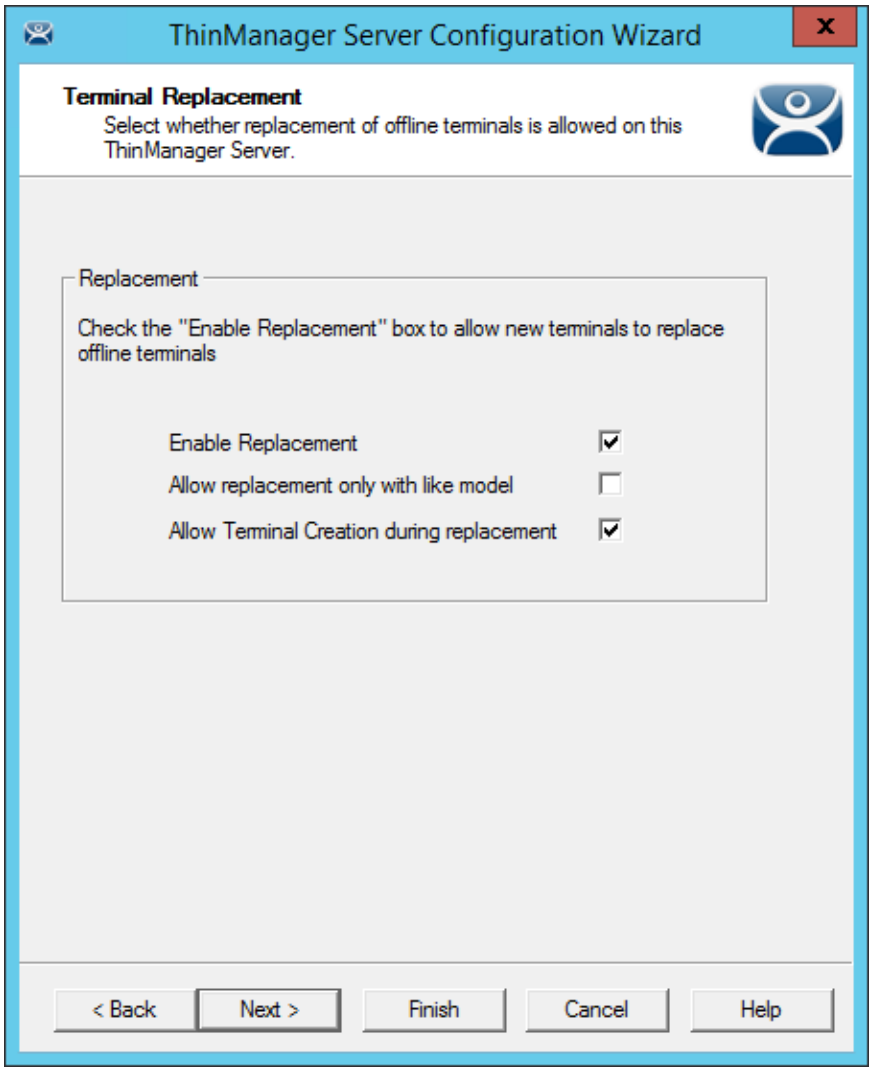
Settings:

- ***Allow unknown Terminals to connect*** - This checkbox lets new Terminals be added to the ThinManager Server. Replacements and new Terminals are prevented if this box is un-selected.
- ***Authentication Required for Replacement*** - This drop-down controls replacement authorization.
    - ***None***- This allows a Terminal to be added without authentication.
    - ***ThinManager Password*** – This allows you to set a password so that only authorized personnel can add Terminals to the ThinManager Server. If checked, the password fields become active and allow the addition of a password.
    - ***Windows Account*** – – This requires that the replacer enter their Windows account on the Terminal as it is being replaced. ThinManager will check and allow the replacement if the replacer is a member of a Windows Security Group that has the *Allow Terminal Replacement* task granted.

- ***Enable Terminal AutoCreate*** - This checkbox, if selected, allows the auto-creation of an array of Terminals as described in Auto-Creation of Terminals.
- ***AutoCreate Mask*** - This field is the base name used in the array of Terminals when using Auto-Creation of Terminals.
- **Require authentication to change local settings** – This checkbox will require authentication from a Windows Group that was granted the ***Edit Local ThinManager Server List*** function on the **ThinManager Security Page** in the **ThinManager Server Configuration Wizard**. This applies to mobile devices like iTMC, aTMC, and WinTMC.

Why Change from Default Settings: requiring a password can control who adds Terminals. Using auto-creation can be helpful is some large deployments**.**

Select ***Next*** to continue, ***Finish*** to save and close, or ***Cancel*** to close without saving.



Terminal Replacement

Importance of Page: Sets the global setting for enabling replacement of offline Terminals.

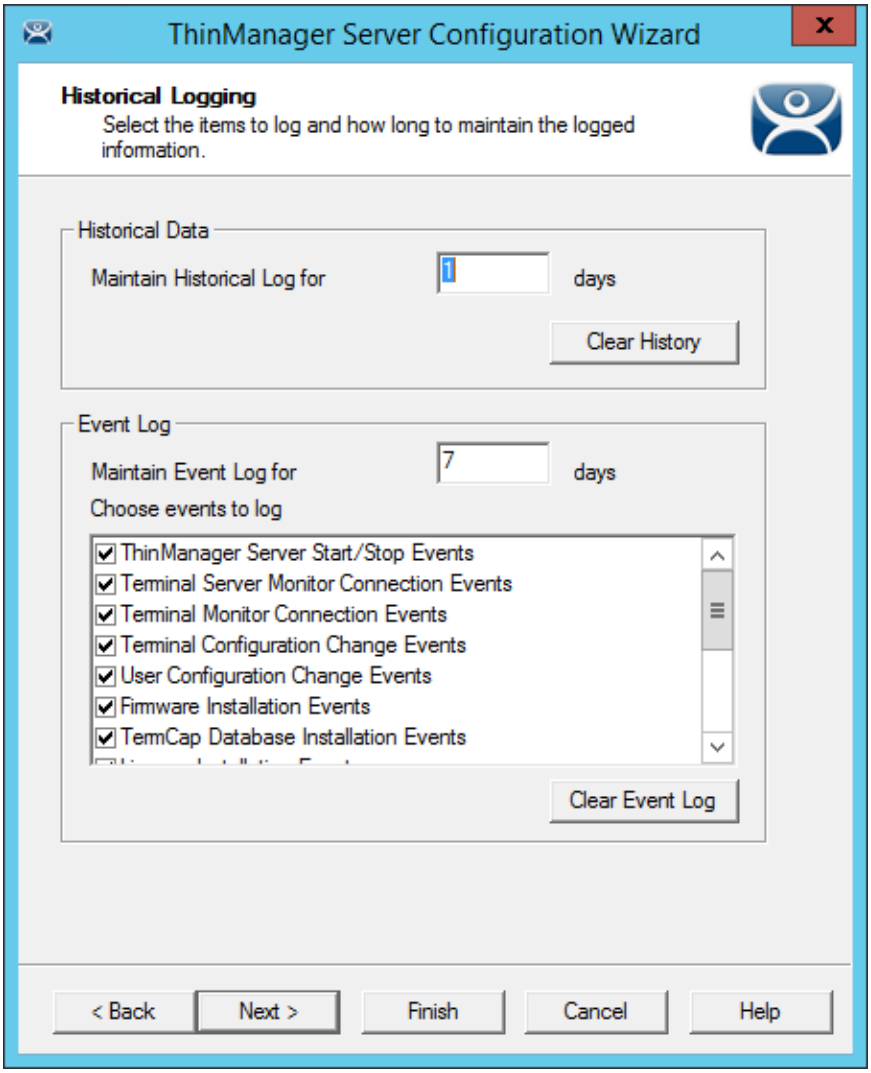
Note: Terminals that are on cannot be replaced until they are turned off.

Settings:

- ***Enable Replacement*** – This checkbox gives **global permission** for Terminals to be replaced. Un-selecting this will prevent **all** Terminals from showing up in the replacement list when a new Terminal is added, making **Create New Terminal** the only option. This feature is also available for the Group and Terminal level on the first page of the corresponding wizard. However, if this checkbox is unselected in the **ThinManager Server Configuration Wizard**, checking it in a **Terminal Configuration Wizard** will have no effect.
- ***Allow Replacement only with like model* –** This checkbox prevents the replacement of a Terminal with a different model to prevent configuration changes, a PXE for a PXE or an Android for an Android, for example.
- ***Allow Terminal Creation during replacement* –** Normally a Terminal displays the “Create New Terminal” option during replacement. Unchecking this checkbox will remove that option and only allow a Terminal replacement, not a new configuration.

Why Change from Default Settings: Un-selecting this will prevent **all** Terminals from showing up in the replacement list when a new Terminal is added, making **Create New Terminal** the only option.

Select ***Next*** to continue, ***Finish*** to save and close, or ***Cancel*** to close without saving.



Historical Logging

Importance of Page: Sets the duration that logs are maintained.

Settings:

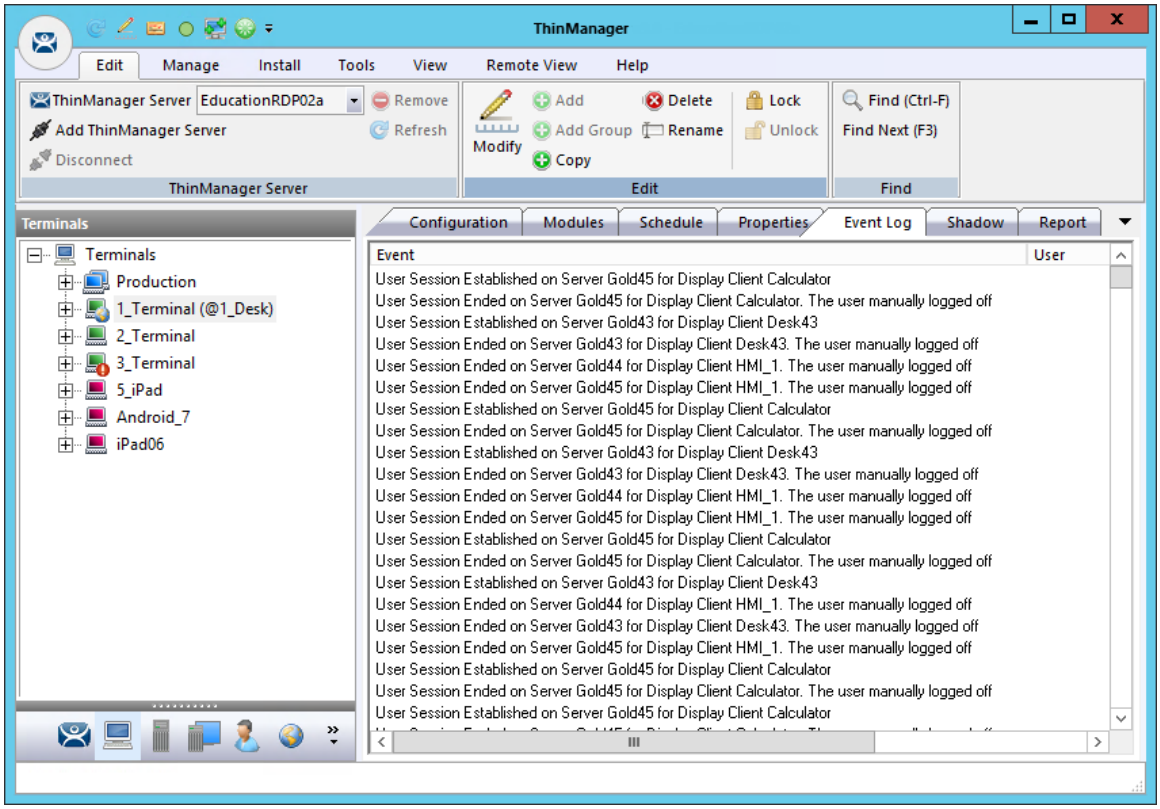
- ***Maintain Historical Log for X days*** - This field determines the length of time that the Remote Desktop Server CPU and memory data from the **Remote Desktop Server Graph** tab is stored. See Details Pane for an example of the graph.
- ***Maintain Event Log for X days*** - This field determines how long the event log is kept.
- **Choose events to log** - These checkboxes determine what events are stored in the log.

Buttons:

- ***Clear History*** - This button will erase the Historical log.
- ***Clear Event Log*** - This button will erase the Event log.

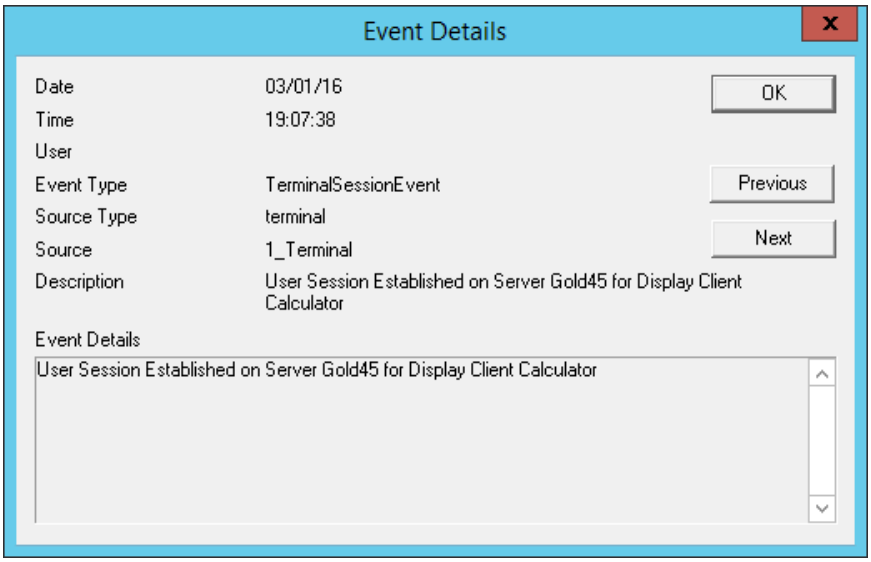
Why Change from Default Settings: You can add Remote Desktop Server events and Relevance User events that aren't collected by default. You can change the duration of the logs.

Selecting the **Event Log** tab will show the events for the highlighted tree icon.



Event Log Tab

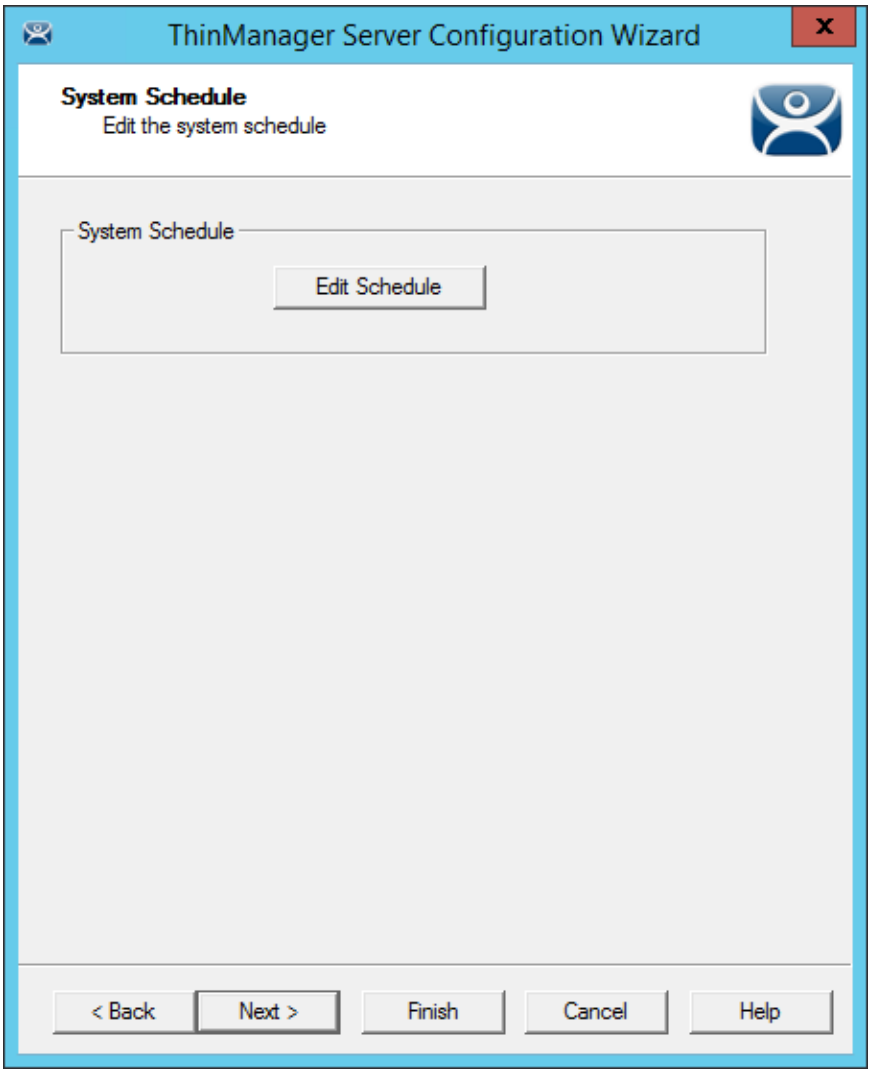
Details of an event can be obtained by double-clicking on an event.



Event Detail

Double clicking on an event will open an **Event Details** window that shows details of the selected event. Select either the ***OK*** or ***Cancel*** button to close.

Select ***Next*** to continue, ***Finish*** to save and close, or ***Cancel*** to close without saving.



System Schedule

Importance of Page: Allows schedules to be setup for ThinManager and the ThinManager system.

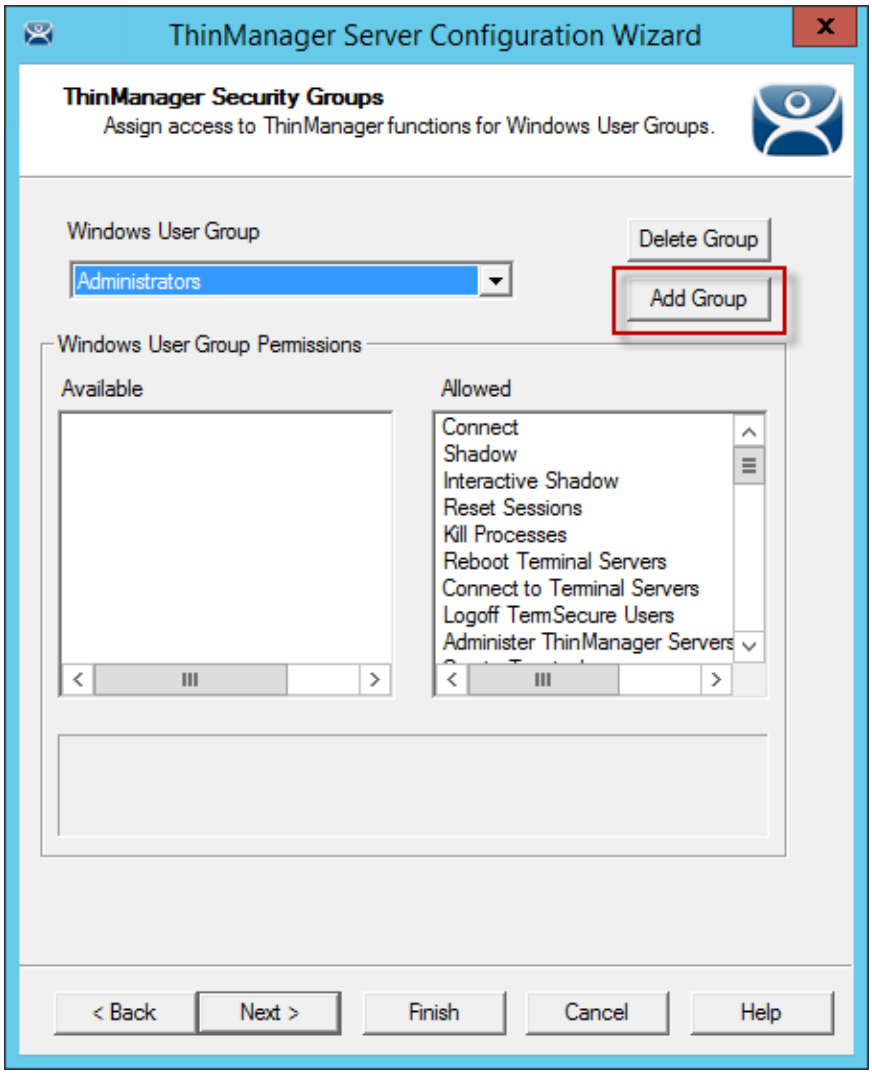
Buttons:

- ***Edit Schedule*** – This button launched the **Event Schedule** window.
  See Scheduling on page 445 for details.

Why Change from Default Settings: Automating backups, reports, and actions with the Scheduler saves time.

Select ***Next*** to continue, ***Finish*** to save and close, or ***Cancel*** to close without saving.

Access to ThinManager can be assigned to Windows User Groups on the **ThinManager Security Groups** page.



ThinManager Security Groups

Importance of Page: Normally administrators are the only people who have access to ThinManager functions. This page allows access to be granted to people so they can perform specific jobs without being elevated to the administrator role.

Settings:

- **Windows User Group –** This drop-down shows the group that is being configured.

Fields:

- **Available –** This list box shows the ThinManager functions that are available to the Windows group displayed in the **Windows User Group** box. These functions can be added to the ***Allowed*** list by double clicking.
- **Allowed –** This list box shows the ThinManager functions that are granted to the Windows group displayed in the **Windows User Group** box. These functions can be removed from the ***Allowed*** list by double clicking.

Buttons:

- **Delete Group –** This button will remove the highlighted group in the **Windows User Group** box.
- **Add Group –** This button launched the **New Window Group** window where a new Windows© group can be added to the configuration.

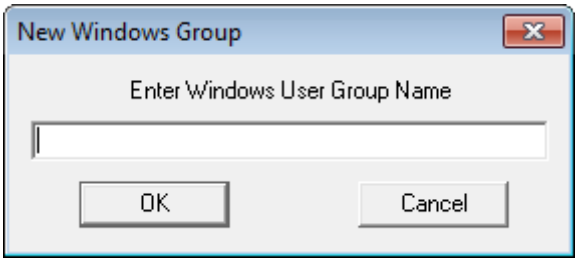
Why Change from Default Settings: Creating a Windows Group and granting access to ThinManager functions allows people to use ThinManager without being an administrator.

ThinManager allows different levels of access and functionality based on standard Windows groups. By default only members of the Windows Administrator group has the ability to connect to ThinManager and use the application. The ThinManager Security Groups allows other Windows groups to be granted privileges in ThinManager.

ThinManager comes with privileges pre-defined for six groups. Each of these groups (except Administrators) needs to be created on the domain controller or in the Local Users and Groups on the Computer Management console and members added before they can be used.

- **Administrators -** The Microsoft defined Administrator group is given all privileges by default in ThinManager. This may be denied by unselecting the various allowed **Windows User Group Permissions.**
- **ThinManager Administrators** have full permission to do anything within ThinManager including the power to logoff sessions, kill processes, send messages, restart Terminals, calibrate touch screens, change Terminal configurations, update firmware, update the TermCap, and restore configurations. Administrators and members of ThinManager Administrators can shadow Terminals and interactively control the Terminal session. **These privileges may not be removed** and will be grayed out**.**
- **ThinManager Interactive Shadow Users** - Members of this group may shadow a Terminal interactively.
- **ThinManager Power Users** can logoff sessions, kill processes, send messages, restart Terminals, and calibrate touch screens. They cannot change Terminal configurations, update firmware, update the TermCap, and restore configurations. ThinManager Power Users can shadow Terminals from within ThinManager but cannot interact with the session.
- **ThinManager Shadow Users** - Members of this group may shadow a Terminal but not interactively.
- **ThinManager Users** can view only. They cannot logoff sessions, kill processes, send messages, restart Terminals, or calibrate touch screens. ThinManager Users cannot shadow a Terminal.

Selecting the ***Add Group*** button in a non-domain ThinManager Server will launch the **New Windows Group** window. This will allow the configuration of additional Windows User Groups.

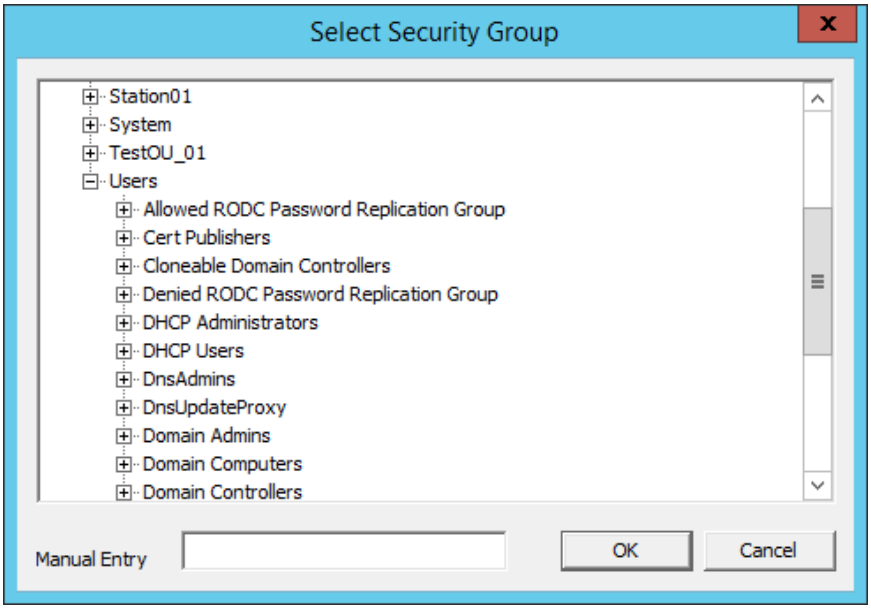


New Window User Group Window in Workgroup

Adding a Windows Group name in the ***Enter Windows User Group Name*** field of the **New Window Group** window and selecting the ***OK*** button will add the Windows User Group to the drop-down list.

Note: This doesn't create the user group on any servers. This just adds the name of an existing group to the list that ThinManager is maintaining.

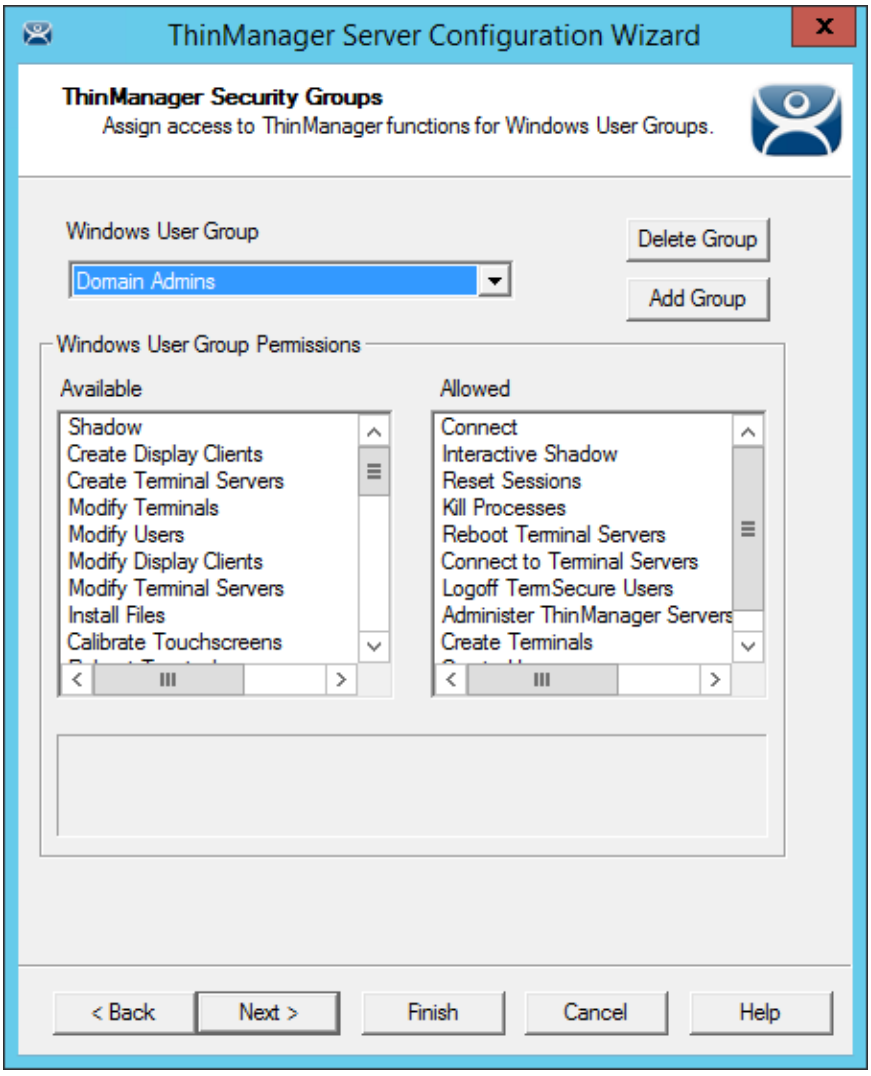
Selecting the ***Add Group*** button in a domain ThinManager Server will launch the **Select Security Group** window. This will allow you to add Active Directory groups and configure their permissions in ThinManager.



New Window User Group Window

Adding a Windows Group name in the ***Enter Windows User Group Name*** field of the **New Window Group** window and selecting the ***OK*** button will add the Windows User Group to the drop-down list.

The ***Manual Entry*** field will allow you to enter a local Windows User Group.



ThinManager Security Groups Page

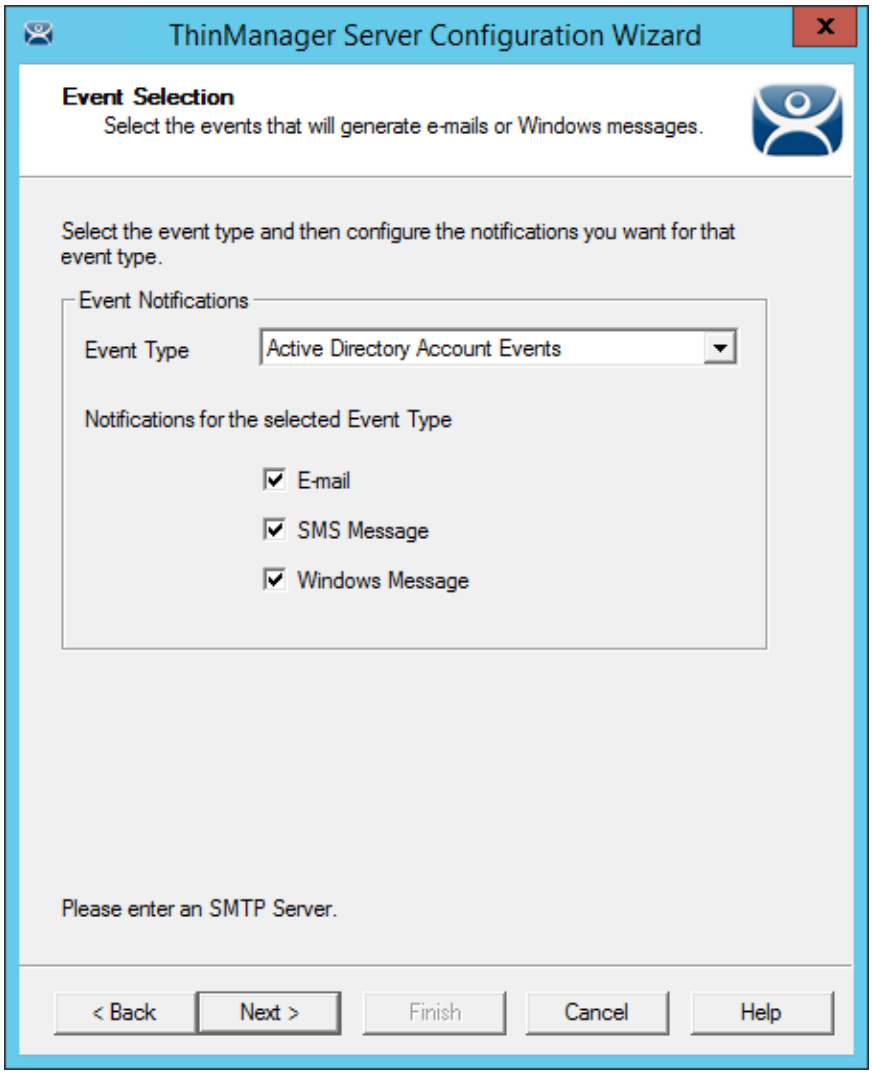
Select the group from the **Windows Users Group** drop-down. Choose the permissions you want to grant to the group by double clicking on the function in the ***Available*** **Windows User Group Permissions** list. Members of the Windows User Group will have the selected permissions the next time they login.

Although ThinManager has Windows User Groups pre-configured with privileges, these groups have not been created on the Remote Desktop Servers. These are merely templates for groups that can be created.

If you need a new Windows group create the Windows User Group using standard Microsoft methods.

Note: The ThinServer service may need to be stop and restarted to load the new ThinManager Security Group settings.

Select ***Next*** to continue the **ThinManager Server Configuration Wizard**, ***Finish*** to save and close, or ***Cancel*** to close without saving.



Event Selection

Importance of Page: ThinManager has event notification. E-mails, SMS Messages, or Windows messages can be sent by ThinManager to identify changes in the setup, configuration or status.

Settings:

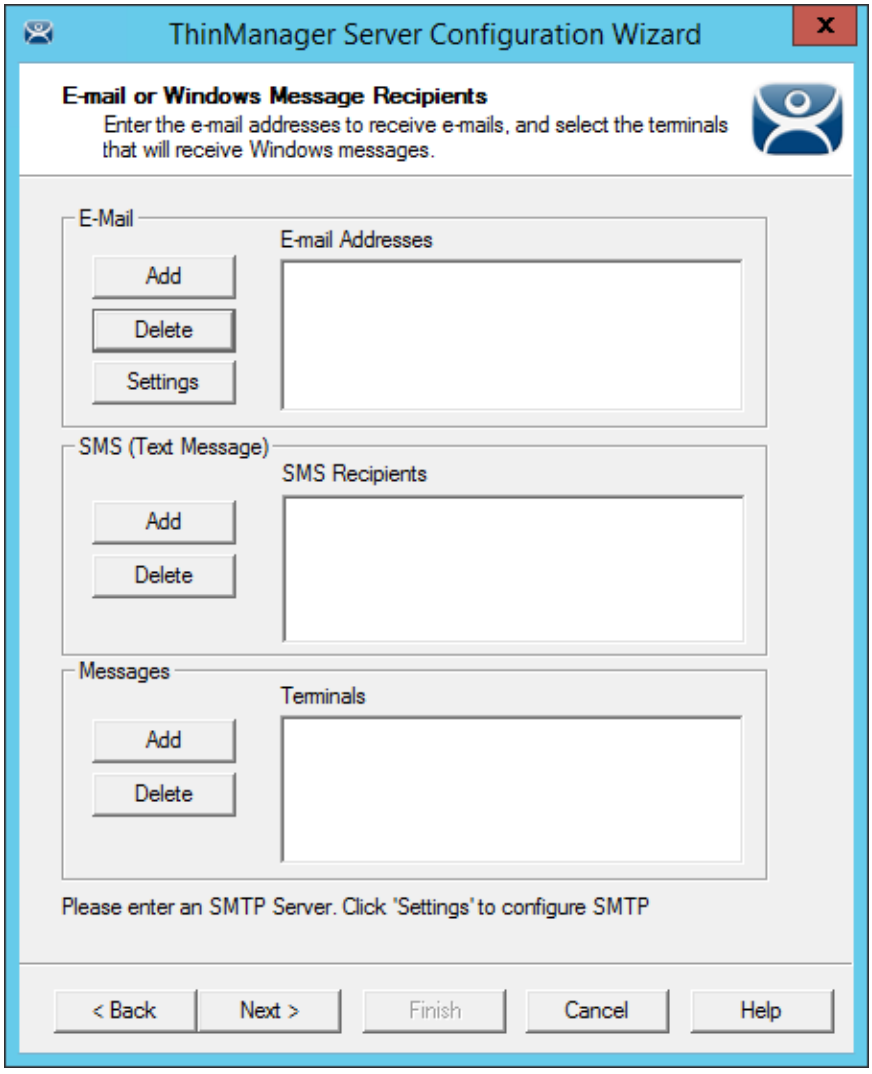
- **Event Type –** This drop-down lists the events that can trigger a message. Select the desired event and select the message type. You may select multiple events.
- **Email –** Checking the ***E-mail*** checkbox will send an e-mail message when that event occurs. The e-mail needs to be set up on the next page of the wizard.
- **SMS Message –** Checking the ***SMS Message*** checkbox will send an SMS message when that event occurs. The SMS Messaging system needs to be defined on the next page of the wizard.
- **Windows Messages –** Checking the ***Windows Message*** checkbox will send a message to a Terminal when that event occurs. The Terminal needs to be defined on the next page of the wizard.

Why Change from Default Settings: Information about these events can be useful. The event needs checked to add the notification.

The ThinManager Server Stop/Start, Remote Desktop Server Monitor Connection, and Terminal Monitor Connection events may indicate the failure of the ThinManager Server, Remote Desktop Server, or Terminal.

Sharing information on configuration changes, firmware, TermCap, or license installation can be useful when management is shared among a group. Sending an e-mail to all group members keeps them informed of all changes.

Select ***Next*** to continue, ***Finish*** to save and close, or ***Cancel*** to close without saving.



Email or Windows Messaging Recipients Page

Importance of Page: This page defines what users are notified of event changes from the **Event Selection** page.

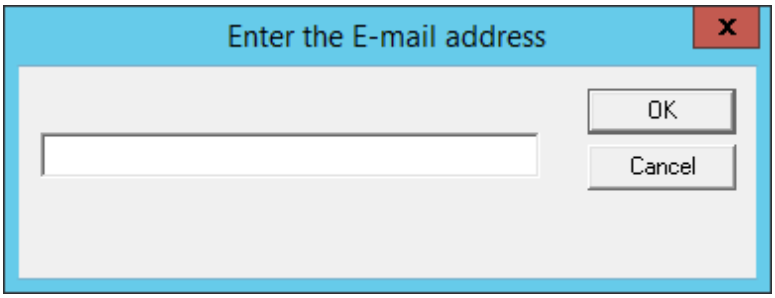
Fields:

- ***E-Mail Addresses*** - ThinManager will send an e-mail message to the addresses in this text box when an event selected on the **Event Select** page occurs.
- ***SMS Recipients*** - ThinManager will send a SMS message to the addresses in this text box when an event selected on the **Event Select** page occurs.

- ***Terminals*** - ThinManager will send a message to the Terminals in this text box when an event selected on the **Event Select** page occurs.

E-mail Buttons:

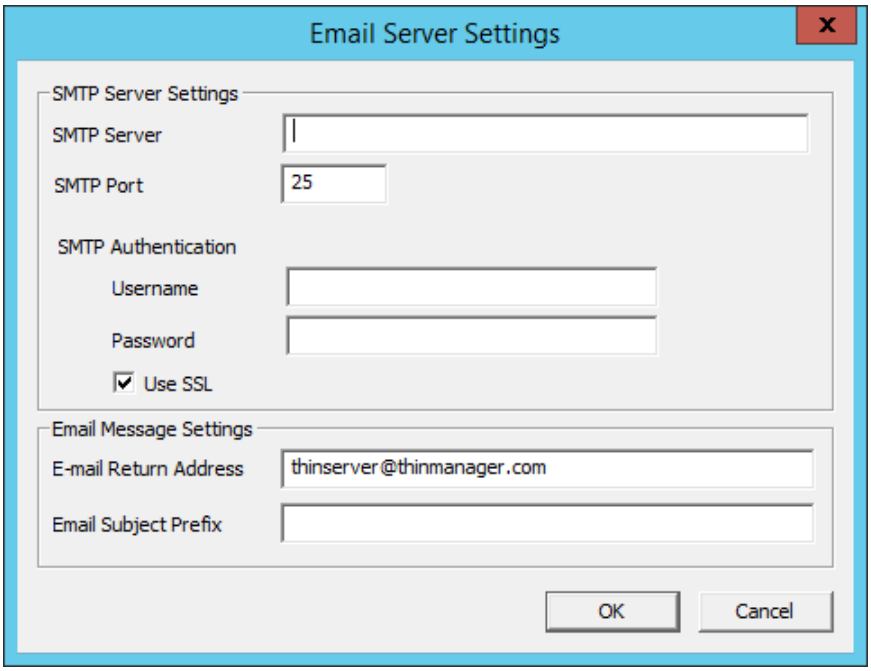
- ***Add*** - Select this button to add e-mail addresses through the **Enter the E-mail address** window.
- ***Delete*** - Select this button to delete a highlighted e-mail address from the **E-mail Addresses** list.
- ***Settings*** - Select this button to add a Terminal through the **Select Terminal(s)** window.



Enter the E-mail Address Window

Selecting the ***Add*** button in the **E-mail** section will open the **Enter the E-mail Address** window that allows you to add an e-mail address to the notification list.

Select the ***OK*** button to accept the setting or ***Cancel*** to close without saving.



E-mail Server Setting Window

Selecting the ***Settings*** button in the **E-mail** section will open the **Email Server Settings** window that allows you to configure the SMTP mail server.

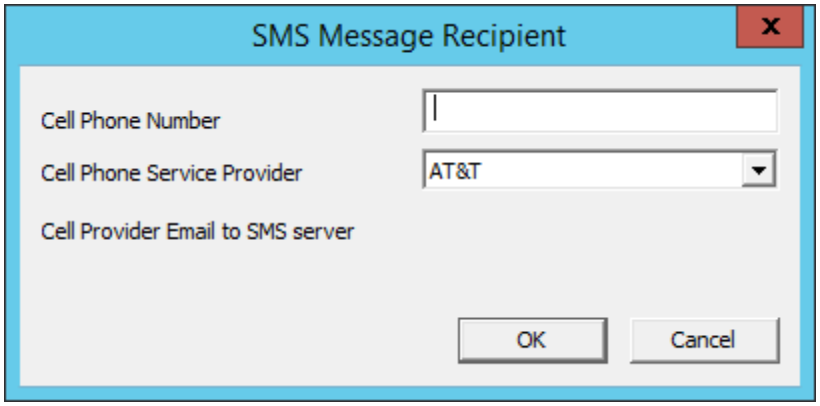
- ***SMTP Server*** – This field is for the name of the SMTP server.
- ***SMTP Port*** - This field is for the port used to connect to the SMTP server.
- ***SMTP Authentication*** – The ***Username*** and ***Password*** fields allow the use of authentication for the connection to the SMTP server.

- ***Use SSL*** – This checkbox allows the use of the SSL (Secure Socket Layer) to communicate with the SMTP server.
- ***E-mail Return Address*** – This field allows you to configure a sender account for replies..
- ***Email Subject Prefix***- This field allows you to configure a subject line for the emails.

Select the ***OK*** button to accept the setting or ***Cancel*** to close without saving.

SMS (Text Message) Buttons:

- ***Add*** - Select this button to open the **SMS Message Recipient** window to add a phone number to the distribution list.
- ***Delete*** - Select this button to delete a highlighted number from the **SMS Recipients** list.



SMS Message Recipient Window

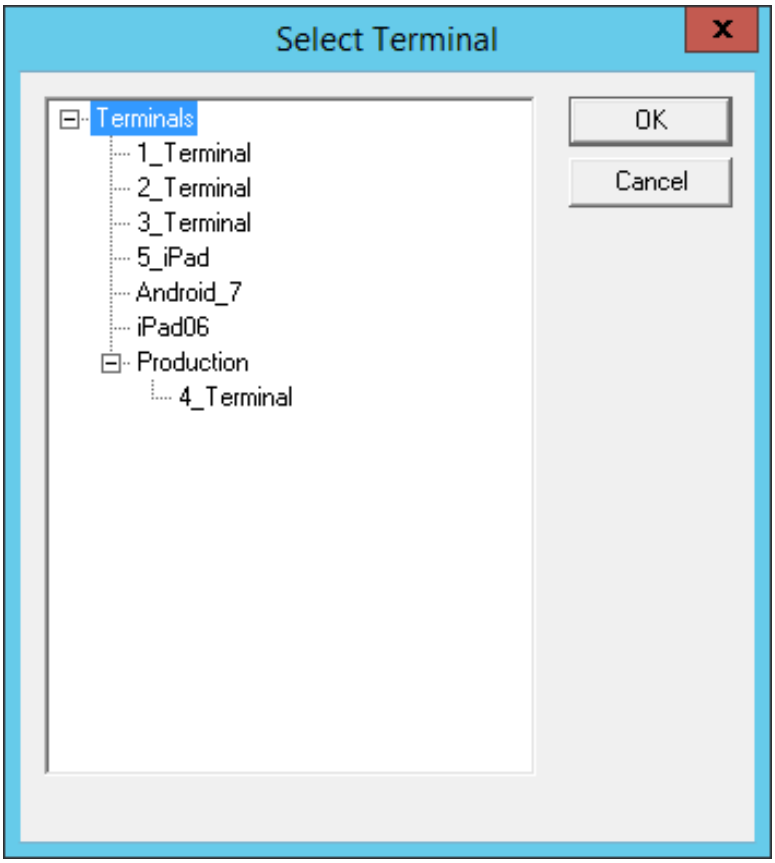
The **SMS Message Recipient** window allows you to add a phone number to the SMS distribution list.

- ***Cell Phone Number*** – This field allows you to enter a phone number.
- ***Cell Phone Service Provider*** – This drop-down allows you to specify what network the cell phone uses. Each service provider uses a unique account so the correct account is important.

Select the ***OK*** button to accept the setting or ***Cancel*** to close without saving.

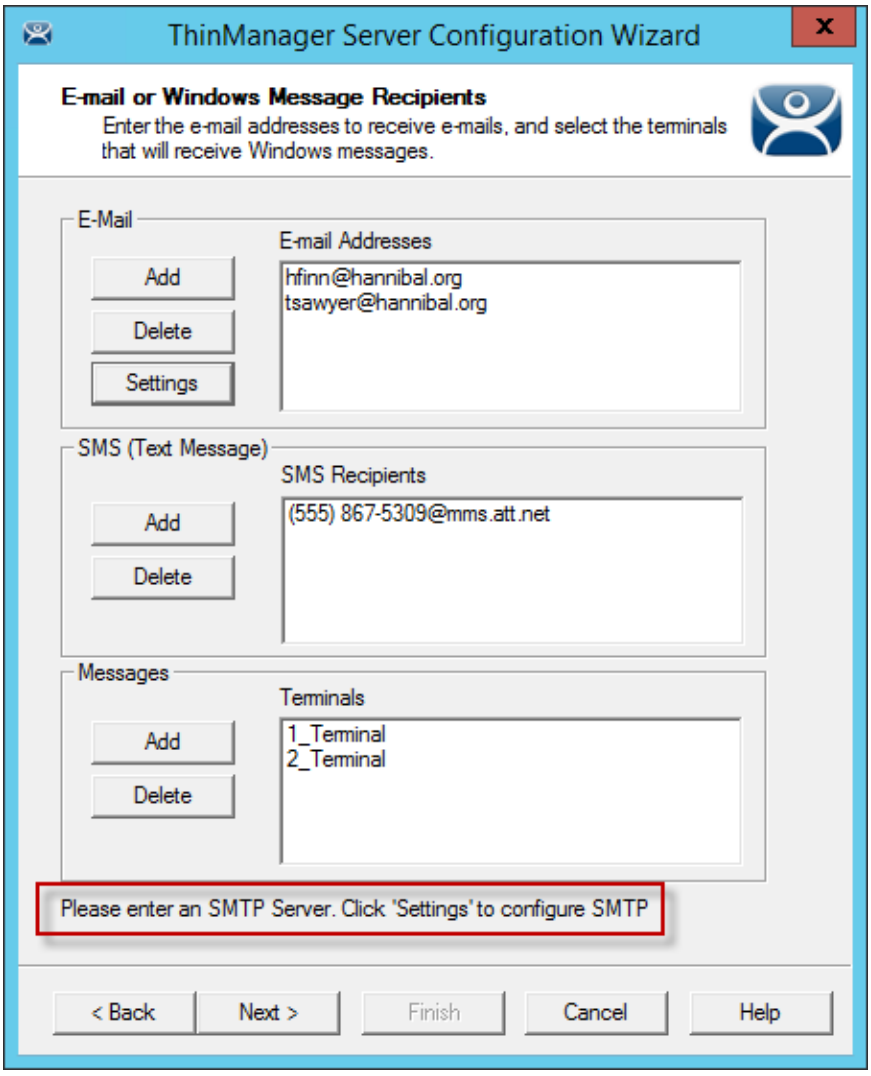
Messages Buttons:

- ***Add*** - Select this button to add a Terminal through the **Select Terminal(s)** window.
- ***Delete*** - Select this button to delete a highlighted Terminal from the **Terminals** list.



Terminal Selection Window

The **Select Terminal(s)** windows will list the Terminals configured on the ThinManager Server. Highlight the desired Terminal and select the ***OK*** button.

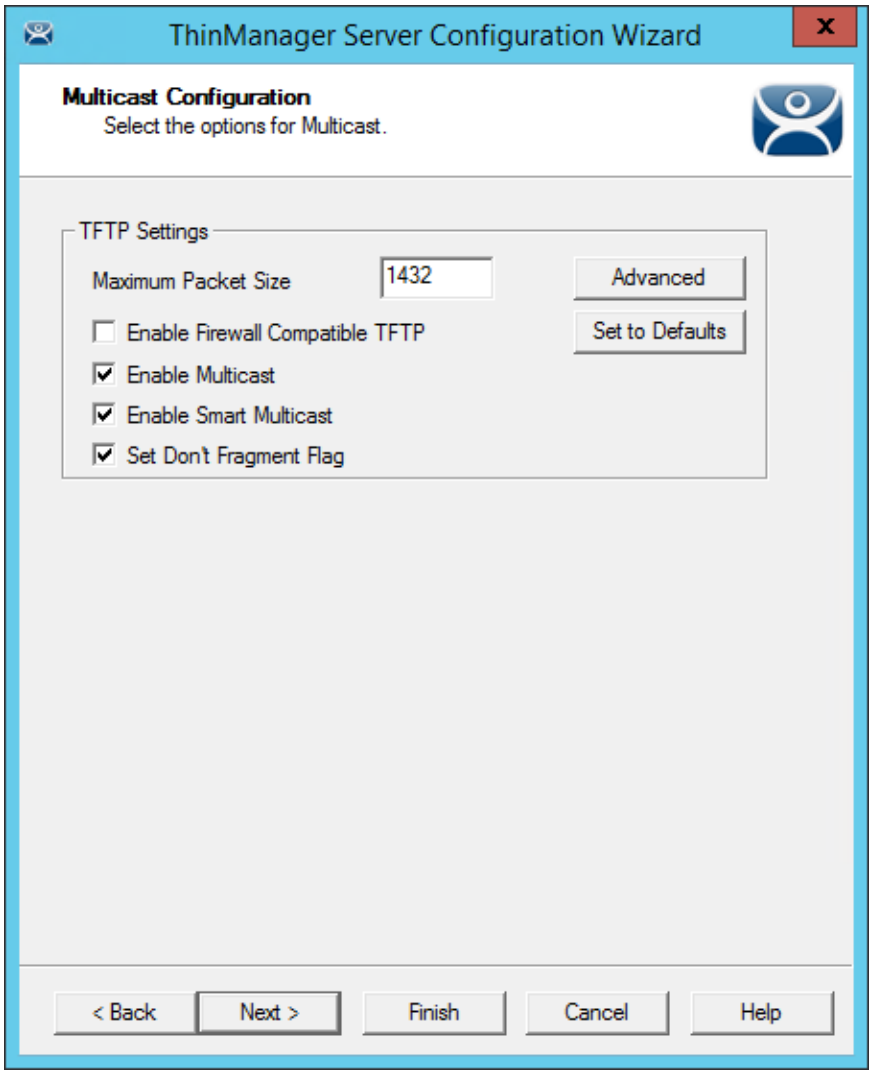


Email or Windows Messaging Recipients Page

This shows the **Email or Windows Messaging Recipients** window populated with different recipients.

Note: The SMTP server wasn't set up properly and an error message was displayed as a reminder.

Select ***Next*** to continue, ***Finish*** to save and close, or ***Cancel*** to close without saving.



Multicast Configuration Page

Importance of Page: Allows multicast to be configured for ThinManager Servers.

Fields:

- ***Maximum Packet Size*** – This allows the firmware download packet size to be changed, if needed.

Settings:

- ***Enable Firewall Compatible TFTP*** – This checkbox enables the firewall friendly TFTP(Trivial File Transfer Protocol) to be used to send firmware to the thin client. This setting will make it easier to get through a firewall.
- ***Enable Multicast*** - This checkbox, if selected, enables Multicast.
- ***Enable Smart Multicast*** - This checkbox, if selected, enables Smart Multicast.
- ***Set Don't Fragment Flag*** – This checkbox, if selected, will tell the switch to keep the packets together instead of breaking them into fragments.

Buttons:

- ***Advanced*** - This button, if selected, displays the advanced settings.

- ***Set to Defaults*** - This button, if selected, sets the advanced settings back to the defaults.

Why Change from Default Settings: You may need to change the settings if there is a conflict with another multicast server on the network.

Multicast provides the ability for an unlimited number of Terminals to boot simultaneously from the same data stream. This feature reduces the amount of network traffic and reduces the amount of load on the ThinManager Server when multiple Terminals are booting concurrently. This function is especially useful for low bandwidth connections and highly utilized networks.

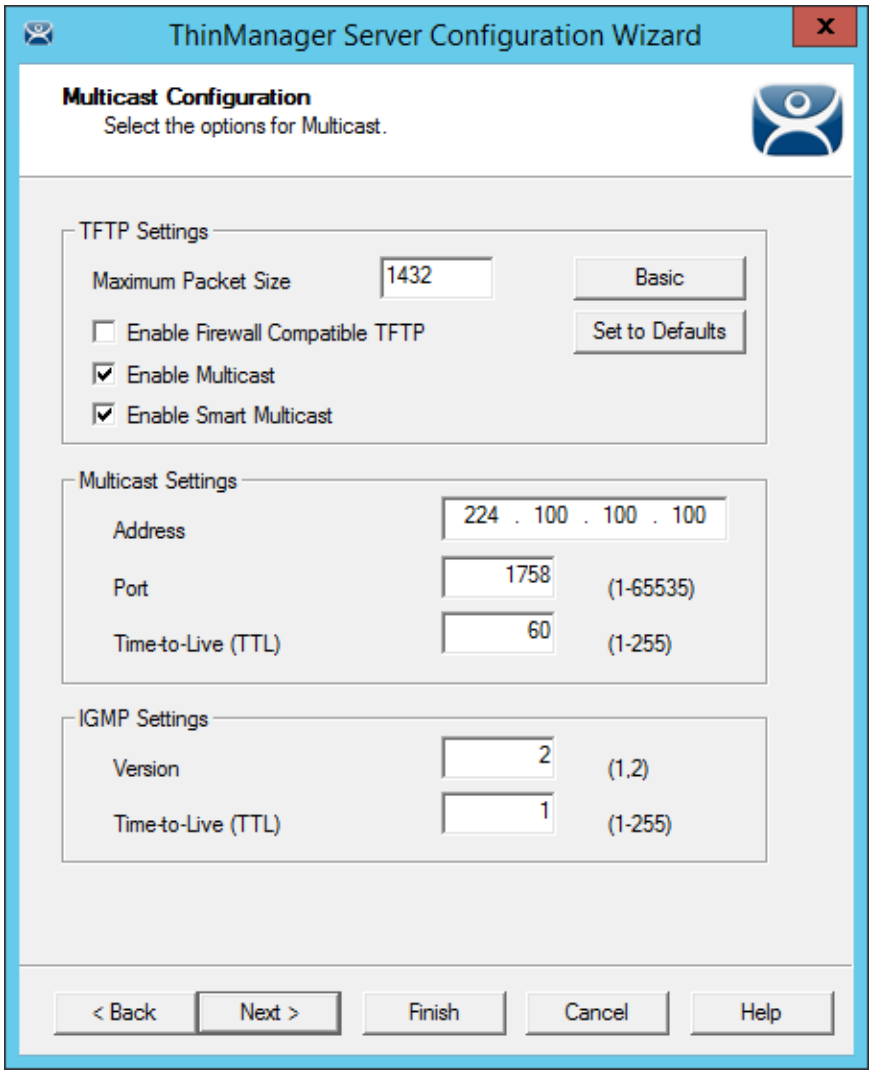
Smart Multicast allows the Terminal firmware to be sent directly to the Terminal while a single Terminal is booting. If additional Terminals request the Terminal firmware during this time, the firmware will be multicast so that all Terminals can receive the firmware from a single data stream. If Smart Multicast is disabled, the firmware will always be sent as a multicast transmission.

Multicast is only available on Terminals with ThinManager Boot Loader Version 5.0 and later. No local Terminal configuration is needed to use Multicast.

Unicast – ThinManager has error checking that will switch a Terminal's firmware download to unicast if the multicast download fails.

The thin client will continue to try to use multicast at each boot but will use unicast if multicast keeps failing.

Advanced Settings – Selecting the ***Advanced*** button will reveal advanced settings for multicast.



Advanced Multicast Options

Importance of Page: This allows changing the multicast settings if there is a conflict with another multicast server on the network.

Settings:

- **Multicast Settings**
  - ***Address*** – This is the IP address that will be used for Multicast transmissions.
  - ***Port*** – This is the destination port that will be used for Multicast transmissions.
  - ***Time-to-Live (TTL)*** – This is the maximum number of router hops for Multicast packets. Setting this value to 255 allows for unlimited hops.
- **IGMP Settings (Internet Group Management Protocol)**
  - **Version** – This sets the IGMP version for use with multicast capable routers.
  - **Time-to-Live (TTL)** – This sets the time-to-live value for IGMP packets.

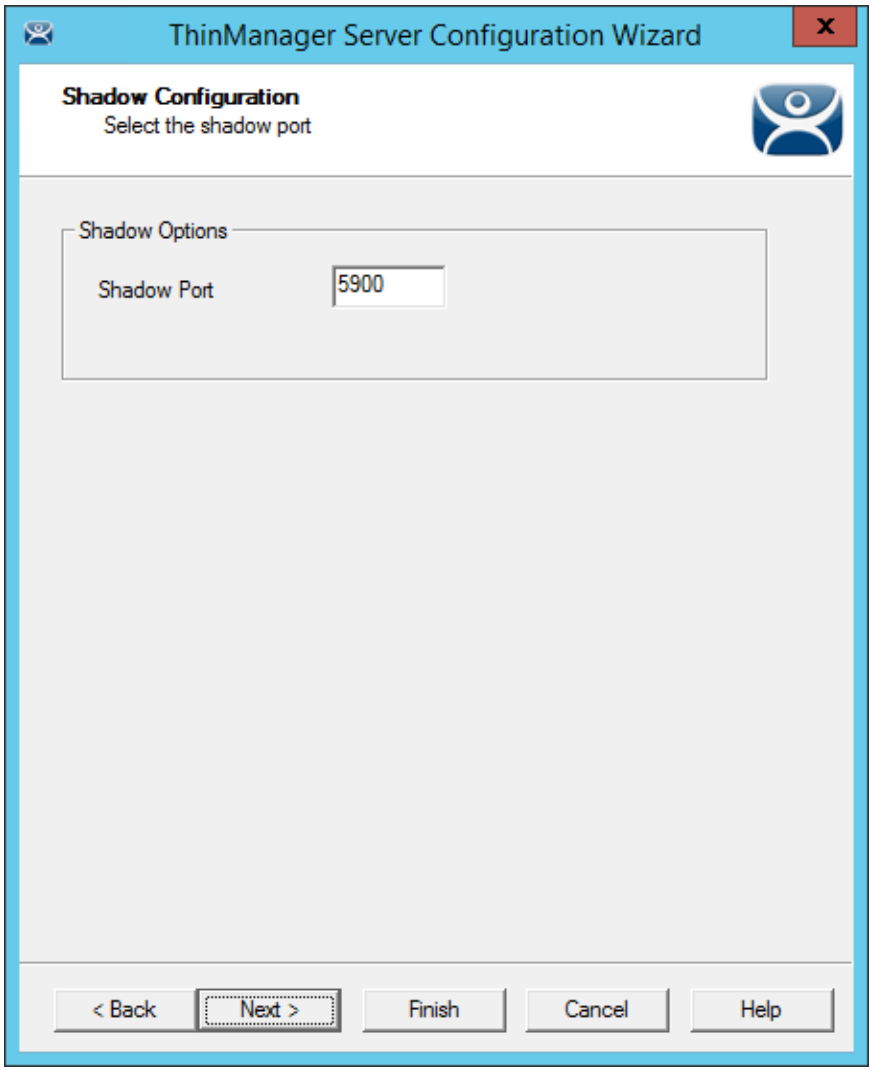
Buttons:

- ***Advanced*** - This button displays the advanced settings.

- ***Set to Defaults*** - This button sets the advanced settings back to the defaults.

Why Change from Default Settings: Change these if a conflict develops.

Select ***Next*** to continue, ***Finish*** to save and close, or ***Cancel*** to close without saving.



Shadow Configuration Port

ThinManager allows the port used for shadowing to be configured.

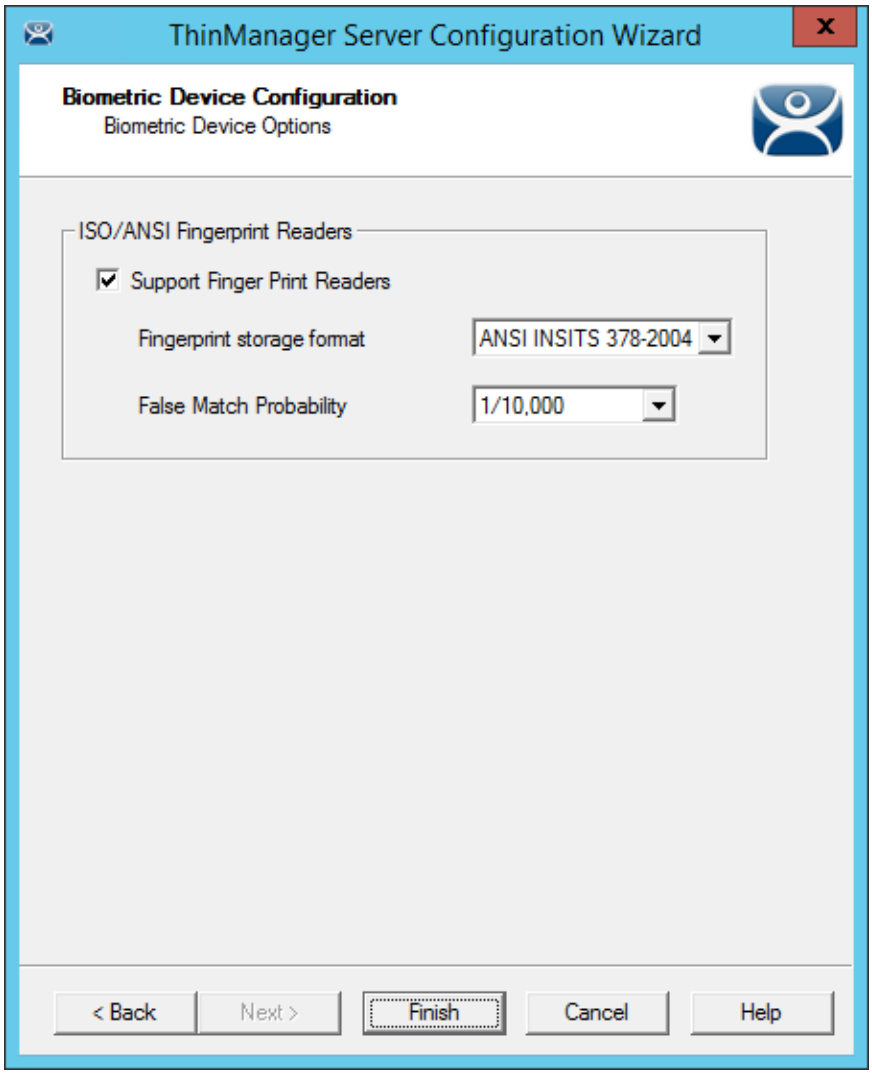
Importance of Page: This allows the port that is used for shadowing to be changed.

Settings:

- **Shadow Port –** ThinManager uses port 5900 as the default port for shadowing. Entering a different port number into the Shadow Port field will change the port used if it is in conflict with another processes use of the port.

Why Change from Default Settings: ThinManager uses the save port as VNC. If VNC is installed on a WinTMC PC then there could be a conflict between shadowing services. If this happens the port can be changed in ThinManager.

Select ***Finish*** to accept changes or select ***Cancel*** to close without making changes.



Biometric Device Configuration

Navigate to the **Biometric Device Configuration** window.

Select the ***Support Finger Print Readers*** checkbox to enable the use of readers.

Select the data format you plan to use. There are two formats to choose, **ISO_19794_2_2005** and **ANSI_378_2004**.

The ***False Match Probability*** sets the sensitivity of the read. 1/100 is less sensitive than 1/1,000,000.

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

27. Reports

ThinManager has the ability to run reports, show data, and collect data on the ThinManager system. These reports can show the event log, configurations, uptimes, and other data.

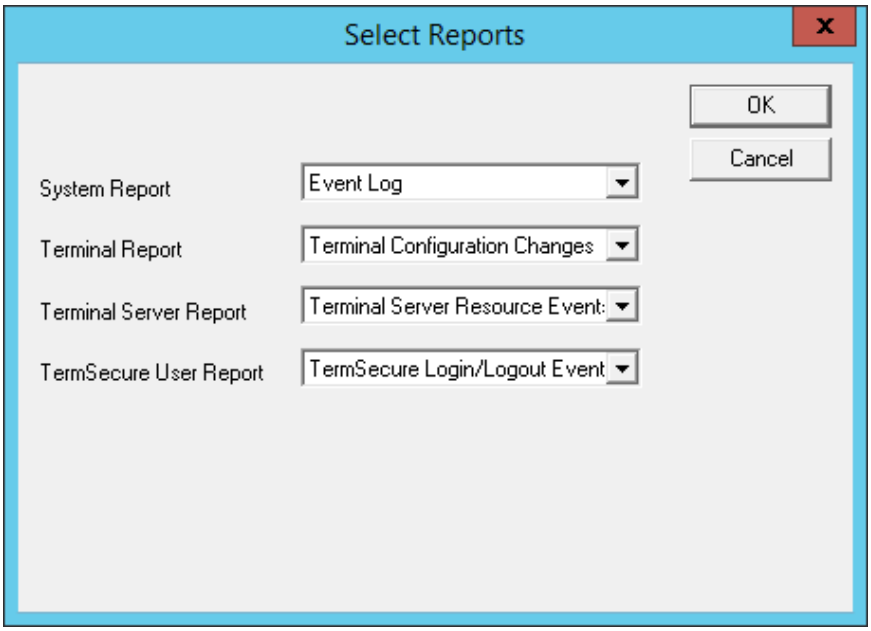
A ***Reports*** tab on the Details pane will show a report for a highlighted ThinManager Server, Terminal, Terminal group, Remote Desktop Server, TermSecure user, or Relevance User group.

Reports can be scheduled to be run and saved as ***.html** or ***.CSV** files for storage or further analysis.

27.1. Selecting Reports

The reports are displayed on a ***Report*** tab in ThinManager.

Select ***View > Select Reports*** from the ThinManager menu to launch the **Select Reports** window.



Select Reports Window

The **Select Reports** window allows the selection of which report to display.

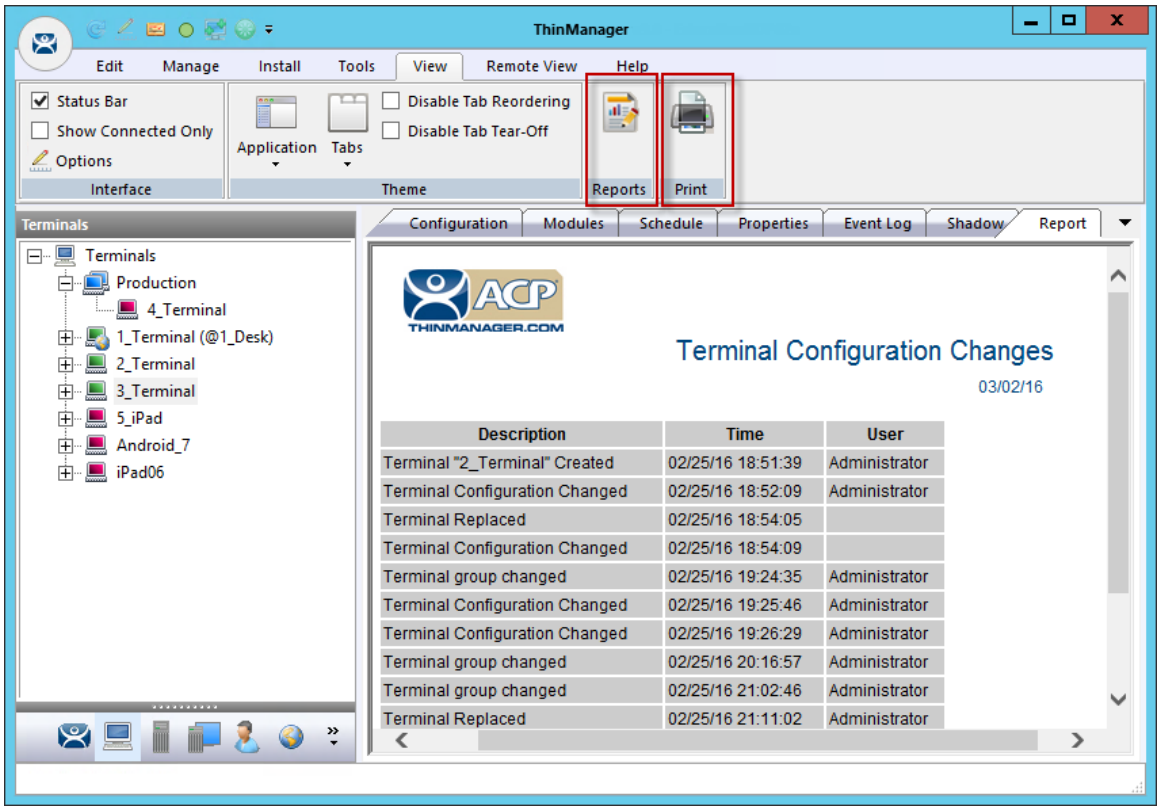
The **Select Reports** window has four fields that determine which report is displayed on the report tab.

- ***System Report*** – This selects the report to display on the ***Report*** tab when the ThinManager Server is highlighted.
- ***Terminal Report*** – This selects the report to display on the ***Report*** tab when a Terminal or Terminal group is highlighted.
- ***Remote Desktop Server Report*** – This select the report to display on the ***Report*** tab when a Remote Desktop Server is highlighted.
- ***Relevance User Report*** – This selects the report to display on the ***Report*** tab when a Relevance User or Relevance User Group is highlighted.

Use the drop-down list to select the desired reports.

27.2. Report Tab

The reports selected in the **Select Reports** window will be displayed on the ***Report*** tab in ThinManager.



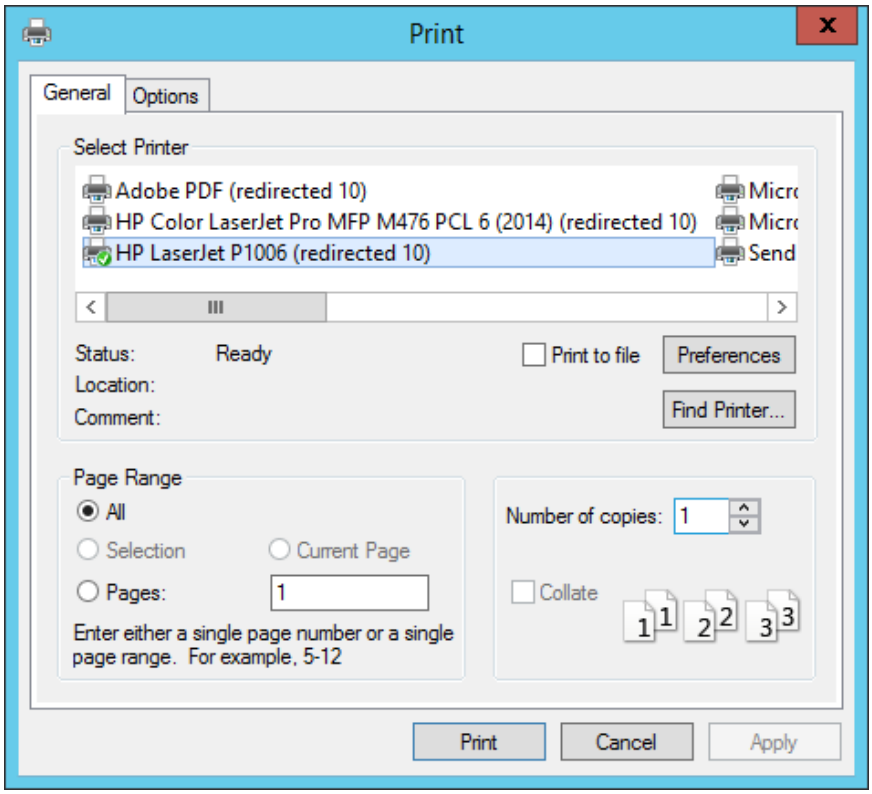
Report Tab

Highlight the desired ThinManager Server, Terminal, Terminal group, Remote Desktop Server, or Relevance user, and then select the ***Report*** tab to display the report.

27.3. Print Report

A Report can be printed by:

- Selecting the Report tab and selecting ***View > Print*** from the ThinManager menu. A **Print** window will be displayed to allow the selection of the printer.
- Right clicking on the report inside of the **Details** pane.



Print Window

A **Print** window will be displayed with all the printers defined on the ThinManager Server.

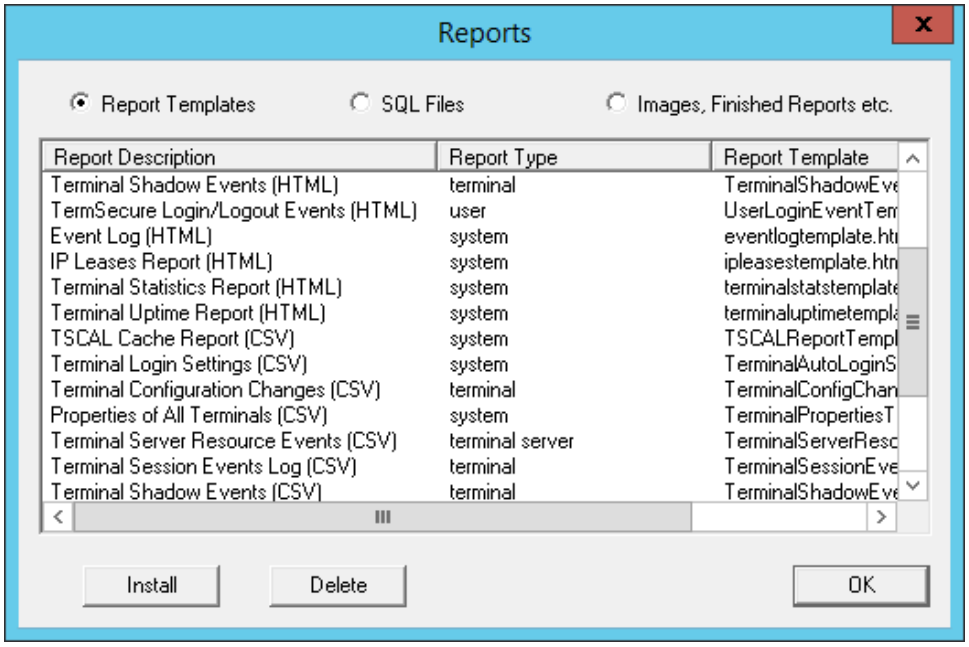
Highlight the desired printer and select the ***Print*** button to print the report.

27.4. Report Template Installation

ThinManager will install a number of reports into the ThinManager folder during installation. The default is ***C:\Program Files\Automation Control Products\ThinManager\ReportTemplates***.

New Reports are added to service packs and new releases. Additional report templates can be downloaded from http://downloads.thinmanager.com/ as they become available.

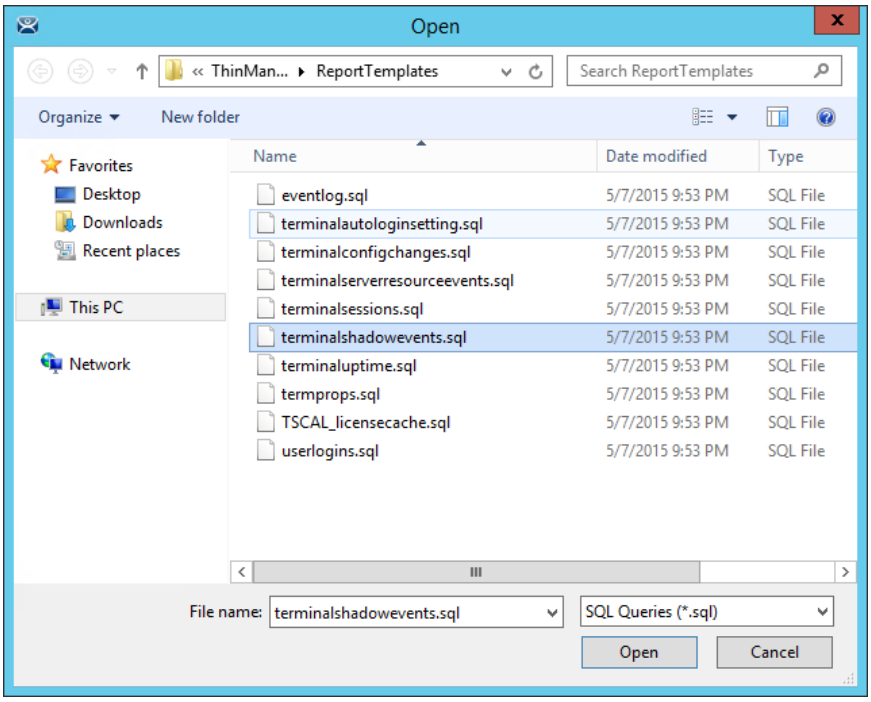
New reports are installed by selecting ***Install > Reports*** from the ThinManager menu. This launches the **Reports** window.



Reports Window

Select the ***Install*** button to launch a file browser.

- ***Report Templates*** – If this radio button is selected the file browser will browse for ***.html** files.
- ***SQL Files*** – If this radio button is selected the file browser will browse for ***.sql** files.
- ***Images, Finished Reports, etc.*** – If this radio button is selected the file browser will browse for assorted files.



File Browser

Each report has a ***.html** or ***.CSV** component and a ***.sql** component. Select the ***Report Templates*** radio button, browse to the new ***.html** file, and select ***Open*** to install. Select the ***SQL Files*** radio button, browse to the new ***.sql** file and select ***Open*** to install. Once these two components are added the report will be available.

28. Scheduling

Reports can be scheduled to be run once at a specified time or to be run regularly at a specific time. The reports are saved as ***.html** files for storage or further analysis.

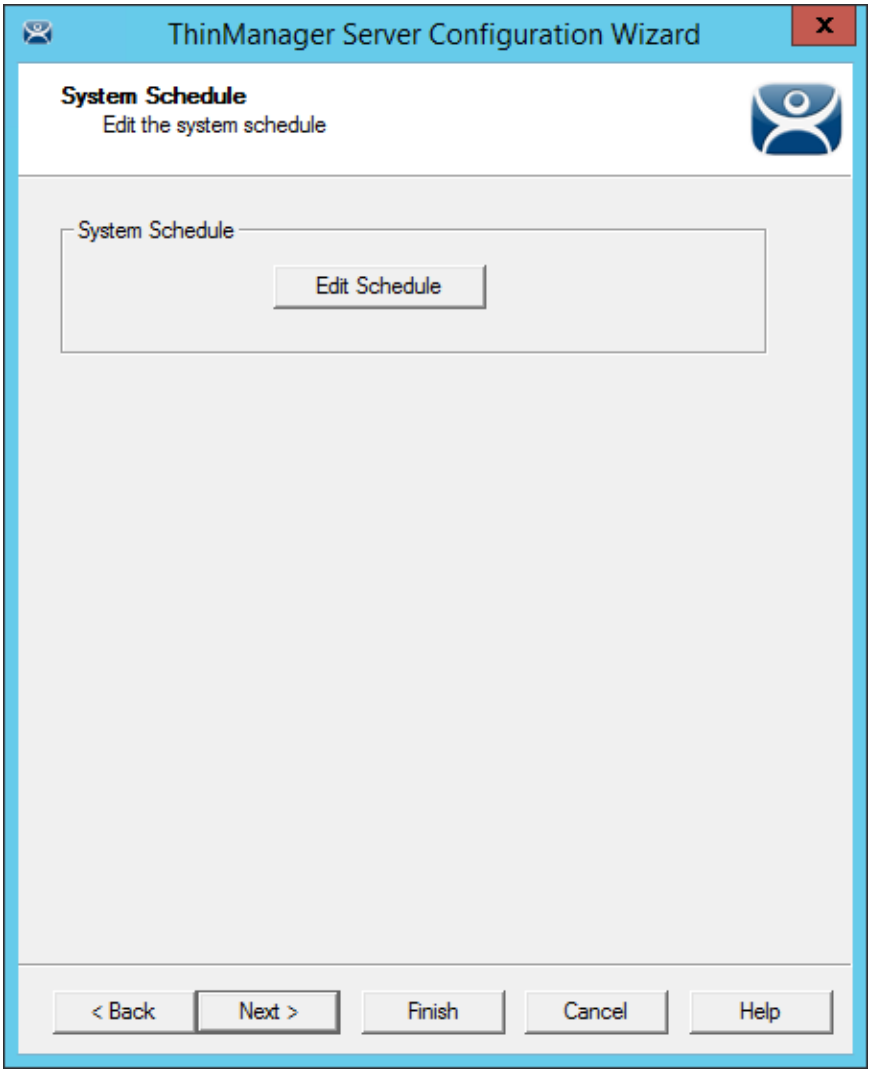
Scheduling is available for more than running reports. Schedules can be created for:

- The System in the ThinManager Server Configuration Wizard.
- Terminals in the Terminal Configuration Wizard.
- Remote Desktop Servers in the Remote Desktop Server Configuration Wizard.
- TermSecure Users in the Relevance User Configuration Wizard.

28.1. System Scheduling of Reports

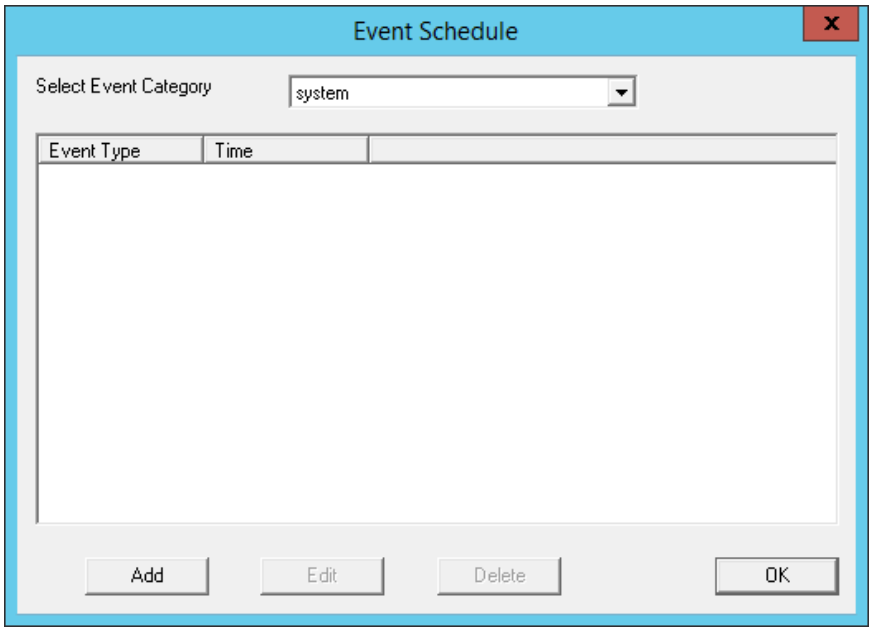
Reports are scheduled on the **ThinManager Server Configuration Wizard.**

Open the **ThinManager Server Configuration Wizard** to schedule report generation by highlighting the **ThinManager Server** icon, right clicking, and selecting ***Modify***.



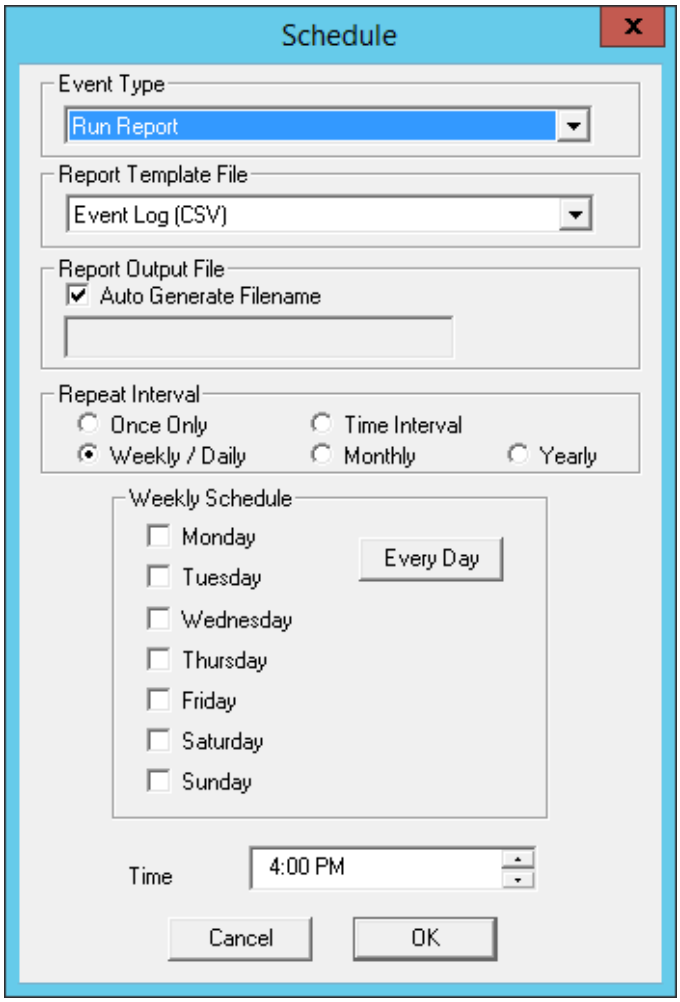
ThinManager Server Configuration Wizard – System Schedule

Navigate to the **System Schedule** page and select the ***Edit Schedule*** button to launch the **Event Schedule** window.



Event Schedule Window

Select the ***Add*** button to open the **Schedule** window.



Schedule Window

The Schedule window allows system events to be configured.

Event Type – This drop-down allows the event to be chosen. There are three types:

- **Backup Biometric Database** – This allows the scheduling of automatic backup of the biometric (fingerprint) data. The fingerprint data is kept in a separate database.
- **Backup Configuration Database** – This allows an automatic scheduling of the configuration database.
- **Run Report** – This allows a report to be run and saved as a ***.html** file on a regular basis.

Report Template File – This drop-down allows you to select the type of report and whether to save as ***.html** or ***.CSV.**

- ***Report Template File*** - This drop-down allows the selection of the report to run.

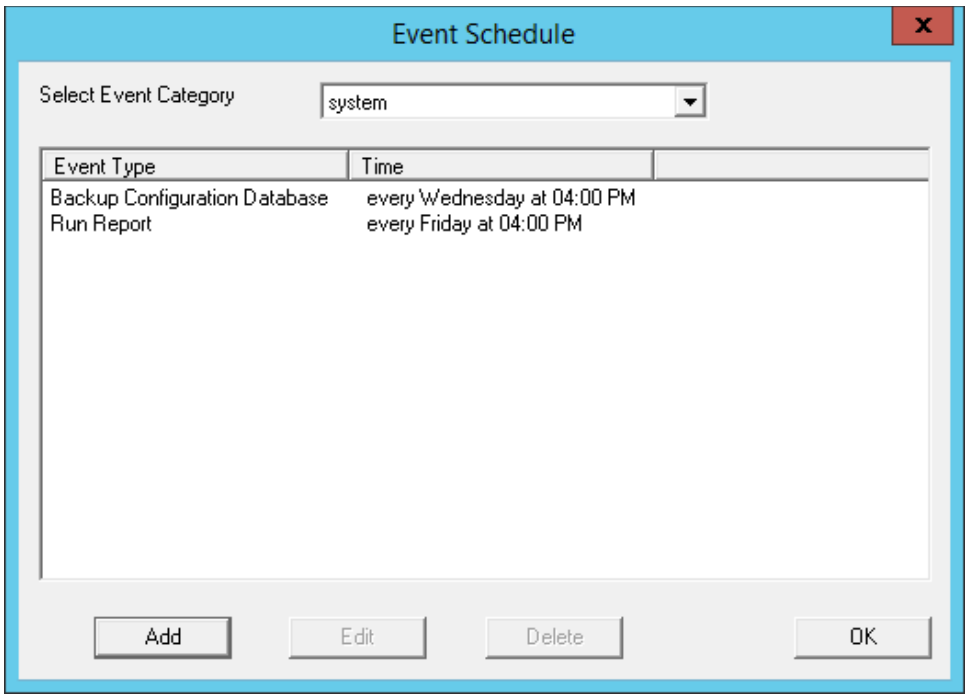
Report Output File – This applies the naming convention to the saved reports.

- ***Auto Generate Filename*** – This checkbox, if selected, will save the file to the ThinManager folder with the report name and a time stamp as its title.
- If the ***Auto Generate Filename*** is unselected, the field allows entry of the desired filename. The filename needs to end in **.html** or ***.CSV** depending on the template.

There are a few switches that allow the file name to be modified with a timestamp for identification purposes. If you do not use a timestamp, the file will be overwritten each time the report is run.

- **%c** – Adds date and time
- **%h** – adds hour (0-24)
- **%M** – adds minute (0-59)
- **%x** – adds date
- **%X** – adds time
- ***Repeat Interval*** – These radio buttons allow the frequency of the report generation to be set.
- ***Time*** – The fields to set the time of the report generation changes to match the ***Report Interval*** selected by the radio button. The ***Time*** field may allow dates, days, hours, or intervals to be set for the report.

Once the report is configured, select ***OK*** to accept the report schedule.

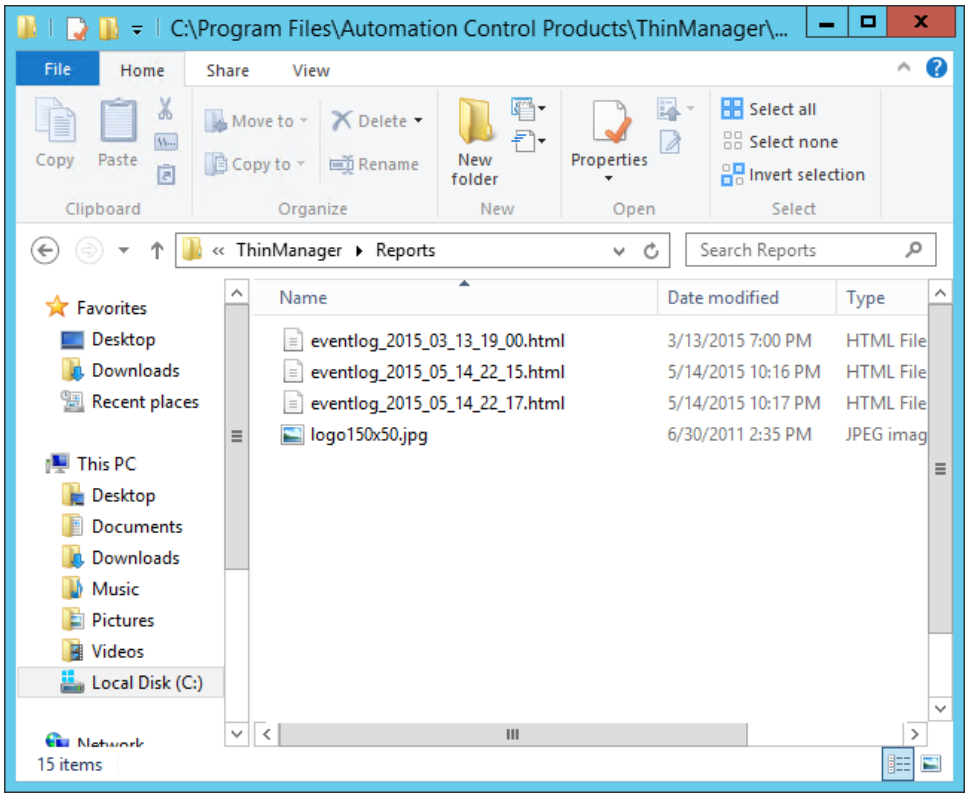


Event Schedule

The scheduled report will be displayed in the Event Schedule window.

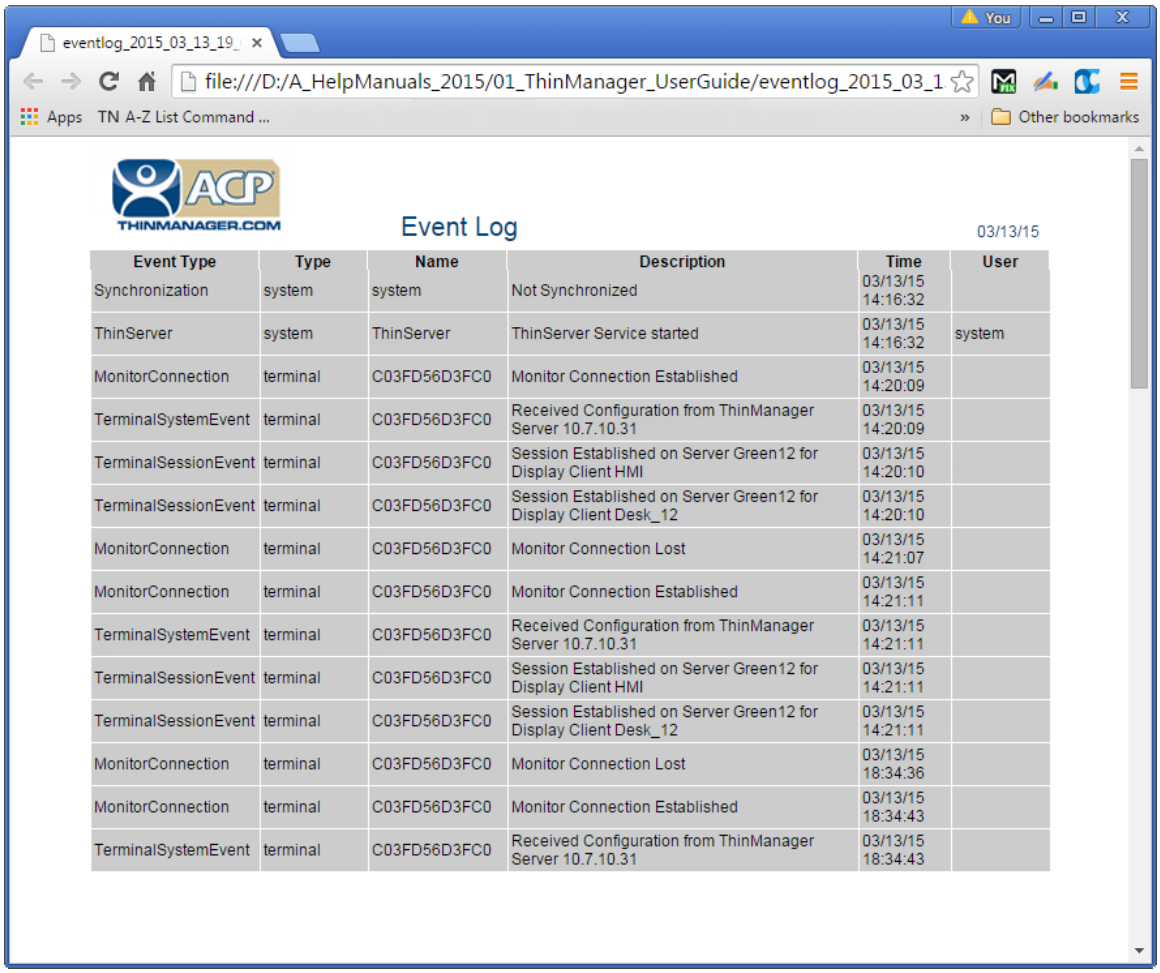
- Select ***Add*** to add another report schedule.
- Select ***Edit*** to edit the schedule of a highlighted report.
- Select ***Delete*** to delete the schedule of a highlighted report.
- Select ***OK*** to accept the schedules and close the window.

When a report is run the files are saved for viewing.



Saved Reports

Once the report has run it can be opened in a web browser if or ***.HTML** or in a spreadsheet app if ***.CSV**.



Event Type	Type	Name	Description	Time	User
Synchronization	system	system	Not Synchronized	03/13/15 14:16:32	
ThinServer	system	ThinServer	ThinServer Service started	03/13/15 14:16:32	system
MonitorConnection	terminal	C03FD56D3FC0	Monitor Connection Established	03/13/15 14:20:09	
TerminalSystemEvent	terminal	C03FD56D3FC0	Received Configuration from ThinManager Server 10.7.10.31	03/13/15 14:20:09	
TerminalSessionEvent	terminal	C03FD56D3FC0	Session Established on Server Green12 for Display Client HMI	03/13/15 14:20:10	
TerminalSessionEvent	terminal	C03FD56D3FC0	Session Established on Server Green12 for Display Client Desk_12	03/13/15 14:20:10	
MonitorConnection	terminal	C03FD56D3FC0	Monitor Connection Lost	03/13/15 14:21:07	
MonitorConnection	terminal	C03FD56D3FC0	Monitor Connection Established	03/13/15 14:21:11	
TerminalSystemEvent	terminal	C03FD56D3FC0	Received Configuration from ThinManager Server 10.7.10.31	03/13/15 14:21:11	
TerminalSessionEvent	terminal	C03FD56D3FC0	Session Established on Server Green12 for Display Client HMI	03/13/15 14:21:11	
TerminalSessionEvent	terminal	C03FD56D3FC0	Session Established on Server Green12 for Display Client Desk_12	03/13/15 14:21:11	
MonitorConnection	terminal	C03FD56D3FC0	Monitor Connection Lost	03/13/15 18:34:36	
MonitorConnection	terminal	C03FD56D3FC0	Monitor Connection Established	03/13/15 18:34:43	
TerminalSystemEvent	terminal	C03FD56D3FC0	Received Configuration from ThinManager Server 10.7.10.31	03/13/15 18:34:43	

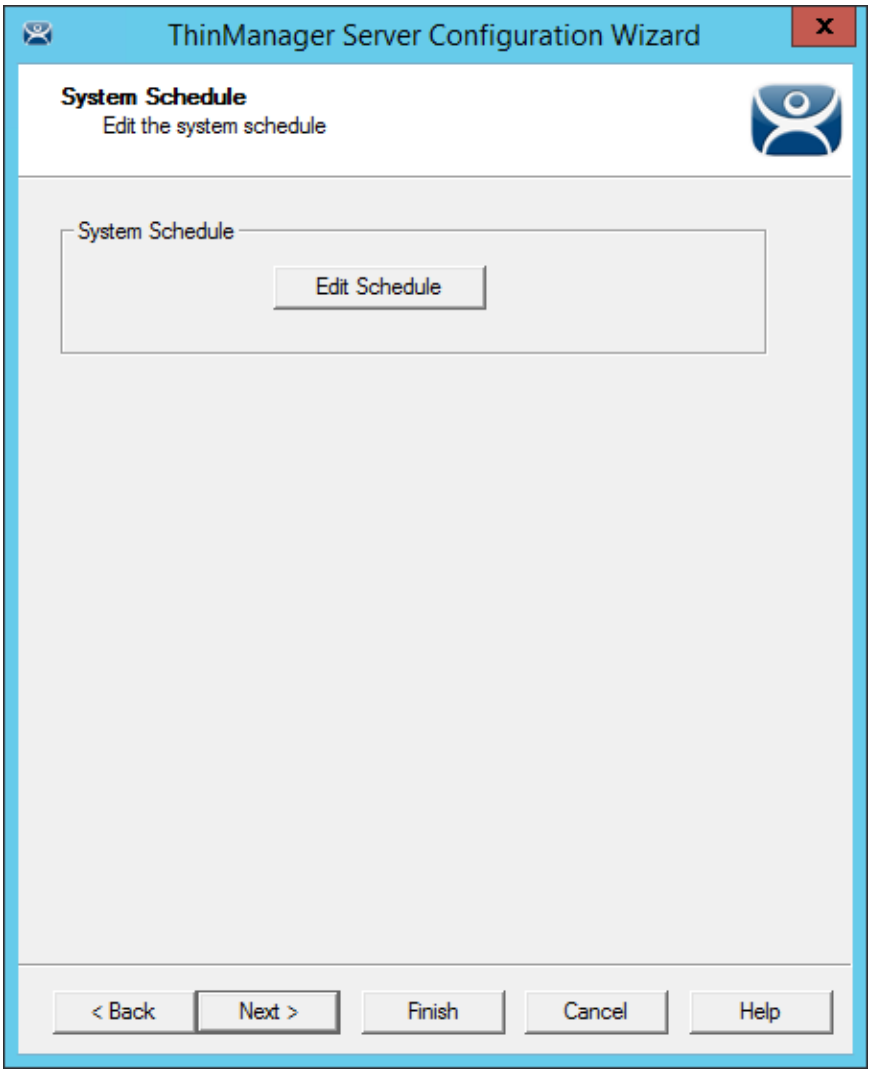
Report Shown in Browser

Once the report is generated the data can be saved or reformatted as desired using standard HTML tools.

28.2. Scheduling Configuration Backups

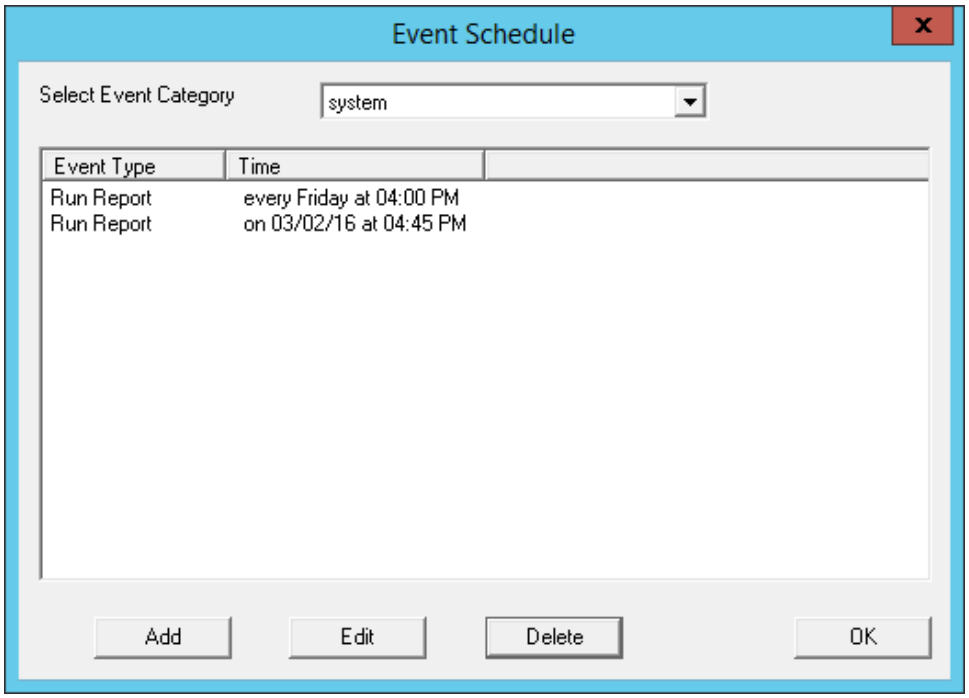
It is a good idea to back up your ThinManager configuration before you make any major changes. You can use the Scheduler to do this automatically.

Open the **ThinManager Server Configuration Wizard** to schedule report generation by highlighting the ThinManager Server and selecting ***File > Modify***.



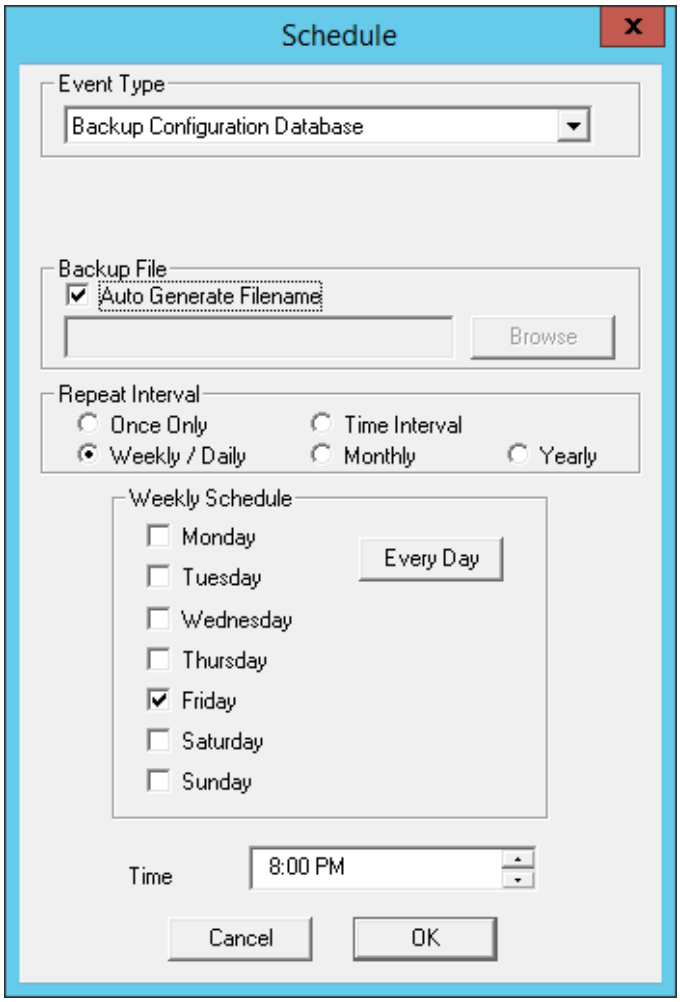
ThinManager Server Configuration Wizard – System Schedule

Navigate to the **System Schedule** page and select the ***Edit Schedule*** button to launch the **Event Schedule** window.



Event Schedule Window

Select the ***Add*** button to open the **Schedule** window.



Schedule Window

The **Schedule** window allows system events like configuration backups to be created.

- Select *Backup Configuration Database* from the Event Type drop-down.
- Select an interval. *Weekly* is adequate.
- Select a day and time.
- Select *OK* to accept the changes.

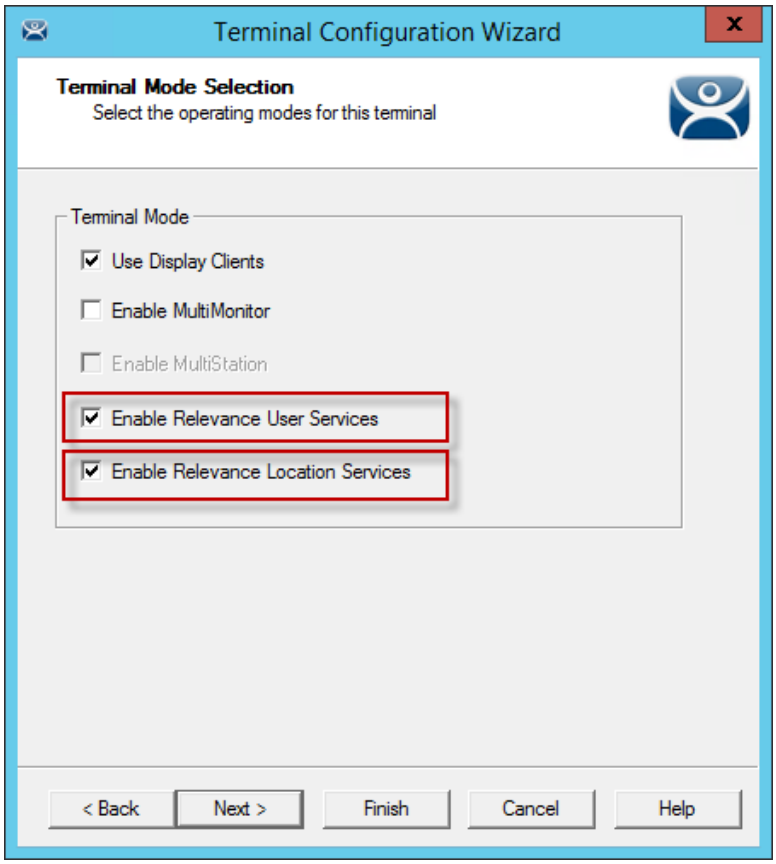
A weekly backup allows you to have a current configuration available in case you need one.

29. Introduction to Relevance

Relevance extends control and management within the ThinManager system. It is integrated into ThinManager with the XLr license.

Relevance is the ***How*** to provide ***What*** you need, ***Where*** and ***When*** you need it.

Relevance has two main functions, the **Relevance User Services** and the **Relevance Location Services**.



Terminal Mode Selection Page of the Terminal Configuration Wizard

Relevance User Services was formerly known as TermSecure. It grants and denies access to applications based on permissions and membership in Access Groups.

It is activated by selecting the ***Enable Relevance User Services*** checkbox on the **Terminal Mode Selection p**age of the Terminal Configuration Wizard.

See Relevance User Services Introduction on page 456 for details.

Relevance Location Services is Location based computing. This isn't just sending an application to a mobile device, but is a way to enable the location to determine the content sent to the device. The mobile device allows the user to interact with the location.

It is activated by selecting the ***Enable Relevance Location Services*** checkbox on the **Terminal Mode Selection p**age of the Terminal Configuration Wizard.

See Relevance Location Services on page 579 for details.

Relevance Location Services has two types of locations, **Assigned** and **Unassigned**.

Assigned locations are locations that have a Terminal and monitor at the given location, much like traditional computing. Relevance adds additional functions to the location that allows mobile devices to

interact with the location and Shadow the Terminal, Clone the applications, or Transfer the control of the location to the mobile device.

Unassigned locations are locations that lack a permanent Terminal and monitor and all of the content is sent to the mobile device. The mobile device becomes the Terminal.

30. Relevance User Services Introduction

Relevance User Services is a ThinManager feature that allows users to use a ThinManager Ready thin client to access user-specific or Terminal-specific Display Clients. This does not replace the Windows logon, but adds an additional layer of security and control to the Window login. This function was formerly called TermSecure.

Relevance User Services has two main functions, **hiding applications from unauthorized users** and **deploying applications to a user at any location**.

- **Permission Deployed Applications:** You can assign a display client to a Terminal and keep it hidden from users until they login with the correct Permissions.
  A user with the proper Relevance User credentials will be able to reveal and access the hidden application.
  An example would be a recipe program that would allow a supervisor to initiate a product change. This belongs to the station on the floor but you want to prevent operators from initiating the change.
- **Roaming User-specific Applications:** You can assign Display Clients to a Relevance user and they can get access to their applications from any Terminal in the system. This can be initiated by either manual login or the use of an authentication device.
  This allows a user to leave one Terminal, logon to a different Terminal, and reconnect to their session, essentially having the session follow him from Terminal to Terminal.
  An example would assign a session with reports to a quality control worker who could login anywhere and retrieve their reports.

Permission Deployed Applications are controlled with **Permissions**. This is covered in Permission Deployed Applications in Relevance on page 457.

Roaming User-specific Applications are controlled by adding the Display Client to the Relevance User configuration. This is covered in Assigning Roaming Display Clients to a Relevance User on page 482.

The **Relevance User Services** section is organized into several sections to walk through the process.

Permission Deployed Applications – See Permission Deployed Applications in Relevance on page 457.

- Creating Access Groups is on page 460.
- Creating Relevance Users and applying Permissions is on 472
- Applying Access Group Permission to Display Clients is on page 463.
- Deploying the Display Clients to Terminals is on page 467.
- Logging into the system is on page 477.

User-specific Applications – See Assigning Roaming Display Clients to a Relevance User on page 482.

- Creating Relevance Users is on page 484.
- Creating login strategies is on 482
- Applying Display Clients is on page 494.
- Configuring Terminals for roaming access is on page 467.

- Logging into the system is on page 501.

Using Active Directory to Create Relevance Users – See Password and Account Management on page 535.

- Creating Relevance Users with Active Directory is on page 527.

31. Permission Deployed Applications in Relevance

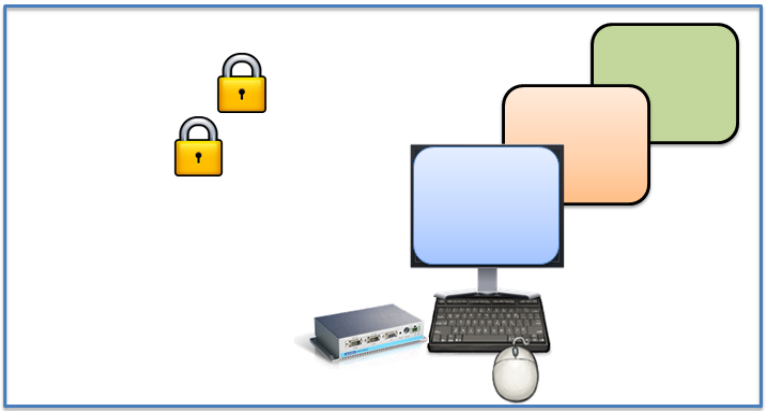
Relevance User Services can use **Access Group Permissions** to control access to display clients on a Terminal. Since the display clients belong to the Terminal they are started with the Terminal's Windows account. The Relevance user does not need a Windows account to start the session.

The scenario described in this section to explain the concept of Access Groups, Permissions, and Relevance Users will not have a Windows account tied to it. Window accounts will be covered in

Create the Relevance User using Active Directory on page 484.

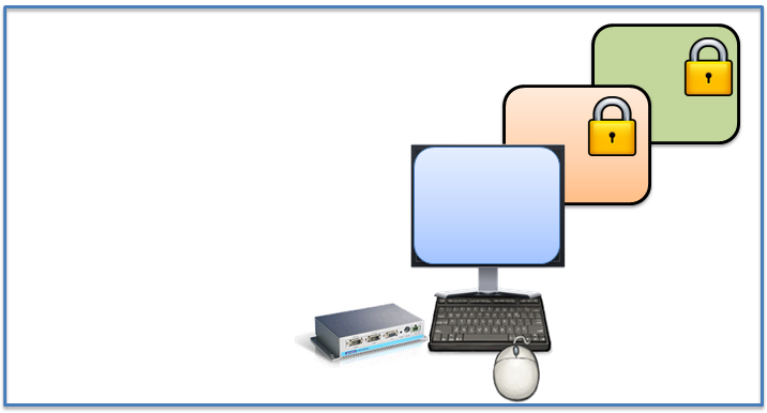
31.1. Permission Deployed Applications Diagram

This is a graphical representation of controlling access to display clients by using the Permission tied to Access Groups.



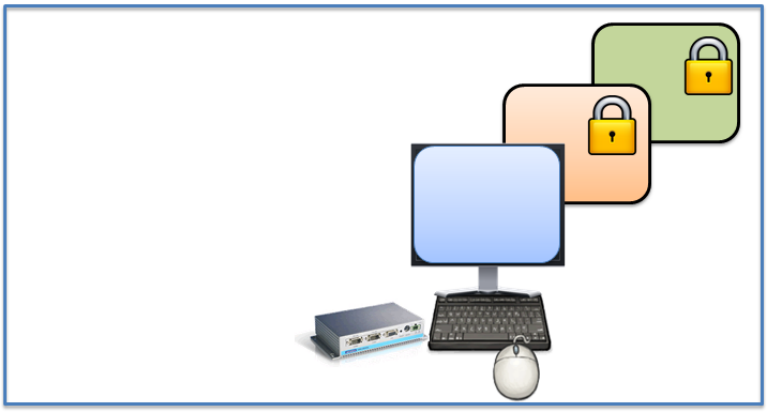
Create Access Groups

See Relevance Access Group Creation on page 460.



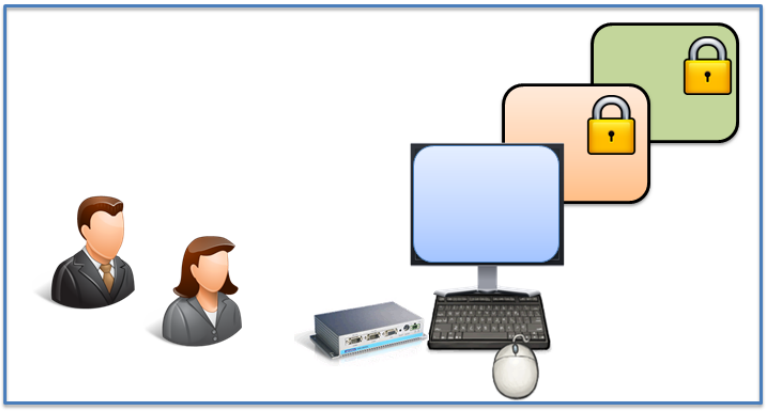
Apply Access Groups to Display Clients

See Add Access Group to a Display Client on page 463.



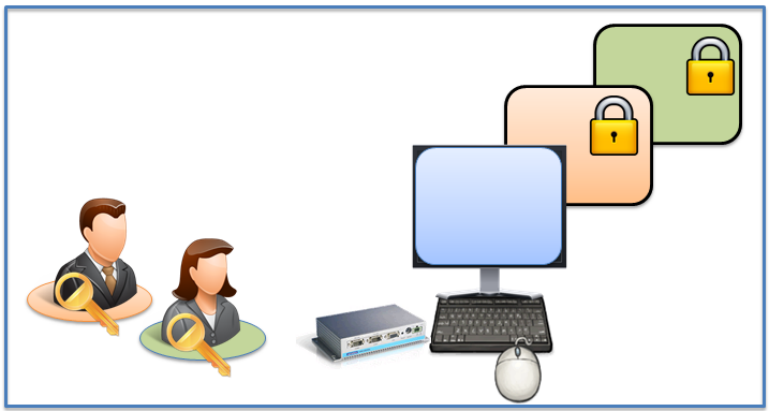
Configure Terminals for Relevance

See Configure Terminals for Relevance on page 467.



Create Relevance Users

See Create the Relevance User without a Windows Account on page 472.



Apply Access Groups to Relevance Users

See Create the Relevance User without a Windows Account on page 472.

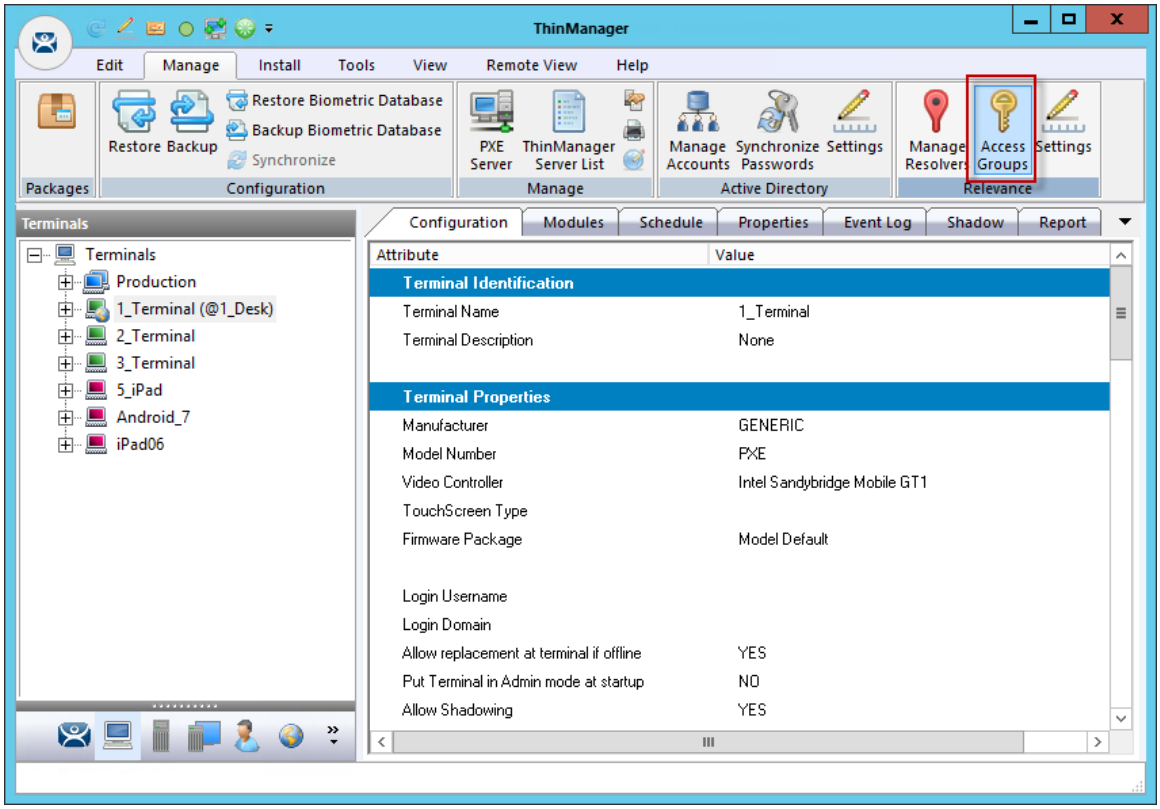
Logging In with Access Group Permission Unlocks Display Client

See Logging On to Relevance on page 477.

Different Permissions Grant Access to Different Display Clients

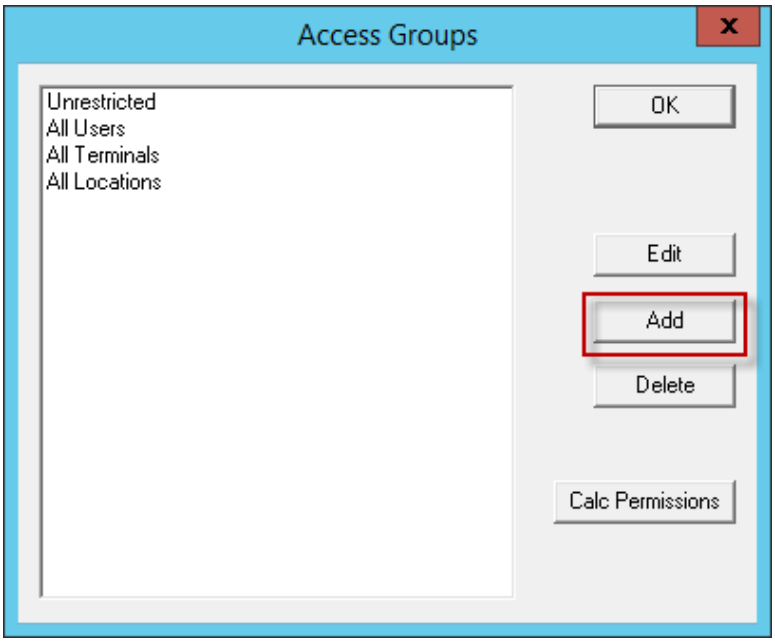
See Logging On to Relevance on page 477.

31.2. Relevance Access Group Creation



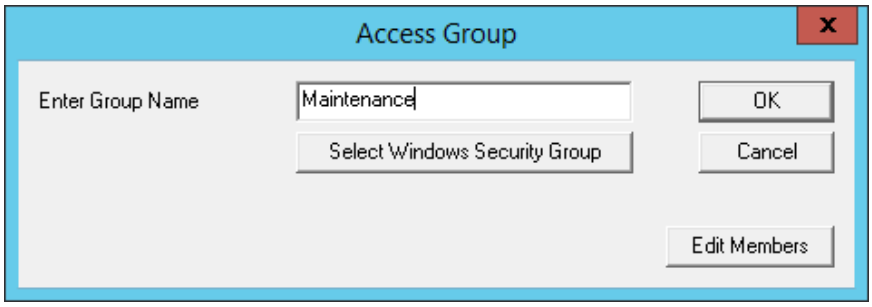
Access Group on ThinManager Menu Bar

The **Access Groups** window is launched by selecting ***Manage > Access Groups*** in the Relevance section of the ThinManager menu bar.



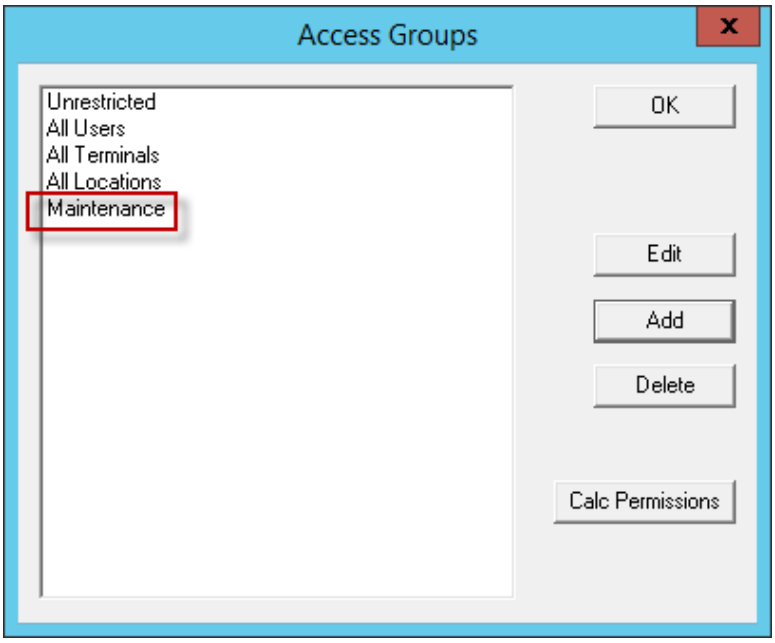
Access Groups Window

The ***Add*** button opens the **Access Group** window that lets you define an Access Group.



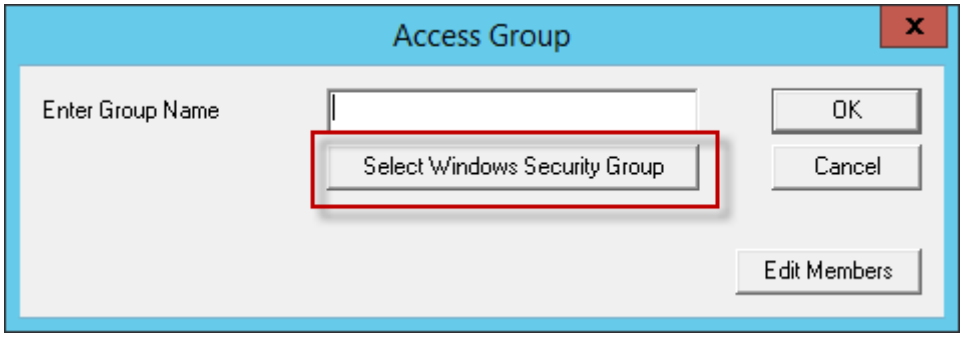
Access Group Window

Enter a name for your Access Group in the ***Enter Group Name*** field and select the ***OK*** button.



Access Groups Window

The Access Group will be listed and available for use to grant or deny access to display clients.

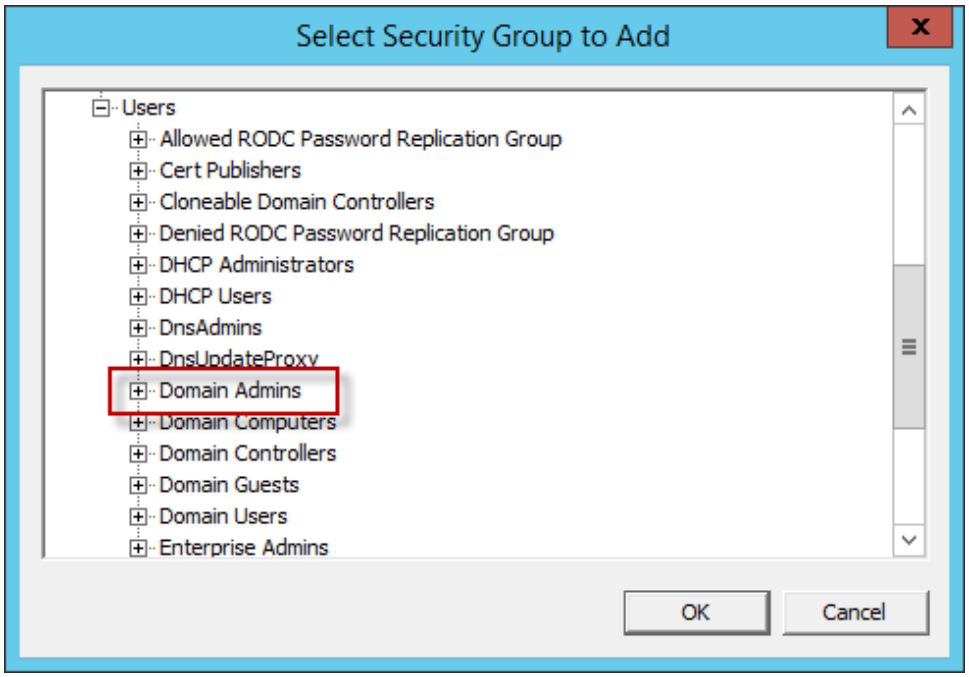


Access Group Window

Windows Security Groups can be added as Access Groups in a domain.

Launch the **Access Group** window by selecting the ***Add*** button on the **Access Groups** window.

Select the ***Select Windows Security Group*** button on the **Access Group** window. This will launch the **Select Security Group to Add** window.



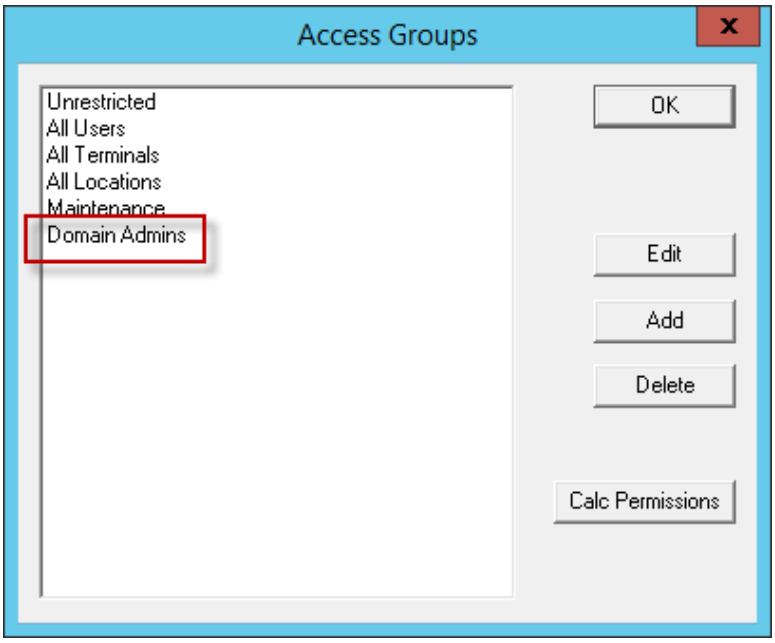
Select Security Group to Add Window

The **Select Security Group to Add** window will show the Active Directory tree.

Highlight the desired Windows group and select the ***Add*** button.

Access Group Window

This adds the Windows security group to the ***Enter Group Name*** field. The Windows security group will be added to the Access Groups once you select the ***OK*** button.



Windows Security Group as Access Group

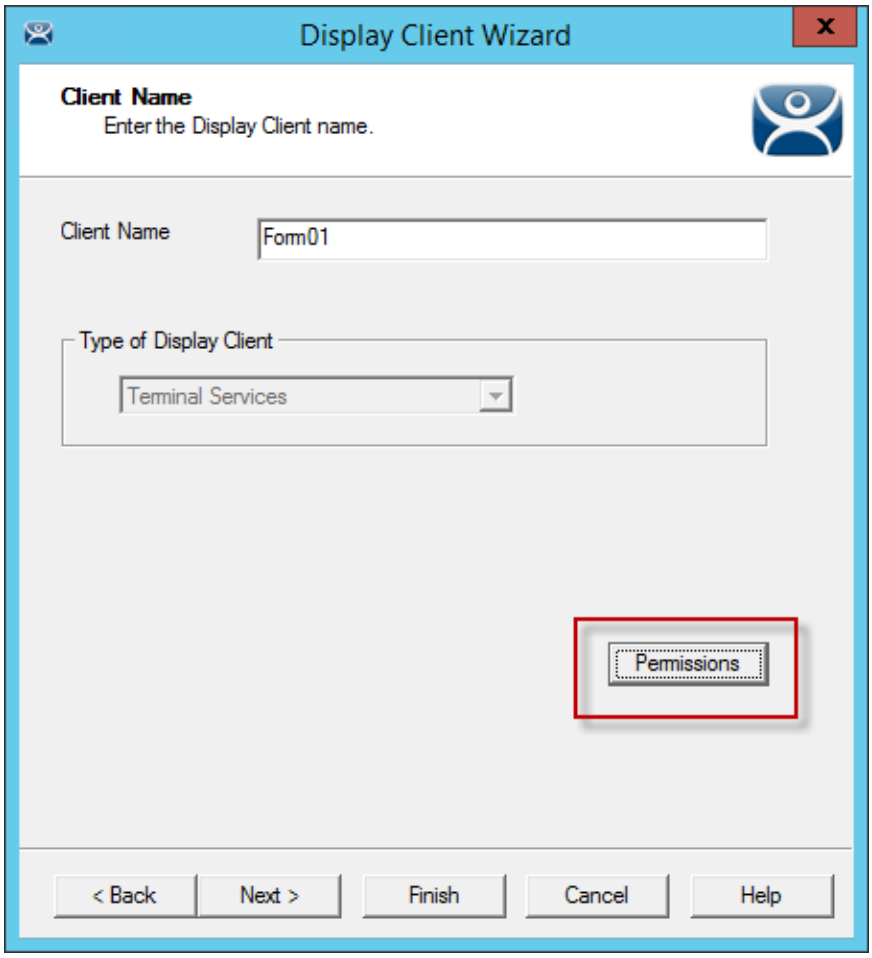
The Windows Security Group is now an Access Group and is available for use to grant or deny access to display clients

31.3. Add Access Group to a Display Client

You need to add the Access Group to the Display Client that you want to hide from un-authorized users. This example will use **Form01** and **Form02**.

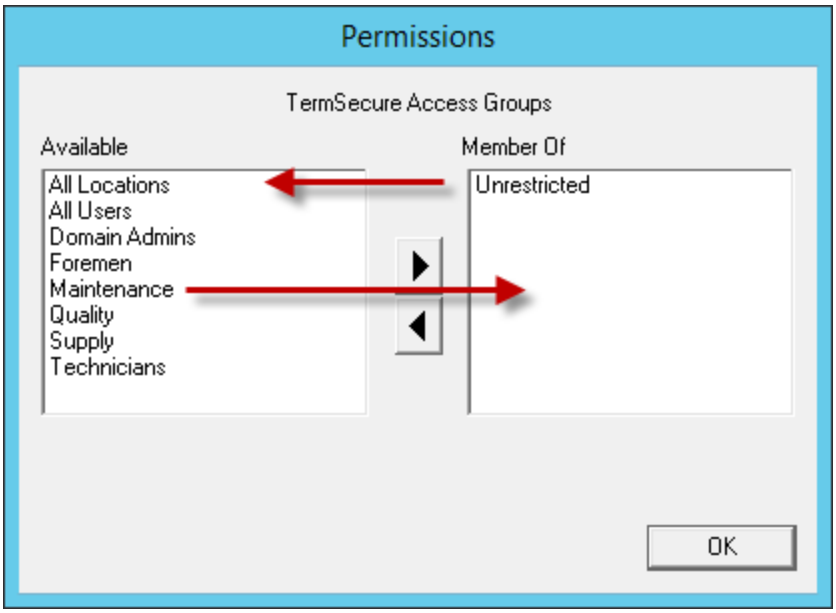
Relevance Access Group	Display Client	Relevance User
Maintenance	Form01	Mike, Bob
Supply	Form02	Steve, Bob

Double click on the desired display client in the ThinManager tree to launch the **Display Client Wizard**.



Client Name Page of the Terminal Configuration Wizard

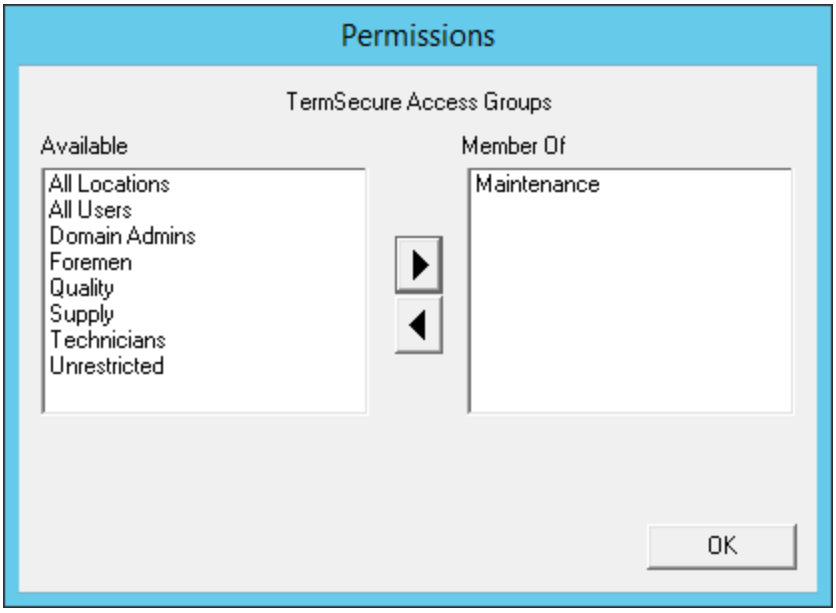
Select the ***Permissions*** button on the **Client Name** page to open the **Permissions** window.



Display Client with Permissions Window

Display clients are members of the ***Unrestricted*** group by default.

Remove ***Unrestricted*** from the **Member Of** list by highlighting it and selecting the ***left arrow*** or double clicking.



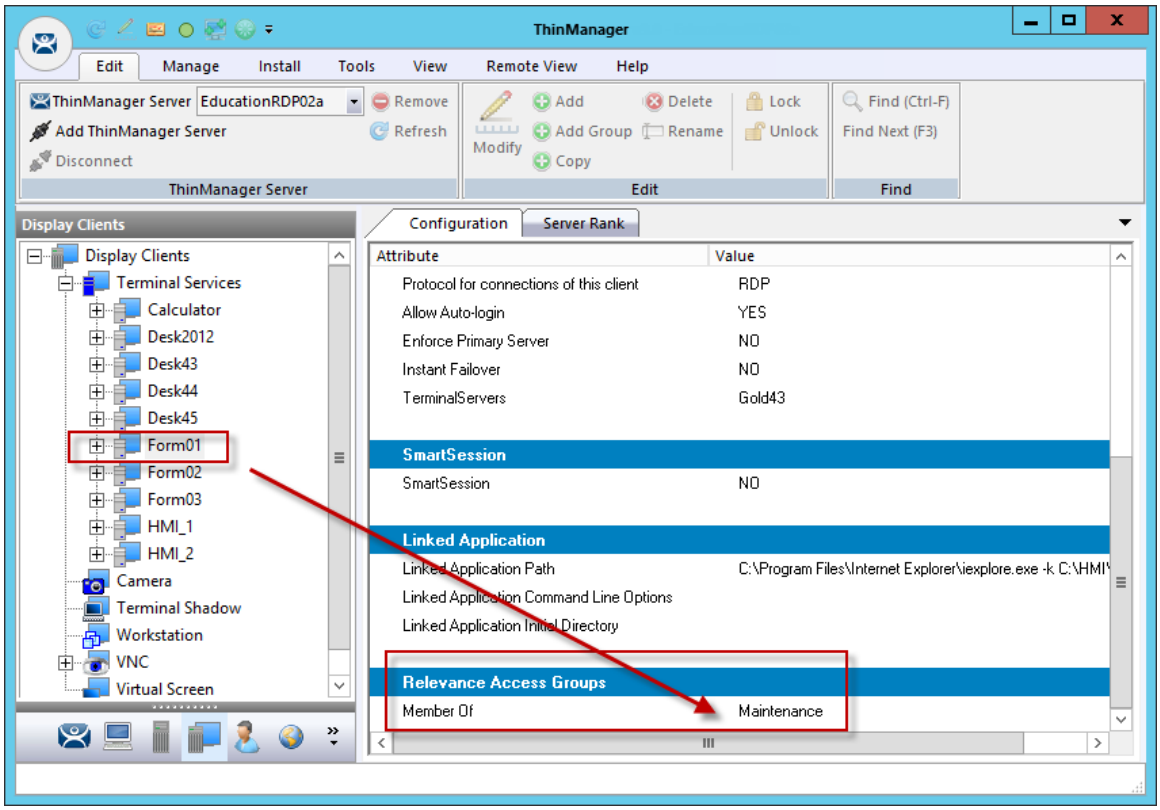
New Group Membership

Add the desired ***Access Group*** to the ***Member Of*** list by highlighting it and selecting the ***right arrow*** or double clicking. A display client can have several Relevance Access Groups added to it.

The **Permissions** window will show the Relevance Access Group membership.

Select the ***OK*** button to accept the change.

Select the ***Finish*** button to close the **Display Client Wizard** and accept the changes.



Display Client Configuration Properties

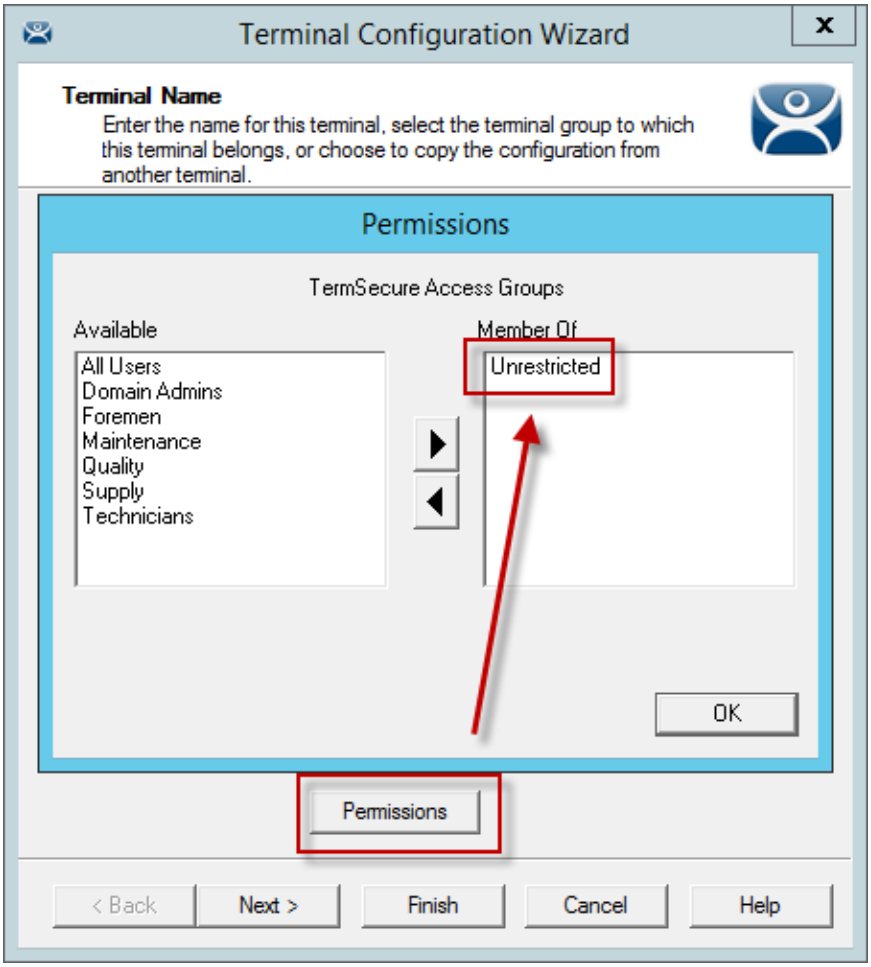
You can see Relevance membership quickly by highlighting the display client in the Display Client tree and selecting the **Configuration** tab. The **Relevance Access Group** membership is at the bottom.

This was repeated to assign **Supply** to **Form02** for this example.

31.4. Configure Terminals for Relevance

Each Terminal can be configured to allow Relevance logins.

Double-click on a Terminal in the ThinManager tree to open the **Terminal Configuration Wizard**.



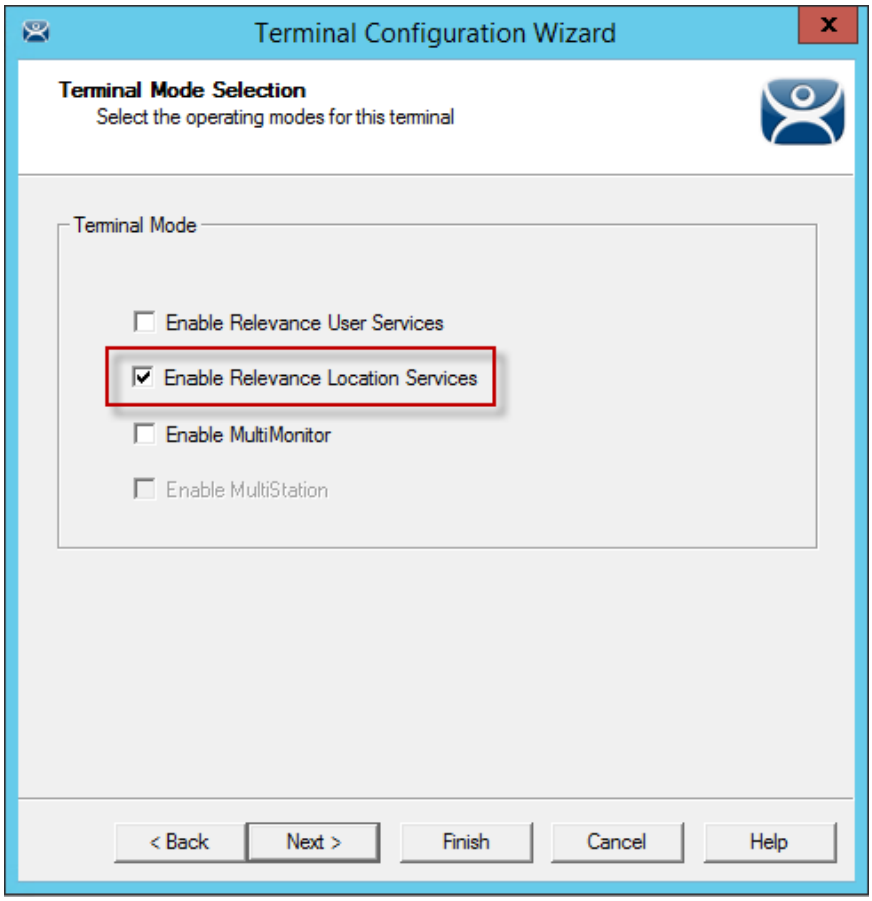
Default Terminal Permissions

Terminals are members of the ***Unrestricted*** Access Group by default. This allows any user to use the Terminal. Leave it this way unless you want to require a Relevance login to allow any access at all.

Note: Setting an Access Group in Permissions for a Terminal will lock users out of the Terminal until they login with a Relevance User account

---

Relevance Access is configured on the **Terminal Mode Selection** window.



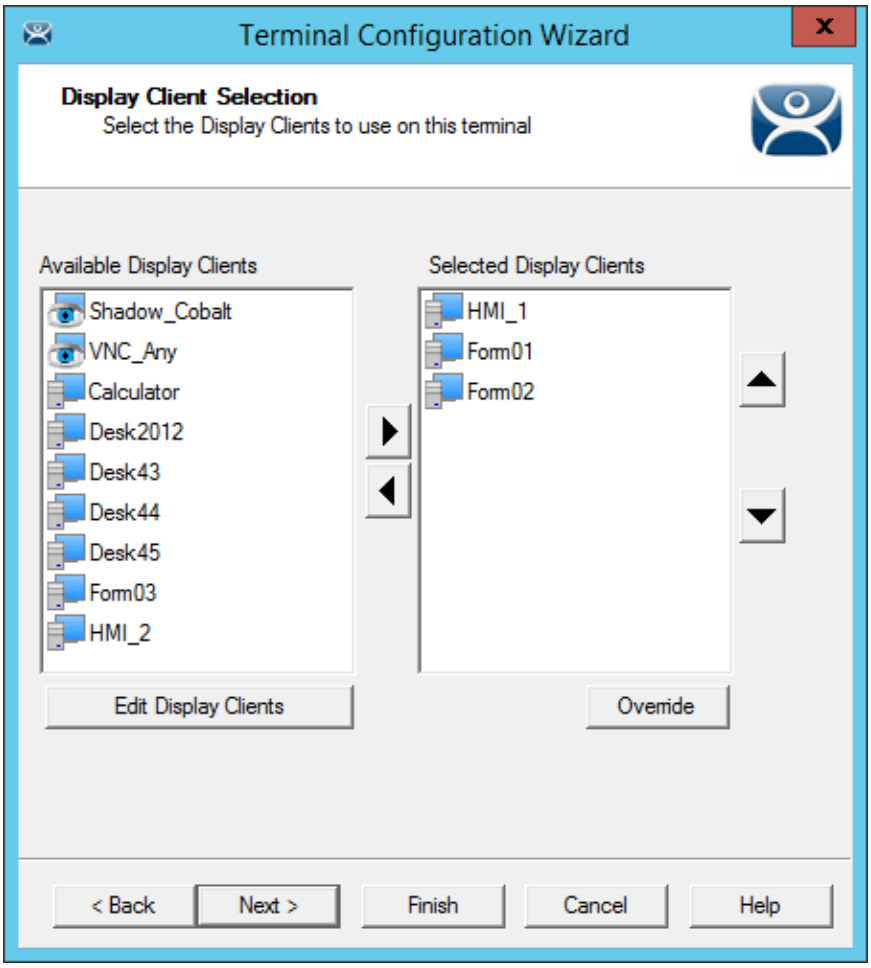
Terminal Mode Selection

Select the ***Enable Relevance*** checkbox to enable Relevance logins on the Terminal.

Note: You must use Display Clients with Relevance.

You may use Relevance User Services in combination with MultiMonitor and/or Relevance Location Services.

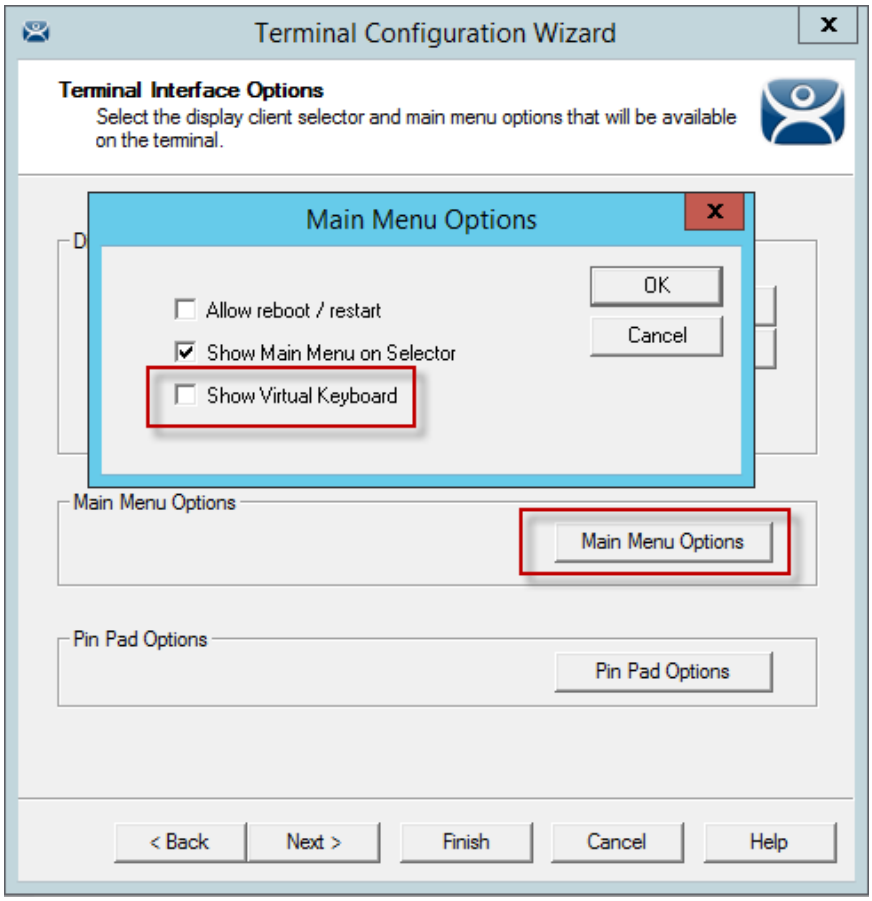
Select ***Next*** and navigate to the **Display Client Selection** page.



Display Client Selection

Add the display clients to the Terminal. In this example **HMI_1** is ***Unrestricted***, **Form01** is restricted to ***Maintenance***, and **Form02** is restricted to ***Supply***.

Select ***Next*** and navigate to the **Terminal Interface Options** page.



Terminal Interface Options Page

When ***Enable Relevance*** is selected on the **Terminal Mode Selection** page, a ***Main Menu Options*** button will be displayed on the **Terminal Interface Options** page. This launches the Main Menu Options window.

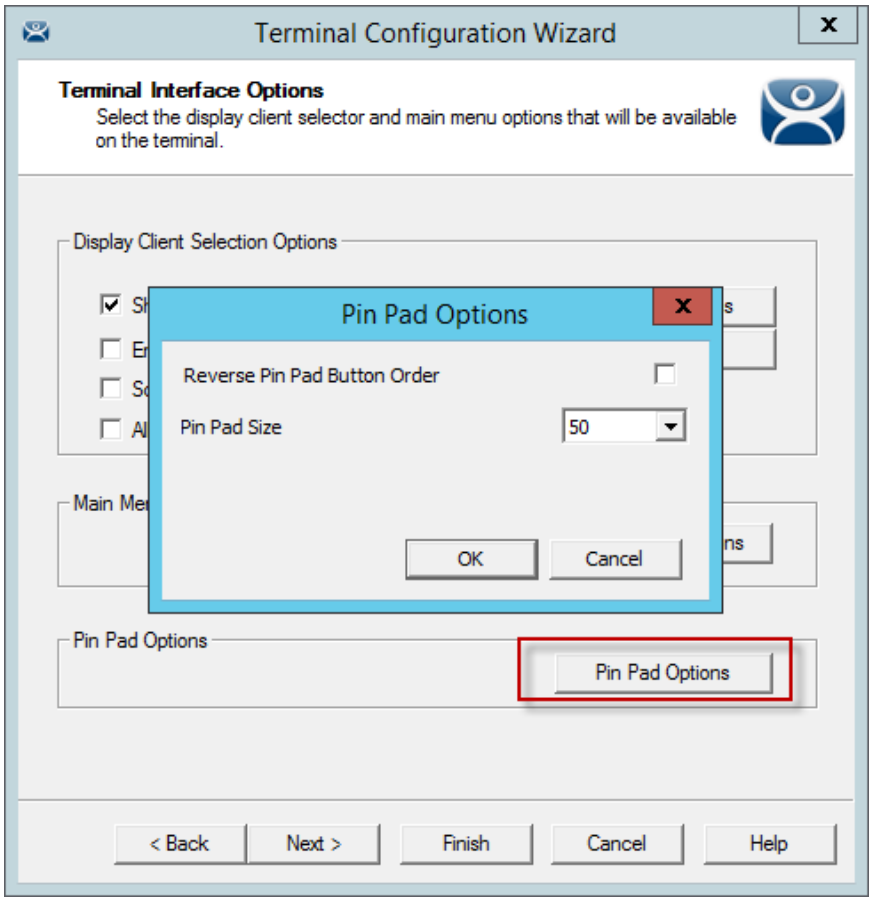
The ***Main Menu Options*** configures the **Relevance Login Menu**.

Select the ***Main Menu Options*** button to launch the **Main Menu Options** window.

- The ***Allow reboot/restart*** checkbox will add ***Reboot*** and ***Restart*** to the menu.
- The ***Show Main Menu on Selector*** checkbox will add the **Relevance Main Menu** to the Display Client drop-down selector.
- The ***Show Virtual Keyboard*** checkbox will show a virtual keyboard to the login process.

✓ **Use the Show Virtual Keyboard to display an on screen keyboard for touch screens.**

Select the ***OK*** button to accept the changes.

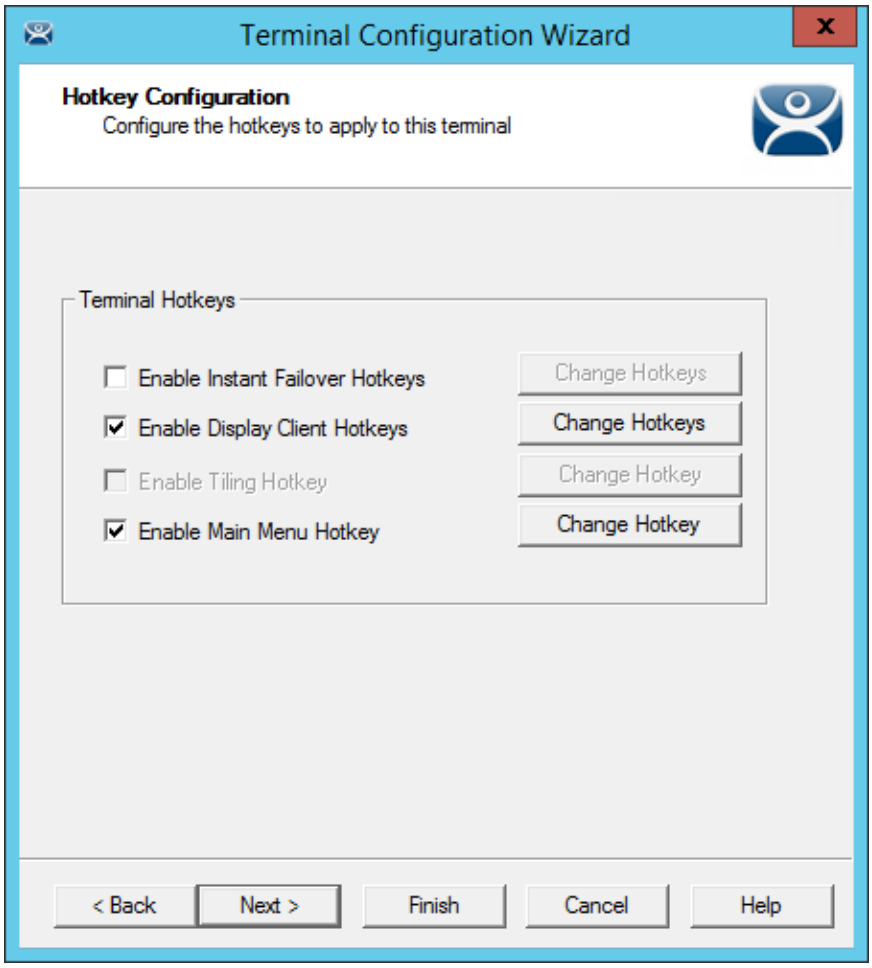


Pin Pad Options Window

The **Pin Pad Options** window allows you to configure the PIN pad when using a Personal Identification Number instead of a password.

- ***Reverse Pin Pad Button Order*** – This checkbox changes the PIN pad from 1-2-3 on the top row like a phone to 7-8-9 on the top row like a calculator.
- ***Pin Pad Size*** – This sets the size of the PIN pad as a percentage of the screen size.

Select ***Next*** on the **Terminal Interface Options** page to navigate to the **Hotkey Configuration** page.



Hotkey Configuration Page

When ***Enable Relevance*** is selected on the **Terminal Mode Selection** page, an ***Enable Main Menu Hotkey*** checkbox is displayed on the Hotkey Configuration page. This allows you to set a keyboard hotkey to launch the Relevance menu.

Select ***Finish*** to apply the changes.

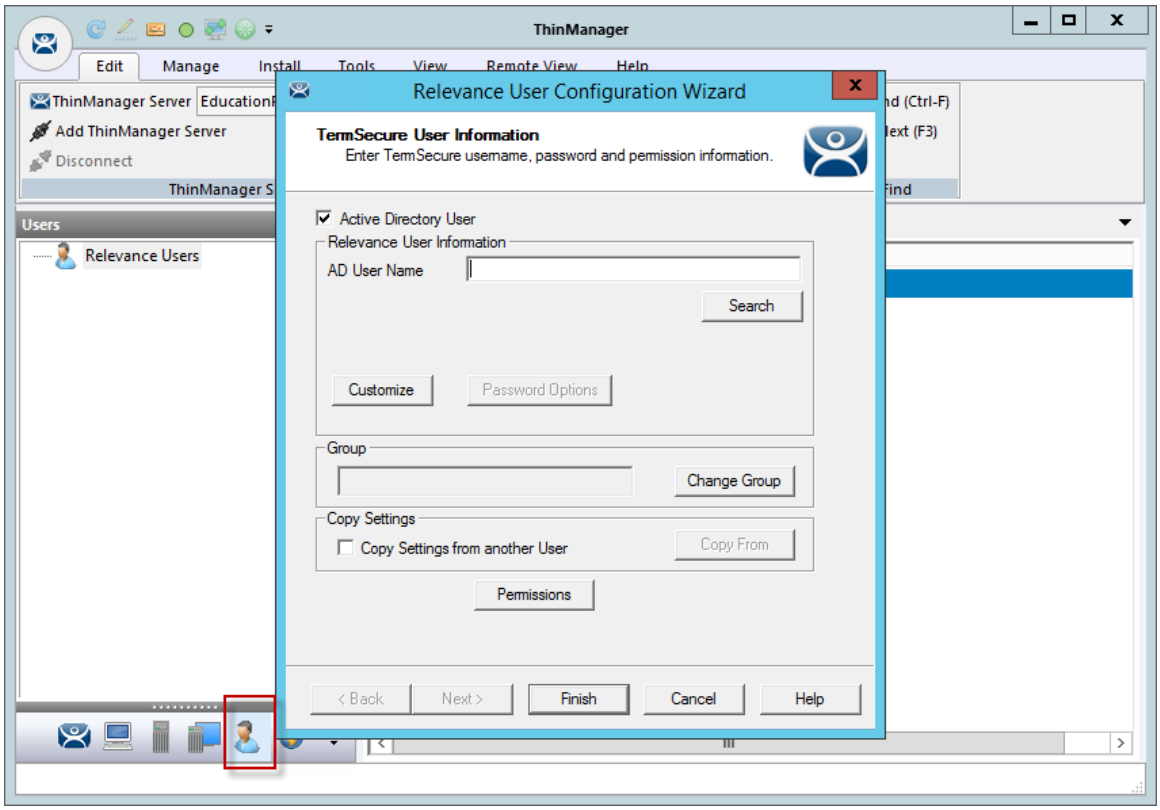
Reboot the Terminal after changes are made.

31.5. Create the Relevance User without a Windows Account

The **Relevance User Configuration Wizard** is launched from the **Relevance User** branch of the ThinManager tree.

Open the **Relevance User** tree by selecting the **User** icon at the bottom of the ThinManager tree.

Right click on the Relevance User branch and select ***Add User*** to launch the **Relevance User Configuration Wizard**.

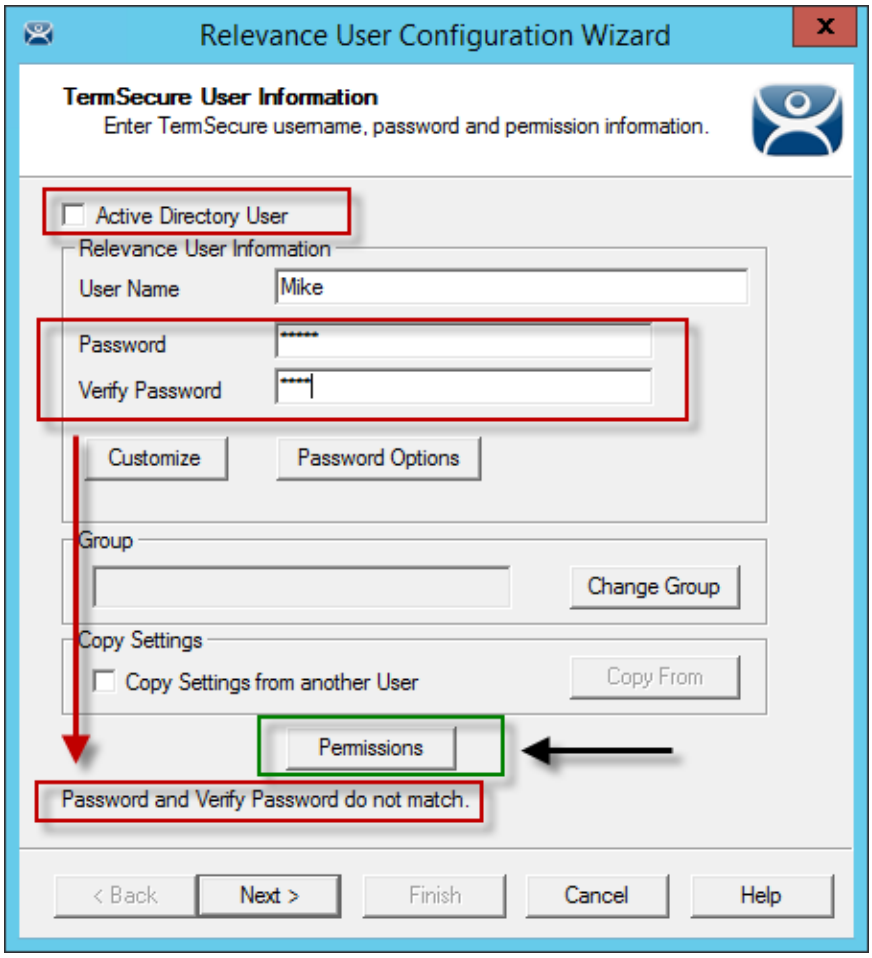


User Branch of the ThinManager Tree

The first page of the **Relevance User Configuration Wizard** is the **Relevance User Information** page that creates the Relevance User account.

Relevance Users that have display clients assigned to them will need to be tied to a Windows account. If a Relevance User does not have a display client assigned to it and it only using the Permissions to access a display client belonging to the Terminal then it does not need a Windows account.

In this scenario a Windows account isn't needed because the display client belongs to the Terminal and is getting logged in with the Terminal's account. A Permission will be applied to the user.



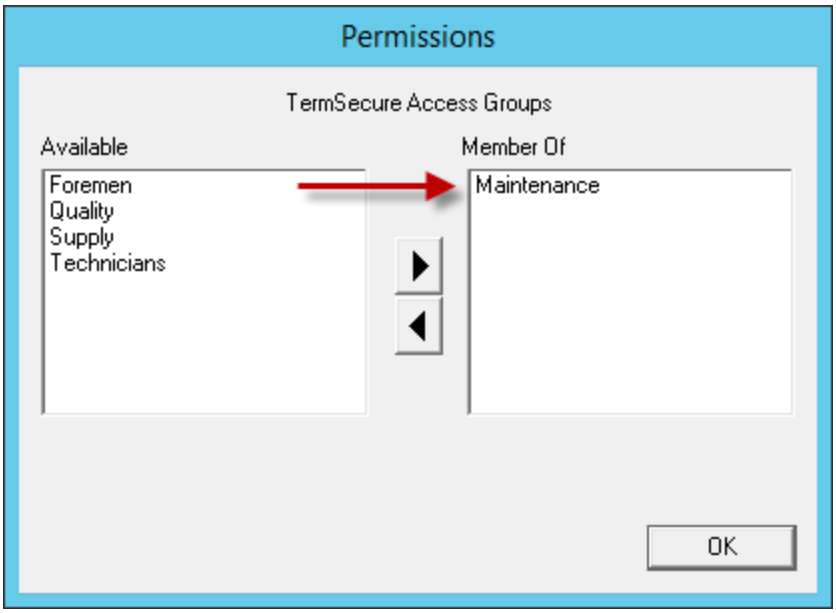
Relevance User Information Page

To create a Relevance User that is not an Active Directory user you first uncheck the ***Active Directory User*** checkbox.

Enter a name in the ***User Name*** field.

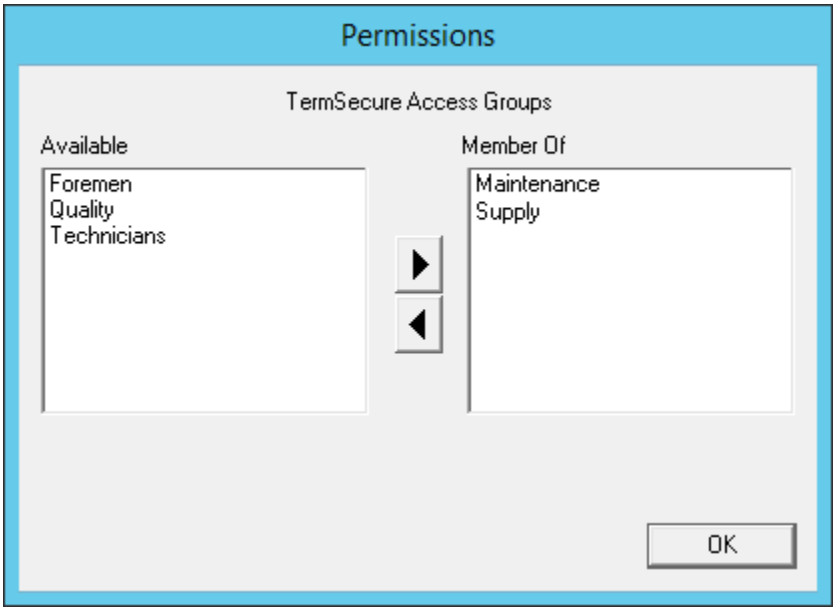
Enter a ***Password*** and ***Verify Password*** fields to provide a password. You will get a message if the passwords don't match.

Select the ***Permissions*** button to launch the **Permissions** window.



Permissions Window

Add your Relevance Access Group to your created user by double clicking on the Access Group in the ***Available*** text box to move it to the ***Member Of*** list.



Multiple Access Groups

A Relevance User can be a member in multiple Access Groups.

Select the ***OK*** button to accept the changes.

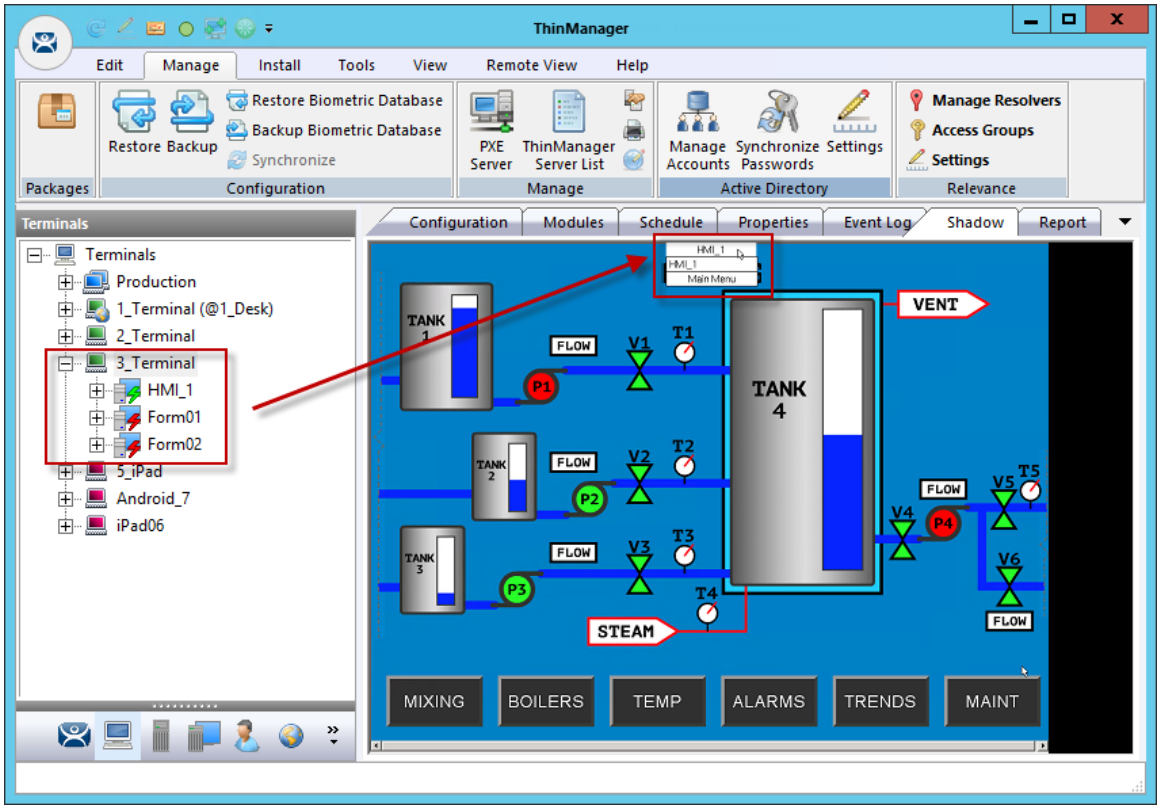
These are the only settings needed for a Relevance User to unlock hidden applications, a Relevance User name and membership in a Relevance Access Group. The wizard has other settings that will be described in section Relevance Configuration Wizard on page 492.

31.6. Relevance Results

This example has the following created:

Relevance Access Group	Display Client	Relevance User
Maintenance	Form01	Mike, Bob
Supervisor	Form02	Steve, Bob

The **3_Terminal** is using Relevance with the unrestricted **HMI_1** display client and the restricted **Form01** and **Form02** display clients.



ThinManager Shadow of Thin Client Example

The example shows the ThinManager tree and the shadowed display of the thin client.

- The Terminal tree shows three display clients assigned to **3_Terminal**. The lightning bolt indicator for the hidden display clients are red to show that it doesn't have a connection. Only **HMI_1** is visible on the Terminal because it is unrestricted.
- The picture shows the group selector in the shadow and displays the "public" display client in the selector, along with the option to launch the Main Menu.

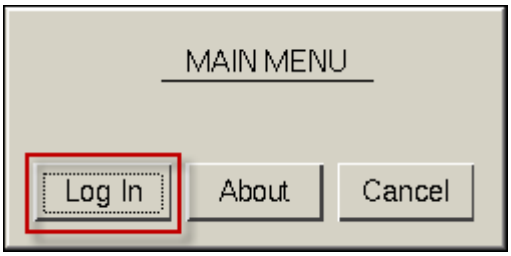
31.7. Logging On to Relevance

To log in a Relevance User on a Terminal, go to a Terminal that has the ***Enable Relevance*** checkbox selected on the **Terminal Mode Specification** page.

You can log in by:

- Opening the display client selector drop-down and selecting ***Main Menu***.
- Typing the ***CTL+m*** hotkey to launch the **Main Menu** if the hotkey checkbox was selected..

The **Main Menu** will be displayed on the Terminal.

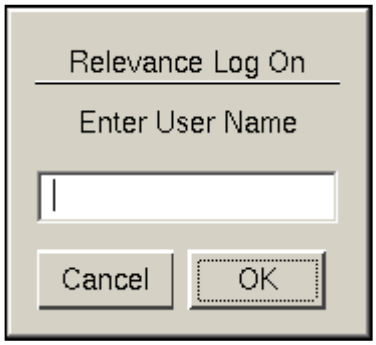


Relevance Main Menu

Select the ***Log In*** button to login.

Relevance Log On Screen with Virtual Keyboard

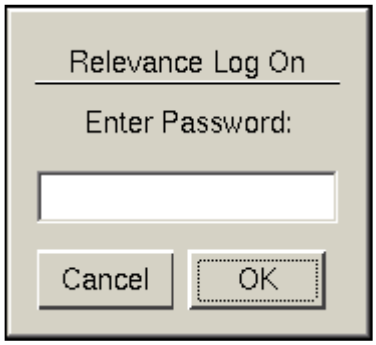
A virtual keyboard will be displayed if ***Show Virtual Keyboard*** was selected on the **Main Menu Options** window when configuring the Terminal for Relevance on the **Terminal Interface Options** page.



Relevance Log On Screen

Enter your Relevance User name in the ***Enter User Name*** field.

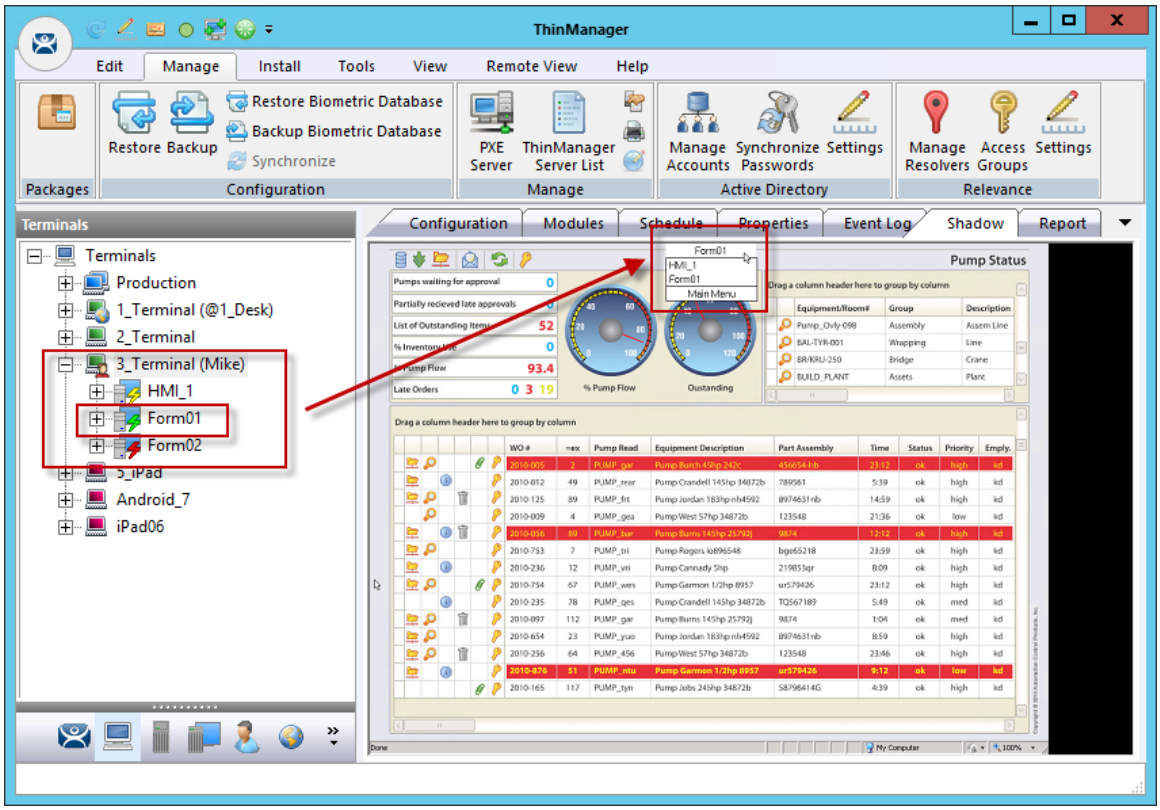
Select **OK**.



Password Screen

Enter the password in the field.

Select the ***OK*** button.

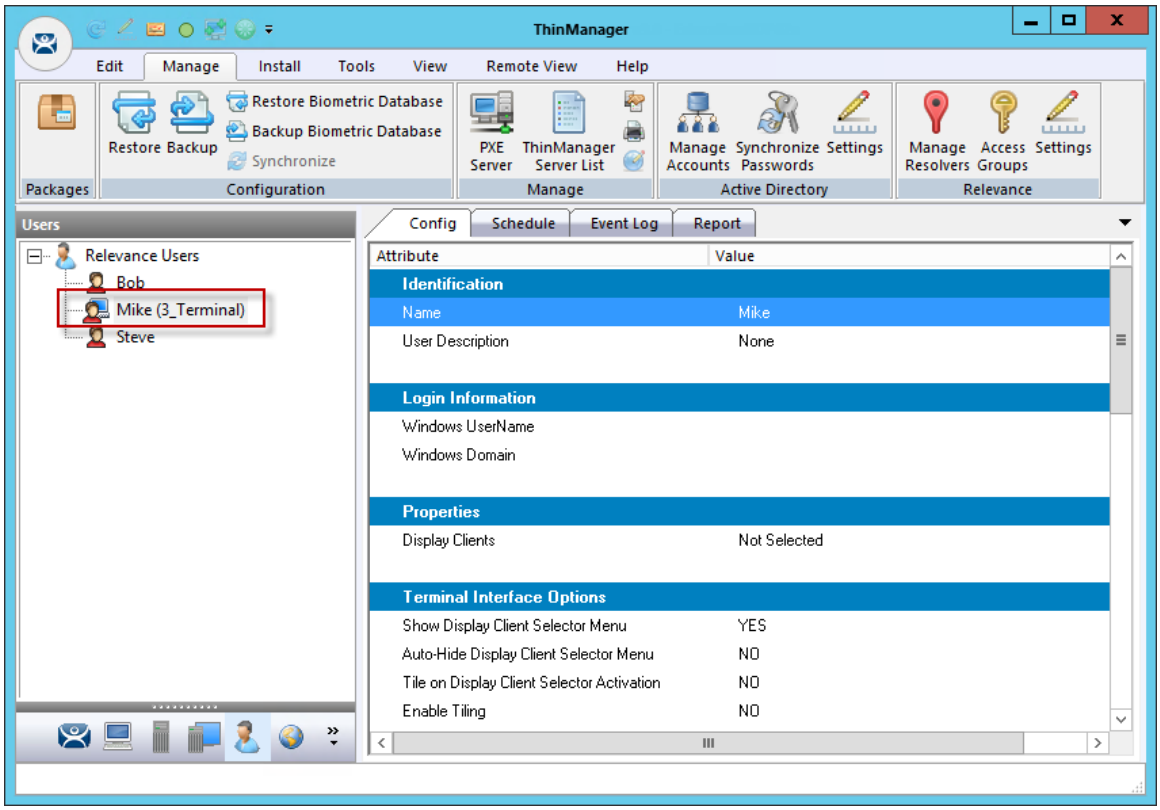


ThinManager with Relevance User Logged On

The example shows Mike logged in to the Terminal.

Notice that the Terminal displays the name of the Relevance User in parentheses.

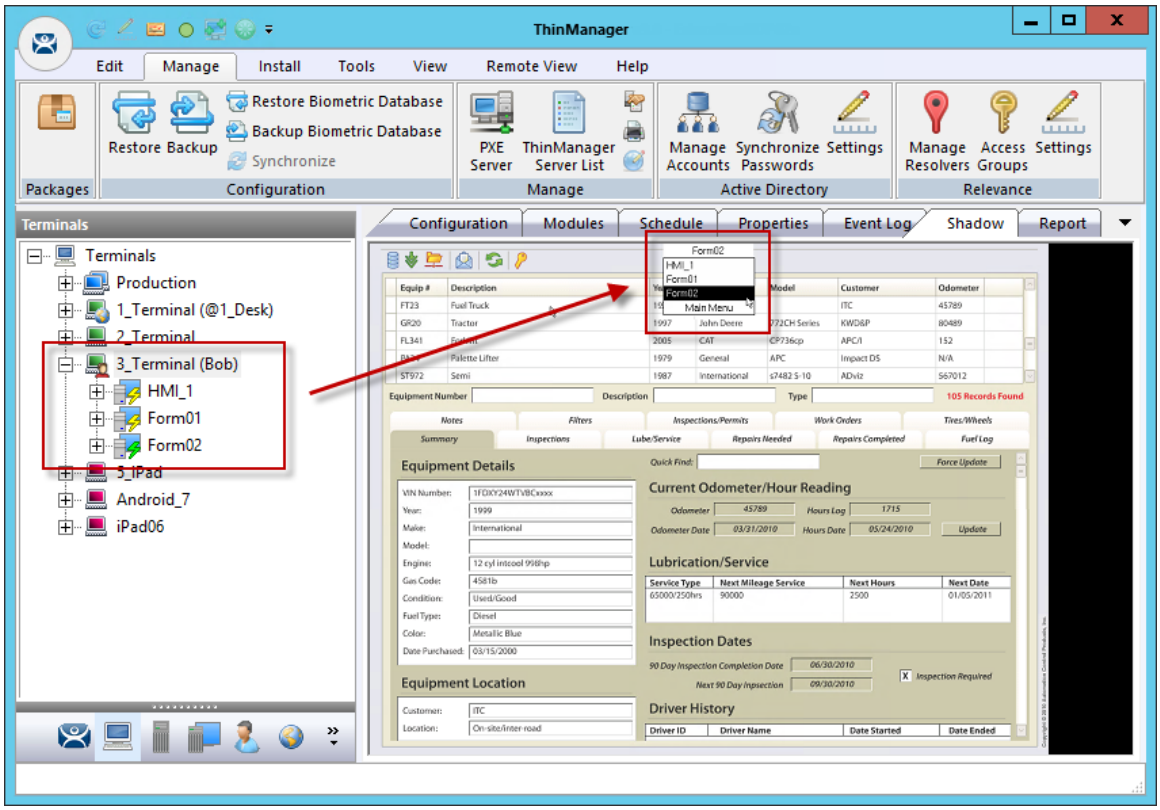
Notice that the group selector on the shadowed Terminal now has the hidden display client showing in the drop-down selector. The lightning bolt indication now shows a connection.



Relevance User Tree

The **Relevance User** tree will list the users.

A user that is logged in to a Terminal with Relevance will show a different icon and will show the name of the Terminal that it is logged in to. Mike is logged into 3_Terminal in this example.



Membership in Multiple Relevance Access Groups

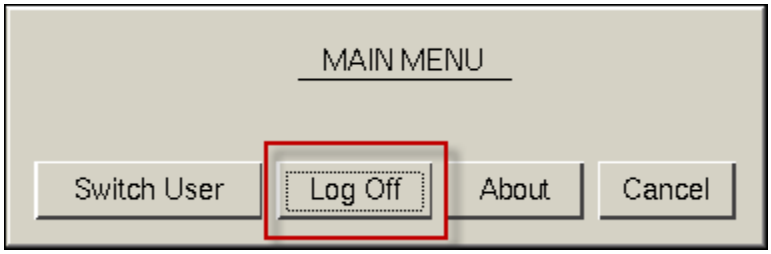
A Relevance User can be a member of multiple Relevance Access Groups.

In this example Bob is a member of both **Maintenance** and **Supply**. When he is logged in the display clients for both **Maintenance** and **Supply** are displayed. They will be hidden when he logs off.

31.8. Logging Out of Relevance

The Relevance User can be logged out by:

- Opening the **Relevance Main Menu** on the Terminal and selecting ***Log Off***.
- Right clicking on the **Relevance User** in the ThinManager tree and selecting ***Logoff User***.
- Restarting or rebooting the Terminal that has a Relevance User logged in.



Main Menu

The ***Switch User*** button will log off the Relevance User and disconnect any sessions from Display Clients assigned to the user. It opens the **Login** screen for another Relevance User.

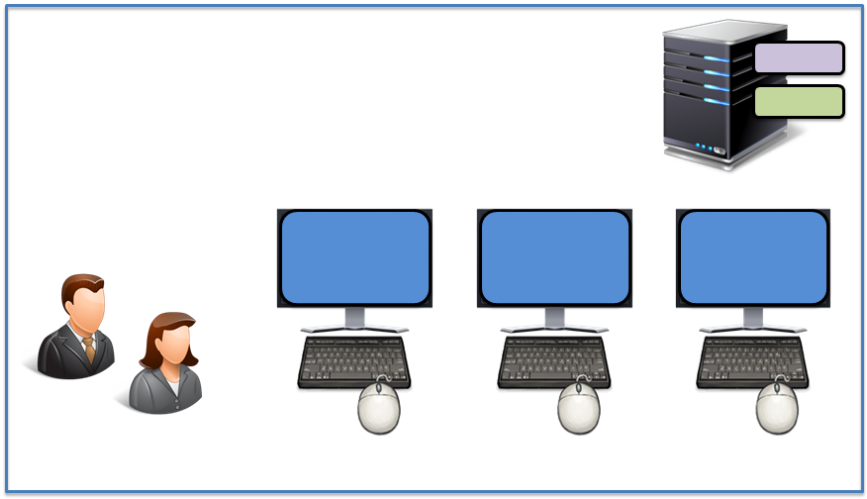
The ***Log Off*** button will log off the Relevance User and log off any sessions form Display Clients assigned to the user and return to the Terminal's display.

32. Assigning Roaming Display Clients to a Relevance User

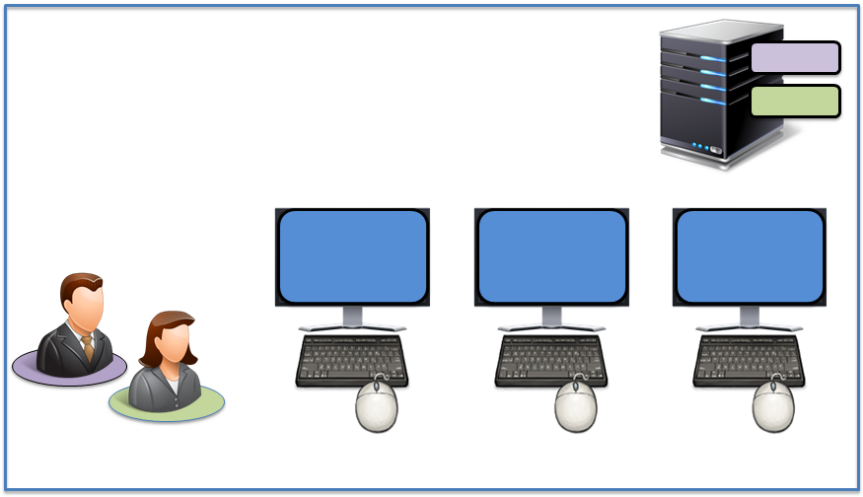
Relevance can assign a User-specific display client to a Relevance User. This display client is accessible from any Terminal or location that has been configured with Relevance User Services. These Relevance Users will require a valid Windows account since they are logging into a Windows session of their own.

32.1. Roaming Display Clients in Relevance Diagram

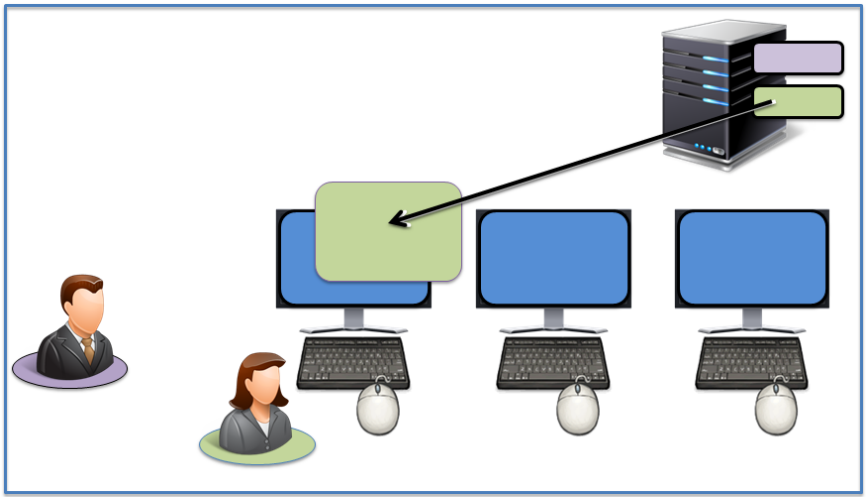
Here is a graphical representation of the process of assigning user-specific display clients to a Relevance user to allow the application to follow the user anywhere they need to go.



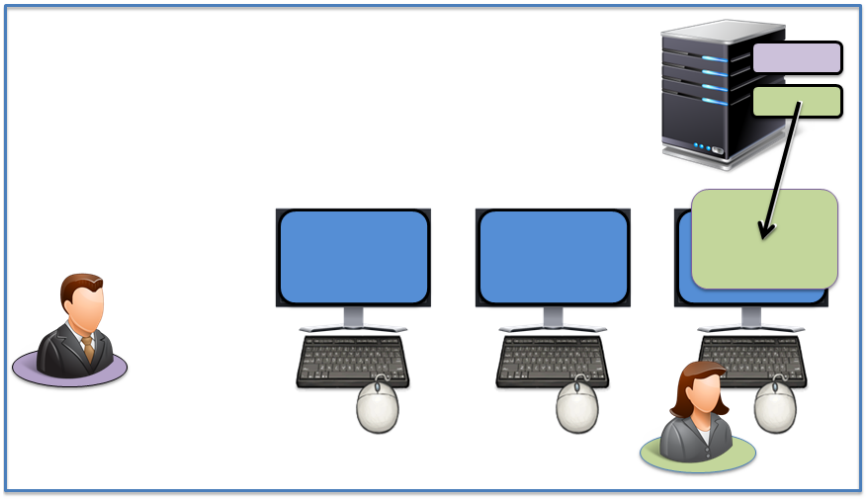
Create Relevance Users and Display Clients



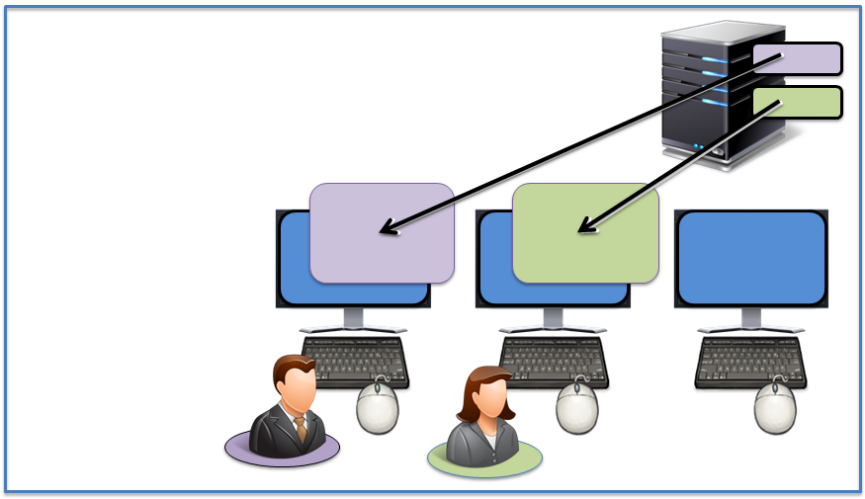
Assign the Display Client to the Relevance User



The Display Client is sent to the Terminal where the Relevance User Logs In



The Display Client Follows the Relevance User



The Display Client Follows the Relevance User

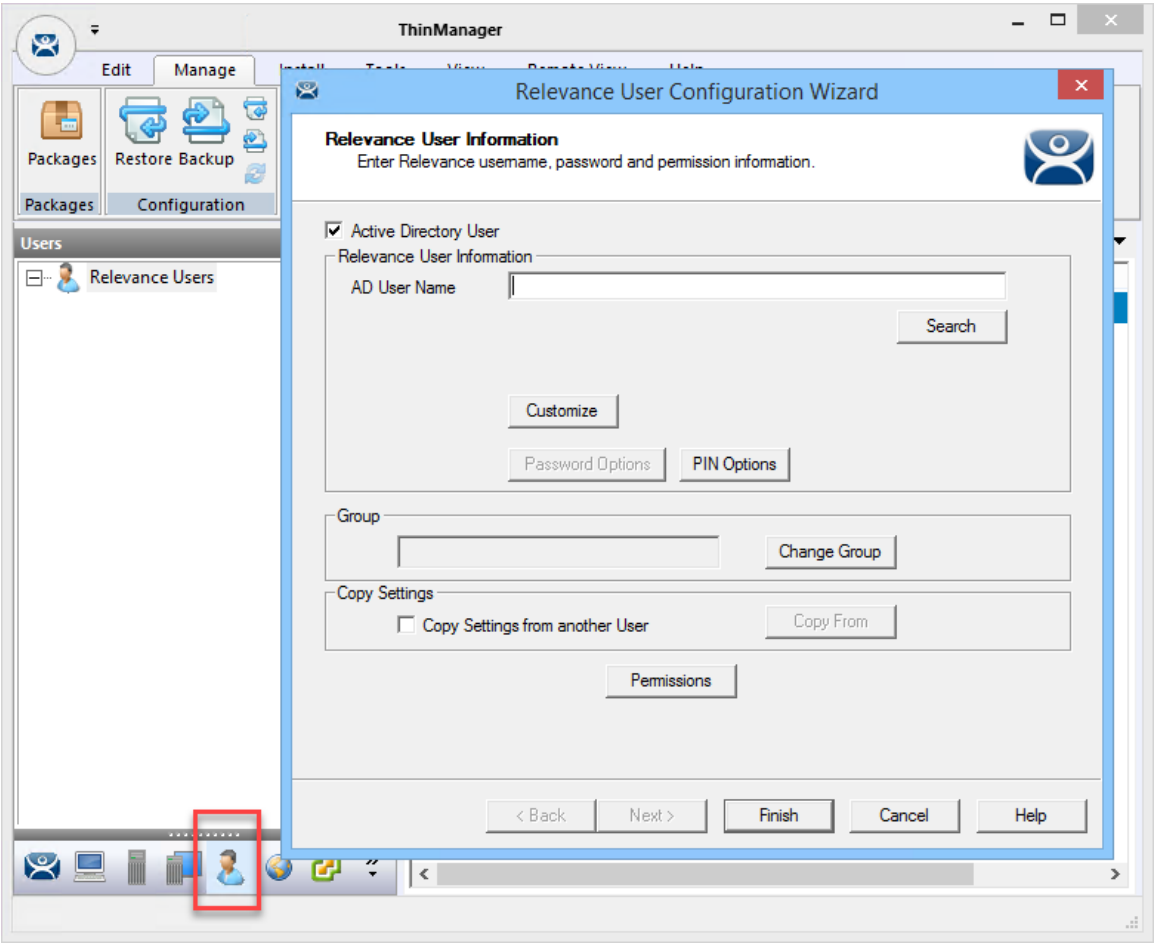
32.2. Create the Relevance User using Active Directory

ThinManager Active Directory integration allows a Relevance User to have its Windows user account drawn from the Active Directory. You allow ThinManager to store the password to streamline password management.

The **Relevance User Configuration Wizard** is launched from the **Relevance User** branch of the ThinManager tree.

Open the **Relevance User** tree by selecting the **User** icon at the bottom of the ThinManager tree.

Right click on the Relevance User branch and select ***Add User*** to launch the **Relevance User Configuration Wizard**.

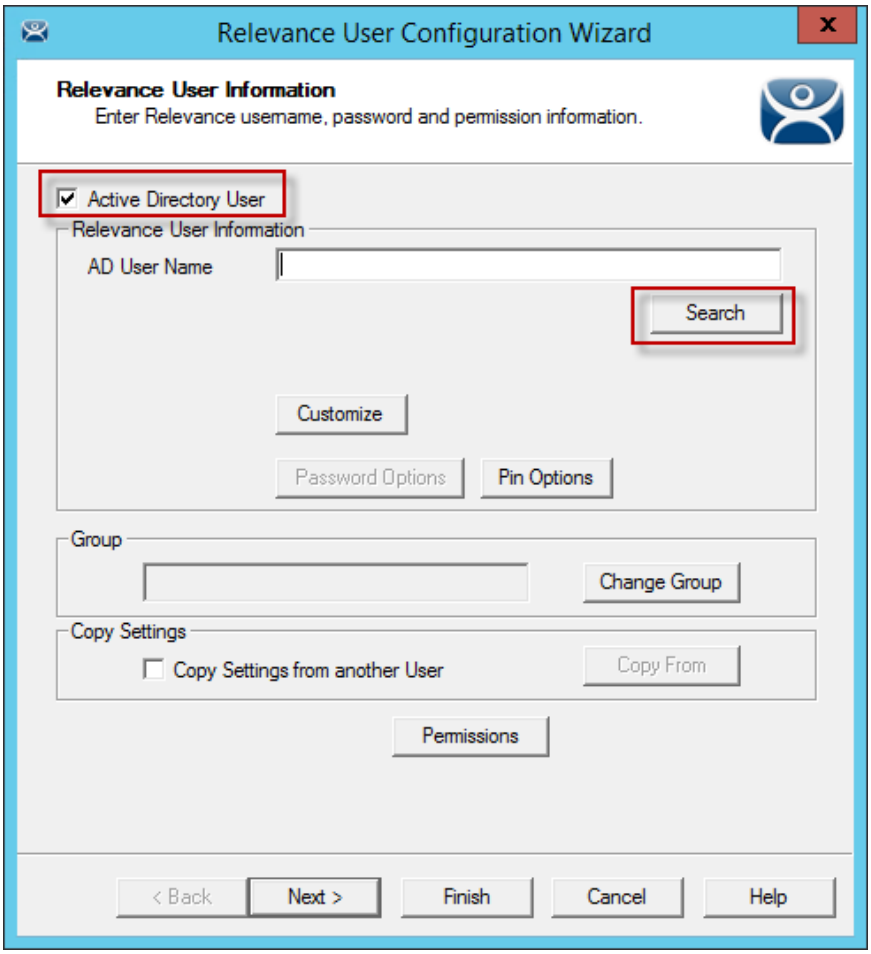


User Branch of the ThinManager Tree

The first page of the **Relevance User Configuration Wizard** is the **Relevance User Information** page that creates the Relevance User account.

Relevance Users that have display clients assigned to them will need to be tied to a Windows account. If a Relevance User does not have a display client assigned to it and it only using the Permissions to access a display client belonging to the Terminal then it does not need a Windows account.

This scenario assigns display clients to the Relevance User so a valid Windows account is needed.

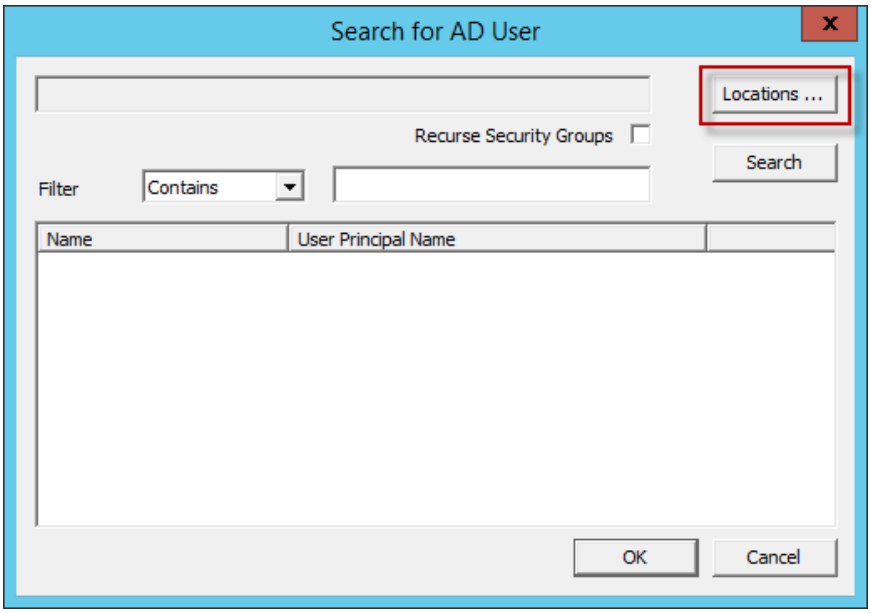


Relevance User Information

The first page of the **Relevance User Configuration Wizard** is the **Relevance User Information** page that creates the Relevance User account.

Selecting the ***Active Directory User*** checkbox allows you to draw the user account from the Active Directory.

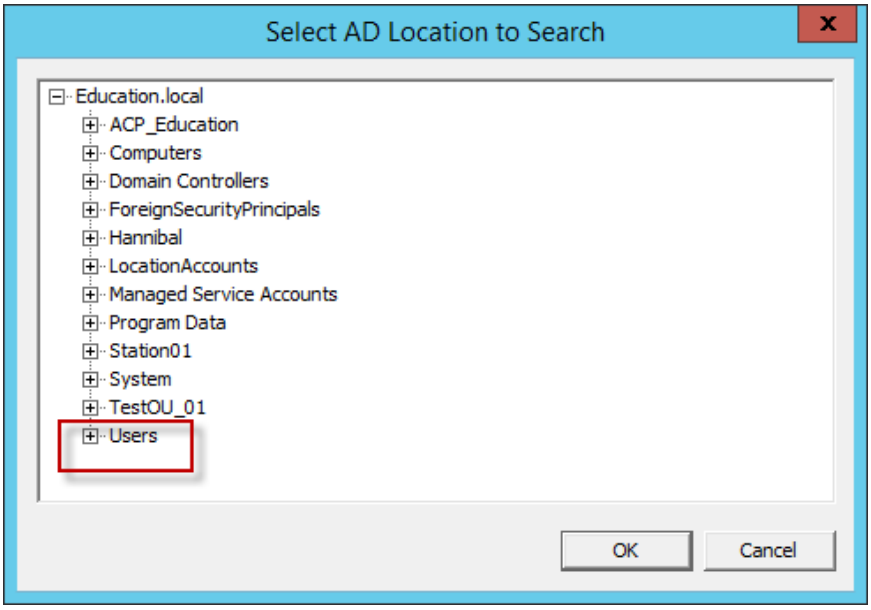
Select the ***Search*** button to begin the Active Directory process by launching the **Search for AD User** window.



Search for AD User Window

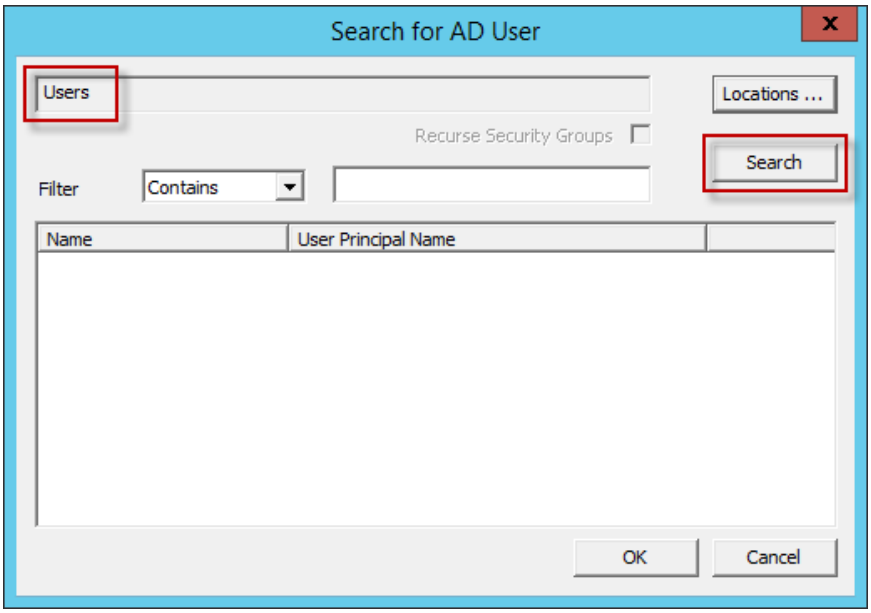
Select the Locations button on the Search for AD User window to choose a location.

This will launch the **Select AD Location to Search** window.



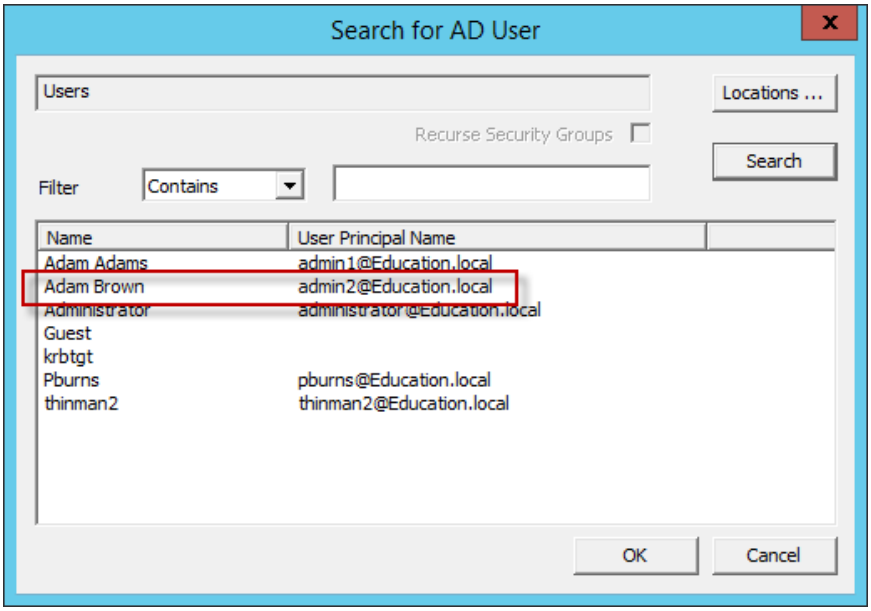
Select AD Location to Search Window

Highlight the AD location you want to select the user from and select the ***OK*** button. This will enter the location into the ***Locations*** field in the **Search for AD User** window.



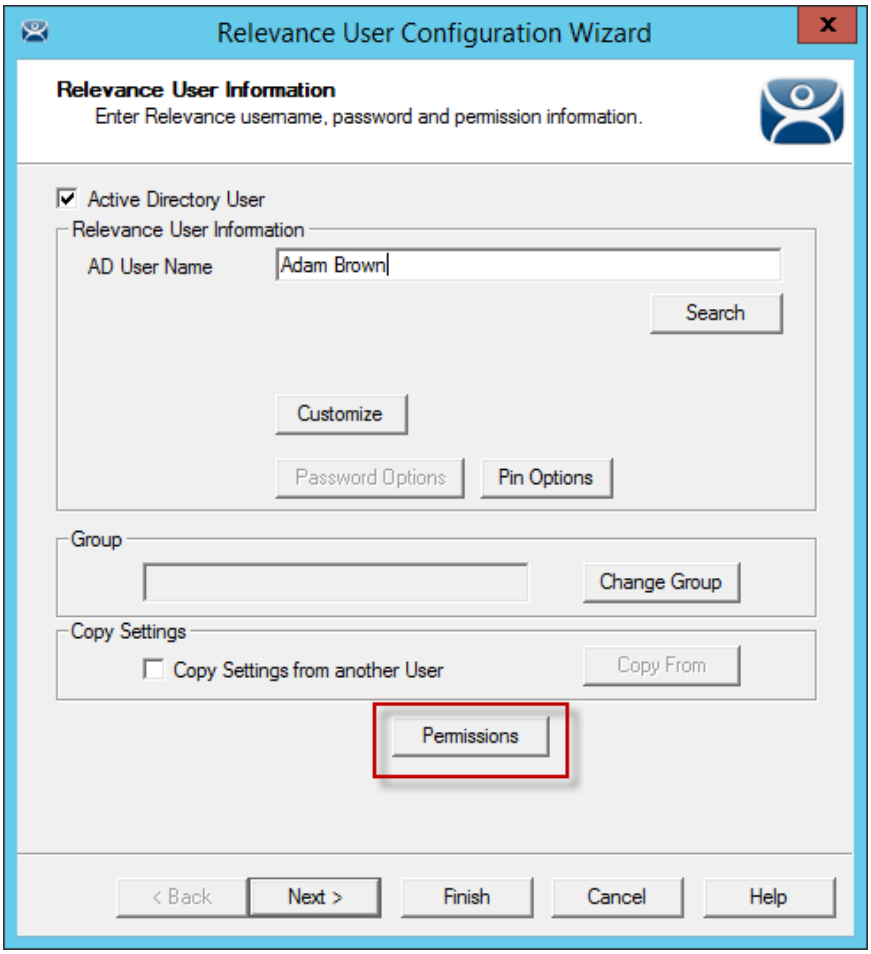
Search for AD User Window – Location Selected

Once the Location has been selected click the ***Search*** button to populate the user field with users from the highlighted location.



Search for AD User Window – Users

Highlight the desired user account from the Active Directory members and select the ***OK*** button. This will enter the user account in the ***AD User Name*** field of the **Relevance User Information** page.



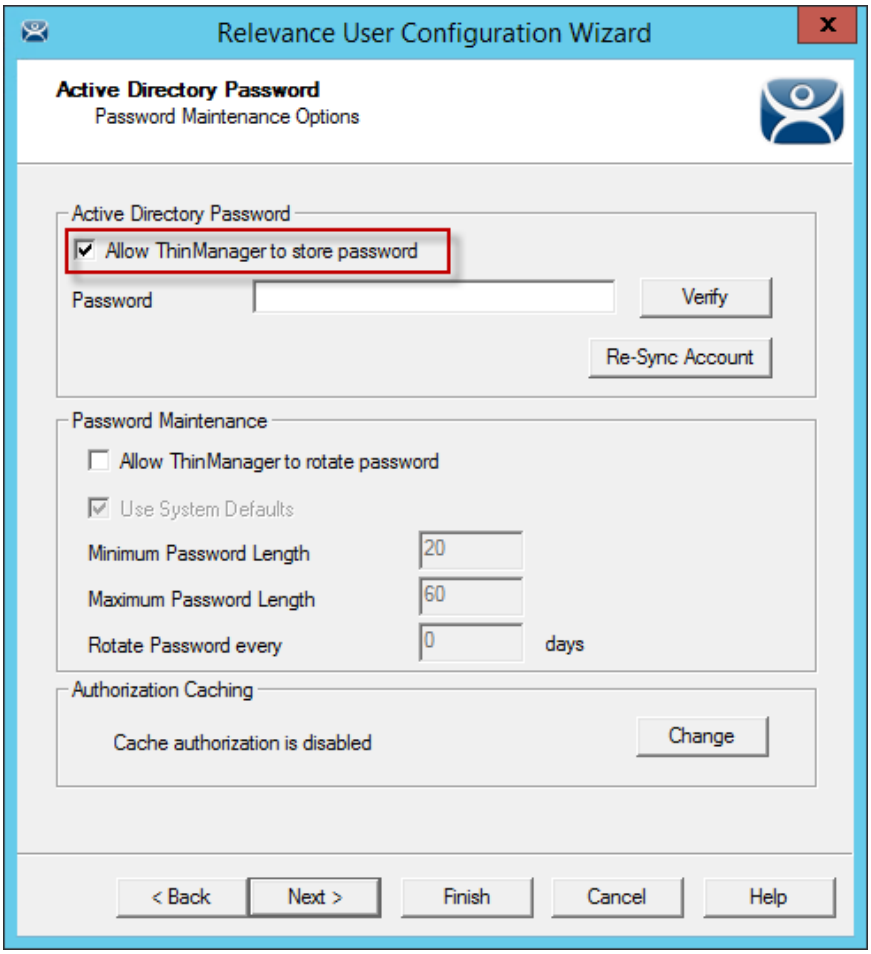
Relevance User Information Window

This shows an Active Directory user in the ***AD User Name*** field.

Select the ***Permission*** button to apply membership in Access Groups as described in Permission Deployed Applications in Relevance on page 457. Select the ***Finish*** button if you only need a **Permission** applied.

- ***Customize*** launches the **User Description** window. See Relevance User Settings for Non-Domain Users on page 508.
- ***Password Options*** are configured in the Active Directory System Settings launched by selecting ***Manage>Active Directory > Settings*** on the ThinManager menu.
- ***Pin Options*** launches the **Pin Maintenance Options** window. See Relevance User Settings for Non-Domain Users on page 508.
- ***Change Group*** launches the **Choose User Group** window. See Relevance User Settings for Non-Domain Users on page 508.
- ***Copy Settings from another user*** – This allows the user to inherit the properties of another user.
- ***Copy From*** - This button will open the Select User window that will allow you to select the user to inherit properties from.

Select the ***Next*** button if you want to apply user-specific display clients.



Active Directory Password Page

The **Active Directory Password** page has an ***Allow ThinManager to store password*** checkbox. If this is unchecked then ThinManager does not store the account and you must enter a password each time the session logs on. This is fine if you are logging in with a Relevance password anyhow.

If the ***Allow ThinManager to store password*** checkbox is checked then you can have the Windows password stored in ThinManager. This allows a fingerprint scan to send the Windows password automatically for authentication.

If the ***Allow ThinManager to store password*** checkbox is checked you can use the system defaults or uncheck the ***Use System Default Password Settings*** to customize the password settings.

The password settings include

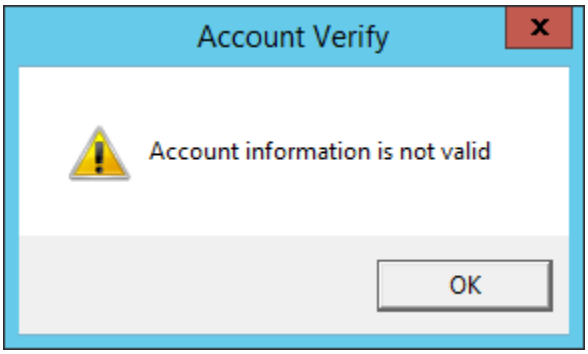
Password Complexity Requirements:

- ***Minimum Password Length*** – This is the minimum number of characters a password may have.
- ***Maximum Password Length*** – This is the maximum number of characters a password may have.

Password Maintenance:

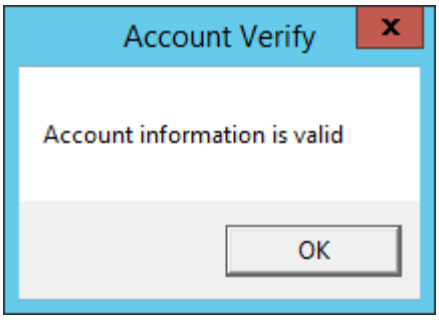
- ***Rotate Password every*** – This is the number of days before the password must be changed.

Enter the user password in the ***Password*** field and select the ***Verify*** button.



Account Verify Dialog - Fail

Selecting the ***Verify*** button will check your password against the Active Directory. If it is incorrect it will show a failed dialog.



Account Verify Dialog - Pass

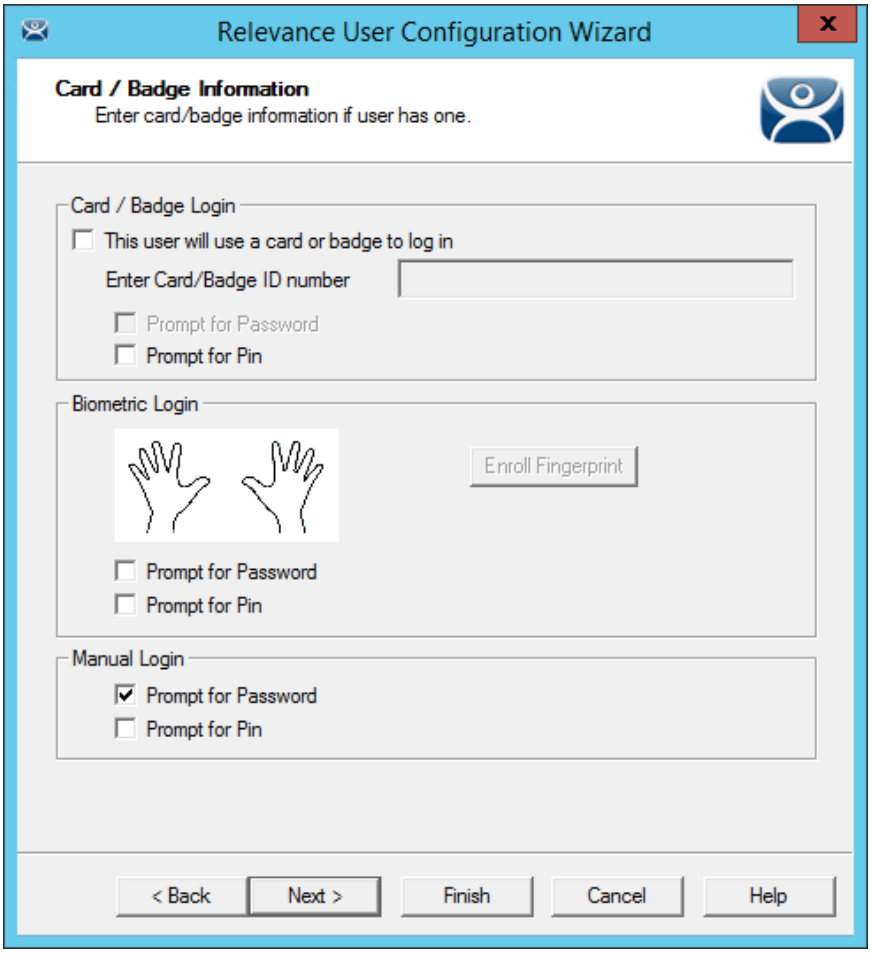
If the password is correct the dialog will show a positive result.

Once you have established your login strategy you continue the Relevance Configuration Wizard.

32.3. Relevance Configuration Wizard

After the username is defined on the **Relevance User Information** page and a password configured on the **Active Directory Password** page the next page is the **Card / Badge Information** page.

Select the ***Next*** button to continue the wizard.



Card/Badge Information

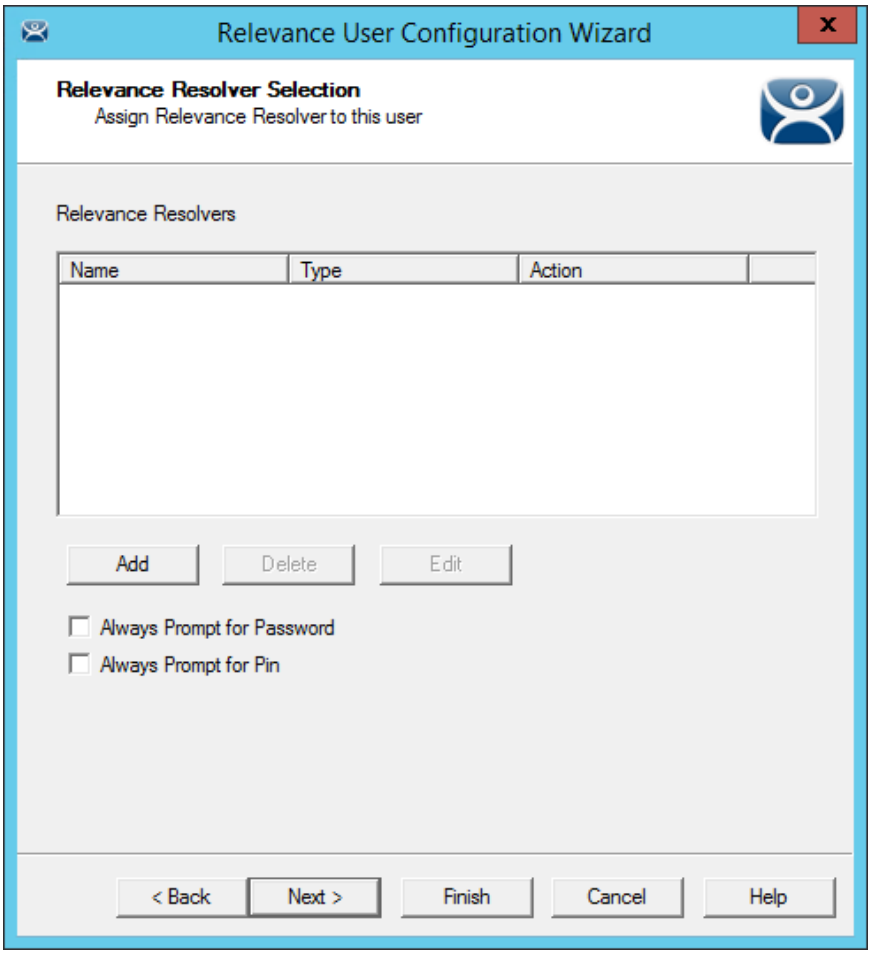
You can tie a Relevance User to a HID card and validate with a card scan or you can associate a user fingerprint to the account and have a fingerprint scan validate the user.

These methods are covered in Card Readers and Fingerprint Scanners on page 553.

A secondary credential can be required by selecting ***Prompt for Password*** or ***Prompt for Pin*** for the **Card/Badge Login**, the **Biometric Login**, or a **Manual Login**.

- ***Prompt for Password*** – This checkbox, is selected, will require the user to enter their password.
- ***Prompt for Pin*** – This checkbox, is selected, will require the user to enter their PIN.

Select the ***Next*** button to continue.



Location Resolver

Relevance allows a Resolver to pass the specific user's credentials for a login.

- Select the ***Add*** button to launch the **Choose a Relevance Resolver** window.
- Select the resolver from the ***Resolver Name*** drop-down,
- Select ***User Login*** from the ***Choose Action*** drop-down.
- Select the ***OK*** button to apply the resolver.

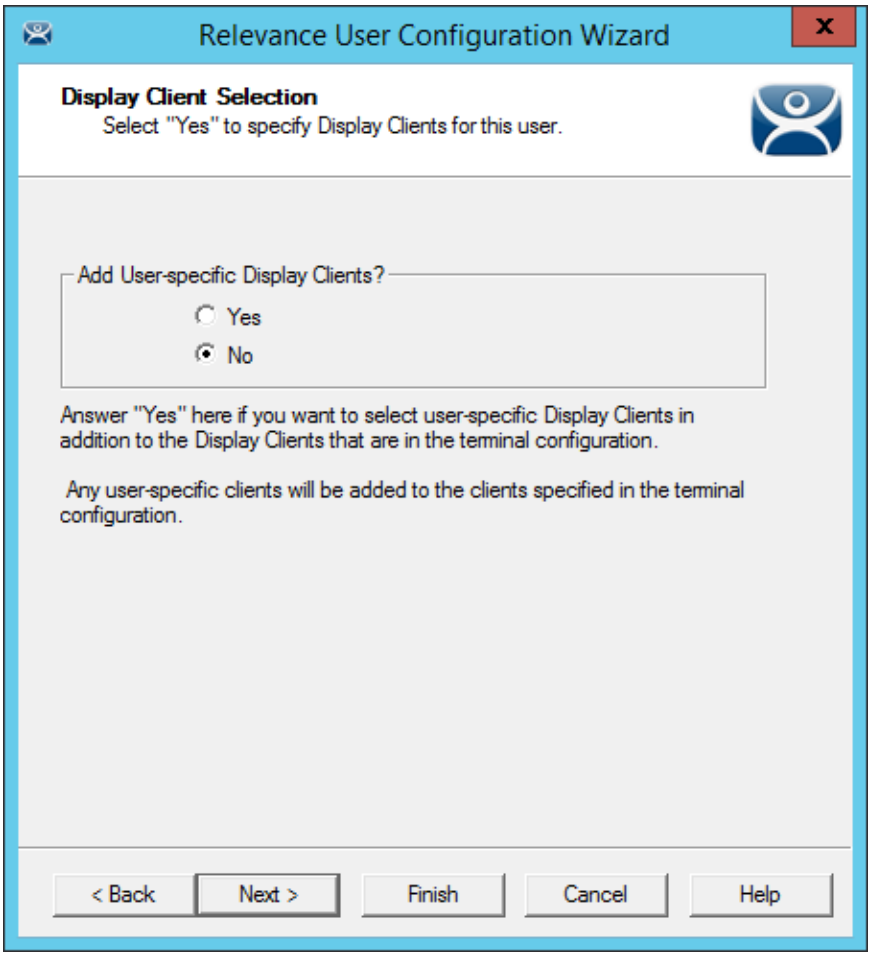
The user will login when the resolver is activated.

- ***Prompt for Password*** – This checkbox, is selected, will require the user to enter their password.
- ***Prompt for Pin*** – This checkbox, is selected, will require the user to enter their PIN.

Select the ***Next*** button to continue.

32.4. Adding User-specific Display Clients

Roaming applications require that display clients are assigned to individuals.

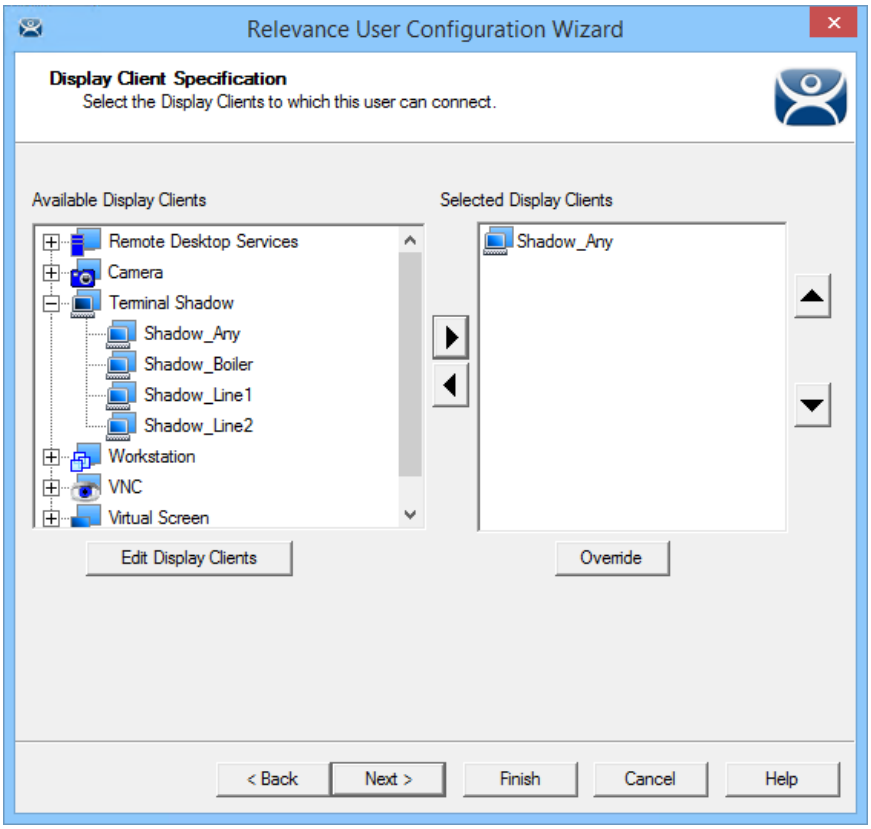


Display Client Selection Window

The **Display Client Selection** window has one setting, ***Add User-specific Display Clients?***

- If ***No*** is selected for ***Add User-specific Display Clients?*** then the user will only be able to access display clients that belong to the Terminal they log in to. This is used with **Permissions** to grant access to applications hidden with Access Group Permissions.
- If ***Yes*** is selected for ***Add User-specific Display Clients?*** then the user can be assigned display client of their own that they can access from any Terminal that has Relevance enabled. You may also assign the user Permissions to let them access hidden applications.

Select the ***Next*** button to continue.



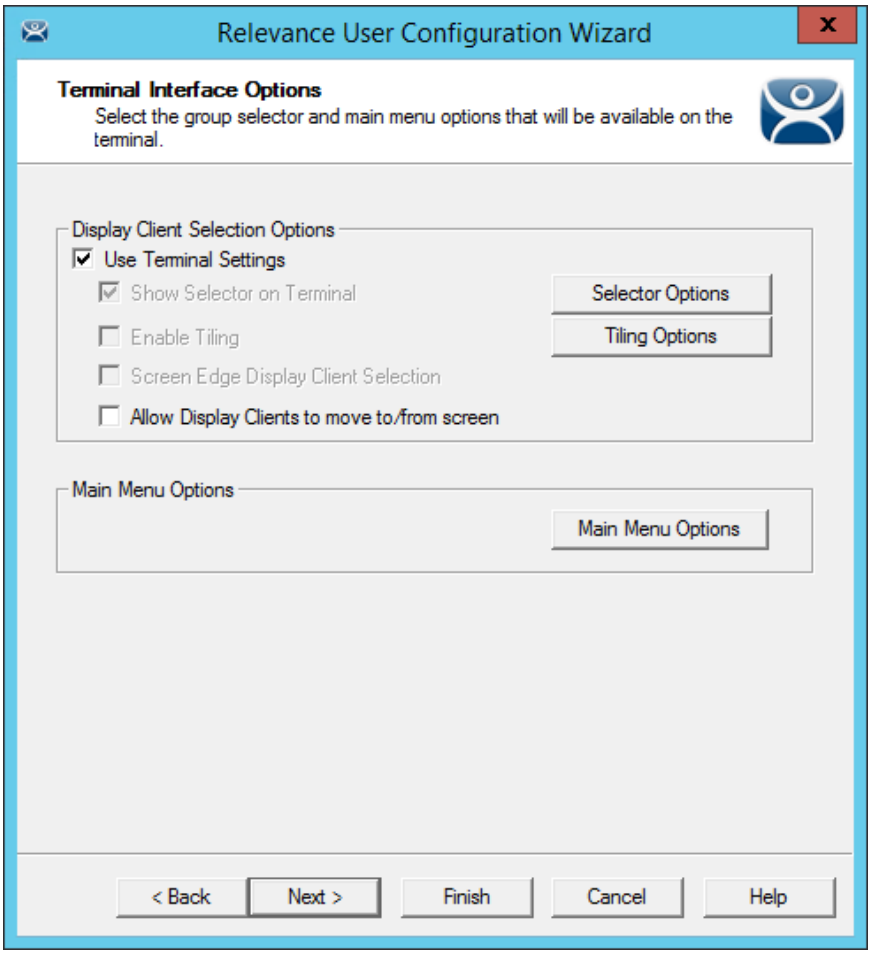
Display Client Specification Page

The **Display Client Specification** page allows Display Clients to be assigned to the Relevance User if the ***Add User specific Display Clients?*** radio button is set to ***Yes***.

Move a Display Client you want the Relevance User to use into the ***Selected Display Clients*** list by double-clicking on it in the **Available Display Clients** list or by highlighting it and clicking the ***Right Arrow*** button.

To add a new Display Client, select the ***Edit Display Clients*** button to launch the Display Client Wizard. See Content – Remote Desktop Services Display Client for details.

Select the ***Next*** button to continue.



Terminal Interface Options

The **Terminal Interface Options** page sets the menus and hotkeys for the Relevance User so a Terminal using MultiSession will need to have a method to switch between sessions. This is similar to the page in the Terminal Configuration Wizard.

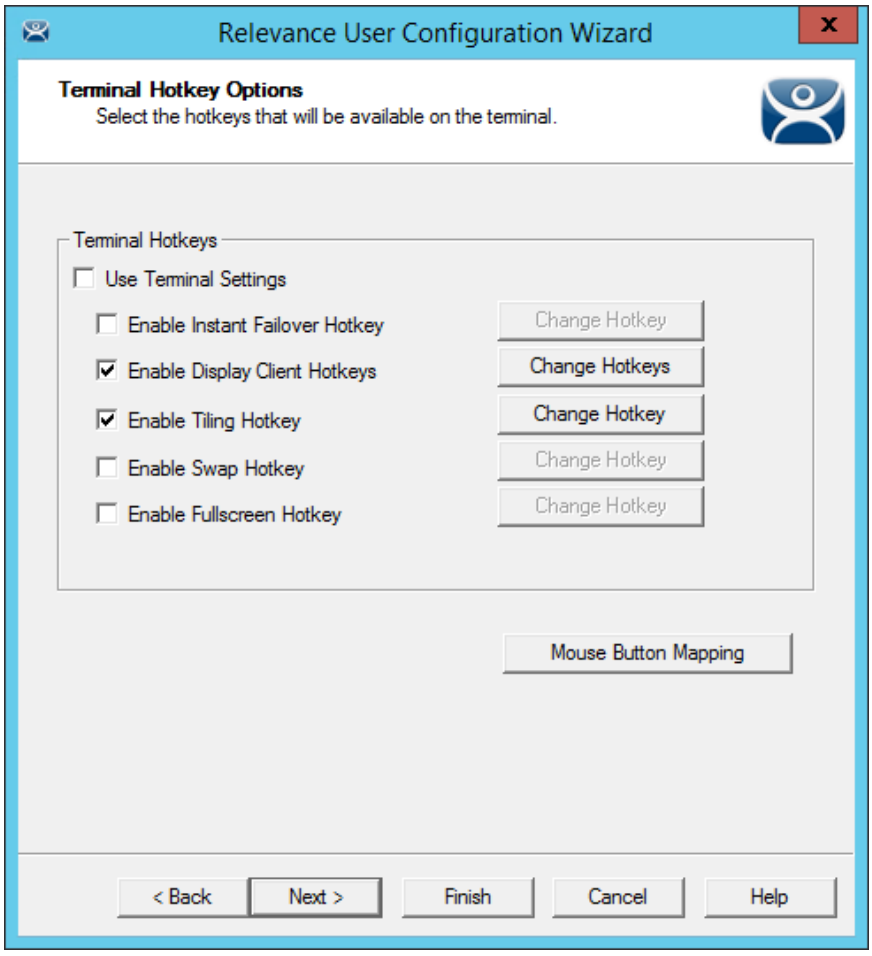
Group Selector Options allow on-screen switching of sessions.

Use Terminal Settings - This checkbox, when selected, will let the Relevance User inherit the properties that were configured for use with the Terminal.

- ***Show Group Selector on Terminal*** - This checkbox, if selected, will display an on-screen drop-down menu that can be activated by mouse.
- ***Enable Tiling*** - This checkbox, if selected, allows the sessions to be tiled so that the user can make a visual selection of the desired selection.
- ***Screen Edge Group Selection*** - This checkbox, if selected, will activate a feature that will switch windows if the mouse is moved off screen.
- ***Allow Display Clients to move to/from screen*** – This checkbox, if selected, will give the user to move display clients from screen to screen.
- ***Selector Options*** - This button, if selected, will launch the **Group Selector Options** window.
- ***Tiling Options*** - This button, if selected, will launch the **Tile Options** window.

The ***Main Menu Options*** button will launch the **Main Menu Options** window that allows configuration of the Relevance Main Menu.

Select the ***Next*** button to continue.



Terminal Hotkey Options

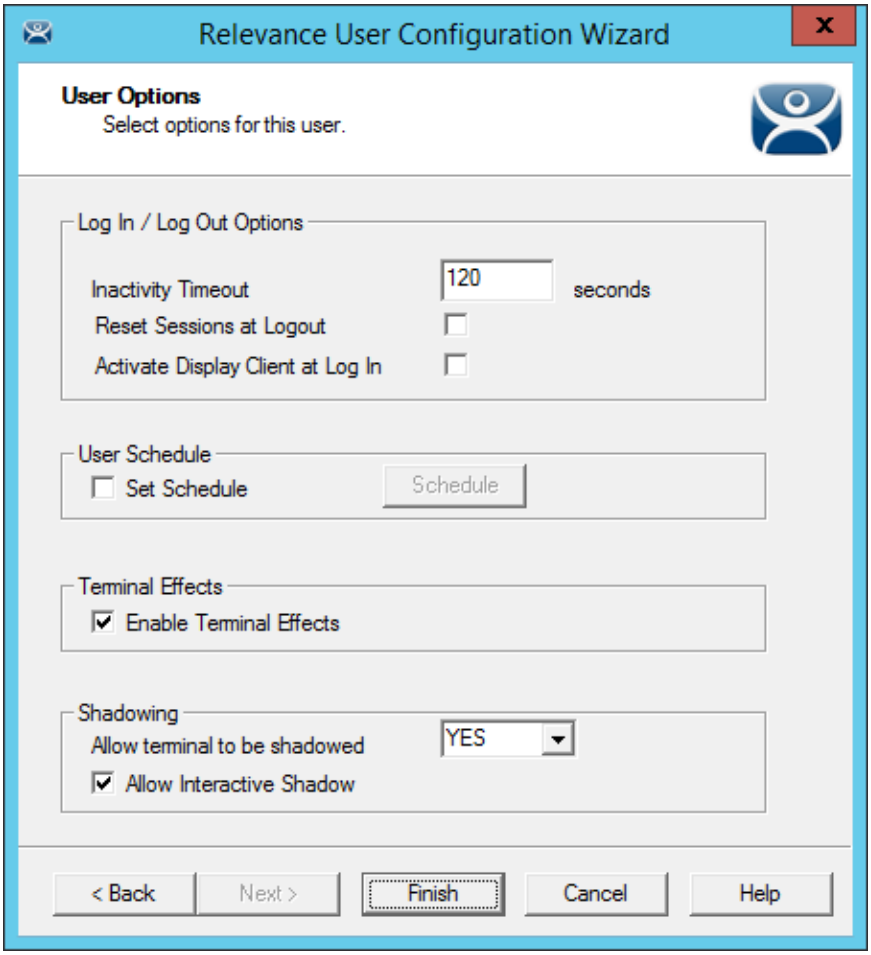
Terminal Hotkeys on the **Hotkey Configuration** page allows the selection of keyboard combinations that allow switching between sessions. This is similar to the page in the Terminal Configuration Wizard.

- ***Use Terminal Settings -*** This checkbox, when selected, will let the Relevance User inherit the properties that were configured for use with the Terminal. If unselected the user receives the settings as configured for them.
- ***Enable Instant Failover Hotkeys*** - This checkbox, if selected, allows the hot key switching between the two active sessions of a Display Client that is using Instant Failover. The Terminal needs to be using a display client with Instant Failover for this to be active.
- ***Enable Display Client Hotkeys*** - This checkbox, if selected, allows the hot key switching between different sessions of a Terminal using MultiSession.
- ***Enable Tiling Hotkey*** – This checkbox, if selected, allows SessionTiling to be activated by a hotkey combination. Tiling has to be selected on the Terminal Interface Options page for this to be active.
- ***Enable Swap Hotkey*** – This checkbox, if selected, allows a hotkey to swap virtual screens instead of a mouse click.

- ***Enable Fullscreen Hotkey*** – This checkbox, if selected, allows the virtual screen to go full sized with a hotkey.
- ***Mouse Button Mapping -*** – This button opens the **Mouse Mapping Option** window that allows functions to be assigned to mouse buttons.

Selecting the ***Change Hotkeys*** button when a setting is selected will allow the hotkeys to be changed from the default.

Select the ***Next*** button to continue.



User Options

The User Options page has a few options for the user experience.

Log In / Log Out Options

- ***Inactivity Timeout*** - Relevance will log a Relevance Users off the Terminal after this much inactive time has passed.
- ***Reset Sessions at Logout*** - This checkbox, if selected, will logoff a session when the Relevance User logs off.
- ***Activate User Group at Log In*** - This checkbox, if selected, will display the Relevance User's first Display Client when the user logs in to the Terminal.

User Schedule

- ***Set Schedule*** -

Selecting the ***Schedule*** button on the **User Options** page will launch the **Event Schedule** window and allow a schedule to be created for Terminal events.

See Terminal Schedule for details.

Terminal Effects

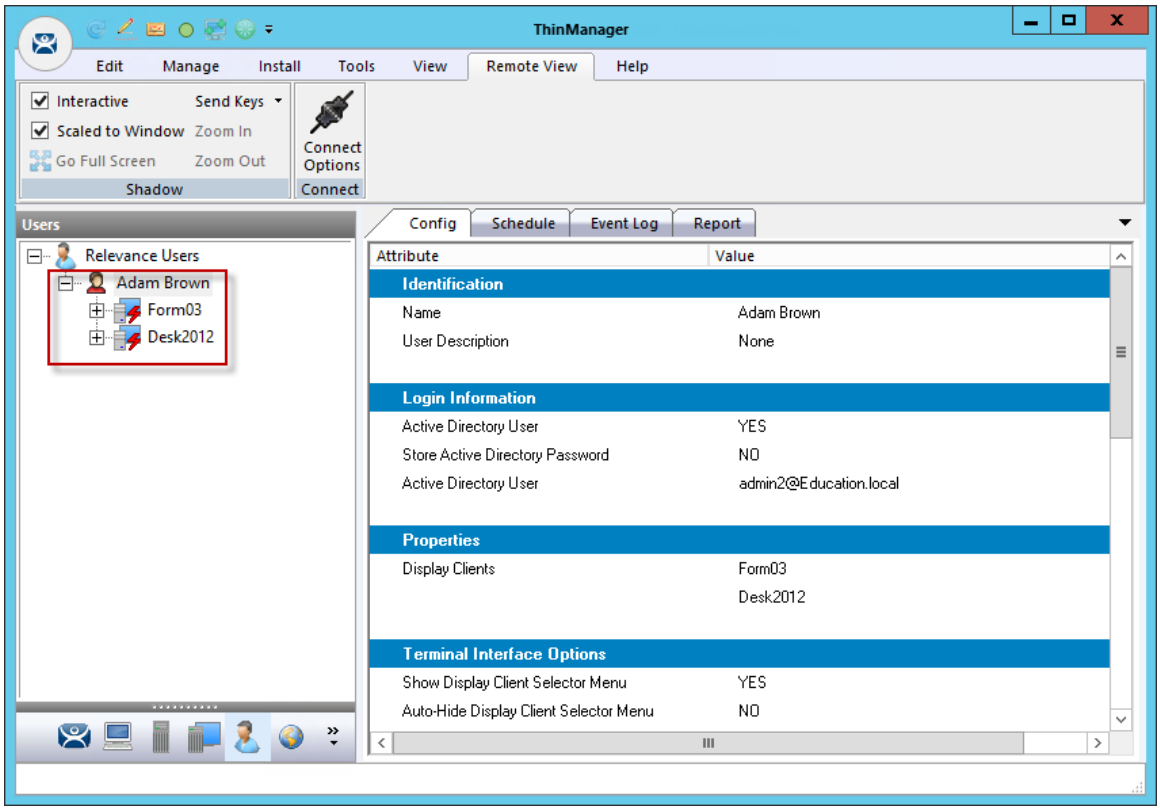
- ***Enable Terminal Effects*** - This allows the use of Terminal Effects. This currently includes sliding Windows and message rollups.

Shadowing

- ***Allow Terminal to be shadowed*** - This drop-down box allows the configuration of Shadowing Options.
    - ***No*** - Prevents the Relevance Users from being shadowed.
    - ***Ask*** - Will display a message window that will prompt for a positive response before the shadowing is allowed.
    - ***Warn*** - Will display a message window alerting the Terminal that it is to be shadowed, but doesn't require a positive response before the shadowing is allowed.
    - ***Yes*** - Allows shadowing to occur without warning or recipient input.
- ***Allow Interactive Shadow*** - This checkbox, if selected, will allow members with Interactive Shadow privileges to shadow this Relevance User.

Shadowing is initiated from the Shadow tab on the Details pane of the ThinManager program. Unselecting this will prevent shadowing from within ThinManager.

Select **Finish** to finish the configuration.



Relevance User with User-Specific Display Clients

The Relevance User tree will show the display clients assigned to the user.

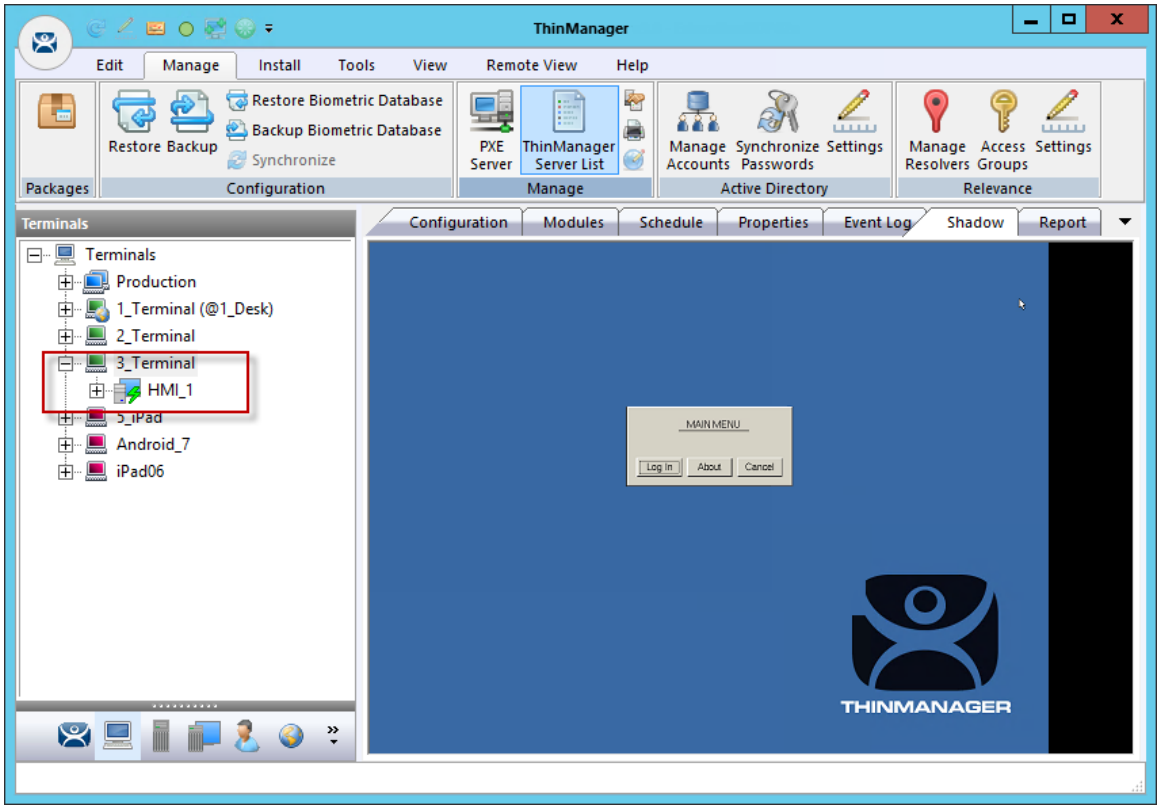
32.5. Logging On with a Relevance User Account

To log in a Relevance User on a Terminal, go to a Terminal that has the ***Enable Relevance*** checkbox selected on the **Terminal Mode Specification** page.

You can log in by:

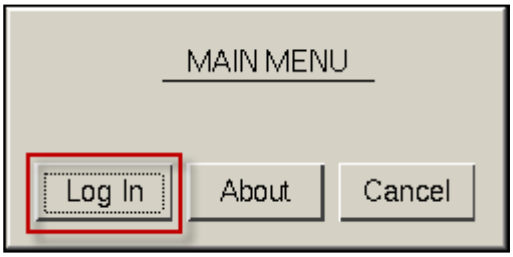
- Opening the display client selector drop-down and selecting ***Main Menu***.
- Typing the ***CTL+m*** hotkey to launch the **Main Menu** if the hotkey checkbox was selected.

The **Main Menu** will be displayed on the Terminal.



ThinManager Console with a Single Display Client on Terminal

The Terminal tree will show the Terminals and the display clients assigned to the Terminals.



Relevance Main Menu

Select the ***Log In*** button on the Main Menu dialog to login.

Relevance Log On Screen with Virtual Keyboard

A virtual keyboard will be displayed if ***Show Virtual Keyboard*** was selected on the **Main Menu Options** window when configuring the Terminal for Relevance on the **Terminal Interface Options** page.

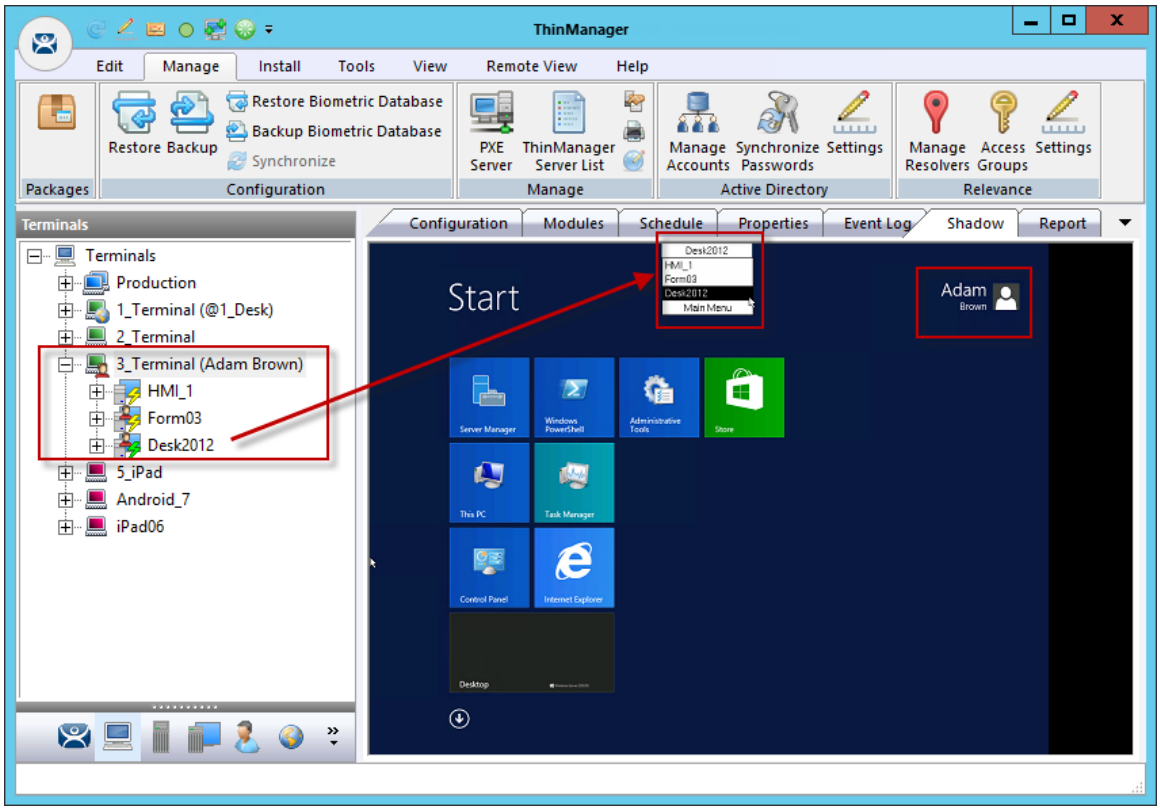
Relevance Log On Dialog

Enter your Relevance User name in the ***Enter User Name*** field.

Select **OK**.

Password Dialog

Enter the password in the field and select the ***OK*** button.

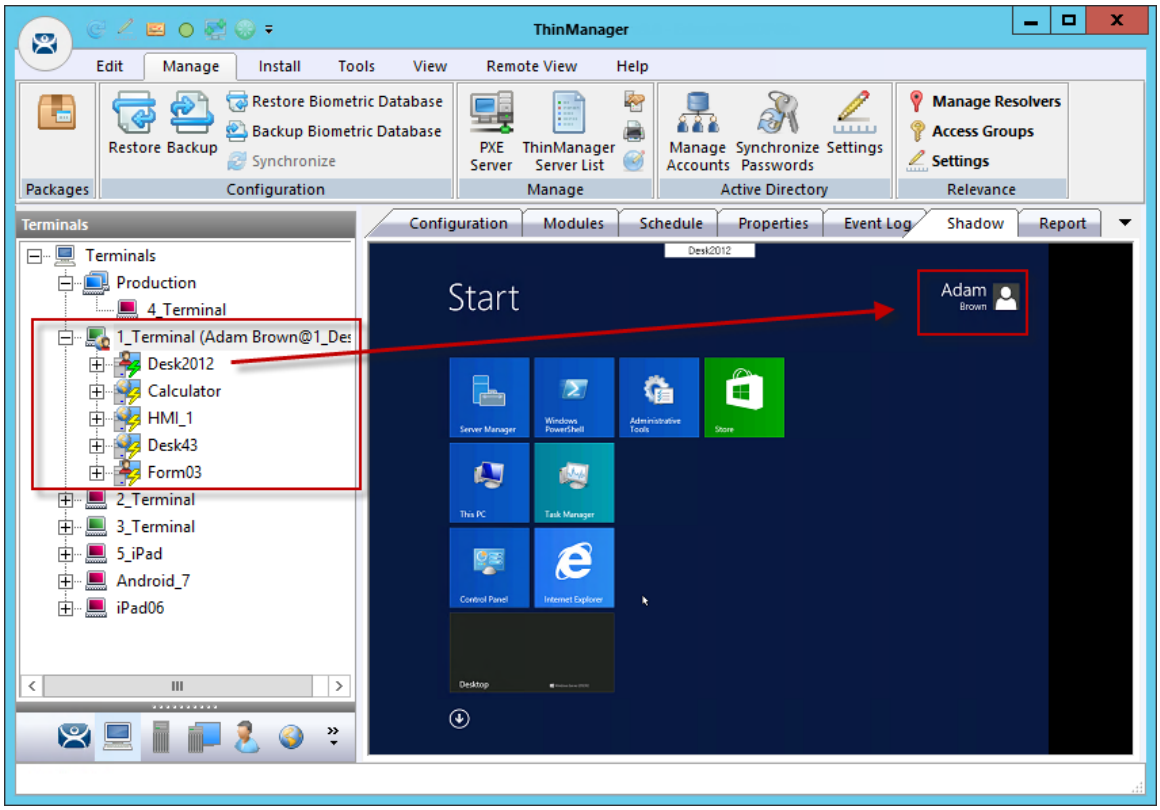


ThinManager with Relevance User Logged On

This will login the user if they have valid Windows credentials.

The Terminal displays the name of the Relevance User in parentheses. The example shows **Adam Brown** logged in to the Terminal.

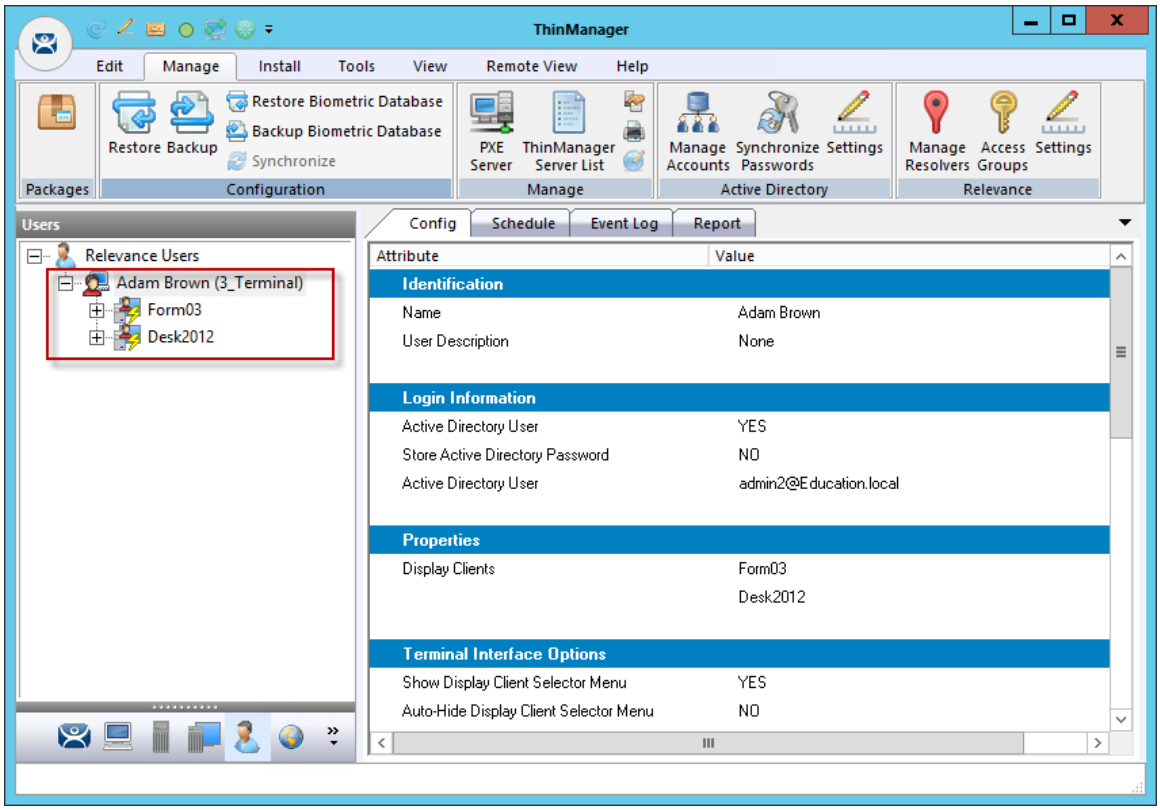
The group selector on the Terminal will show the Relevance User's display client in the drop-down selector. The lightning bolt indication now shows a connection.



ThinManager with Relevance User Logged On

When a Relevance User logs off of a Terminal the sessions disconnect by default and remain in an idle state on the Remote Desktop Servers.

If the Relevance User logs in from another Terminal then Relevance will connect the user to their session and the sessions will be displayed at the new Terminal.



Relevance User Tree

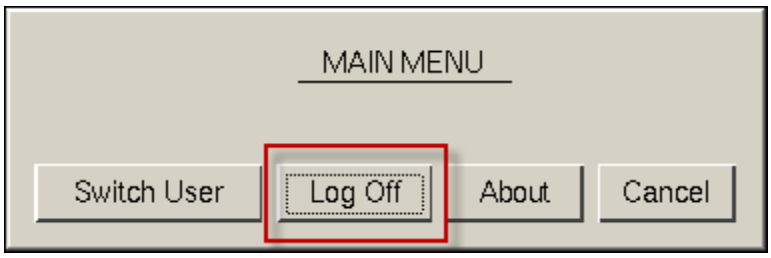
The **Relevance User** tree will list the users.

A user that is logged in to a Terminal with Relevance will show a different icon and will show the name of the Terminal that it is logged in to. Adam Brown is logged into 3_Terminal in this example.

32.6. Logging Out of Relevance

The Relevance User can be logged out by:

- Opening the **Relevance Main Menu** on the Terminal and selecting ***Log Off***.
- Right clicking on the **Relevance User** in the ThinManager tree and selecting ***Logoff User***.
- Restarting or rebooting the Terminal that has a Relevance User logged in.
- The ***Inactivity Timeout*** set on the **User Options** page has been reached.



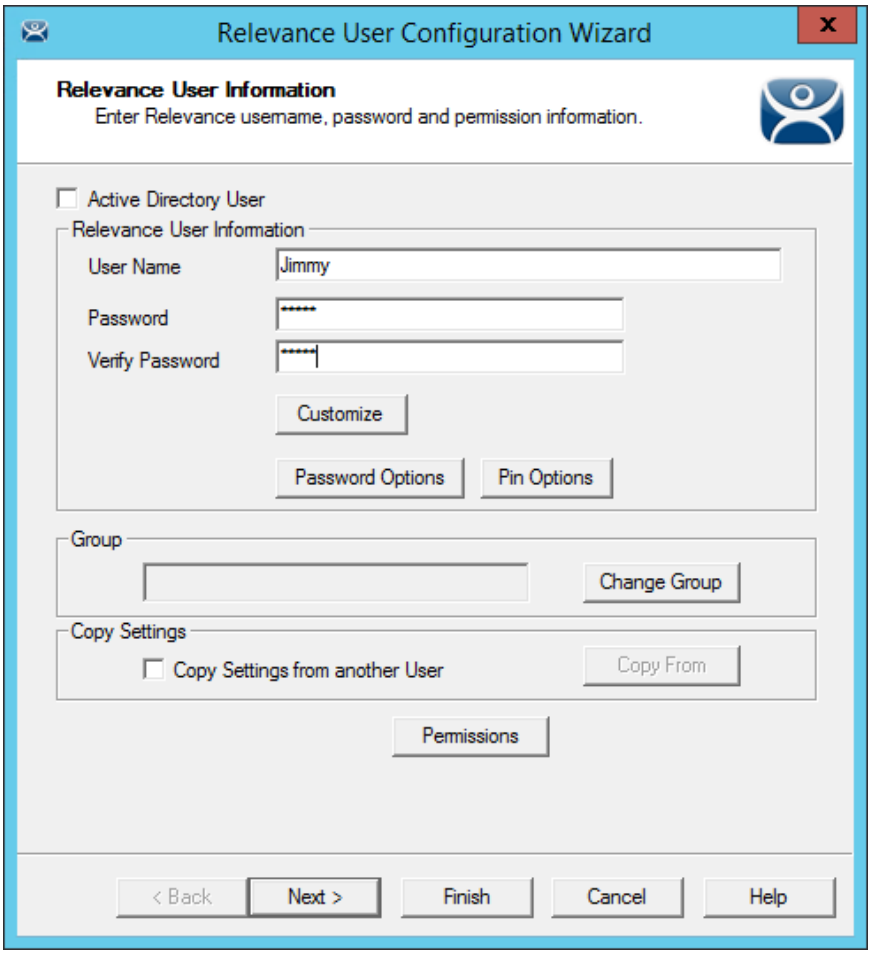
Main Menu

The ***Switch User*** button will log off the Relevance User and disconnect any sessions from Display Clients assigned to the user. It opens the **Login** screen for another Relevance User.

The ***Log Off*** button will log off the Relevance User and log off any sessions form Display Clients assigned to the user and return to the Terminal's display.

32.7. Roaming Applications for Non-Domain Users

Each Relevance User that has its own display client assigned need to be tied to a Windows User account. When a user is created from the Active Directory then the Relevance User account is the Windows user account. When you create a Relevance User that is not from the domain you have a few options to assign the Windows account.



Non-Active Directory Relevance User

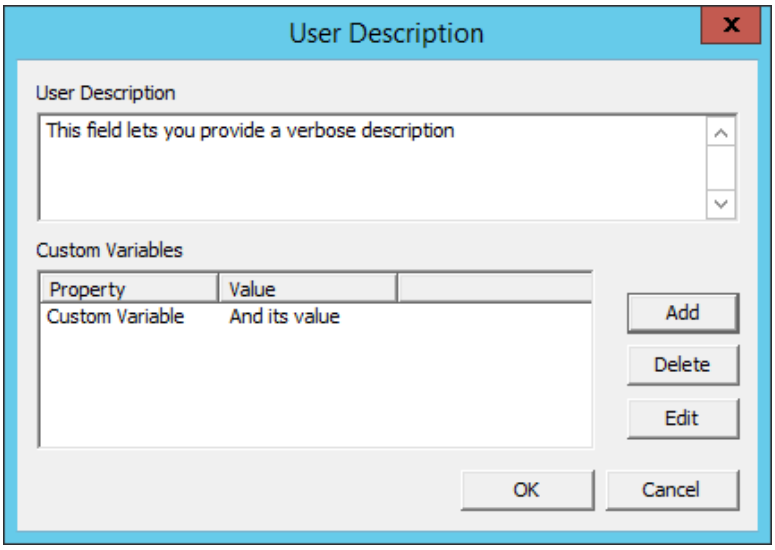
A Non-Active Directory Relevance User can be created by un-selecting the ***Active Directory User*** checkbox.

- The ***Customize*** button will launch the **User Description** window.
- The ***Password Options*** button will launch the **Password Maintenance Options** window.
- The ***Pin Options*** button will launch the **Pin Maintenance Options** window.
- The ***Change Group*** button will launch the **Choose User Group** window.
- The ***Permissions*** button will launch the **User Description** window.

32.7.1. Relevance User Settings for Non-Domain Users

The **Relevance User Information** page has several buttons that configure user settings.

The ***Customize*** button will launch the **User Description** window.



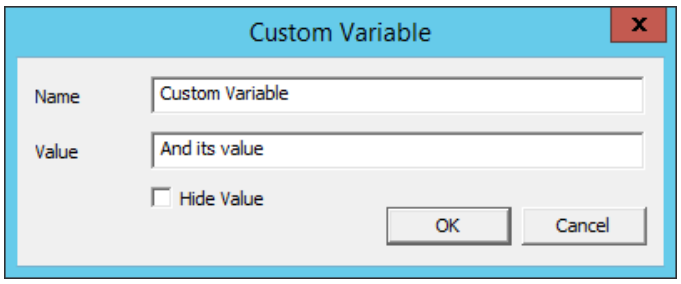
User Description Window

The **User Description** window allows a verbose description to be associated with the user account. It is displayed in the Configuration detail pane.

- **User Description** – This allows a verbose description to be added to the user account.
- **Add** – This opens the **Custom Variable** window for adding a custom variable.

Custom variables allow a single display client can be created with a custom variable as part of the path. Each user, Terminal, or location has specific data in the custom variable to modify the content that the display client delivers, allowing one display client to do the work of many.

The **Custom Variable** window is launched by selecting the ***Add*** button on the **User Description** window.

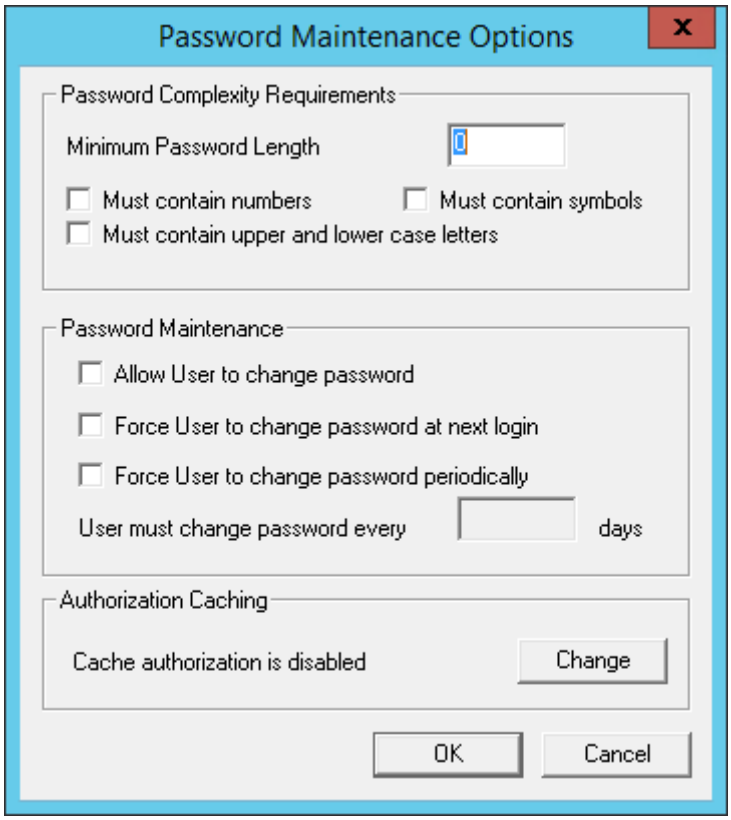


Custom Variable Window

This allows you to add a custom variable. These can be used to pass information to the AppLink display client or to the TermMon ActiveX that you embed in your application.

- ***Name*** – This field assigns the name to the custom variable.
- ***Value*** – This field assigns the value or content to the custom variable.
- ***Hide Value*** – This checkbox, if selected, will obscure the custom variable value. If unselected the value is shown.

The ***Password Options*** button will launch the **Password Maintenance Options** window.

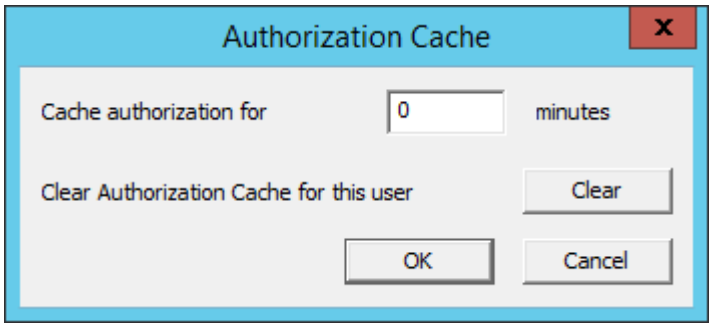


Password Maintenance Options Window

The Password Maintenance Options Window allows the user password to be configured.

- ***Minimum Password Length*** – This sets the length requirement.
- ***Must contain numbers*** – This adds the number requirement to the password.
- ***Must contain symbols*** – This adds the symbol requirement to the password.
- ***Must contain upper and lower case letters*** – This adds the mixed case requirement to the password.
- ***Allow User to change password*** – This checkbox, if unselected, will prevent a user from changing the password. If selected, it allows a user to change the password.
- ***Force User to change password at next login*** - This checkbox, if selected, will prompt the user to change their password at the next login.
- ***Force User to change password periodically*** - This checkbox, if selected, will prompt the user to change their password at the interval set in the User must change password every __ days field.
- ***User must change password every __ days*** – This sets the interval for password changes.

The ***Change*** button at **Cache authorization is disabled** will open the **Authorization Cache** window.

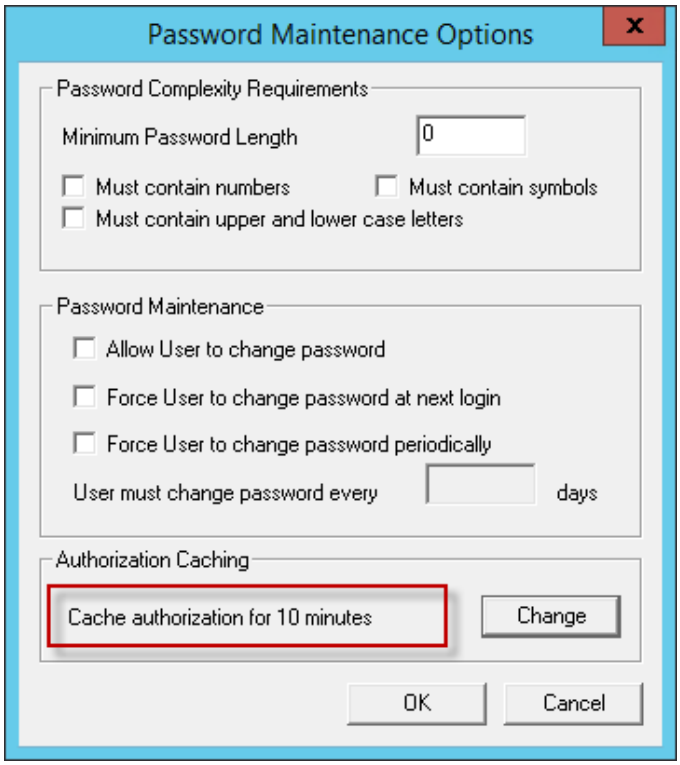


Authorization Cache Window

- ***The Cache authorization for _ minutes –*** This allows a password to be cached for the time interval set.

The user enters their password once and it is cached and provided for the duration. For example "**60**" would grant an hour and "**480**" would cover a shift of work.

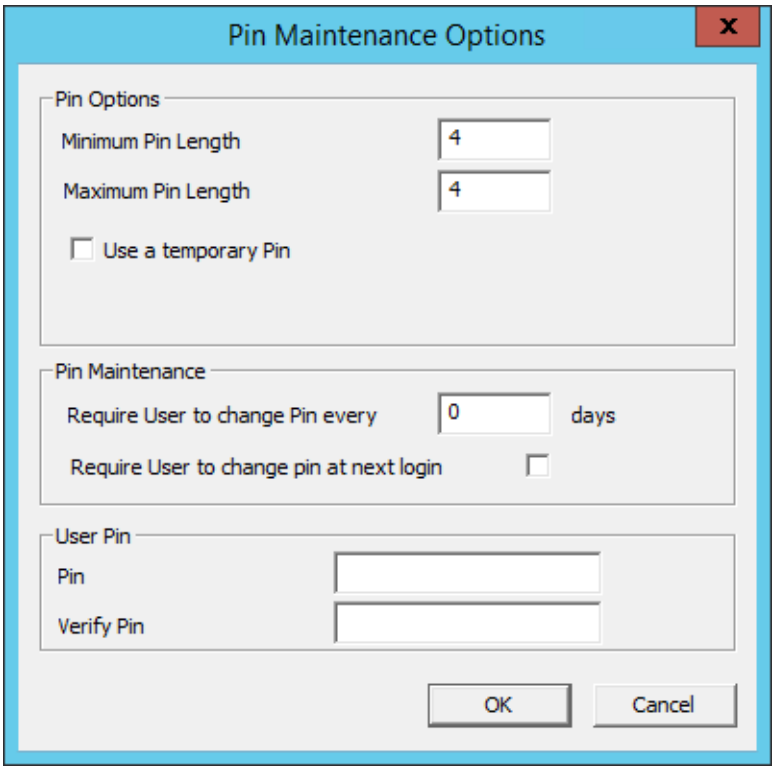
- **Clear** - This removes the cache authorization for the user and requires the user to use the password again.



Password Maintenance Options Window

The **Password Maintenance Options** window will show when a user has a cached password.

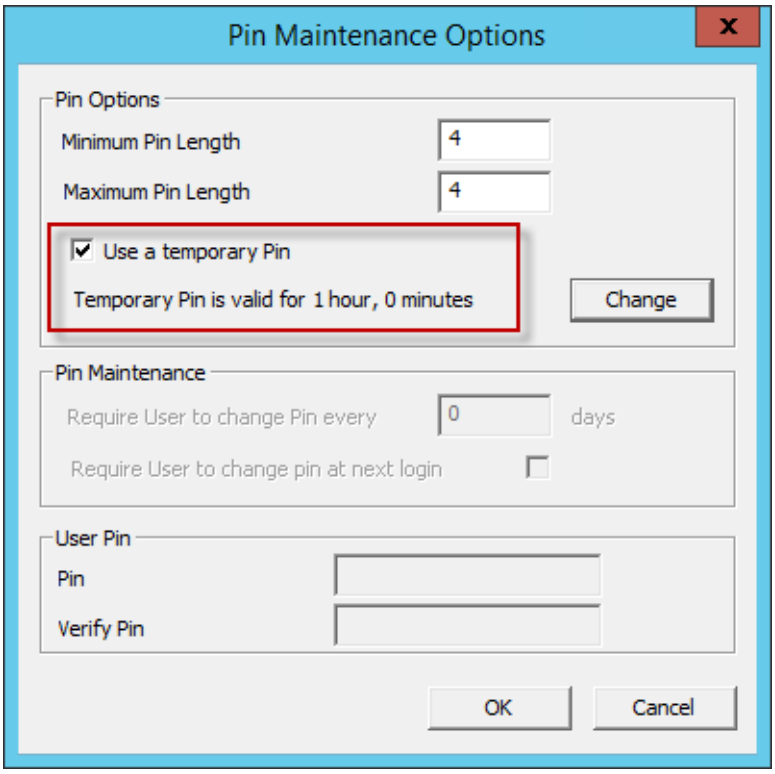
The ***Pin Options*** button will launch the **Pin Maintenance Options** window.



Pin Maintenance Options Window

The **Pin Maintenance Options** window allows the configuration of a Personal Identification Number, or PIN.

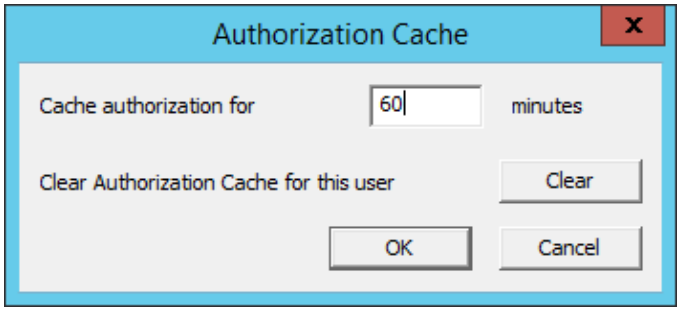
- ***Minimum Pin Length*** – This field sets the minimum length requirement for the PIN.
- ***Maximum Pin Length*** – This field sets the maximum length requirement for the PIN.
- ***Use a Temporary Pin*** – This will allow use of a PIN for the duration set in the **Authorization Cache** window. It is launched by the ***Change*** button.
- ***Require User to change Pin every _ days*** – This field sets the frequency that the PIN needs set.
- ***Require User to change pin at next login*** – This checkbox, if selected, will require the user to create a new PIN the next time they login.
- ***User Pin*** – This field sets the PIN.
- ***Verify Pin*** – This field double checks the PIN.



Pin Maintenance Options Window

A user with a temporary PIN will show the time in the Pin Maintenance Options window. This is set with the ***Change*** button.

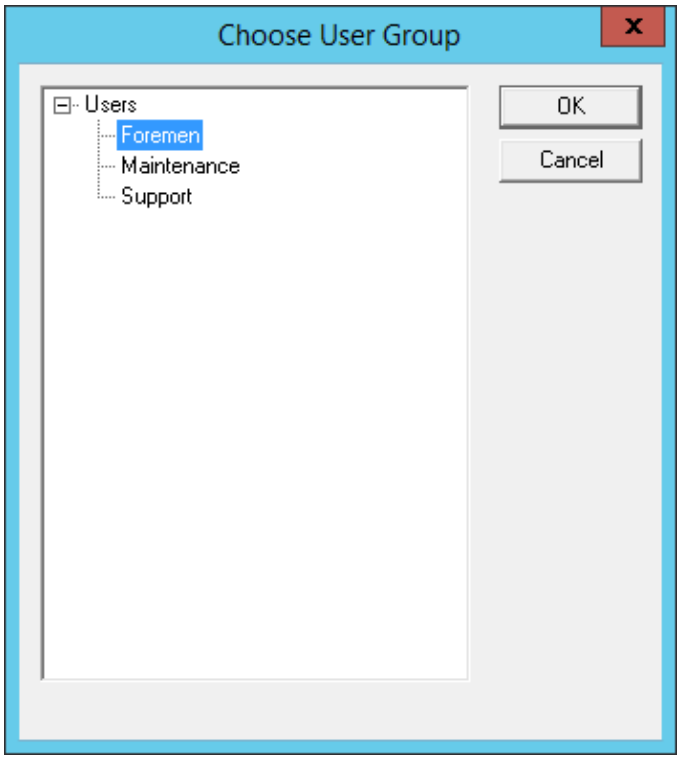
The ***Change*** button launches the **Authorization Cache** window.



Authorization Cache Window

The **Authorization Cache** window allows the duration of the temporary PIN in the ***Cache authorization for __ minutes*** field. ***Clear*** will clear the cache.

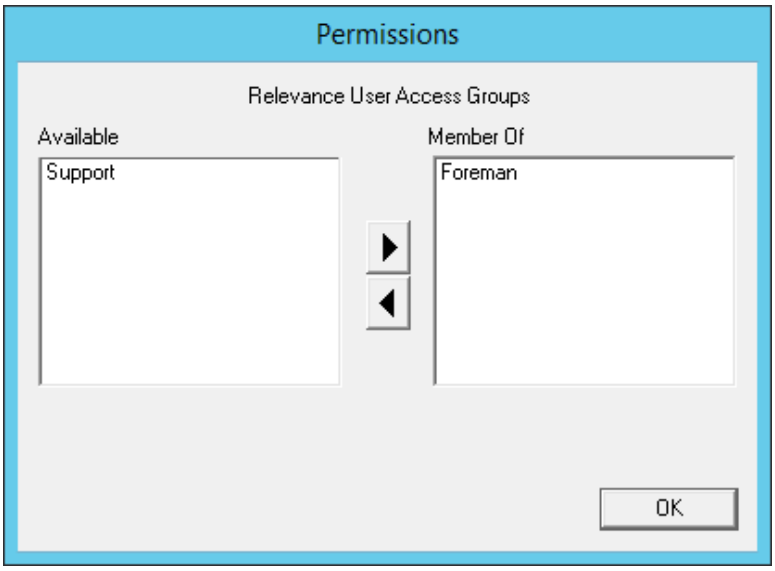
The ***Change Group*** button will launch the **Choose User Group** window.



Choose User Group

The **Chose User Group** allows you to select the Relevance User group to nest the user in.

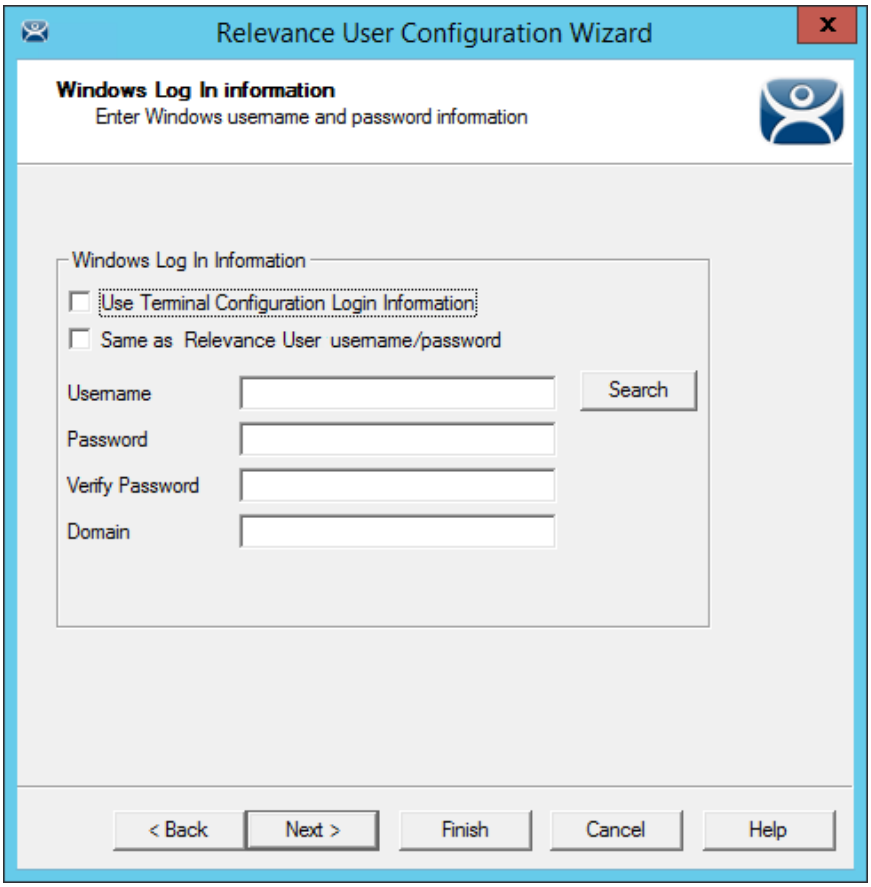
The ***Permissions*** button will launch the **Permissions** window.



Permissions Window

The user can be granted permissions by moving the desired Access Group into the ***Member Of*** column.

The **Relevance User Configuration** wizard is the same until the **Windows Log In Information** page.



Windows Log In Information Page

If you chose to assign a display client to the user by selecting the ***User-specific Display Clients*** on the **Display Client Selection** page then you will need to provide a Windows account to start the session.

This page will not be displayed if the Relevance User is selected from the Active Directory.

Windows Log In Information page has four options for logging on to a session

- **Use Terminal Configuration Login Information checkbox**

The Relevance User can use the Terminal's username and password to auto-log on to the Remote Desktop Server. To do this, check the ***Use Terminal Configuration Login Information*** checkbox

Since a different account is used at each Terminal this doesn't keep a consistent session for the Relevance User.

- **Same as Relevance User username/password checkbox.**

The Relevance User can use the Relevance User username and password to auto-log on to the Remote Desktop Server. To do this, check the ***Same as Relevance User username/password*** checkbox.

The Relevance User username and password must match a Windows User username and password to get authenticated by Windows.

If the Relevance User is selected from the Active Directory then this is the default behavior.

- **Use the *Username* and *Password* fields.**

The Relevance User can use an aliased username and password to auto-log on to the Remote Desktop Server. To do this, use the fields for the ***Username***, ***Password***, and ***Domain*** that are provided.

This allows you to tie the Relevance User account to a different Windows account. This allows you to alias the login, hiding the actual Windows account from the user.

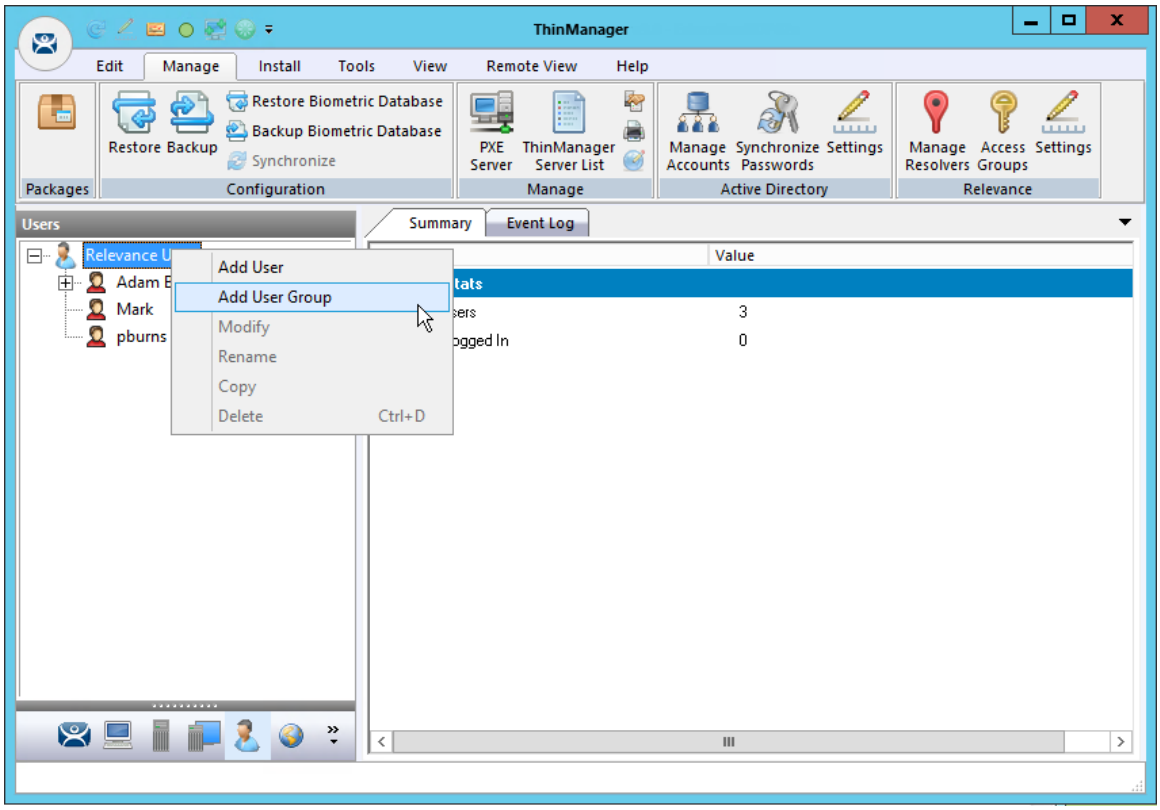
- **Blank Username and Password fields.**

The Relevance User can be required to manually log onto the Remote Desktop Servers. To do this, leave the checkboxes unchecked and the ***Username***, ***Password***, and ***Domain*** empty. When a Relevance User logs in with their Relevance account they will be prompted to enter a valid Windows account and password.

33. Relevance User Groups

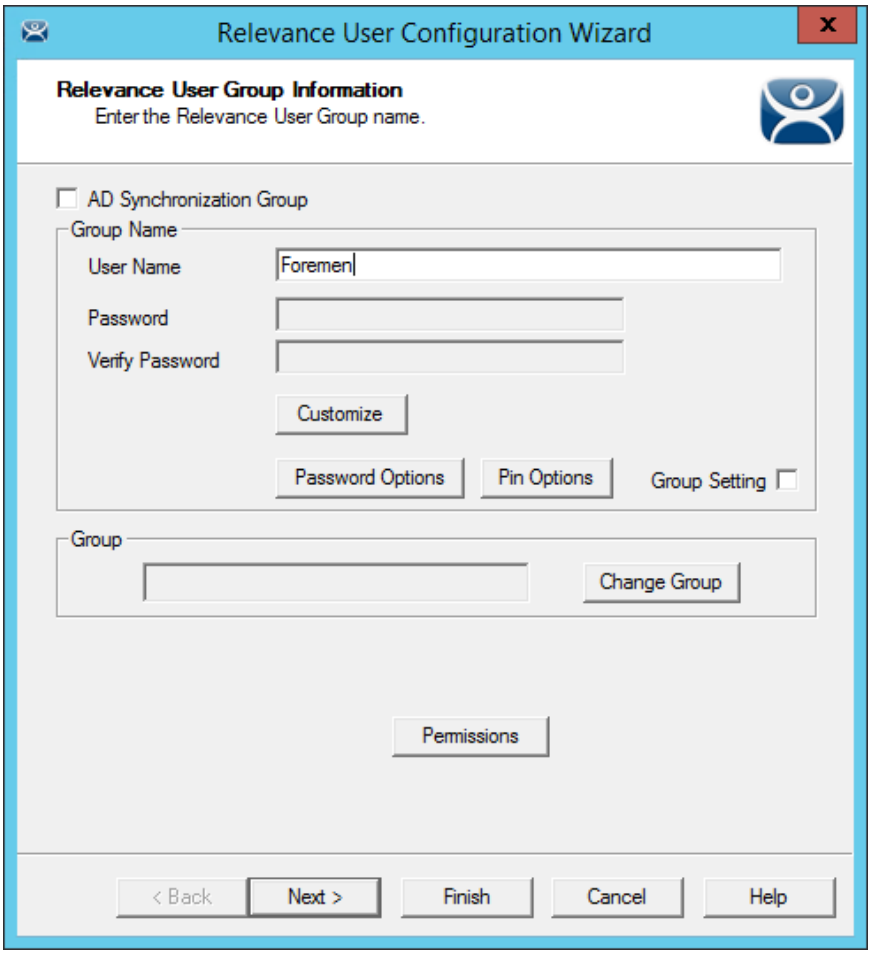
Relevance Users can be organized into Relevance User Groups, just as Terminals can be organized into Terminal Groups. This section will show the configuration of a Relevance User Group.

The **Relevance Users Group Configuration Wizard** can be launched by right clicking on the **Relevance User**s branch of the tree and selecting ***Add Relevance User Group***.



Add User Group Command

Relevance User Groups are defined using the **Relevance User Configuration Wizard**. It is launched by selecting the **User icon** at the bottom of the ThinManager tree, right clicking on the **Relevance User** branch, and selecting ***Add User Group***.

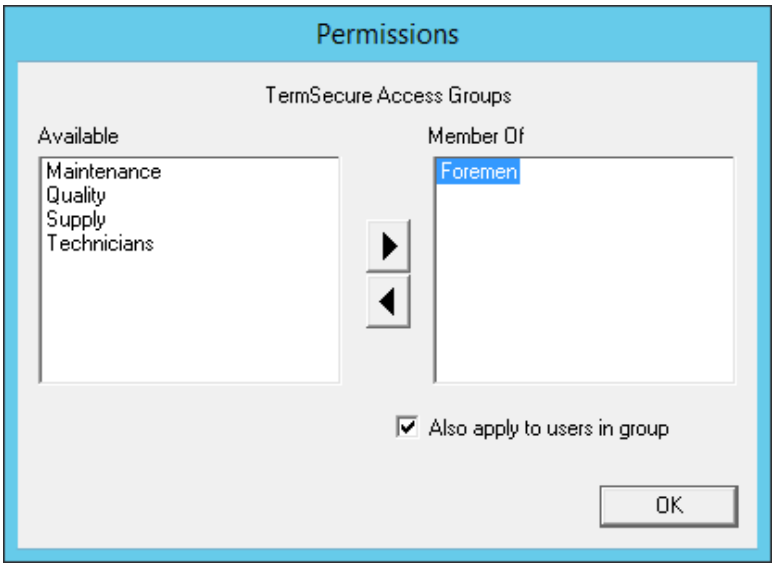


ThinManager User Information

The **Relevance User Group**, like the **Terminal Group**, has a ***Group Setting*** checkbox. Selecting the ***Group Setting*** checkbox will apply the setting to all members of the group.

The ***Permission*** button allows you to apply permissions to the group.

Active Directory Integration allows a Relevance Group to be formed and populated straight from the Active Directory. See Batch Create Relevance Users using Active Directory OU on page 527.



Permissions Window

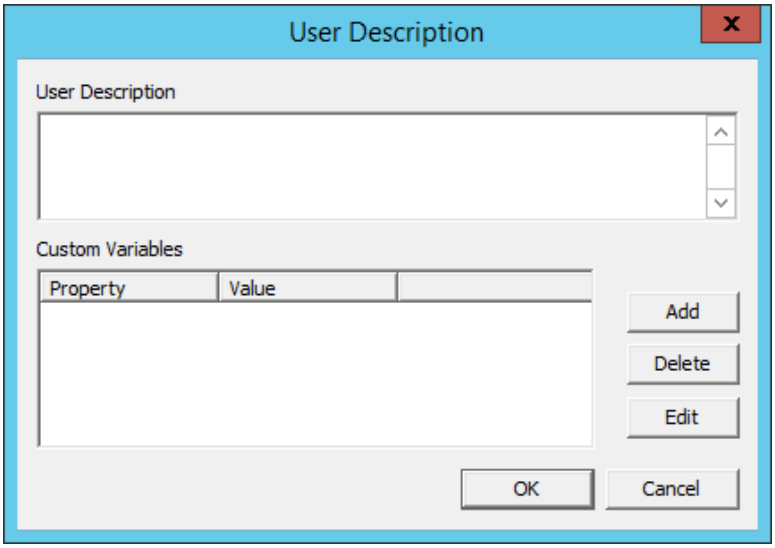
Highlight the desired permission and move it to the ***Member Of*** list to add.

Highlight the group and check the ***Also apply to users in group*** checkbox to apply the permission to all group members.

Click the ***OK*** button to close and apply.

The ***Customize*** button on the **Relevance User Group Information** page launches the **User Description** window.

The **User Description** window allows a verbose description to be associated with the user account. It is displayed in the Configuration detail pane.

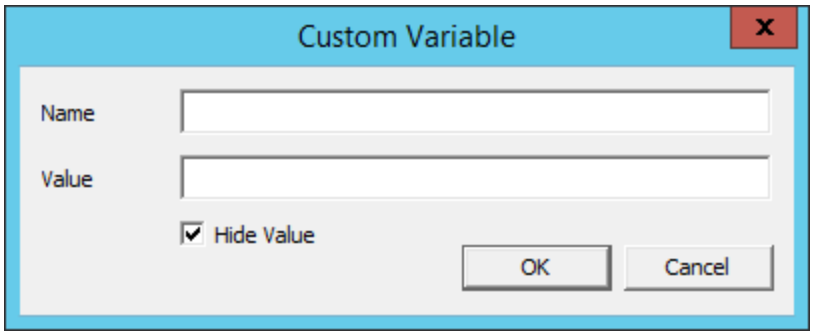


User Description Window

- **User Description** – This allows a verbose description to be added to the user account.
- **Add** – This opens the **Custom Variable** window for adding a custom variable.

Custom variables allow a single display client can be created with a custom variable as part of the path. Each user, Terminal, or location has specific data in the custom variable to modify the content that the display client delivers, allowing one display client to do the work of many.

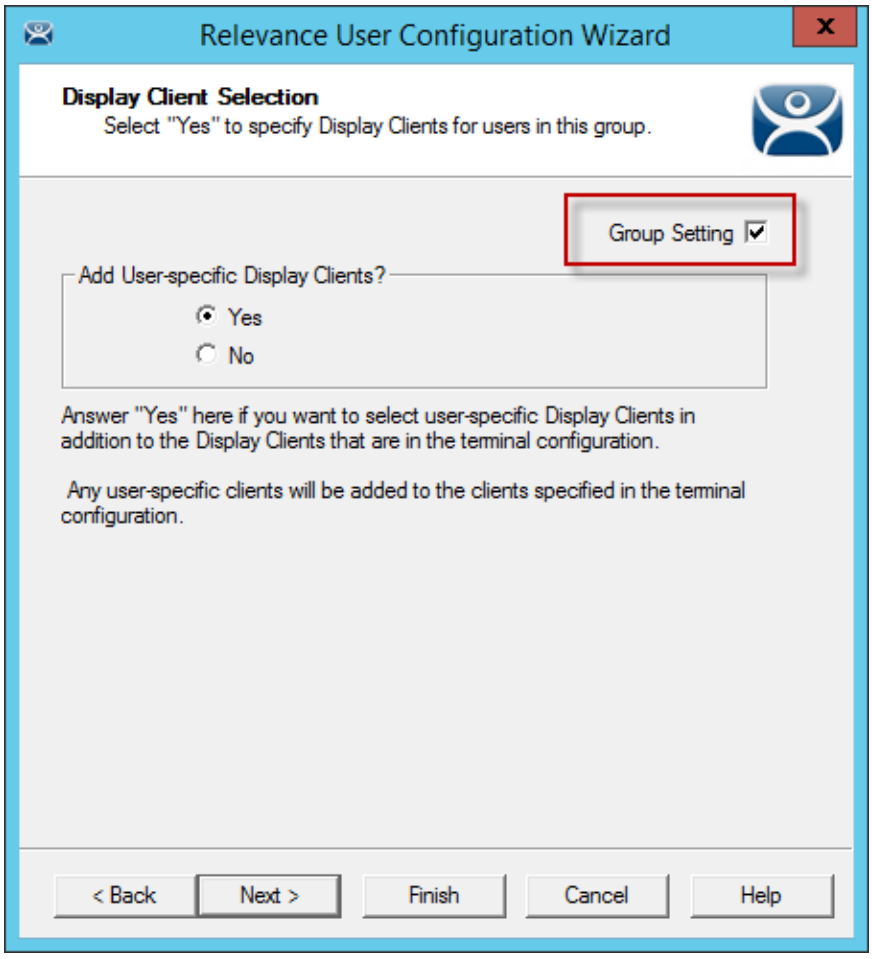
Additionally a custom variable can pass specific data to an application through the TermMon ActiveX.



Custom Variable Window

- ***Name*** – This field assigns the name to the custom variable.
- ***Value*** – This field assigns the value or content to the custom variable.
- ***Hide Value*** – This checkbox, if selected, will obscure the custom variable value. If unselected the value is shown.
- **OK** – accepts the changes and closes the window.

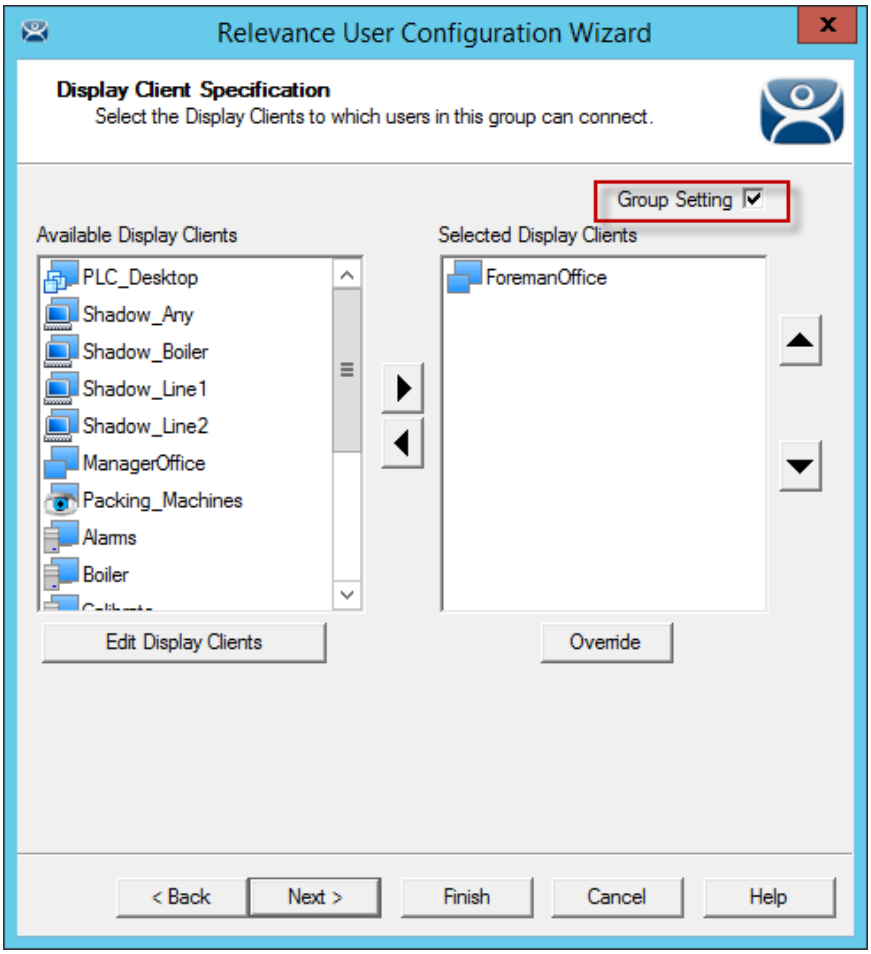
Select ***Next*** on the **Relevance User Group Information** page to go to the **Display Client Selection** page.



ThinManager User Information

Select ***Yes*** to specify Display Clients for this user.

Select ***Next*** to go to the **Display Client Specification** page.

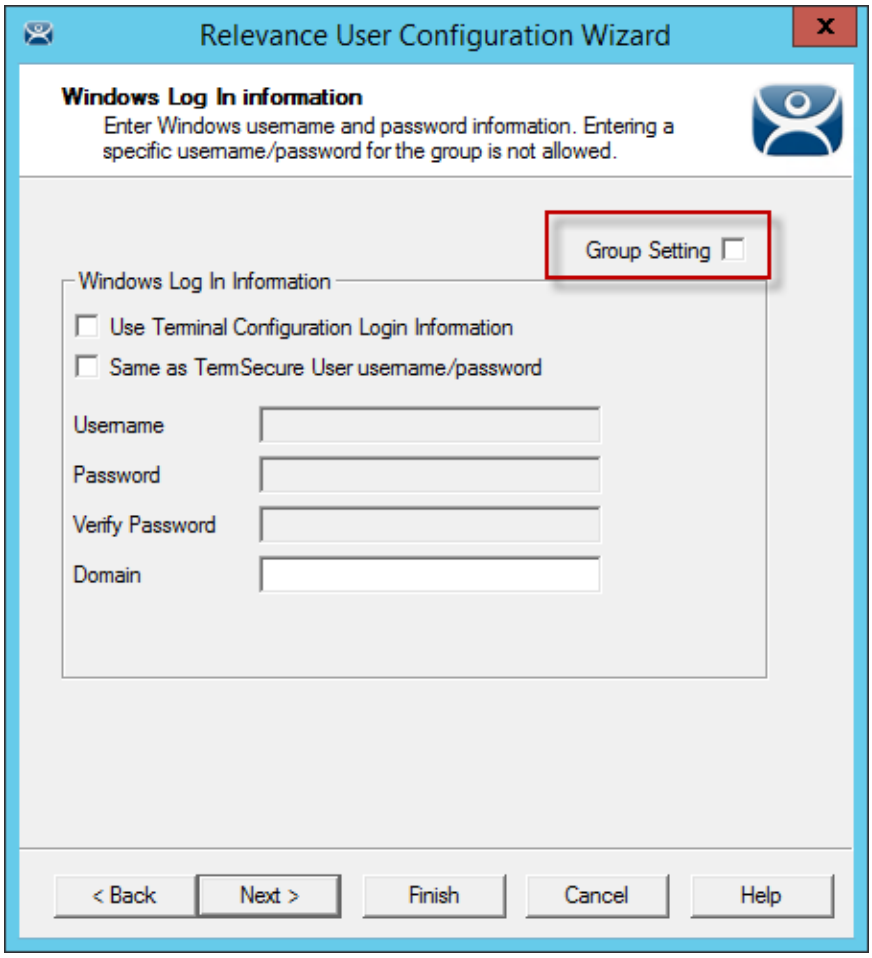


ThinManager User Information

Select the display clients for the group and move them to the ***Selected Display Clients*** list by double clicking on them.

Select the ***Group Settings*** checkbox.

Select ***Next*** to continue the group configuration.



Windows Log In Information Page

The **Windows Log In Information** page has a ***Group Setting*** checkbox for the ***Use Terminal Configuration Login Information*** checkbox and ***Same as Relevance User username/password*** checkbox.

The ***Username*** and ***Password*** fields are inactive because every user needs a unique Windows account and so a group setting isn't allowed.

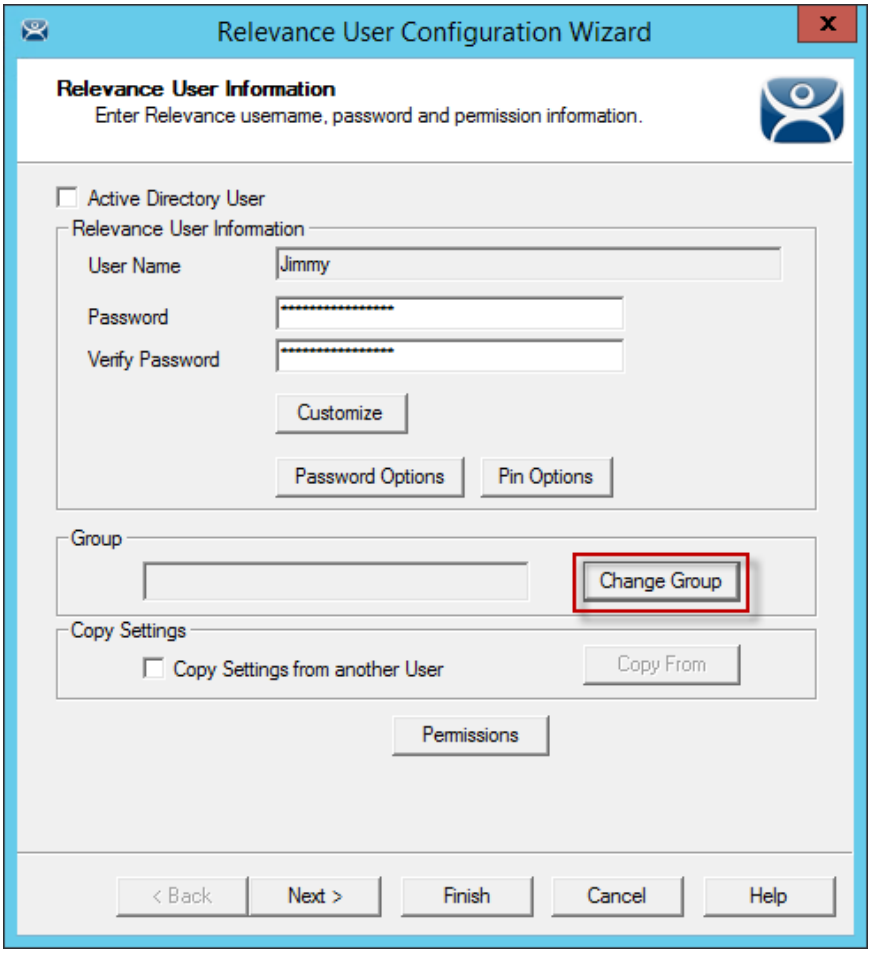
The rest of the wizard follows the **Relevance User Configuration** wizard. Select the ***Next*** button to continue or select the ***Finish*** button to close and save the settings.

Note: Any member of this group will receive the Group Settings. Change a Group Setting will change that Group Setting for all members.

33.1. Adding a Relevance User to a Relevance User Group

Relevance Users can be added to the Relevance Group.

Create a new Relevance User by right clicking on the **Relevance Users** branch in the ThinManager tree and select ***the Add Relevance User*** option.

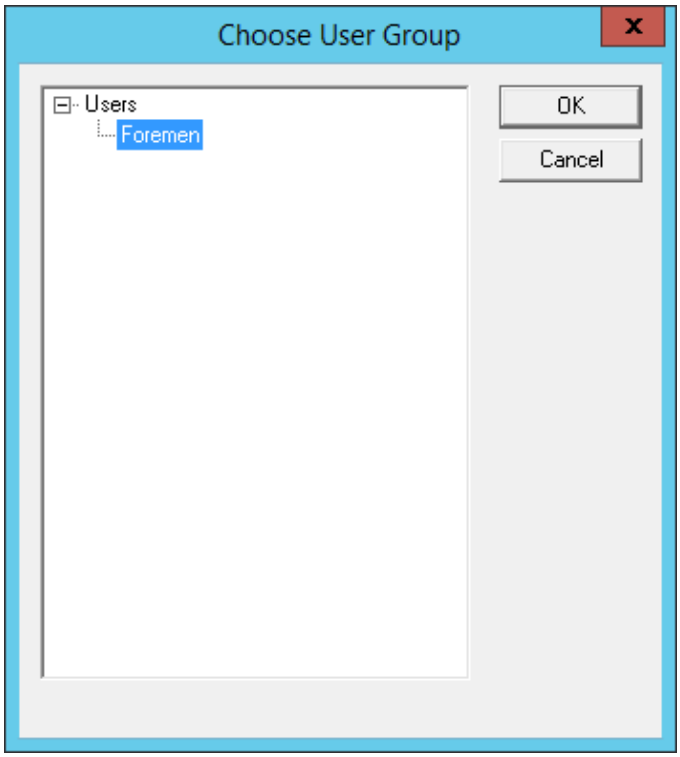


Relevance User Information Page

Enter a name for the Relevance User in the ***User Name*** field.

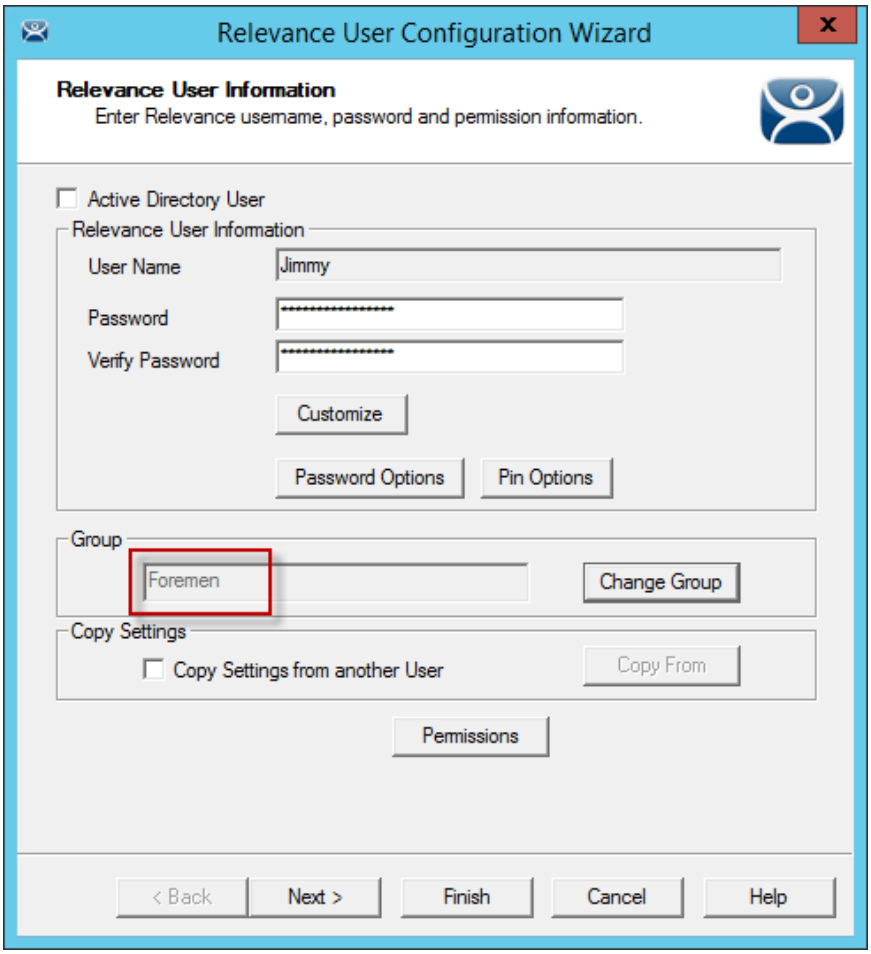
Select the ***Change Group*** button.

This will launch the **Choose User Group** window.



Choose User Group Window

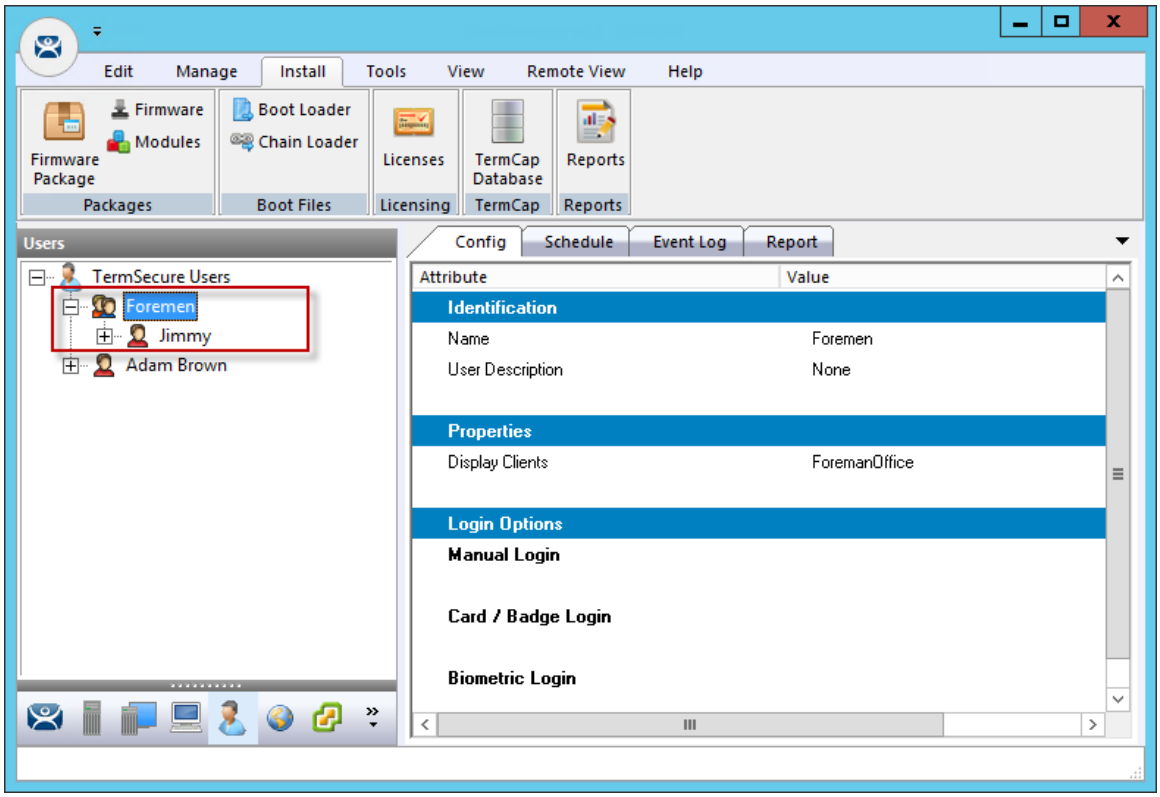
Highlight your **Relevance Users Group** and select ***OK*** to close the window and accept the changes.



Relevance User Information Page

The **Relevance User Group** will now be displayed in the ***Group*** field.

Select the ***Finish*** button to accept the configuration.



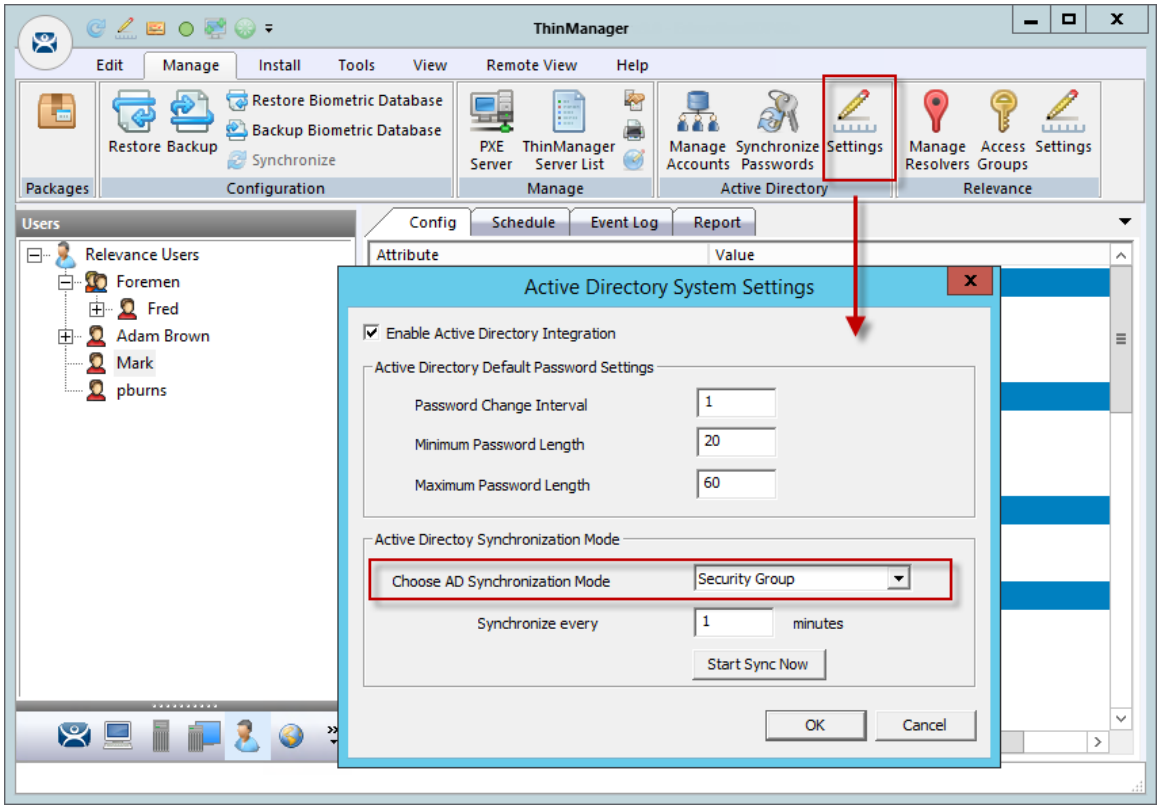
Group Membership

Once a Relevance User has joined a group it will be displayed in the tree under the group.

33.2. Batch Create Relevance Users using Active Directory OU

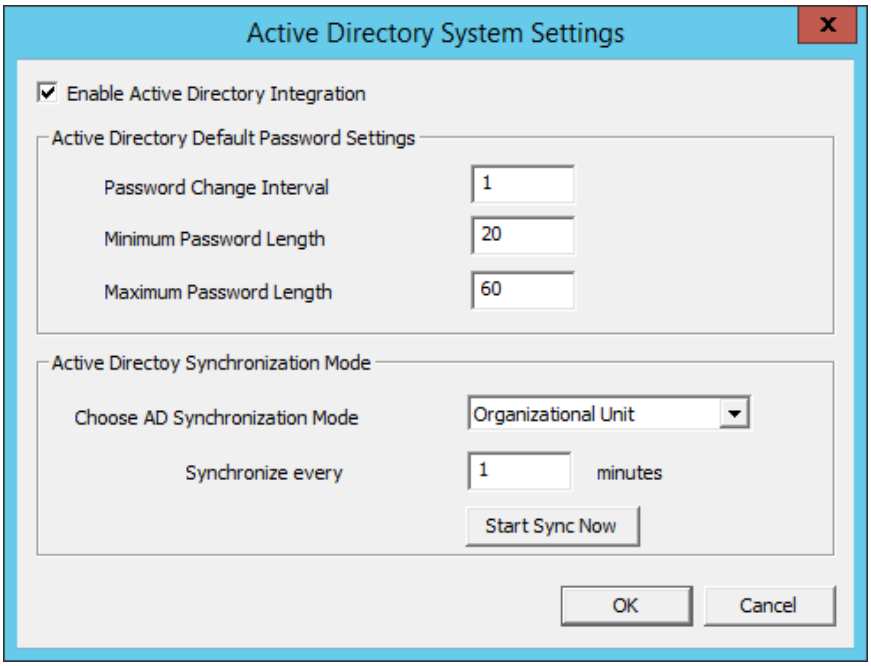
You can create Relevance Users in a batch, either by selecting one Windows Security Group or multiple Active Directory organizational units (OU).

You can select multiple OUs but only one Security Group because a user can only reside in one OU but they can be members in multiple Security Groups. Limiting to a single Security Group prevent duplicate accounts.



Active Directory System Settings

Select ***Manage > Active Directory Settings*** to launch the **Active Directory System Settings** window.



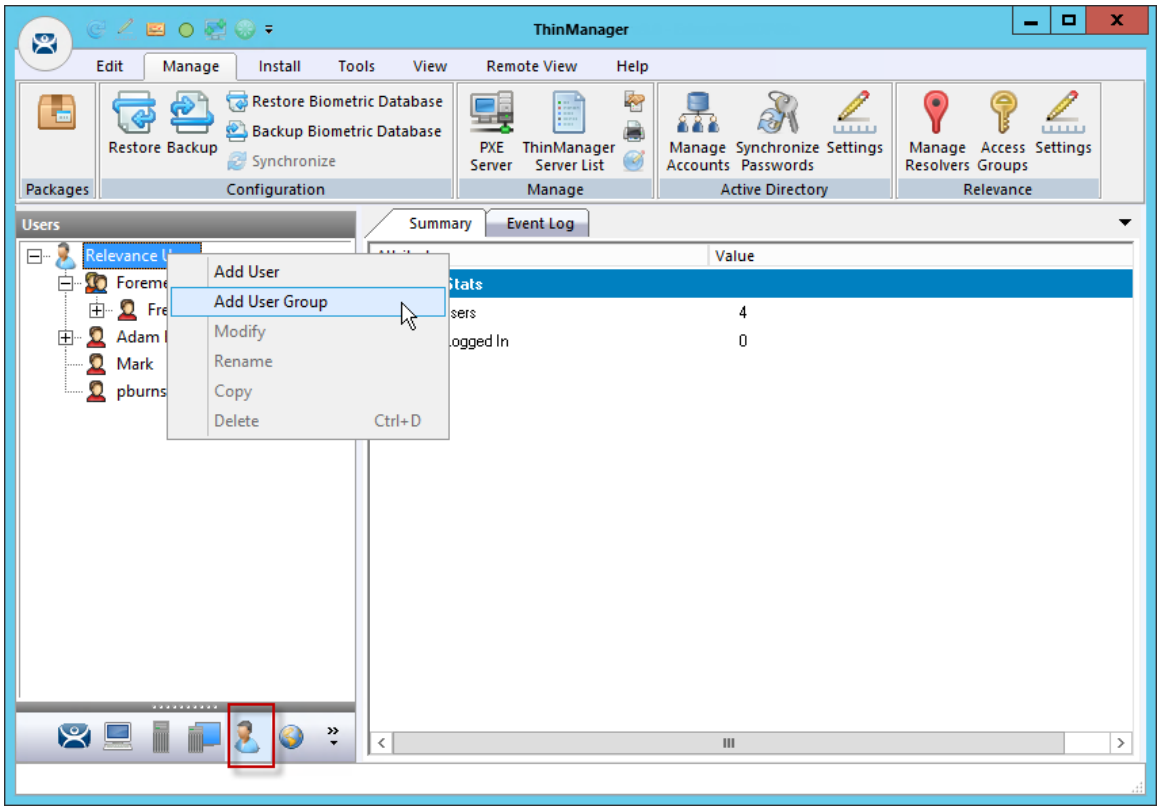
Active Directory System Settings window

Select either **Organizational Unit** or **Security Group** in the ***Choose AD Synchronization Mode*** drop-down.

This manual will show the batch creation of Relevance Users using Active Directory Organizational Units.

Note: Since a user can be in several Windows Security Groups but only one Organizational Unit you can only select one Windows Security Group as a Relevance User Group but you can add many Organizational Units.

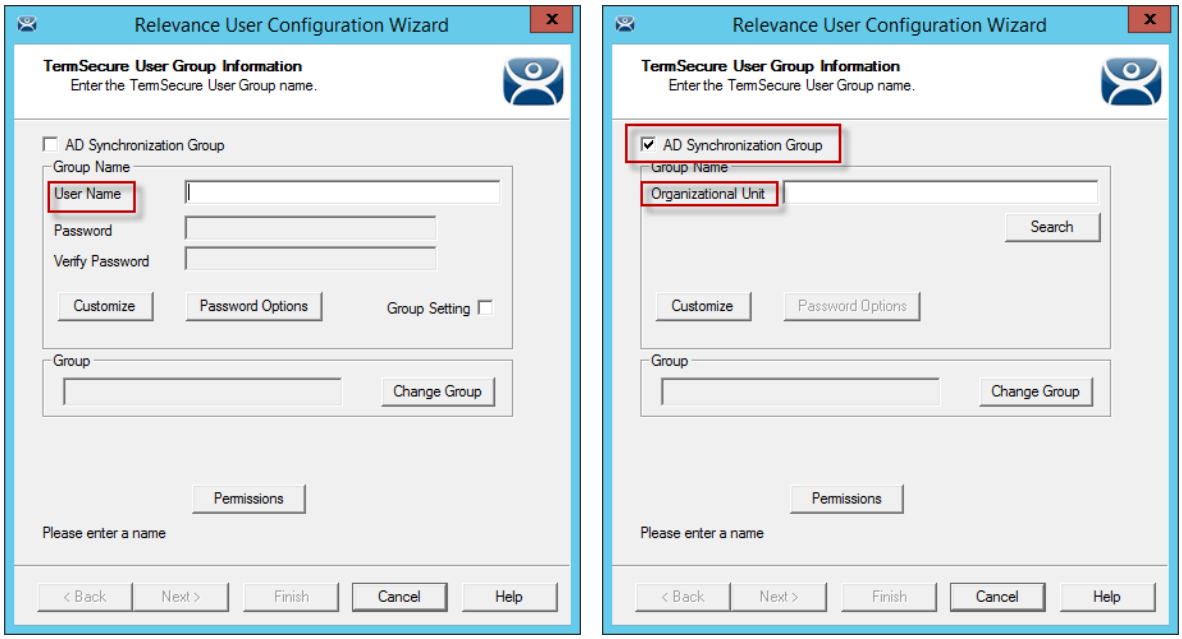
Select ***OK*** to close.



Add User Group Command

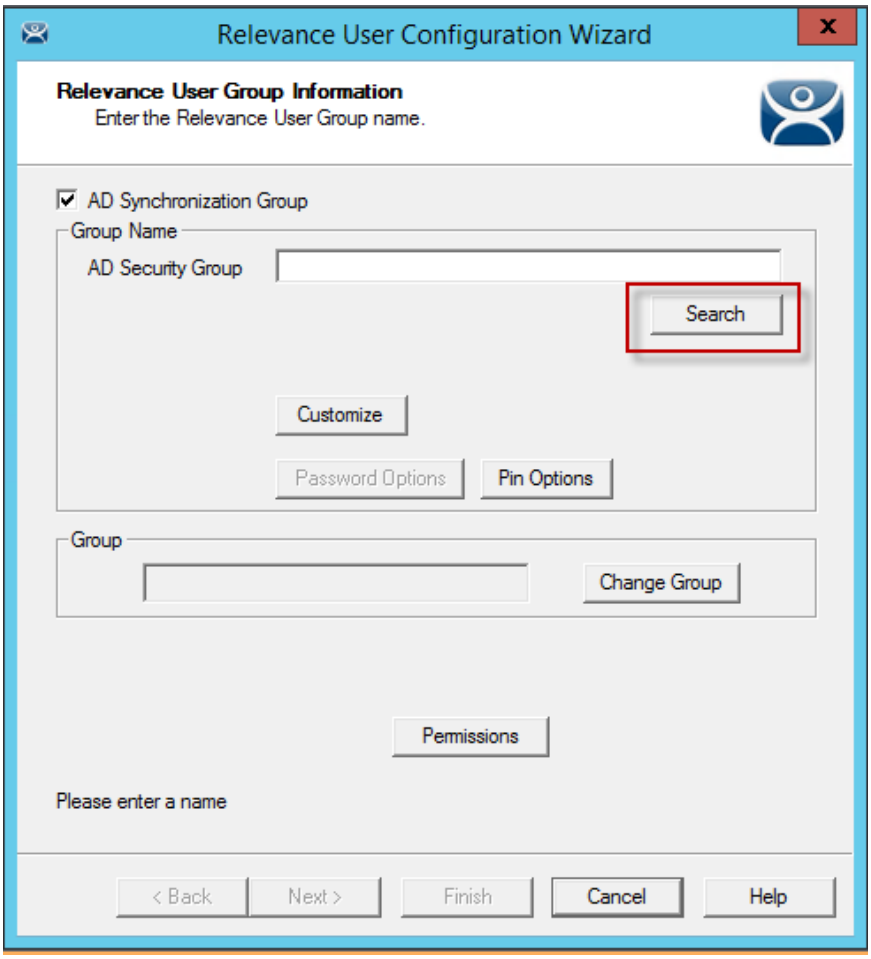
Relevance User Groups are defined using the **Relevance User Configuration Wizard**. It is launched by selecting the **User icon** at the bottom of the ThinManager tree, right clicking on the **Relevance User** branch, and selecting ***Add User Group***.

This will launch the **Relevance User Configuration Wizard** for the Relevance User Group.



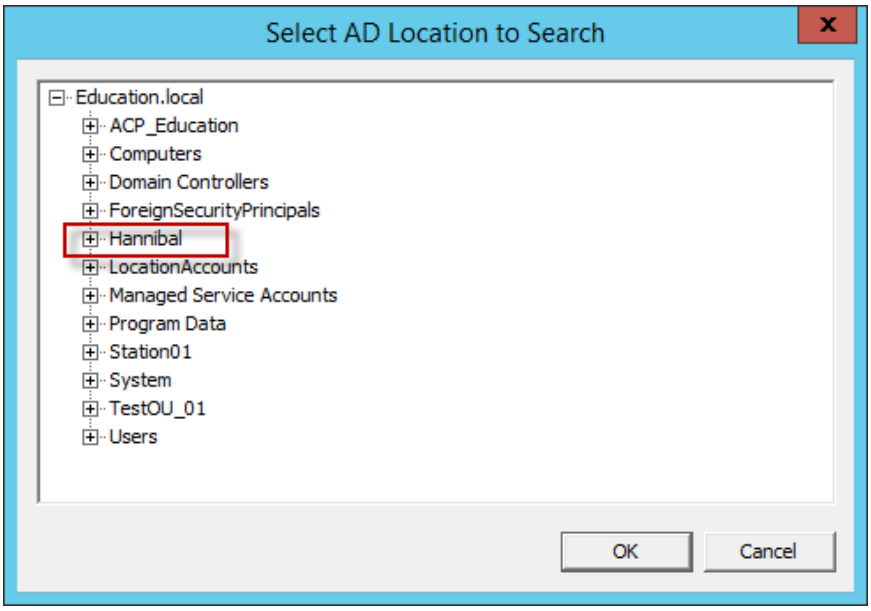
Relevance User Group Information Page

Check the ***AD Synchronization Group*** checkbox on the **Relevance User Group Information** page. This will change the ***User Name*** field to an ***Organizational Unit*** field.



Relevance User Group Information Page

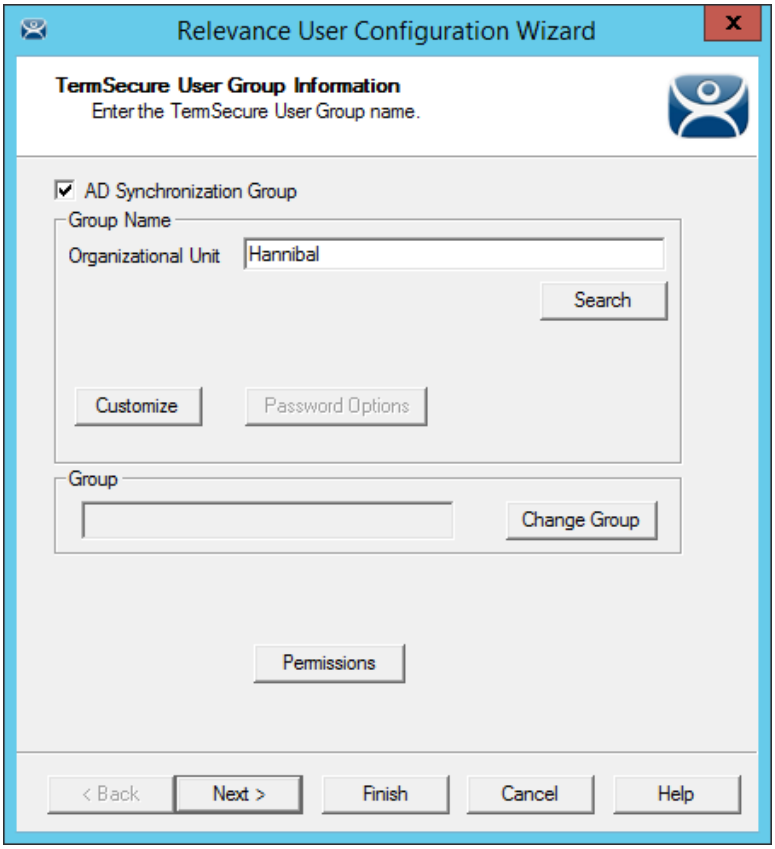
Select the ***Search*** button to launch the **Select AD Location to Search** window.



Select AD Location to Search Window

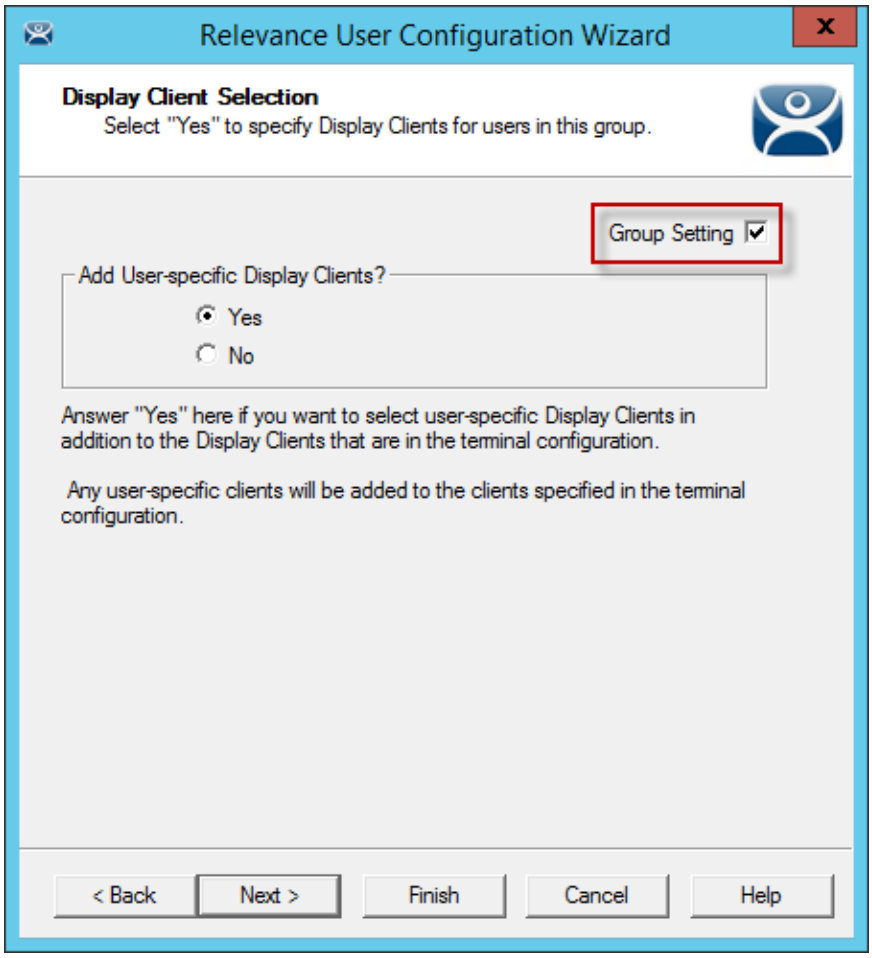
The **Select AD Location to Search** window will list the Organizational Units for the domain that the ThinManager Server is a member.

Highlight the desired Organizational Unit and select the ***OK*** button.



Relevance User Group

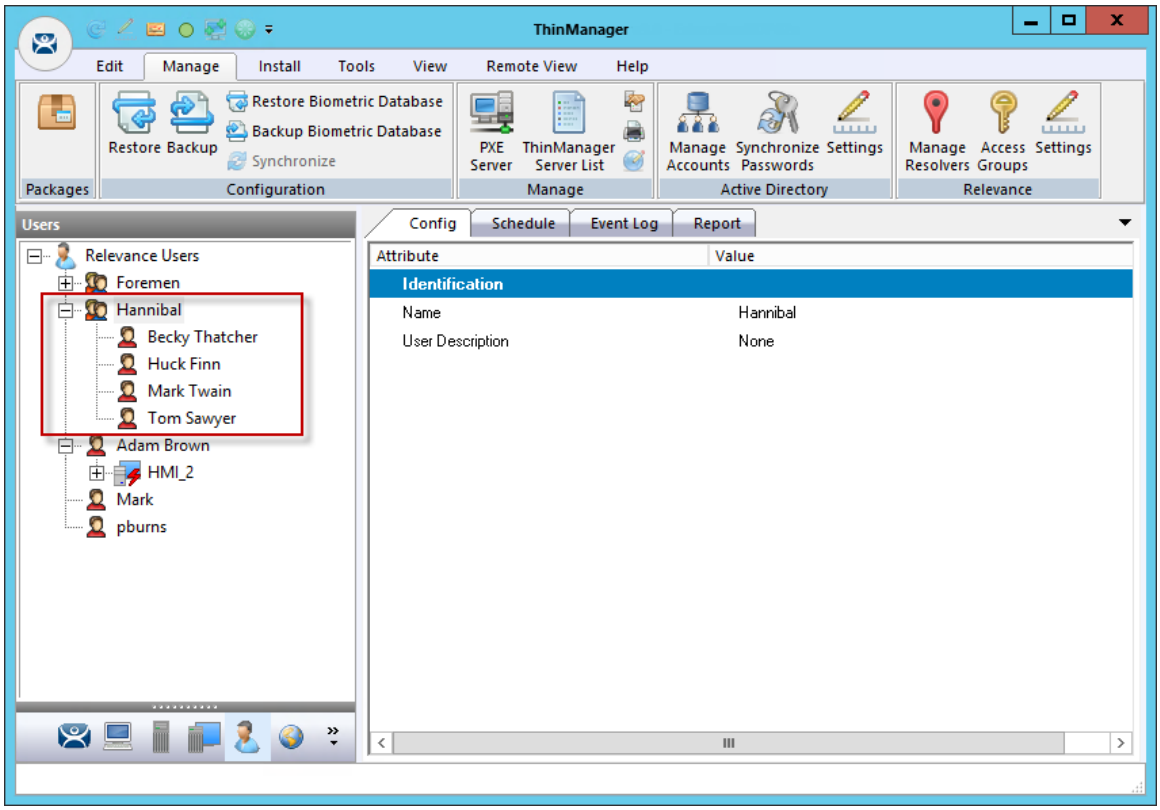
This will name the **Relevance User Group** after the Organizational Unit. Select ***Next.***



Group Settings

Once a Relevance User Group is created a ***Group Setting*** checkbox appears on each page. Selecting this checkbox will apply the setting to all members of the group. This speeds configuration by have a change applied to all members at once.

You may select ***Finish*** now or select ***Next*** to complete the entire wizard.

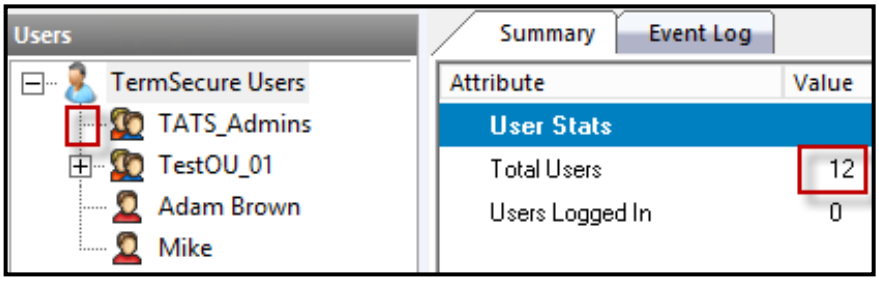


Hannibal Relevance User Group

Once the ***Finish*** button is selected the Relevance User Group will be created. It may take some time to populate the Relevance User Group depending on the Active Directory size.

Once populated all members of the Organizational Unit will show up as members of the Relevance User Group.

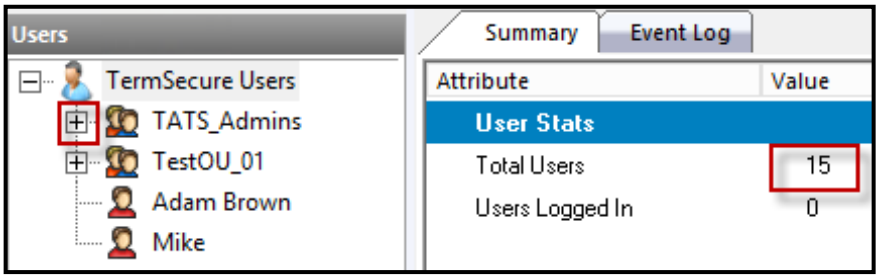
Users added to AD will be added to the ThinManager tree, users deleted from AD will be removed from the ThinManager tree.



Relevance User Group Created but Not Populated

One way to see if the users are created is to monitor the Total Users count by highlighting the Relevance User branch in the ThinManager tree.

When the Relevance User group is first created it won't have an expansion box and the user count won't have increased.



Relevance User Group Created and Populated

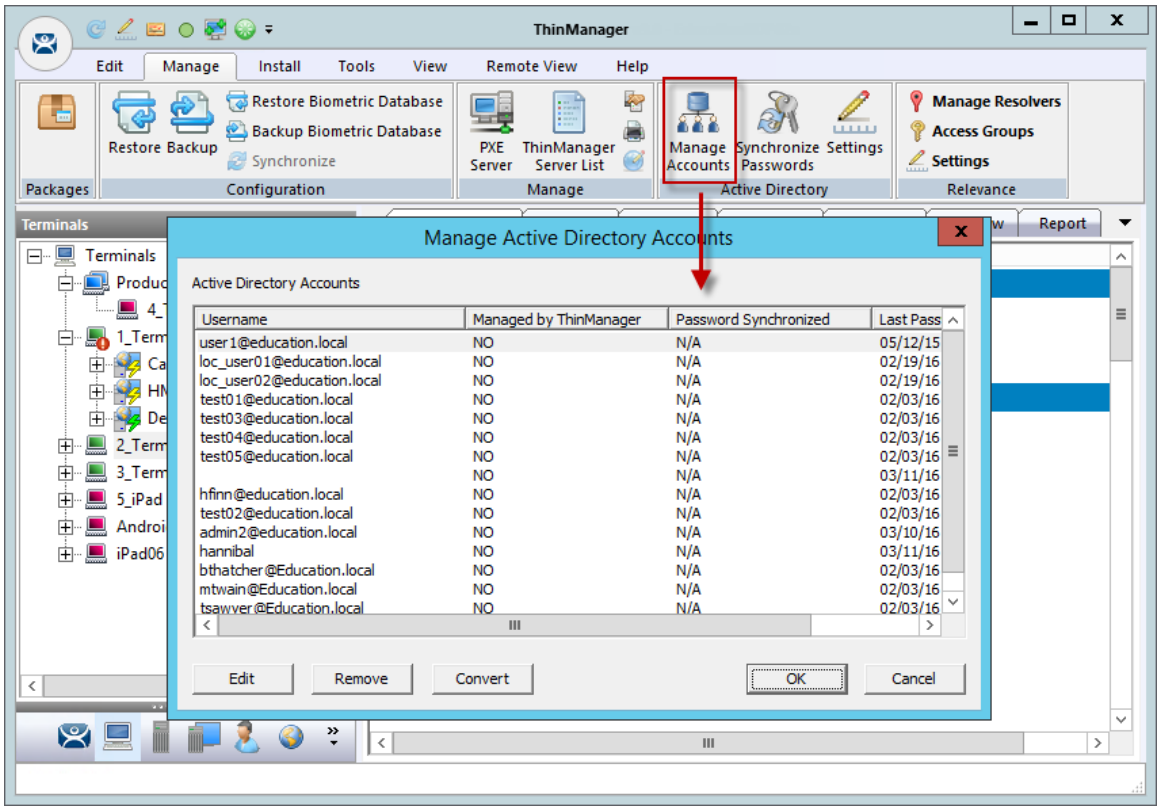
Once ThinManager has imported the Relevance Users the user count will increase and the expansion box will appear.

34. Password and Account Management

ThinManager has tools to manage domain accounts and passwords.

34.1. Active Directory - Manage Accounts Management

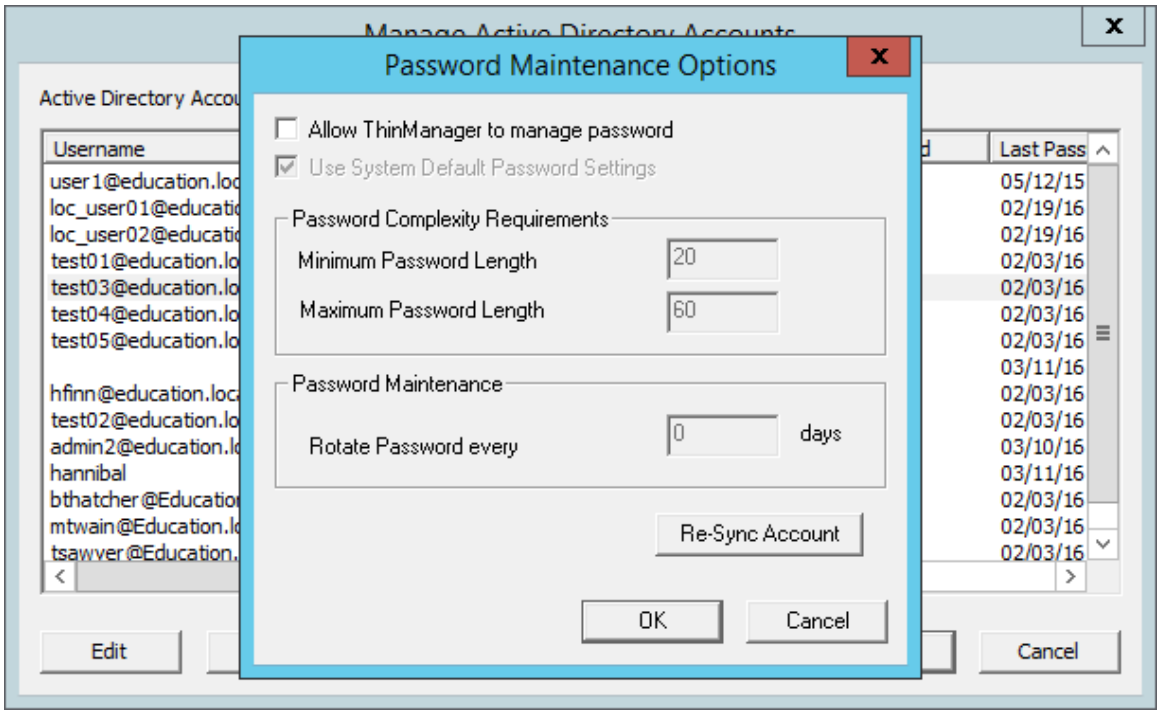
The first tool is the **Manage Accounts** tool.



Manage Active Directory Accounts

Selecting ***Manage > Manage Accounts*** will launch the **Manage Active Directory Accounts** window. It lists all the AD user accounts that have been referenced in ThinManager.

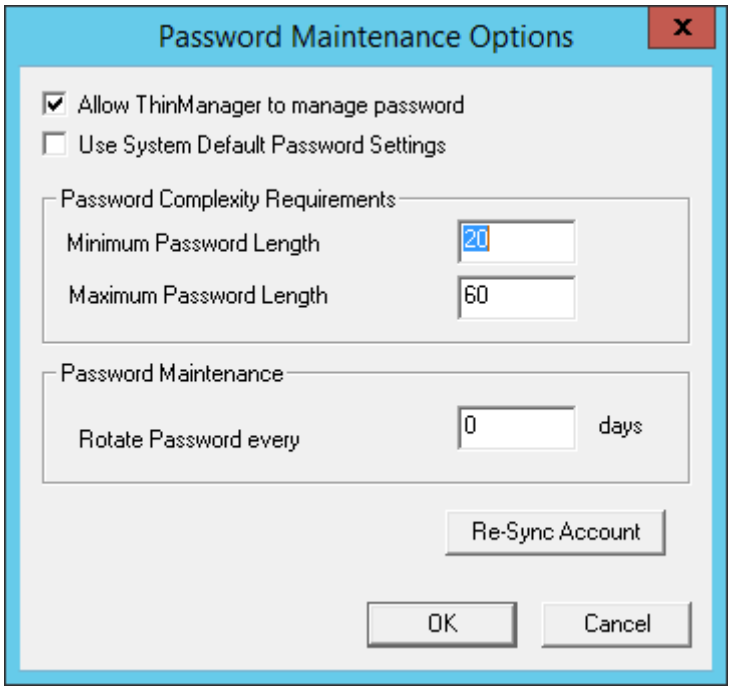
Double click on an account to launch the **Password Maintenance Options** window.



Password Maintenance Options Window

The **Password Maintenance Options** window allows you to have ThinManager manage the password for the account.

Check the ***Allow ThinManager to manage password*** checkbox to add this account to the list of managed accounts.



Password Maintenance Options

Once the ***Allow ThinManager to manage password*** checkbox is checked you can use the system defaults or uncheck the ***Use System Default Password Settings*** to customize the password settings.

The password settings include

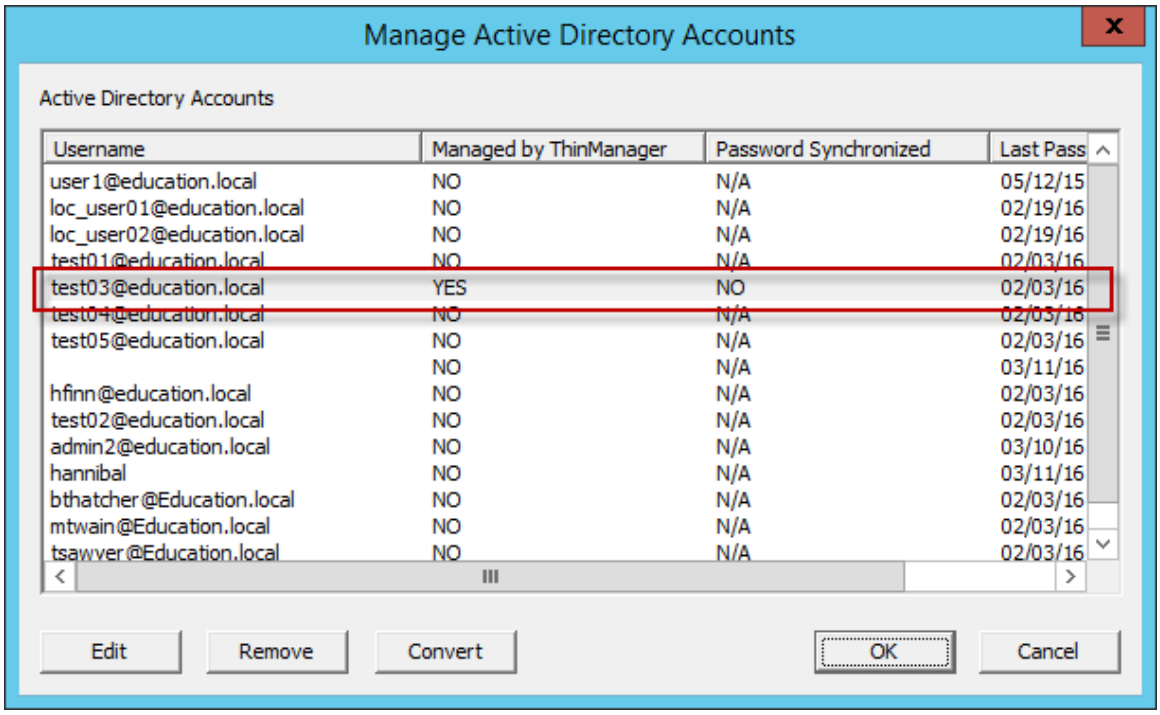
Password Complexity Requirements:

- ***Minimum Password Length*** – This is the minimum number of characters a password may have.
- ***Maximum Password Length*** – This is the maximum number of characters a password may have.

Password Maintenance:

- ***Rotate Password every*** – This is the number of days before the password must be changed.

Select the ***OK*** button to accept the changes or select the ***Cancel*** button to close the dialog without saving.

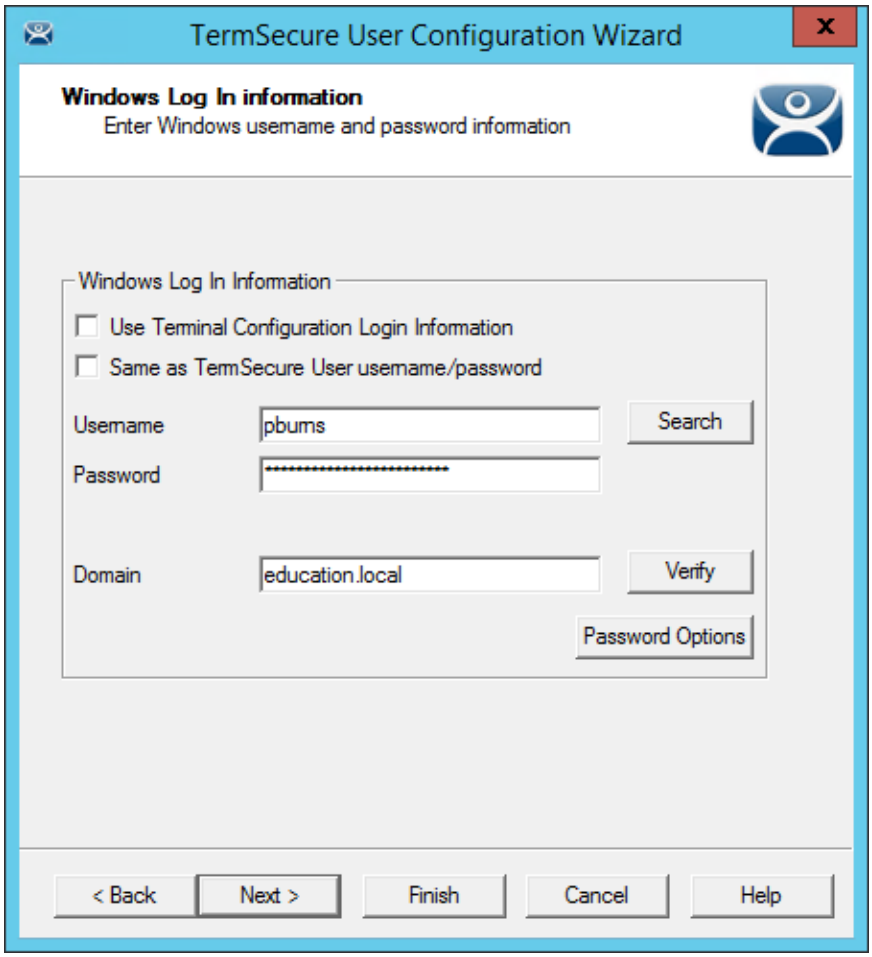


Manage Active Directory Accounts

Once the ***Allow ThinManager to manage password*** checkbox is checked then the account will be displayed as a managed account.

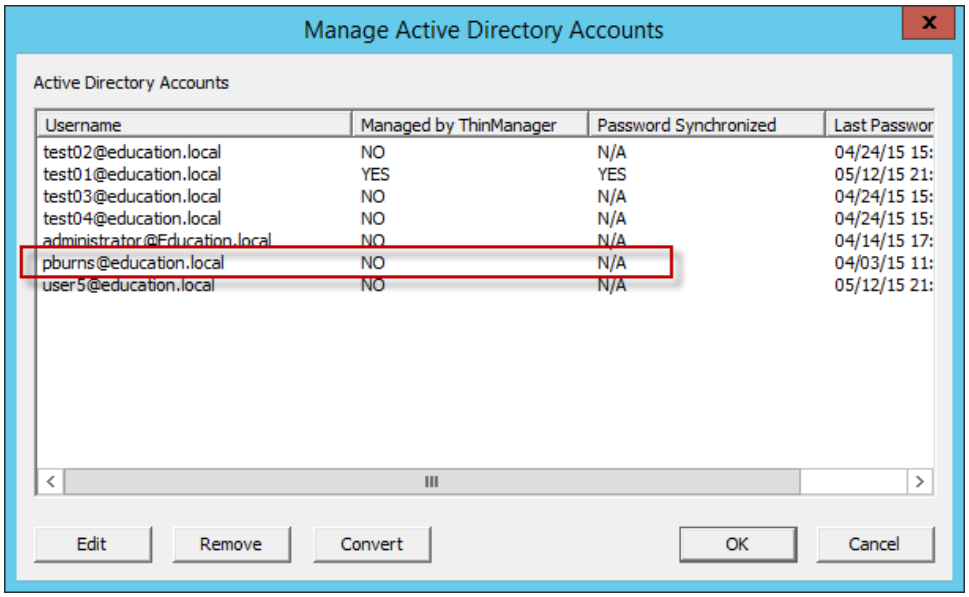
34.2. Active Directory – Convert Accounts

Domain accounts that were used in previous versions of ThinManager can be converted to a managed account with the ***Convert*** function.



Legacy Domain Log In

This shows a domain account that was entered in an earlier version of ThinManager that didn't have Active Directory integration.

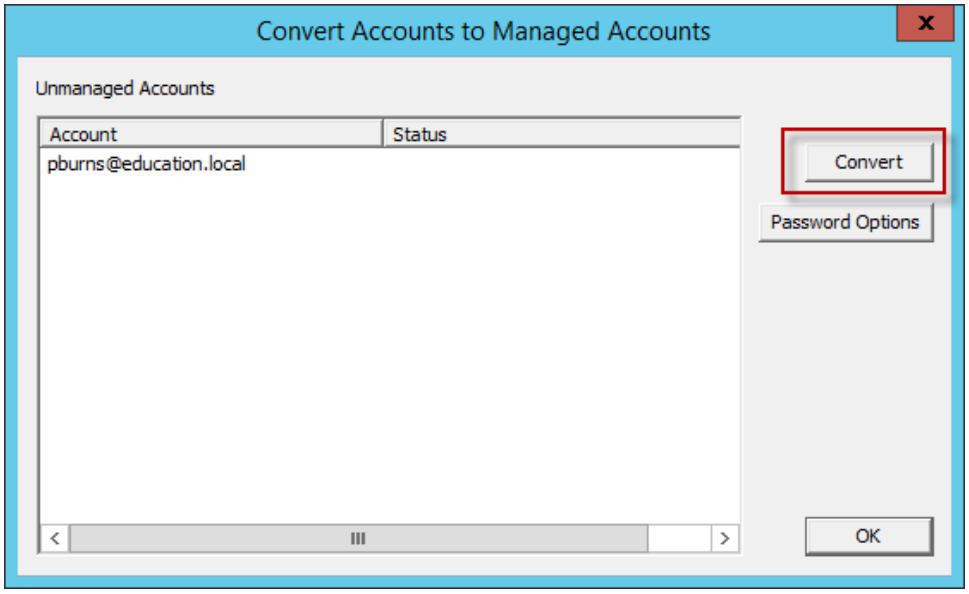


Manage Active Directory Accounts

Open the **Manage Active Directory Accounts** window by selecting ***Manage > Manage Accounts***.

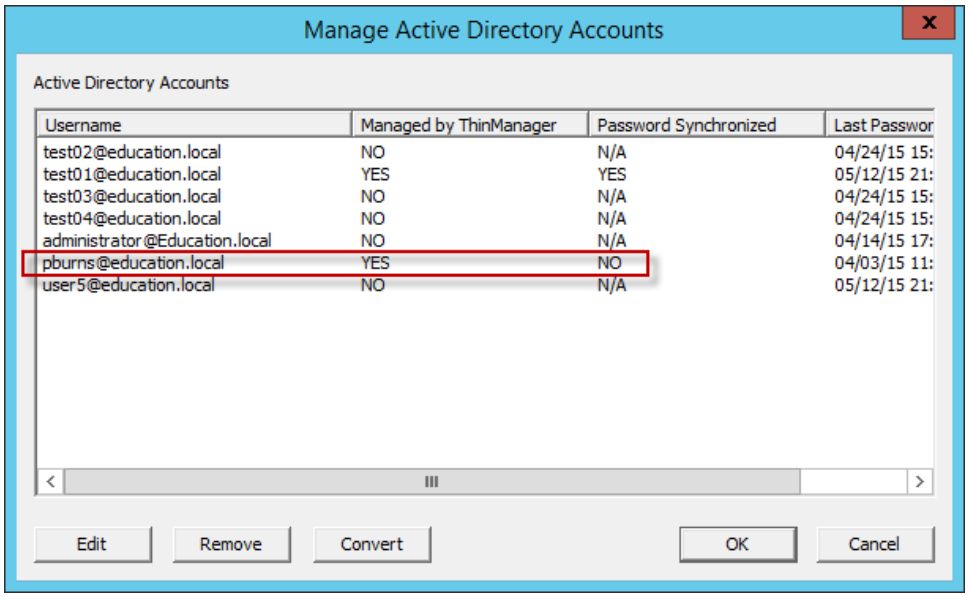
Highlight the legacy account and select the ***Convert*** button.

This will launch the **Convert Accounts to Managed Accounts** window.



Convert Accounts to Managed Accounts Window

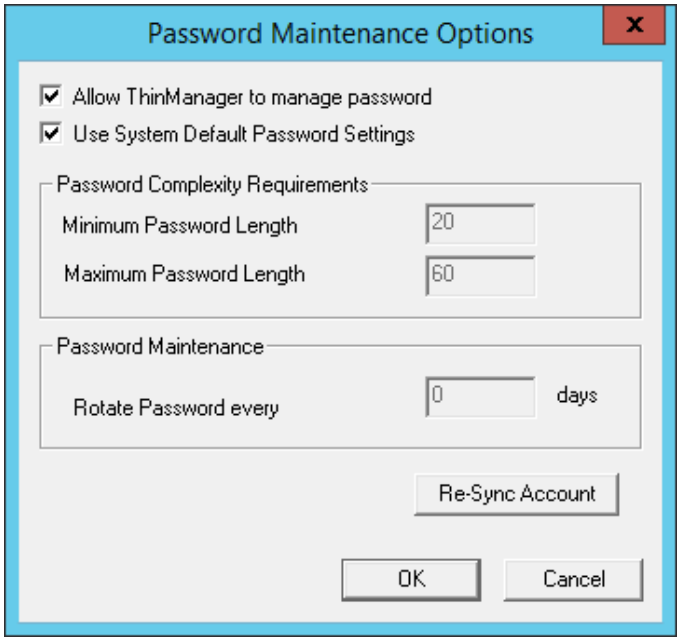
Highlight the legacy account and select the **Convert** button.



Manage Active Directory Accounts Window

The Manage Active Directory Accounts Window will show that the account is now managed by ThinManager.

Double click on a legacy domain account to launch the **Password Maintenance Options** window for that account.



Password Maintenance Options Window

Once the ***Allow ThinManager to manage password*** checkbox is checked you can use the system defaults or uncheck the ***Use System Default Password Settings*** to customize the password settings.

The password settings include

Password Complexity Requirements:

- ***Minimum Password Length*** – This is the minimum number of characters a password may have.

- ***Maximum Password Length*** – This is the maximum number of characters a password may have.

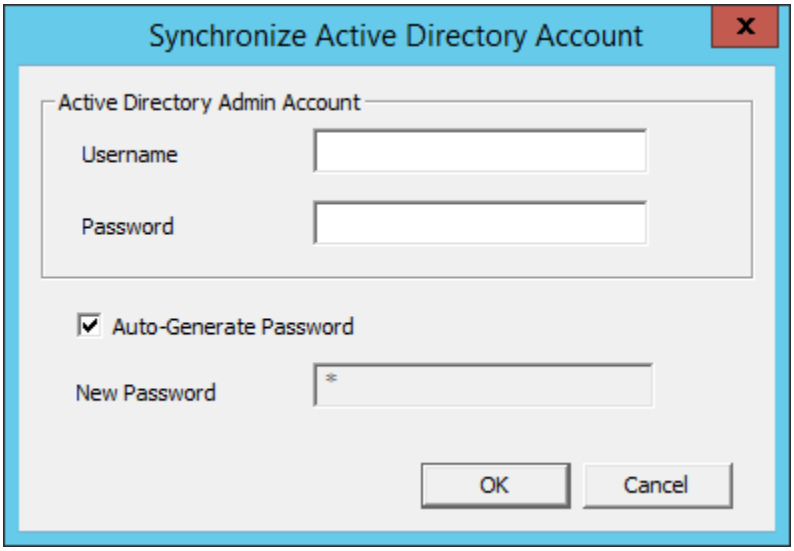
Password Maintenance:

- ***Rotate Password every*** – This is the number of days before the password must be changed.

***Re-synch Account* Button** – This will launch the **Synchronize Active Directory Account** window that allows you to re-synchronize the password in ThinManager with the password in the Active Directory.

Select the ***OK*** button to accept the changes or select the ***Cancel*** button to close the dialog without saving.

Selecting the ***Re-synch Account*** button will launch the **Synchronize Active Directory Account** window.



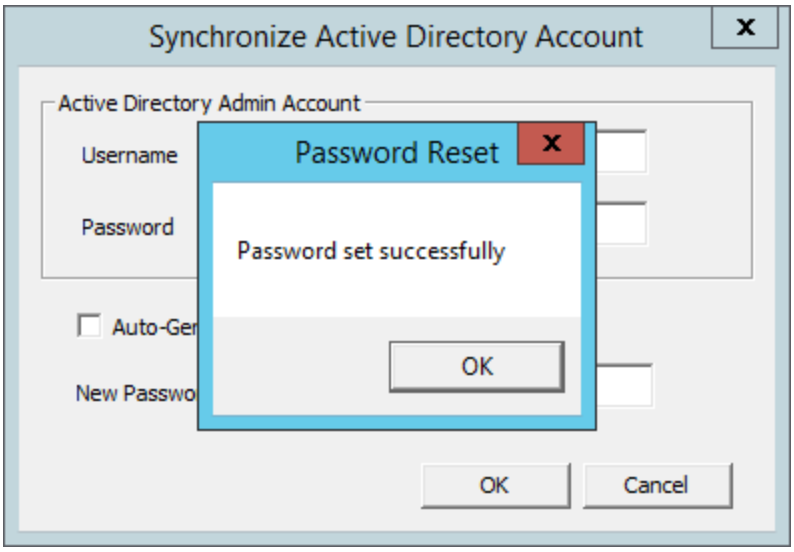
Synchronize Active Directory Account

Synchronizing the Active Directory account requires a Domain Administrator password. Enter domain admin credentials.

You can have the ThinManager program automatically create a password by checking the Auto-Generate Password checkbox.

You can create a password of your choosing by un-checking the Auto-Generate Password checkbox and entering the password in the New Password field.

Select the ***OK*** button to synchronize the password or select the ***Cancel*** button to close the dialog without saving.

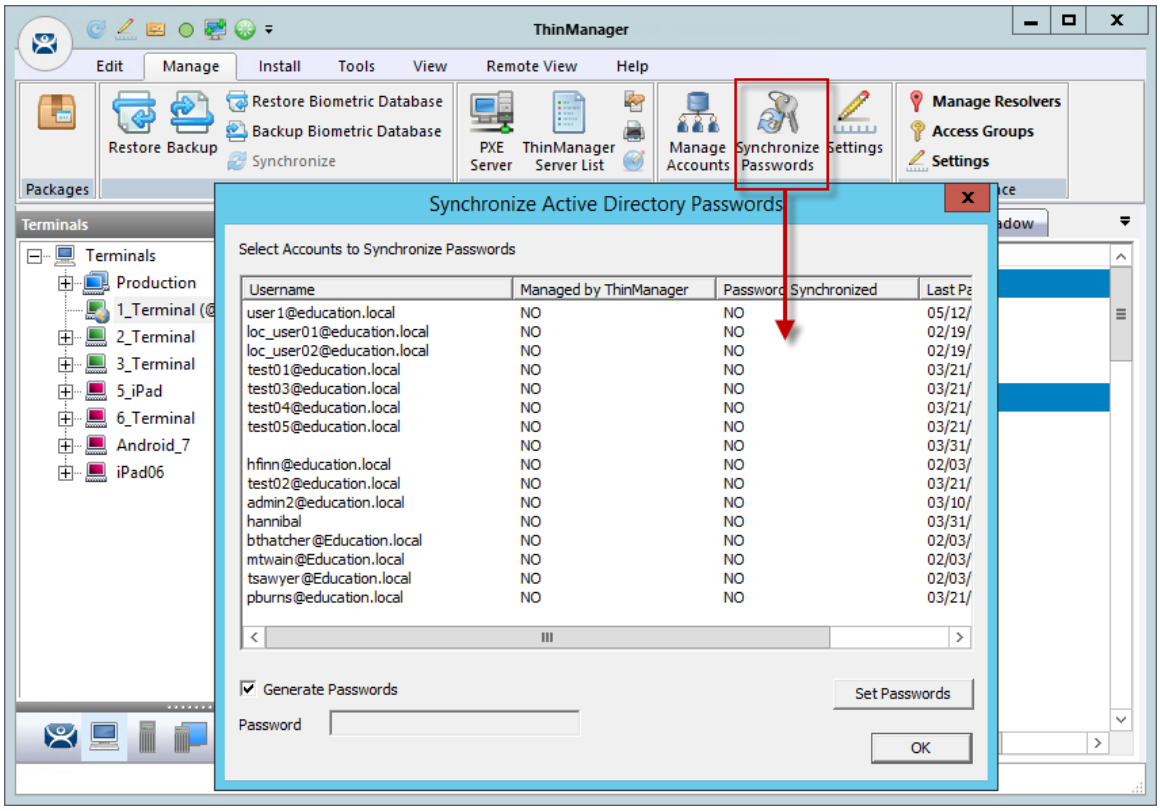


Password Reset Dialog

A dialog box will acknowledge a successful synchronization.

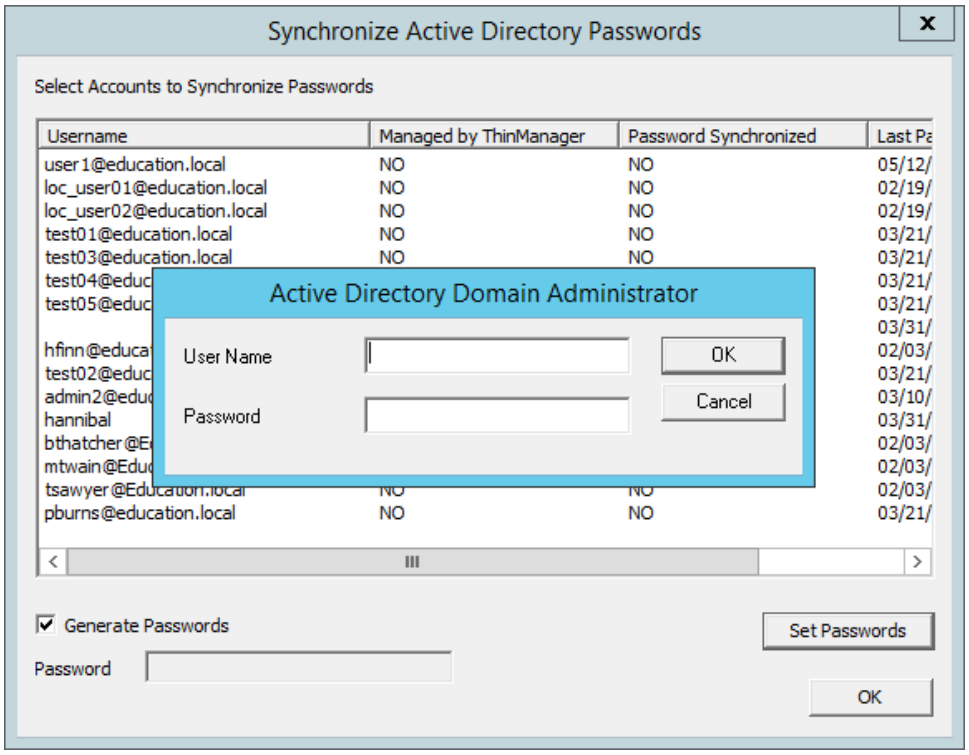
34.3. Active Directory - Synchronize Password

Selecting ***Manage > Synchronize Passwords*** will launch the **Synchronize Active Directory Passwords** window.



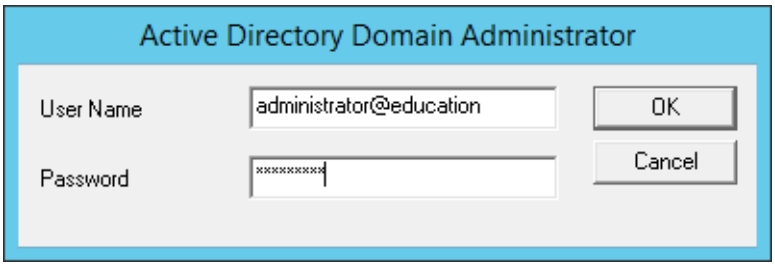
Synchronize Active Directory Passwords Window

This allows the synchronization of passwords for many accounts at once.



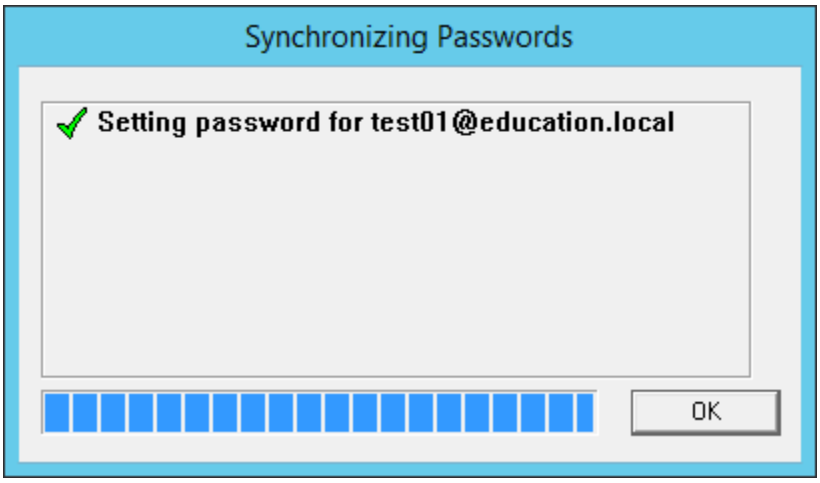
Active Directory Domain Administrator Log In Window

This action requires a Domain Administrator account.



Active Directory Domain Administrator Log In Window

Enter the credentials in the appropriate fields.

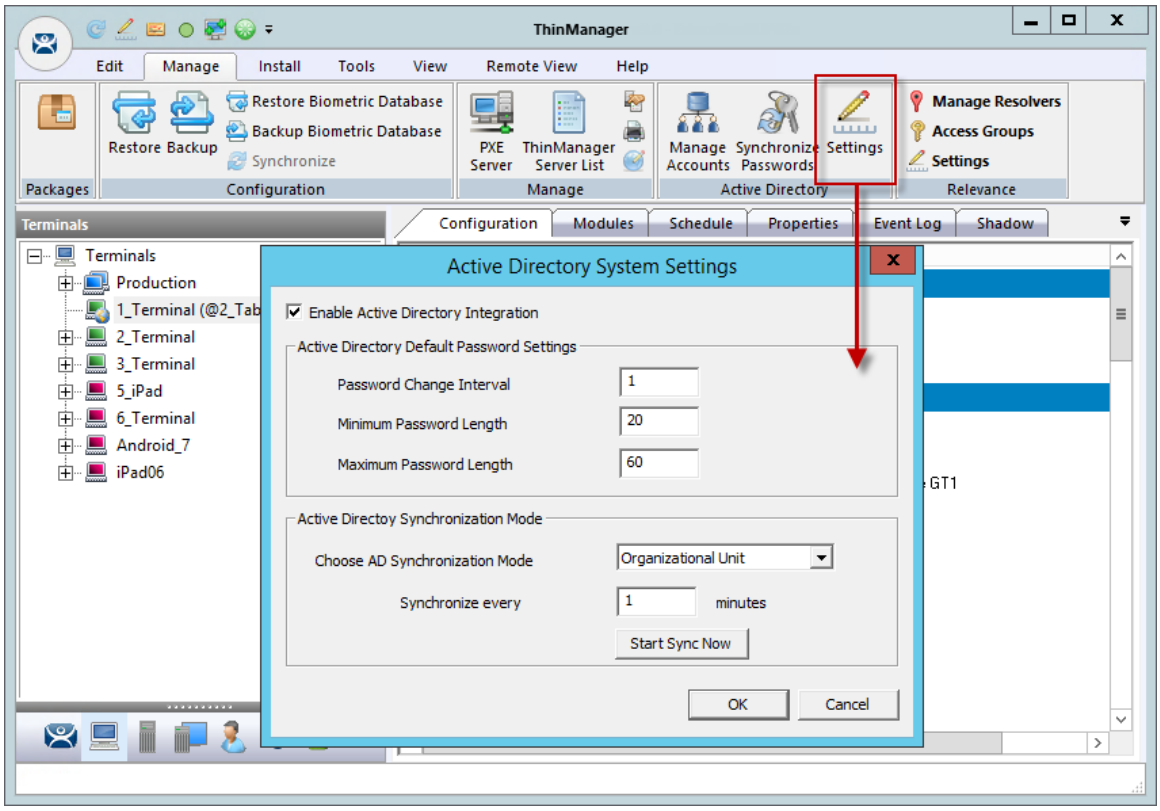


Synchronizing Passwords Window

The selected accounts will have their passwords synchronized between ThinManager and the Active Directory.

34.4. Active Directory - Settings

Selecting ***Manage > Settings (Active Directory)*** will launch the **Active Directory System Settings** window.



Active Directory System Settings

The Settings (Active Directory) button launches the Active Directory System Settings window. This has the settings for the passwords. They include:

Active Directory Default Password Settings

- ***Password Change Interval*** – This is the number of days before the password must be changed.
- ***Minimum Password Length*** – This is the minimum number of characters a password may have.
- ***Maximum Password Length*** – This is the maximum number of characters a password may have.

Active Directory Synchronization Mode

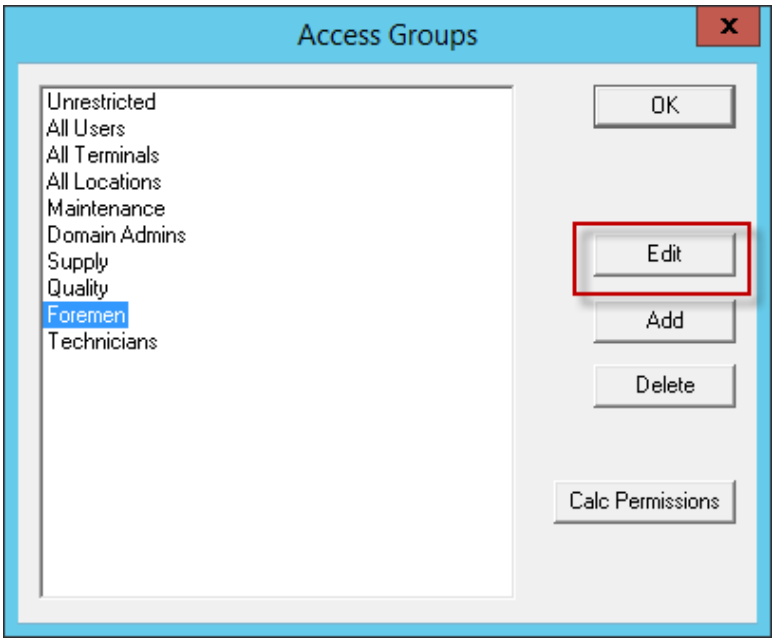
- ***Choose AD Synchronization Mode*** – This is used when batch creating TermSecure Users. You may generate users from one Windows Security Group or multiple Organizational Units.
- ***Synchronize every X Minutes*** – This is how often that ThinManager will synchronize with the Active Directory. Password communication is encrypted for security.
- ***Start Sync Now*** – This will manually start the synchronization between the ThinManager Server and the Active Directory.

34.5. Shortcut Method of Adding Relevance Access Groups

Members can be added to Relevance Access Groups quickly through the **Relevance Access Group Wizard**.

Open the Relevance Access Group Wizard by selecting ***Manage> Access Groups*** from the ThinManager menu.

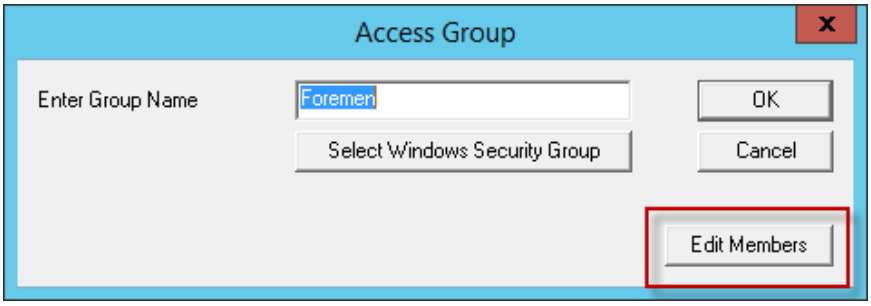
This will launch the **Access Groups** window.



Access Groups Window

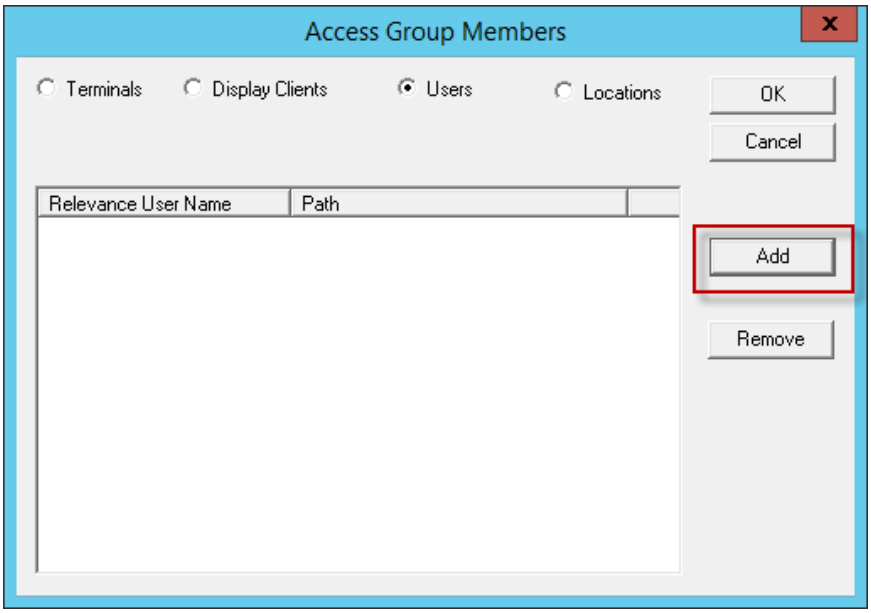
Relevance Access groups can be added, deleted, or edited by highlighting the access group and selecting the appropriate button.

Highlight the desired **Relevance Access Group** and select the ***Edit*** button.



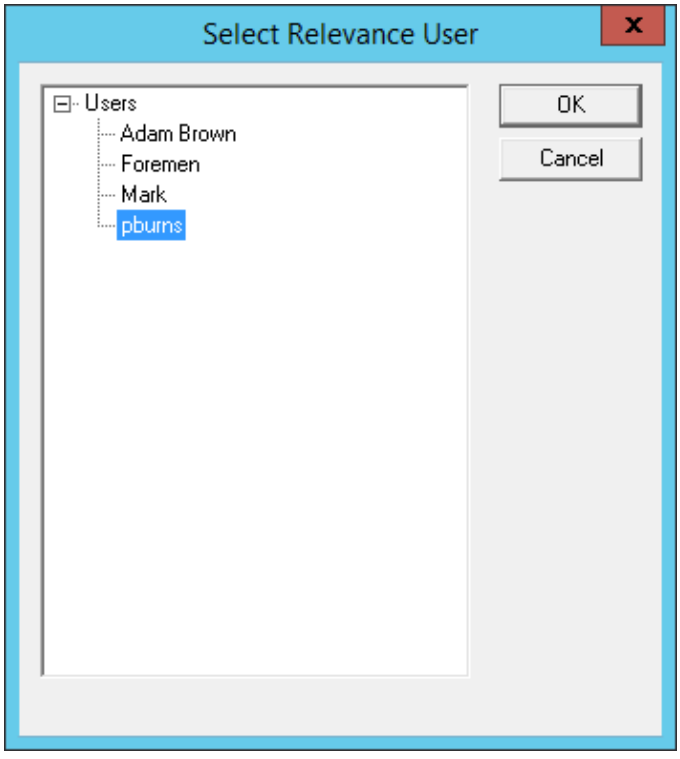
Access Group Window

Select the ***Edit Members*** button to launch the **Access Group Members** window.



Access Group Members Window

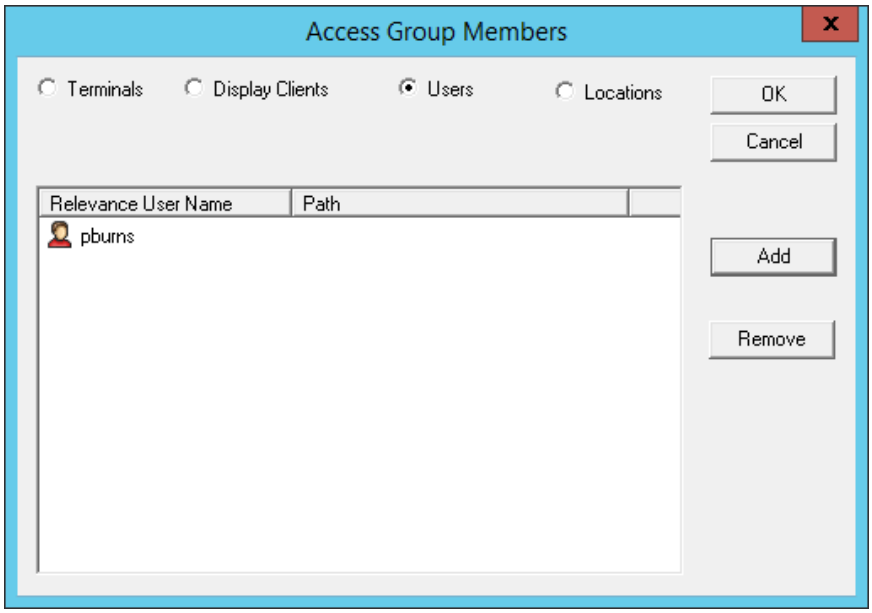
Select the **Terminals**, **Display Clients**, or **Relevance Users** radio button to configure that category and select the ***Add*** button.



Select Relevance User Window

A **Select** window will be displayed with a tree of the configured Terminals and Terminal groups.

Select the desired Relevance User and select ***OK*** for each addition.



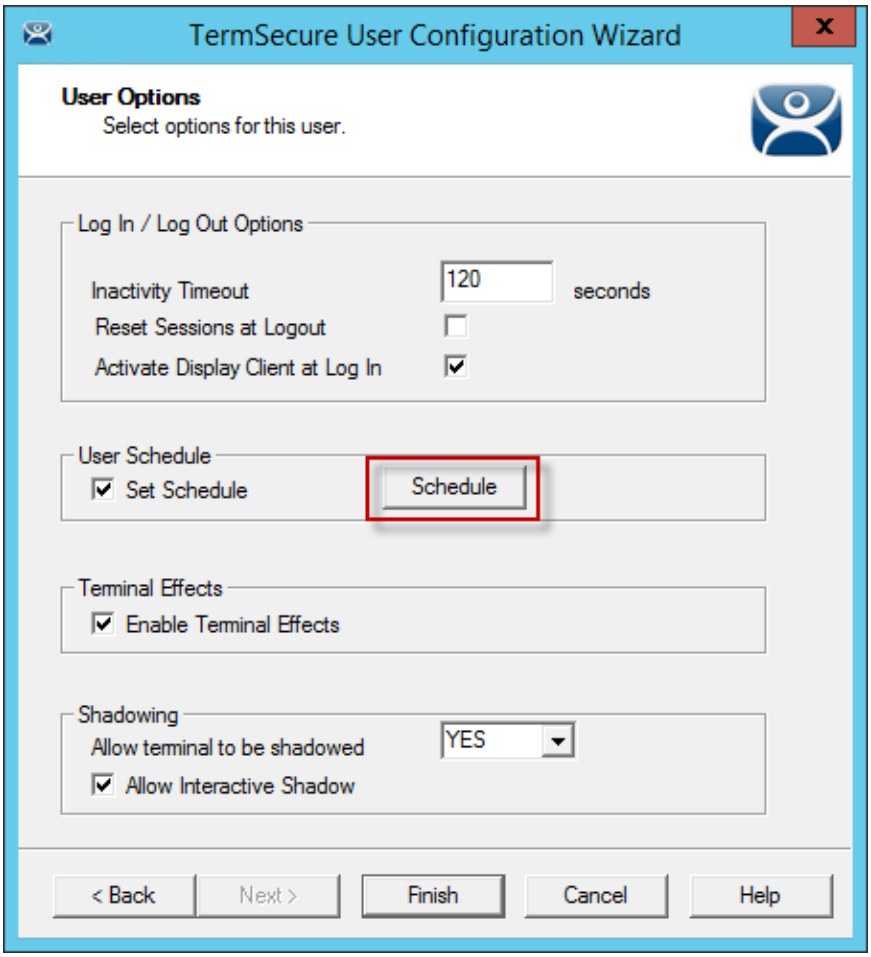
Access Group Members

The **Access Group Members** window will show the members of the **Relevance Access Group**. These can be removed by highlighting and selecting the ***Remove*** button.

Display Clients and Relevance Users can be added by the same process of adding.

34.6. Relevance User Schedule

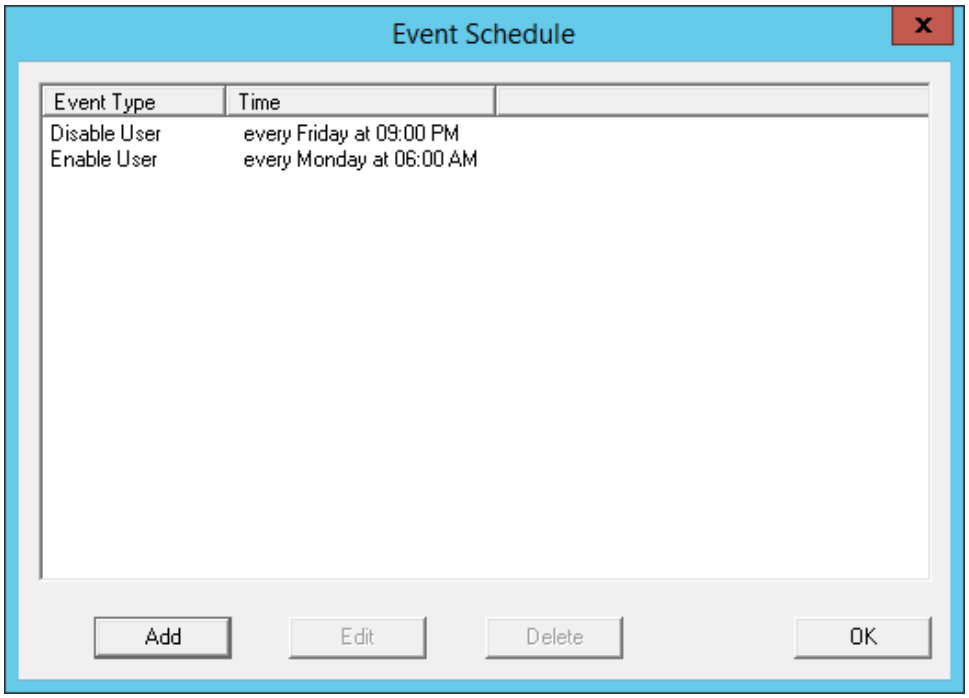
Relevance Users and Relevance User Groups have a schedule on the **User Options** page of the Relevance User Configuration Wizard.



Relevance User Terminal Configuration Wizard – User Options Page

Check the ***Set Schedule*** checkbox and select the ***Schedule*** button to launch the **Event Schedule** window.

Note: The Schedule for Relevance User Groups is the same as for individual Relevance Users. It has an advantage of applying the scheduled events to a whole group of users instead of requiring a configuration for each event on each user.

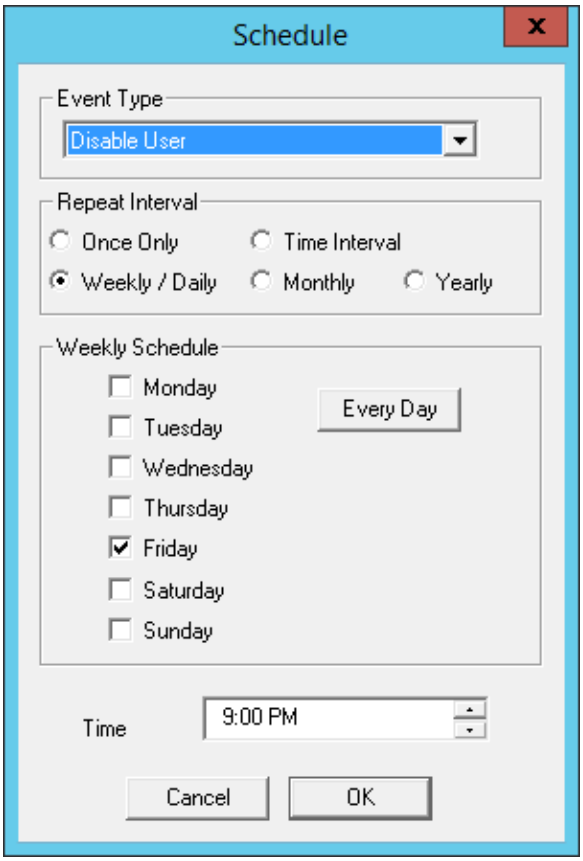


Event Schedule

The Event Schedule will list events for the Relevance User or Relevance User group. It has four buttons:

- The ***Add*** button will launch a **Schedule** window to allow an event to be configured.
- The ***Edit*** button will allow a highlighted event to be changed.
- The ***Delete*** button will remove a highlighted event.
- The ***OK*** button will accept changes and close the **Event Schedule** window.

Events can be added by selecting the ***Add*** button to launch the **Schedule** window.



Schedule Window

The **Schedule** window has several configuration settings.

Event Type is a drop-down box that allows event selection:

- ***Disable User*** - This will prevent a user from logging in through Relevance or will disconnect an existing session.
- ***Enable User*** - This will allow a user to become active again.

The **Repeat Interval** radio buttons allow the event in the **Event Type** drop-down to be run ***Once Only***, ***Weekly/Daily***, ***Monthly***, or ***Yearly***.

- Selecting ***Once Only*** will show a ***Select Date*** field for the event.
- Selecting ***Weekly/Daily*** will show a **Weekly Schedule** list for the event to run. The ***Every Day*** button will select all the days in the list.
- Selecting ***Monthly*** will show a ***Select Day of Month*** field for the event.
- Selecting ***Yearly*** will show a ***Select Date*** field for the event.
- The ***Time*** field allows the selection of the time that the event should occur.

Select the ***OK*** button to close the **Schedule** window.

Select ***Add*** to add another event to the **Event Schedule** or select ***OK*** to close the **Event Schedule** window and return to the Terminal configuration.

35. Card Readers and Fingerprint Scanners

35.1. Card and Badge Configuration for a Relevance User

ThinManager has the ability to use Prox (proximity) cards for Relevance logins. This requires:

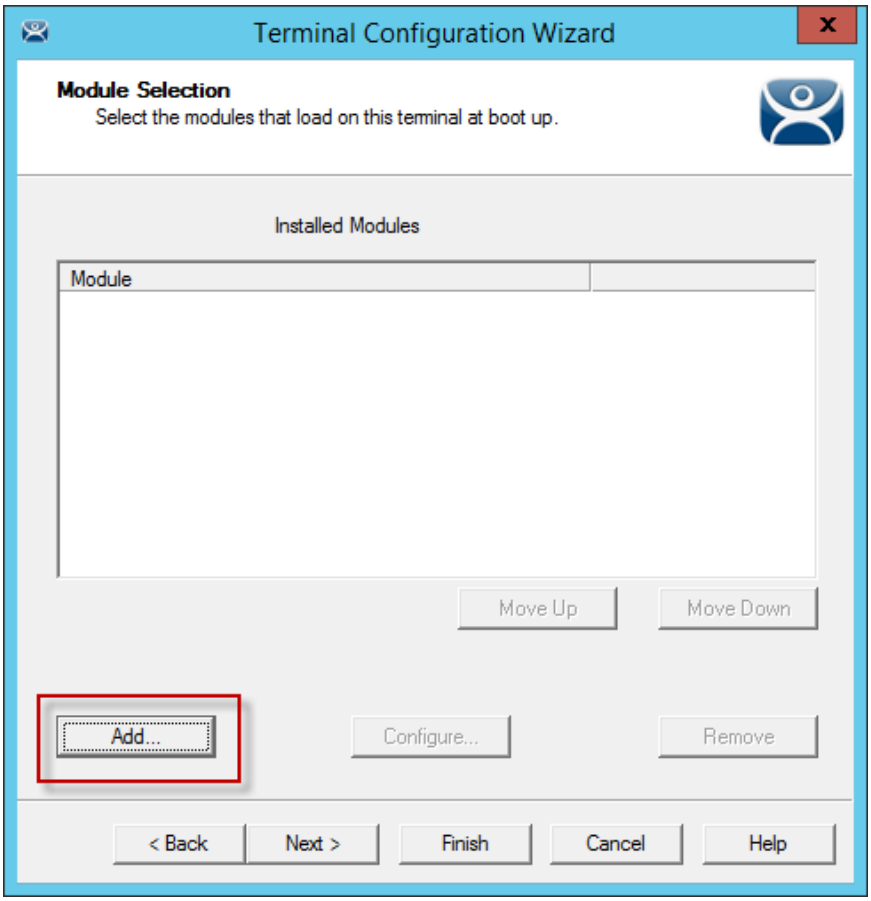
- Adding a card reader to the ThinManager Ready thin client
- Adding the card reader module to the Terminal configuration
- Associating the card number to the Relevance User configuration.

ThinManager has support for the **RF Ideas Inc.** serial **RDR-6081AK2** pcProx card reader and the **USB RDR-6081AKU** and **RDR-80582AK0** pcProx card reader (www.rfideas.com).

35.1.1. Configure a Terminal with the Card Reader Module

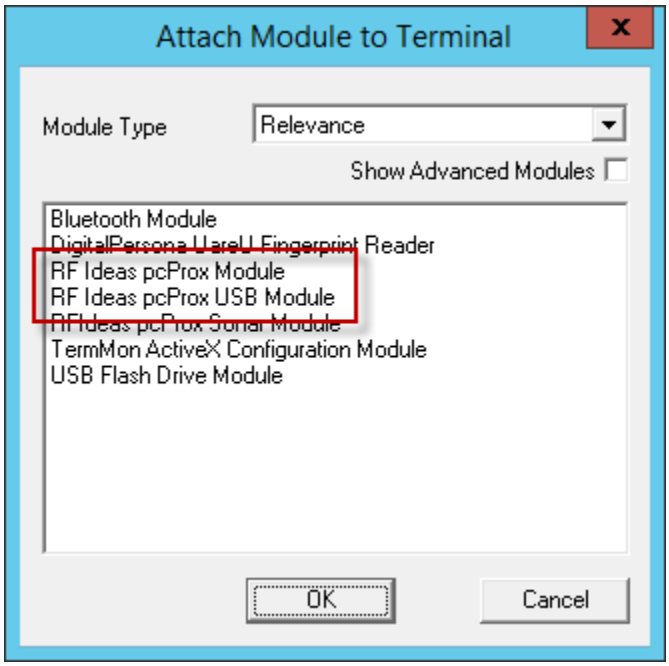
Open the **Terminal Configuration Wizard** by double clicking on the Terminal in the tree.

Navigate to the **Module Selection** page.



Module Selection Page

Select the ***Add*** button to launch the **Attach Module to Terminal** window.



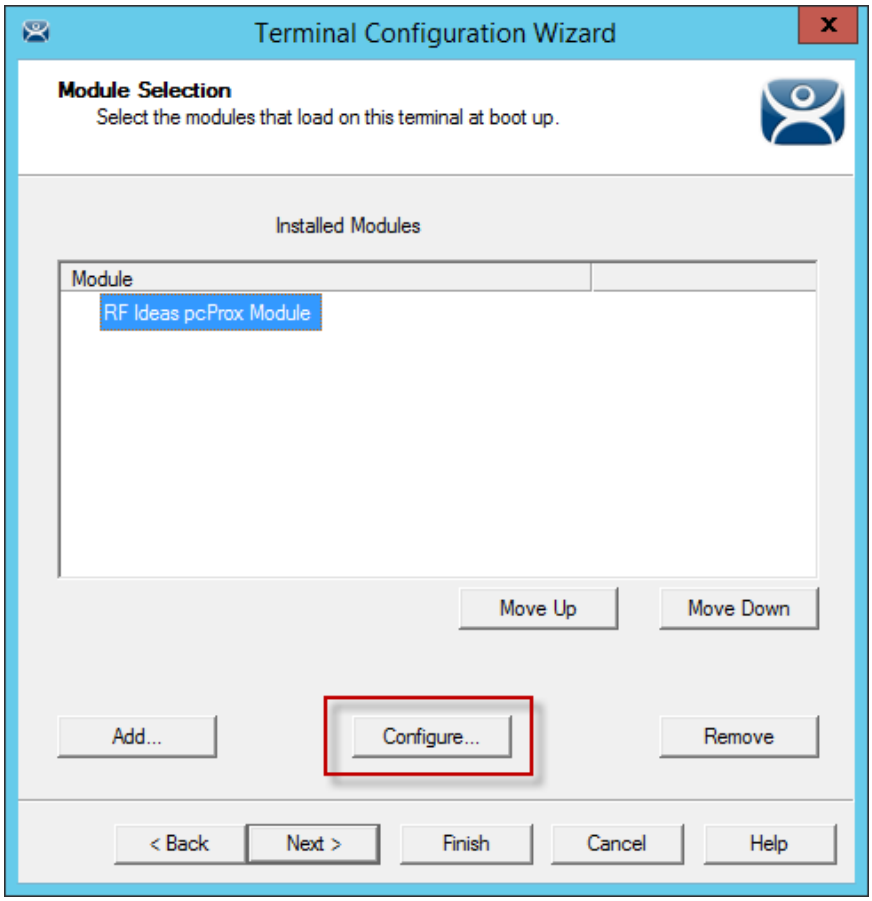
Attach Module to Terminal Window

Select **Relevance** in the ***Module Type*** drop-down.

Highlight a **RF Ideas pcProx Module** and select the ***OK*** button.

- Use the **RF Ideas pcProx Module** for serial devices.
- Use the **RF Ideas pcProx USB Module** for USB devices.

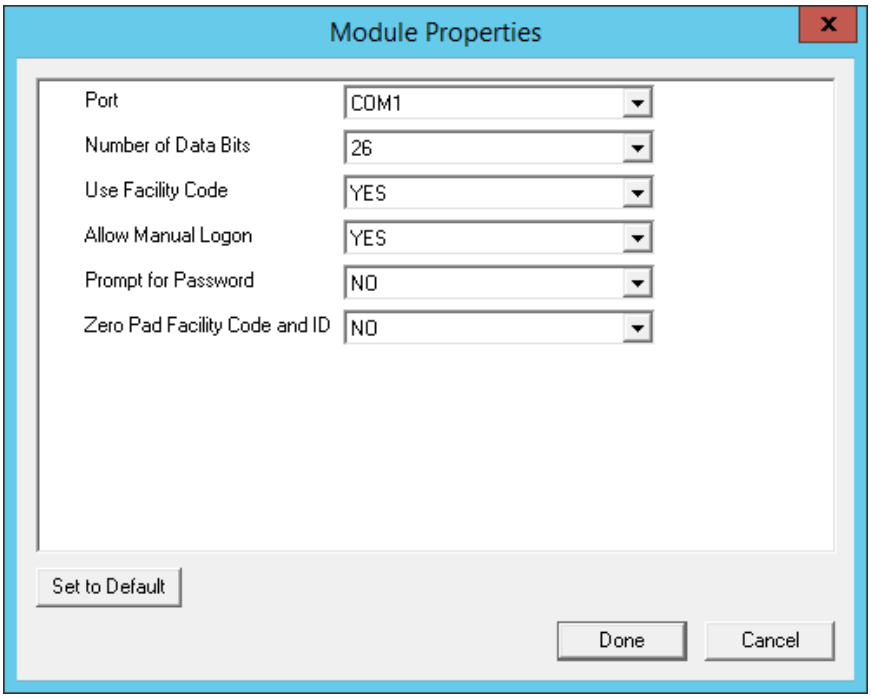
Select the ***OK*** button to attach the module to the Terminal.



Module Selection Window

The module can be configured once it is attached to a Terminal.

Highlight the **RF Ideas pcProx Module** and select the ***Configure*** button to launch the **Module Properties** window.

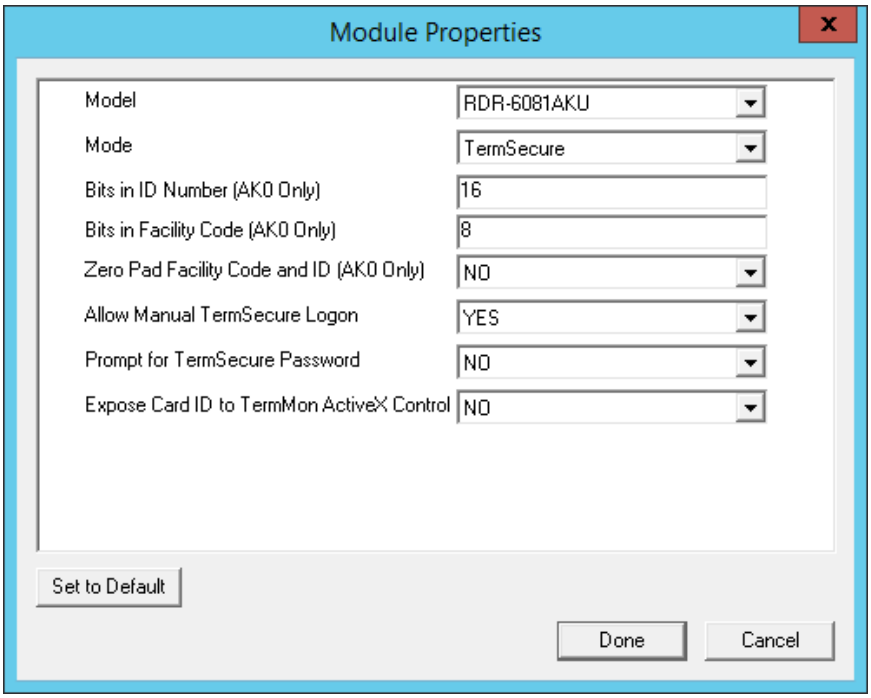


Serial pcProx Card Module Properties Window

The **RF Ideas Serial pcProx Module** has parameters that can be configured:

- **Port -** This selects the port that the serial RF Ideas pcProx card reader is installed.
- **Number of Data Bits –** Different cards use different numbers of data bits in their format. This sets the number of data bits to match that used by the card as an identifier. The choices are ***26***, ***37***, or ***Raw***.
- **Use Facility Code -** This value, when set to ***Yes***, will add the card's Facility Code to the Card / Badge ID number.
- **Allow Manual Login** - This, when set to ***Yes***, will allow a Relevance User to log into a Terminal without a TermSecure ID device. If set to ***No***, TermSecure users must use a TermSecure ID device to log in.
- **Prompt for Password** - This, when set to ***Yes***, will require a TermSecure to enter their password for access, even if the password is configured in ThinManager.

Note: The **USB RDR-6081AKU** does not have the Facility Code option. Do not use the Facility code on serial pcProx card readers if you are using a mix of both **USB RDR-6081AKU** and **RDR-6081AK2** serial devices.



USB pcProx Card Module Properties Window

The **RF Ideas USB pcProx Module** has parameters that can be configured:

- **Model -** This allows you to select between different USB pcProx card readers. These include:
  - **RDR-6081AKU**
  - **RDR-6011AKU**
  - **RDR-80582AK0**
  - **RDR-80082AK0**
- **Mode –** This allows you to select between **TermSecure**, **Wedge**, and **TermMon** modes.
  - **TermSecure Mode** – This allows the card to be used with TermSecure as a login device.
  - **Wedge Mode** – This allows the data to be sent to the session as a character string.
  - **TermMon Mode** – This allows the data to be sent to the TermMon ActiveX.
- **Bits in ID Number (AK0 Only) –** Different cards use different numbers of data bits in their format. This sets the number of data bits to match that used by the card as an identifier.
- **Bits in Facility Code (AK0 Only) -** Different cards use different numbers of data bits in their format. This sets the number of data bits of the Facility Code.
- **Zero Pad Facility Code and ID (AK0 Only) –** This adds a leading 0 to the Facility Code if needed.
- **Allow Manual TermSecure Login** - This, when set to ***Yes***, will allow a Relevance User to log into a Terminal without a TermSecure ID device. If set to ***No***, TermSecure users must use a TermSecure ID device to log in.
- **Prompt for TermSecure Password** - This, when set to ***Yes***, will require a TermSecure to enter their password for access, even if the password is configured in ThinManager.
- **Expose Card ID to TermMon ActiveX Control –** Allows the card data to be sent to the TermMon ActiveX without incorporating TermSecure.

To configure a parameter:

- Highlight the parameter.
- Change the ***value***.
- Select ***Done*** to accept the changes.

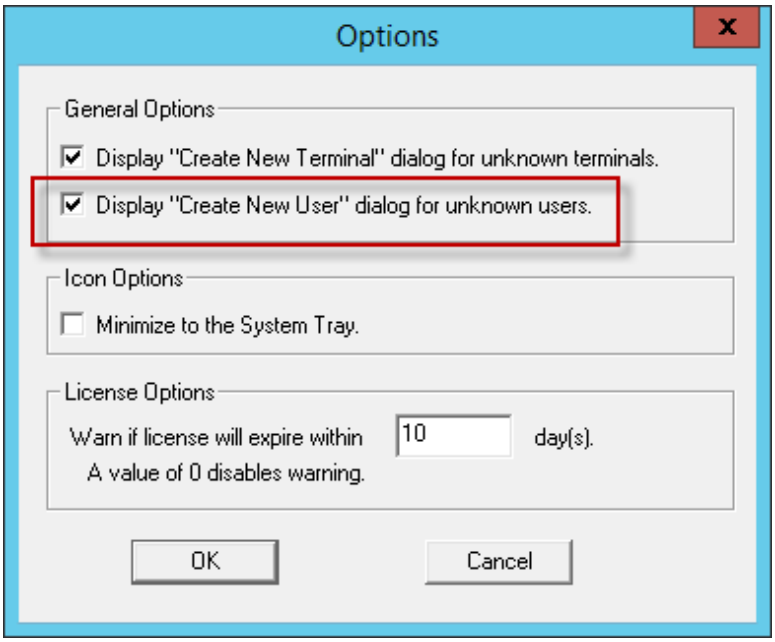
Once the Terminal has the module added it will need to restart to apply the changes.
Select the *Finish* button to close the Terminal Configuration Wizard.

Right click on the Terminal in the ThinManager tree and select *Restart*.

35.1.2. Configure ThinManager for Automatic User Configuration

A card reader can be used to associate cards with TermSecure Users using wizards.

Select ***View > Options*** from the ThinManager menu to open the **Options** window.



Options Window

Select the ***Display "Create New User" dialog for unknown users*** check box.

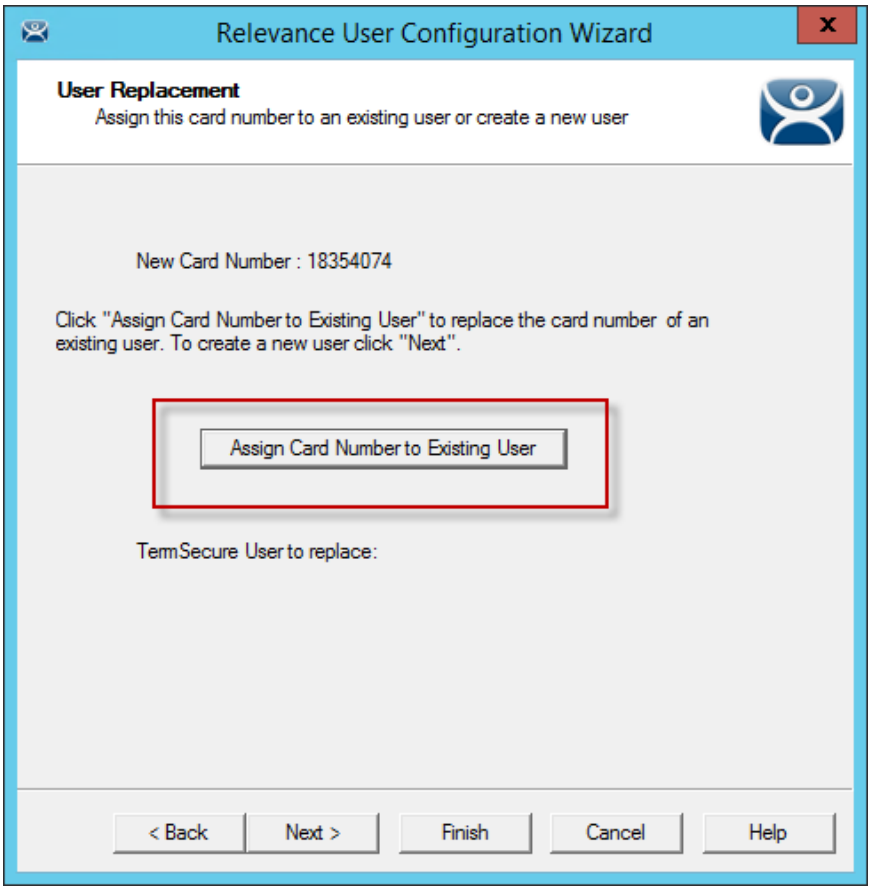
Select the ***OK*** button to accept the change.

The ***Display "Create New User" dialog for unknown users*** check box will launch the **Relevance User Configuration Wizard** on the ThinManager Server when an unknown ID device (USB key or ID card) is read by a Terminal. Once this checkbox is selected, scanning a new ID card or inserting an undefined USB key will launch the **Relevance User Configuration Wizard** with the ***Enter Card/Badge ID number*** automatically filled in.

35.1.3. Automatically Applying the Card to a Configuration

Scanning a card on a Terminal it can be used to associate cards with Relevance once ThinManager has the ***Display "Create New User" dialog for unknown users*** checkbox selected

Pass an HID card over the card reader on the Terminal to launch the **Relevance User Configuration Wizard**.

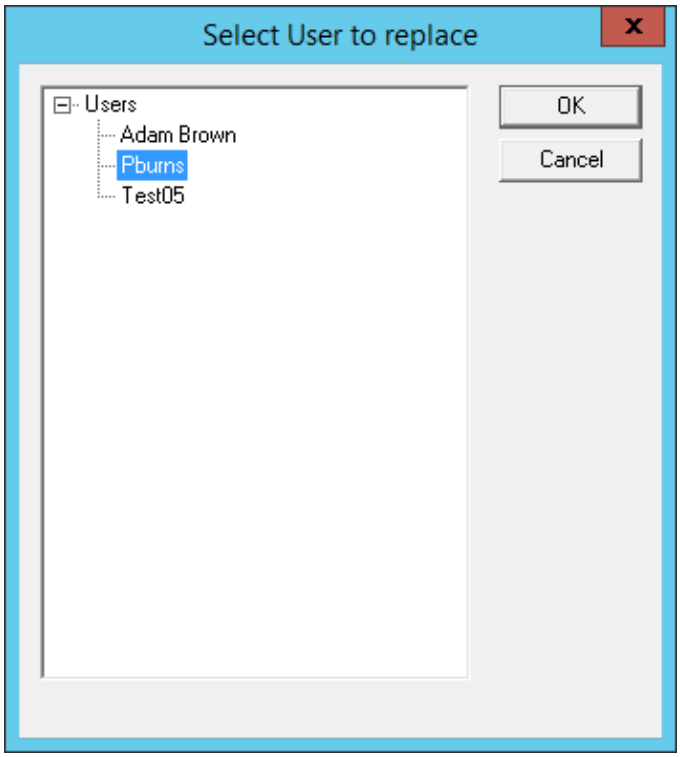


Card / Badge Information Page

Once the card reader has scanned an unknown Prox card a **Relevance User Configuration Wizard** will be launched associated with the new card number.

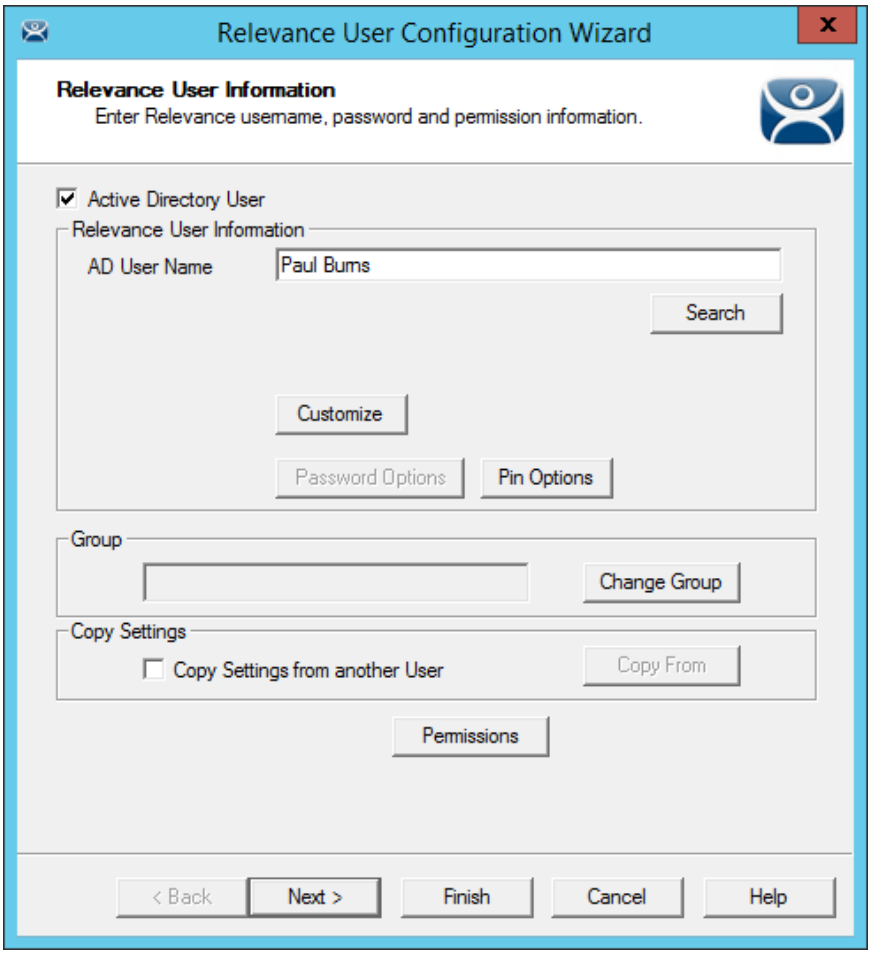
Select the ***Assign Card Number to Existing User*** button to launch the **Relevance User Replacement page**.

If you want to create a new Relevance User for this card instead of associating it with a pre-created TermSecure User, then select the ***Next*** button to navigate to the **Relevance User Configuration Wizard**.



User Replacement Page

The **User Replacement Page** allows you to select an existing Relevance User to associate the card. Select a Relevance User from the tree and select the ***OK*** button.

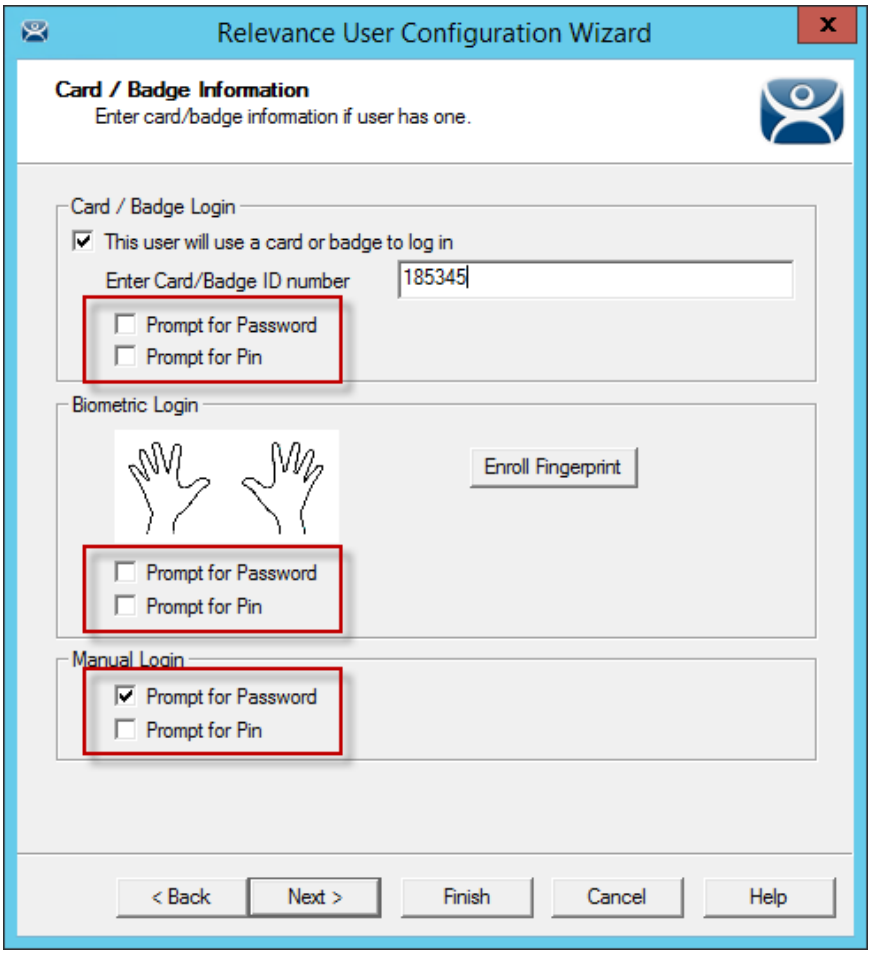


Relevance User Configuration Wizard

The **Relevance User Configuration Wizard** for the selected user will be displayed.

The ***Password*** and ***Permissions*** can be modified at this time if it isn't an Active Directory user.

Select ***Next*** to continue to the **Card/Badge Information** page.



Card/Badge Information Page

The **Card/Badge Information** page will now have the ***This user will use a card or badge to login*** checkbox selected. The serial number of the HID card will be entered in the ***Enter Card/Badge ID number*** field.

A secondary credential can be required by selecting ***Prompt for Password*** or ***Prompt for Pin*** for the **Card/Badge Login**, the **Biometric Login**, or a **Manual Login**.

- ***Prompt for Password*** – This checkbox, is selected, will require the user to enter their password.
- ***Prompt for Pin*** – This checkbox, is selected, will require the user to enter their PIN.

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

The card can now be used to login at Terminals configured with card readers.

35.1.4. Manually Applying the Card to a Configuration

Although the easiest method for assigning a card or badge is automatic as described in the previous section, ThinManager can be configured for manual entry.

If the ***Display "Create New User" dialog for unknown users*** check box on the Options window is unselected, the ***Enter Card/Badge ID number*** field will need to be entered manually. The Card/Badge ID number is accessible in the event log. To configure a Terminal to allow a device one needs to:

- Turn the Relevance User Event Log on in the ThinManager Server Configuration Wizard.
- Have the appropriate hardware on the Terminal, either a USB or Serial ProxCard reader.
- Add the appropriate module.
- Use the device once to have the device's identifier entered to the event log.
- Open the Relevance User Configuration Wizard and enter the ID number to tie the Relevance User to the device.
- Login with the ID device.

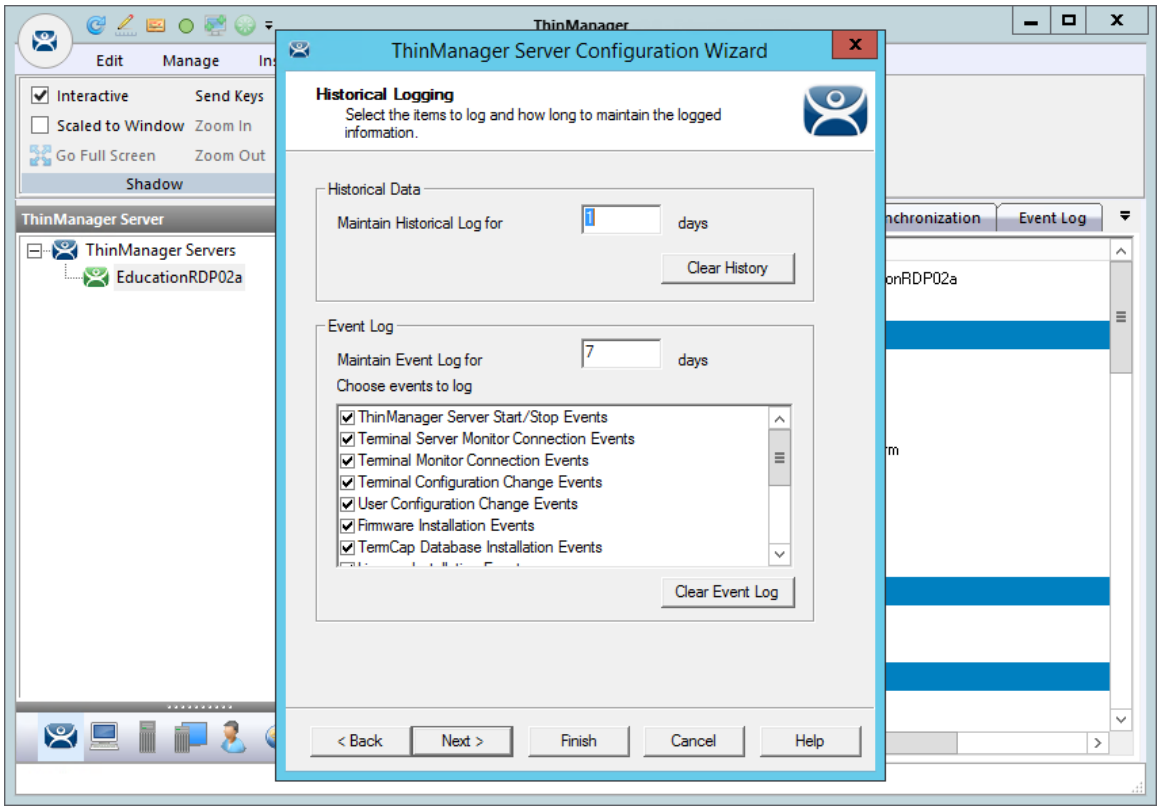
35.1.5. Event Log

The Event Log is configured in the ThinManager Server Configuration Wizard.

Go to the **ThinManager Server** branch of the ThinManager tree by selecting the ThinManager Server icon.

Open the **ThinManager Server Configuration Wizard** by double clicking on the ThinManager Server icon, or by selecting ***Edit > Modify*** from the menu.

Navigate to the **Historical Logging** page.



Historical Logging Page

All events may be selected to be logged, but the ***Relevance User Configuration changes*** checkbox is critical to the TermSecure Device detection.

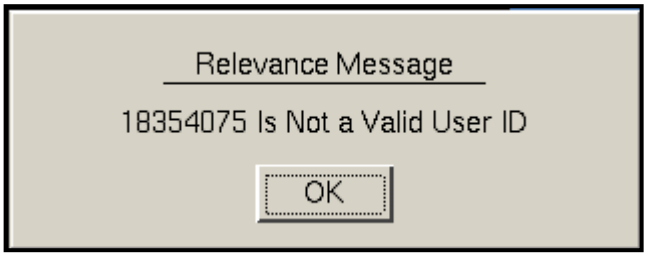
Select the ***Relevance User Configuration changes*** checkbox and select the ***Finish*** button.

35.1.6. Device Identifier Number

Next the HID card needs to be scanned to help find the ID number.

Pass the HID card over the pcProx Card scanner attached to a Terminal.

A TermSecure message should be displayed.



TermSecure Message

The ID device will not work so the Terminal will send a message with the ID device's identifier number.

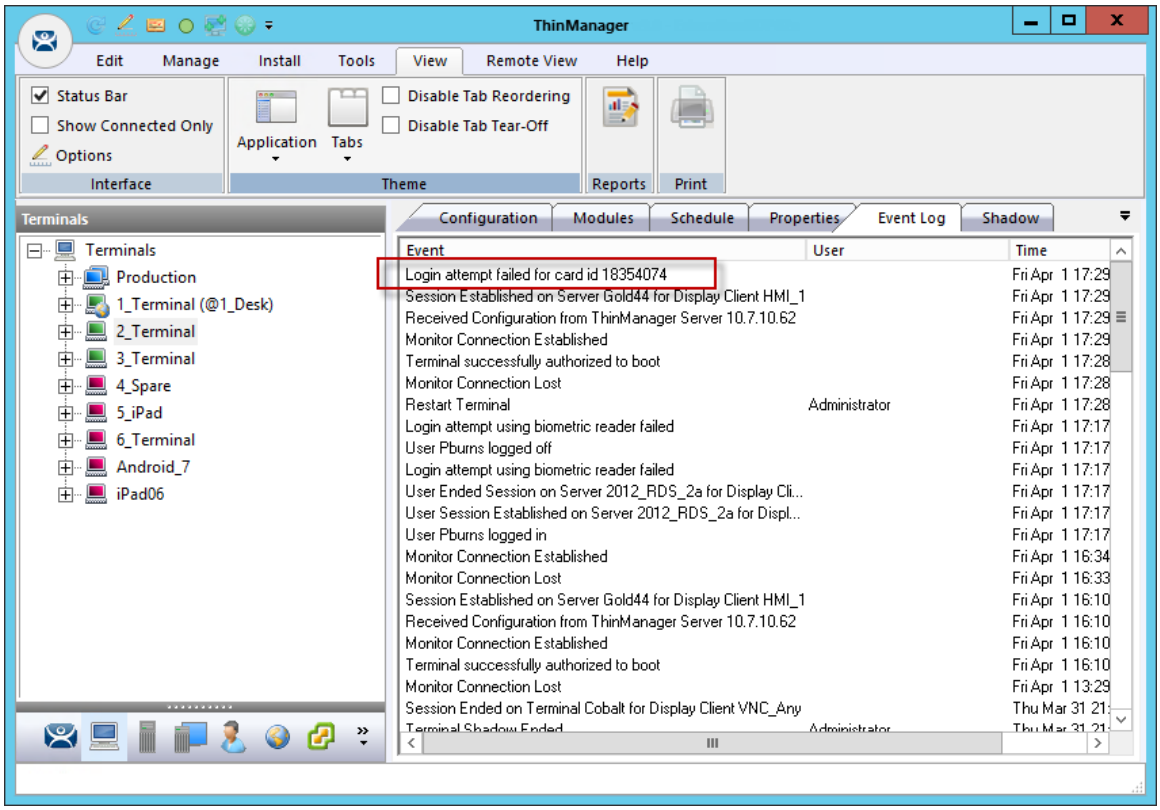
Record the number displayed.

This number is also entered in the event log if the Terminal Events were selected in the ThinManager Server Configuration Wizard.

Open ThinManager.

Highlight the Terminal in the tree and select the Event Log tab.

The ID for the device is entered in the log.

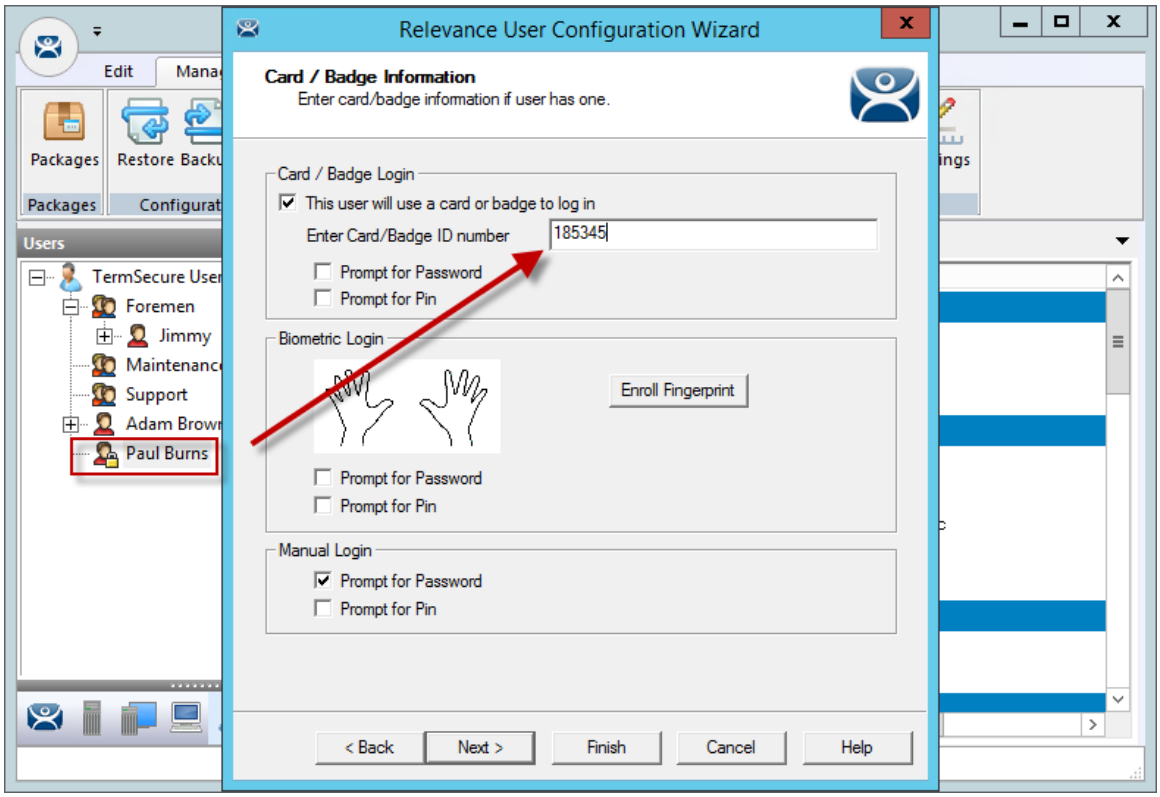


ThinManager Event Log

Next the ID number needs to be associated with the Relevance User.

Open the **Relevance User Configuration Wizard** for the user you want to associate with that ID card.

Navigate to the **Card / Badge Information** page.



Card / Badge Information Page

Select the ***This user will use a card, badge, or other device to log in*** checkbox.

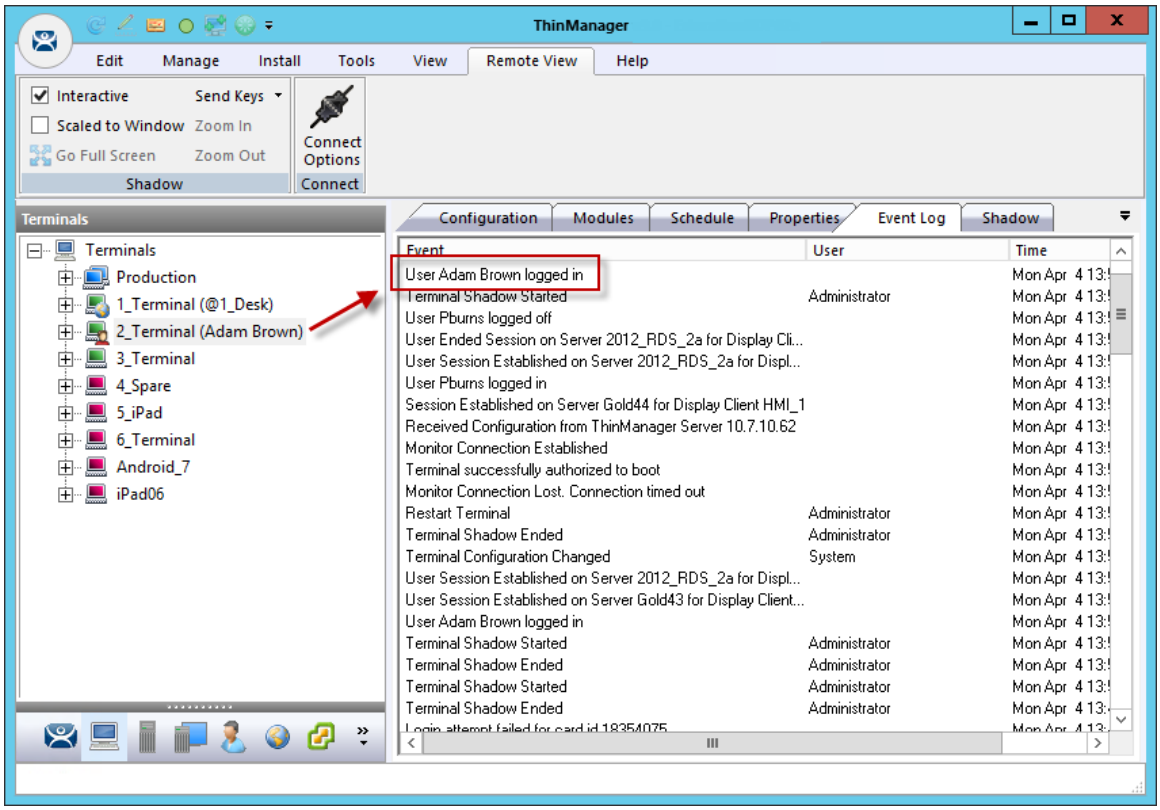
Enter the ID Identifier from the earlier steps into the ***Enter Card/Badge ID number*** field.

A secondary credential can be required by selecting ***Prompt for Password*** or ***Prompt for Pin*** for the **Card/Badge Login**, the **Biometric Login**, or a **Manual Login**.

- ***Prompt for Password*** – This checkbox, is selected, will require the user to enter their password.
- ***Prompt for Pin*** – This checkbox, is selected, will require the user to enter their PIN.

Now the Terminal is configured, the ID device is identified, and the Relevance User is configured to use the device.

Select the ***Finish*** button to complete the configuration.



Event Log

Rescan the card now that is associated with a Relevance User account.

The Event Log will show the results of the successful login. The Terminal will have the Relevance User added to its icon in the tree, while the Relevance User icon will show the name of the Terminal that it is logged into.

35.2. Fingerprint Reader

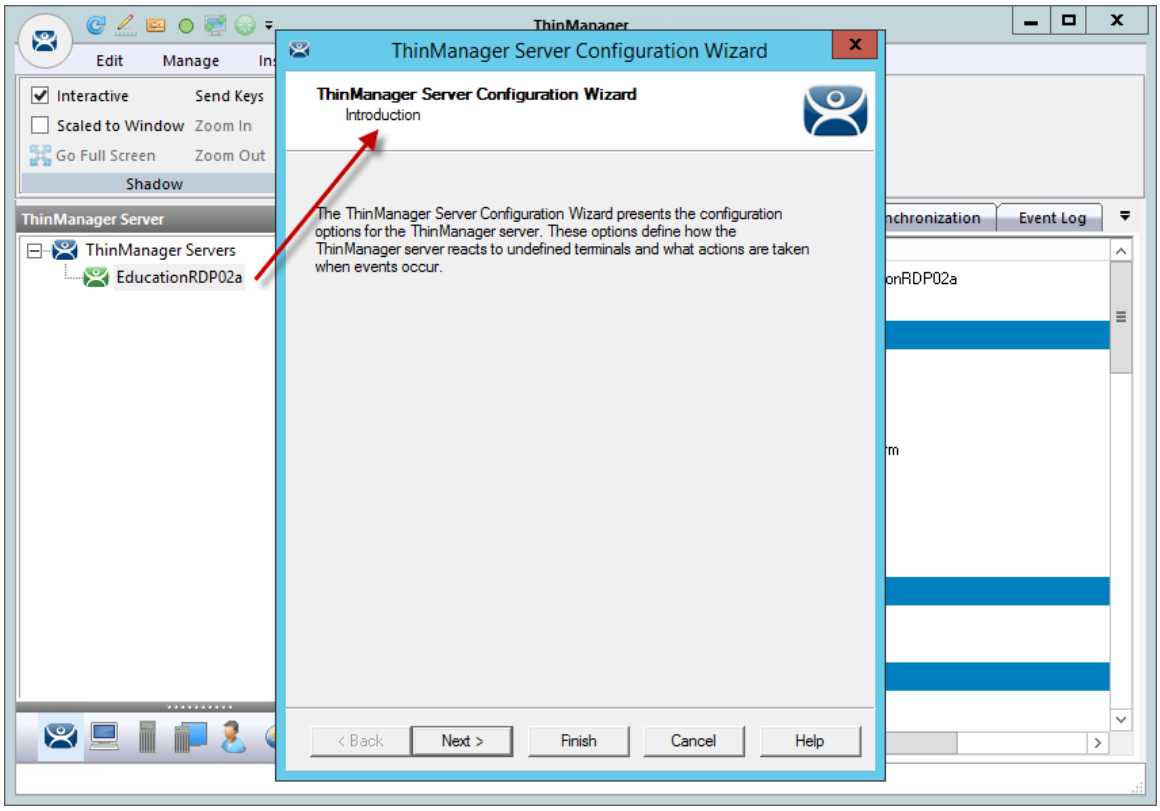
ThinManager supports the DigitalPersona UareU model 4500 and 5160 fingerprint readers as biometric readers. These can be used as an identifier for TermSecure.

The DigitalPersona UareU model 4500 fingerprint scanner requires:

- Activation in the ThinManager Server Configuration Wizard.
- The unit plugged into a Terminal and the DigitalPersona UareU Fingerprint Reader module added to the Terminal.
- The user fingerprint scanned in TermSecure to associate a user with the fingerprints.

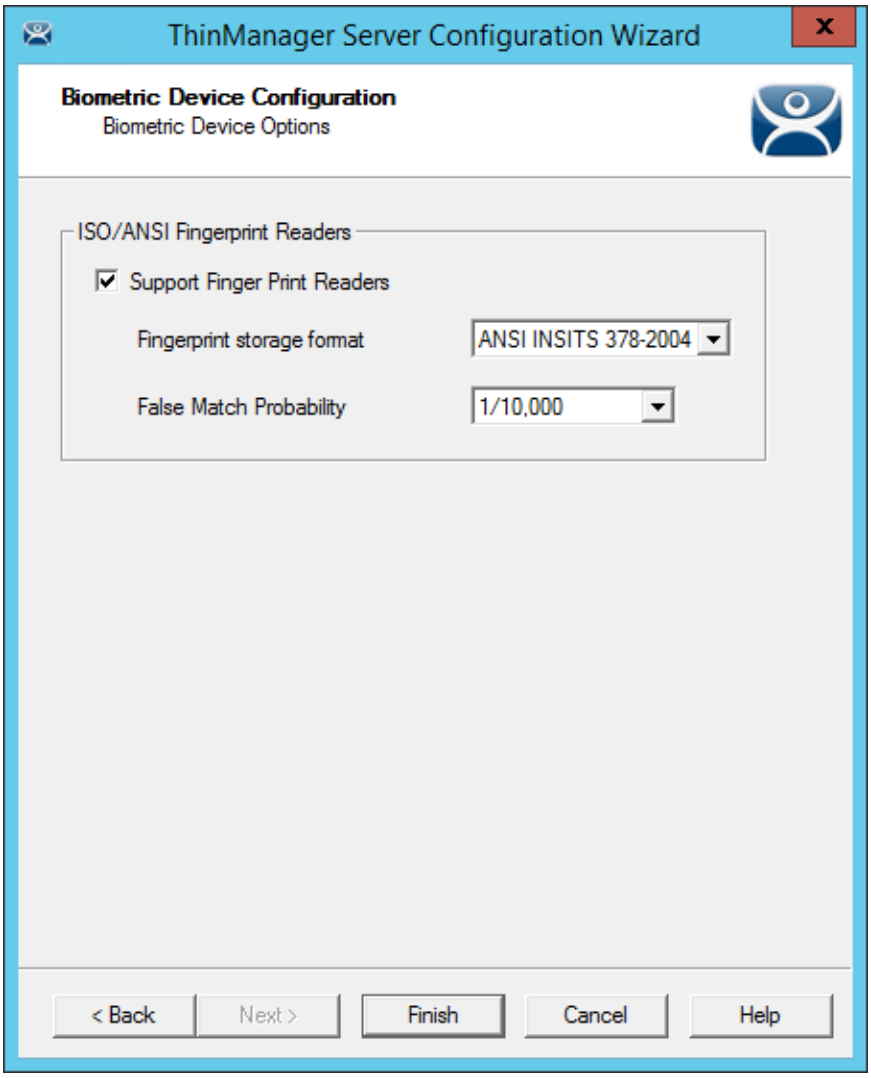
35.2.1. Fingerprint Reader in ThinManager

The DigitalPersona UareU fingerprint reader needs activated in the ThinManager Server Configuration Wizard.



ThinManager Server Configuration Wizard

Open the **ThinManager Server Configuration Wizard** by double clicking on the ThinManager Server icon in the ThinManager branch of the ThinManager Server tree.



Biometric Device Configuration Window

Navigate to the **Biometric Device Configuration** window.

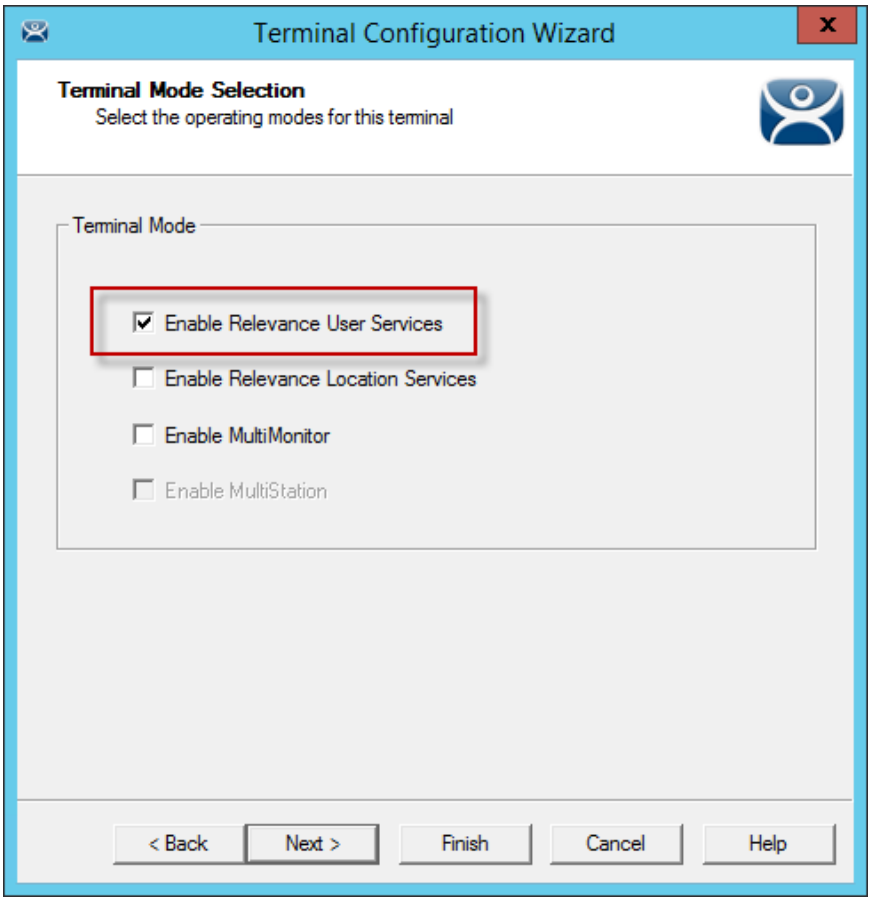
- ***Support Finger Print Readers*** - Select this checkbox to enable the use of readers.
- ***Fingerprint storage format*** - Select the data format you plan to use. There are two formats to choose:
    - **ISO IEC 19794_2_2005**
    - **ANSI INSITS 378_2004**.
- ***False Match Probability*** – This sets the sensitivity of the read. 1/100 is less sensitive than 1/1,000,000.

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

35.2.2. Fingerprint Reader on the Terminal

You need to add the **DigitalPersona UareU Fingerprint Module** to a Terminal if you plan on plugging a DigitalPersona UareU fingerprint reader into the Terminal.

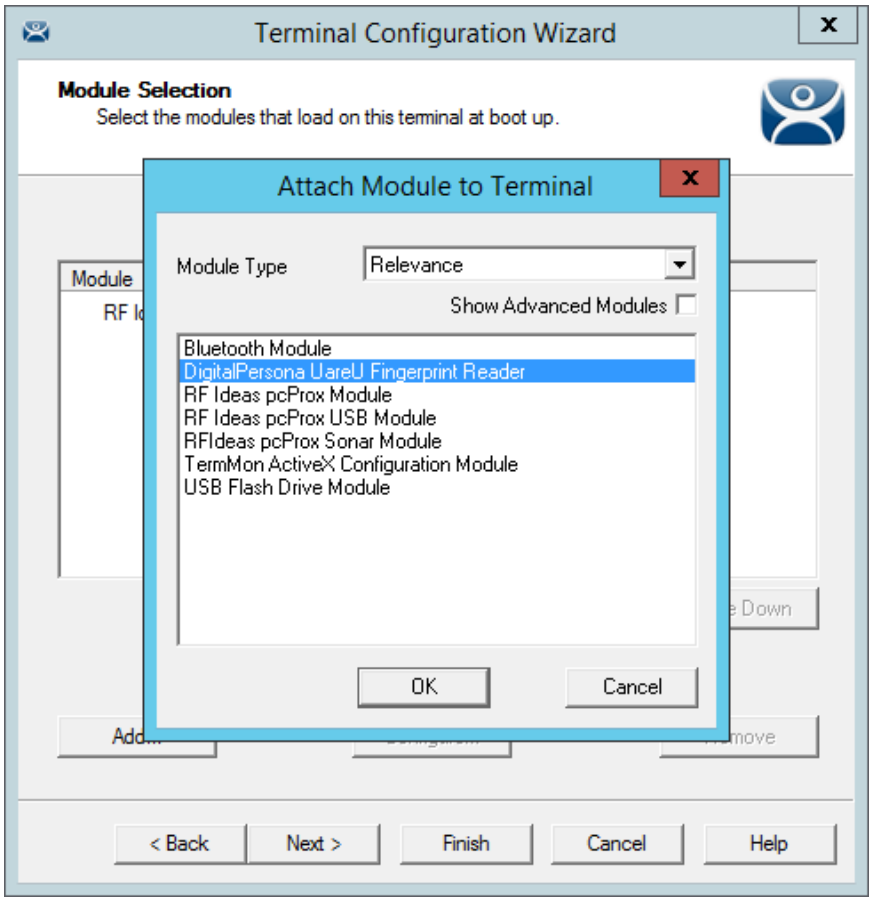
Open the **Terminal Configuration Wizard** by double clicking on the Terminal icon in the Terminal branch of the ThinManager Server tree.



Terminal Mode Selection Page of the Terminal Configuration Wizard

Navigate to the **Terminal Mode Selection Page** of the **Terminal Configuration wizard** and select the ***Enable Relevance User Services*** checkbox to make the fingerprint reader work with TermSecure.

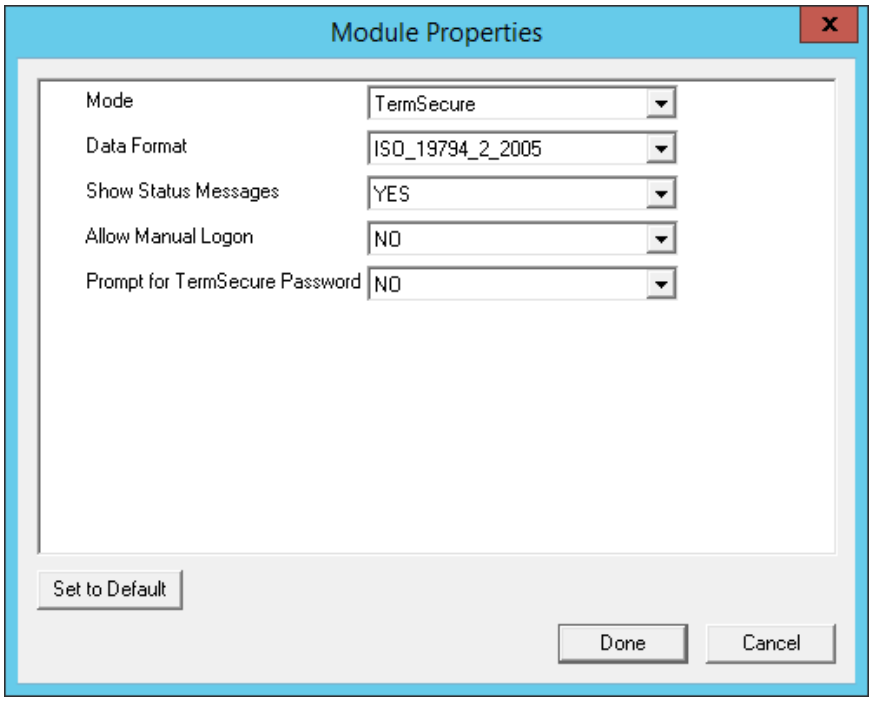
Select the ***Next*** button to navigate to the **Module Selection** page.



Attach Module to Terminal Window

Select the ***Add*** button on the **Module Selection** page to launch the **Attach Module to Terminal** window.

Select **Relevance** in the ***Module Type*** drop-down and highlight the **DigitalPersona UareU Fingerprint Reader module**. Select the ***OK*** button to add the module to the Terminal.



DigitalPersona UareU Fingerprint Reader Module Properties

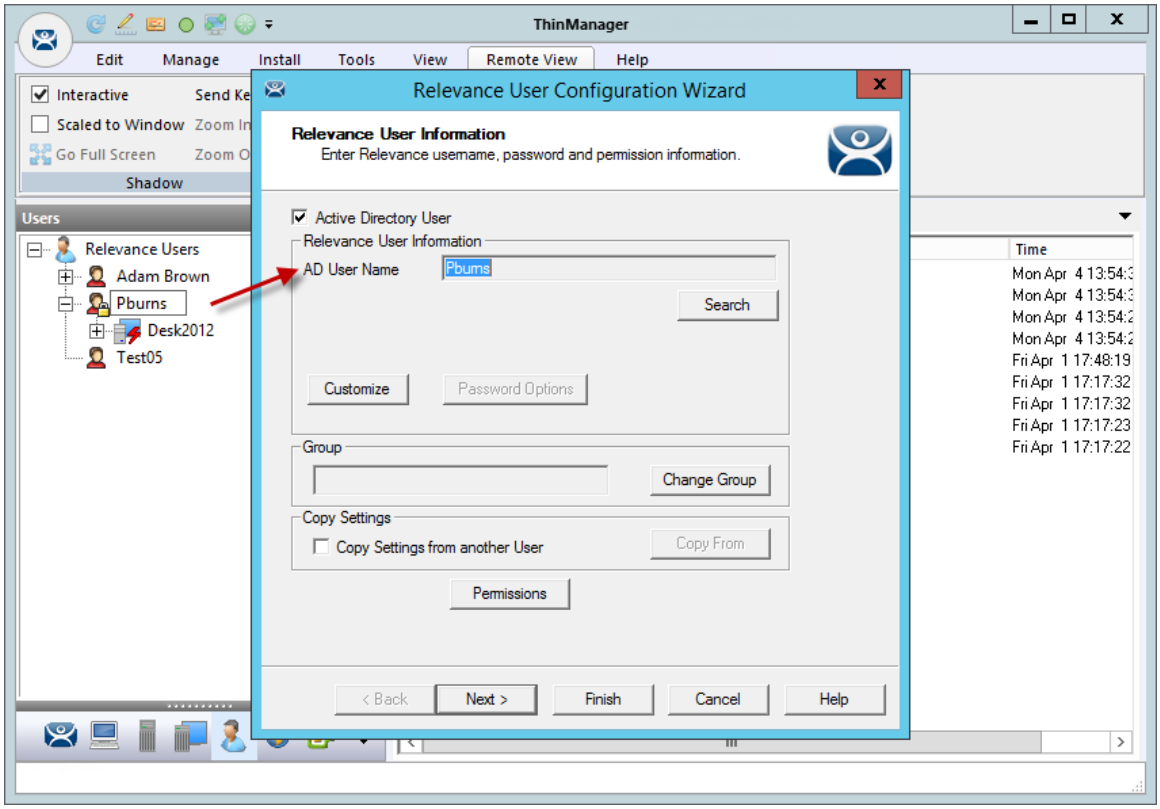
Highlighting the DigitalPersona UareU Fingerprint Reader module and selecting the ***Configure*** button on the **Module Selection** page will launch the **Module Properties** window.

The DigitalPersona UareU Fingerprint Reader module has several configurable settings:

- ***Mode*** – This allows you to choose the Mode. The modes are:
  - **TermSecure** – This is used to identify a Relevance User.
  - **TermMon** – This sends the fingerprint data to the TermMon ActiveX.
  - **TermMon Lookup** – This allows the TermMon ActiveX to identify the user without logging them in.
- ***Data Format*** – This sets the data format for the fingerprint reader. It should match the configuration in the ThinManager Server Configuration Wizard. The data formats are:
  - ISO_19794_2_2005
  - ANSI_378_2004
  - DigitalPersona
- ***Show Status Messages*** – Setting this will show a brief message in the upper right corner of the Terminal for each fingerprint reader event.
- ***Allow Manual Logon*** – If set to ***No*** then a user must use the fingerprint reader to logon. If set to ***Yes*** then you can use the fingerprint scanner or manually logon.
- ***Prompt for TermSecure Password*** – If set to ***Yes*** then the user will be required to enter a password in addition to the fingerprint scan. If set to ***No*** then the fingerprint scan is enough to allow a logon.

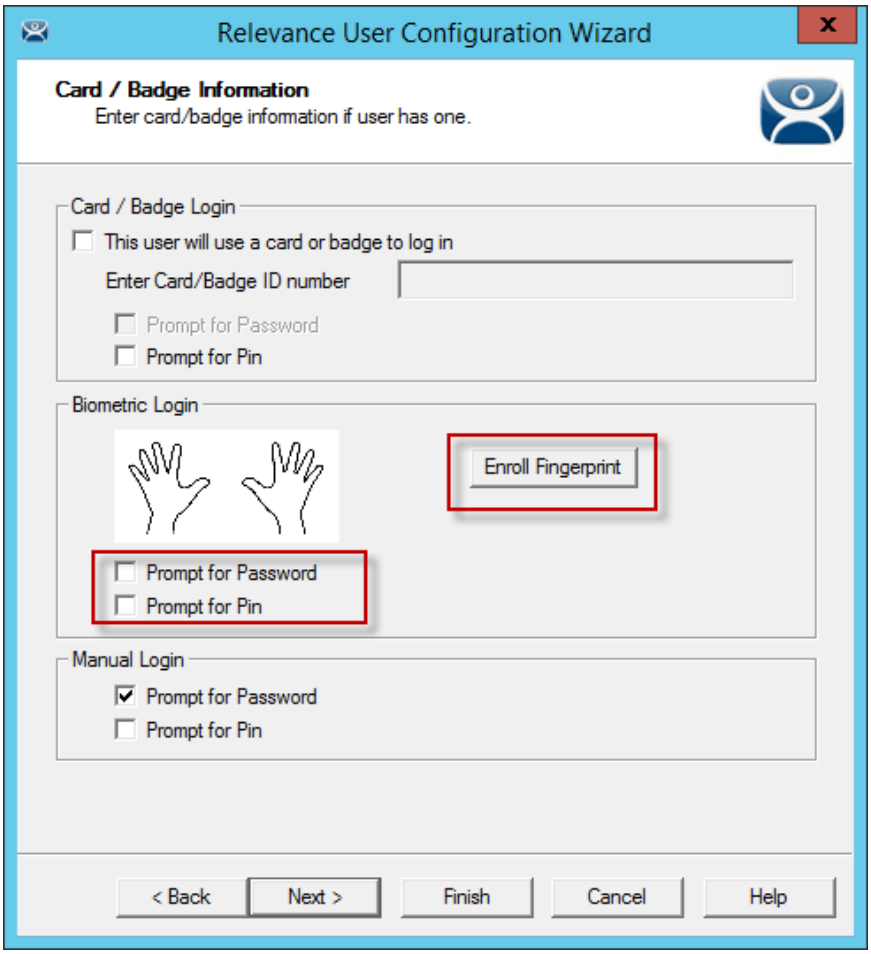
35.2.3. Fingerprint Reader for the Relevance User

Fingerprint data is associated with a user in the **Relevance User Configuration Wizard**.



Relevance User Configuration Wizard

Open the ***Relevance Users*** branch of the ThinManager tree and double click on the Relevance User whose fingerprints you want to register. This will launch the **Relevance User Configuration** wizard.



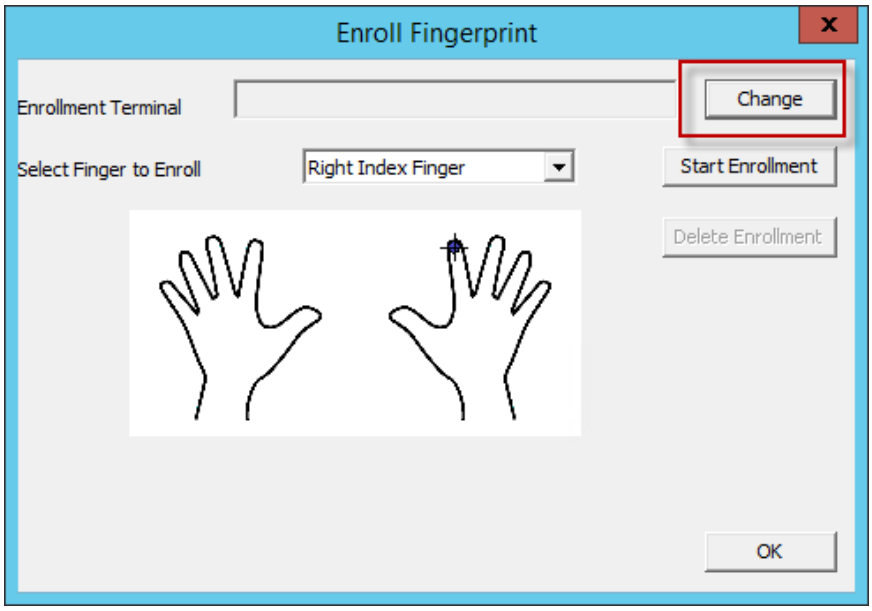
Card / Badge Information Page

The **Card / Badge Information Page** has an ***Enroll Fingerprint*** button that begins the registration process.

Select the ***Enroll Fingerprint*** button to launch the **Enroll Fingerprint** window.

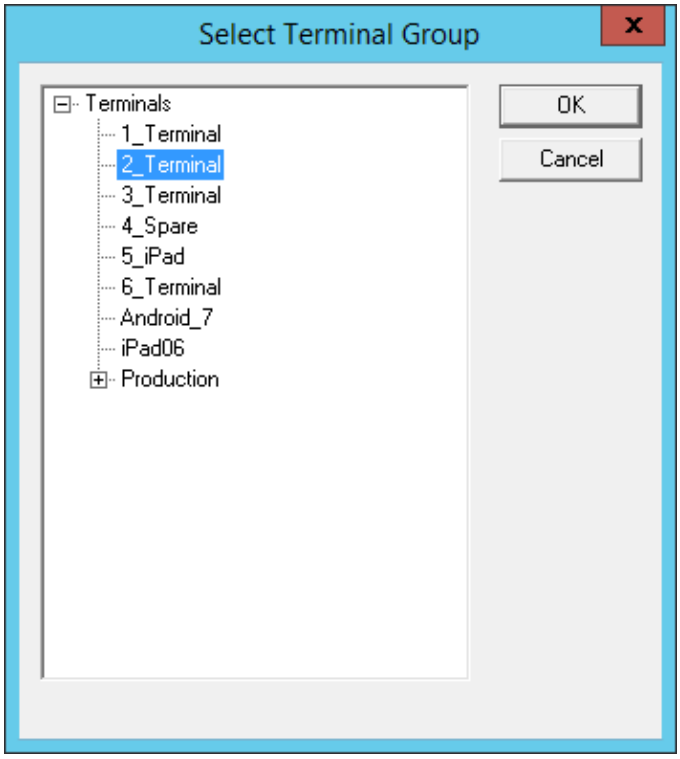
Note: A secondary credential can be required by selecting ***Prompt for Password*** or ***Prompt for Pin*** for the **Card/Badge Login**, the **Biometric Login**, or a **Manual Login**.

- ***Prompt for Password*** – This checkbox, is selected, will require the user to enter their password.
- ***Prompt for Pin*** – This checkbox, is selected, will require the user to enter their PIN.



Enroll Fingerprint Window

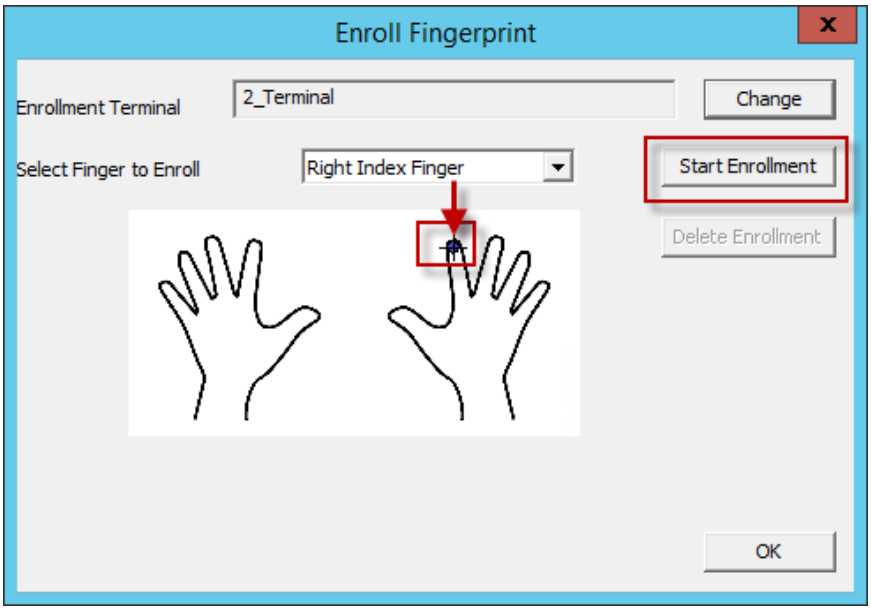
Select the ***Change*** button to open the **Select Terminal Group** window to select the Terminal that has the fingerprint scanner you will use for registration.



Select Terminal Group Window

Highlight the Terminal that has the fingerprint scanner you will use for registration in the **Select Terminal Group** window and select the ***OK*** button.

This Terminal will be registered as the **Enrollment Terminal**.

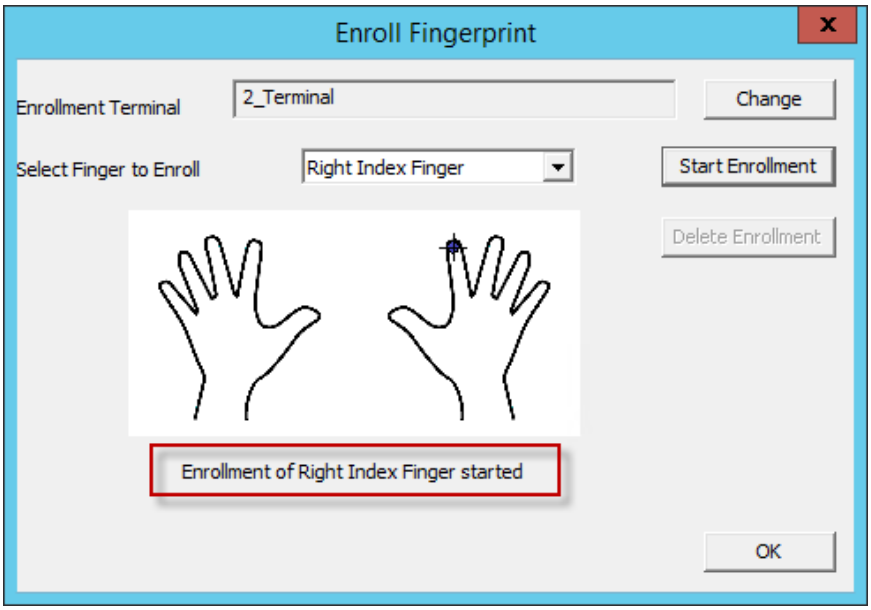


Enroll Fingerprint Window

Once you have selected the Enrollment Terminal select the finger you want to enroll in the ***Select Finger to Enroll*** drop-down.

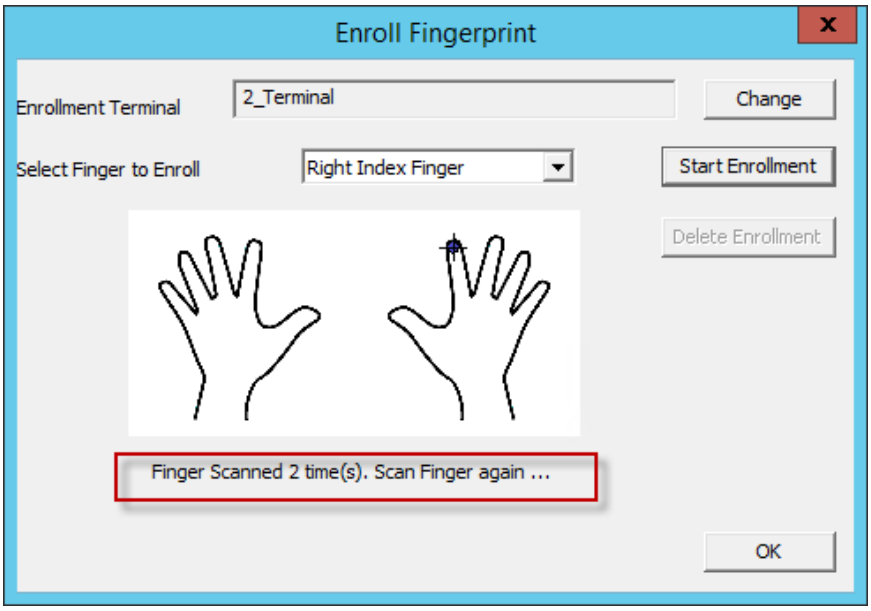
The selected finger will show a crosshair logo.

Select the ***Start Enrollment*** button to begin.



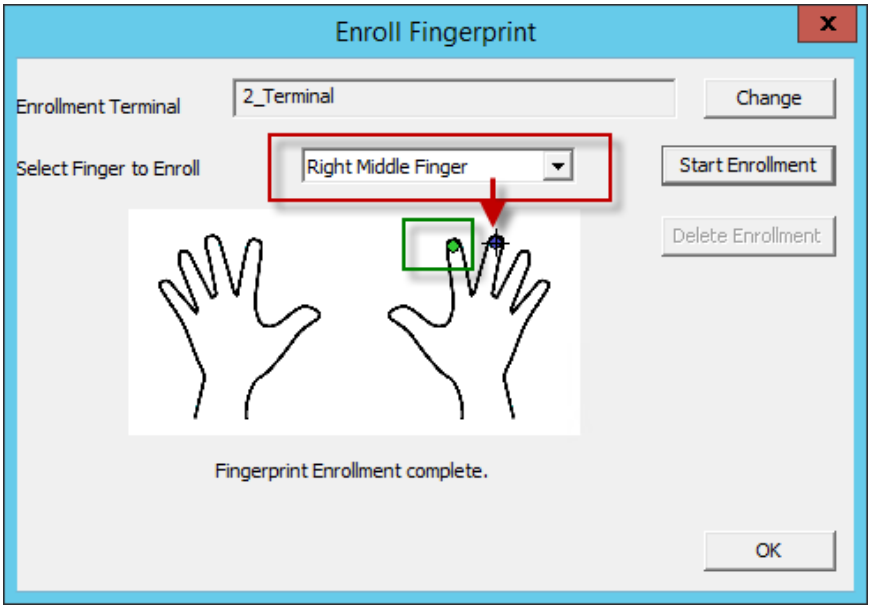
Enroll Fingerprint Window

The enrollment requires four scans of the fingerprint. Place it on the scanner. The blue light should turn red, and then back to blue. Leave it on until the red light turns off.



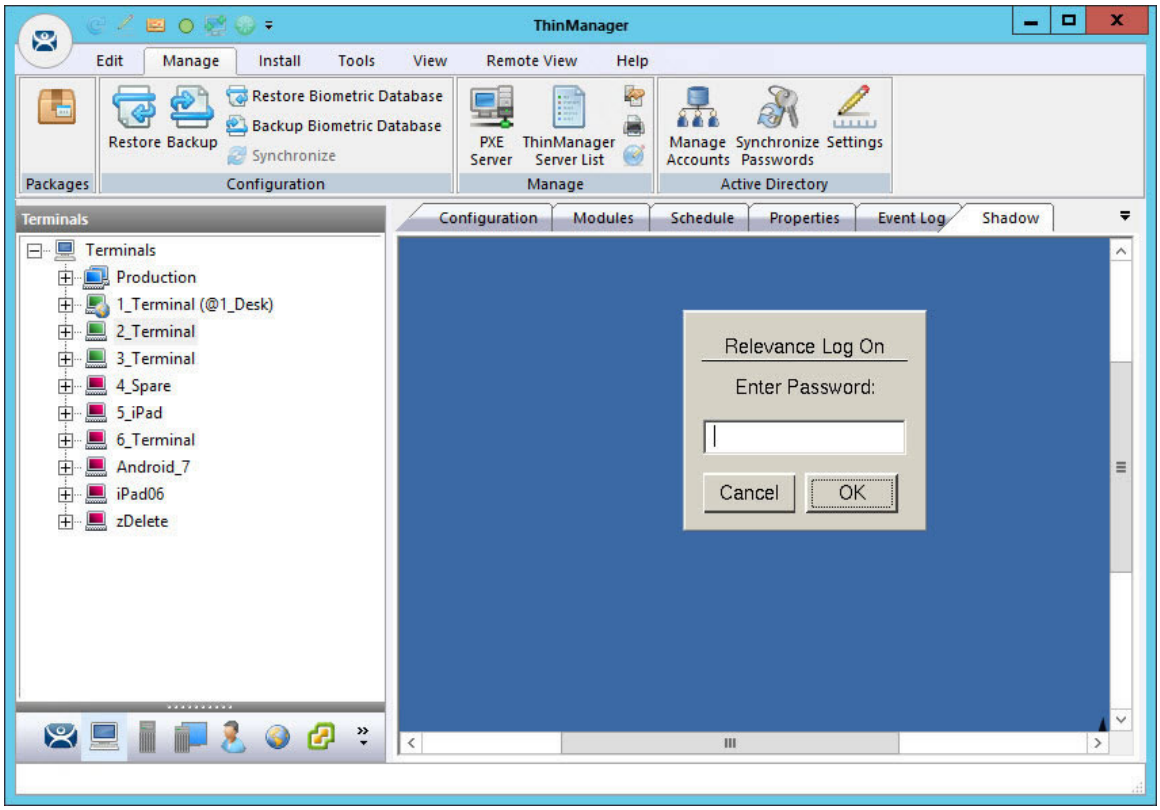
Enroll Fingerprint Window

The enrollment requires four scans of the fingerprint. Repeat until complete.



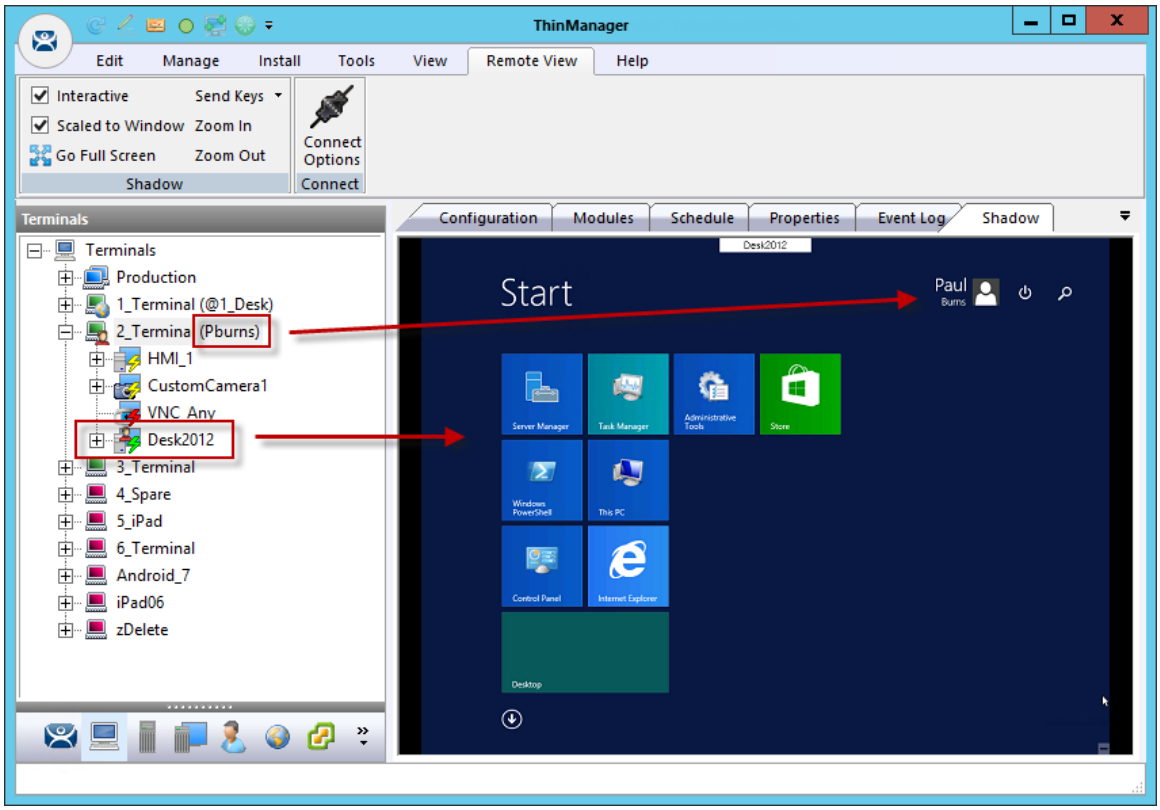
Enroll Fingerprint Window

Once the finger has been scanned and enrolled the scanned finger will show as green on the **Enroll Fingerprint Window**. A new finger will be selected in the ***Select Finger to Enroll*** drop-down.



Shadow of a Terminal Scan

Scanning a registered fingerprint will trigger a TermSecure logon. If the ***Always Prompt for Password*** checkbox was checked then a dialog box will appear requesting the Windows password for the Windows account.



Shadow of a Terminal Scan

This picture shows a Relevance User logged into a Terminal using a DigitalPersona UareU Fingerprint Reader.

The Terminal icon shows a user logged in, it names the user, and the Desktop2012 application shows a user login to show that that display client was assigned through the Relevance User.

36. Relevance Location Services

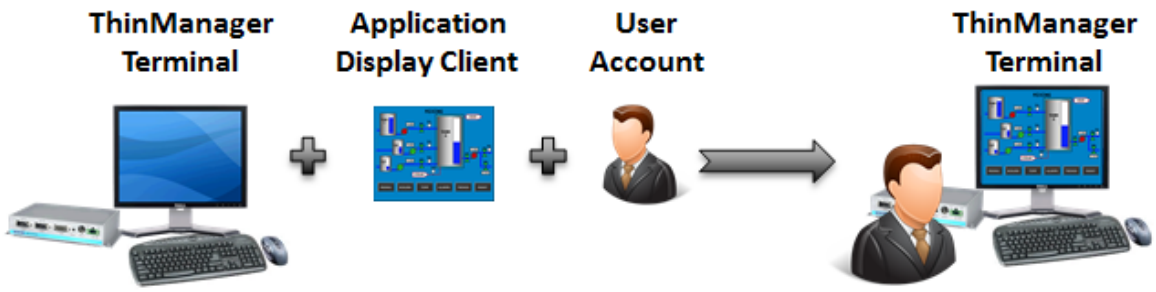
Relevance is mobile computing based on location. It doesn't just sending an application to a mobile device, but is a way to enable the location to determine the content sent to the device. The mobile device allows the user to interact with the location.

Relevance is the ***How*** to provide ***What*** you need, ***Where*** and ***When*** you need it.

There are two types of locations in Relevance, **Assigned** and **Unassigned**.

Assigned locations are locations that have a Terminal and monitor at the given location, much like traditional computing. Relevance adds additional functions to the location that allows mobile devices to interact with the location and Shadow the Terminal, Clone the applications, or Transfer the control of the location to the mobile device.

Unassigned locations are locations that lack a permanent Terminal and monitor and all of the content is sent to the mobile device.



ThinManager Deployment

In ThinManager you deploy applications by defining a Terminal, configuring it with applications and a user account. This allows the operator to access the applications needed.

Relevance Assigned Location

Using the Relevance method starts with location creation. The application, user account, and Terminal will be added to the location.

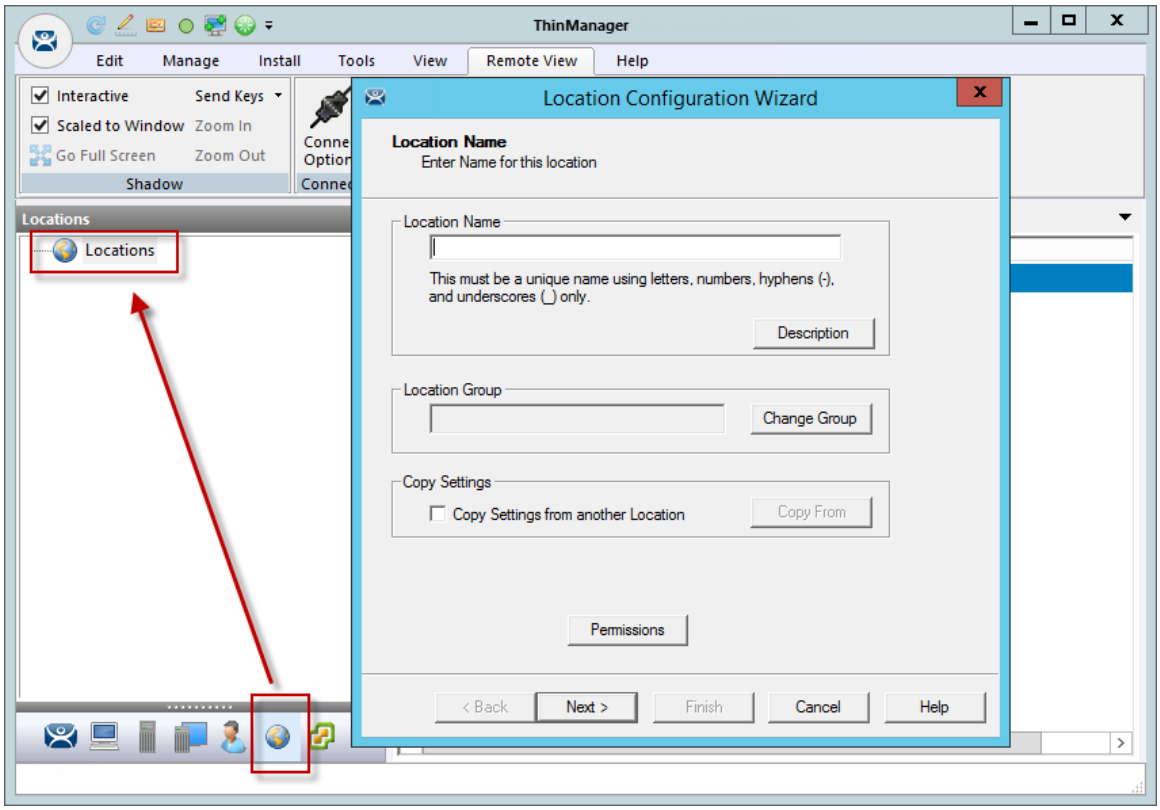
Relevance Unassigned Location

Relevance can deploy applications to locations without Terminals. Your mobile device becomes the Terminal.

36.1. Creating a Location with the Location Configuration Wizard

The first task is to create a location and apply the application and user account to the location which will then be assigned to the Terminal.

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

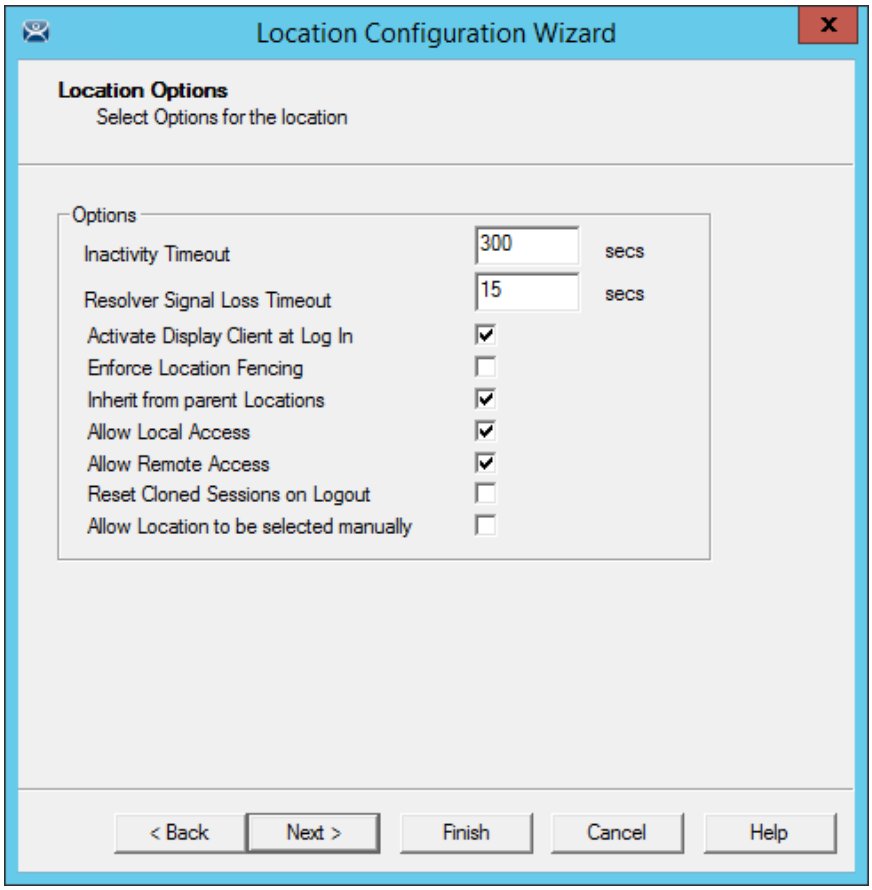


Location Configuration Wizard

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

Name the location.

Select ***Next*** to continue.

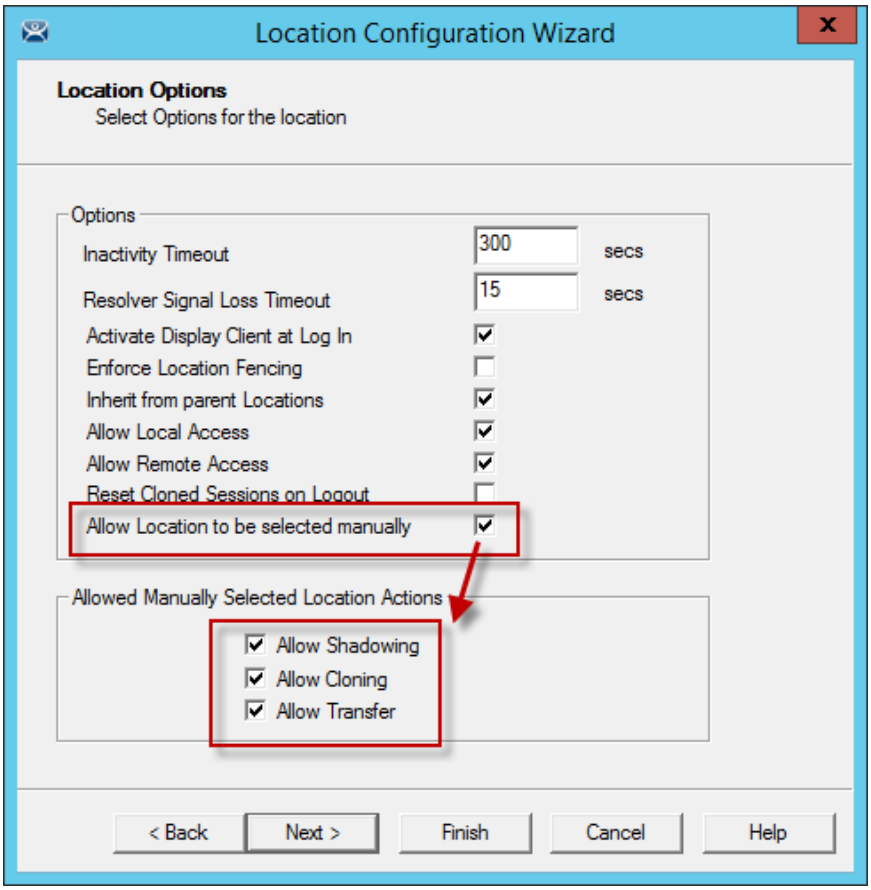


Location Options Page

The **Location Options** page has several configurable options that control the remote access.

- ***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 Connection* -** 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.

Checking the ***Allow Location to be selected manually*** checkbox reveals other settings.



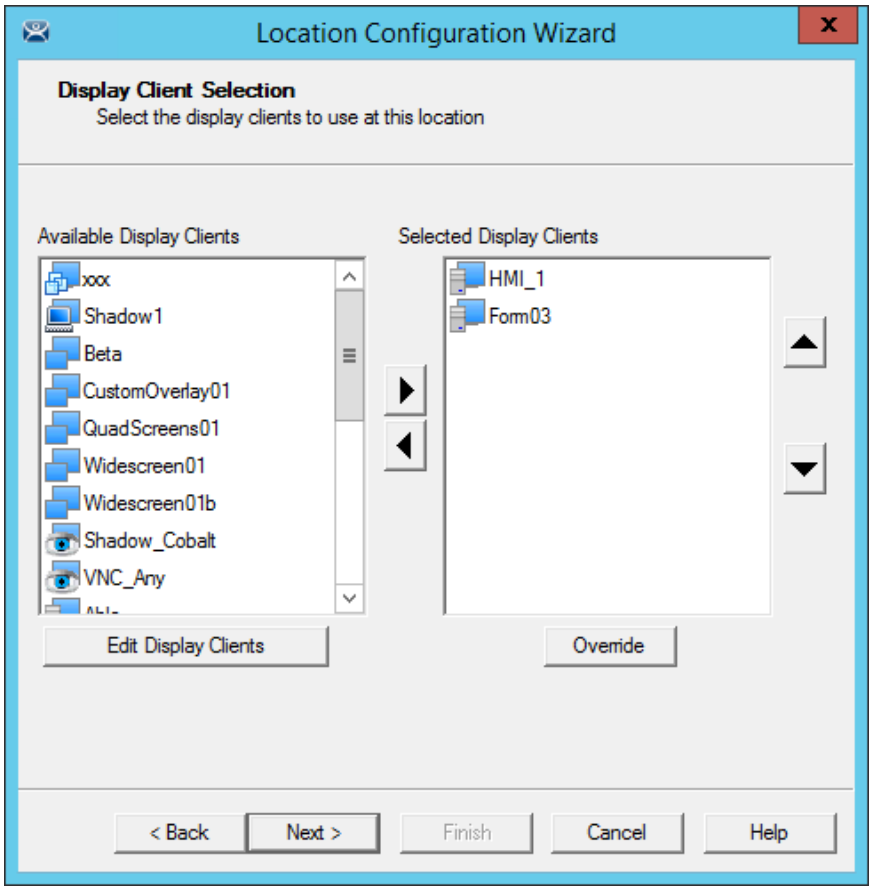
Location Options Page

Allow Manually Selected Location Actions – These are the actions you can manually select. You can allow all, or none.

- ***Allow Shadowing*** – This allows a duplicate of the display to be shown on the mobile device.
- ***Allow Cloning*** – This allows the user to launch the same applications as the location but using their Windows account.
- ***Allow Transfer*** – This allows the display to be moved from the location to the mobile device.

Select the manual connections of your choice. Any left unchecked will not be available in the manual selection menu.

The defaults are fine but you have the option to customize the settings as needed.

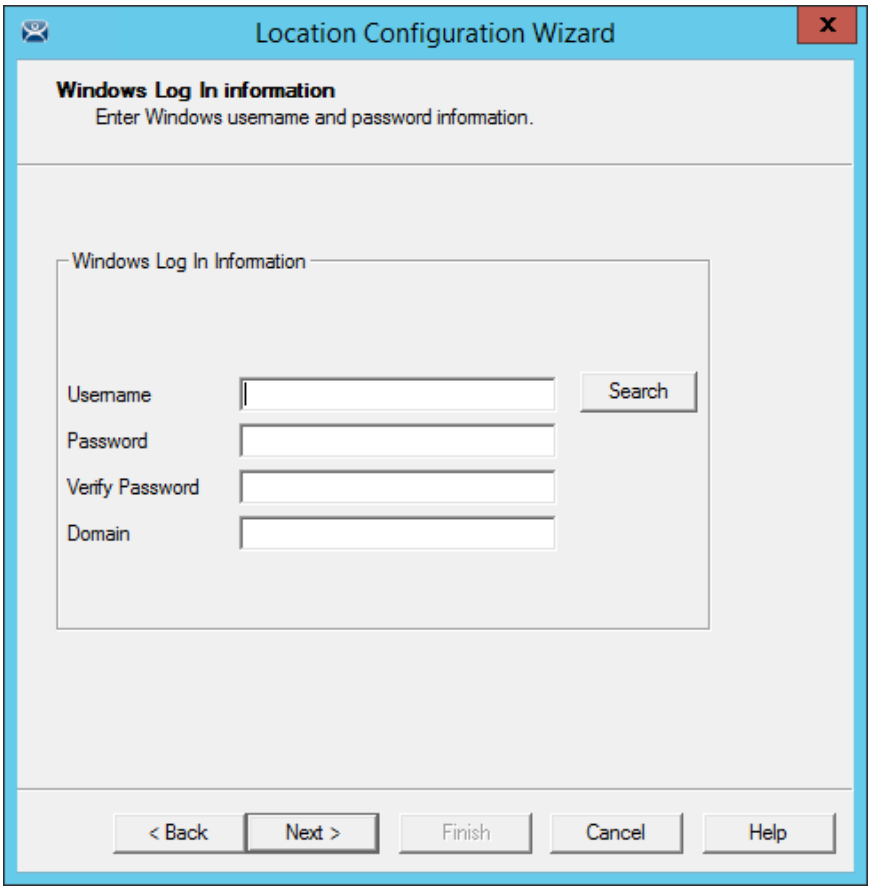


Remote Desktop Server Selection

Select the display clients that you want displayed on the Location.

The Override button launches the Override Settings window that allows you to add a different user name to a highlighted display client.

Apply the desired display clients to the location and select ***Next*** to continue.



Window Log In Information Page

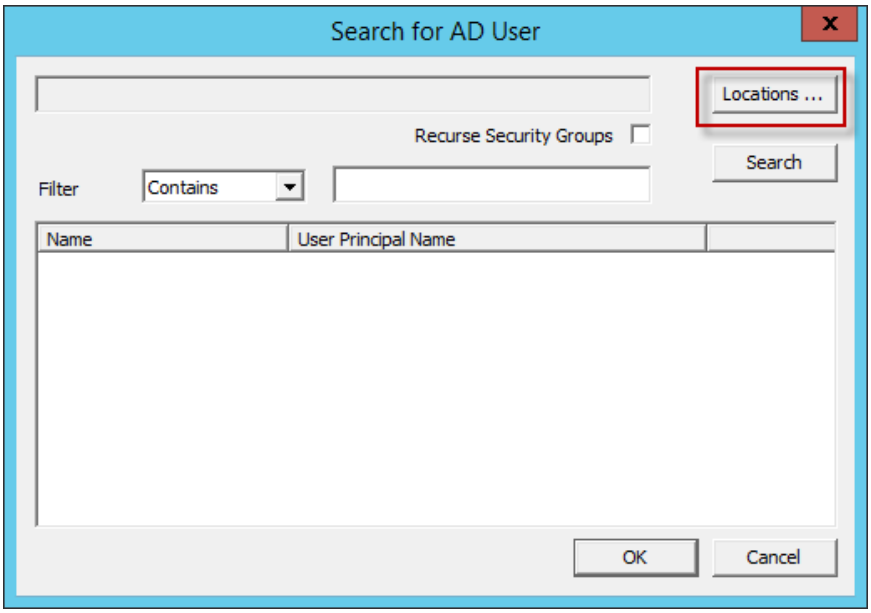
A location with a display client will require a Windows username.

Non-Domain Windows Account:

- Enter a valid Windows username in the ***Username*** field.
- Enter the password in the ***Password*** and ***Verify Password*** fields.
- Select the ***Next*** button to continue.

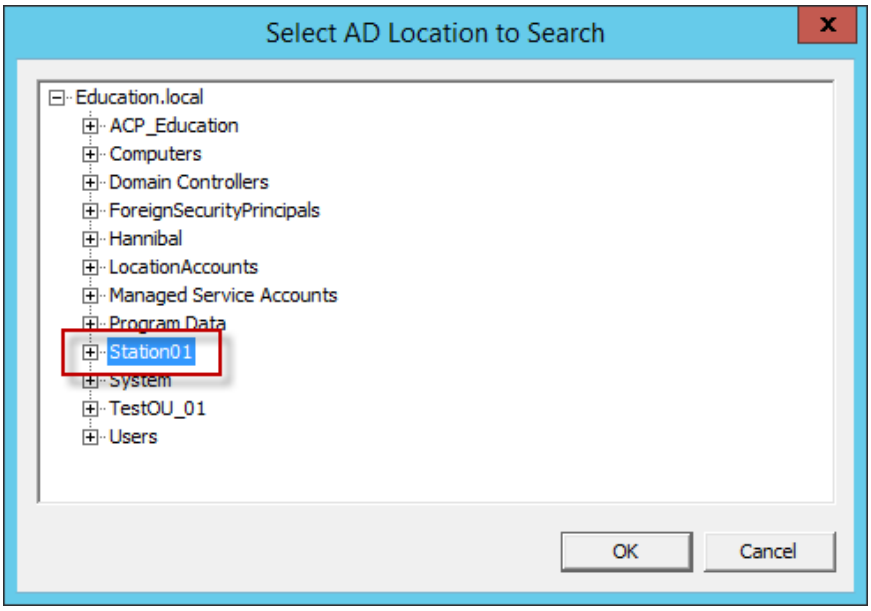
Domain Windows Account:

- Select the ***Search*** button will open the **Search for AD User** window.



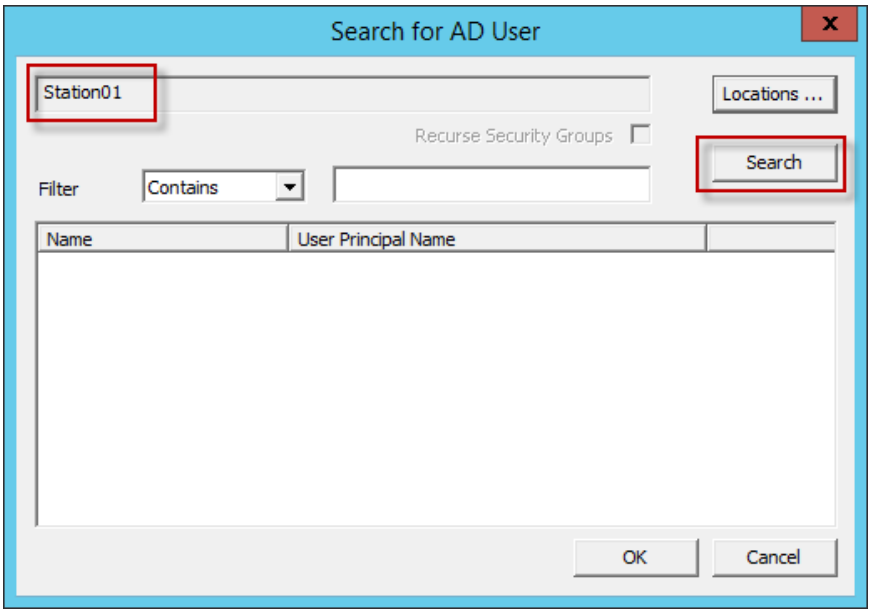
Search for AD User

The **Search for AD User** window allows you to reference users from the Active Directory. Click the ***Locations…*** button to choose where to select users.



Select AD Location to Search

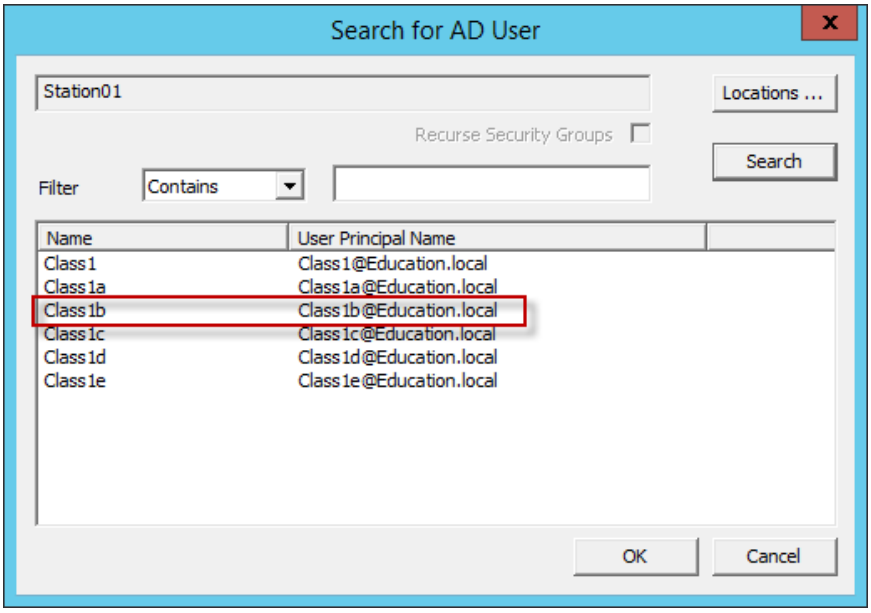
Clicking the ***Locations…*** button will launch the **Select AD Location to Search** window. Highlight the domain branch you want to use and select the ***OK*** button.



Search for AD User Window

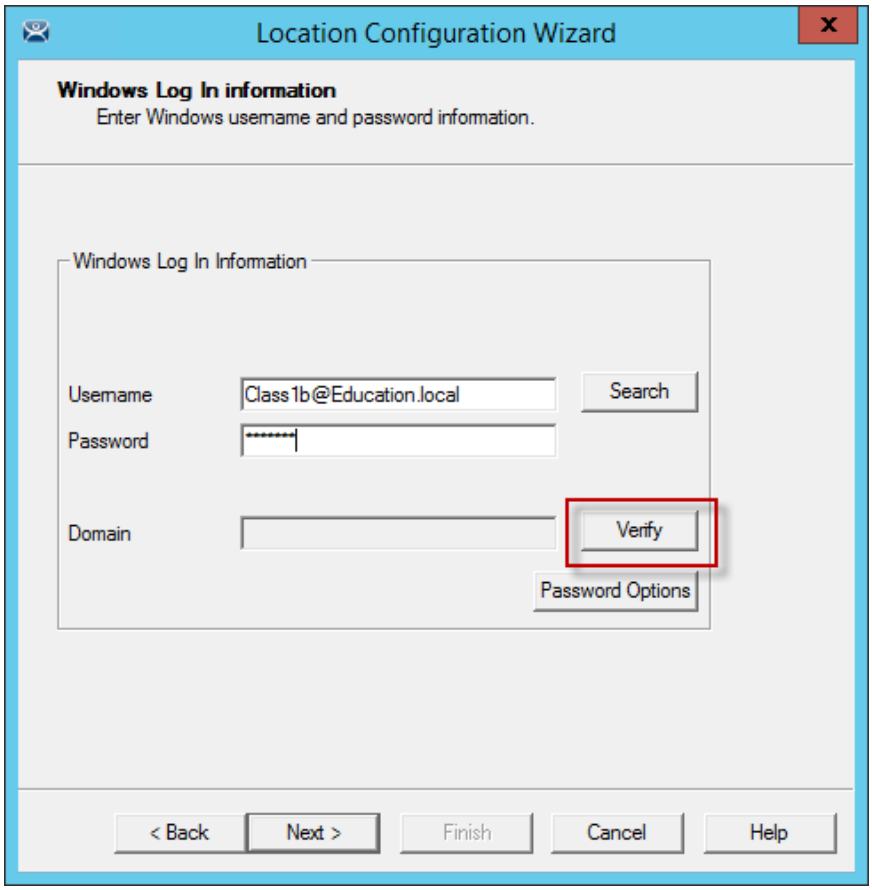
Highlighting the domain branch you want to use and select the ***OK*** button will add the Location for the search.

Selecting the ***Search*** button will fetch the user accounts and populate the **Search for AD User** window.



Populated Search for AD User Window

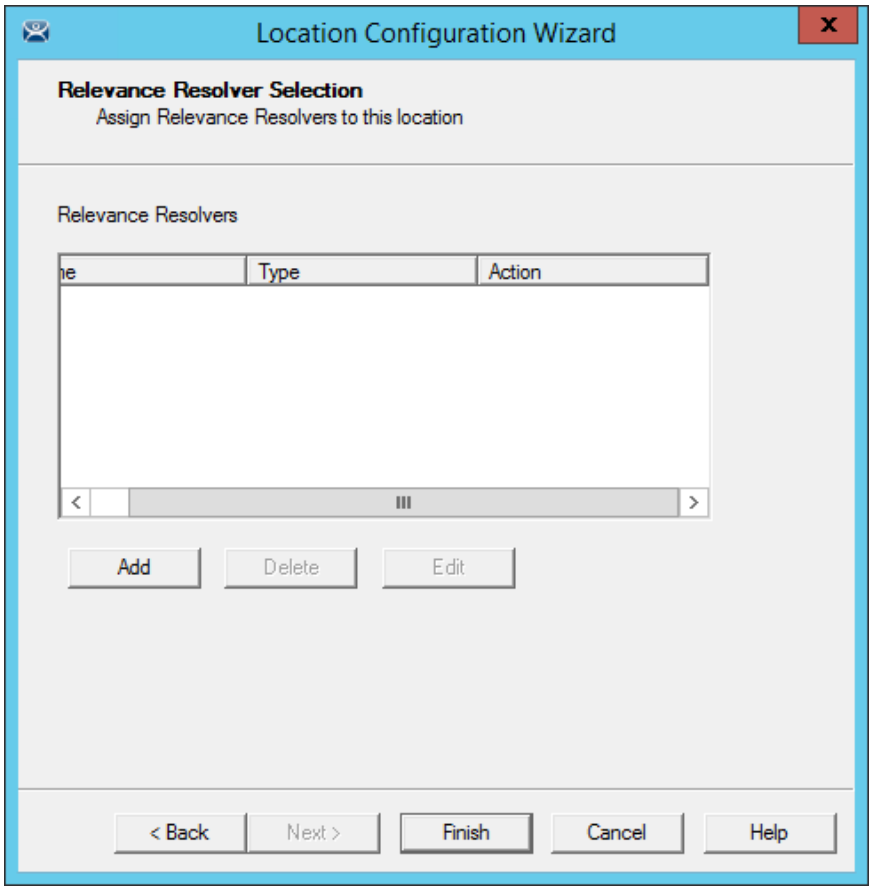
Highlight the domain user you want and select the ***OK*** button. This will reference the user for the Terminal log in account.



Window Log In Information Page

The Location is now configured to use an Active Directory user account.

Select ***Next*** to continue.



Relevance Resolver Selection Page

The **Relevance Resolver Selection** page allows the association of Resolvers to the location.

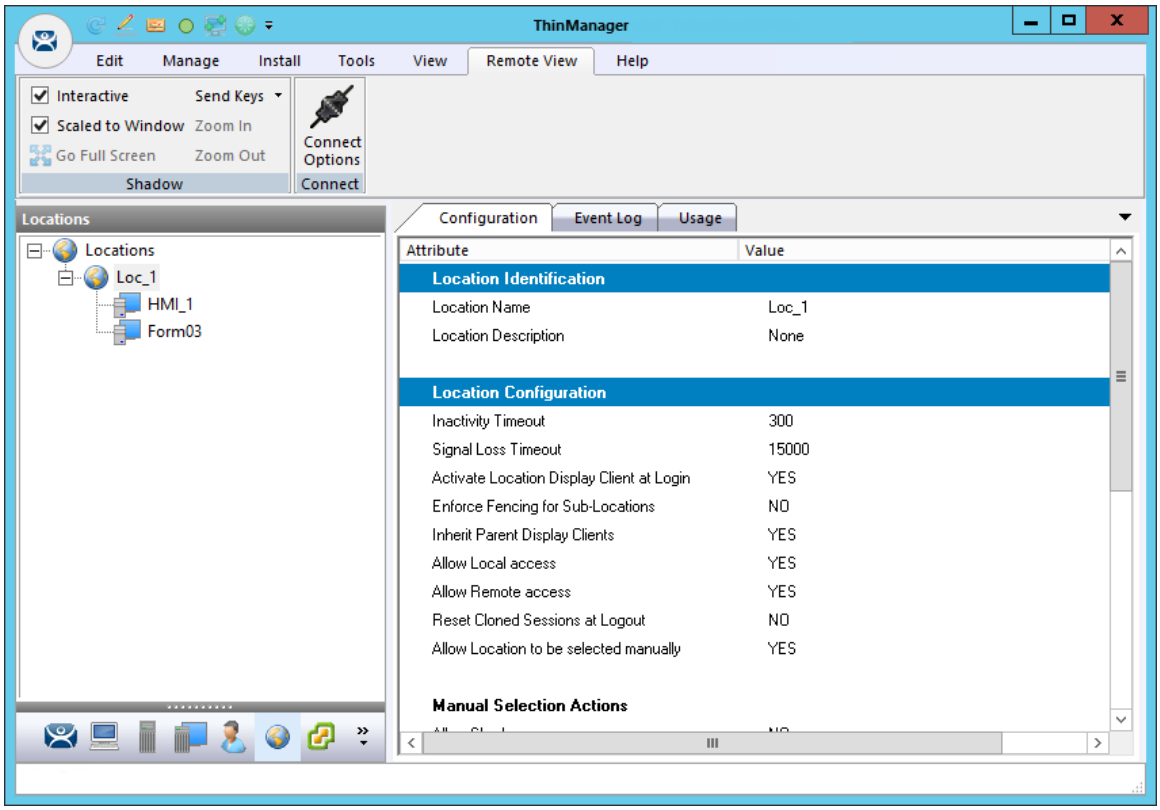
Resolvers include

- QR Codes
- Bluetooth Beacons
- Wi-Fi Access Points
- GPS

We will explain the configuration of Relevance Resolvers later.

See **Using the Mobile Device to Add Resolver Codes** at page 618.

Select the ***Finish*** button to create the **Location**.



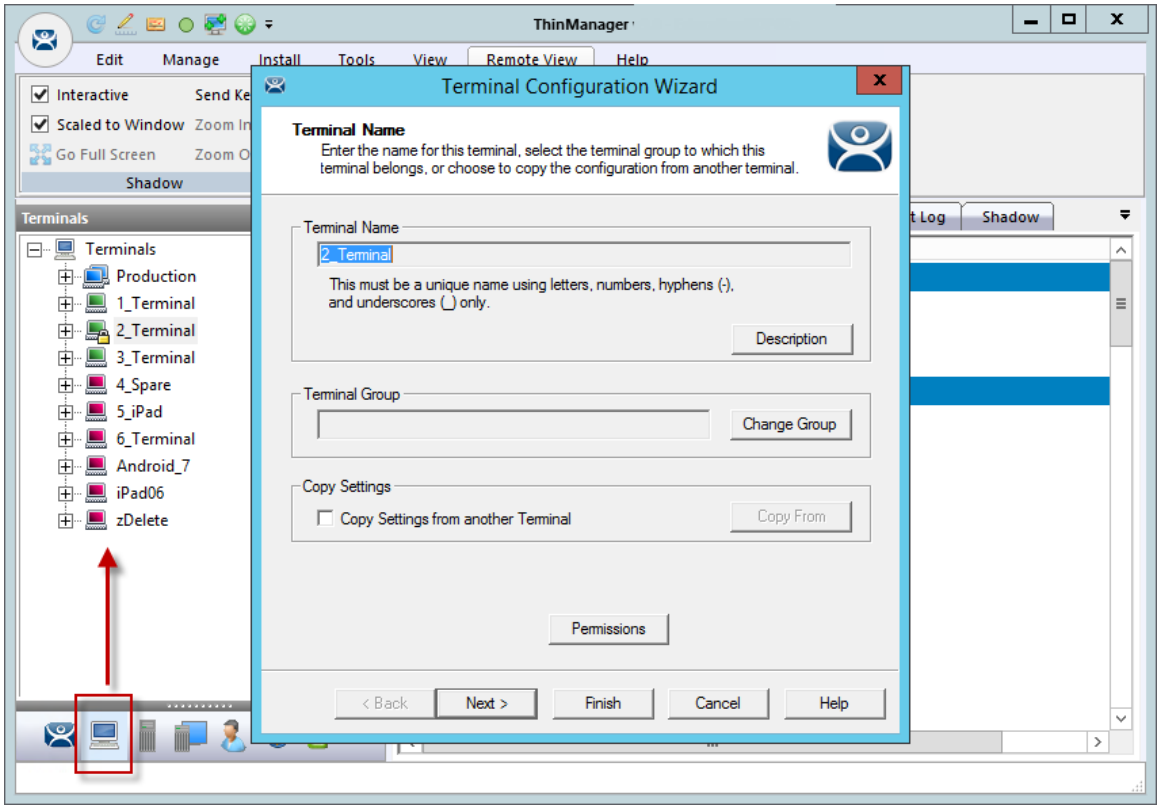
Location with Assigned Display Clients

The **Location** tree will show the created Locations and the display clients assigned to it.

36.2. Adding a Location to a Terminal

Now the newly created location needs to be attached to a Terminal.

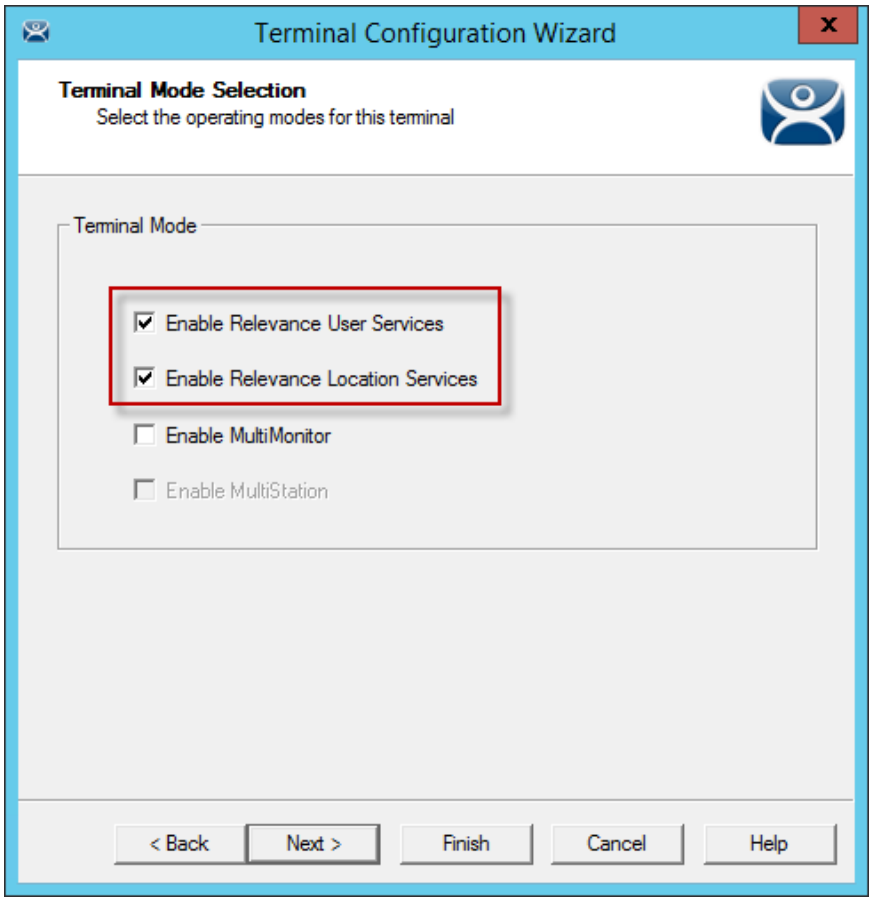
This shows adding a Location to an already configured Terminal. You can create the Terminal from scratch and add the location as you configure the Terminal.



Terminal Configuration Wizard

Select the **Terminal** icon on the Tree Selector at the bottom of the tree to open the Terminals branch.

Highlight a Terminal and double click or select ***Modify*** to open the **Terminal Configuration Wizard**.



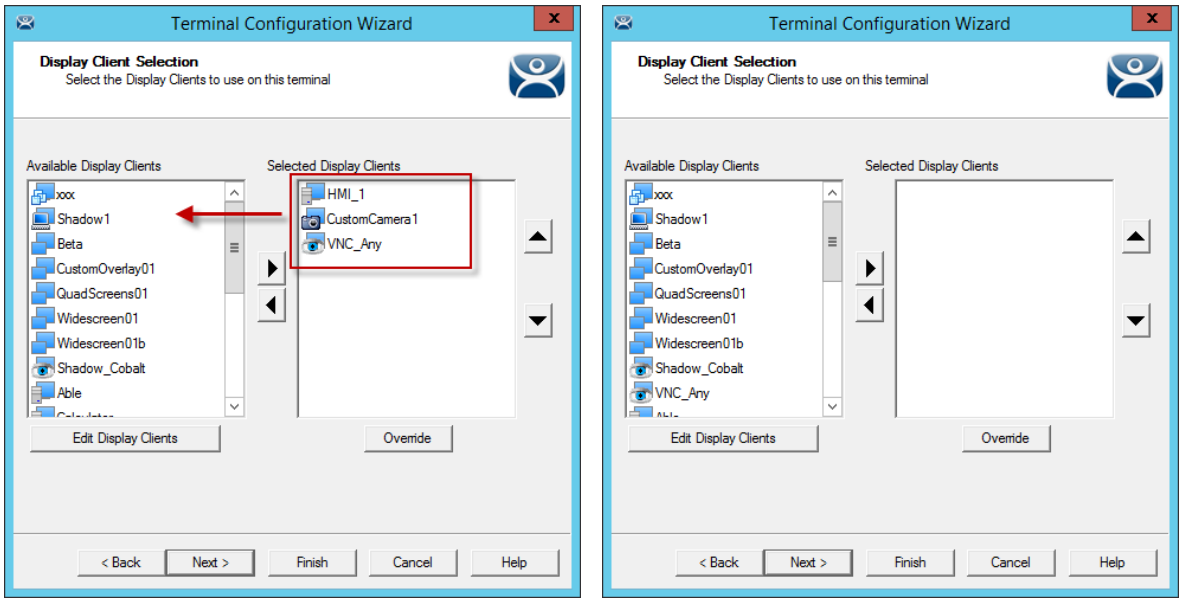
Terminal Mode Selection Page

Navigate to the **Terminal Mode Selection** page. There are two Relevance checkboxes.

- ***Enable Relevance User Services –*** This uses the ThinManager Relevance Access to control access to applications.
- ***Enable Relevance Location Services –*** This allows the Terminal to use Locations in its configuration.

Check the ***Enable Relevance Location Services*** checkbox to use Locations.

Select ***Next*** to navigate to the Display Client Selection page.



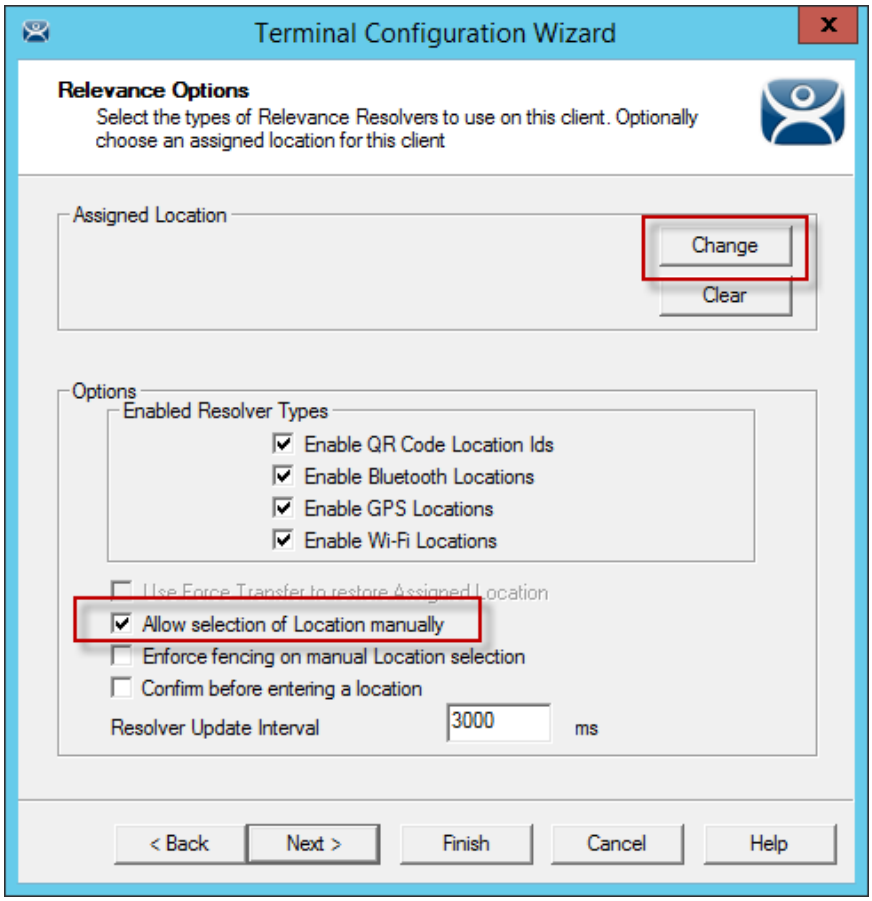
Remove Display Clients on the Display Client Selection Page

Remove any existing display clients from an existing Terminal by highlighting them and selecting the left arrow button.

Leave the Selected Display Clients list blank if you are configuring a new Terminal.

The user will access the display clients through the location, not the Terminal.

Select ***Next*** and continue to the **Relevance Options** page.



Relevance Options Page

Select the ***Options*** before choosing a location. Once the Location is assigned the ***Options*** are locked.

Note: Select the ***Options*** before choosing a location. If you need to change an option you can clear the location with the ***Clear*** button, change the option, and then re-assign the Location.

The **Options** include:

- ***Use Force Transfer to restore Assigned Location*** – This gives the operator to take a transferred session back without having to wait for the other device to approve of the transfer.
- ***Allow Selection of the Location manually*** – This will let the user select the location manually from a menu on the mobile device. If this is unselected then the user must use a Resolver.
- ***Use Force Transfer to restore Assigned Location*** – This gives the operator to take a transferred session back without having to wait for the other device to approve of the transfer.
- ***Enforce fencing on manual Location selection*** – This enforces the fencing on a location during manual selection.
- ***Confirm before entering a location*** – This notifies you as you enter a fence and asks for an acknowledgement.

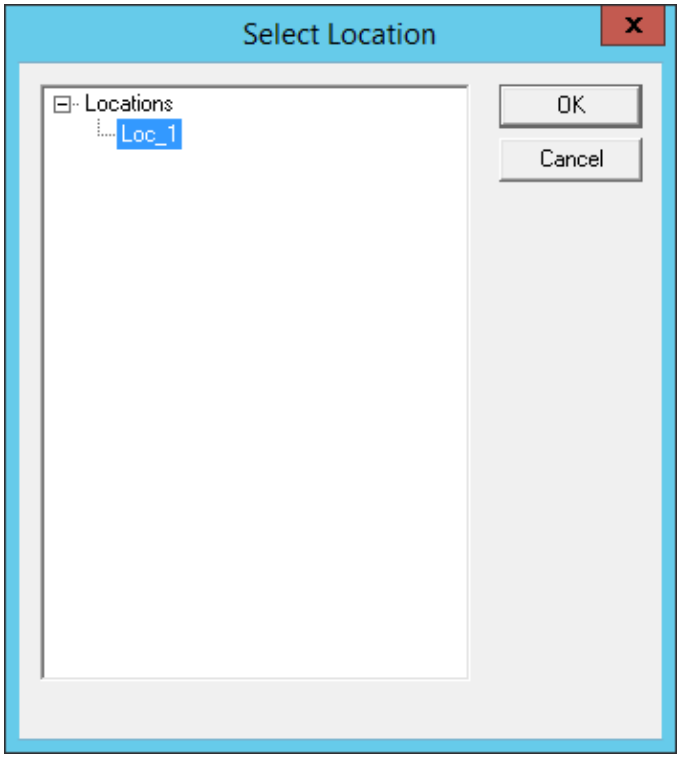
Enable Resolver Types – Relevance has several methods of resolving the location to allow specific applications to get sent to specific locations.

- ***Enable QR Code Location Ids*** – This allows the scanning of a QR code to determine the location.
- ***Enable Bluetooth Locations*** – This allows the use of Bluetooth beacons to determine the location.

- ***Enable GPS Locations***– This allows the Global Positioning System of the mobile device to determine the location.
- ***Enable Wi-Fi Locations*** – This allows the signal strength of Wi-Fi access points to determine the location.

Each method selected will require configuration to associate a location with the Resolver data.

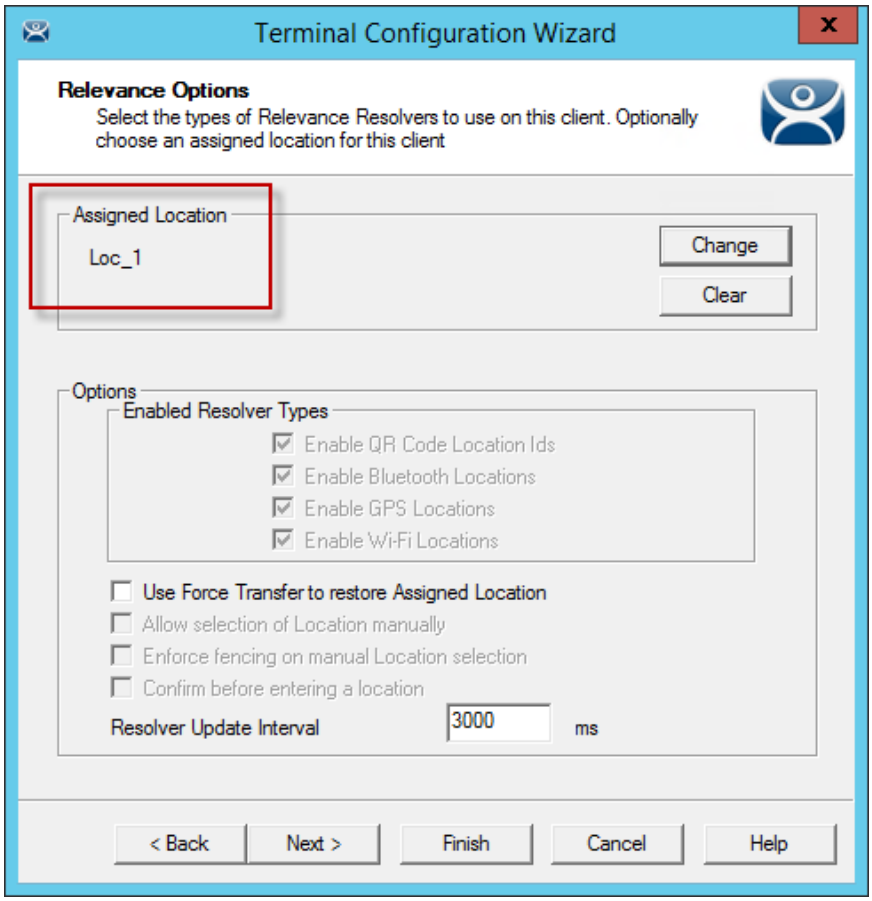
Select the ***Change*** button to open the **Select Location** window.



Select Location Window

The created **Locations** will be displayed in the **Select Location** tree.

Highlight the desired Location and select the ***OK*** button.



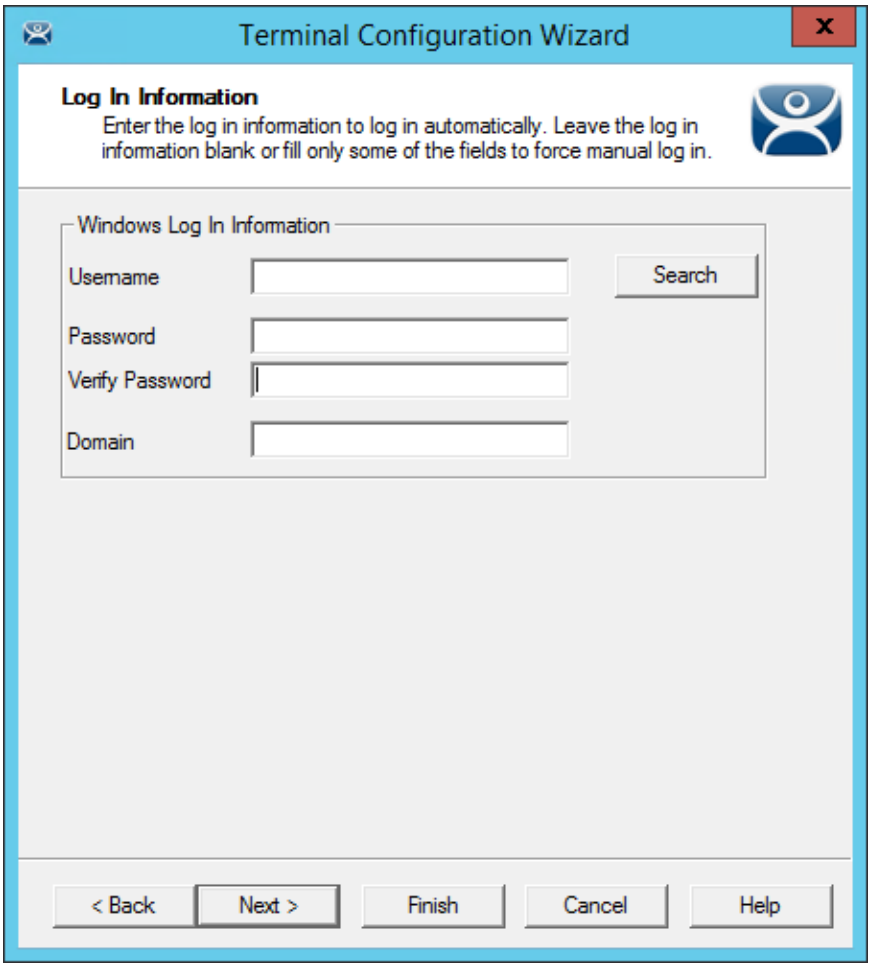
Location Assigned

The Location will be displayed in the Assigned Location field once it is assigned to the Terminal.

Once the Location is assigned the ***Options*** are locked.

Note: If you need to change an option you can clear the location with the ***Clear*** button, change the option, and then re-assign the Location.

Once the location is assigned select ***Next*** and navigate to the **Log In Information** page.

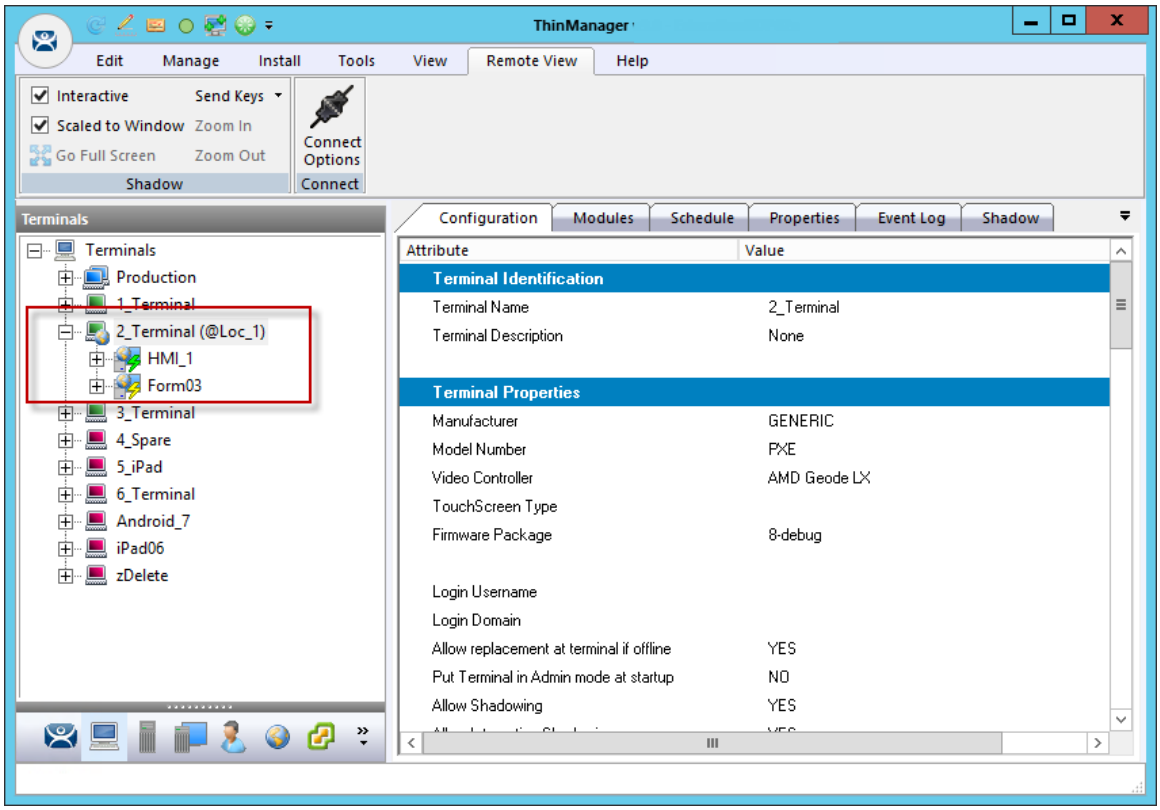


Log In Information Page

A preconfigured Terminal would have been assigned a user account to allow it to log in to the servers. This is not needed now because it will use the user account is assigned to the location.

- Leave the ***Username*** and ***Password*** fields blank.
- Once the ***Username*** is cleared select the ***Finish*** button to complete the wizard.

Once the wizard is closed you need to restart the Terminal to load the changes. Right click on the Terminal in the tree and select ***Restart Terminal*** to load the new configuration.



Locations on Terminals in Terminal Tree

The application is now running on the location which is assigned to the Terminal.

The tree will show location icons to show what display clients are from the location.

In this example the Terminal **2_Terminal** is using location **Loc_1**.

Note: The user should see no difference in the application deployment between a Terminal with display clients deployed with Locations and a Terminal without Locations.

The big difference Relevance makes is when a mobile device interacts with the location.

37. Using Mobile Devices to Interact with Relevance

Adding a location to a Terminal doesn't seem like it makes any difference. The application runs the same on the Terminal versus a location on a Terminal. The difference is the interaction a user can have with that location using a mobile device.

Configuration of mobile devices is covered in Devices – Mobile Devices on page 321.

Relevance uses Resolvers to define the location.

- ***Manual Selection*** – This allows user select the location manually from a menu on the mobile device.
- ***QR Code*** – QR codes can be created to define a location.
- ***Bluetooth*** – This allows the use of Bluetooth beacons to determine the location.
- ***GPS*** – This allows the Global Positioning System of the mobile device to determine the location.
- ***Wi-Fi*** – This allows the signal strength of Wi-Fi access points to determine the location.
- ***iBeacon*** – This is an Apple version of Bluetooth

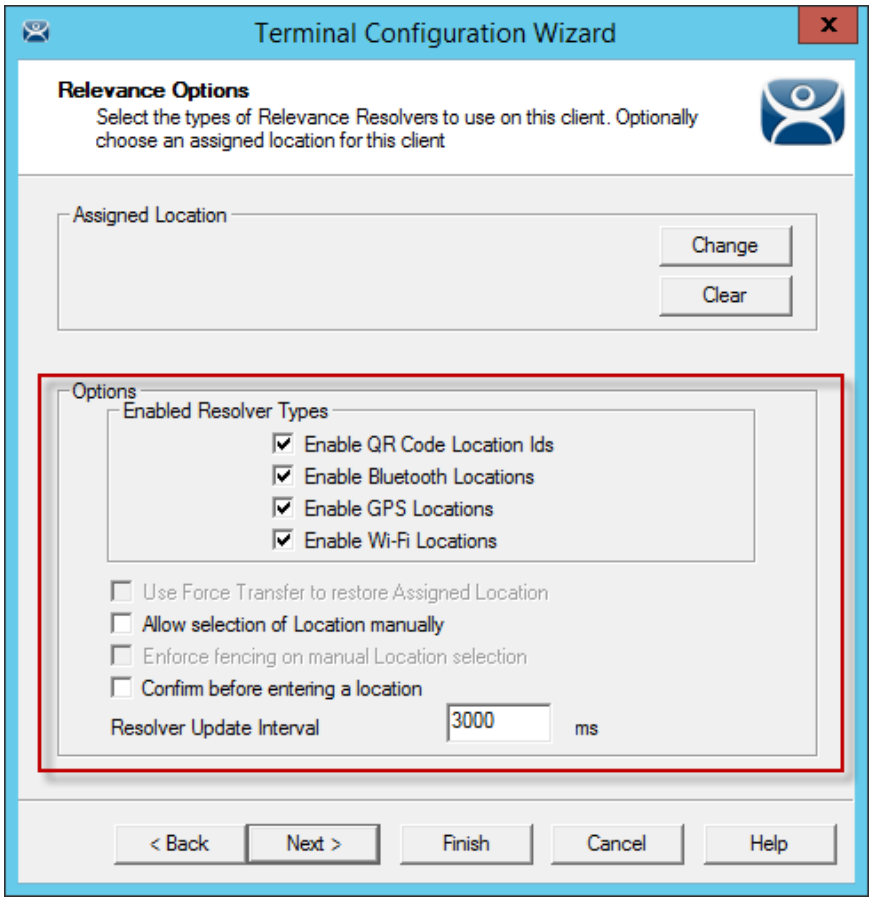
Resolvers are identified and marked using the mobile device so it is important to configure a mobile device for identifying the resolvers in Relevance

---

Note: The iTMC application can be installed for free from the App store on iTunes.
The aTMC application can be downloaded for free from the Google Play Store.
The WinTMC client for Windows can be downloaded at the ThinManager web site at http://downloads.thinmanager.com/.

Mobile devices have two pages in the Terminal Configuration Wizard that enable Relevance interaction.

The first page for interacting with a Location is the **Relevance Options** page of the Terminal Configuration Wizard. This page lets you select what Resolver methods you want to use to interact with the Location. These are listed in the ***Enable Resolver Types***.



Relevance Options

Select the Resolvers you want to use, including the ***Allow selection of Location manually*** checkbox.

Note: You can start with one Resolver Type selected and add the others as you deploy them, or start with all the Resolver Types selected and remove the ones you chose not to use. The central management of ThinManager and Relevance make changes to configuration easy.

Enable Resolver Types – Relevance has several methods of resolving the location to allow specific applications to get sent to specific locations.

- ***Enable QR Code Location Ids*** – This allows the scanning of a QR code to determine the location.
- ***Enable Bluetooth Locations*** – This allows the use of Bluetooth beacons to determine the location.
- ***Enable GPS Locations***– This allows the Global Positioning System of the mobile device to determine the location.
- ***Enable Wi-Fi Locations*** – This allows the signal strength of Wi-Fi access points to determine the location.

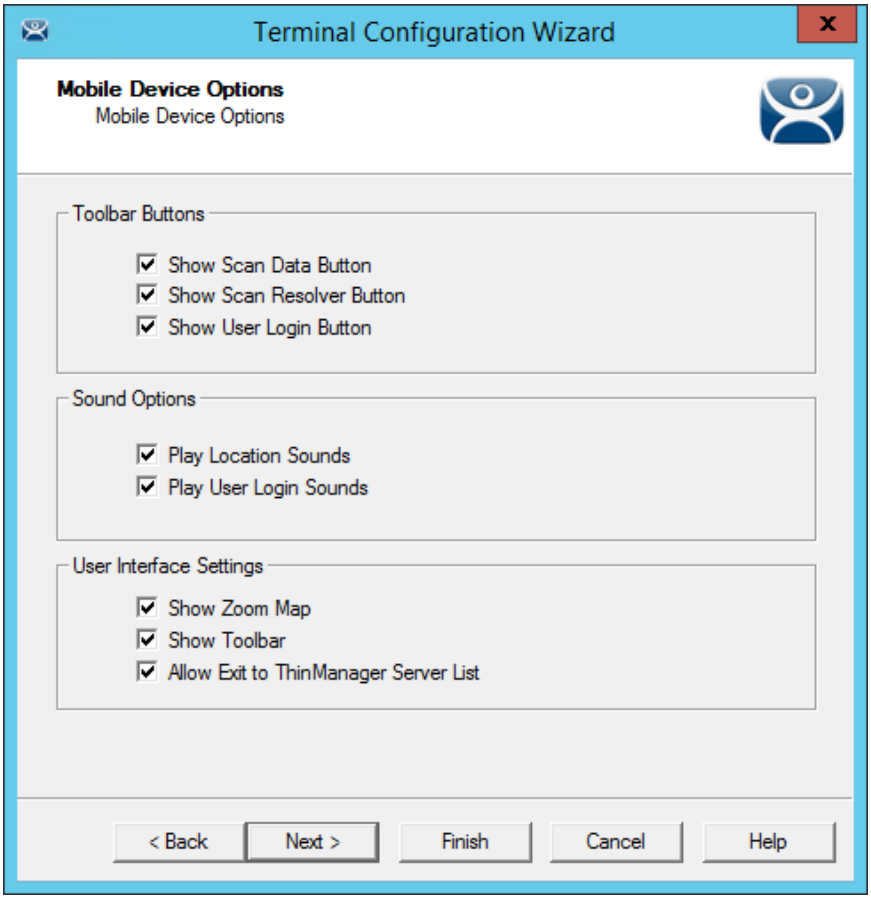
Each method selected will require configuration to associate a location with the Resolver data.

The **Options** include:

- ***Use Force Transfer to restore Assigned Location*** – This gives the operator to take a transferred session back without having to wait for the other device to approve of the transfer.
- ***Allow Selection of the Location manually*** – This will let the user select the location manually from a menu on the mobile device. If this is unselected then the user must use a Resolver.

- ***Use Force Transfer to restore Assigned Location*** – This gives the operator to take a transferred session back without having to wait for the other device to approve of the transfer.
- ***Enforce fencing on manual Location selection*** – This enforces the fencing on a location during manual selection.
- ***Confirm before entering a location*** – This notifies you as you enter a fence and asks for an acknowledgement.

Select ***Next*** to navigate to the **Mobile Device Options** page.



Mobile Device Options

The **Mobile Device Options** window has several settings that control the user experience on mobile devices. This page allows you to disable features normally displayed in the mobile apps.

Toolbar Buttons

- ***Show Scan Data Button*** – This checkbox, when unselected, will hide the Scan Data button.
- ***Show Scan Resolver Button***– This checkbox, when unselected, will hide the Scan Resolver button.
- ***Show User Login Button***– This checkbox, when unselected, will hide the User Login button.

Sound Options

- ***Play Location Sounds*** – This checkbox, when selected, will play a sound when a location is entered.

- ***Play User Login Sounds*** – This checkbox, when selected, will play a sound when the user logs in as a Relevance or Relevance user.

User Interface Settings

- ***Show Zoom Map*** – This checkbox, when unselected, will hide the screen map while zooming.
- ***Show Toolbar*** – This checkbox, when unselected, will hide the app toolbar.
- ***Allow Exit to ThinManager Server List*** – This checkbox, when unselected, will prevent the user from leaving the app to switch ThinManager Servers.

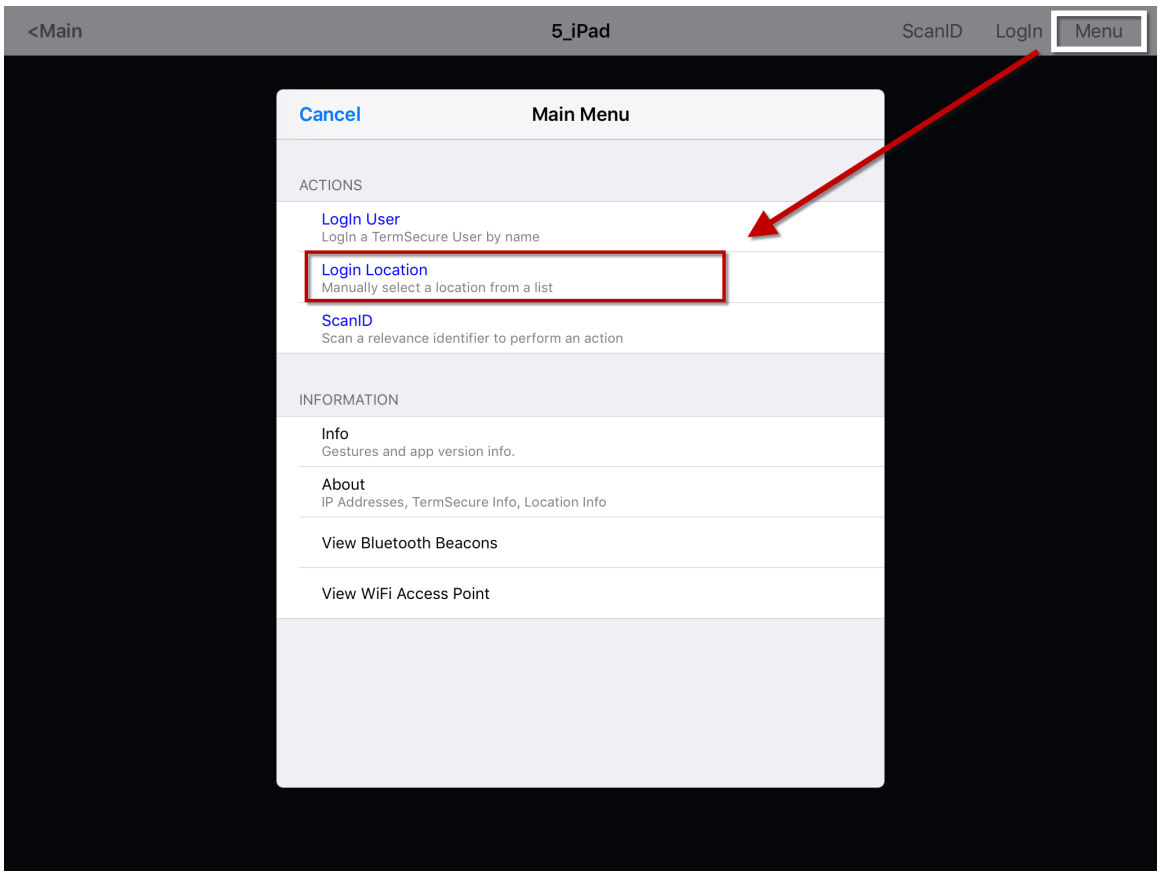
Select ***Finish*** to complete the configuration of the mobile Terminal.

38. Manual Interaction with Locations

A mobile device can connect to a **Location** and manually interact with the applications.

Connect the mobile device to the ThinServer and connect as shown in Devices – Mobile Devices on page 321.

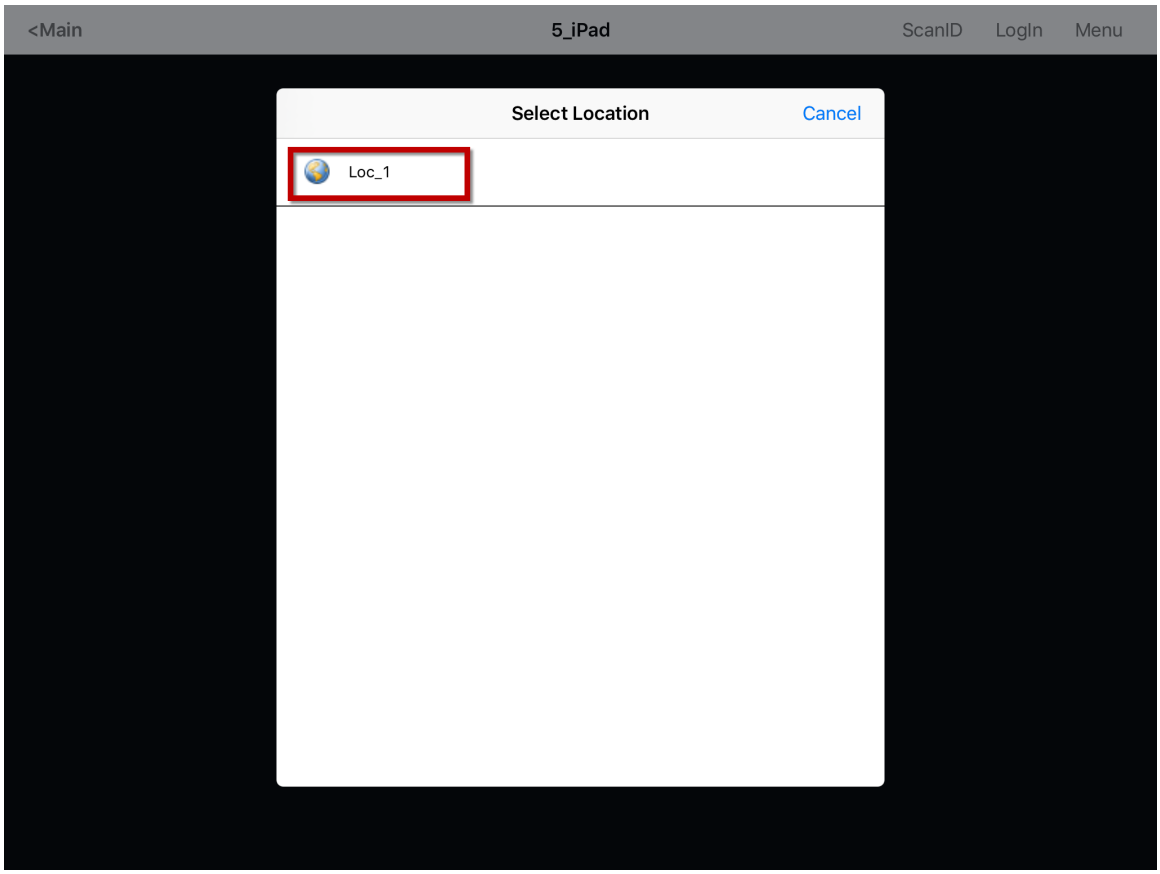
The Main Menu can be launched from the mobile device menu bar.



Main Menu on a Mobile Device

The ***Login Location*** is the command to manually connect to a Location.

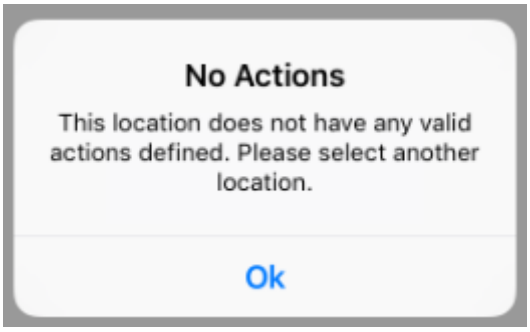
Selecting ***Login Location*** will open the **Select Location** window.



Select Location

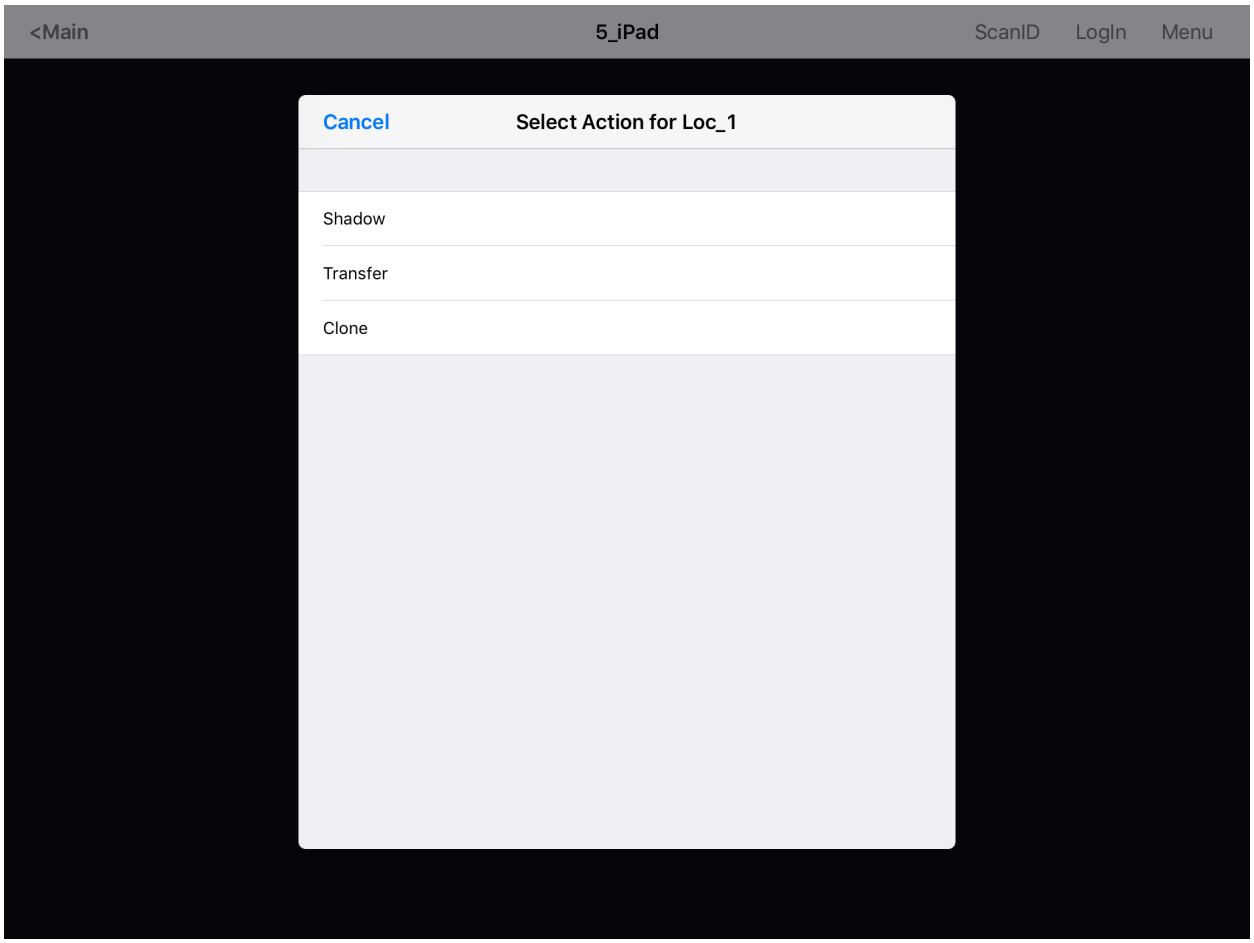
The **Select Location** window will list all Locations that are allowed to have a manual configuration. In this example only one Location has been created.

Selecting the **Location** will open the **Select Action** window.



No Actions Error

The ***No Actions*** error means that either there were no ***Actions*** checked on the **Location Options** page of the **Location Configuration** wizard, or a Relevance Permission has been applied and the user isn't a member of a permitted access group.



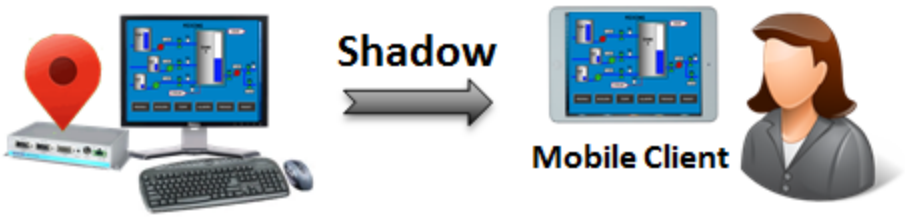
Actions for Manual Interaction

The three manual interactions between a mobile device and a location are:

- **Shadow** – Shadowing duplicates the graphic output of the Location screen and sends it to the mobile device.
- **Transfer** – Transferring sends the graphic output of the location to the mobile device instead of the location. This requires the operator to manually allow the transfer.
- **Clone** – Cloning will create a duplicate session for the mobile device using the configuration of the location and the user credentials of the mobile device.

38.1. Shadow

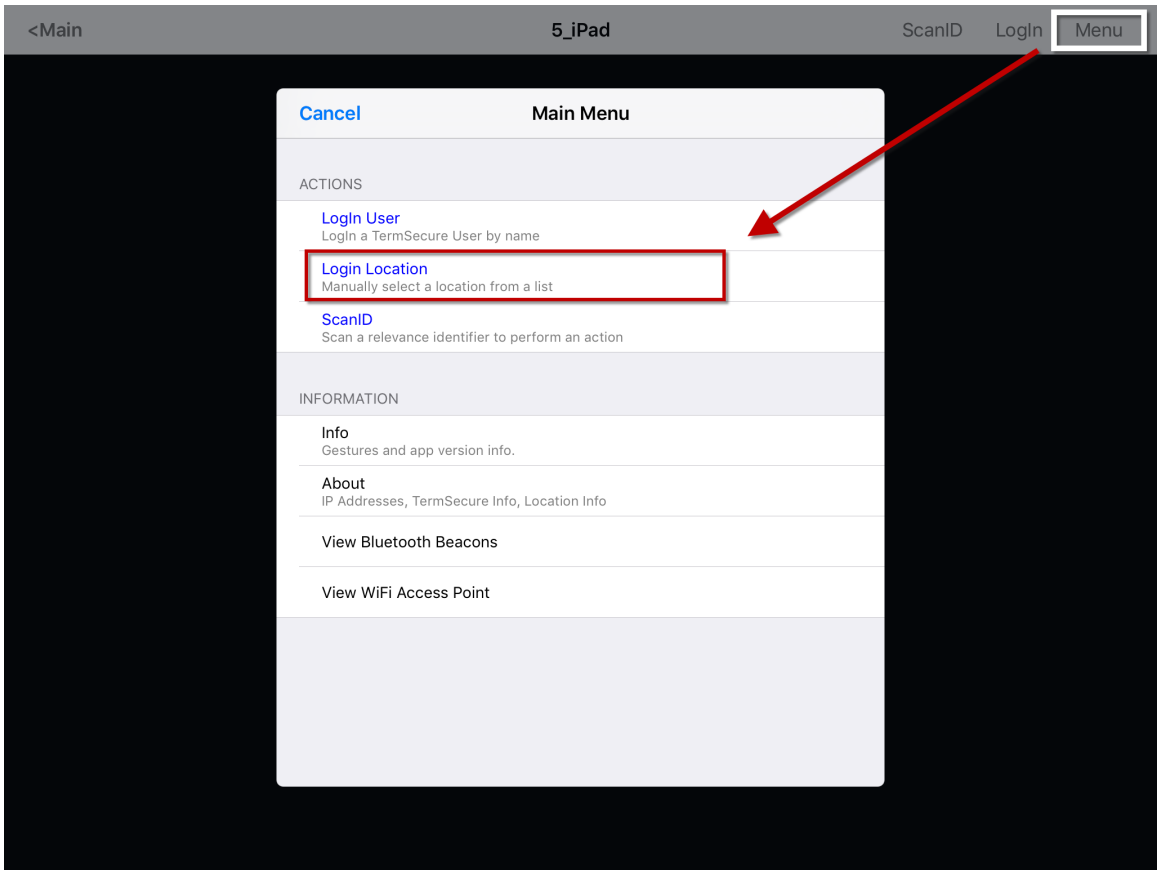
Shadowing duplicates the graphic output of the location and sends it to the mobile device.



Shadowing

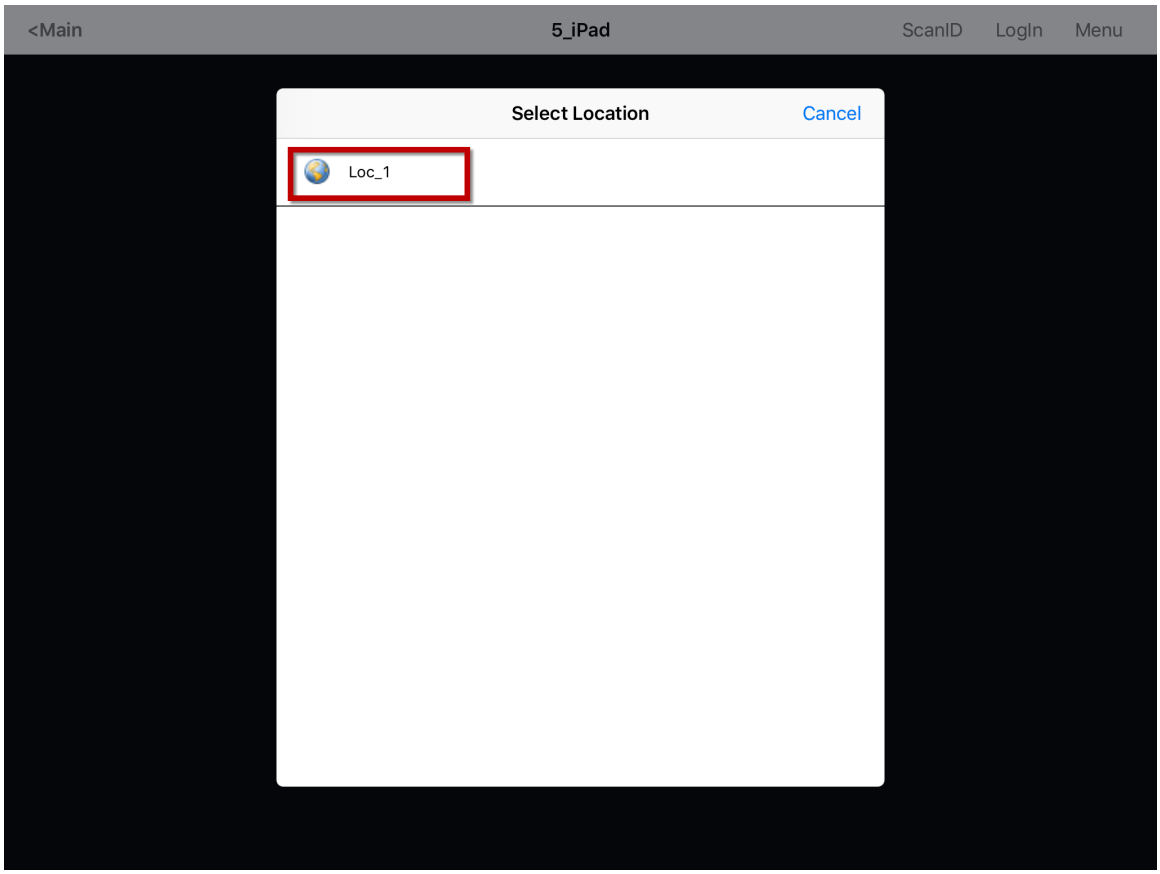
The mobile user will see the exact display as the location.

Open the mobile program, select your ThinManager Server, and touch the ***Menu*** button in the upper right corner to launch the **Main Menu** window.



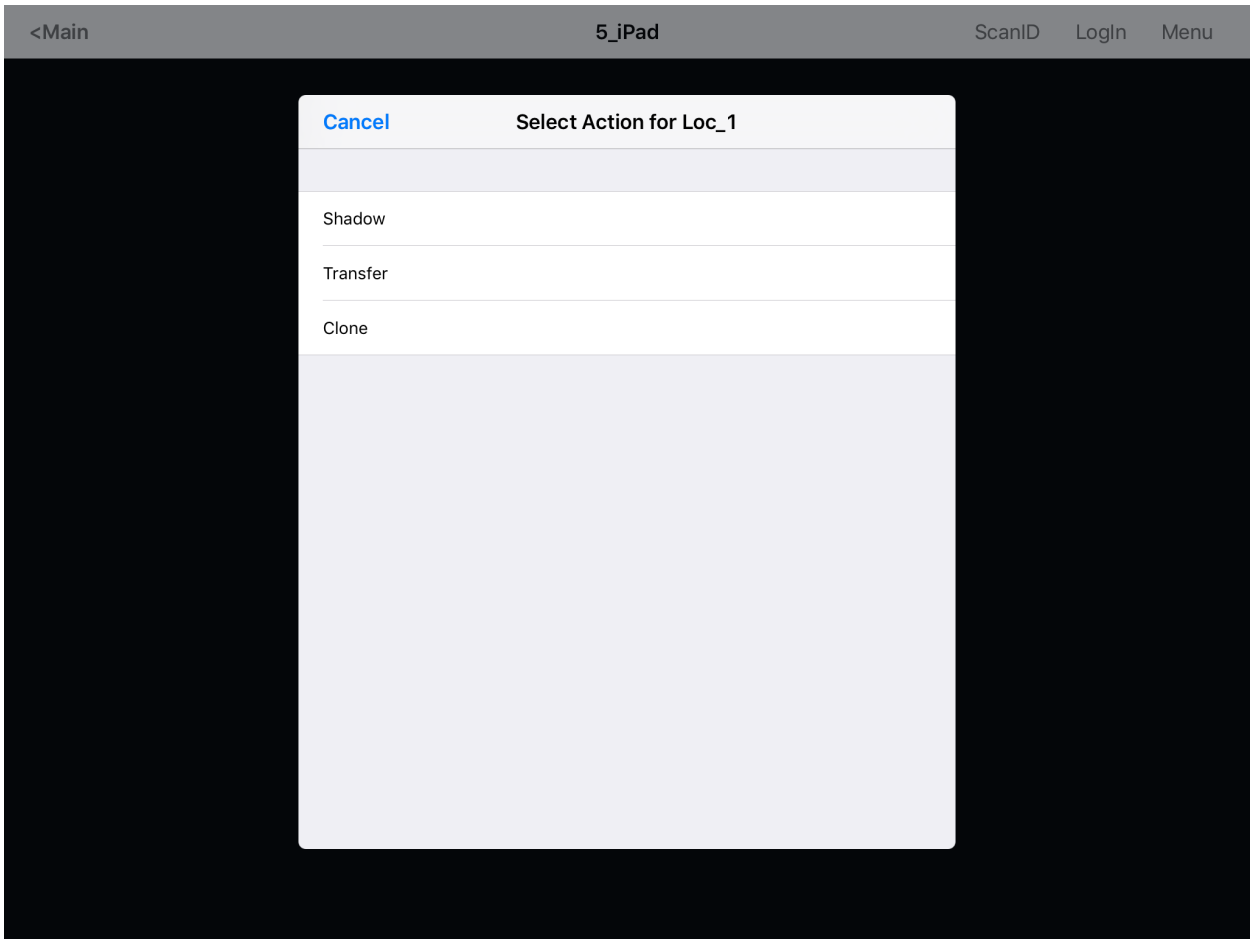
Main Menu

Touch the ***Login Locations*** on the menu to open the **Select Location** window.



Select Location Menu

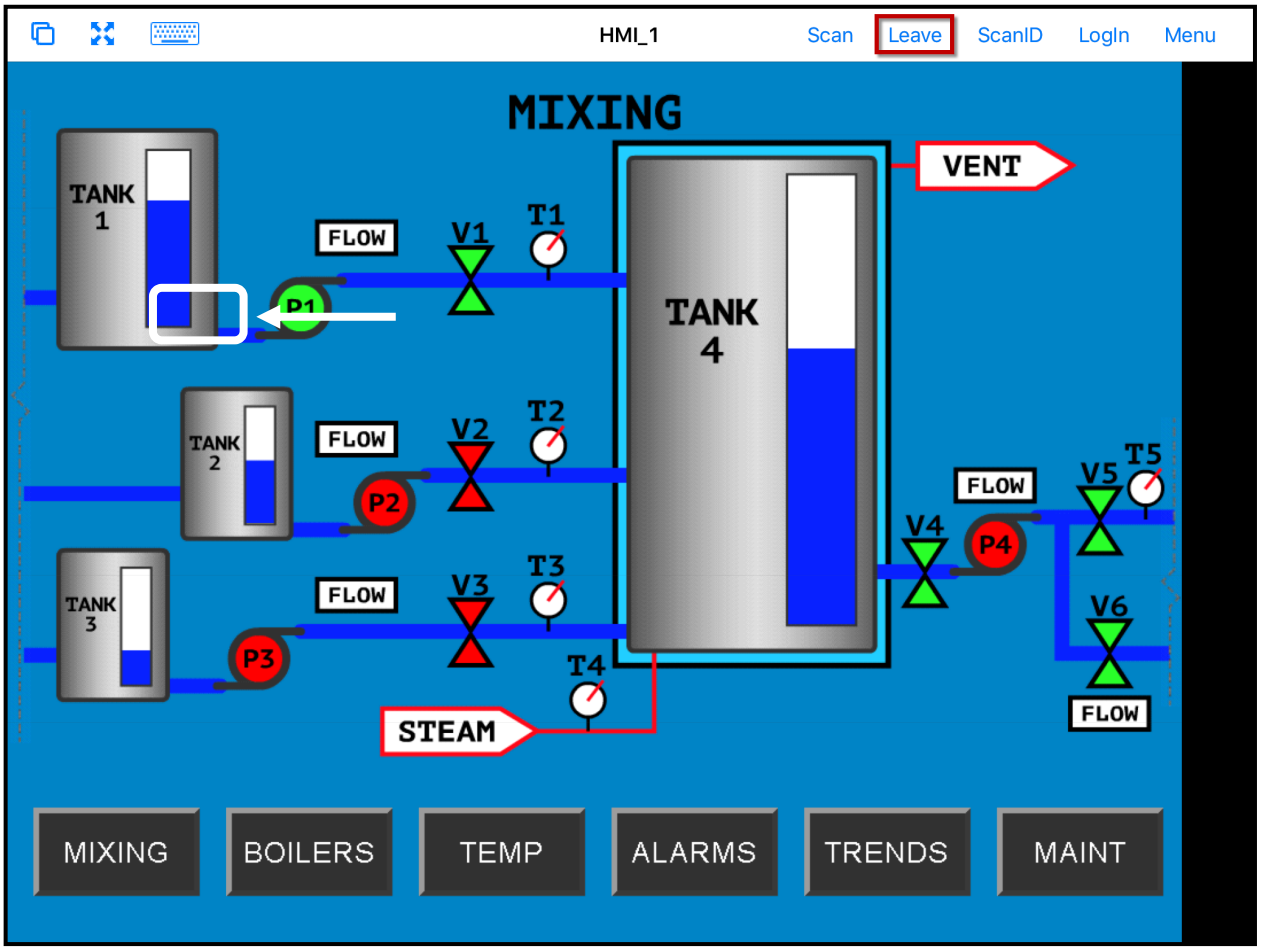
Select a Location to open the **Select Action** window.



Select Action Window

The **Select Action** window will list the actions that are allowed at the location.

Touch ***Shadow*** to connect and shadow the Location.



iTMC Shadowing Location

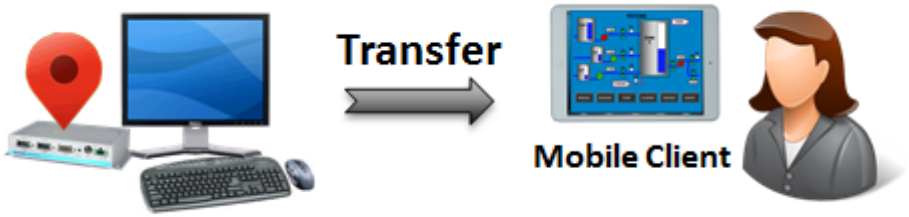
The screen will show the shadow of the location.

The shadow will only show one display client window because you are shadowing the location and are receiving the current graphic output from the location.

Touch ***Leave*** to end the shadow.

38.2. Transfer

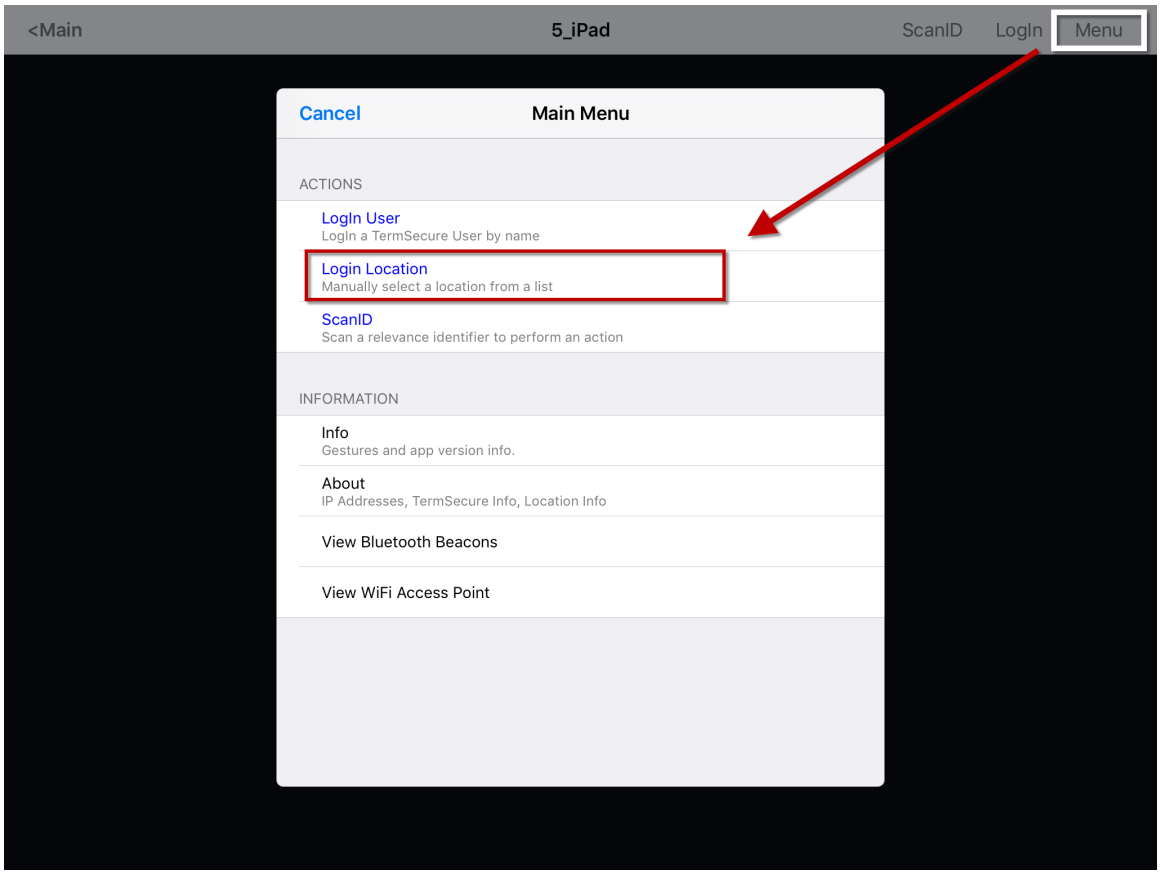
Transfer is similar to Shadow except that the user has to allow the transfer at the location.



Transfer

This prevents someone from taking the session while the operator is busy with a process. It also allows a mobile user to take sole control of the location.

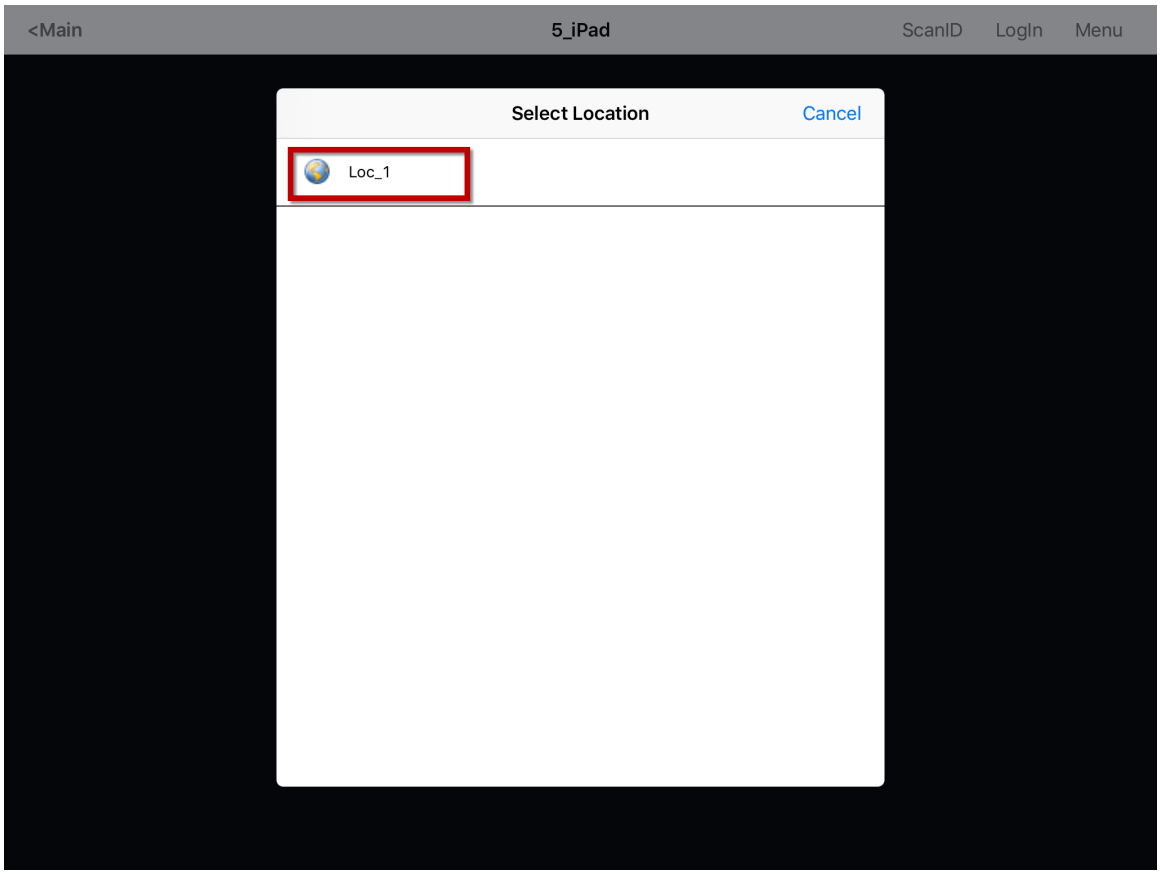
Open the mobile program, select your ThinManager Server, and touch the ***Menu*** button in the upper right corner to launch the **Main Menu** window.



Main Menu on a Mobile Device

The ***Login Location*** is the command to manually connect to a Location.

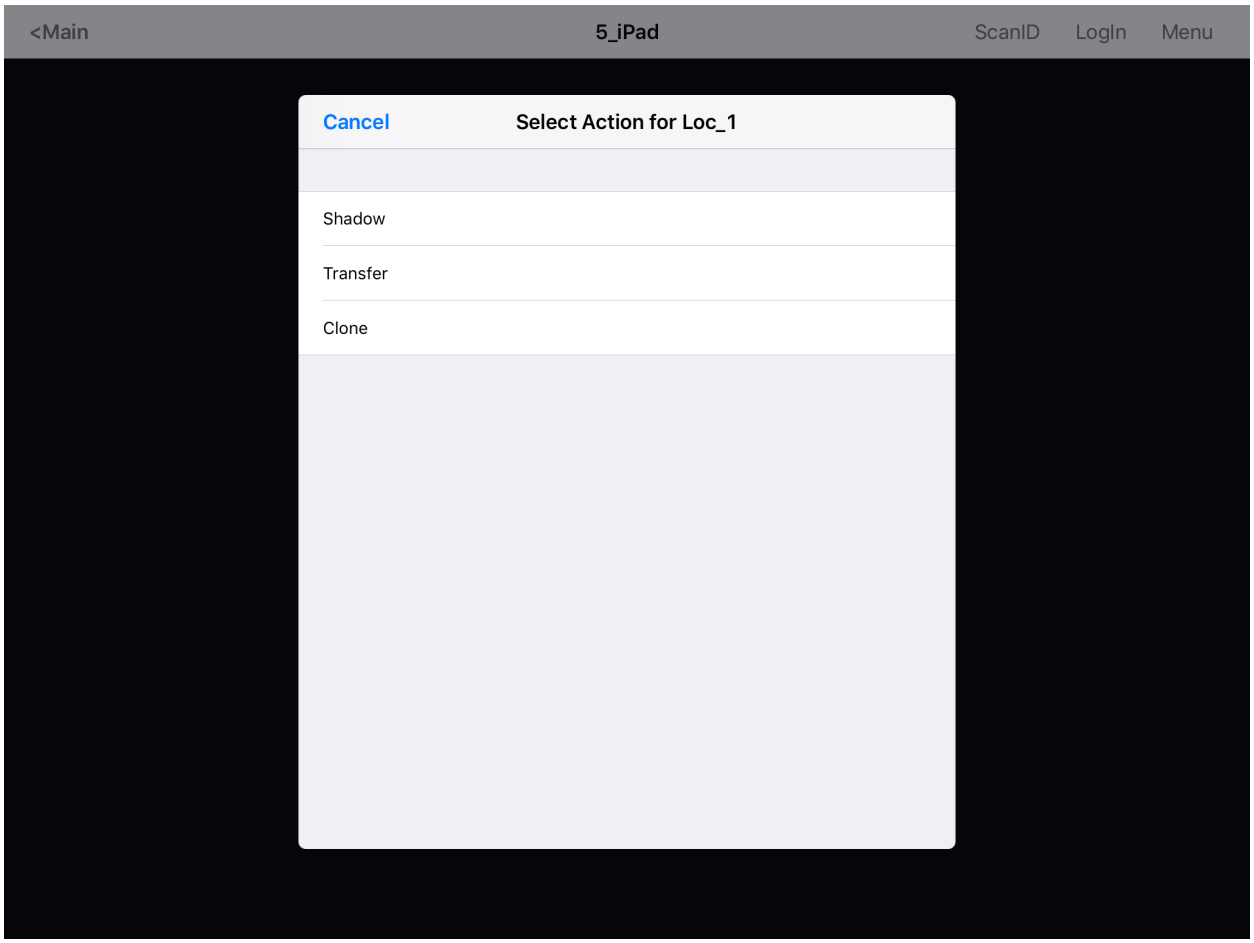
Selecting ***Login Location*** will open the **Select Location** window.



Select Location

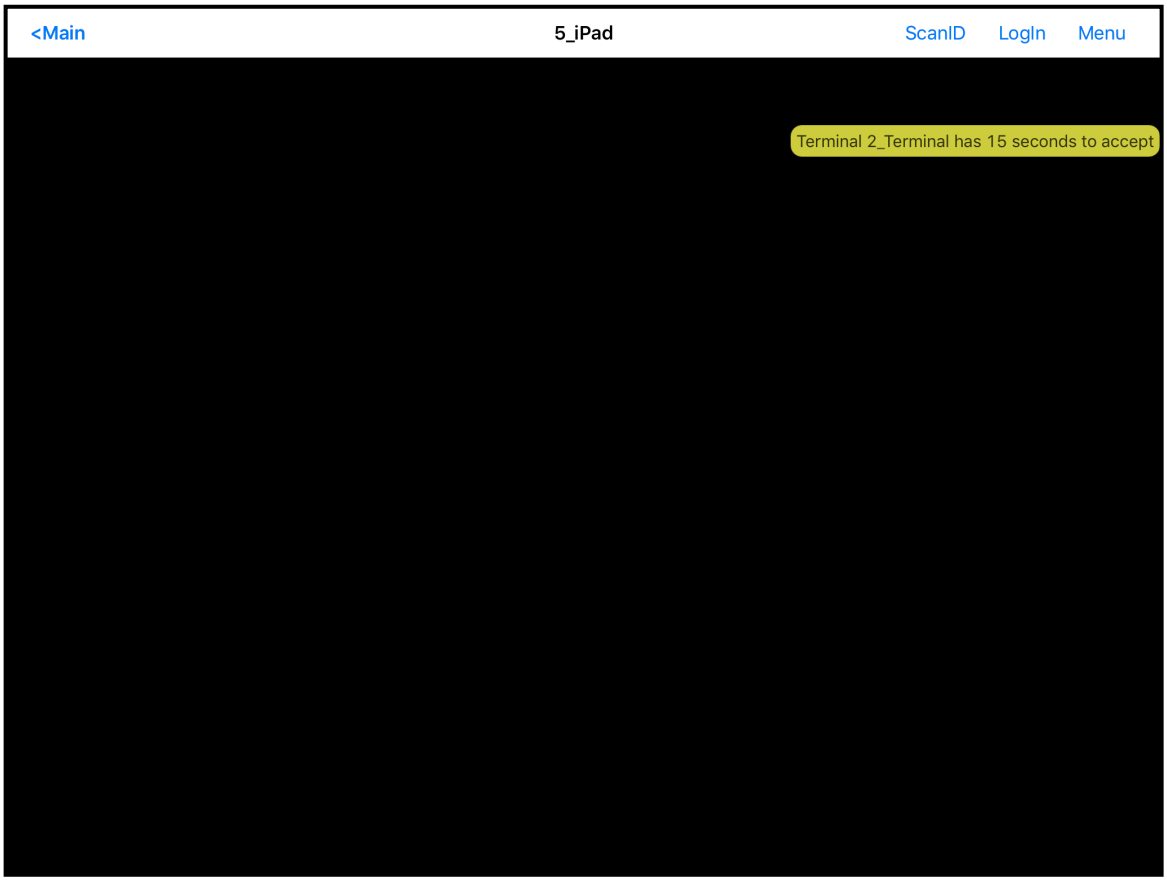
The **Select Location** window will list all Locations that are allowed to have a manual configuration. In this example only one Location has been created.

Selecting the **Location** will open the **Select Action** window.



Actions for Manual Interaction

Select ***Transfer*** from the **Select Action** window.

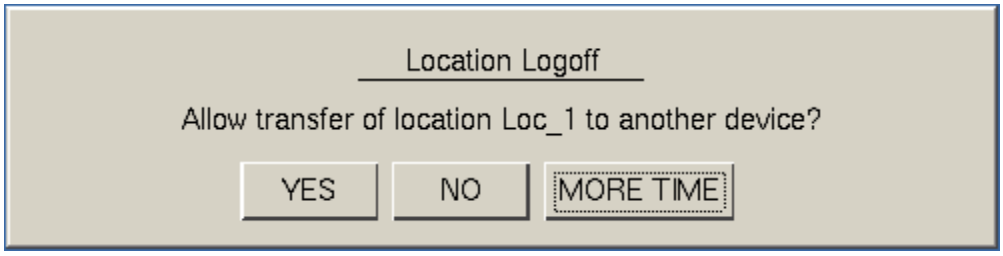


Wait for Transfer Permission Message

The user of the location will need to allow the transfer. This “handshake” prevents the mobile user from taking the session while the local user is performing a task.

38.2.1. Transfer at the Location

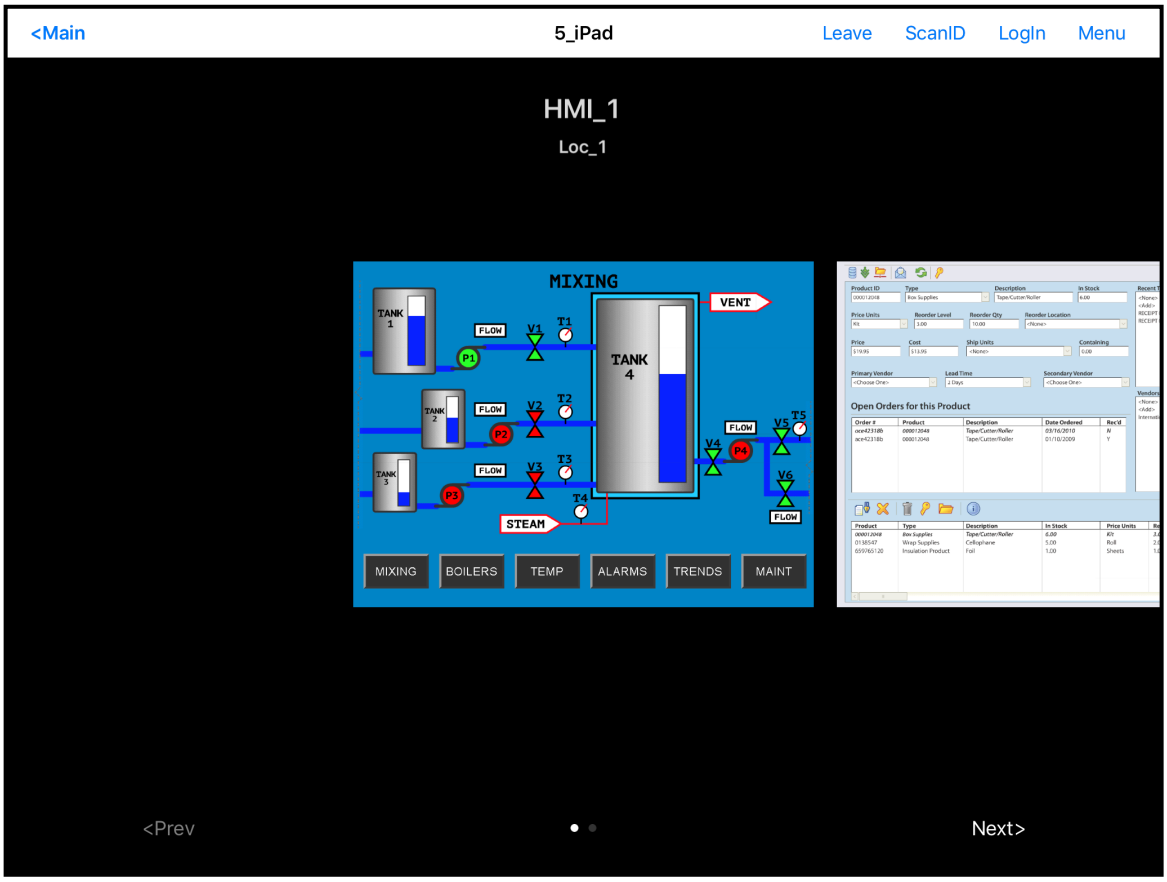
A dialog box will be displayed at the location to allow the transfer.



Location Logoff Dialog Box

The local user needs to select the ***Yes*** button to allow the transfer.

The mobile client will be allowed to display the location display.



Transferred Location Display

The Transfer will show all the display clients on the location instead of just showing the display output of the location

The location display can be restored from the iTMC client or the location.

Selecting the ***Leave*** button on the iTMC client menu will restore the display back to the location.

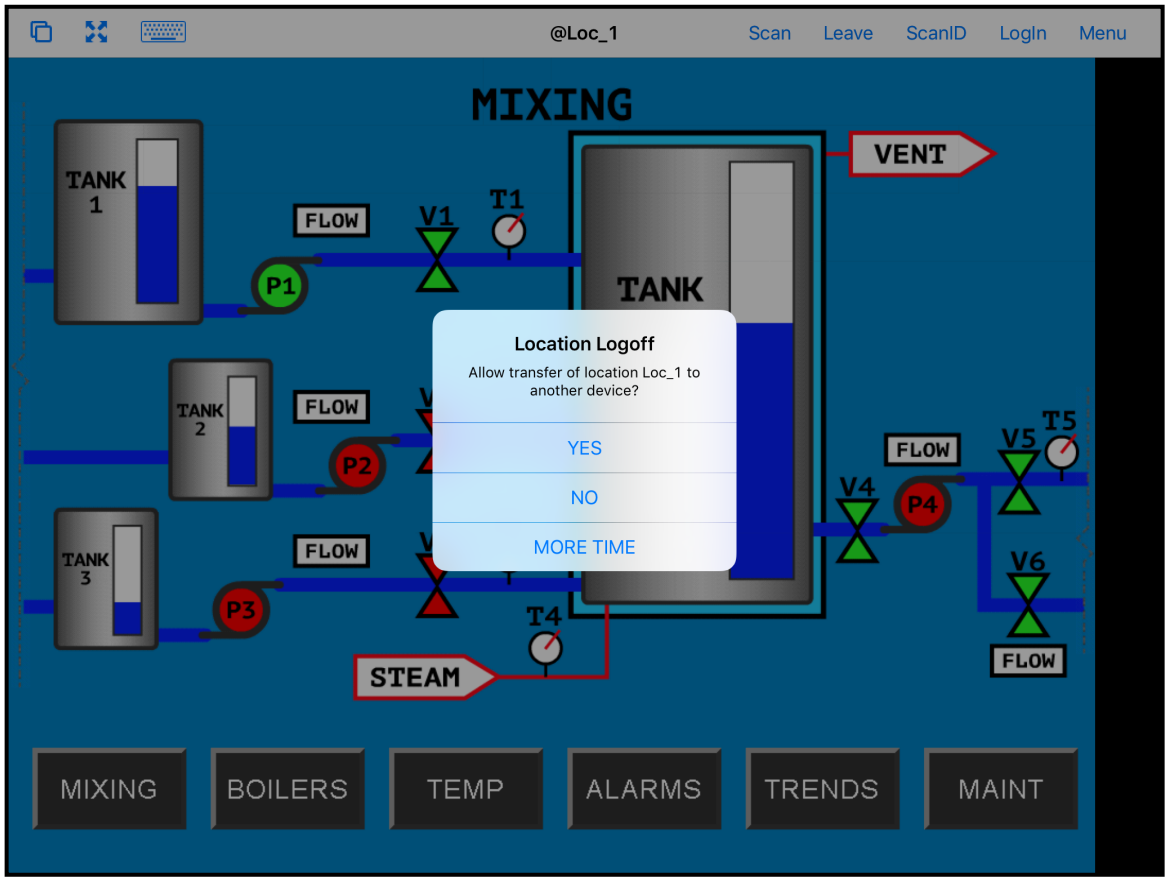
Selecting the ***Restore Location*** button at the location will also restore the display.

Main Menu at the Location

The Location will display the Main Menu during the transfer.

The session can be returned by selecting the ***Restore Location*** button.

This will launch a dialog box on the mobile client to warn the mobile user that they will be losing the transfer.



Location Logoff Dialog

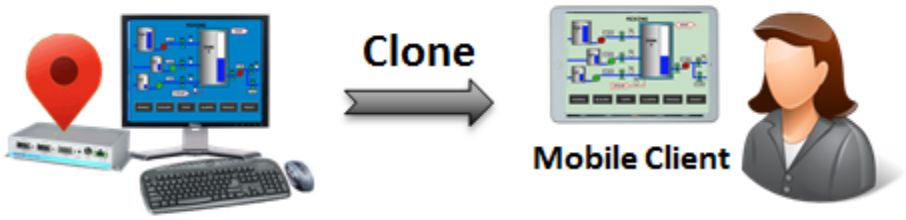
When the user at the location selects the ***Restore Location*** button a warning message will be sent to the mobile device.

The mobile user can select ***Yes*** to allow the transfer back to the original location, ***No*** to refuse the restoration, or they can select the ***More Time*** button to delay the restoration.

The amount of time that an operator has to acknowledge and allow the transfer can be set on the Relevance Setting window. See Bluetooth Beacons on page 632 for details.

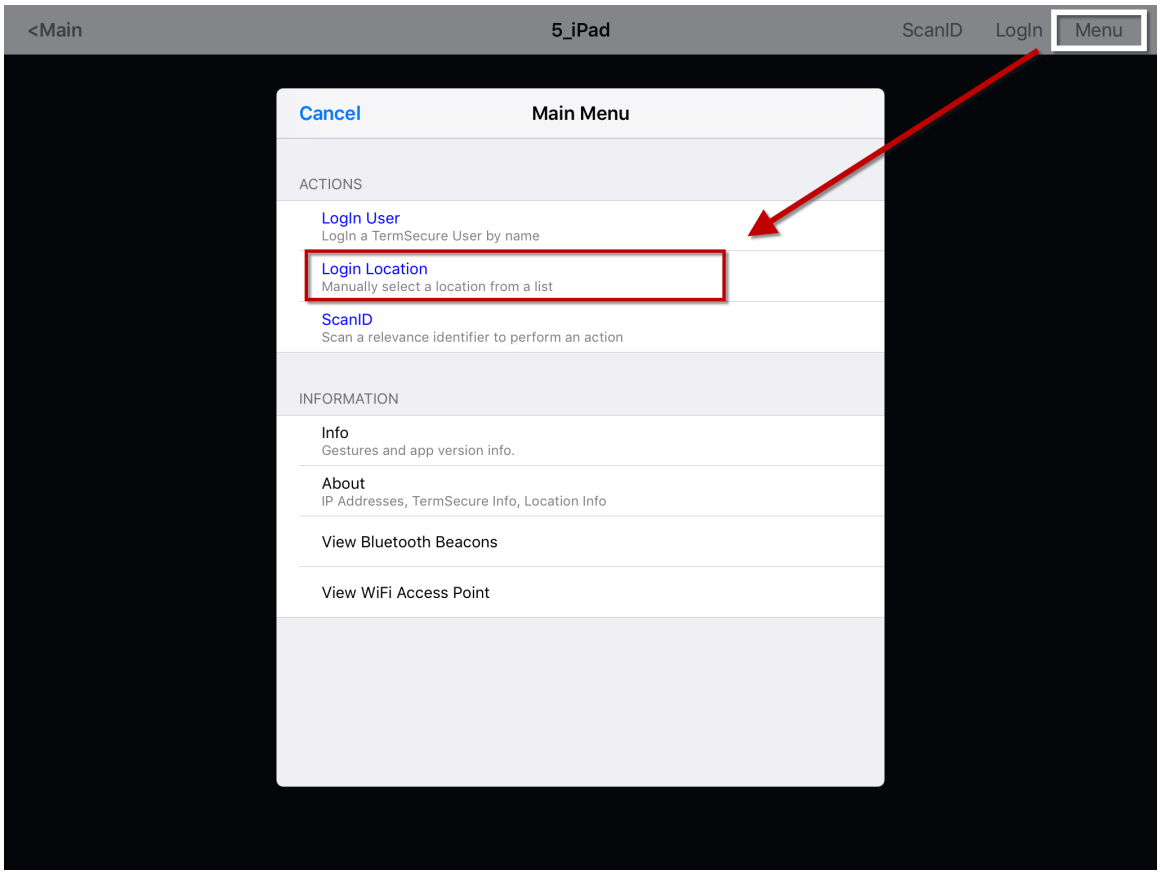
38.3. Clone

Clone will duplicate the display clients of the location on the mobile device but the sessions will be created with the mobile device Windows user account.



Clone

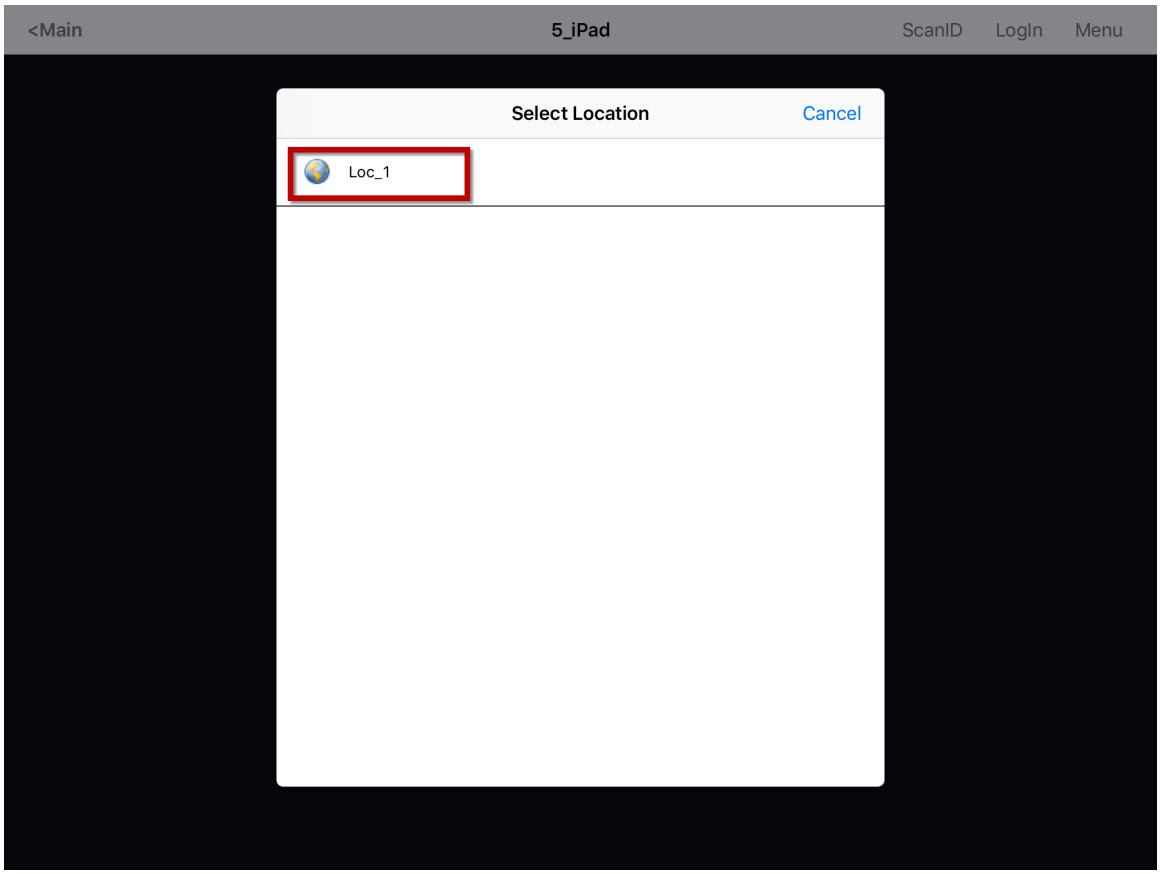
This allows a mobile user to get the HMI or other software and have independence from the user at the location.



Main Menu on a Mobile Device

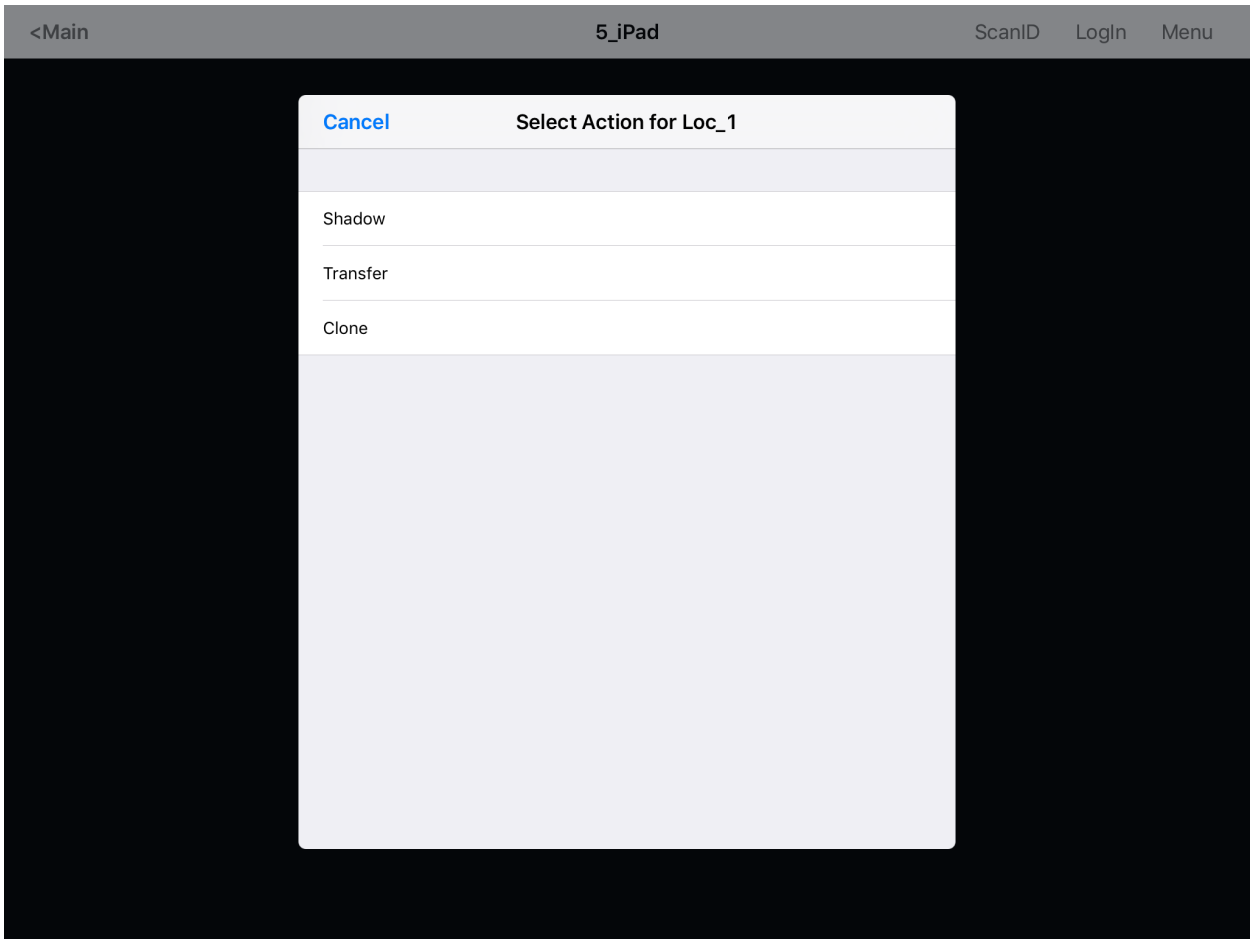
The ***Login Location*** is the command to manually connect to a Location.

Selecting ***Login Location*** will open the **Select Location** window.



Select Location

The **Select Location** window will list all Locations that are allowed to have a manual configuration. In this example only one Location has been created.

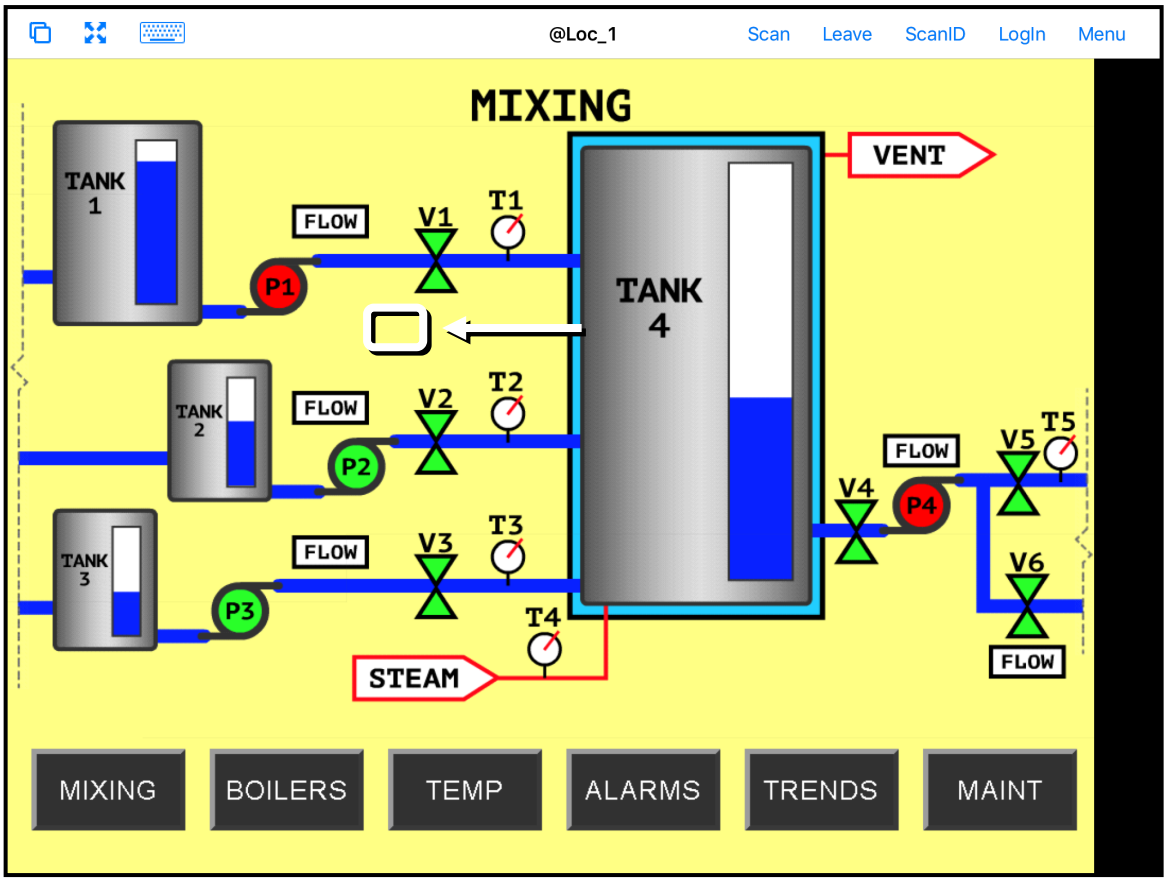


Actions for Manual Interaction

The three manual interactions between a mobile device and a location are:

- **Shadow** – Shadowing duplicates the graphic output of the Location screen and sends it to the mobile device.
- **Transfer** – Transferring sends the graphic output of the location to the mobile device instead of the location. This requires the operator to manually allow the transfer.
- **Clone** – Cloning will create a duplicate session for the mobile device using the configuration of the location and the user credentials of the mobile device.

Select the Clone action. The mobile device will launch copies of the location's display clients but use the mobile device login.



Cloned Session

This shows a session running the same application but with a different set of credentials.

Touch ***Leave*** in the top corner to close the mobile client.

39. Using the Mobile Device to Add Resolver Codes

Resolvers help a mobile device know what location it is in. These can be configured to tell the mobile device what action to take.

Resolvers include

- QR Codes
- Bluetooth Beacons
- Wi-Fi Access Points
- GPS

Assignment of Resolvers

Because Resolvers can only be assigned to one location they identify the Location for Relevance. Each location can have more than one Resolver and action assigned. You may use Permissions and assign a resolver several times with a different action tied to each set of permissions.

Fencing uses combinations of resolvers to limit actions to specific locations. An action may require being in an area can be covered by a Bluetooth beacon of GPS site before a QR code can be scanned. This can prevent a user from walking away from an area with a critical process. The Fence prevents the user from running the application out of the assigned areas.

39.1. QR Codes

Quick Response Codes are an improved form of barcode. They can store text, numeral data, and URLs. These can be read quickly and easily. There are many programs which generate them, including free sites on the web.

QR Codes provide pinpoint location as you need to be at the QR code to read it. This allows you a high degree of granularity in your configuration. You can put QR Codes anywhere, and not worry about overlap of signals or interference.

One issue with QR Codes is that they are easy to duplicate. If you want to use Relevance to limit an operator to a particular location then QR Codes should be coupled with other devices like Wi-Fi, GPS, or Bluetooth to provide fencing. See Fencing and Sub-Locations on page 697 for details.

The iTMC program and aTMC use the built in camera as a scanner to read the QR codes. The procedure is:

- Create the QR codes.
- Launch the iTMC program and select the ***Settings*** button.
- Select the Register QR Code command under Relevance Resolvers. If you have more than one ThinManager Server defined you will need to pick the ThinManager Server you want the QR code registered.
- Scan the QR code in the camera window.
- Enter a name and select Register.
- The QR code will be registered and entered in the **Resolver Management** window that is accessed by selecting ***Manage > Manage Resolvers***.

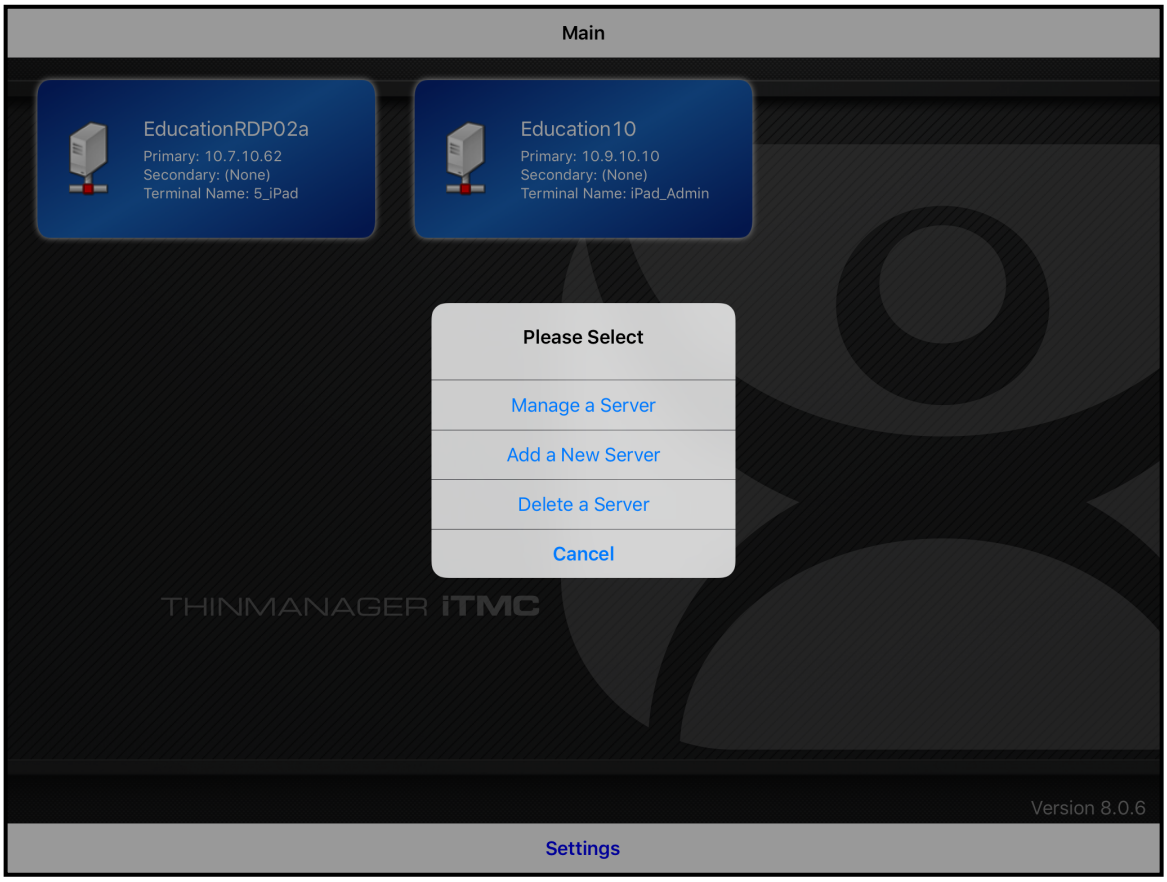
Sample QR Code

39.1.1. Registering QR Codes with an iPad

QR codes need to be registered with a mobile device

Open the iTMC program on the iPad.

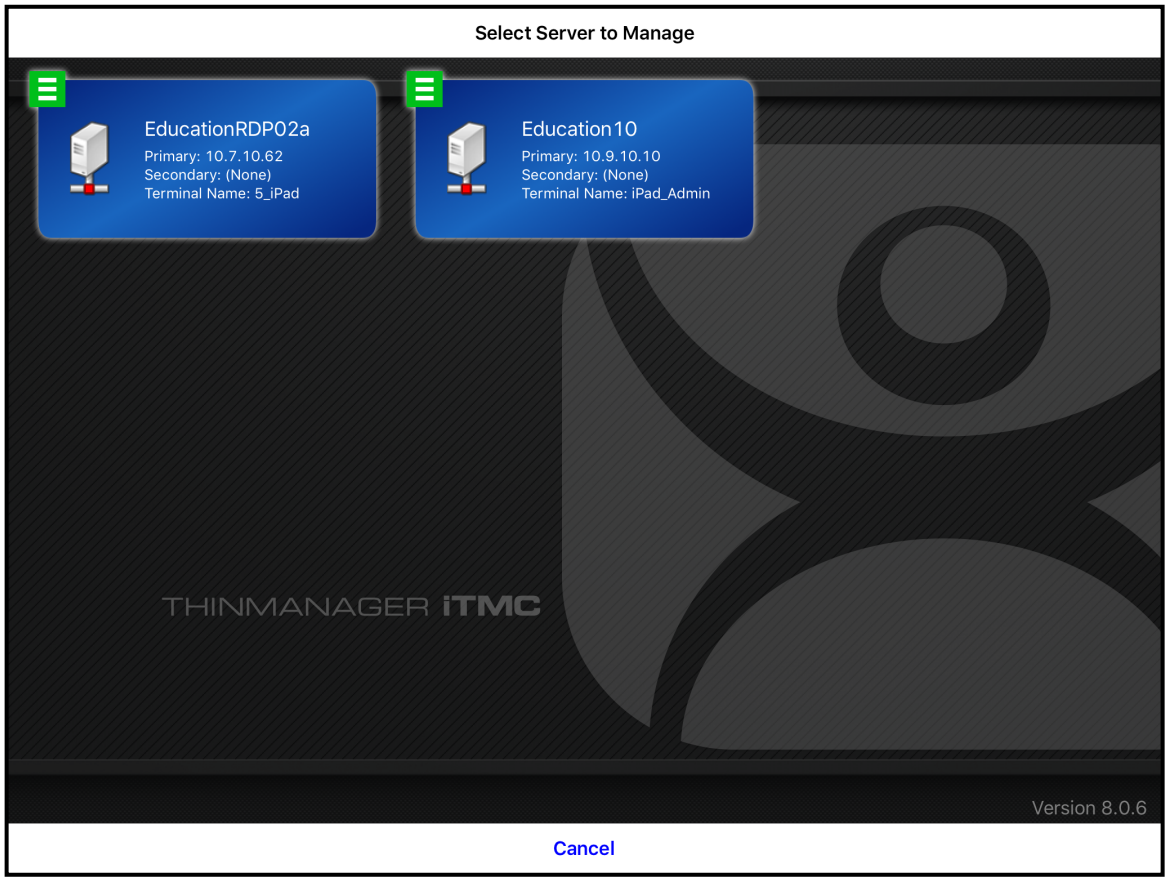
Select the ***Settings*** button on the bottom to launch the **Settings** screen.



iPad Setting Menu

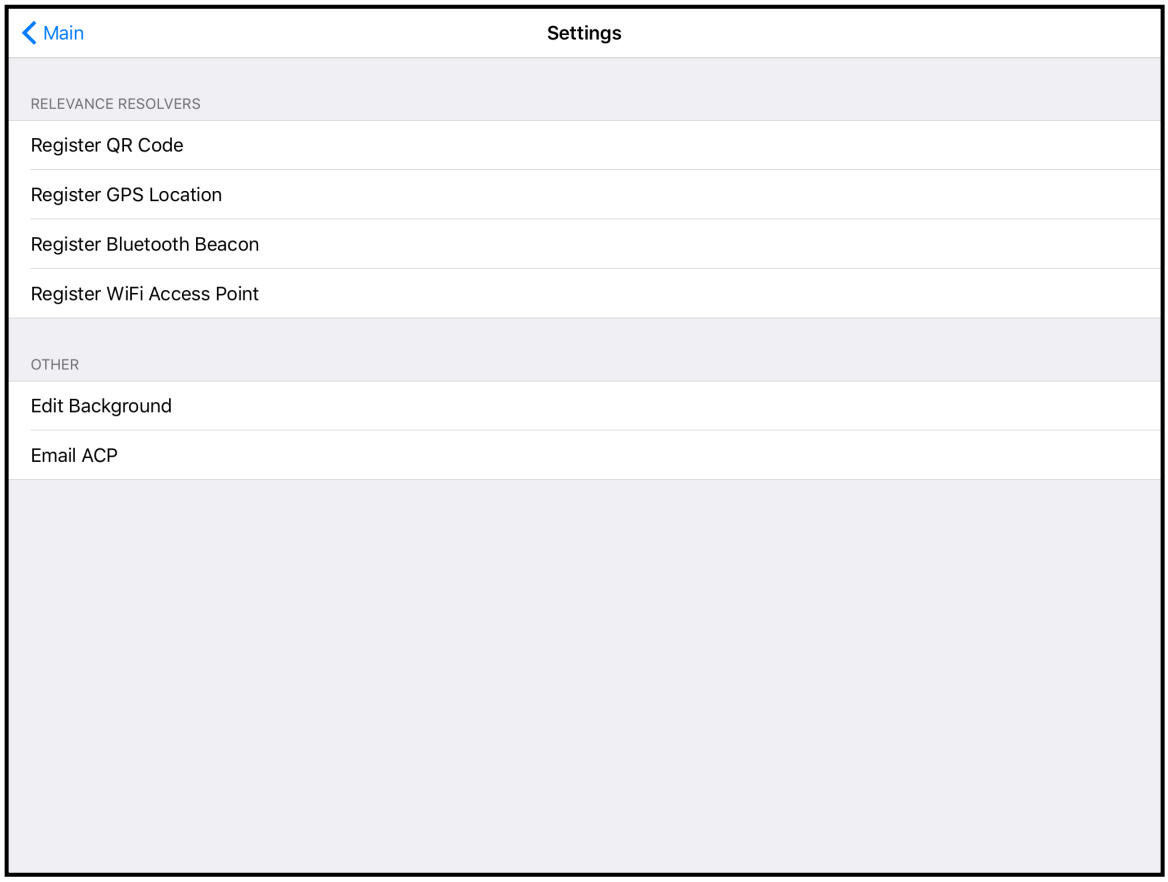
A selection menu will launch.

Select the ***Manage a Server*** link.



Select Server to Manage Screen

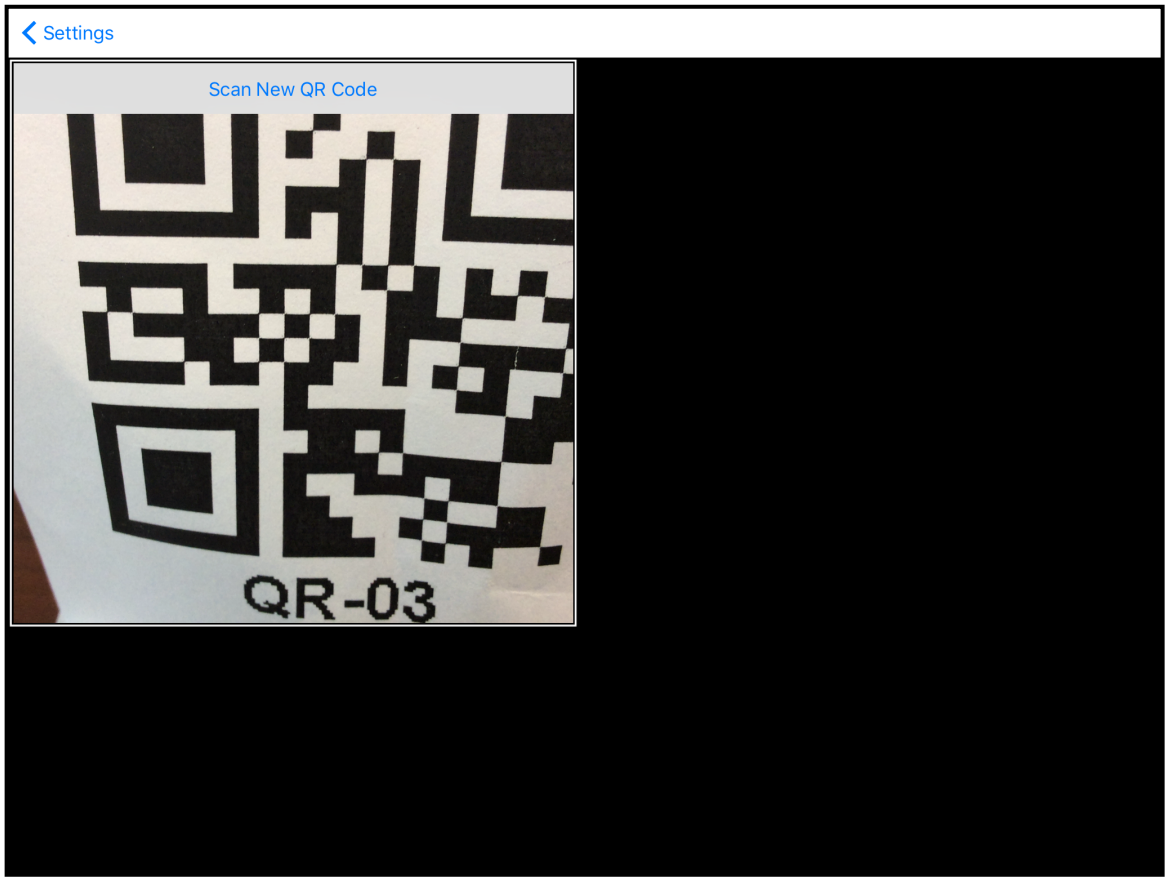
If you have multiple ThinManager Servers defined you will need to select the ThinManager Server that you want to apply the QR codes by selecting the correct server.



iTMC Settings Page

The **iTMC Settings** page has the links to register the various resolvers.

Select the ***Register QR Code*** link to open the camera to scan and register the QR code.



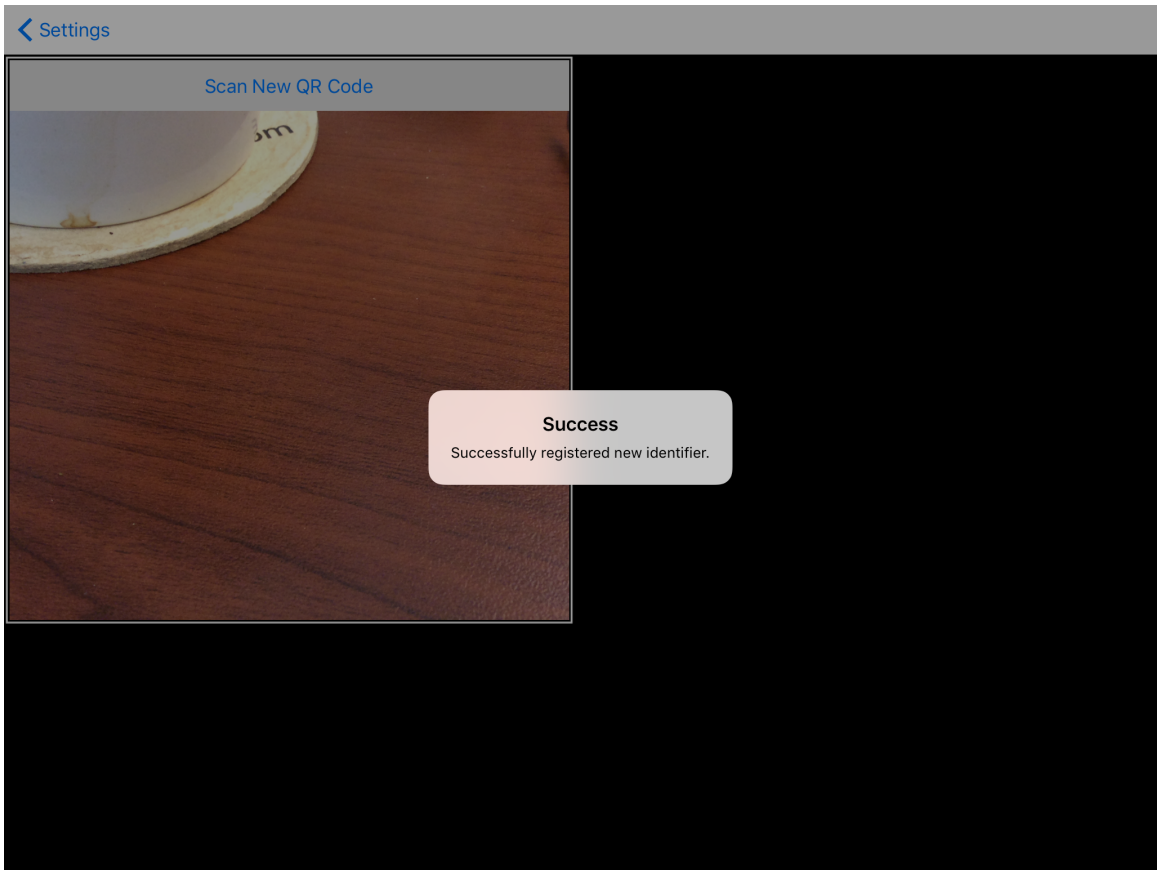
Scan New QR Code Window

Selectin the ***Register QR Code*** link will open the camera. Point the camera to the QR code. Once it is framed in the window it will read the code and register it.

Enter Description for QR Code

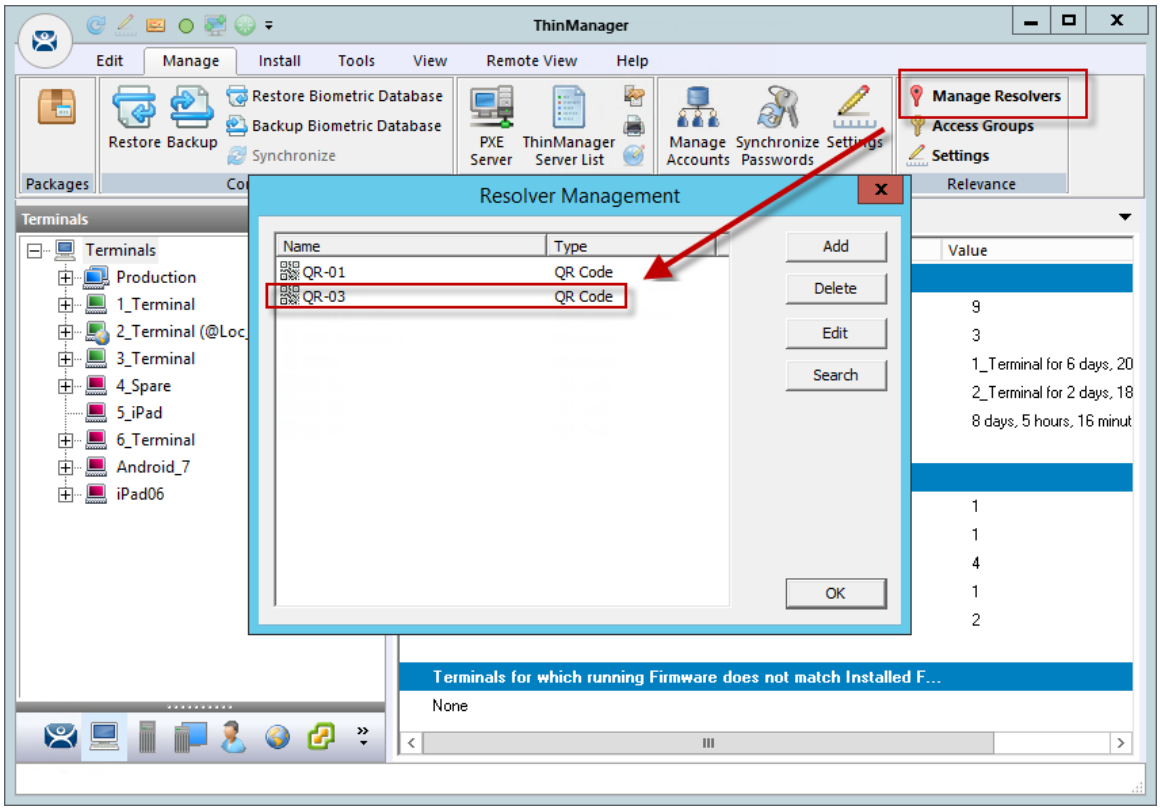
Once the iTMC program has read the QR code it will ask you to name it.

Enter a description in the **Enter Description** window.



Successful Registration Confirmation

The iTMC program will confirm a successful registration.



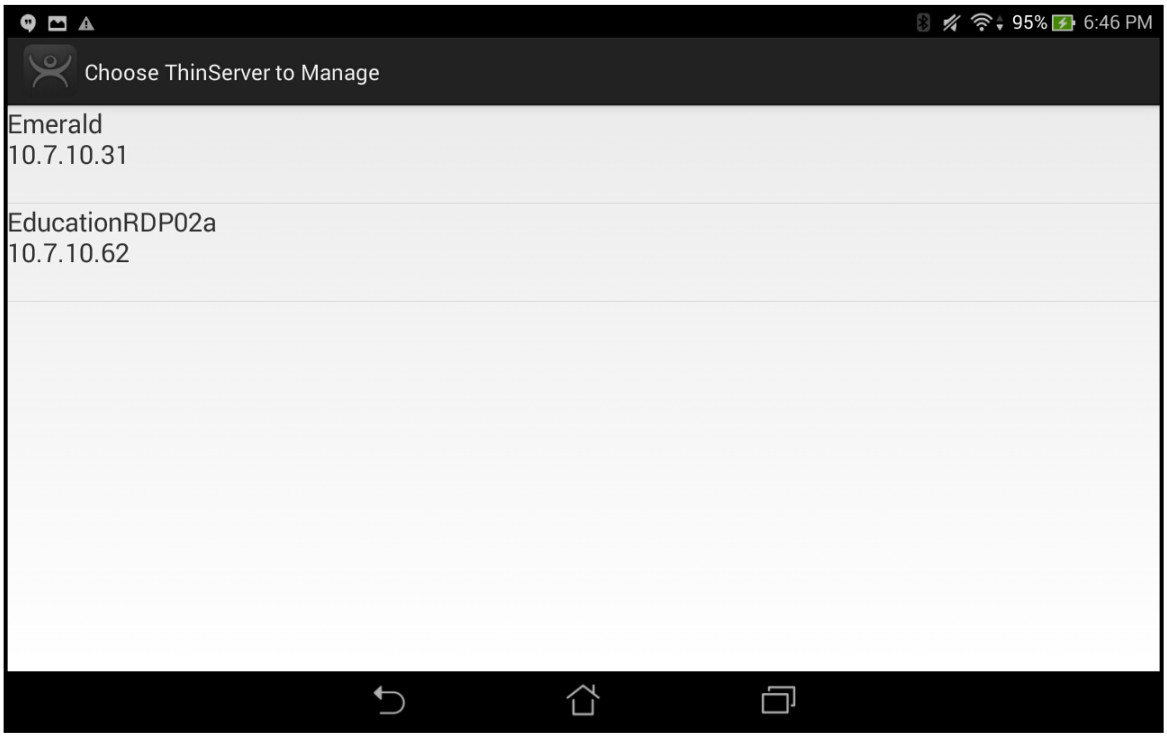
QR Code in Resolver Management Window

The Resolvers are listed in the **Resolver Management** window. This is opened by selecting ***Manage > Manage Resolvers*** from the ThinManager menu bar.

39.1.1. Registering QR Codes with an Android Device

QR codes need to be registered with a mobile device

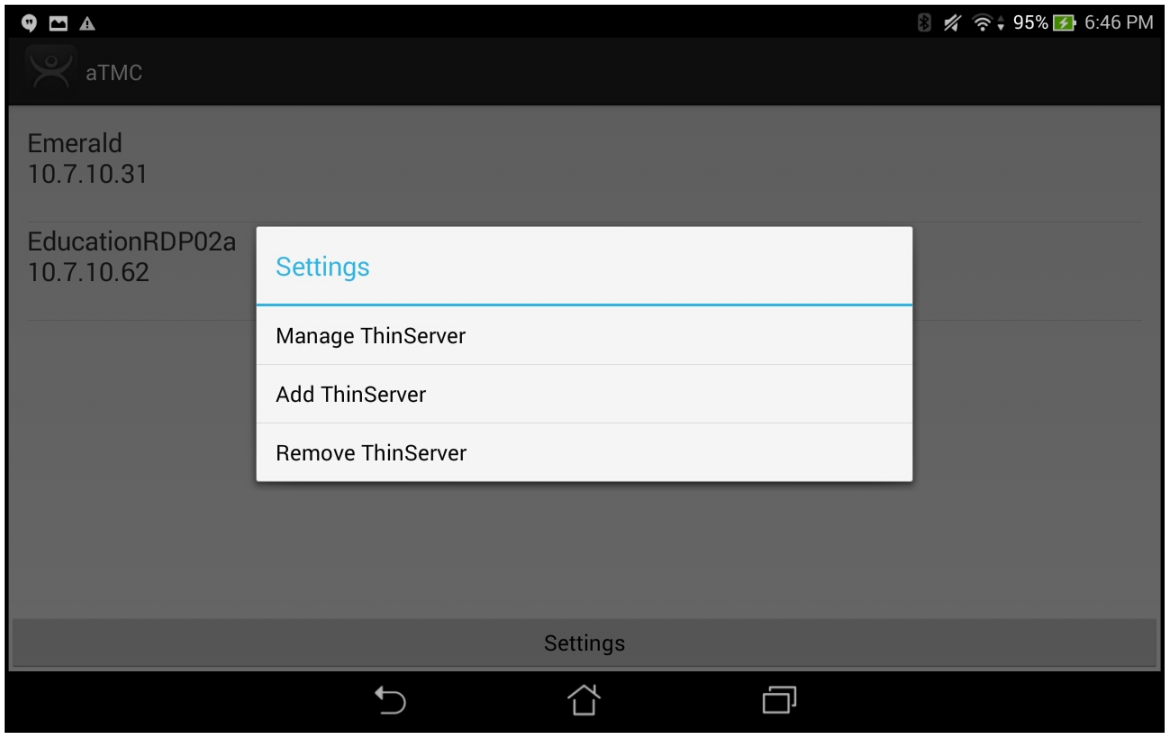
Open the aTMC program on the Android device



aTMC Home Screen

Select the ***Settings*** button on the bottom to launch the **Settings** screen.

A selection menu will launch.

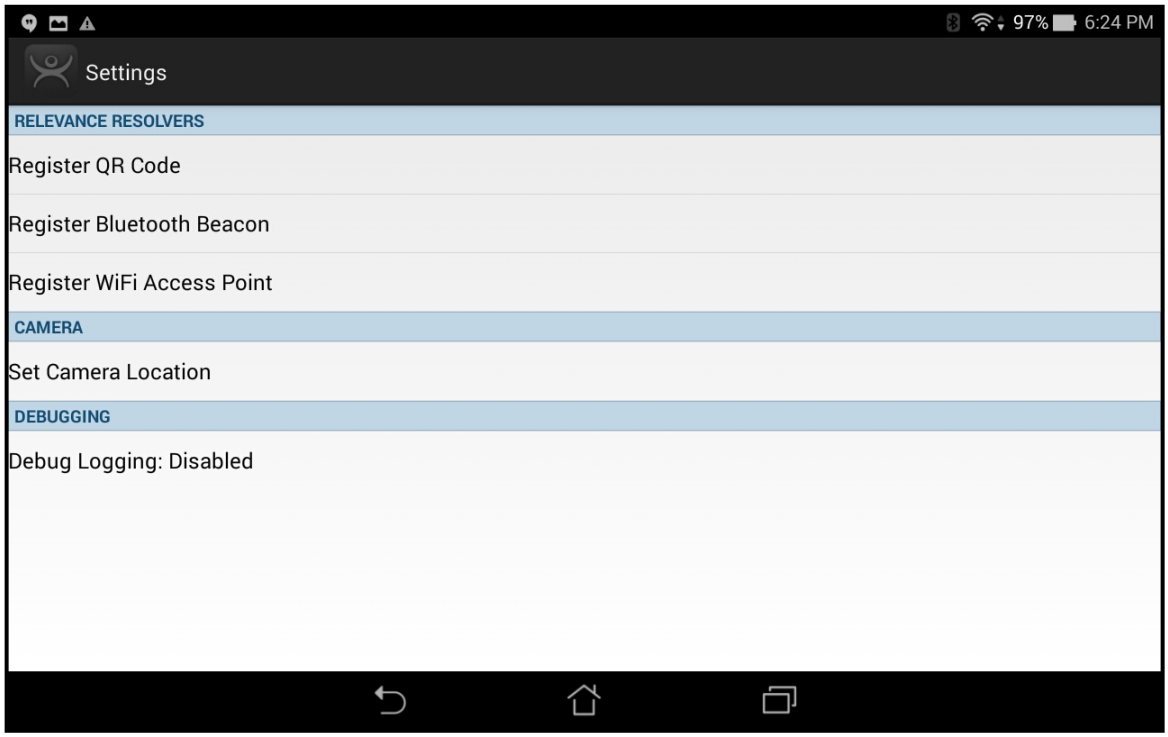


Setting Selection Menu

Selecting the ***Setting*** link will open a **Setting** menu with several choices.

- ***Manage ThinServer*** – This opens the **Settings Menu** and lets you register resolvers.
- ***Add ThinServer*** – This opens the Add New ThinServer page that lets you define a new ThinManager Server.
- ***Remove ThinServer*** – This allows you to delete a defined ThinManager Server.

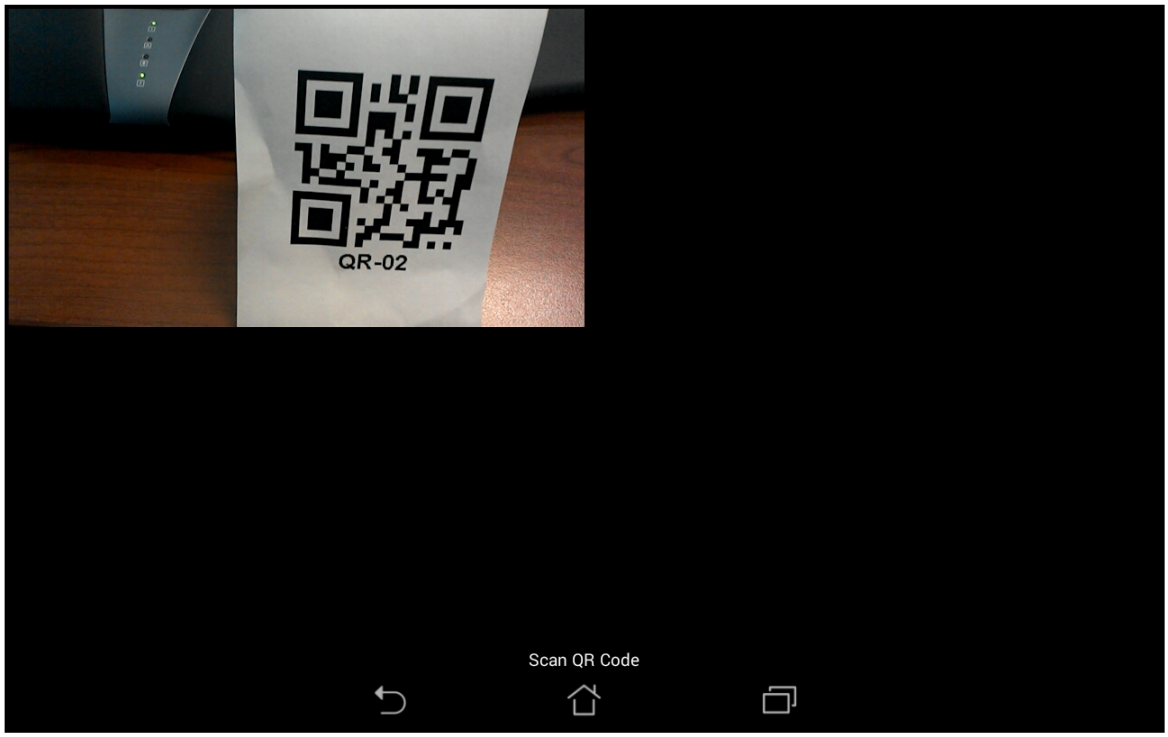
If you have multiple ThinManager Servers defined you will need to select the ThinManager Server that you want to apply the QR codes by selecting the correct server.



aTMC Settings Page

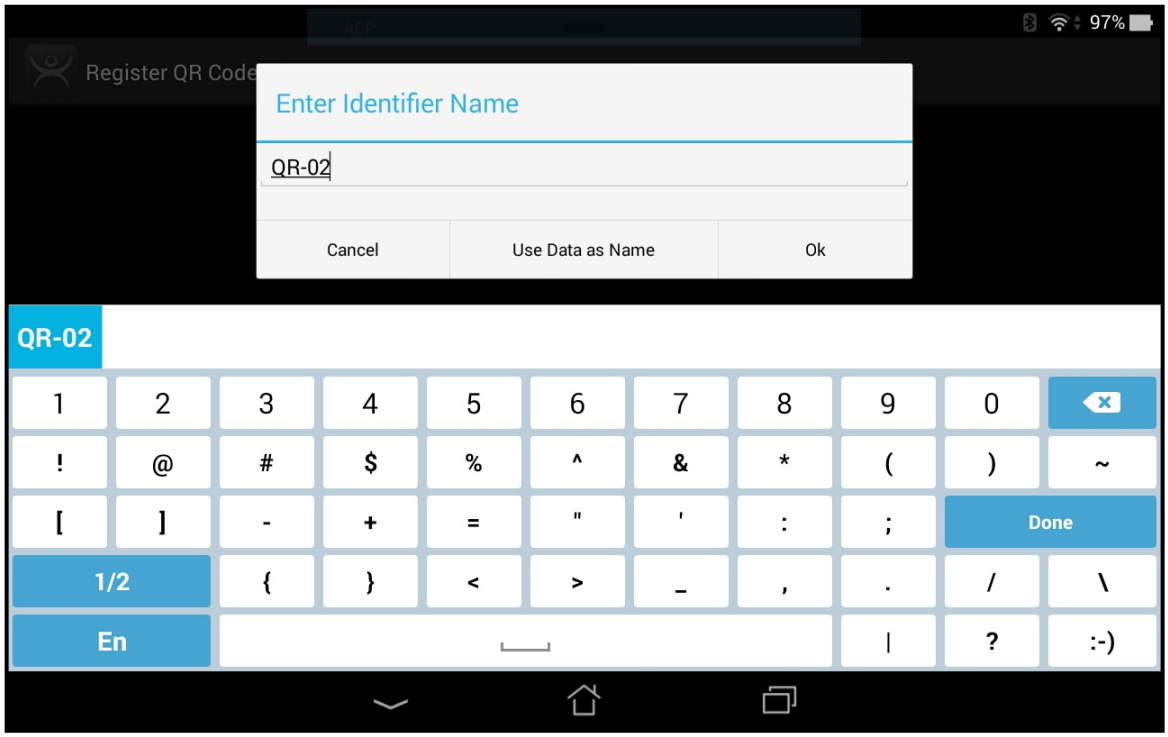
The **Settings** page has the links to register the various resolvers.

Select the ***Register QR Code*** link to open the camera to scan and register the QR code.



Scan New QR Code Window

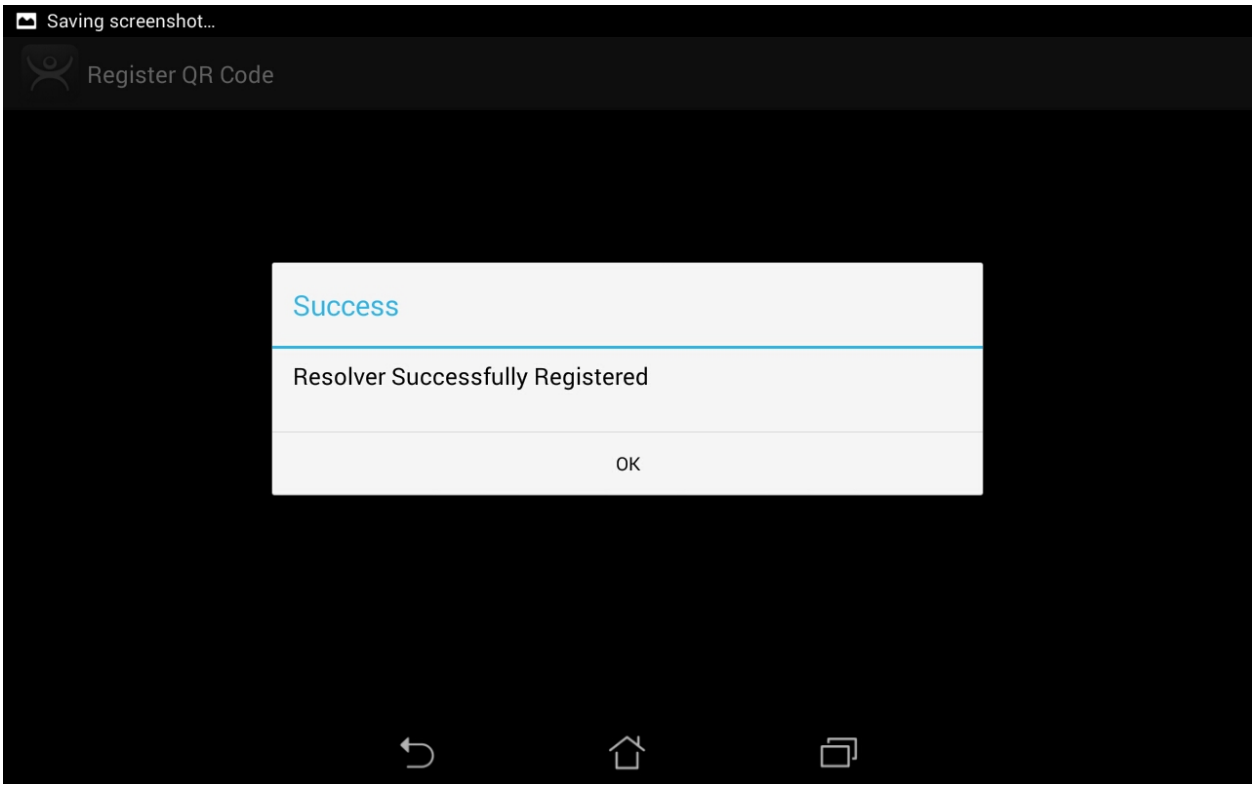
Selecting the ***Register QR Code*** link will open the camera. Point the camera at the QR code. Once it is framed in the window it will read the code and register it.



Enter Description for QR Code

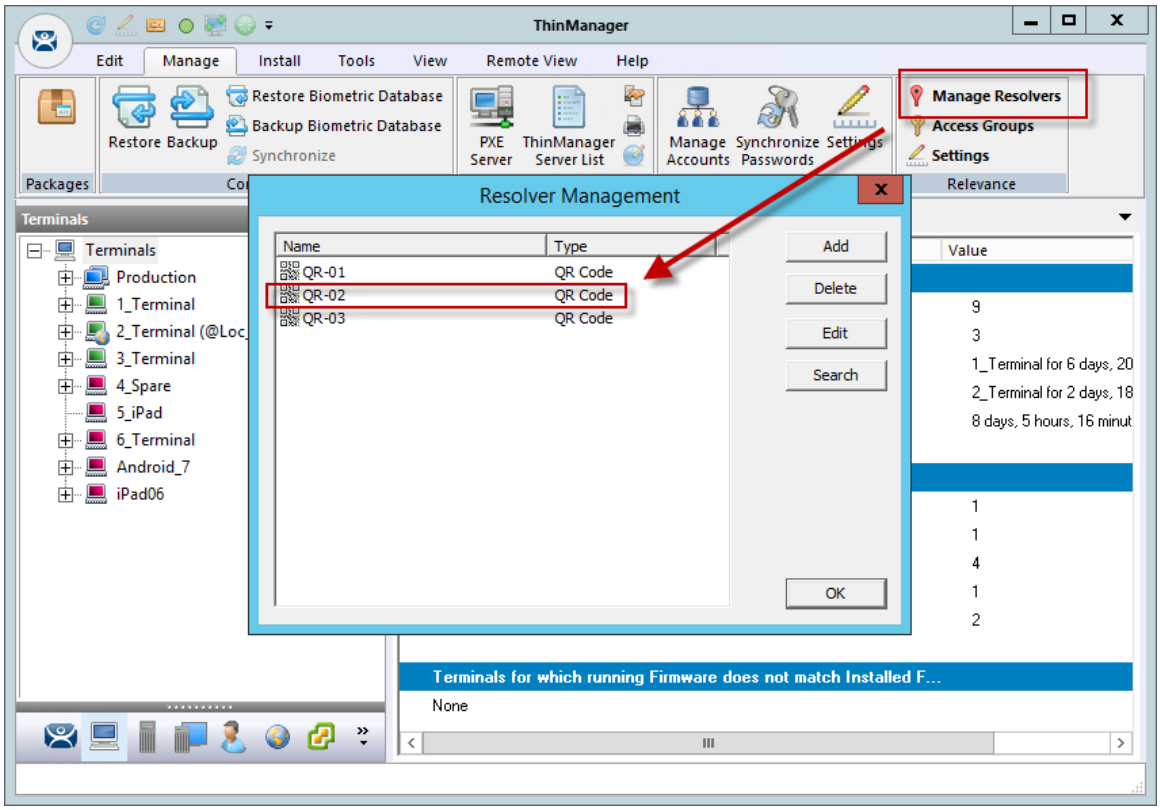
Once the iTMC program has read the QR code it will ask you to name it.

Enter the name for the Resolver in in **Enter Identifier Name** window.



Successful Registration Confirmation

The aTMC program will confirm a successful registration.



QR Code in Resolver Management Window

The Resolvers are listed in the Resolver Management window. This is opened by selecting ***Manage > Manage Resolvers*** from the ThinManager menu bar.

39.2. Bluetooth Beacons

ThinManager supports Bluetooth Beacons that use the **Bluetooth Low Energy (LE)** standard, which is part of the **Bluetooth Core Specification Version 4.0**. In order to work with these beacons, your mobile device also needs to support Bluetooth Version 4.0 or newer. In the case of an iPad, this would be any iPad (regular, Mini, Air) that uses the Lightning (new, small) connector.

Relevance can use Bluetooth beacons as location resolvers. These need to be Low Energy Bluetooth beacons that provide a unique name in the Advertising Packet.

See Fencing and Sub-Locations on page 697.

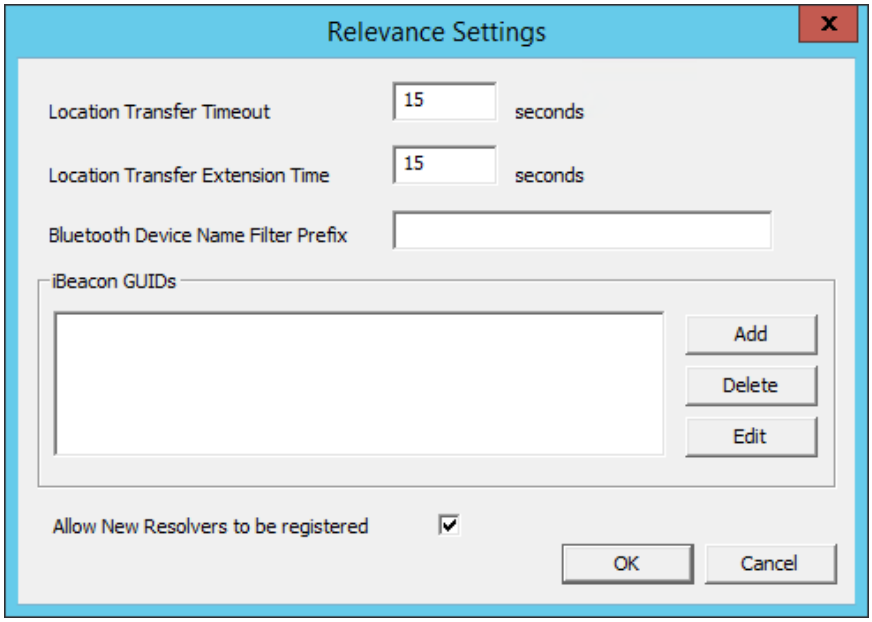
To add new beacons to the system, you can use the mobile device to find them, and add them in a manner similar to the other resolvers. In the case of these devices, you stand at the entry point, and allow the device to get a few readings so that it can get an average measure of the signal strength at that point. It will automatically add 10 to this number for the exit point. You can adjust these in ThinManager in the Manage Resolvers section.

The procedure for defining a Bluetooth with a mobile device is:

- Place the Bluetooth beacons in the locations that you want.
- Launch the iTMC or aTMC program and select the ***Settings*** button.
- Select the ***Register Bluetooth Beacon*** command under Relevance Resolvers. If you have more than one ThinManager Server defined you will need to pick the ThinManager Server you want the Bluetooth beacons registered.

- Select the desired Bluetooth beacon from the generated list.
- Enter a name and select ***Register***.
- The Bluetooth beacon will be registered and entered in the **Resolver Management** window that is accessed by selecting ***Manage > Manage ID's***.

39.2.1. Relevance Settings



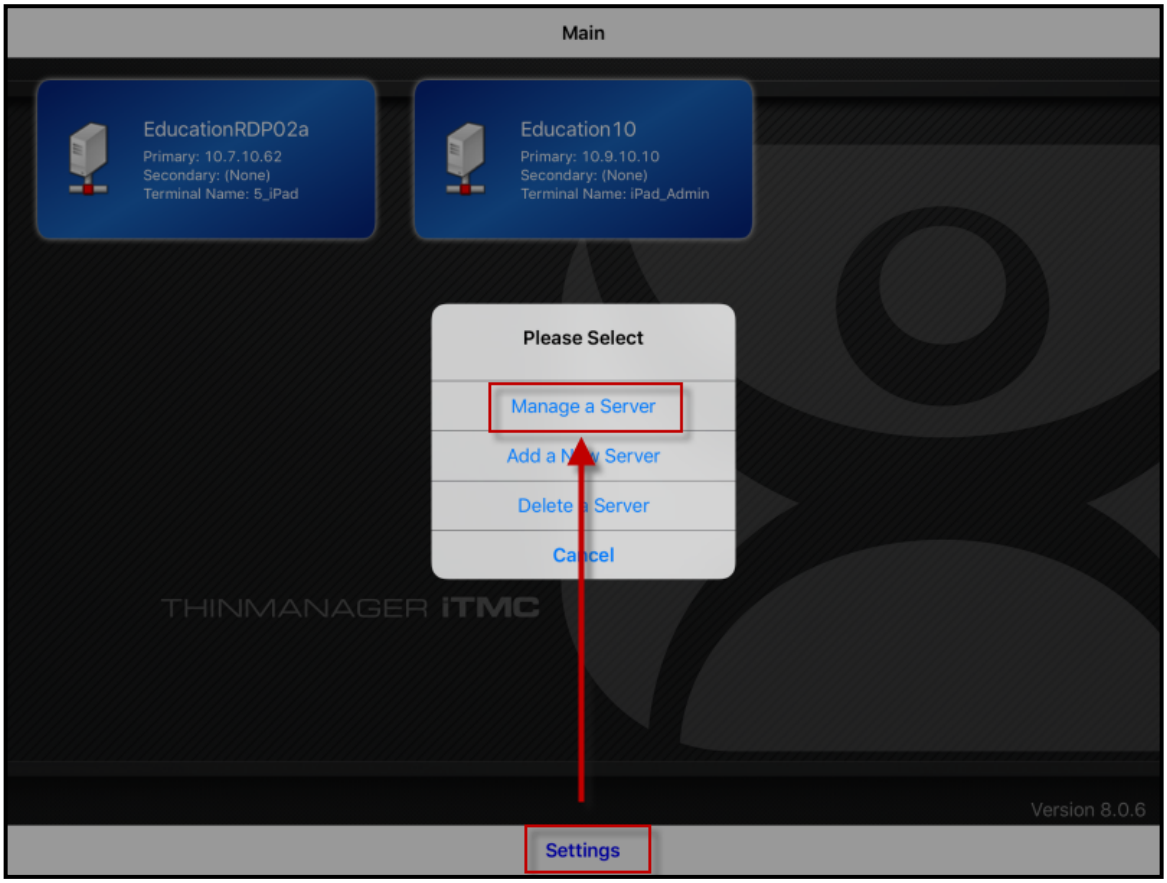
Relevance Settings Window

The **Relevance Settings** window has some settings that can affect Bluetooth beacons. It is launched by selecting ***Manage > Relevance Settings*** on the ThinManager menu bar.

- ***Location Transfer Timeout*** – This sets the time that an operator has to acknowledge and allow a Transfer. See Transfer on page 609.
- ***Location Transfer Extension Time*** – This sets the interval of extra wait time that a refused transfer will allow.
- ***Bluetooth Device Name Filter*** – Entering a name in this field will limit the display of Bluetooth devices that have that prefix. This is helpful because ThinManager Bluetooth devices have an ACP prefix.
- ***iBeacon GUIDs*** – This field shows the registered iBeacons.
  - ***Add*** – This button launches the Enter iBeacon GUID window that allows definition of a new iBeacon.
  - ***Delete*** – This button will delete a highlighted iBeacon from the list.
  - ***Edit*** – This button launches the Enter iBeacon GUID window for a highlighted iBeacon for editing.
- ***Allow New Resolvers to be registered*** – This checkbox allows new resolvers. Unchecking it will prevent unauthorized users from adding Bluetooth beacons.

39.2.2. Defining Bluetooth Beacons on an iPad

Defining a Bluetooth beacon is similar to defining a QR code.

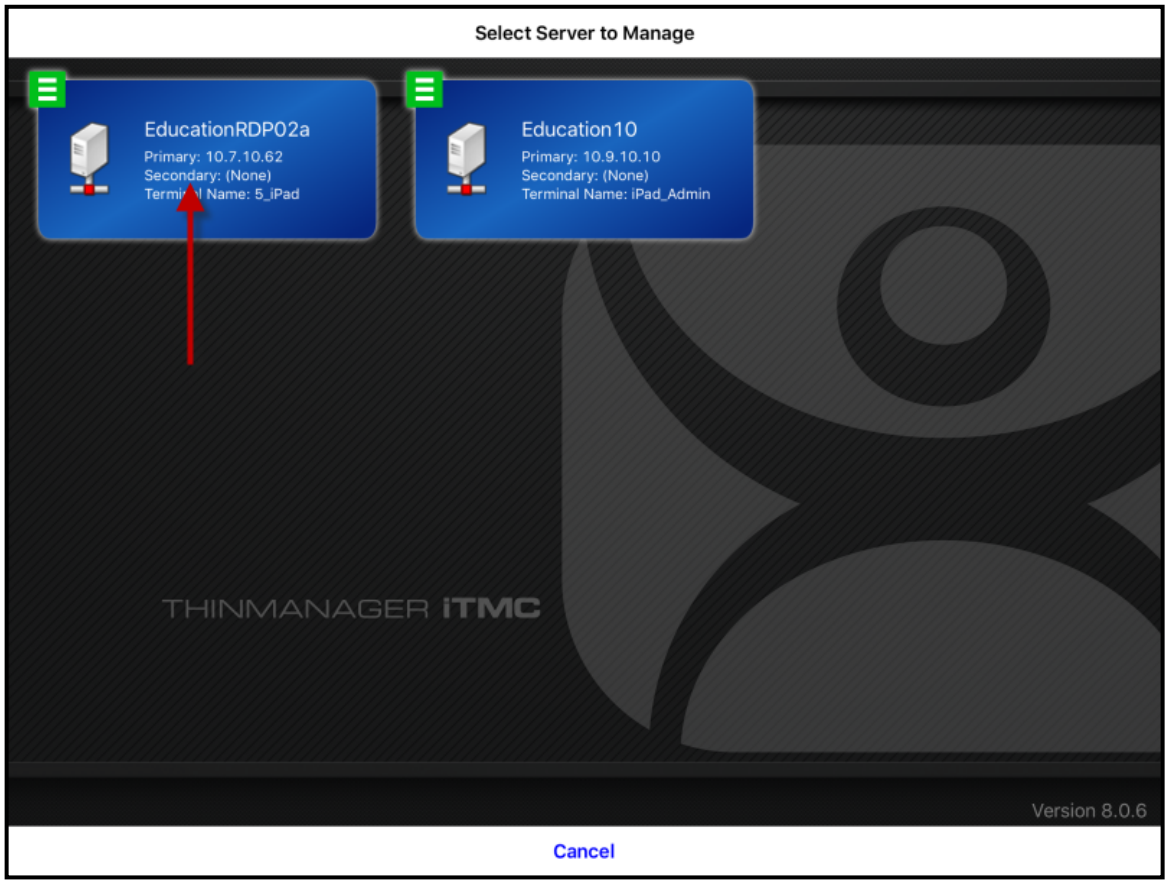


ThinManager iTMC Program

Open the **iTMC** program on the iPad.

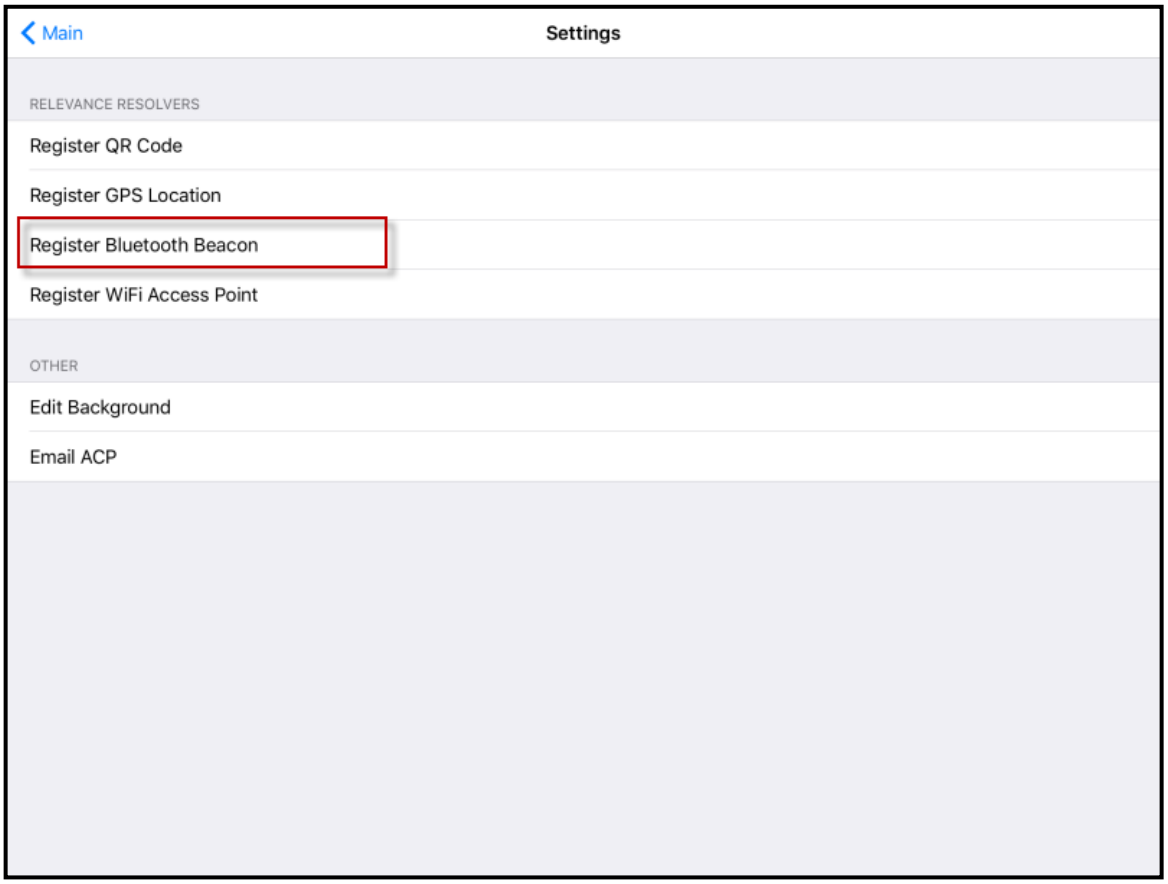
Select the ***Settings*** button on the bottom to launch the **Settings** menu.

Select the ***Manage a Server*** link.



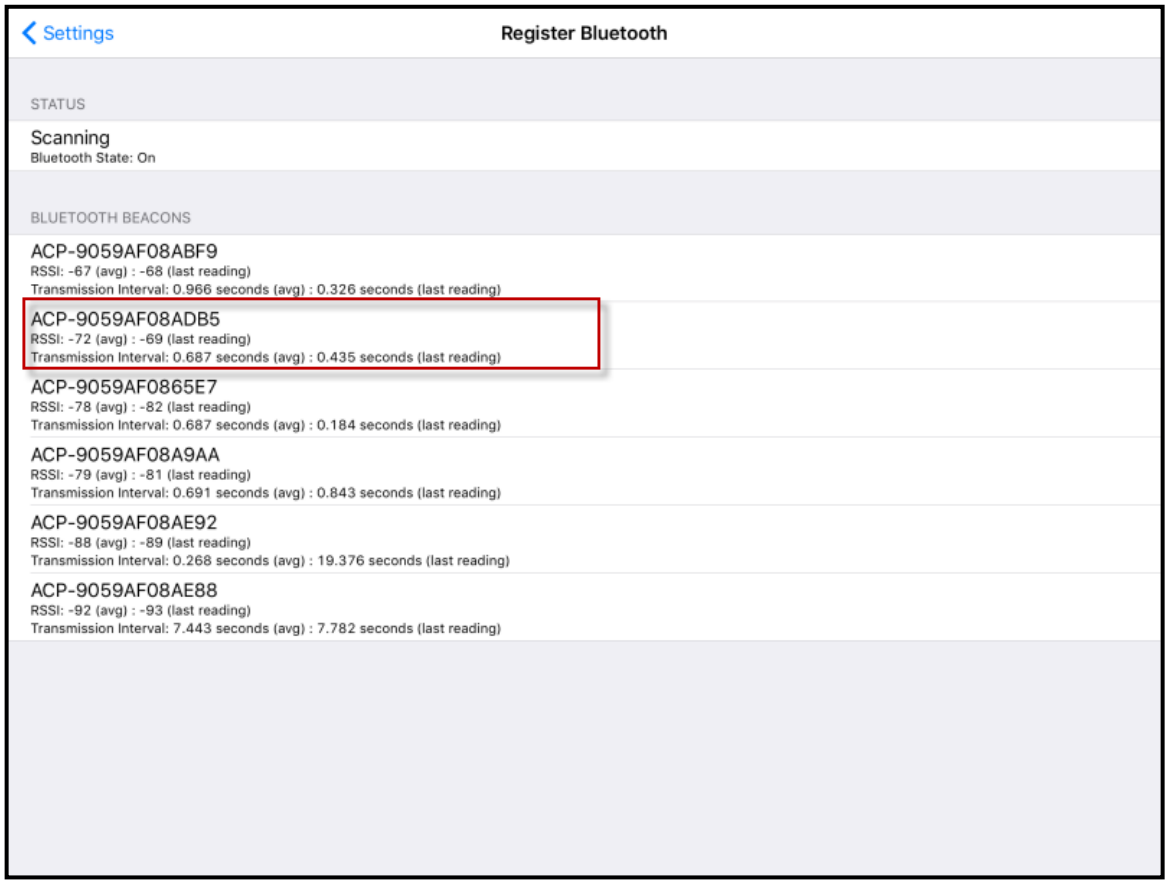
Select Configuration

Select the ThinManager Server you want to register the Bluetooth beacon on.



Register Bluetooth Beacon Command on the Settings Page

Select the *Register Bluetooth Beacon* command on the **Settings** page.

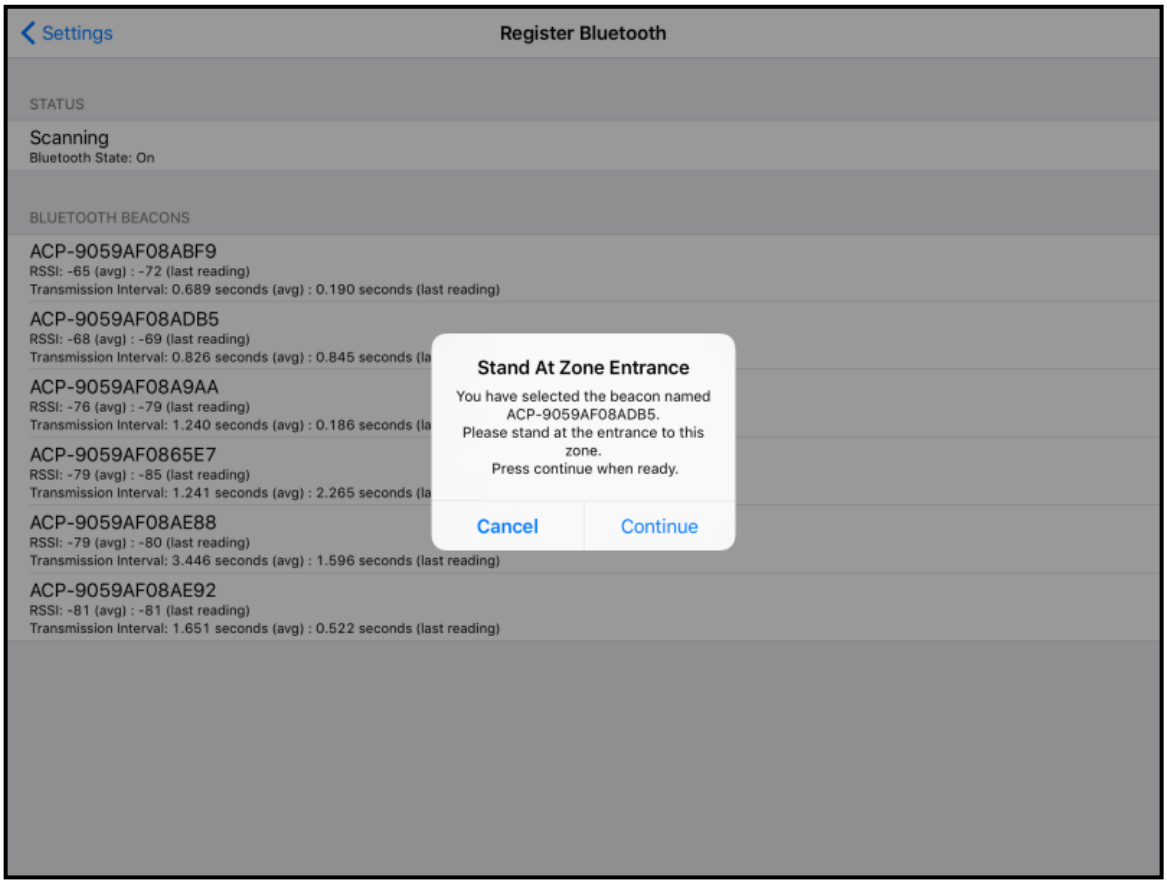


Available Bluetooth Beacons

The mobile device will search for the Bluetooth beacons and list them on the **Register Bluetooth** page.

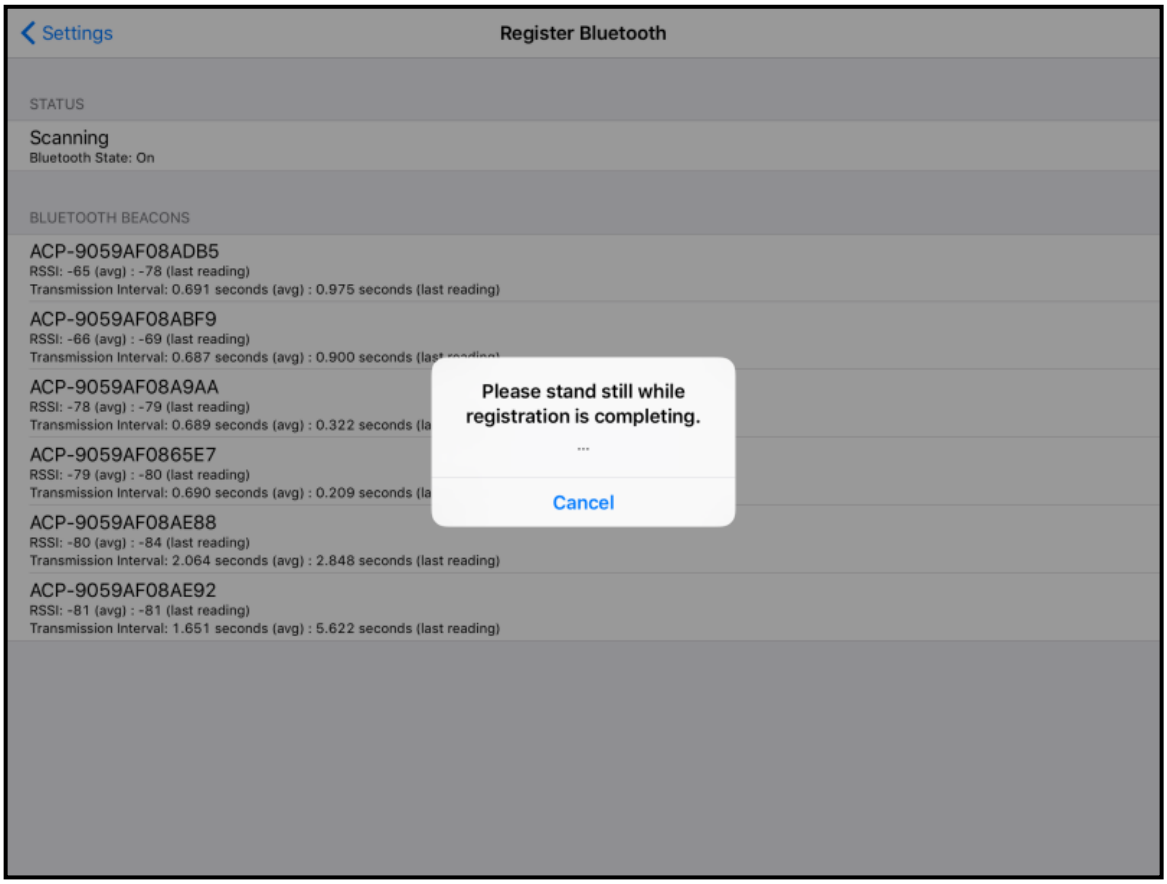
Select the desired Bluetooth beacon. ACP-9059AF08ADB5 was chosen in this example.

Note: This ThinManager Server is using ACP as a filter in the **Relevance Settings** window to limit the number of Bluetooth beacons shown. See Bluetooth Beacons on page 632 for details.



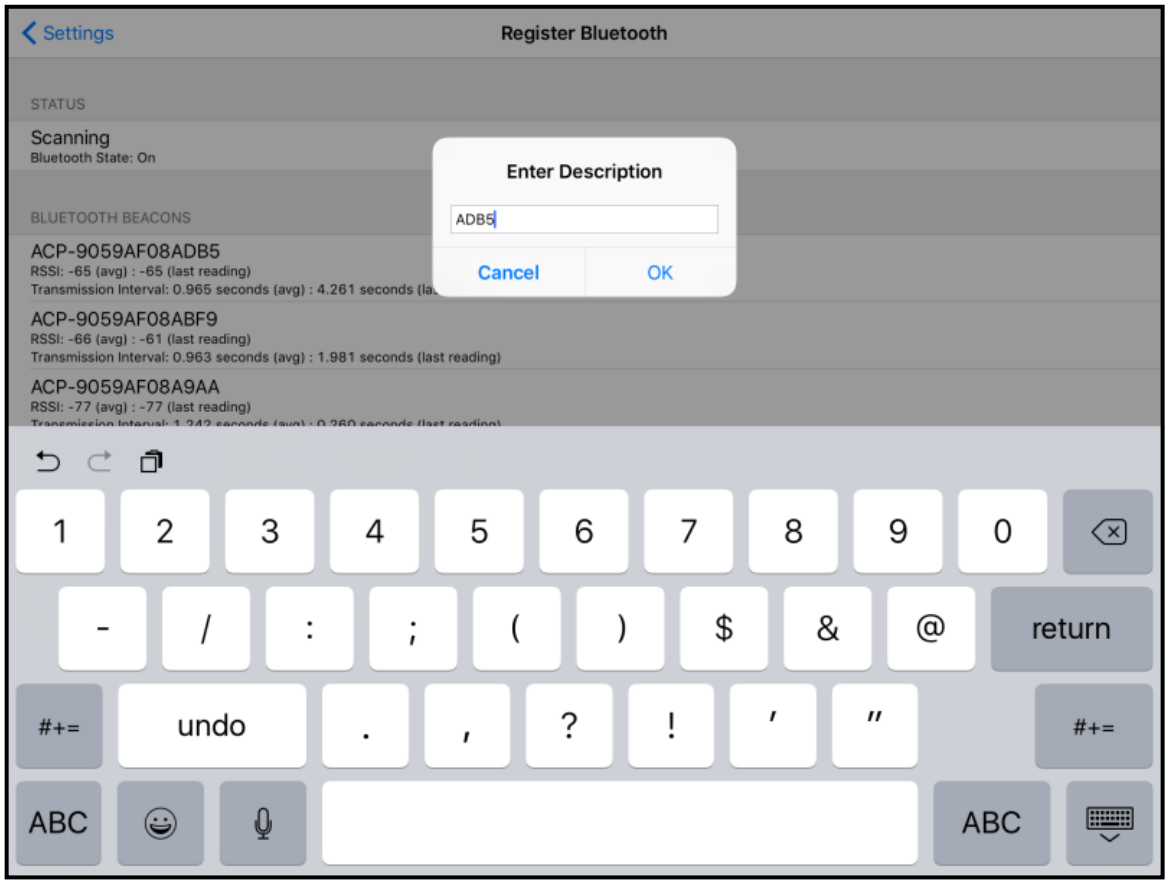
Stand At Zone Entrance Dialog

The mobile device will prompt you to go to the location that you want as the entrance point for the zone. Select ***Continue***.



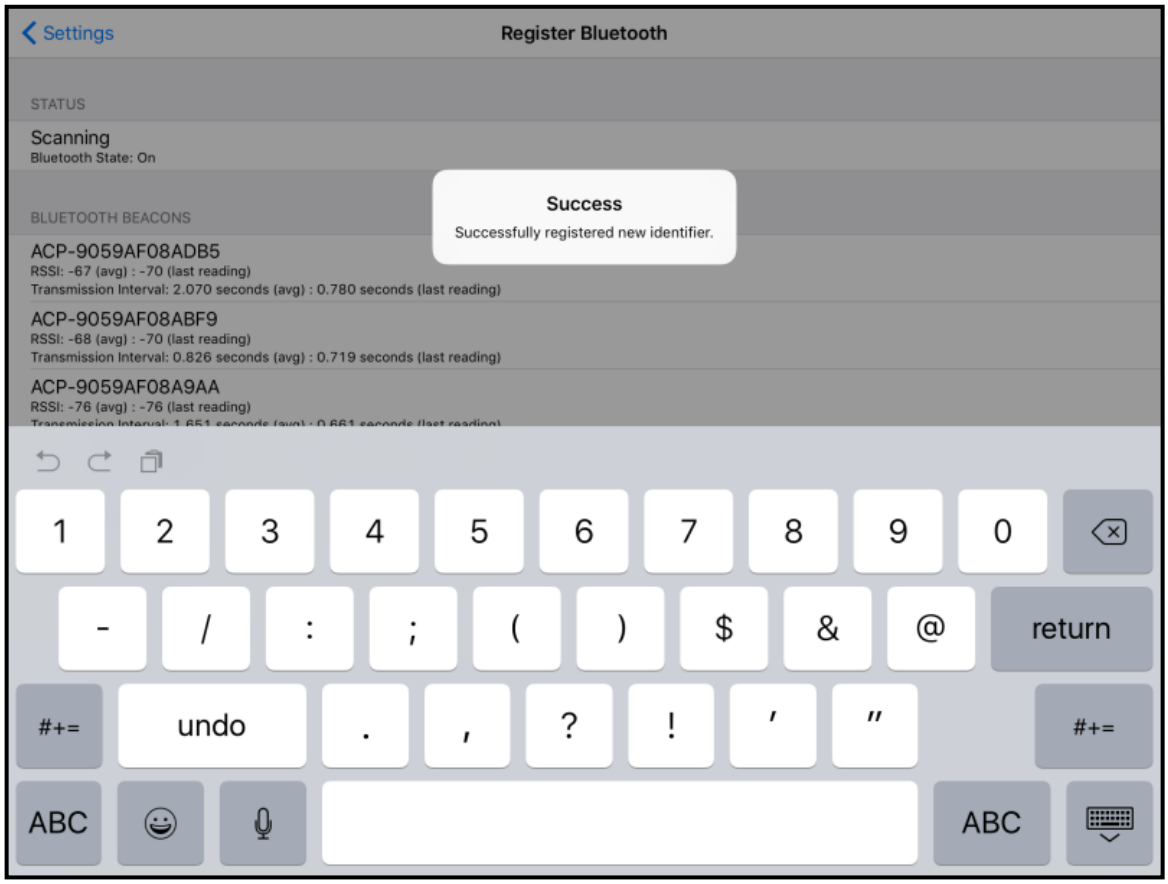
Please Wait Message

It may take a few seconds to allow the device to read the signal strength to create the resolver data. Do not move around while the device is registering.



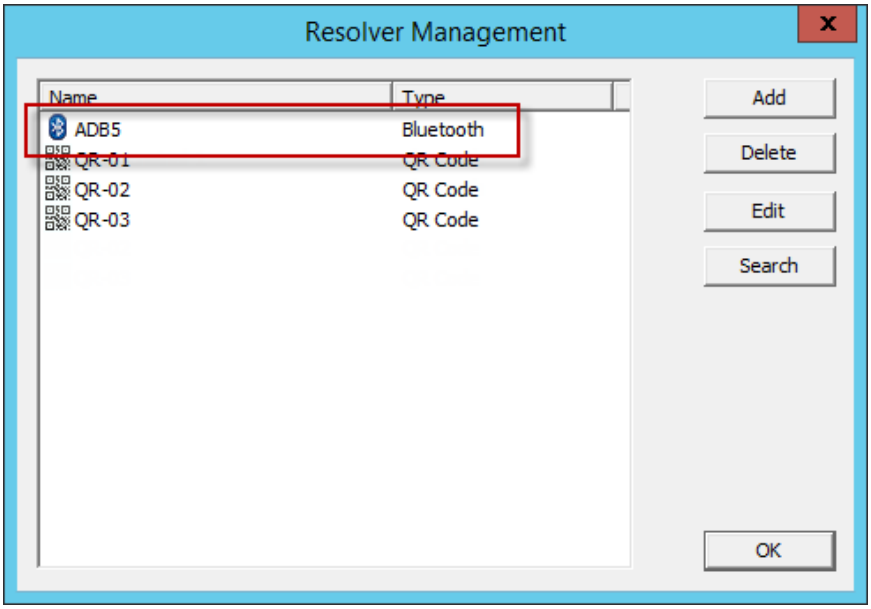
Enter Location Description

Once the data has been collected and the Bluetooth beacon is registered you will be prompted to name the location.



Success Dialog

The program will confirm successful Bluetooth registrations.



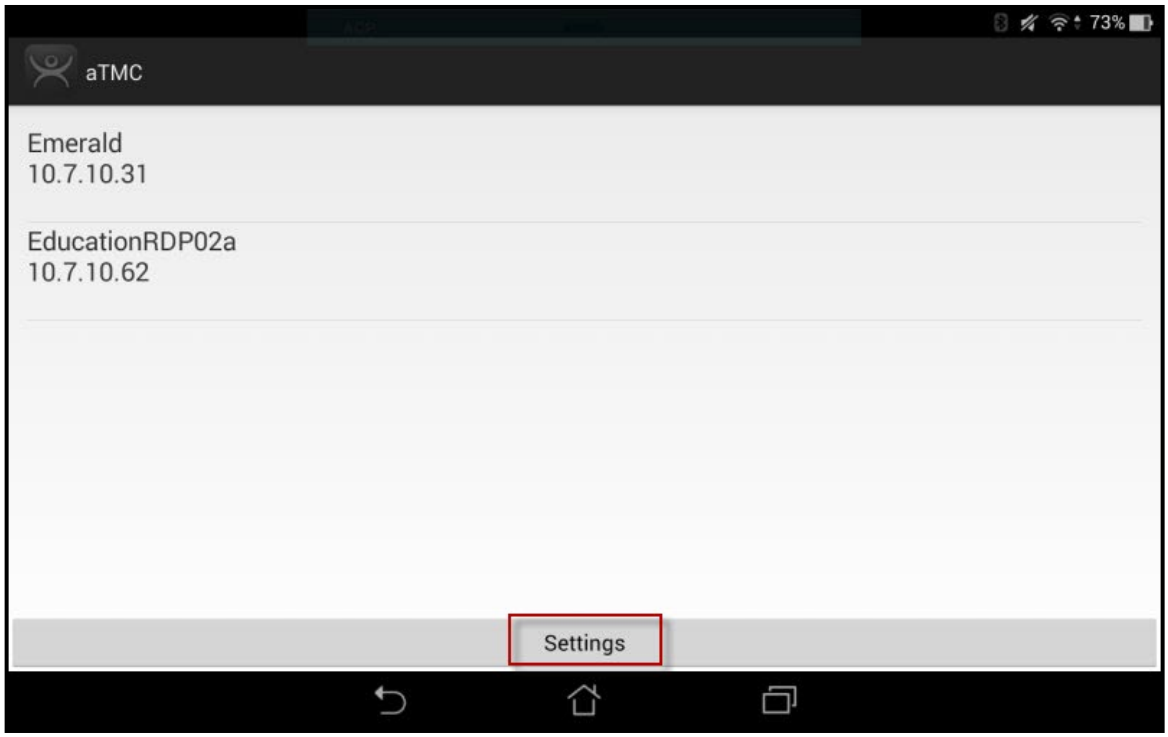
Resolver Management Window

The QR code will be registered and entered in the **Resolver Management** window that is accessed by selecting ***Manage > Manage ID's***.

39.2.3. Defining Bluetooth Beacons on an Android

The procedure for defining a Bluetooth with an iPad is:

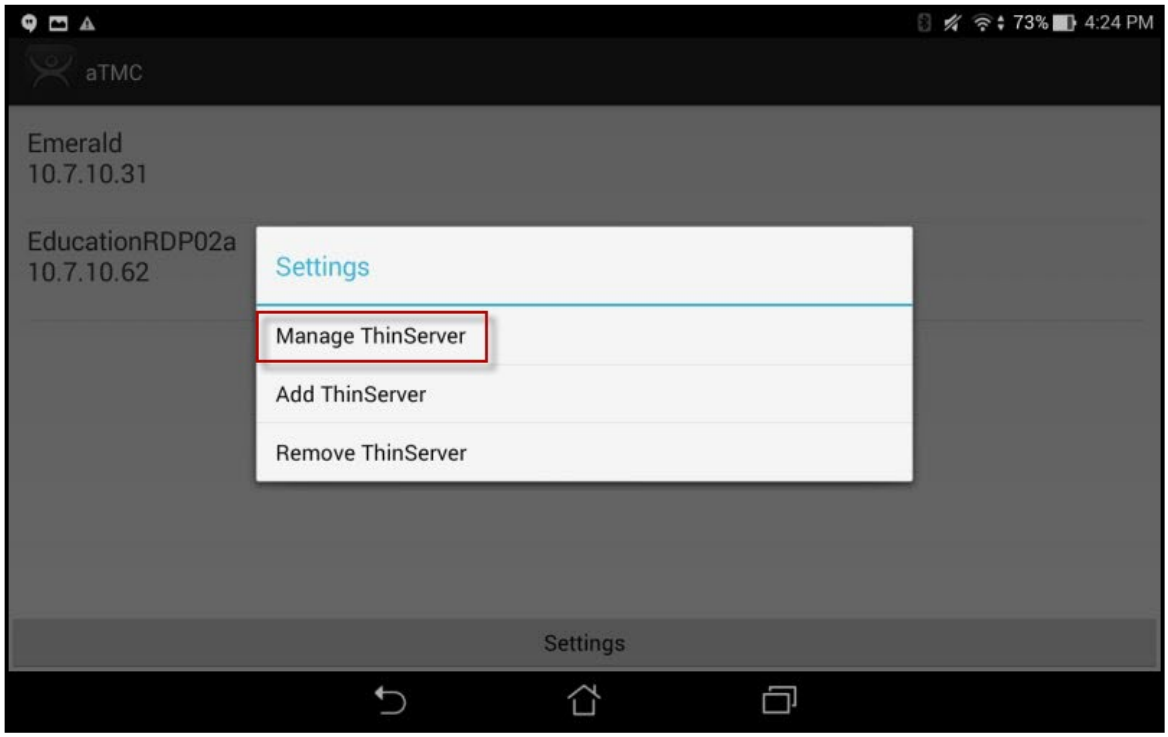
- Place the Bluetooth beacons in the locations that you want.
- Launch the aTMC program and select the ***Settings*** button.
- Select the ***Register Bluetooth Beacon*** command under Relevance Resolvers. If you have more than one ThinManager Server defined you will need to pick the ThinManager Server you want the Bluetooth beacons registered.
- Select the desired Bluetooth beacon from the generated list.
- Enter a name and select ***Register***.
- The Bluetooth beacon will be registered and entered in the **Resolver Management** window that is accessed by selecting ***Manage > Manage ID's***.



ThinManager aTMC Program

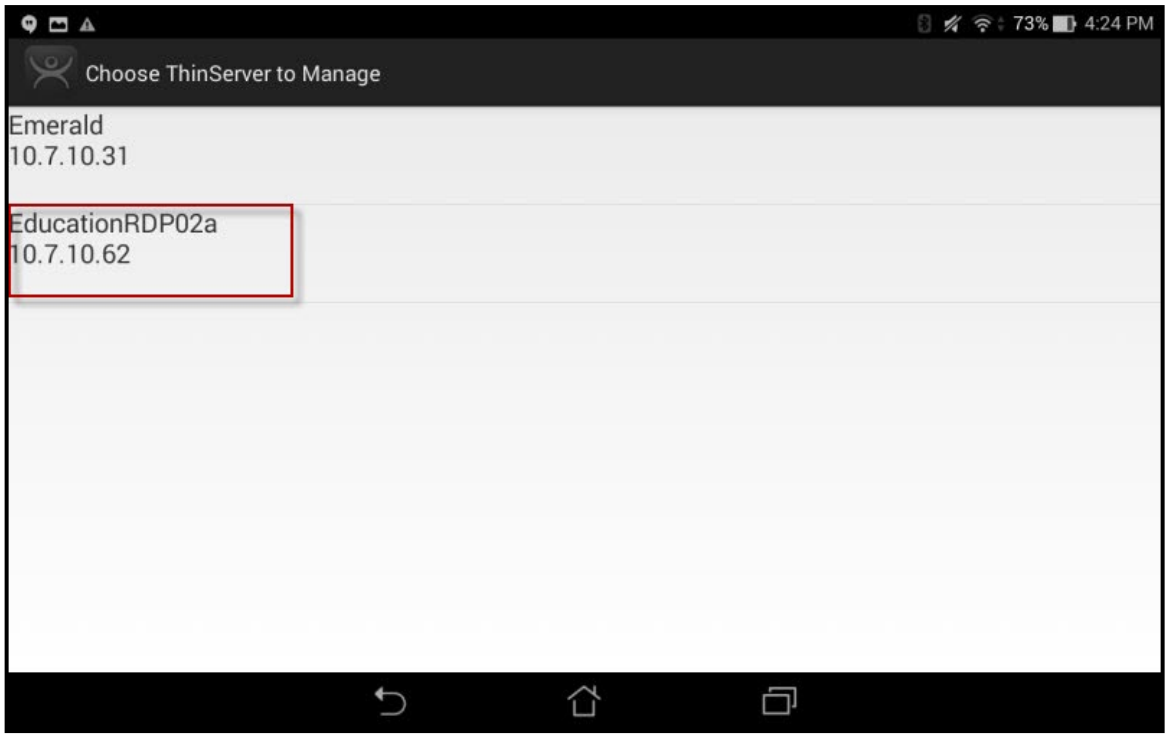
Open the **aTMC** program on the iPad.

Select the ***Settings*** button on the bottom to launch the **Settings** screen.



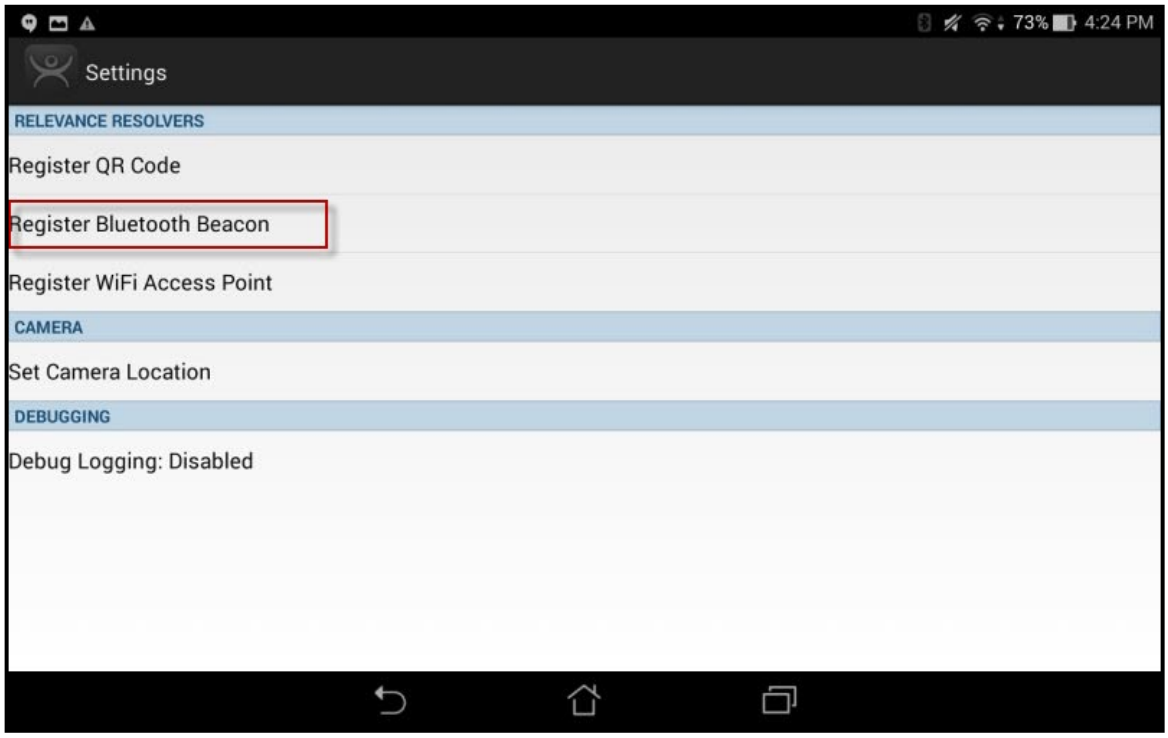
Settings Menu

Select the ***Manage ThinServer*** link.



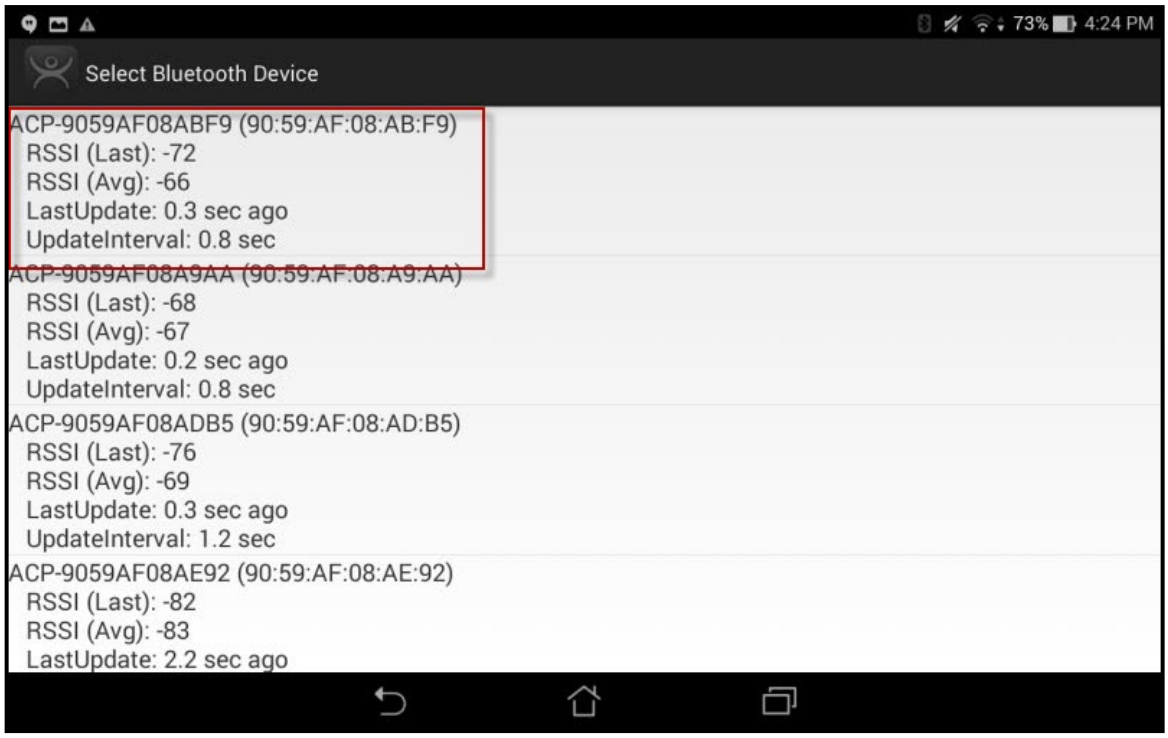
Select Configuration

Select the ThinManager Server you want to register the Bluetooth beacon on.



Register Bluetooth Beacon Command on the Settings Page

Select the ***Register Bluetooth Beacon*** command on the **Settings** page.



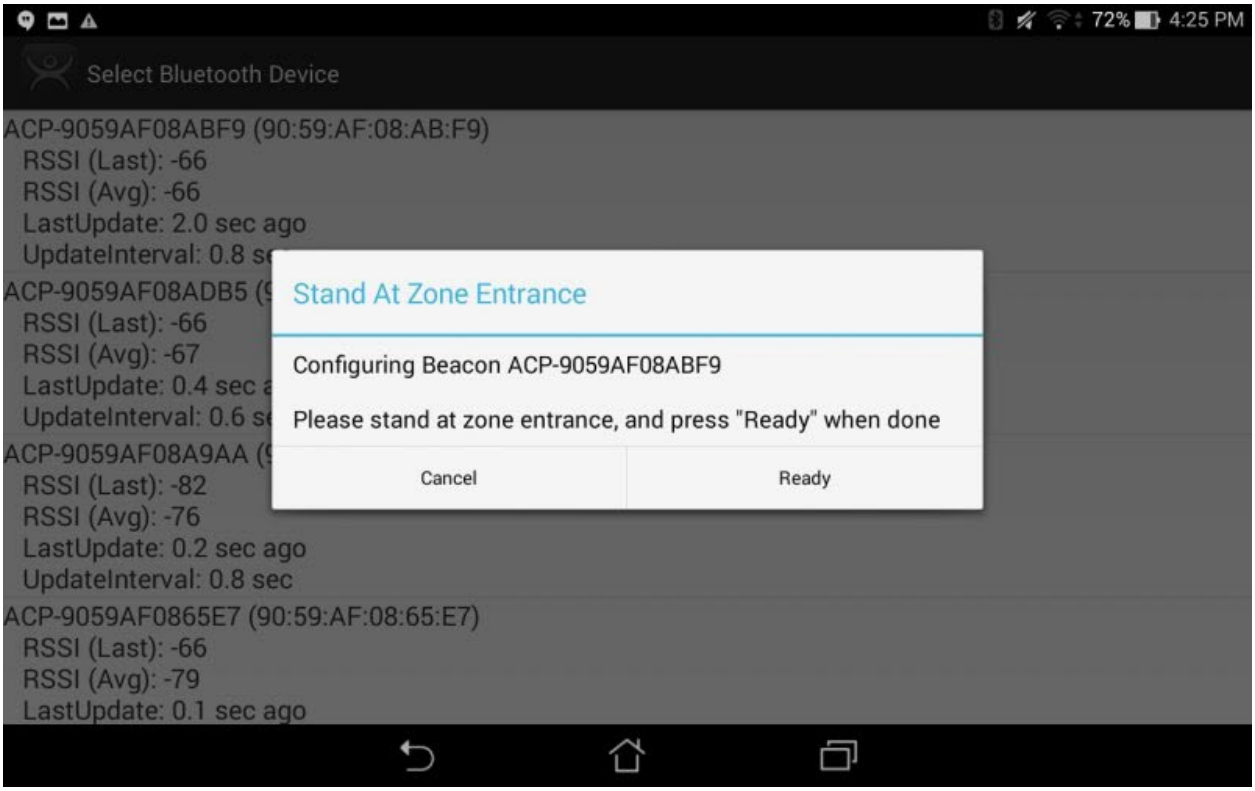
Available Bluetooth Beacons

The mobile device will search for the Bluetooth beacons and list them on the **Register Bluetooth** page.

Select the desired Bluetooth beacon.

Note: This ThinManager Server is using ACP as a filter in the **Relevance Settings** window. See Bluetooth Beacons on page 632 for details.

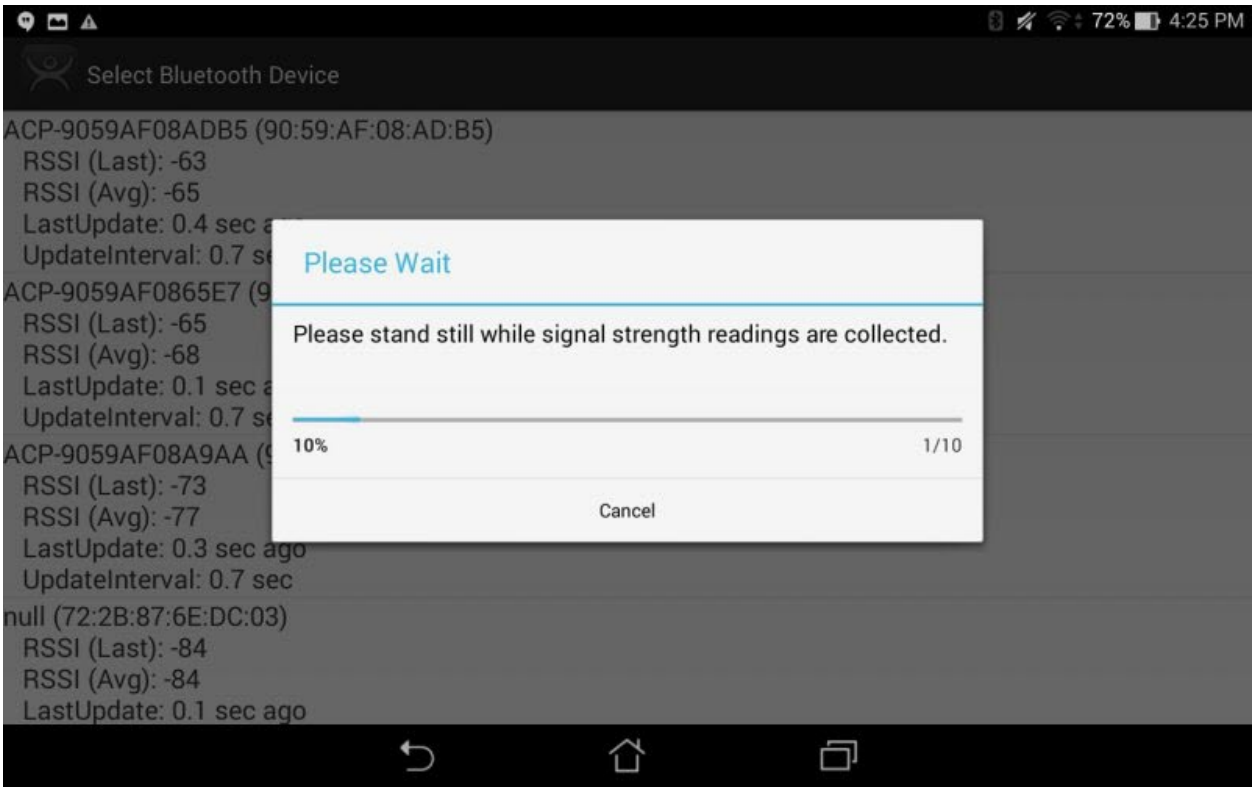
Select the desired Bluetooth beacon. ACP-9059AF08ABF9 was chosen in this example.



Stand At Zone Entrance Dialog

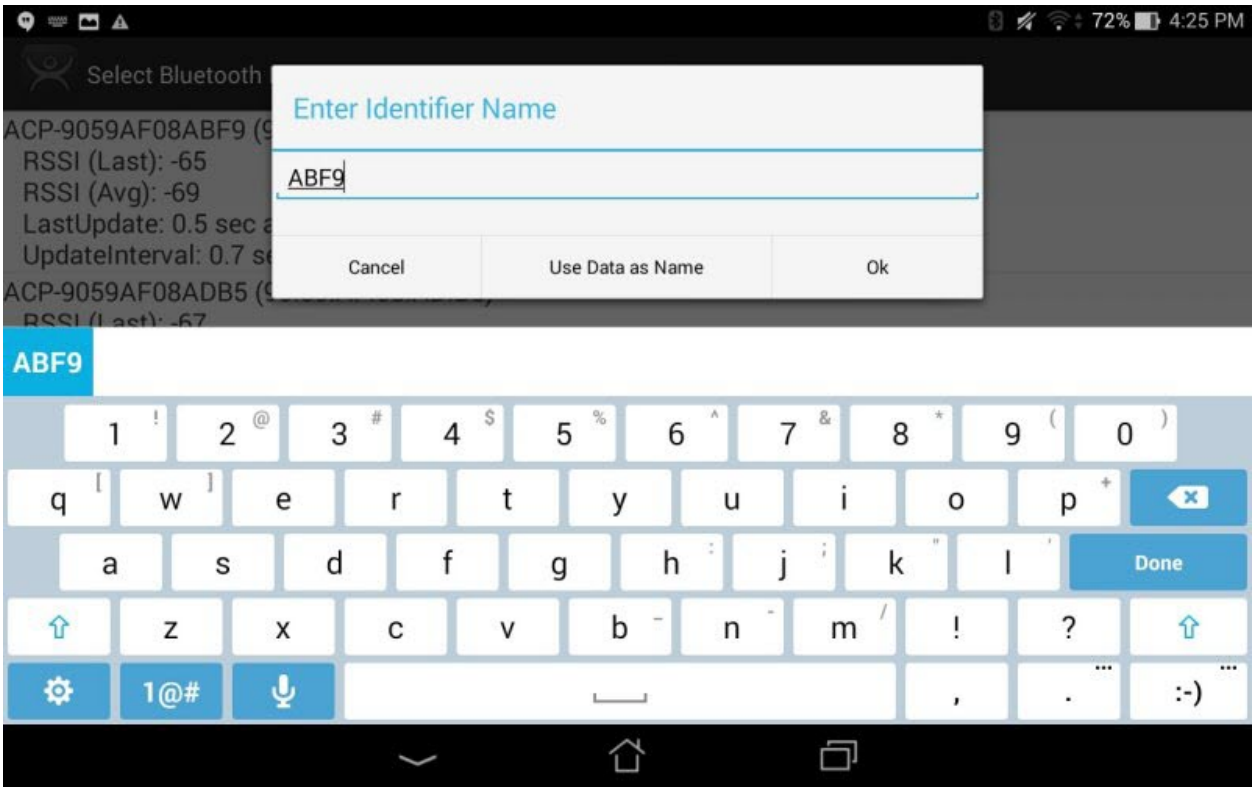
The mobile device will prompt you to go to the location that you want as the entrance point for the zone.

Select ***Continue***.



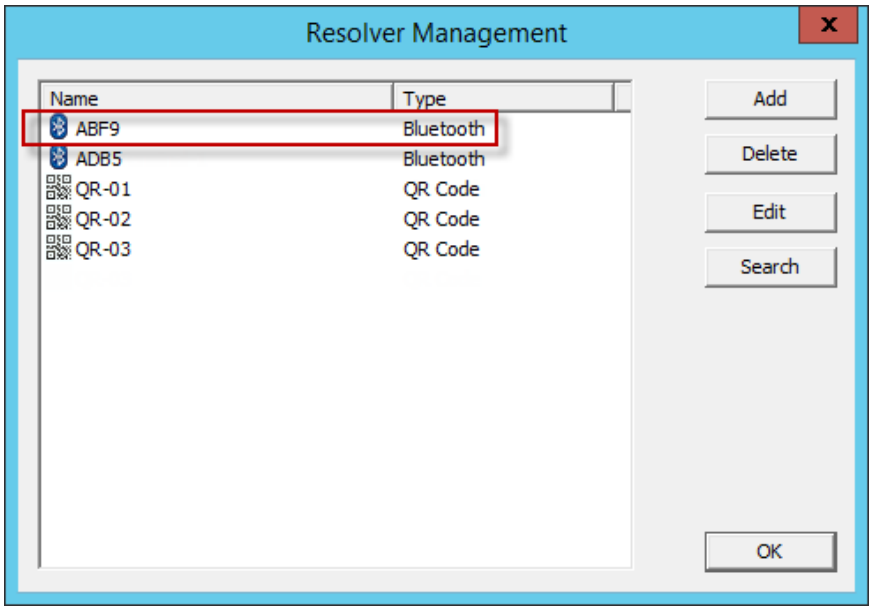
Please Wait Message

It may take a few seconds to allow the device to read the signal strength to create the resolver data.



Enter Location Description

Once the data has been collected and the Bluetooth beacon is registered you will be prompted to name the location.



Resolver Management Window

The QR code will be registered and entered in the **Resolver Management** window that is accessed by selecting ***Manage > Manage ID's***.

39.3. Wi-Fi Access Points

This resolver is based on the BSSID (a MAC type address) of the Wireless Access Point (WAP) that the mobile device is connected to at the time.

Relevance can use Wi-Fi access points as location resolvers. Wi-Fi Resolvers work well in situations where there are multiple access points. Membership of a network will give you access to functions in that area.

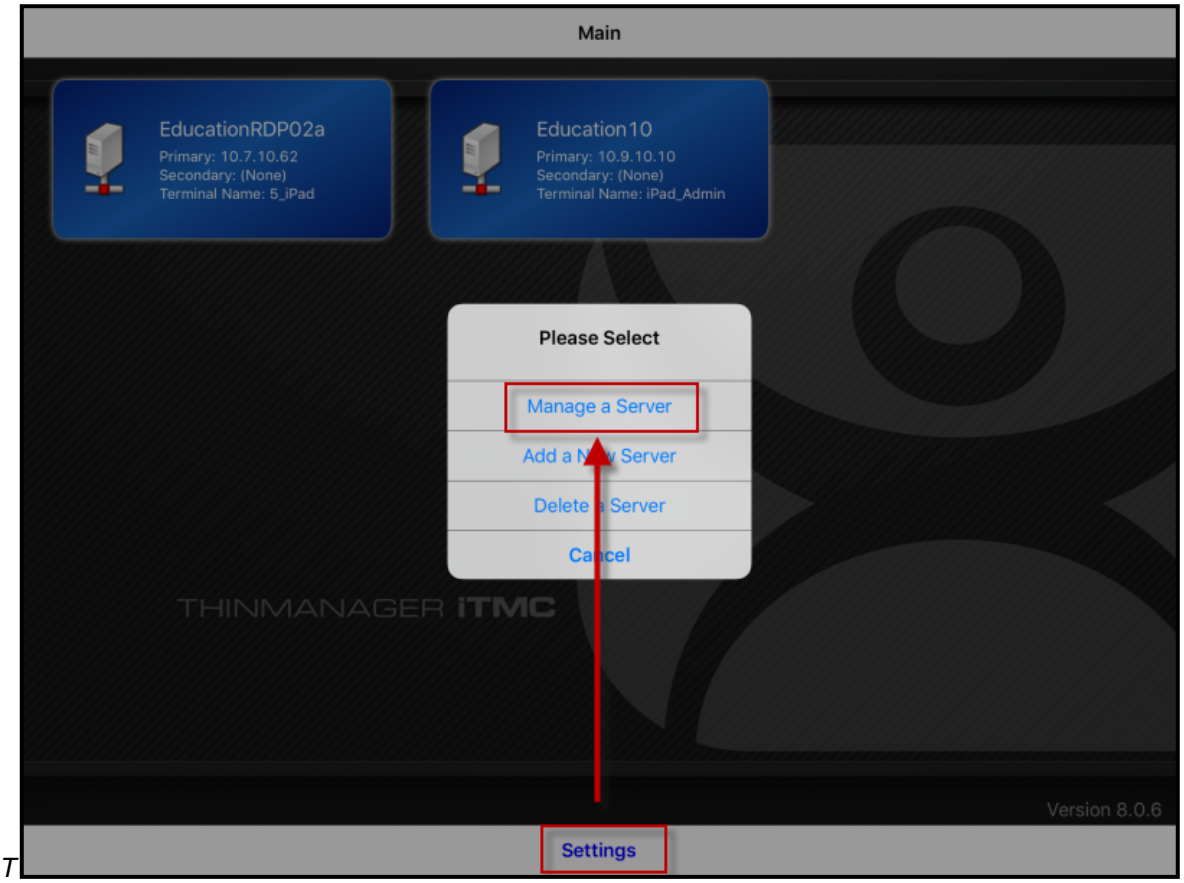
See Fencing and Sub-Locations on page 697.

The procedure is:

- Install Wi-Fi access points in the areas you need.
- Launch the mobile program and select the ***Settings*** button.
- Select the ***Register Wi-Fi Access Point*** command under Relevance Resolvers. If you have more than one ThinManager Server defined you will need to pick the ThinManager Server you want the QR code registered.
- Select the access point from the generated list.
- Enter a name and select Register.
- The Wi-Fi Access Point will be registered and entered in the **Resolver Management** window that is accessed by selecting ***Manage > Manage ID's***.

39.3.1. Defining Wi-Fi Access Points with an iPad

The Wi-Fi resolver is defined like a Bluetooth beacon.

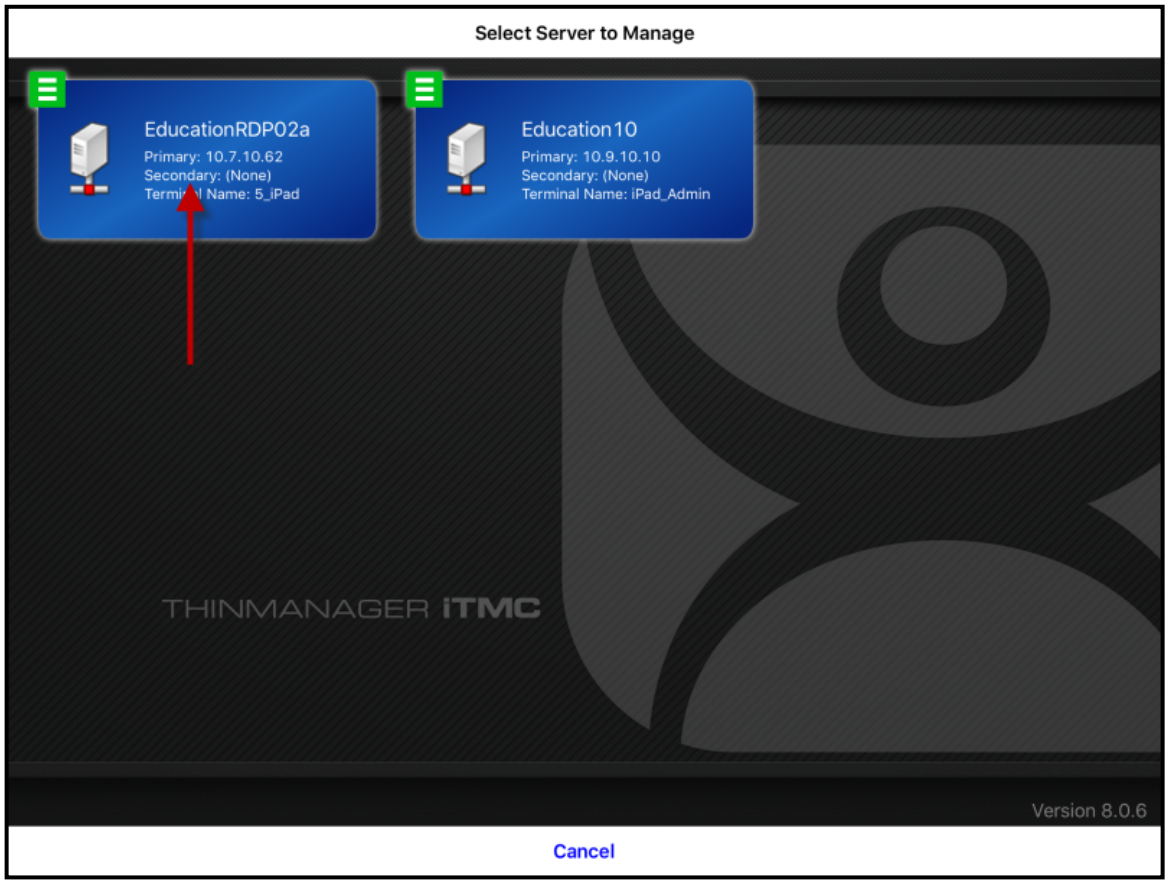


ThinManager iTMC Program

Open the **iTMC** program on the iPad.

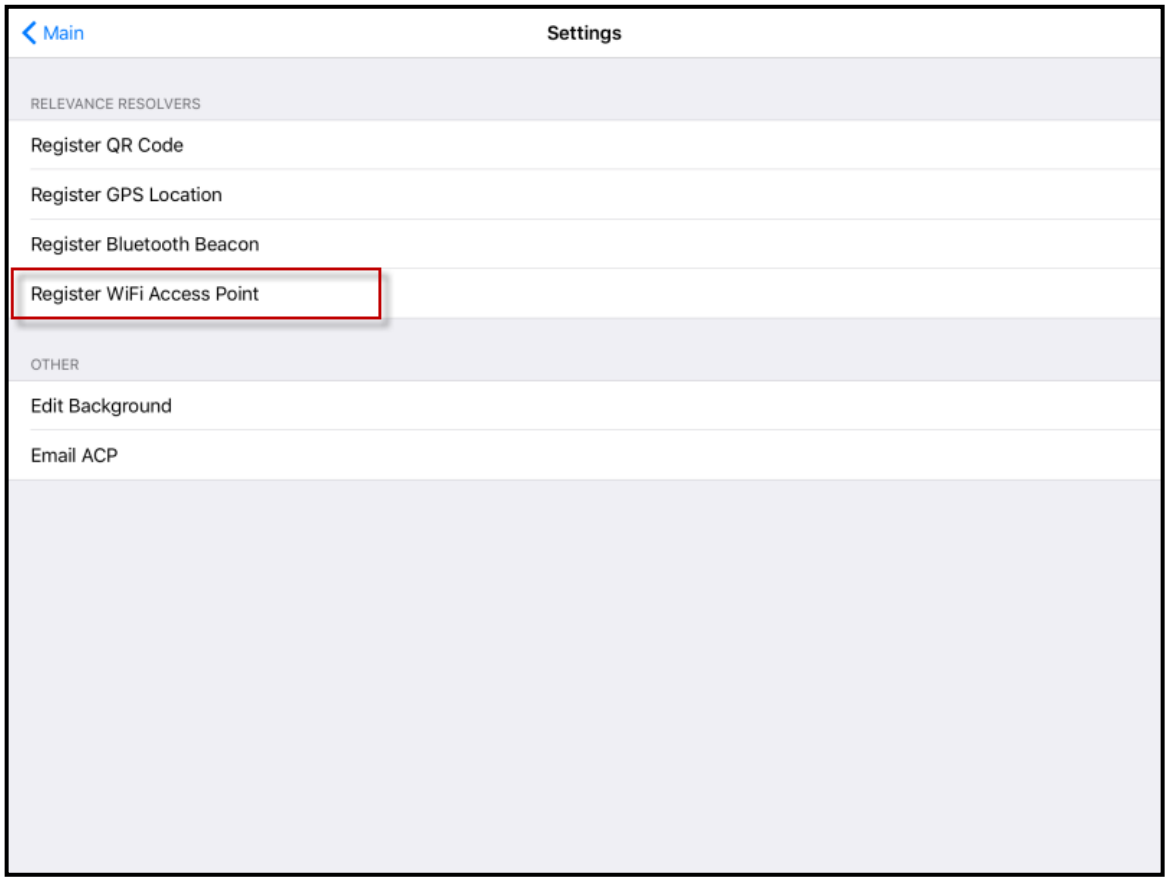
Select the ***Settings*** button on the bottom to launch the **Settings** menu.

Select the ***Manage a Server*** link.



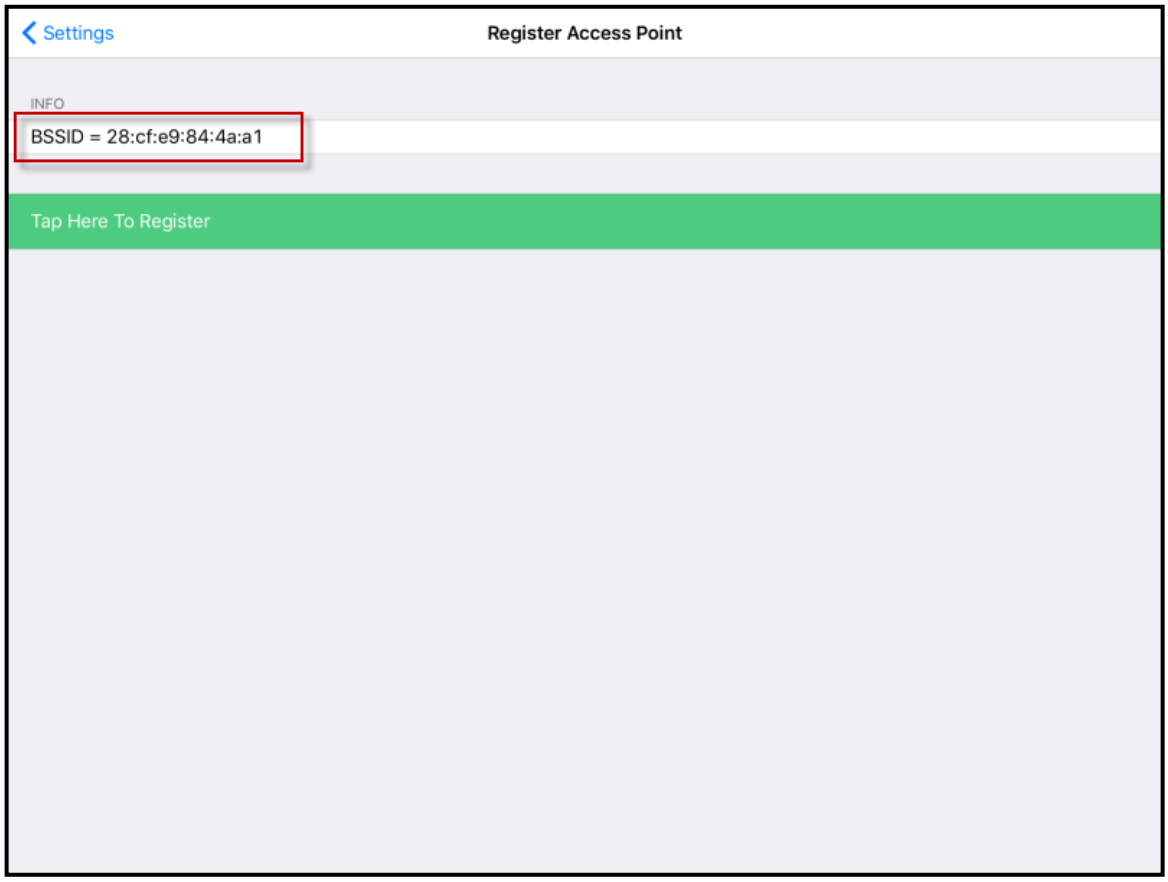
Select Configuration

Select the ThinManager Server you want to register the Wi-Fi resolver with.



Setting Page of iTMC

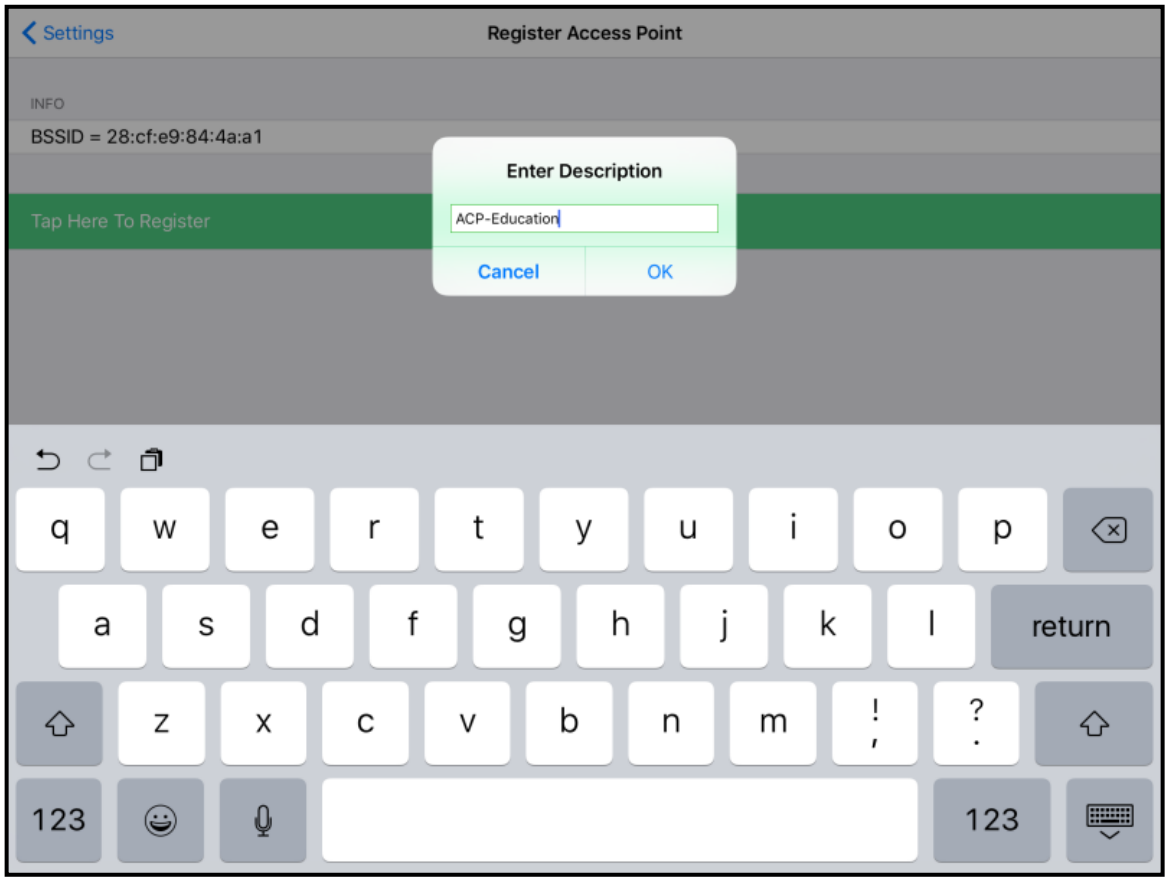
Select the ***Register Wi-Fi Access Point*** link.



Available Wi-Fi Access Points

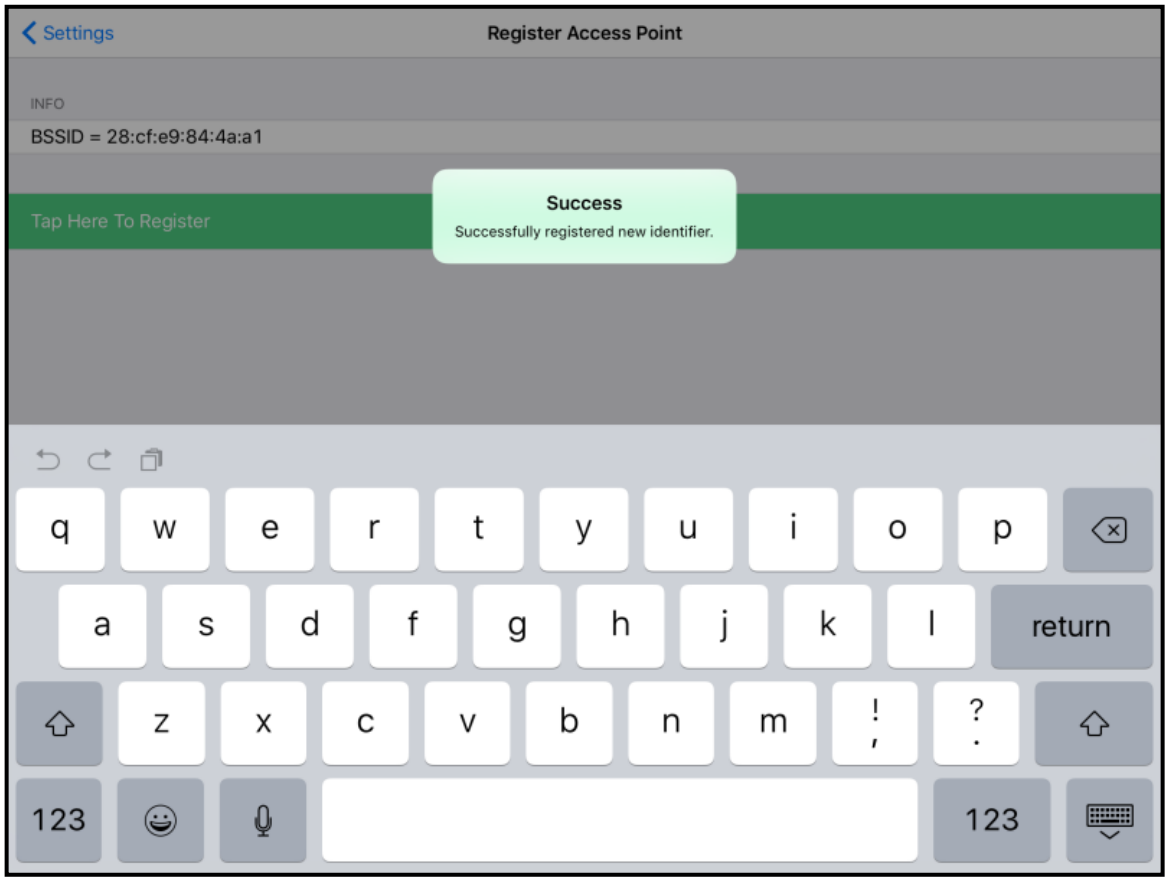
The mobile device will allow you to register the Wi-Fi Access Point you are connected to and list it on the **Register Access Points** page.

Select the access point.



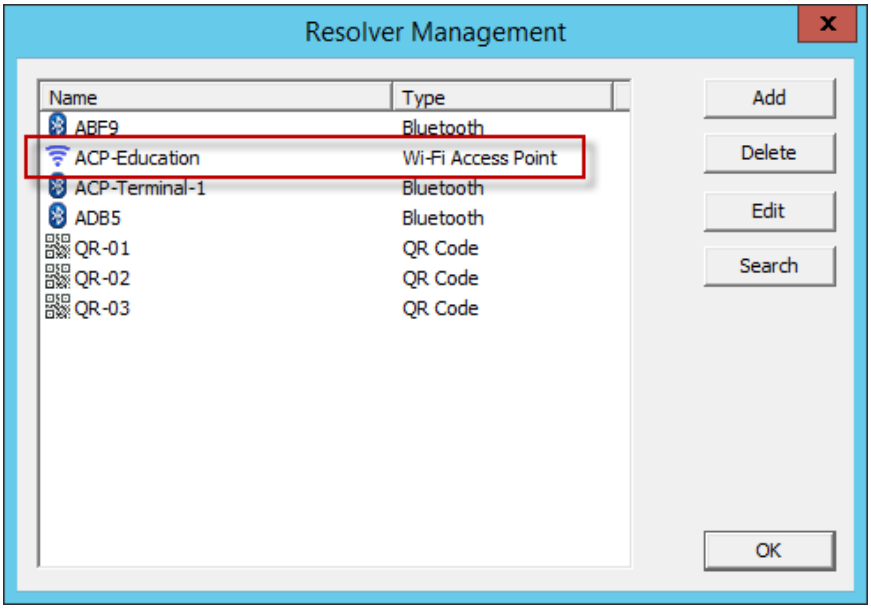
Enter Location Description

Once the data has been collected and the Wi-Fi access point is registered you will be prompted to name the location.



Success Dialog

The program will confirm successful Wi-Fi registrations.

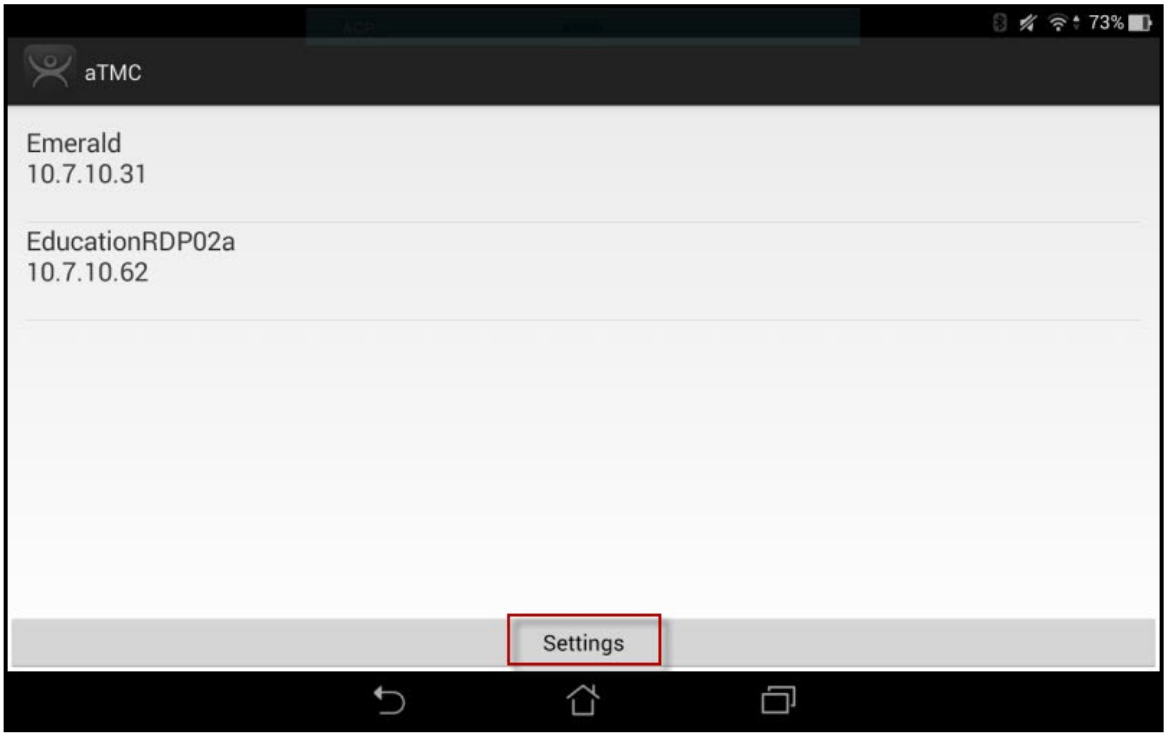


Resolver Management Window

The Wi-Fi resolver will be registered and entered in the **Resolver Management** window that is accessed by selecting ***Manage > Manage ID's***.

39.3.2. Defining Wi-Fi Access Points with an Android

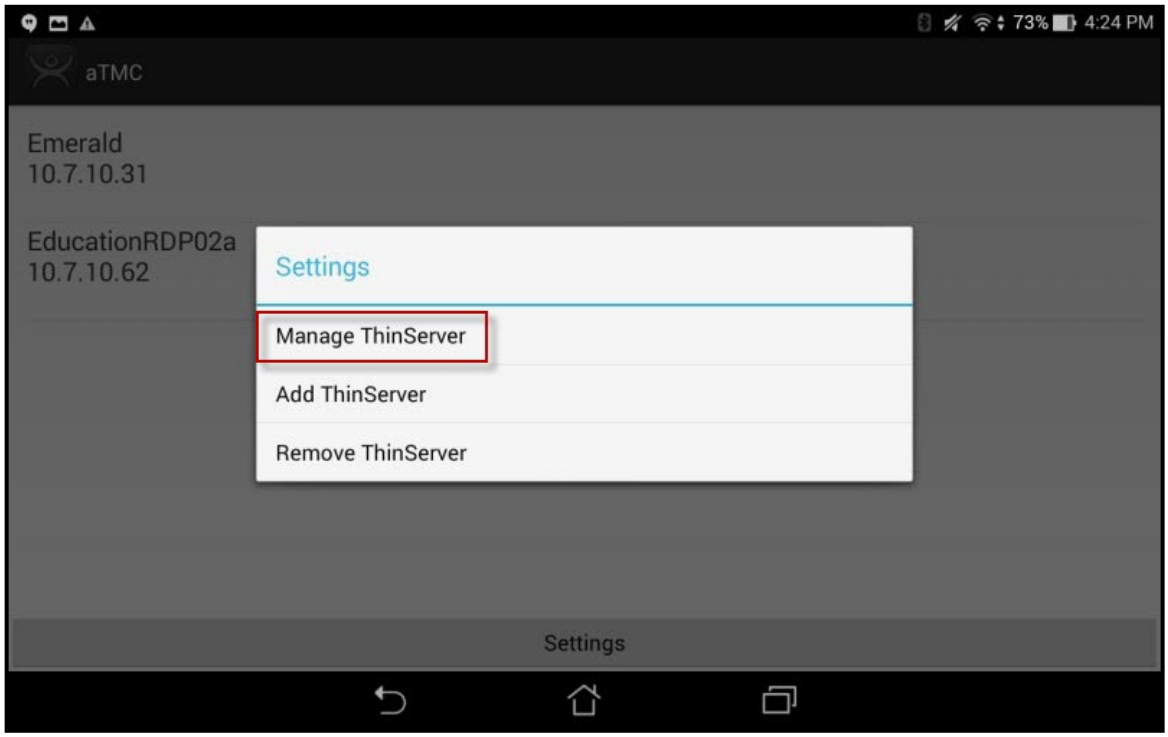
Wi-Fi access points are defined and register like the Bluetooth beacon.



ThinManager aTMC Program

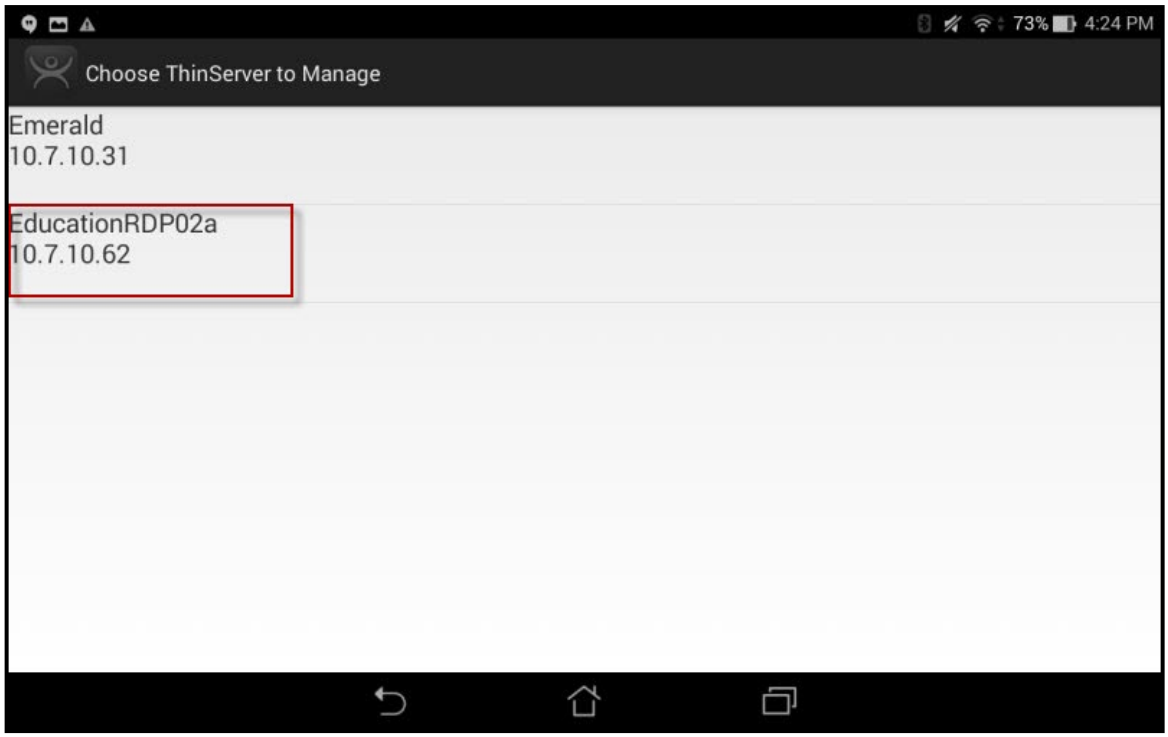
Open the **aTMC** program on the iPad.

Select the ***Settings*** button on the bottom to launch the **Settings** screen.



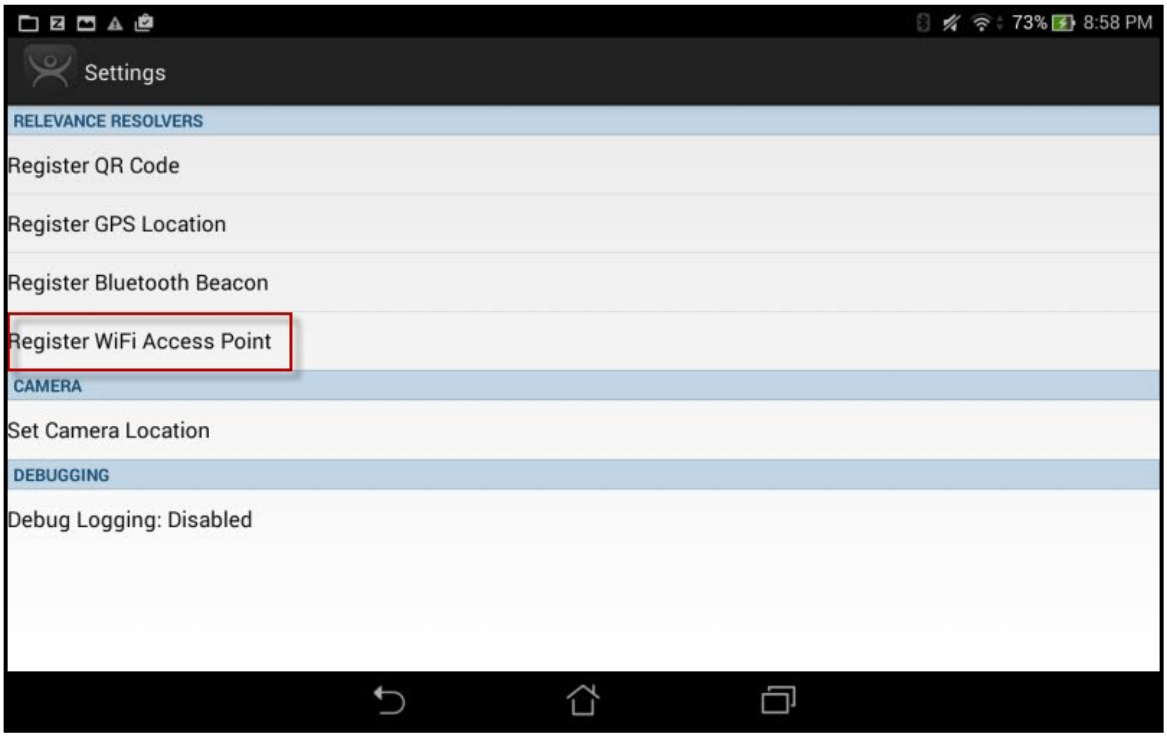
Settings Menu

Select the ***Manage ThinServer*** link.



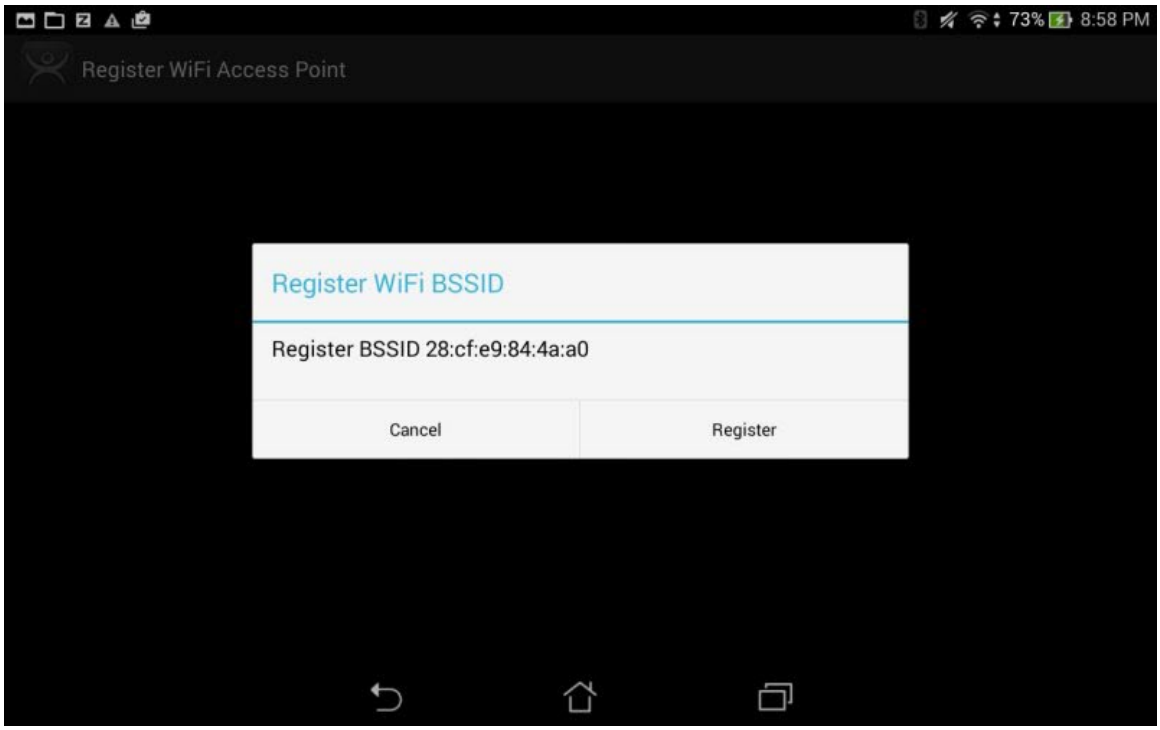
Select Configuration

Select the ThinManager Server you want to register the Wi-Fi network with.



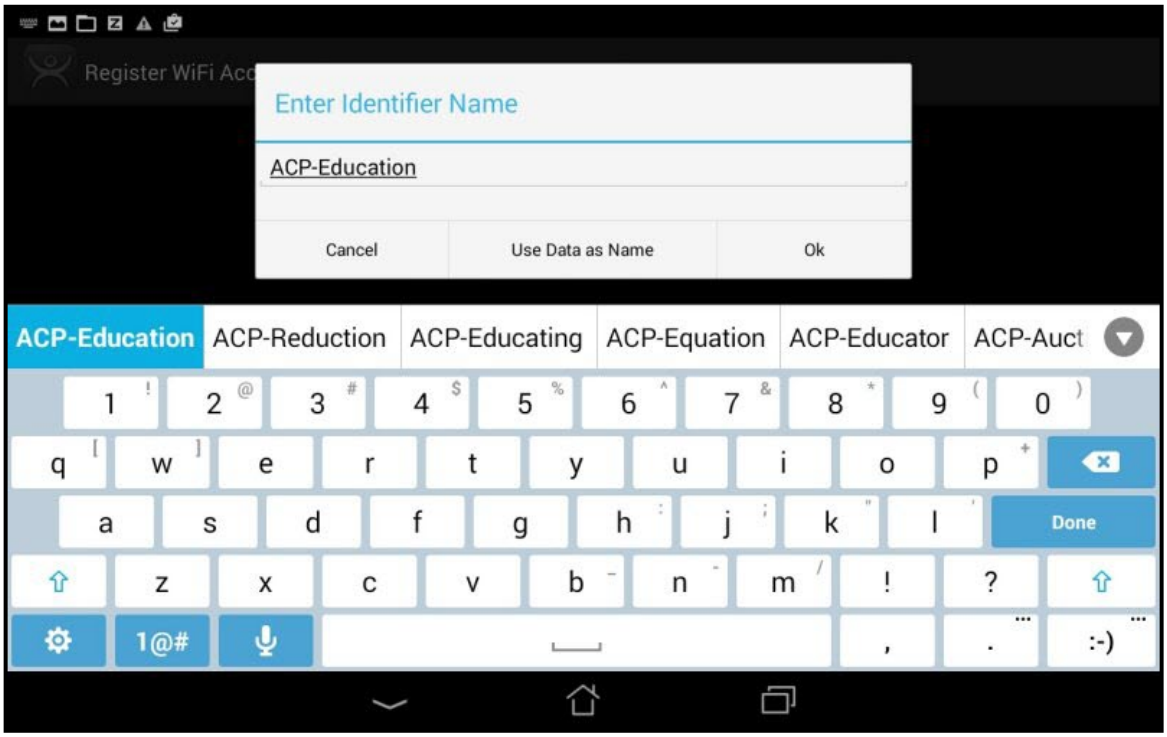
Register Bluetooth Beacon Command on the Settings Page

Select the ***Register Wi-Fi Access Point*** command on the **Settings** page.



Register Configuration

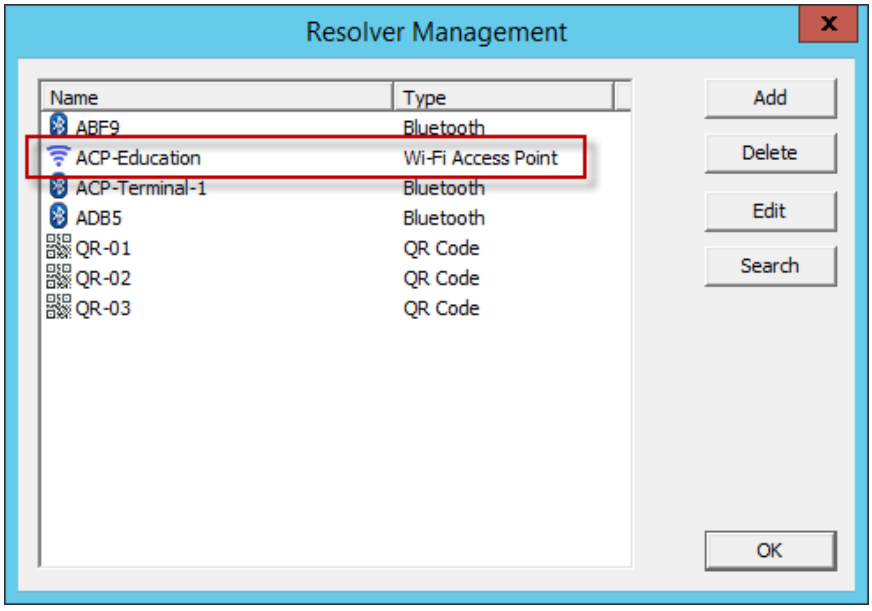
The ThinManager Server will let you register the wireless network you are connected to.



Enter Location Description

Once the Wi-Fi access point is identified you will be prompted to name the location.

Name the Wi-Fi access point and select the ***OK*** link to finish the registration process.



Resolver Management Window

The Wi-Fi access point will be registered and entered in the **Resolver Management** window that is accessed by selecting ***Manage > Manage ID's***.

39.4. GPS

Relevance can use Global Positioning, or GPS, as a location resolver. The mobile program uses the build in GPS system to identify the location.

The Global Positioning System resolver type works well for outdoor areas. It can be used to create a large Parent Location. You set up so that you must be within the GPS area for other actions to take place.

When you assign the GPS resolver to a Location, you can set the range for altitude and radius from your initial point. This will give you the ability to create a rather large area for something like an oil field, a large processing facility, or an entire building complex. You could also use it for finer resolution of individual buildings, tanks, pump jacks, or other smaller outdoor areas.

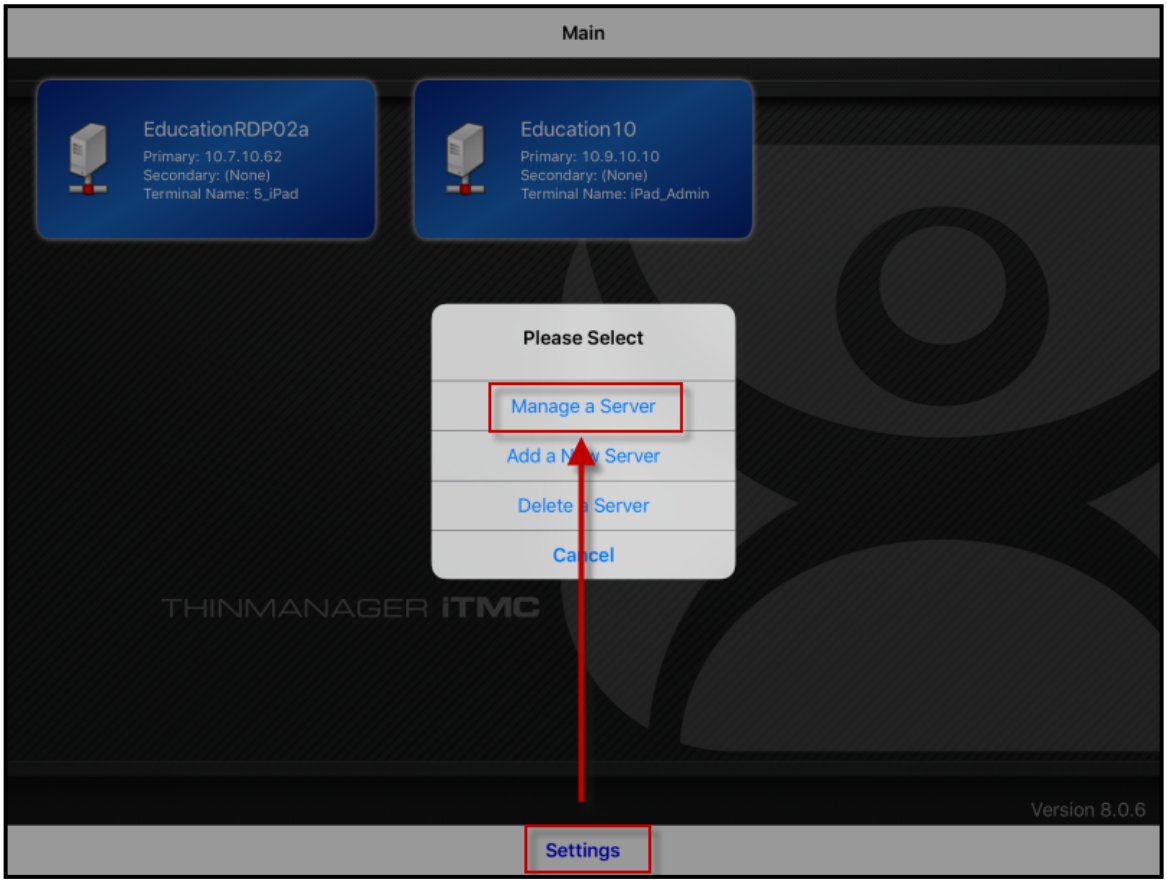
As you assign these types of resolvers, it would be best to try and avoid overlap of GPS areas.

The procedure for using GPS is:

- Allow GPS on the mobile device and in the iTMC or aTMC program.
- Launch the mobile program and select the ***Settings*** button.
- Select the ***Register GPS Location*** command under **Relevance Resolvers**. If you have more than one ThinManager Server defined you will need to pick the ThinManager Server you want the QR code registered.
- Select the location to register.
- Enter a name for the location.
- The GPS location will be registered and entered in the **Resolver Management** window that is accessed by selecting ***Manage > Manage ID's***.

39.4.1. Registering GPS with an iPad

Defining a GPS location is similar to defining a Bluetooth beacon.

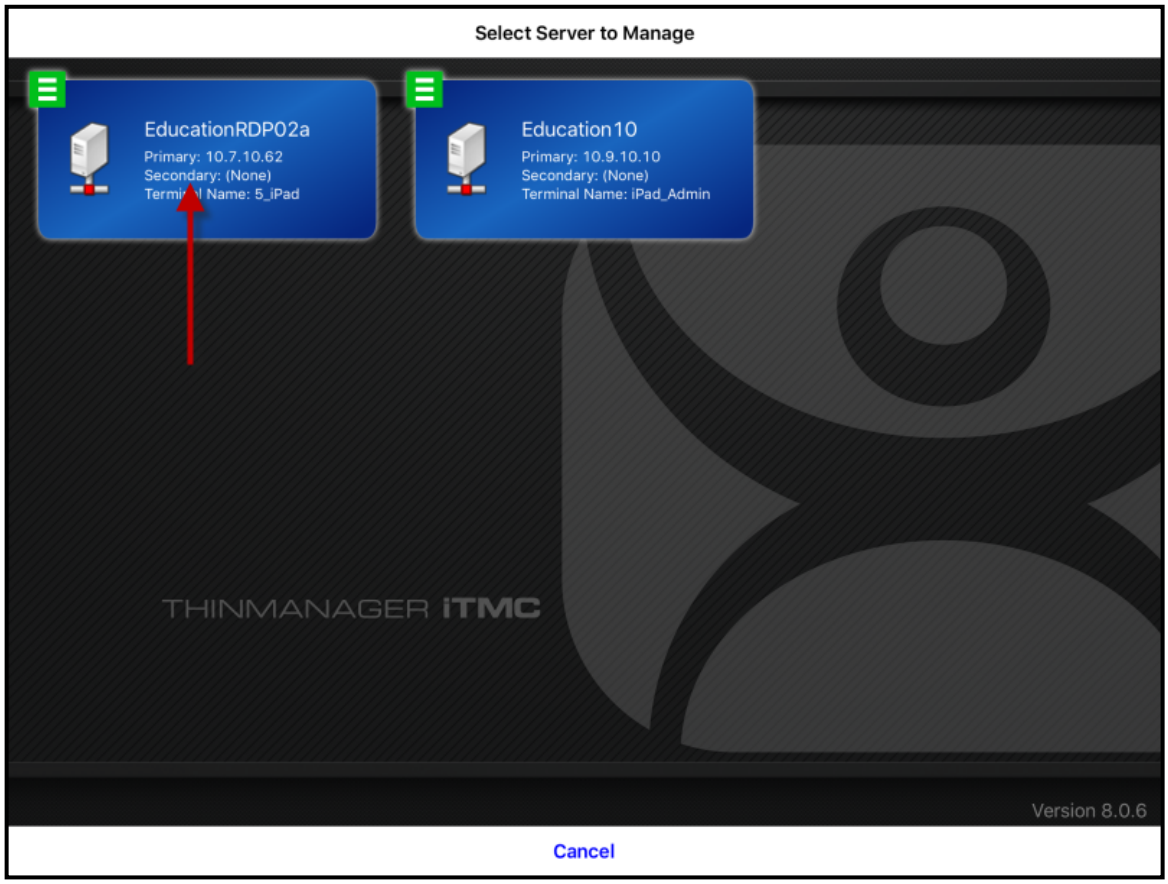


ThinManager iTMC Program

Open the **iTMC** program on the iPad.

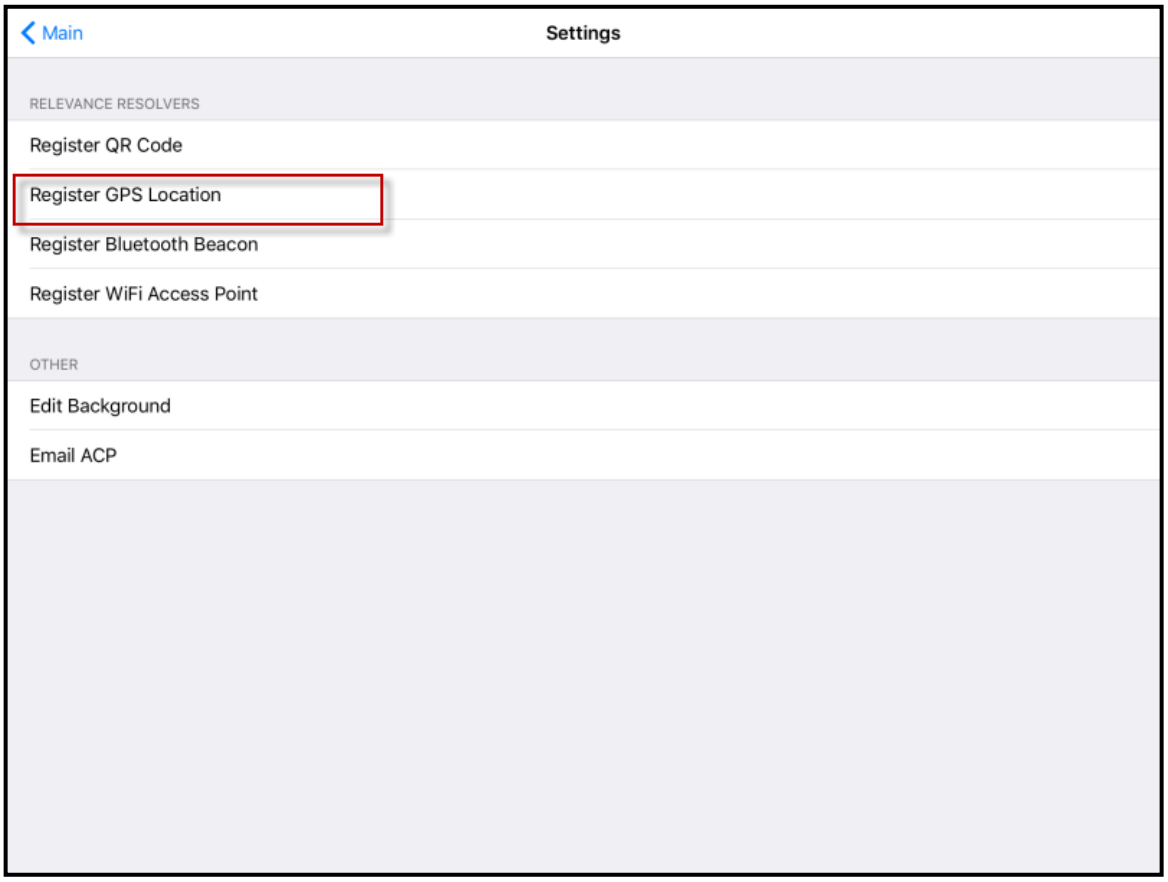
Select the ***Settings*** button on the bottom to launch the **Settings** menu.

Select the ***Manage a Server*** link.



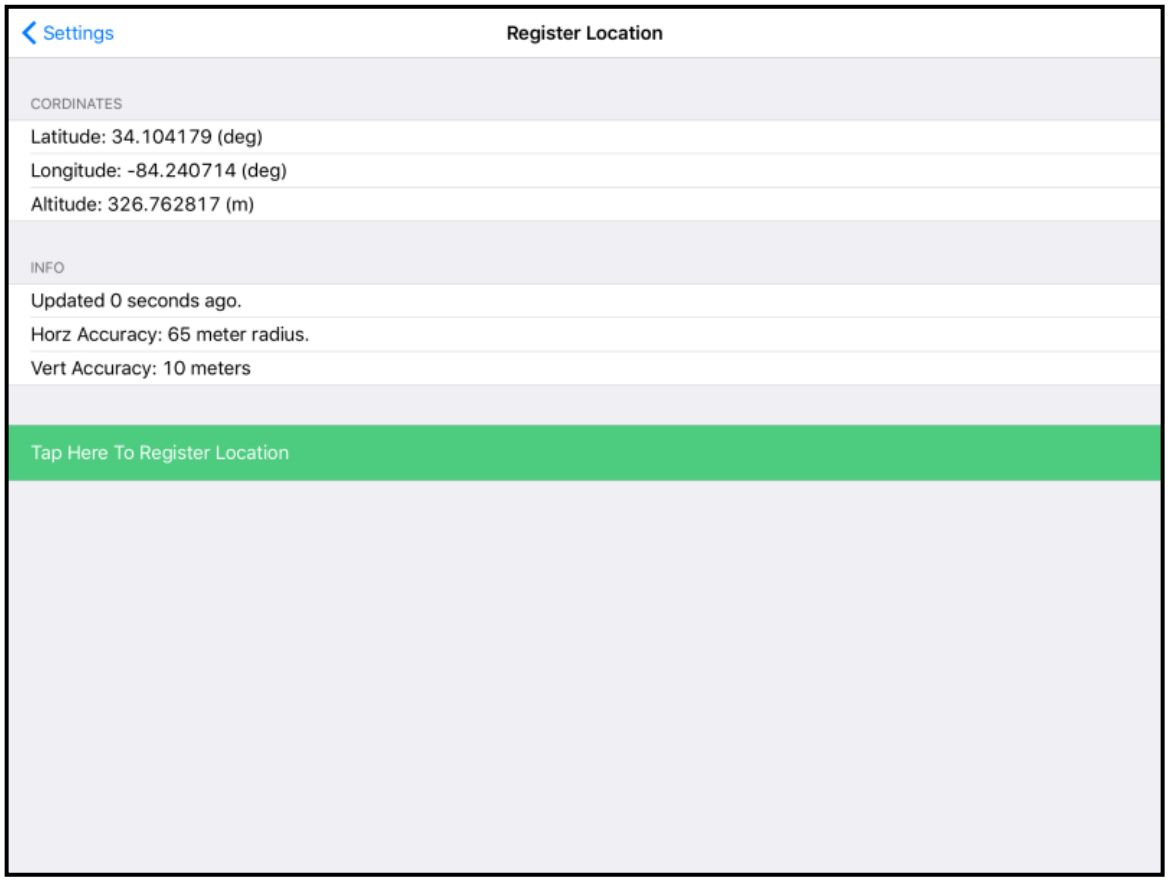
Select Configuration

Select the ThinManager Server you want to register the GPS location on.



Register GPS location Command on the Settings Page

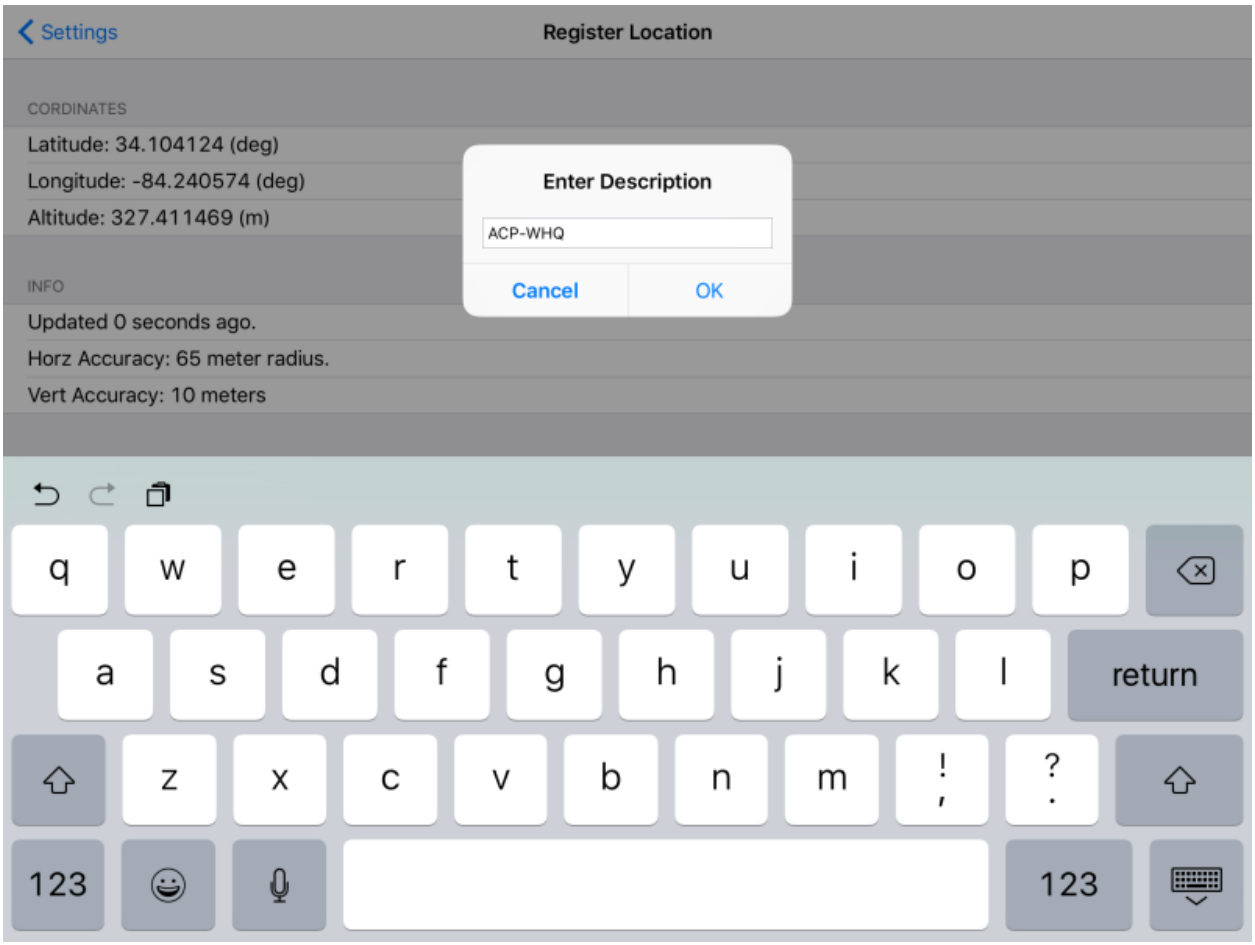
Select the ***Register GPS location*** command on the **Settings** page.



Available GPS location

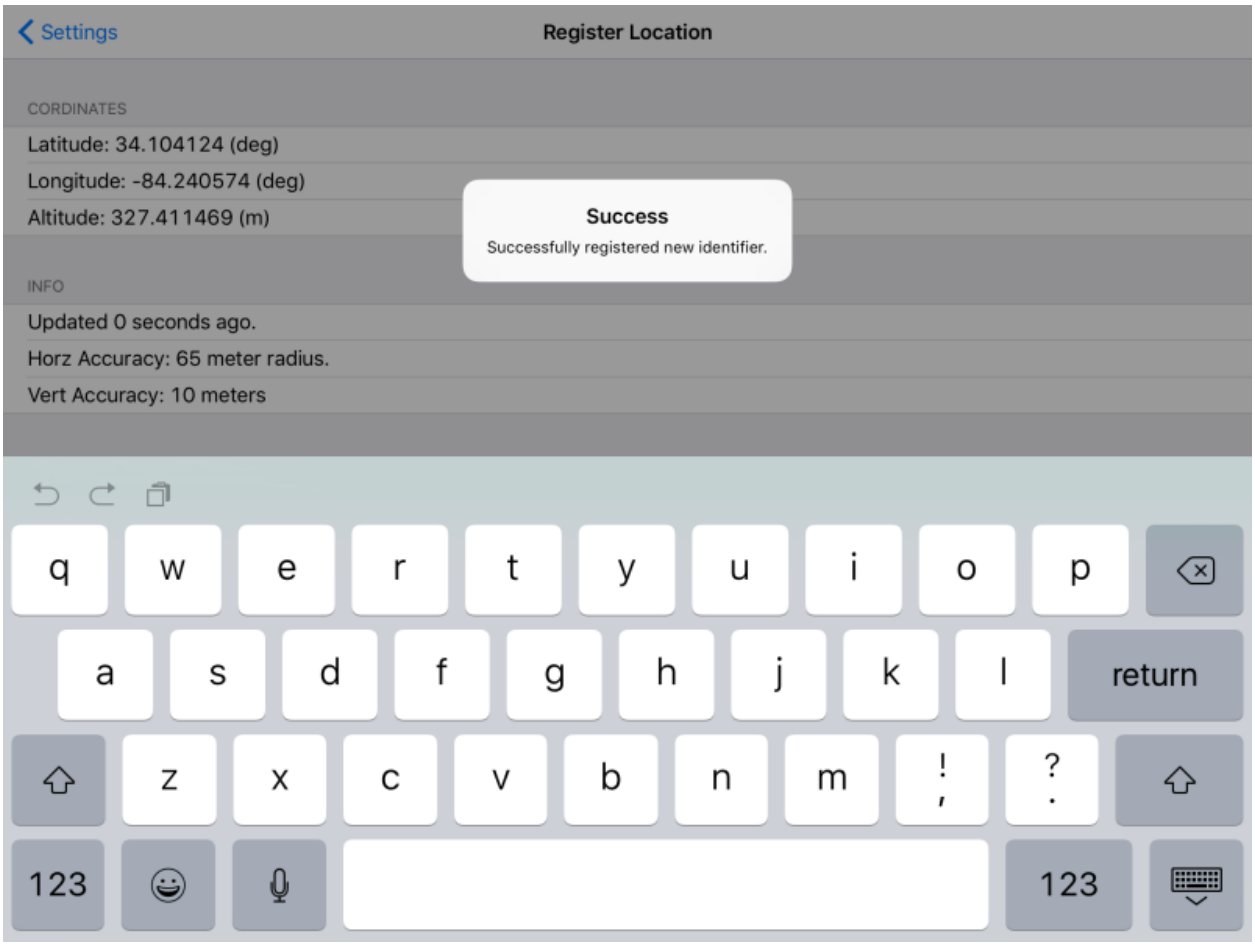
The mobile device will search for the GPS location and list it on the **Register Location** page.

Select the ***Tap Here To Register Location*** link.



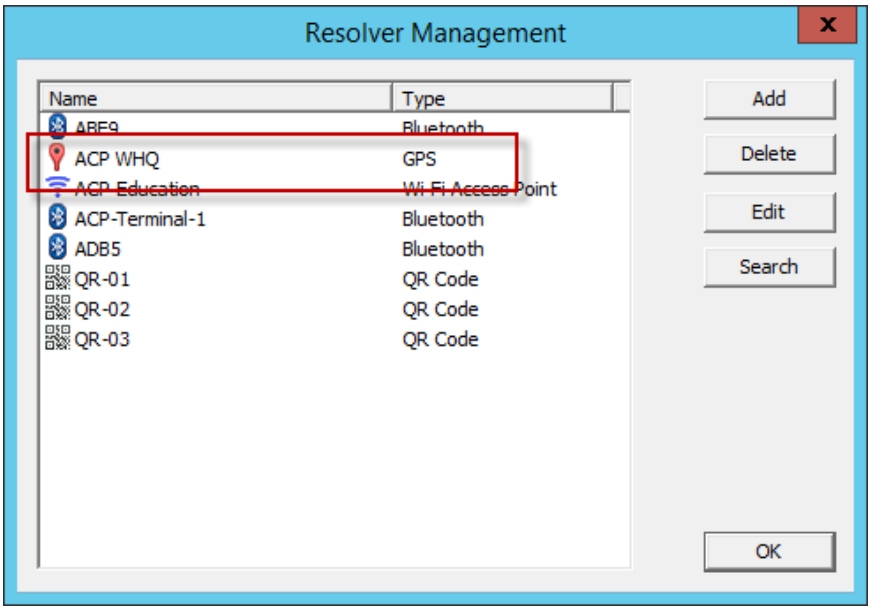
Enter Location Description

Once the data has been collected and the GPS location is registered you will be prompted to name the location.



Success Dialog

The program will confirm successful GPS location registration.

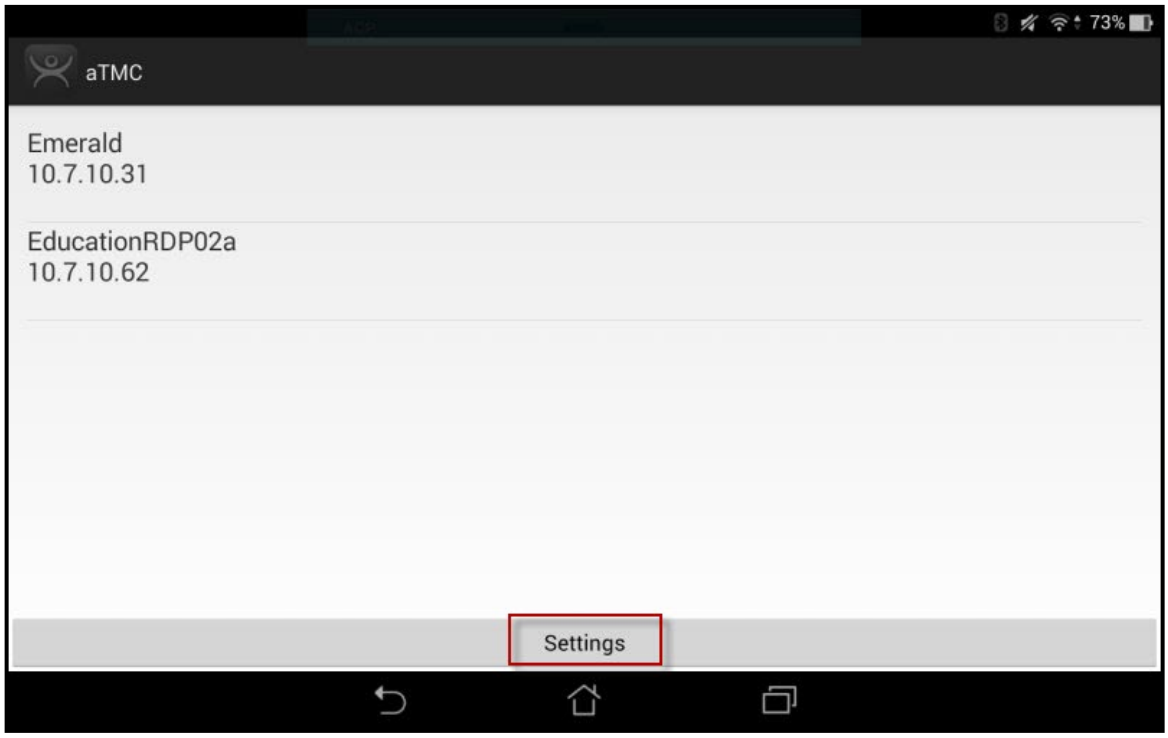


Resolver Management Window

The GPS location will be registered and entered in the **Resolver Management** window that is accessed by selecting ***Manage > Manage ID's***.

39.4.1. Registering GPS with an Android

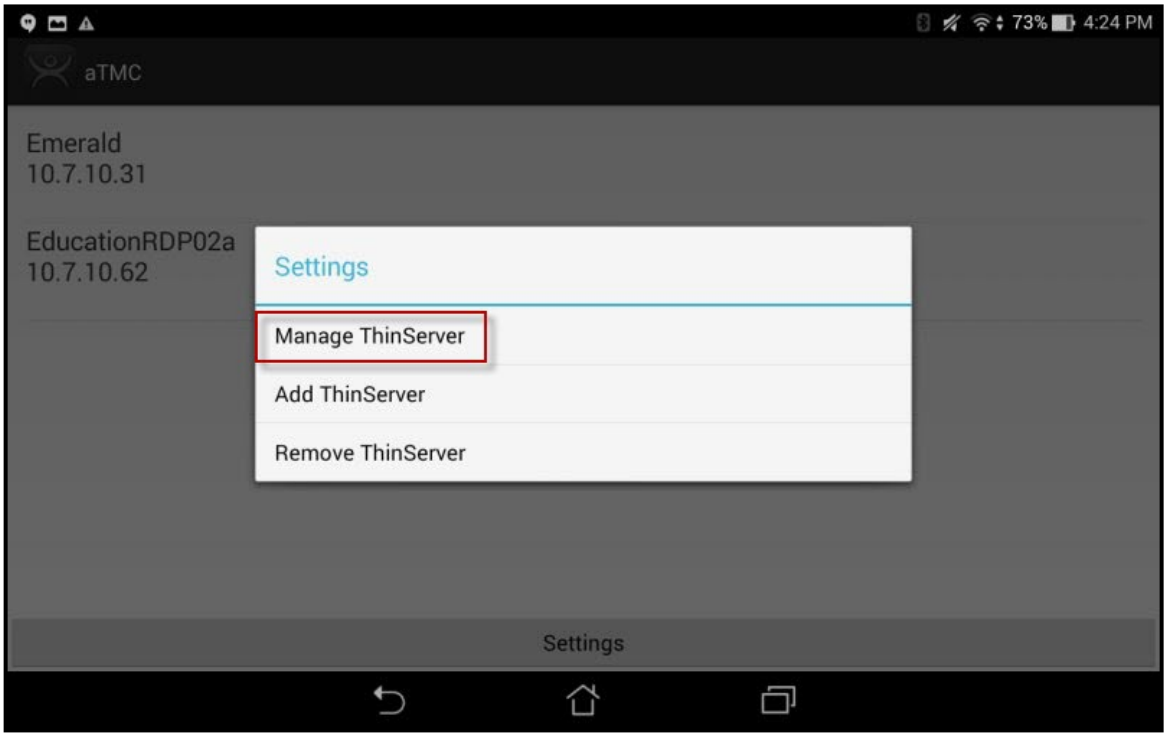
GPS locations are defined and register like the Bluetooth beacon.



ThinManager aTMC Program

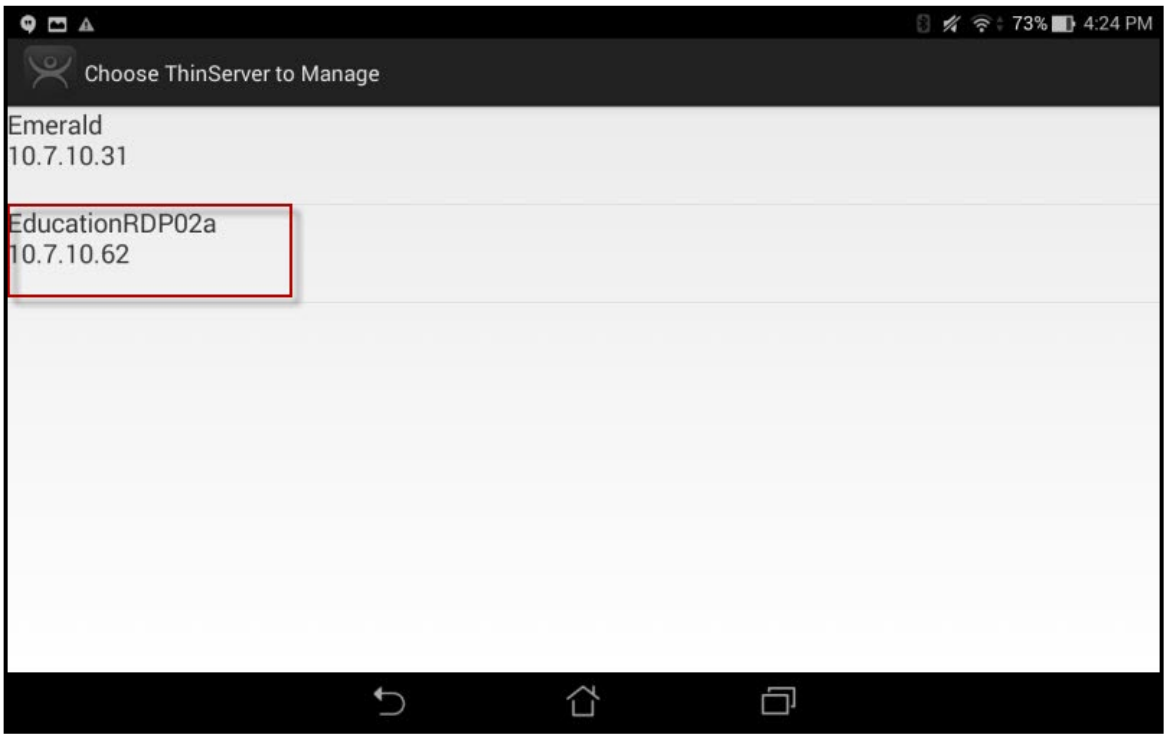
Open the **iTMC** program on the tablet.

Select the ***Settings*** button on the bottom to launch the **Settings** screen.



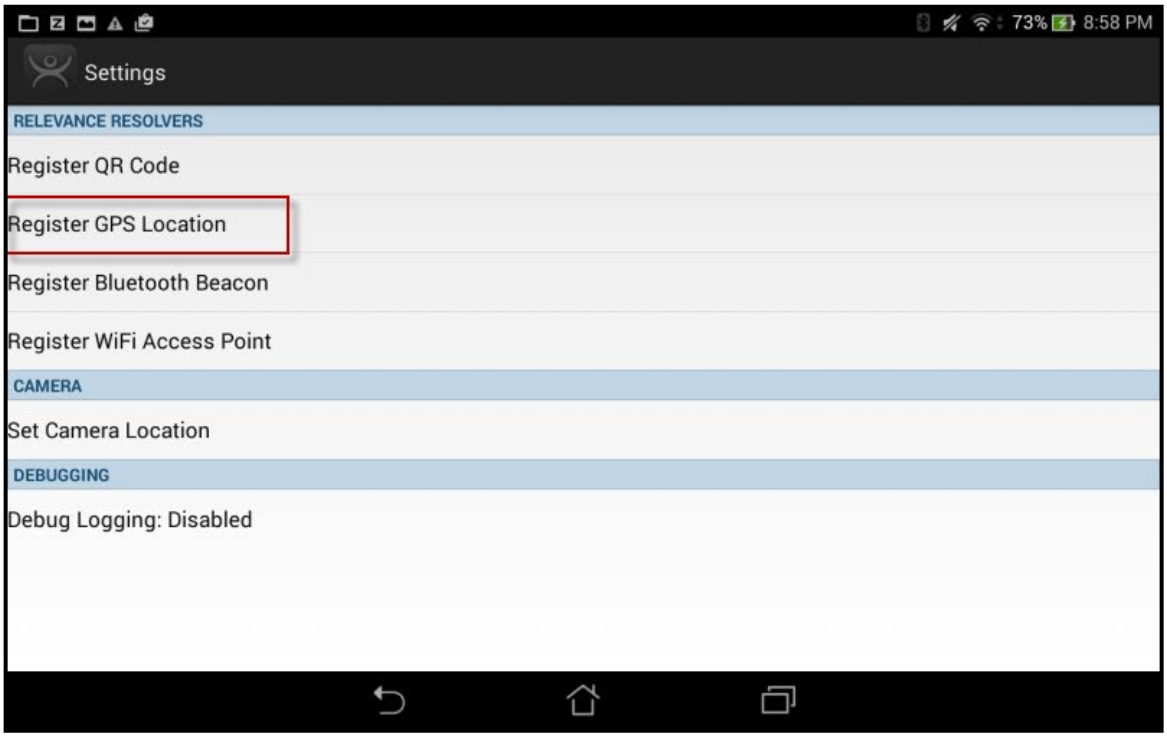
Settings Menu

Select the ***Manage ThinServer*** link.



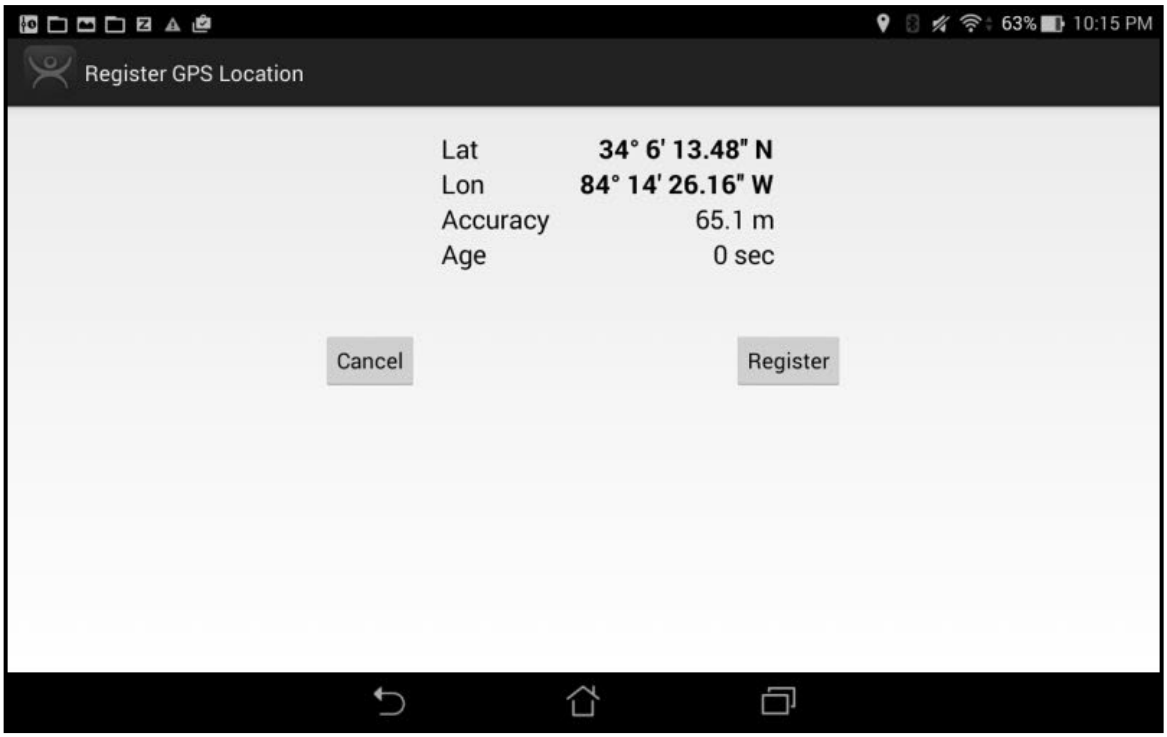
Select Configuration

Select the ThinManager Server you want to register the GPS locations with.



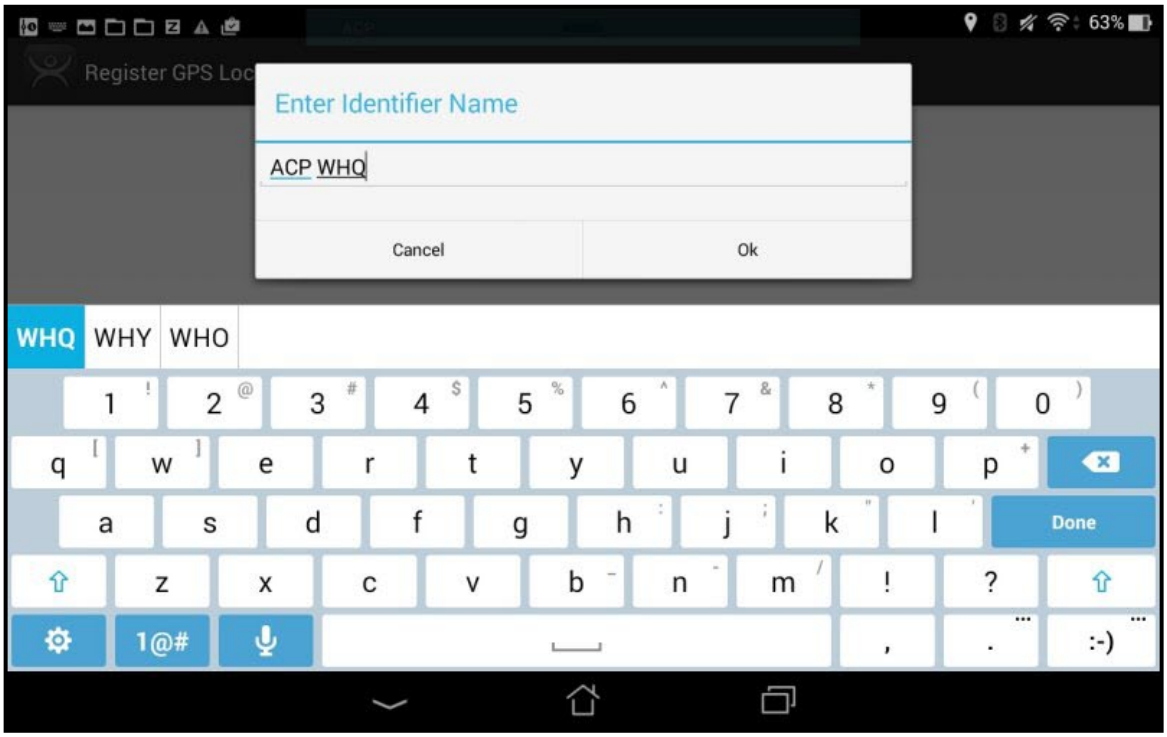
Register GPS locations Command on the Settings Page

Select the ***Register GPS Location*** command on the **Settings** page.



Register GPS Location

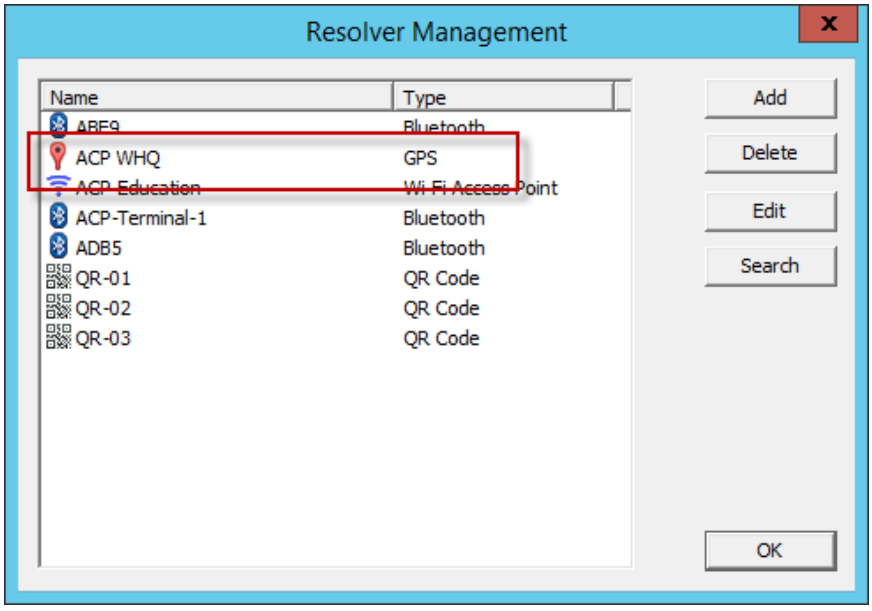
The ThinManager Server will let you register your GPS location.



Enter Location Description

Once the GPS location is identified you will be prompted to name the location.

Name the GPS location and select the ***OK*** link to finish the registration process.



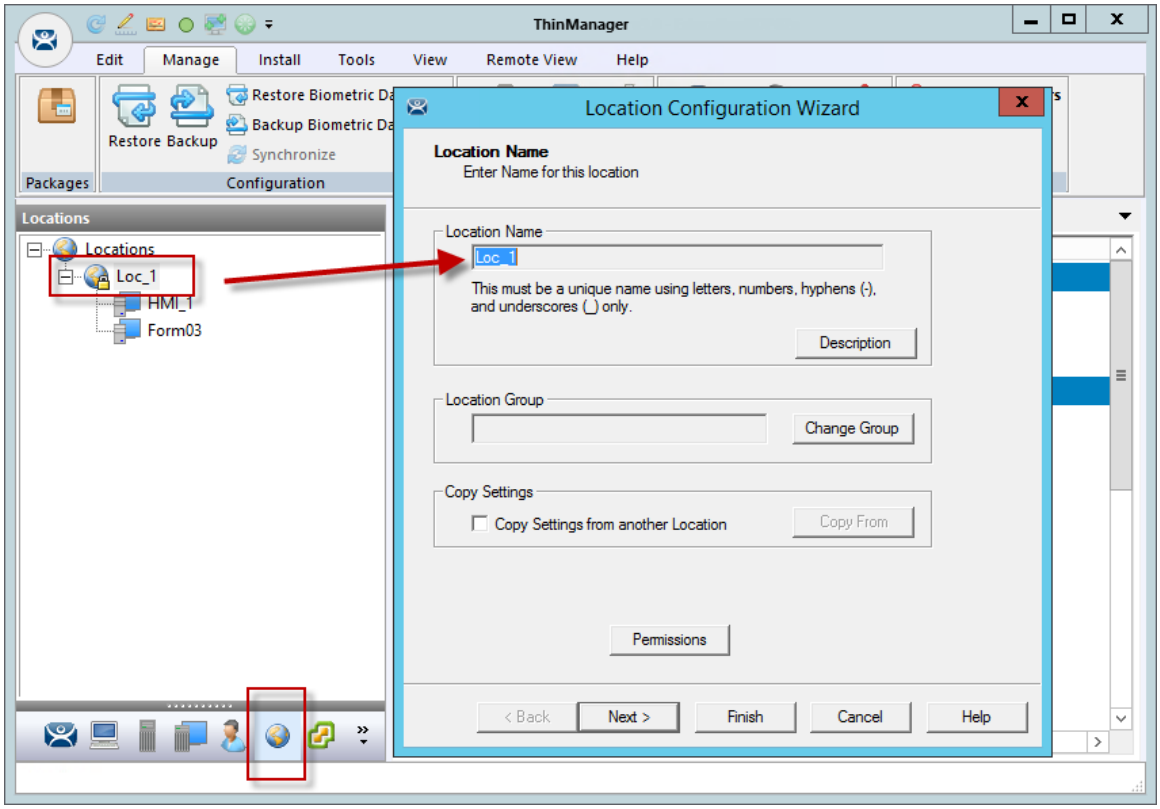
Resolver Management Window

The GPS location will be registered and entered in the **Resolver Management** window that is accessed by selecting ***Manage > Manage ID's***.

40. Adding Actions to Resolver Codes

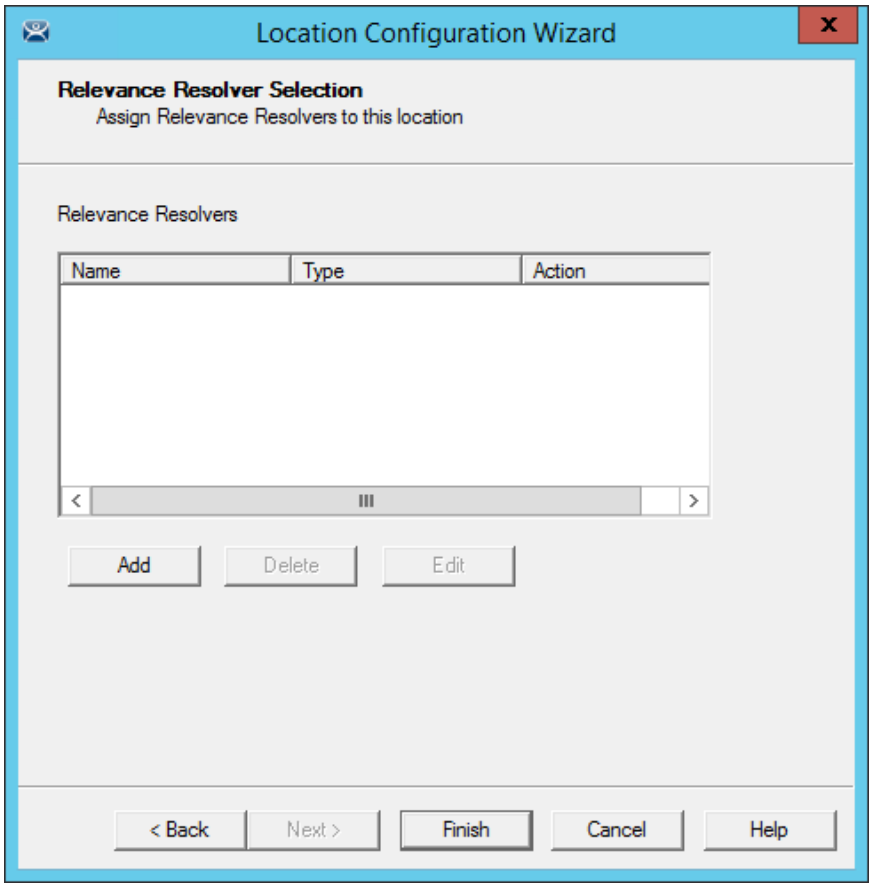
The Resolvers can be applied to a location and can have an action associated with it so that using a resolver will launch a particular action.

Select a **Location** tree from the Tree selector at the bottom of the ThinManager tree.



Location Configuration Wizard

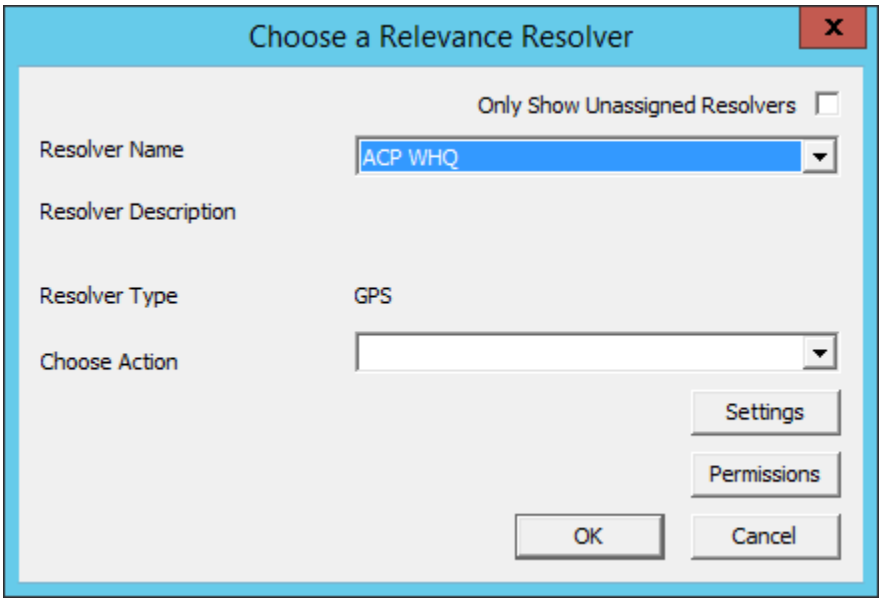
Double click a location to open the Location Configuration Wizard.



Relevance Resolver Selection Page

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

Select the ***Add*** button to open the **Choose a Relevance Resolver** window.

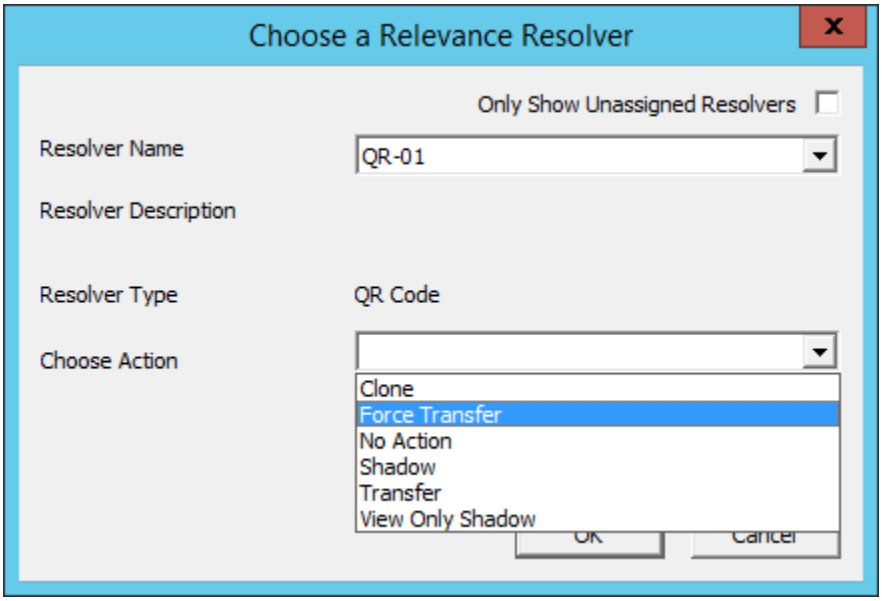


Choose a Relevance ID Window

The **Choose a Relevance ID** window has a drop-down to let you select which resolver to configure.

You can limit the list to unassigned resolvers by checking the ***Only Show Unassigned Resolvers*** checkbox. This prevents duplication.

Select a resolver in the ***Resolver Name*** drop-down.



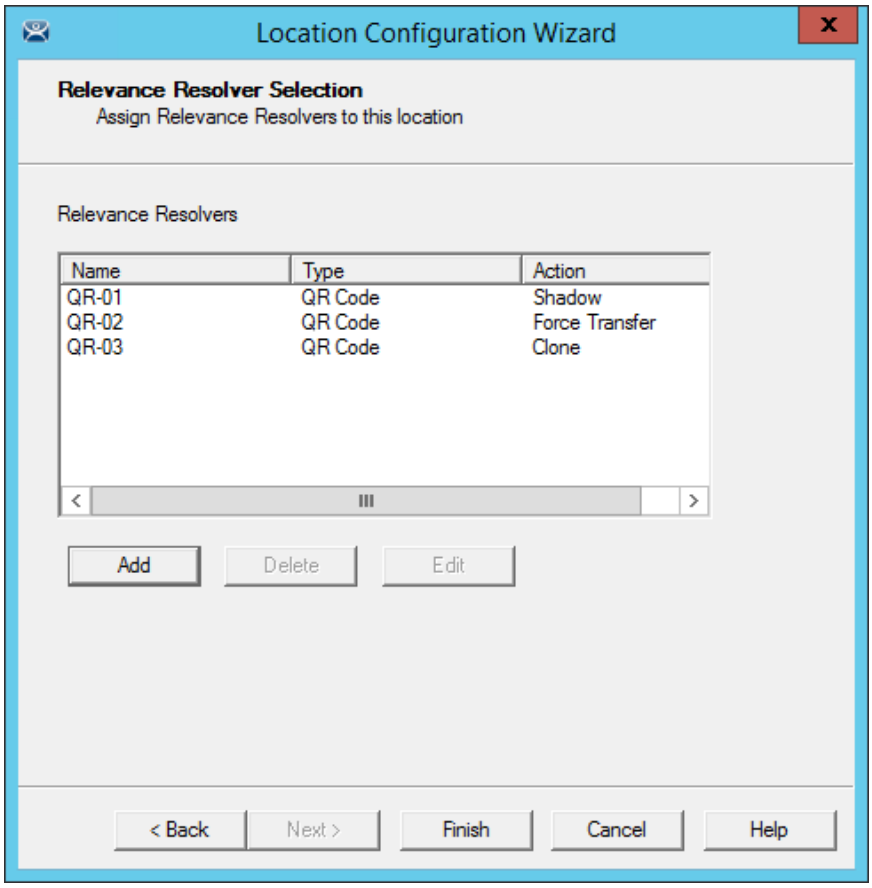
Choose Action Selection

The ***Resolver Type*** will show whether it is a QR code, Bluetooth beacon, GPS, or Wi-Fi resolver.

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 diverts the location graphic to the mobile device.
- **No Action** – This initiates no new action.
- **Shadow** – This provides an interactive shadow on the mobile device.
- **Transfer** – This diverts the location graphic to the mobile device after operator input.
- **View Only Shadow** – This provides a shadow without allowing any input from the mobile device.

Each location can have several Relevance IDs with different actions.



Relevance ID Selection Page

This example shows a location with three QR codes, each with their own action. Scanning a code will initiate the associated action.

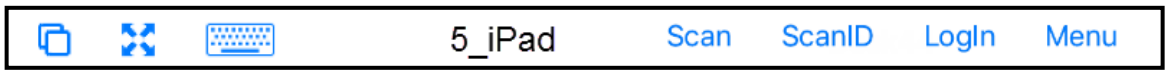
QR Code Resolver	*Action*
QR-01	Shadow
QR-02	Force Transfer
QR-03	Clone

Note: Normally you would use a **single QR code and use Permissions** to deploy the different functions. This is just a simplified example to show the concept of different actions.
See One QR Code, Multiple Actions on page 723.

41. Interacting with the Location

The iTMC client can be used to interact with the location by scanning the four resolvers configured with different actions in the previous example.

The iTMC window has a menu bar at the top with several command buttons.

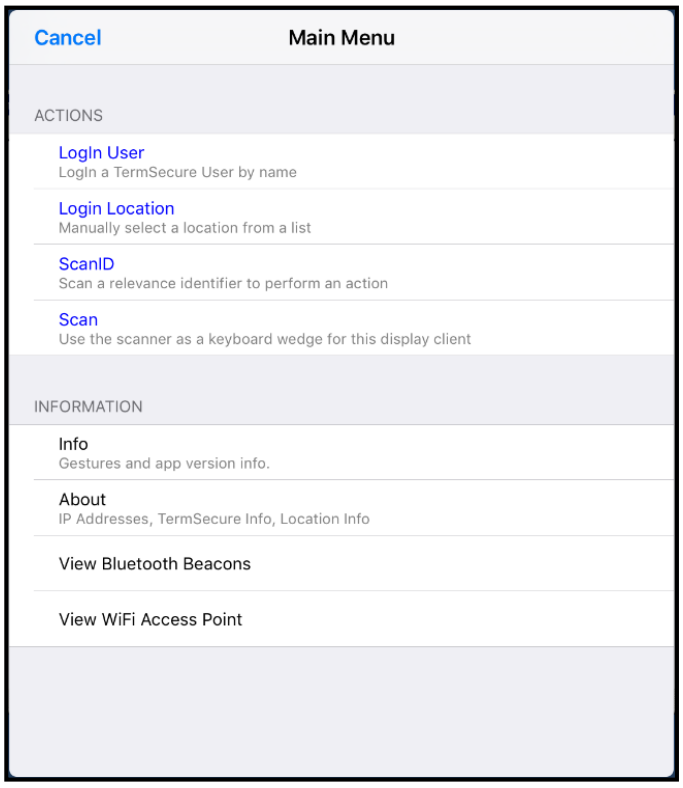


iTMC Menu Bar

The buttons are, from right to left:

- **Switch** – The cascaded square icon will allow you to switch between two or more Display Clients.
- **Full Screen** – The four arrow icon will make the display client full screen. Touching the screen with three fingers will restore the view.
- **Keyboard** – The keyboard icon will launch an on-screen keyboard.
- **Name** – The center space will show the name of the Terminal, the name of the Relevance user, or the name of the display client, depending on the state of the Terminal.
- **Leave** – This will end the action that was initiated by the original scan.
- **Scan**– This allows the scan window to act as a keyboard wedge to pull data into the session.
- **Scan ID** – This will open the Scan Identified window to scan QR codes to resolve a location or action.
- **Login** – This opens the Relevance login window to allow you to login with a Relevance user name.
- **Menu** – This will launch the Main Menu screen.

Touch the ***Main Menu*** button to launch the main menu.



Main Menu

The **Main Menu** has a variety of functions. What is displayed depends on the state of the application

Actions:

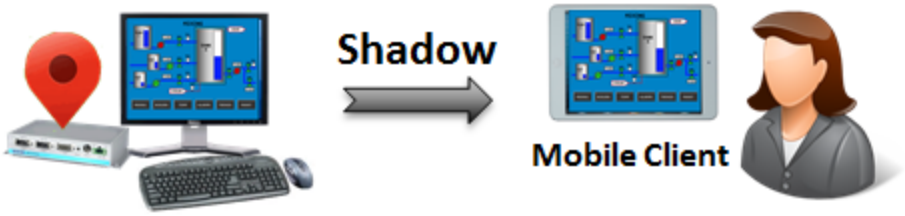
- **Login User** – this launches a dialog box for logging in as a Relevance user.
- **Login Location**– This allows you to manually select a location.
- **Login Location**– This allows you to manually select a location.
- **Scan ID** – This will open the Scan Identified window to scan QR codes to resolve a location or action.
- **Scan**– This allows the scan window to act as a keyboard wedge to pull data into the session.

Information

- **Info** – This gives version numbers and lists gestures for navigating the program.
- **About** – This launches a dialog box with user, location, and network information.
- **View Bluetooth Beacons** – This lists the Bluetooth beacons within range and their signal strength
- **View Wi-Fi Access Point** – This lists the BSSID of the Wi-Fi network you are connected to.
- **Hide Map When Zoomed** – Normally zooming on the screen provides a map so you can see what part of the screen you are looking at. This hides the map during zooming.

41.1. Shadow

Shadowing duplicates the graphic output of the location and sends it to the mobile device.

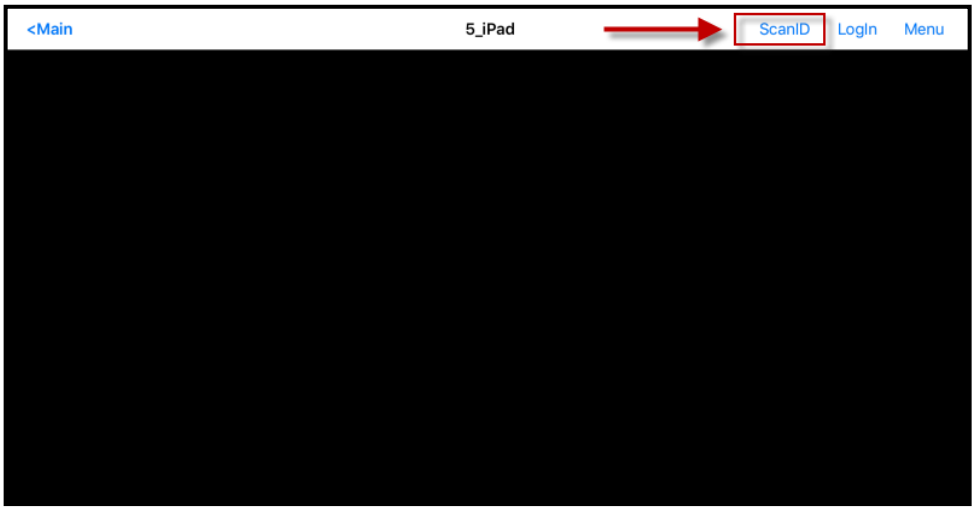


Shadowing

The mobile user will see the exact display as the location.

Launch the iTMC application.

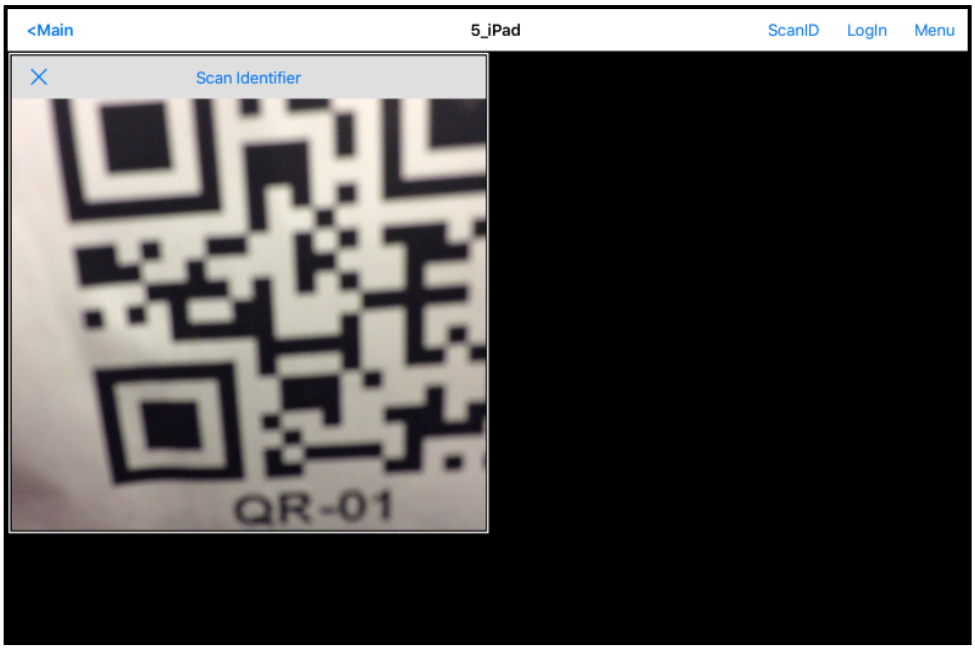
Select your ThinManager Server on the configuration screen to run your iPad as a Terminal.



ThinManager iTMC Main Screen

The Main Screen has a menu bar at the top with ***<Main***, ***ScanID***, ***Login***, and ***Menu***.

Touch the ***ScanID*** button in the upper right to launch the **Scan Identifier** window.



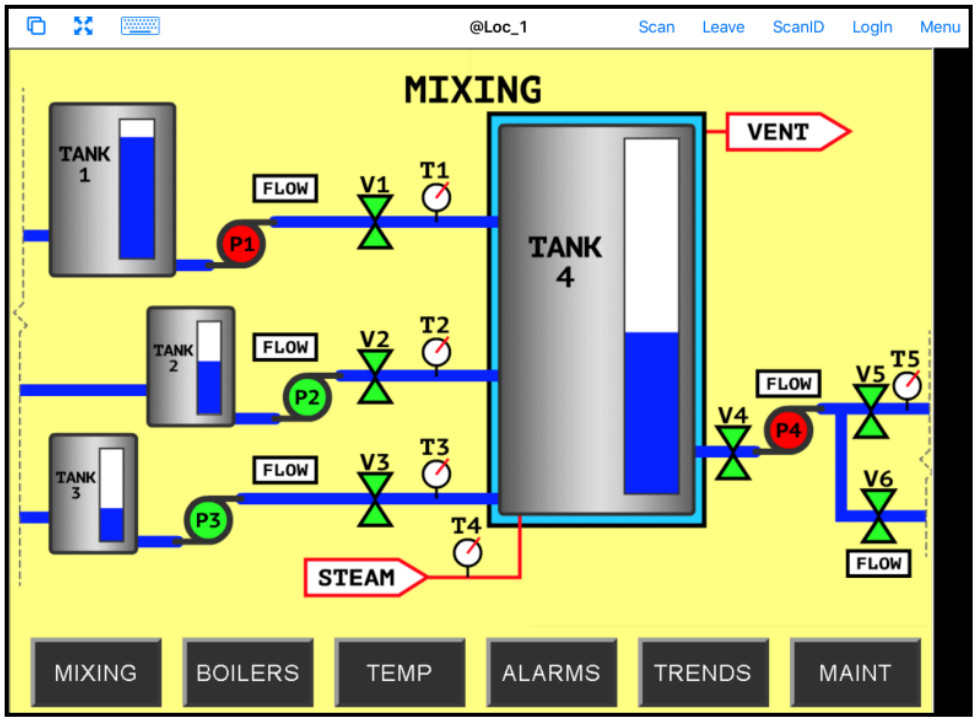
Scan Identifier Window

Touching the ***Scan ID*** button will launch the onboard camera as the **Scan Identifier** window.

Position the camera over the resolver code.

The device will read the code and act on it.

Note: The screenshots of QR codes are blurry because they register and close as soon as they are in focus.



Shadowed Session on iTMC Client

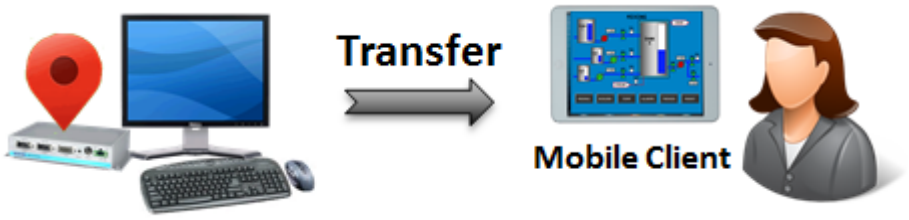
The iTMC client is now be shadowing the location because the resolver had the shadow action applied to it.

Press ***Leave*** to end the **Shadow** action.

41.2. Forced Transfer

Transferring sends the graphic output of the location to the mobile device instead of the location. This can be done automatically with Forced Transfer or set to require the operator to manually allow the transfer.

Forced Transfer takes control without operator input.

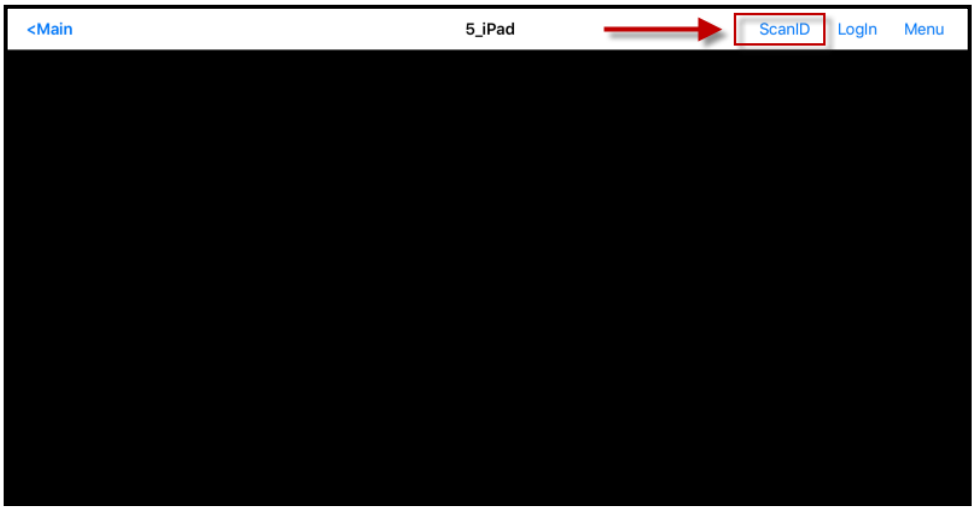


Forced Transfer

This prevents someone from taking the session while the operator is busy with a process. It also allows a mobile user to take sole control of the location.

Launch the iTMC application.

Select your ThinManager Server on the configuration screen to run your iPad as a Terminal.



ThinManager iTMC Main Screen

The Main Screen has a menu bar at the top with ***<Main***, ***ScanID***, ***Login***, and ***Menu***.

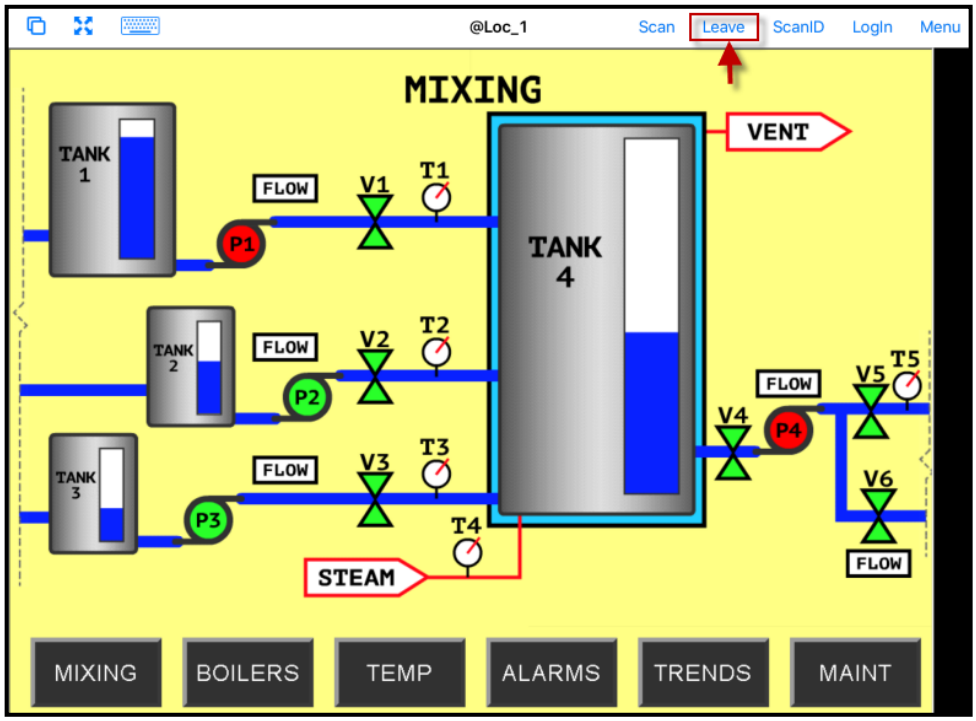
Touch the ***ScanID*** button in the upper right to launch the **Scan Identifier** window.

Touching the ***Scan ID*** button will launch the onboard camera as the **Scan Identifier** window.

Scan Identifier Window

Scan the resolver associated with Forced Transfer. The display will be ported to the mobile device.

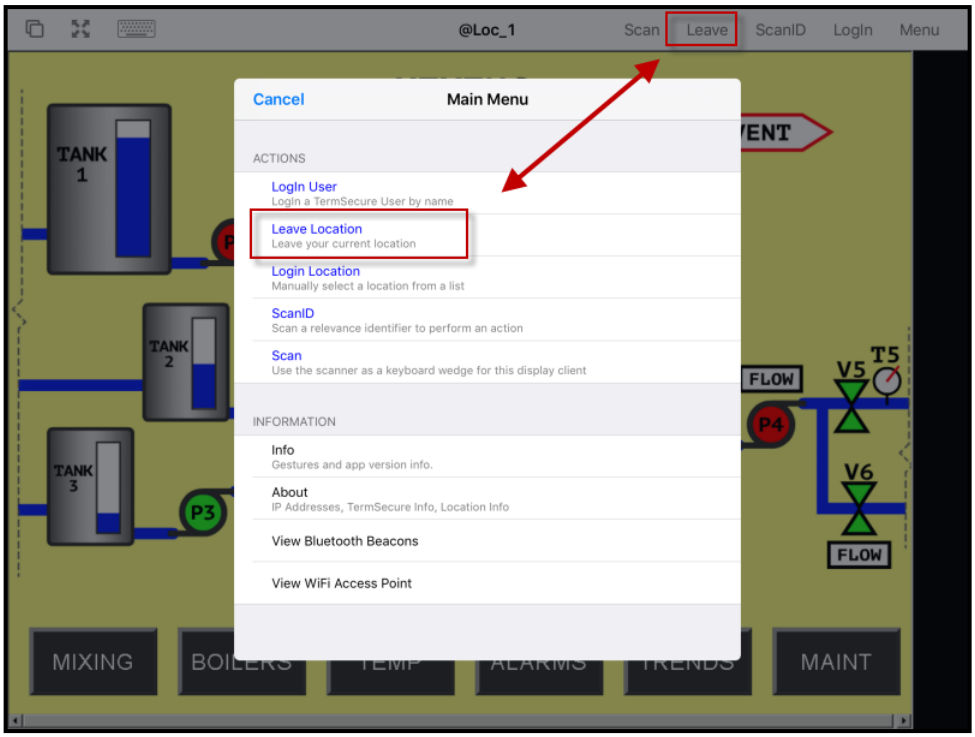
Note: The screenshots of QR codes are blurry because they register and close as soon as they are in focus.



Transfer on the Mobile Device

The display from the location will be moved to the mobile device.

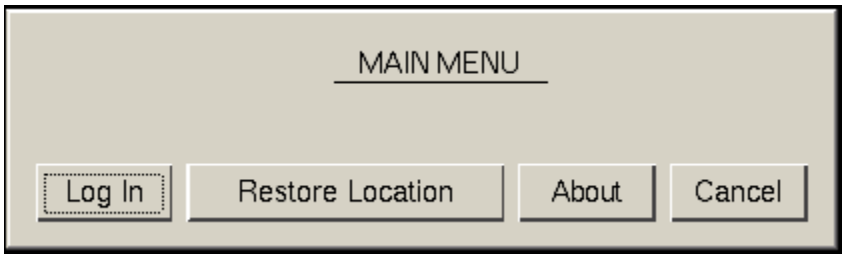
When the action of the resolver is "**Forced Transfer**" the display at the location will automatically be transferred to the scanning iTMC client



Forced Transfer at Location

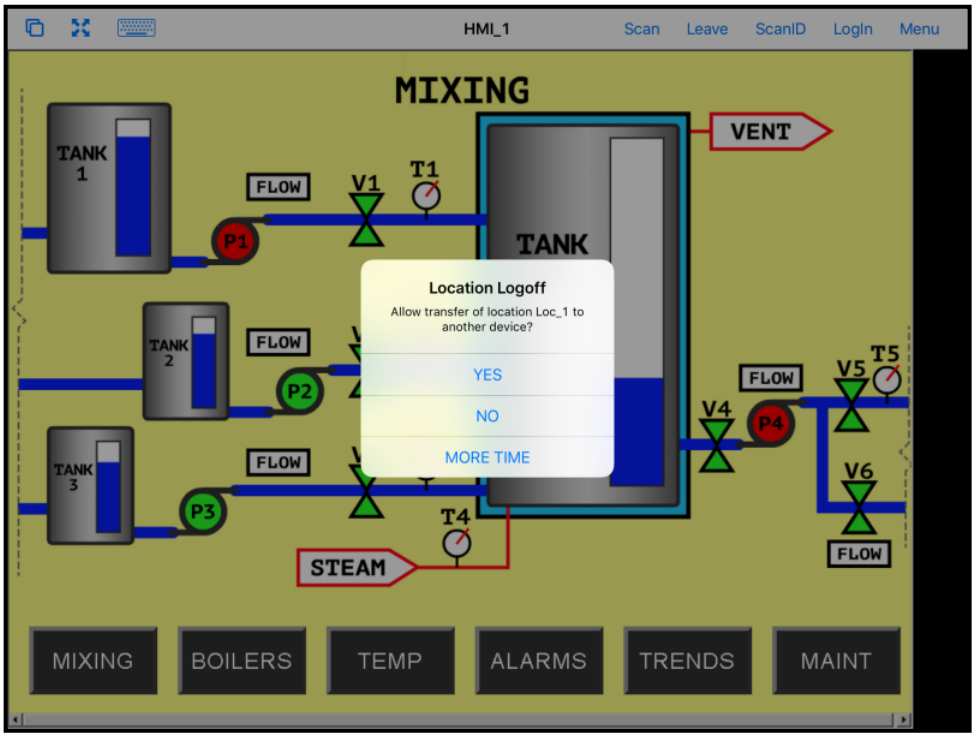
The mobile user can end the transfer by selecting the ***Leave*** command form the top menu bar or the ***Leave Location*** command on the **Main Menu**.

A message box will be displayed on the client to explain that the display is transferred. You can recall the display with the ***Restore Location*** button.



Main Menu at the Location

Go to the location and ***Select Restore Location***.



Location Logoff Dialog Box

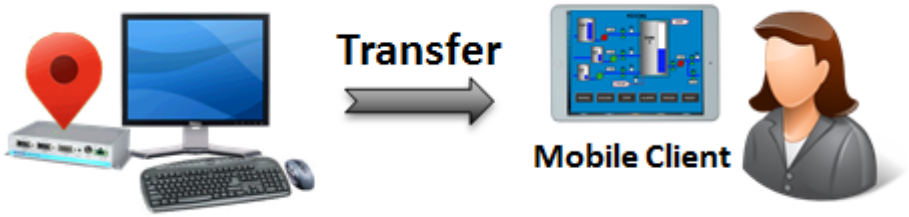
The iTMC client will display a Location Logoff dialog box when a restoration request is initiated.

- ***Yes*** – This allows the restoration of the display.
- ***No*** – This refuses the restoration of the display.
- ***More Time*** – This sends a request to the location asking for more time. The location gets a message with Yes and No that gives them the power to allow more time or to end the transfer.

41.3. Transfer

Transferring sends the graphic output of the location to the mobile device instead of the location. This can be done automatically with Forced Transfer or set to require the operator to manually allow the transfer.

Transfer requires operator input to allow the transfer.

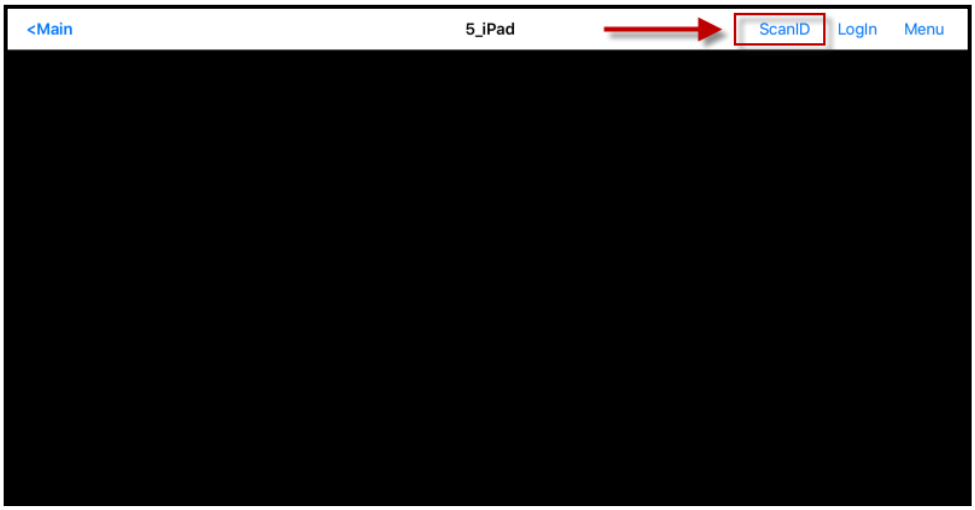


Transfer

This prevents someone from taking the session while the operator is busy with a process. It also allows a mobile user to take sole control of the location.

Launch the iTMC application.

Select your ThinManager Server on the configuration screen to run your iPad as a Terminal.

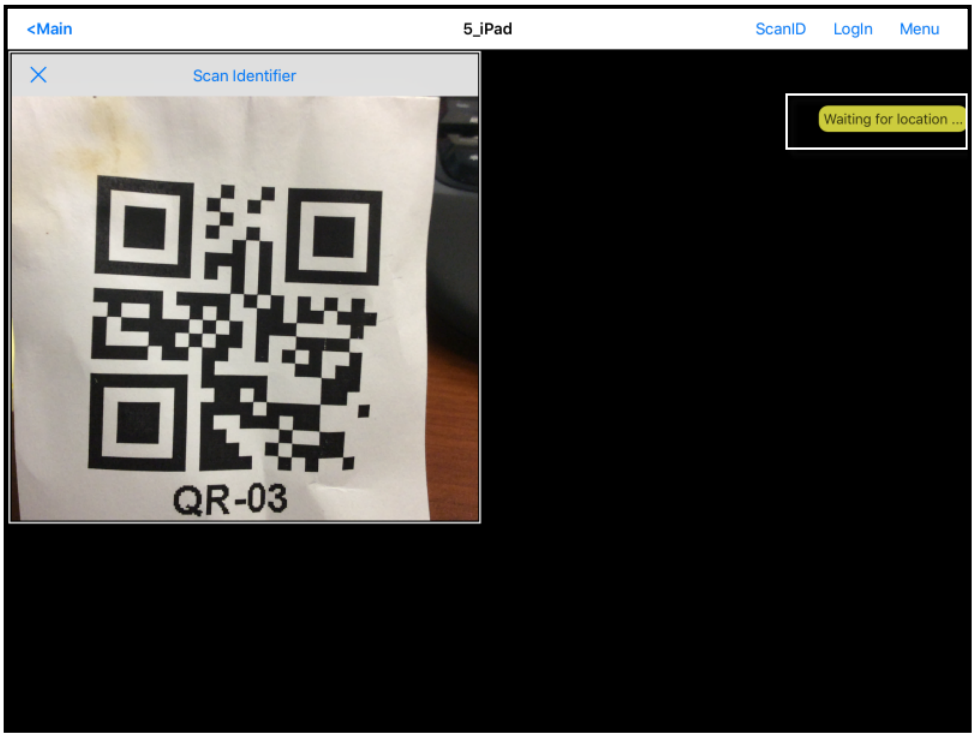


ThinManager iTMC Main Screen

The Main Screen has a menu bar at the top with ***<Main***, ***ScanID***, ***Login***, and ***Menu***.

Touch the ***ScanID*** button in the upper right to launch the **Scan Identifier** window.

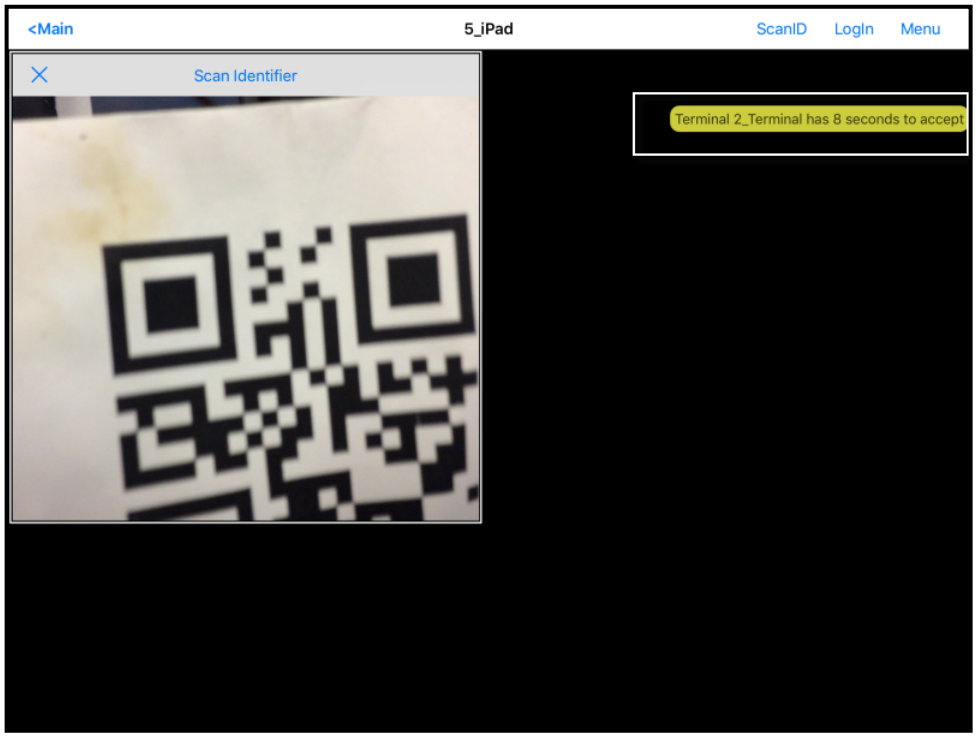
Touching the ***Scan ID*** button will launch the onboard camera as the **Scan Identifier** window.



Scan Identifier Window

Scan the resolver associated with **Transfer**. A request for transfer will be sent to the location.

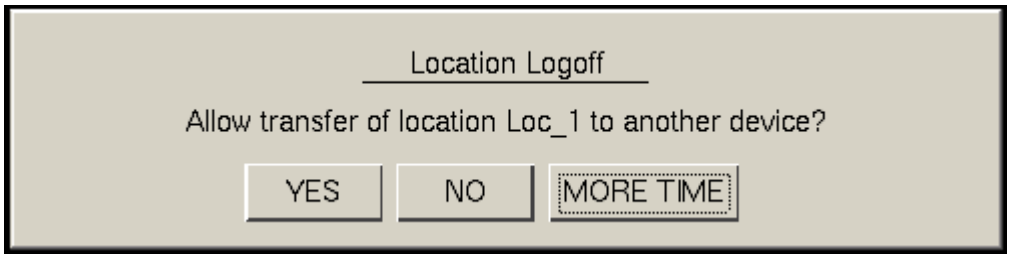
Note: The screenshots of QR codes are blurry because they register and close as soon as they are in focus.



Transfer Notification

A message will be sent to the mobile device telling it that the location has to respond.

The scan will initiate the transfer but this isn't a forced transfer, but a manual transfer. This requires confirmation at the location.

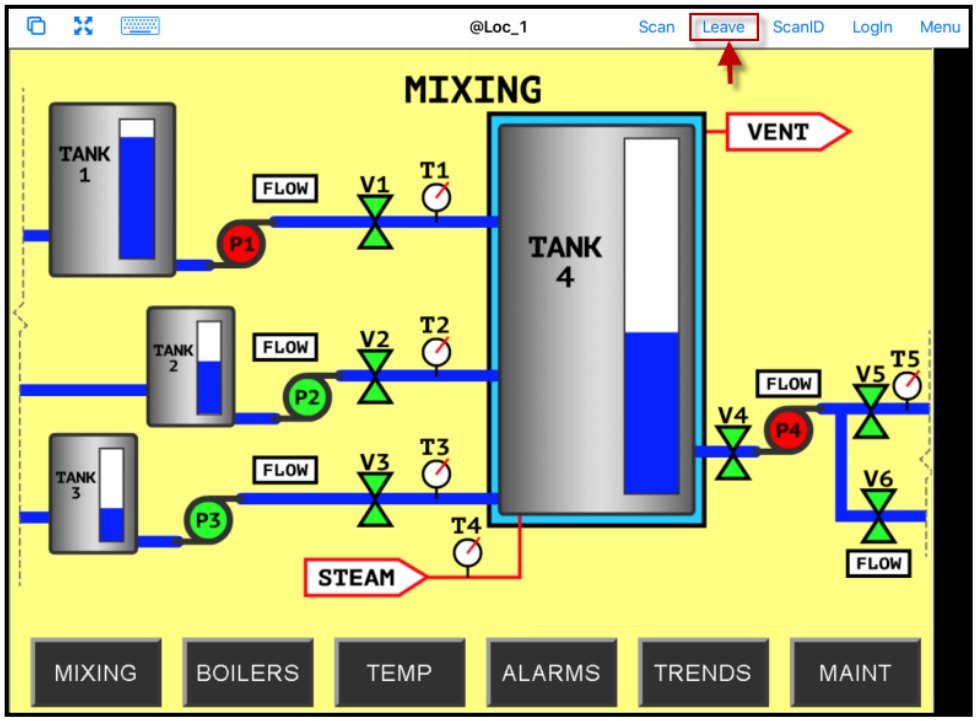


Location Logoff Dialog Box

The operator at the location will be shown a dialog box that requires approval to transfer.

Selecting the ***Yes*** button to allow the transfer.

The iTMC client will be allowed to display the location display.



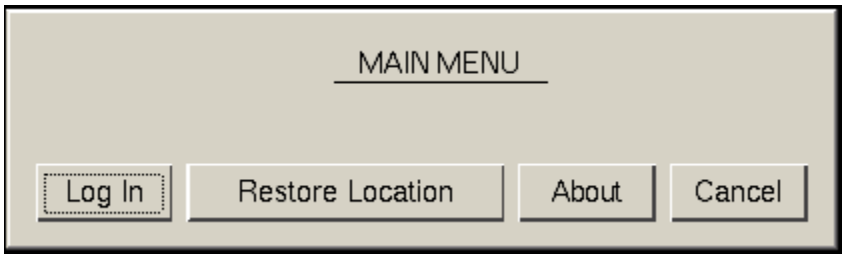
Transfer on the Mobile Device

The display from the location will be moved to the mobile device.

The location display can be restored from the iTMC client or the location.

Selecting the ***Leave*** button on the iTMC client menu will restore the display back to the location.

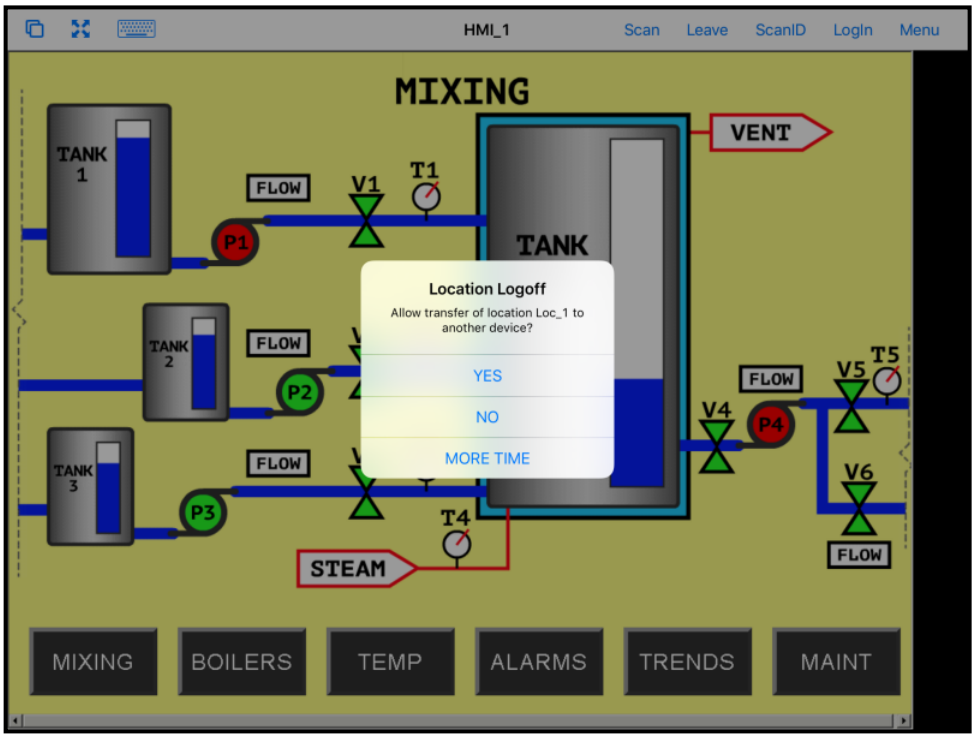
Selecting the ***Restore Location*** button at the location will also restore the display.



Main Menu at the Location

Go to the location and ***Select Restore Location***.

This will launch a dialog box on the iTMC client.



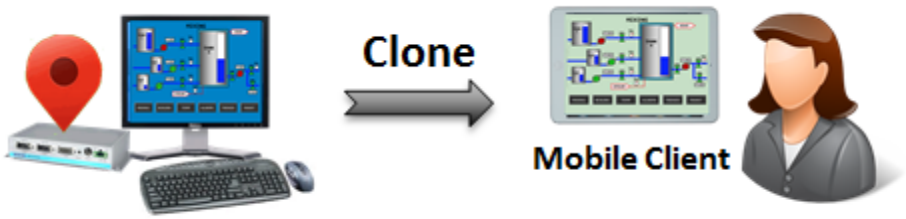
Location Logoff on the Mobile Device

Go to the iTMC client.

Select ***Yes*** to allow the transfer back to the location.

41.4. Clone

Clone will duplicate the display clients of the location on the mobile device but the sessions will be created with the mobile device Windows user account.

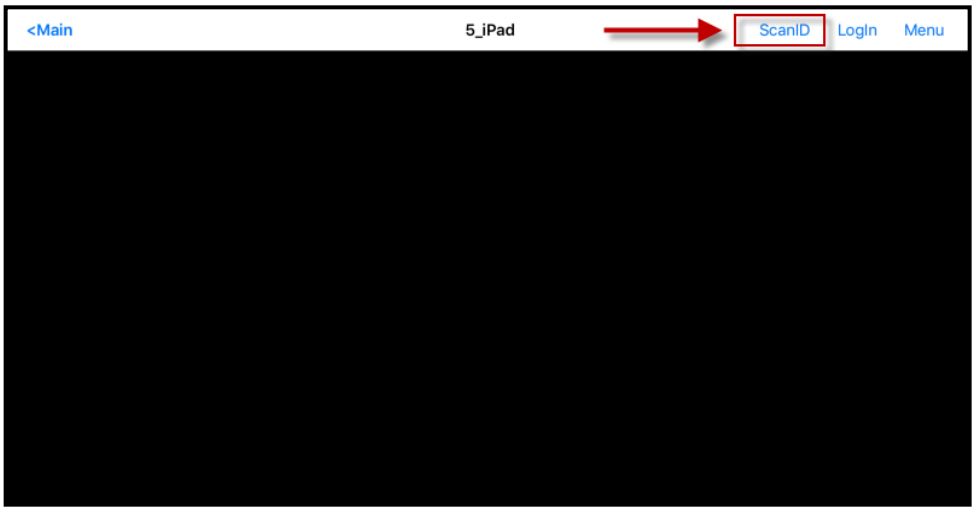


Clone

This allows a mobile user to get the HMI or other software and have independence from the user at the location.

Launch the iTMC application.

Select your ThinManager Server on the configuration screen to run your iPad as a Terminal.

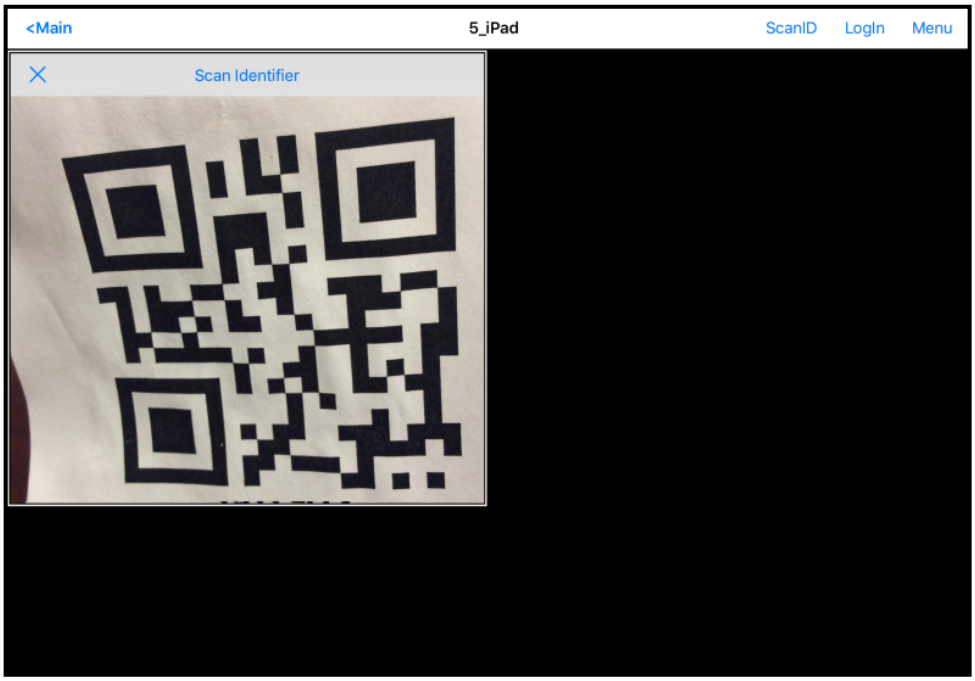


ThinManager iTMC Main Screen

The Main Screen has a menu bar at the top with ***<Main***, ***ScanID***, ***Login***, and ***Menu***.

Touch the ***ScanID*** button in the upper right to launch the **Scan Identifier** window.

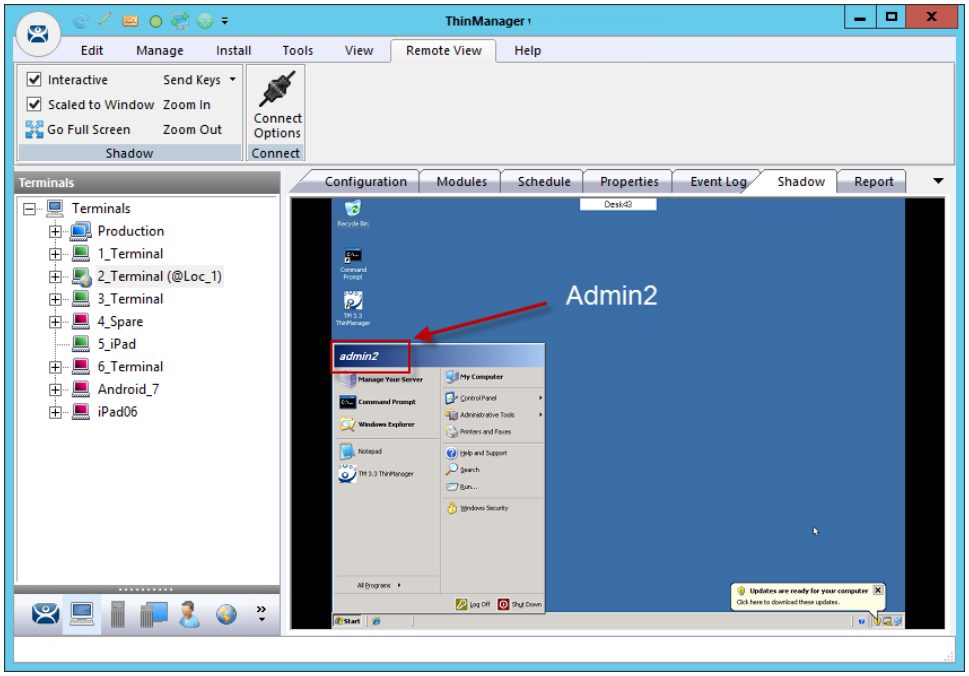
Touching the ***Scan ID*** button will launch the onboard camera as the **Scan Identifier** window.



Scan Identifier Window

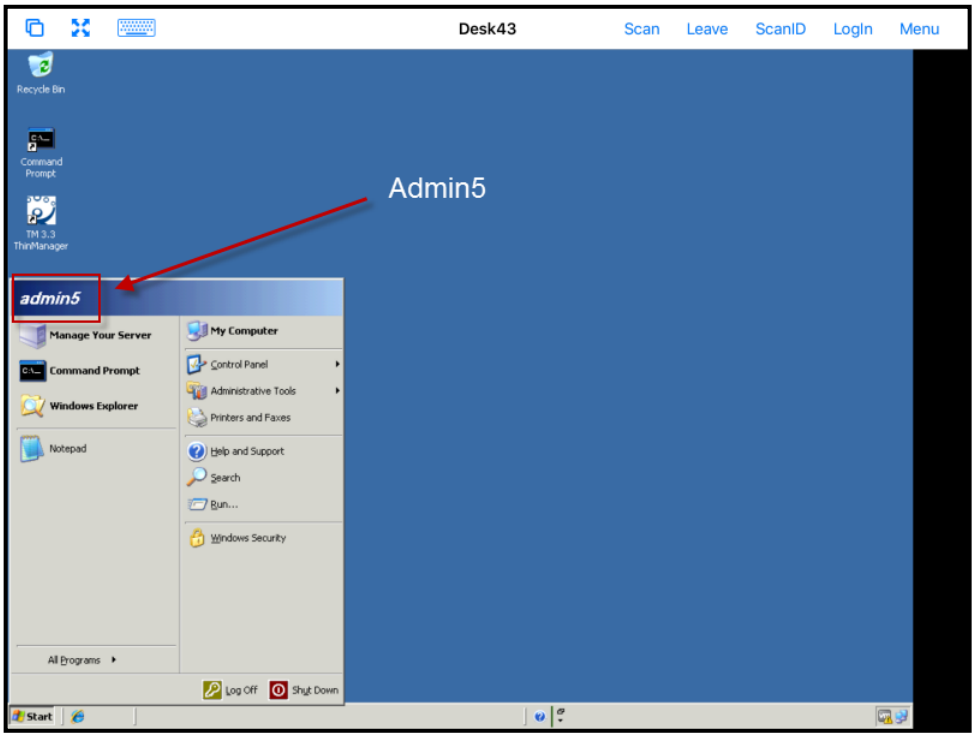
Scan the resolver associated with **Clone**. Relevance will launch the display clients used at the location on the mobile device but using the mobile device account.

This gives a mobile user the same applications but with an independent session instead of sharing as in Shadow, or taking it as in Transfer and Forced Transfer.



Cloned Session

This is a shadow from ThinManager showing the Terminal logged in as **Admin2**.



Cloned Session

Cloning will duplicate the sessions on the location but create them with the Windows user account of the mobile device.

This example shows the iPad cloning the 2_Terminal and running the same applications, but logging in with the Windows account of the iPad, **Admin5**.

42. Unassigned Locations

Deploy applications to locations that don't have assigned Terminals.

A big change in application deployment in Relevance is that you no longer have to deploy applications to a tethered Terminal. You can create a location, deploy apps to it, and access these apps with a mobile device when you are at that location.

Unassigned Locations support **Transfer**, which acts like Forced Transfer, and **Cloning**. It does not support **Shadow** as there is no Terminal to shadow.

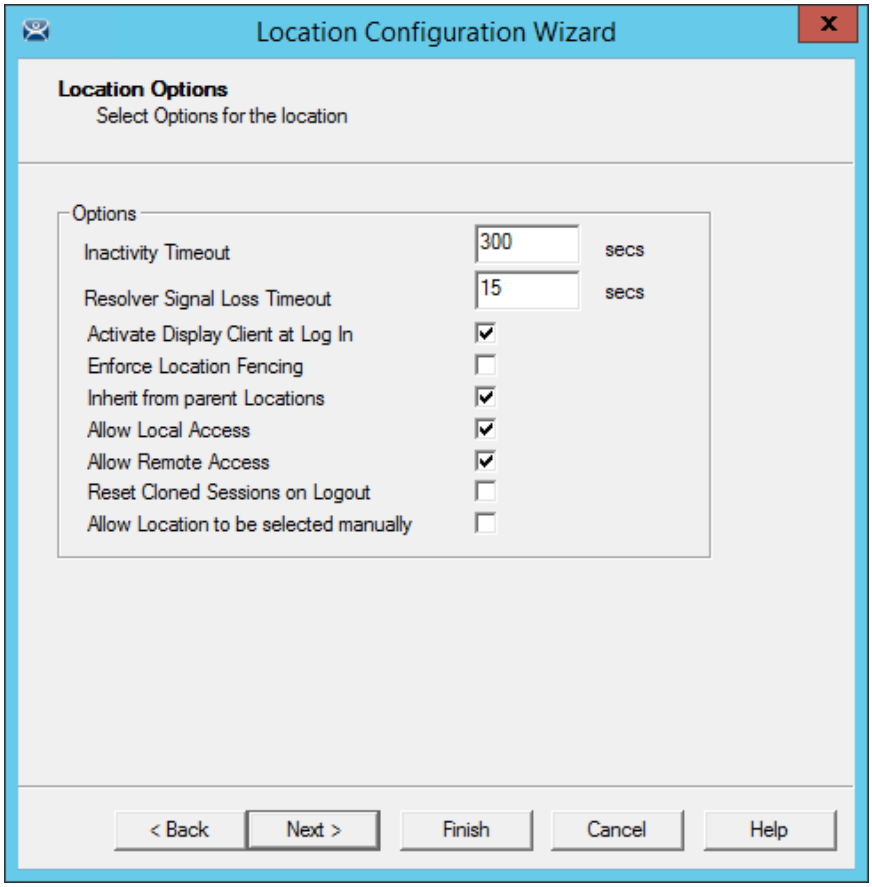
42.1. Create an Unassigned Location

This example will use GPS so that when the mobile user enters the area the appropriate applications are delivered to the user.

Open the **Locations** branch of the tree by selecting the **Location** icon from the Tree Selector.

Right click on the **Locations** branch and select ***Add Location***.

Navigate to the **Locations Options** page of the **Location Configuration Wizard**.



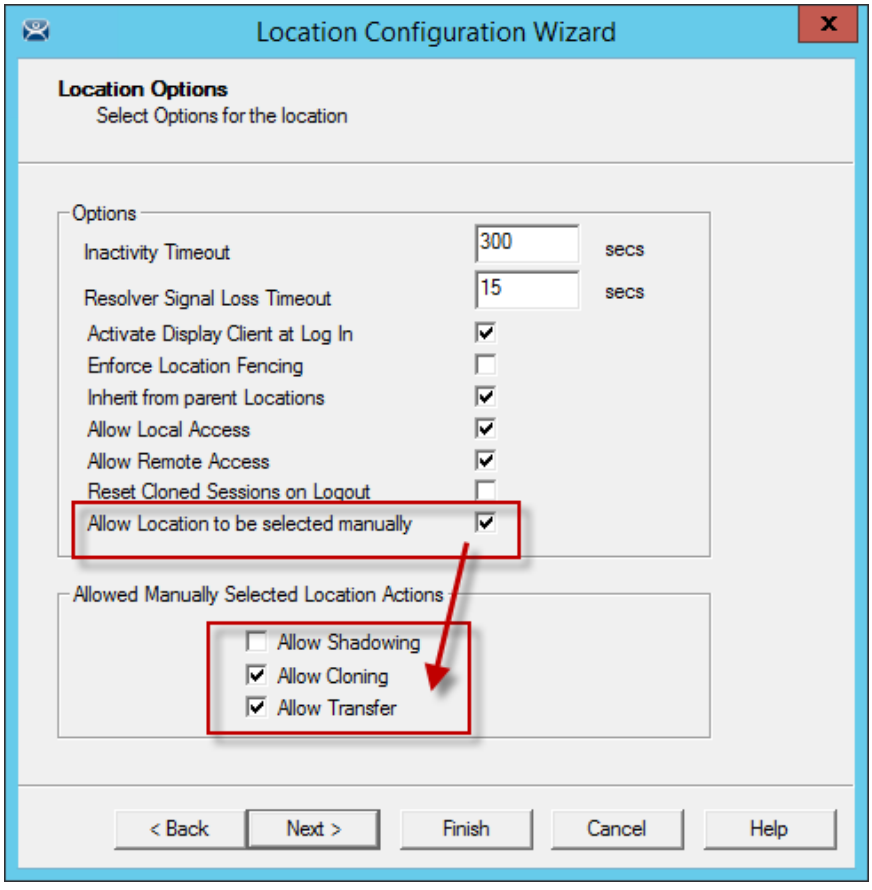
Location Options

The **Location Options** page has several configurable options that control the remote access.

- ***Inactivity Timeout* –** A Relevance user will be logged off after this interval if inactive.
- ***Resolver 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.

Checking the ***Allow Location to be selected manually*** checkbox reveals other settings.



Location Options Page

Allow Manually Selected Location Actions – These are the actions you can manually select. You can allow all, or none.

- ***Allow Shadowing*** – This is not supported in Unassigned Locations as there isn't a Terminal to shadow.

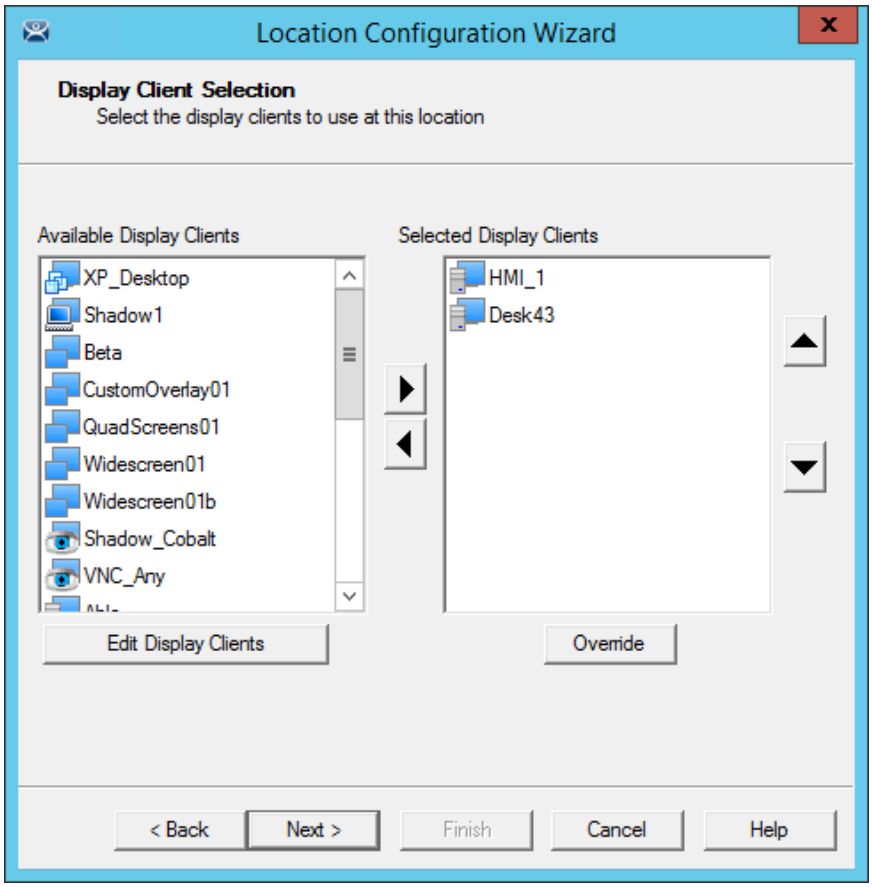
- ***Allow Cloning*** – This allows the user to launch the same applications as the location but using the Windows account of the mobile device.
- ***Allow Transfer*** – This allows the display to be shown on the mobile device with the Windows account of the Unassigned Location.

Checking the ***Allow Location to be selected manually*** will let you manually choose the location from the mobile device. It may be let unchecked and you can rely on another resolver like QR code or Bluetooth to select the location.

Unassigned Locations do not support **Shadow** so the ***Allow Shadowing***, checkbox isn't checked in this example. The ***Allow Cloning***, and ***Allow Transfer*** check boxes are selected in this example.

The defaults are fine but you have the option to customize the settings as needed.

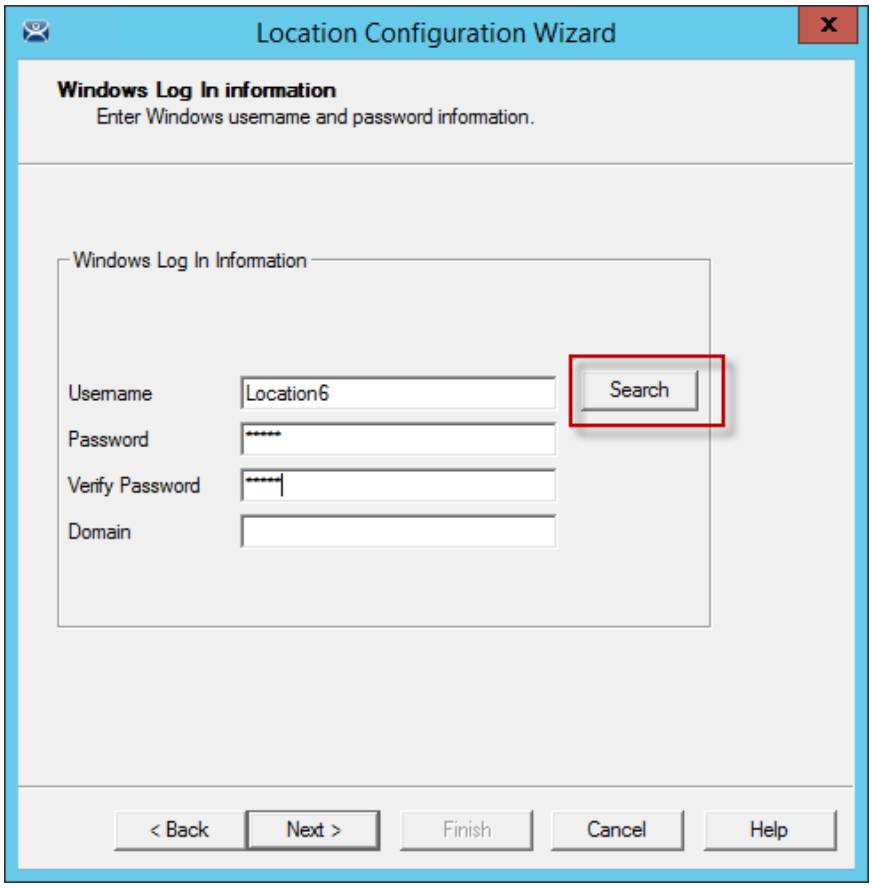
Select ***Next*** to continue.



Remote Desktop Server Selection Page

Add the display clients you want on the **Remote Desktop Server Selection** page. This could be an HMI, a maintenance record, equipment manuals, or combinations of these and other applications.

Select ***Next*** to continue.

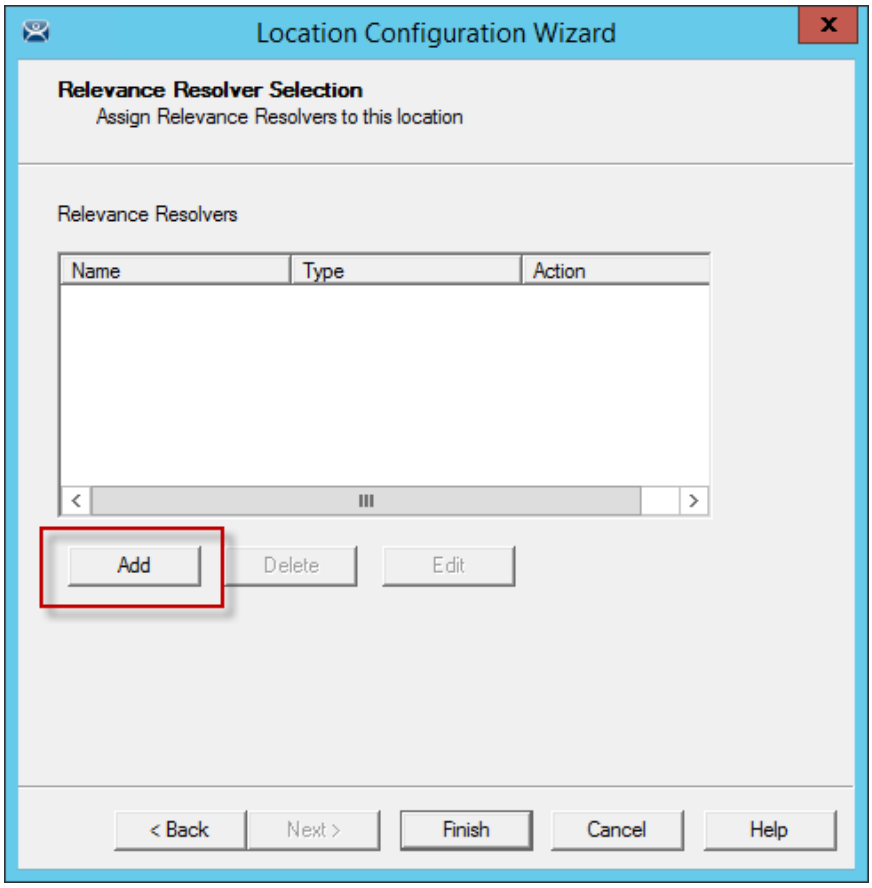


Windows Log In Information Page

The Location will need a Windows user account entered in the ***Username*** field on the **Windows Log In Information** page.

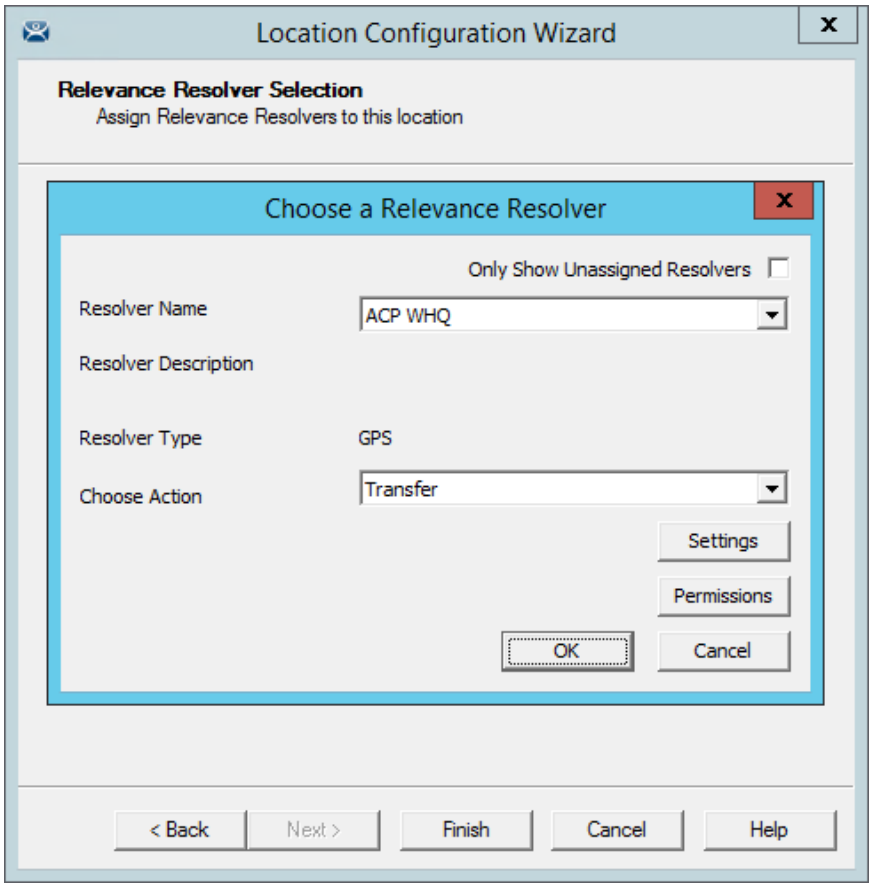
You may use the ***Search*** button to use an Active Directory user as described in with the Location Configuration Wizard on page 580.

Select ***Next*** to continue.



Relevance ID Selection Page

Select the ***Add*** button to add the resolver on the **Relevance ID Selection** page and add an action.



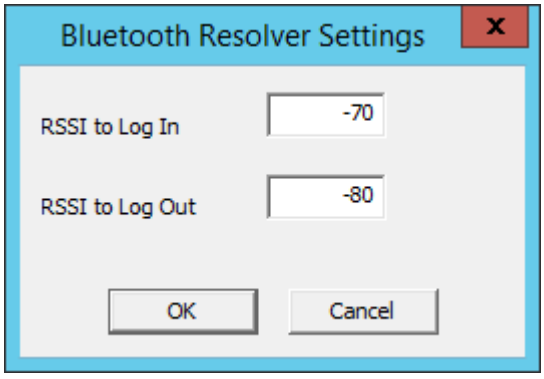
Choose a Relevance Resolver Page

Select a resolver from the ***Resolver Name*** drop-down.

Chose the action from the ***Choose Action*** drop-down.

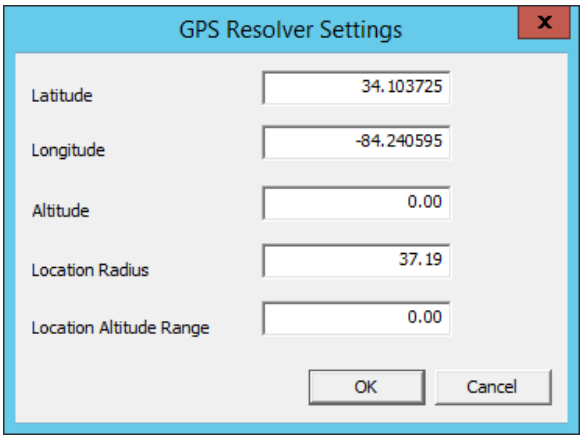
Select ***OK*** to accept the configuration.

There is a ***Settings*** button for the resolvers.



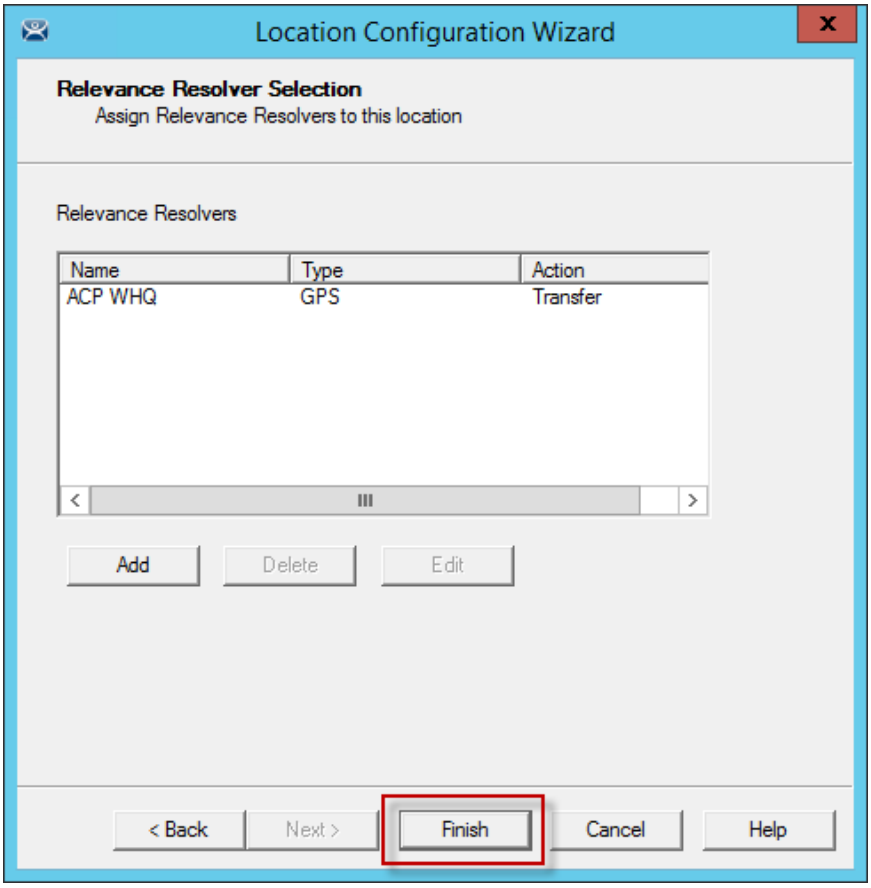
Bluetooth Resolver Settings

A **Bluetooth Resolver** settings show the signal strength that was measured when the Bluetooth beacon was registered as the ***RSSI to Log In***. The log out strength is automatically added as the ***RSSI to Log Out*** value is generated by subtracting 10 from the ***RSSI to Log In*** value..



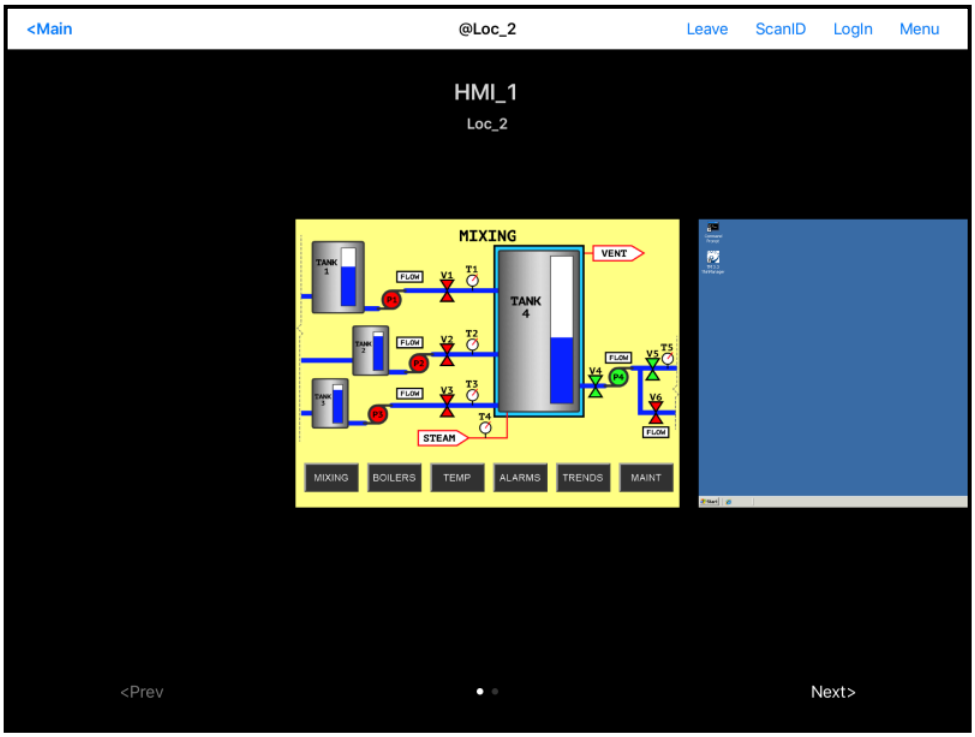
GPS Settings

The **GPS Resolver Setting** shows the ***Latitude***, ***Longitude***, and ***Altitude*** that was measured when the GPS was registered. The ***Location Radius*** and ***Location Altitude R***ange are added automatically.



Selected Resolver

Once a resolver is added you can click ***Finish*** to close the wizard and accept the configuration.



Display Clients Launched by GPS

Launch the iTMC client.

The display clients will appear on the mobile device once the resolver is triggered, either by scanning a QR code or bar code, or entering within the range of the Bluetooth beacons, Wi-Fi area, or GPS zone.

This allows you to deploy applications without deploying permanent Terminal hardware.

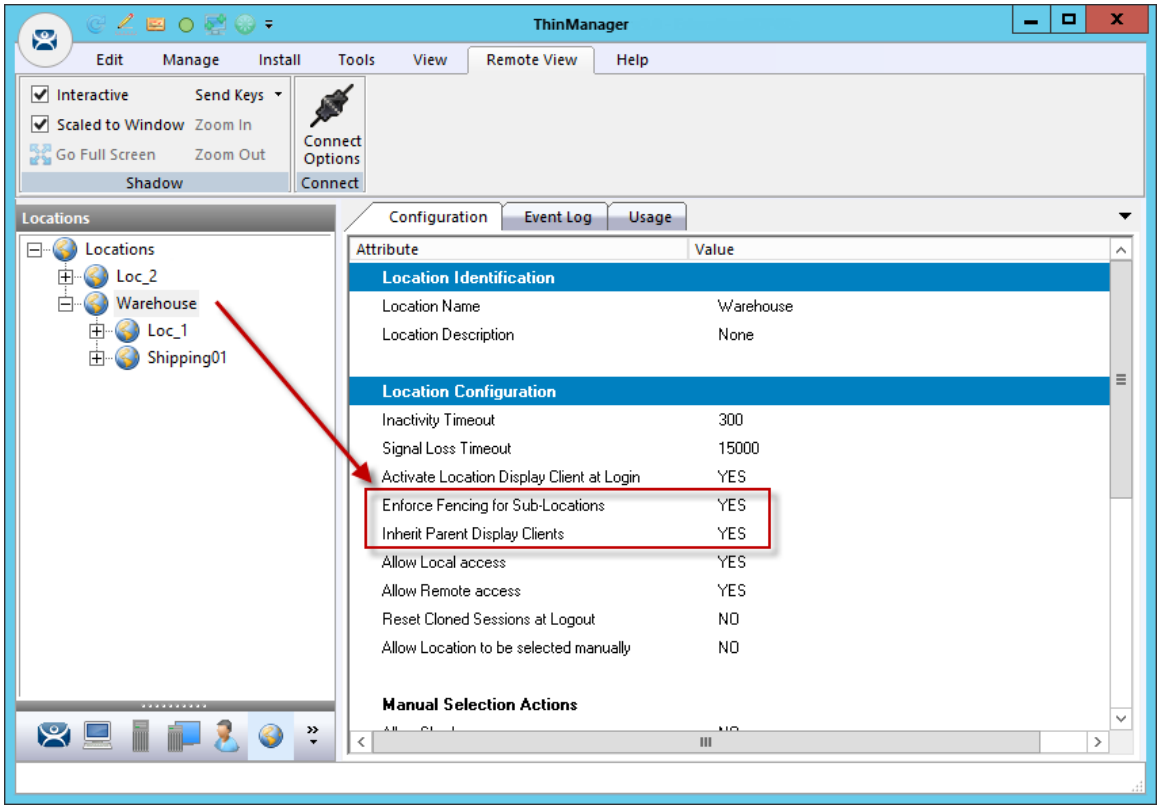
43. Fencing and Sub-Locations

Fencing is a hierarchy that allows the organize locations by nesting locations within locations. This can be useful for organization but it also allows control of access through Fencing.

Fencing allows you to create a location that has to be entered or authenticated before you can access the sub-locations. It is a way to ensure the user in in the right location before they can access a display client or action.

Fencing is useful to make sure the worker is in the area they are supposed to be. A worker can't take a photo of a QR code and log in at their desk with this method. Fencing can force them to enter an area controlled by Bluetooth beacons, Wi-Fi access points, or GPS before they can scan the QR code or bar code. If they are running the application and leave the Fence then the application will no longer be transmitted.

- ✓ **Fencing is best initiated by Bluetooth beacons, Wi-Fi Access Points, or GPS.**



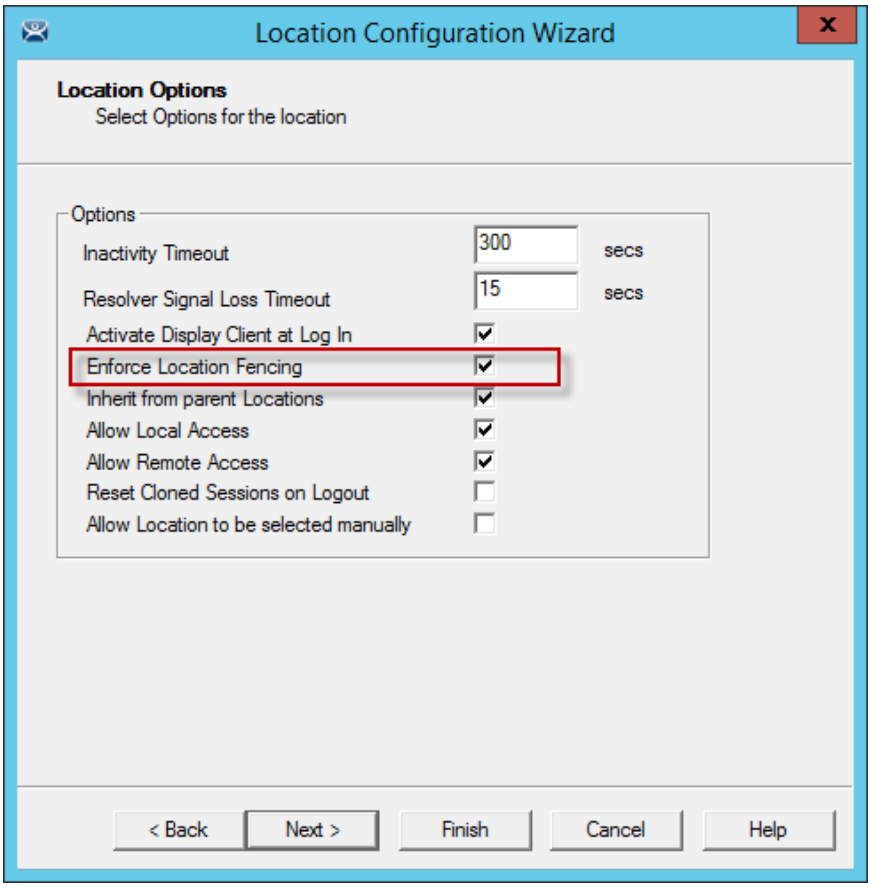
Location Using Fencing

The **Warehouse l**ocation was created as the parent group with ***Fencing Enforced***. You have to enter the Warehouse location before you are allowed to access the Loc_1 or Shipping01 locations and applications.

43.1. Parent Locations

A Fence needs a parent location that authenticates a high level location that must be resolved before the child sub-locations can become active.

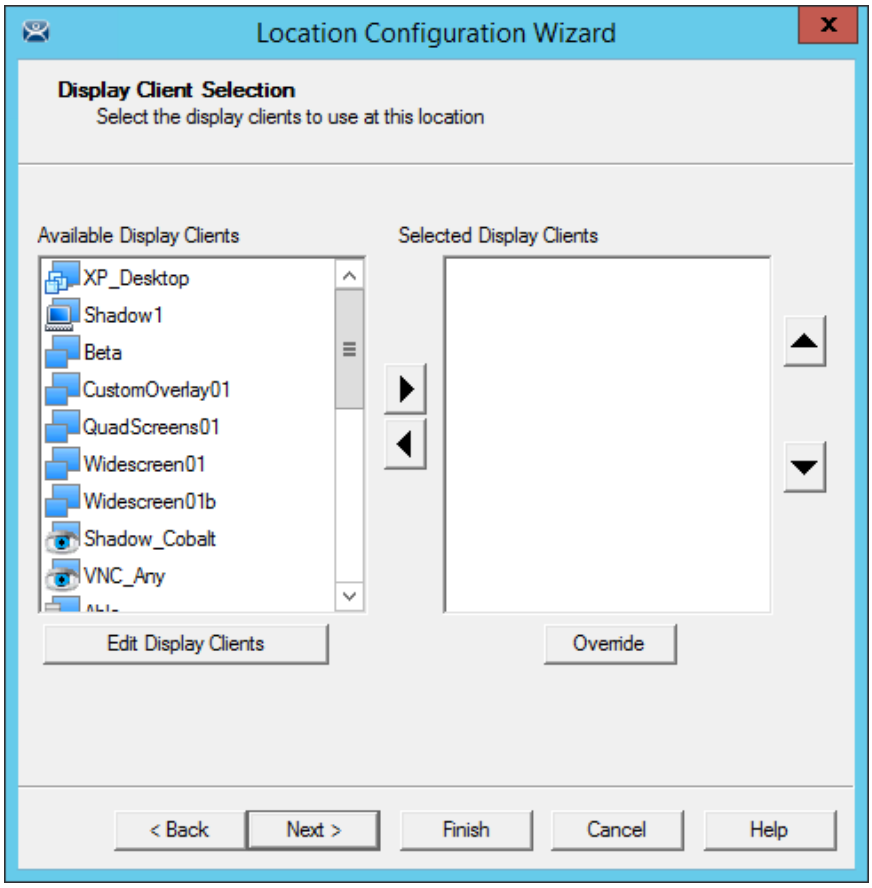
The parent location can be configured without display clients and actions, merely providing proof of location. The applications and actions are delivered by the child sub-locations.



Location Options for Parent Location

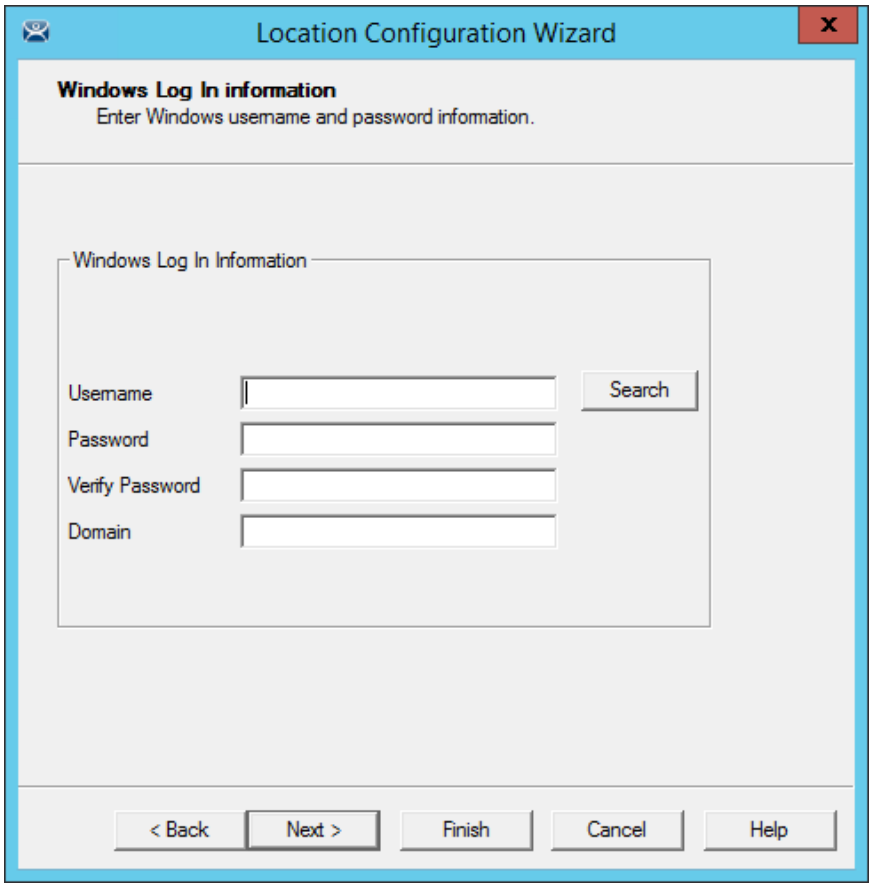
The **Warehouse** parent location has ***Enforce Location Fencing*** enabled.

A user will have to authenticate to the **Warehouse** location before accessing the child sub-locations.



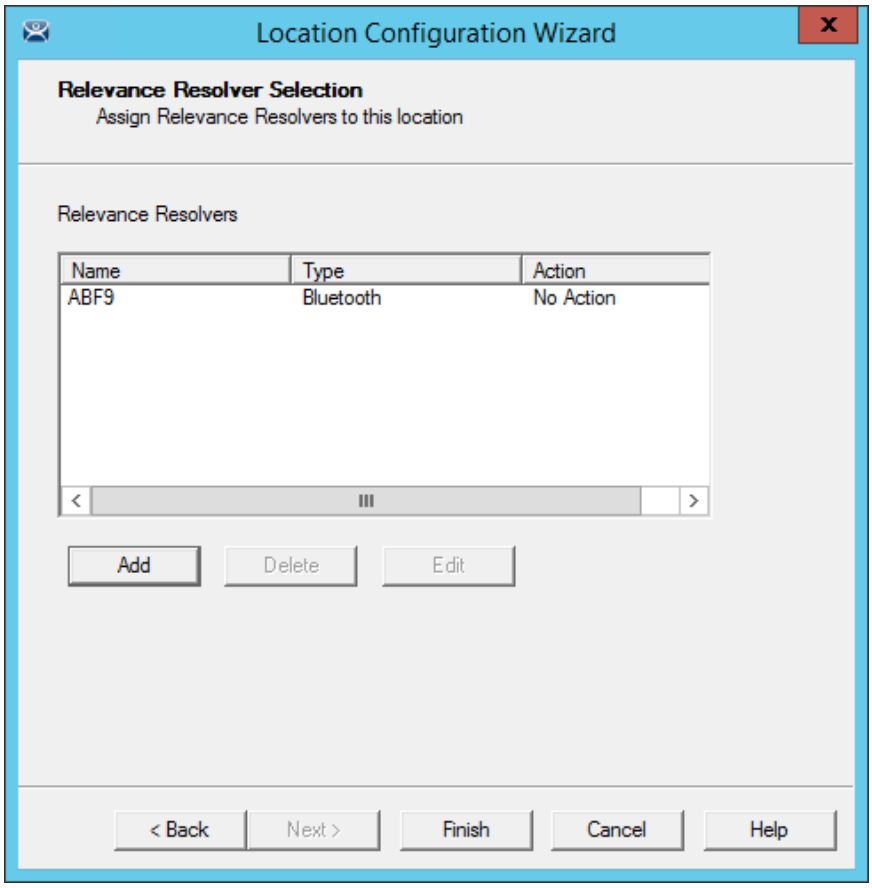
Display Client Selection

The **Warehouse** parent location is not being assigned display clients. It is only being used for authentication so display clients are left off the location.



Windows Log In Information Page

The **Warehouse** parent location is not being assigned a Windows user account because it has no display clients of its own.



Relevance Resolver Selection Page

The **Warehouse** parent location is assigned the **ABF9** Bluetooth resolver. It has no action listed because the intent isn't to launch a program or initiate an action other than identifying the user as being in the parent location.

A user will have to be on the range of the **ABF9** Bluetooth beacon to access the sub-locations.

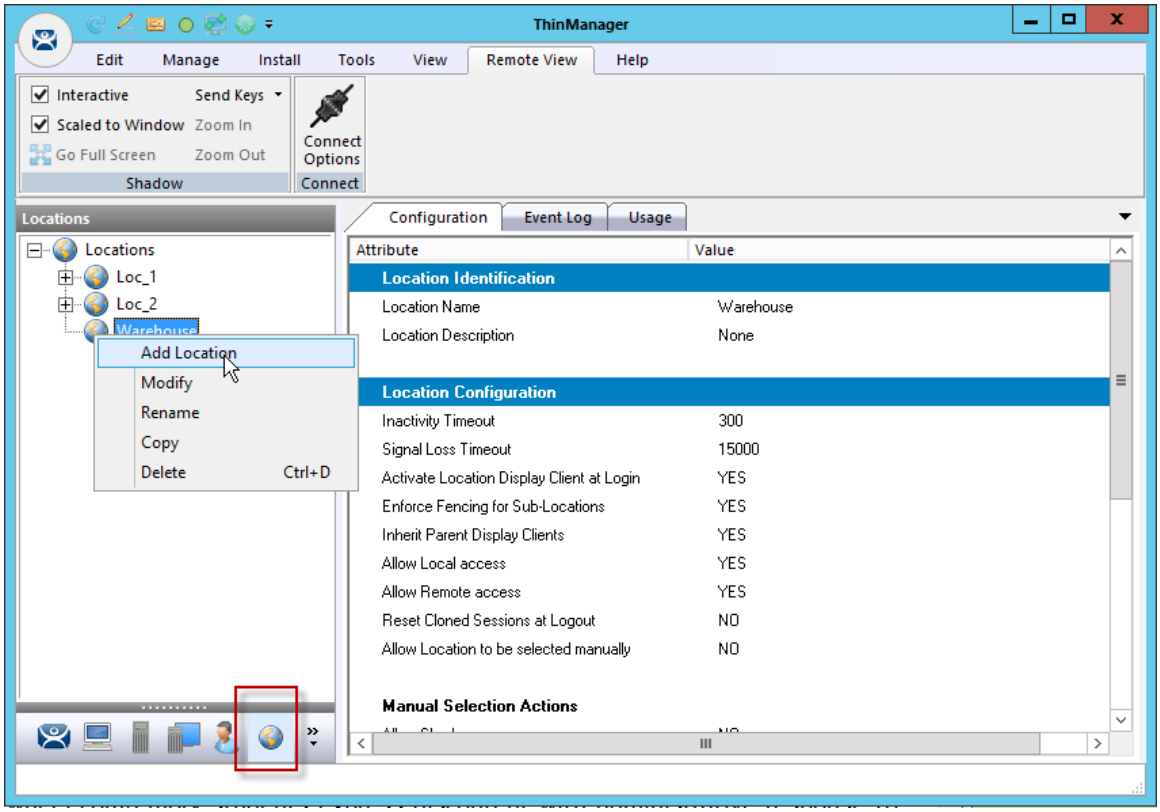
A GPS location or Wi-Fi Access Point could have been used instead.

43.2. Child Sub-Locations

Sub-locations that are nested under a parent location must resolve the parent location before it can initiate the action of the sub-location.

You can create a sub-location in two methods.

The first method to create a sub-location is to right click on the parent location, select the ***Add Location*** command, and launch the **Location Configuration Wizard**. The created location will be nested under the parent location.

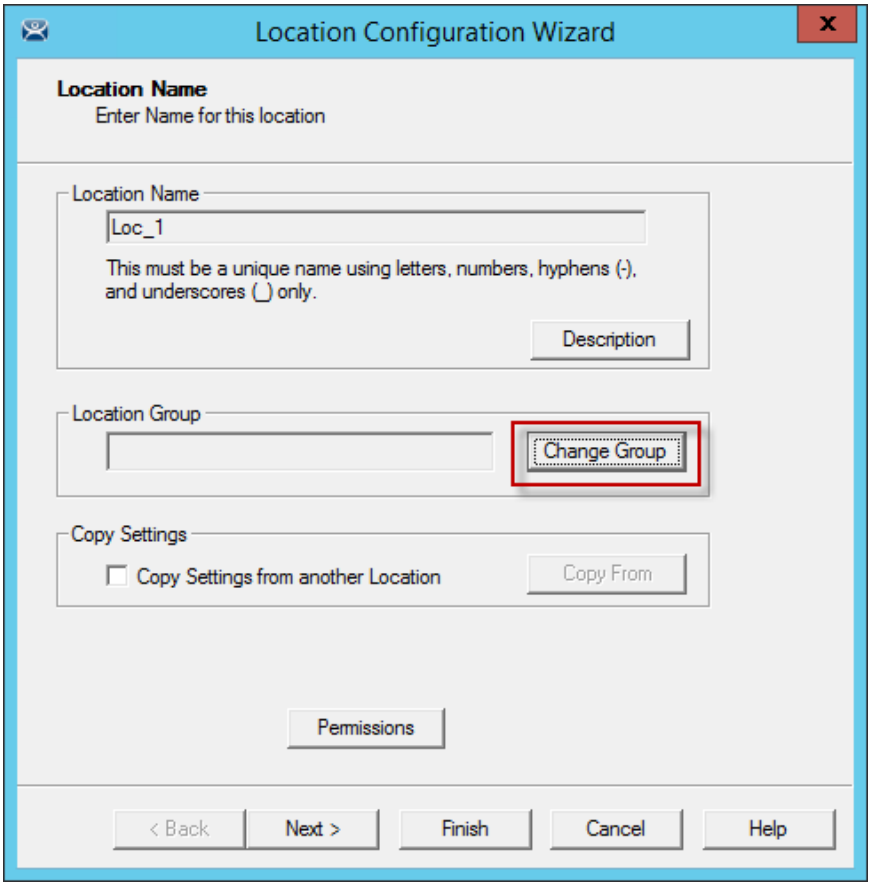


Location Right Click Menu

This picture shows the ***Add Location*** command.

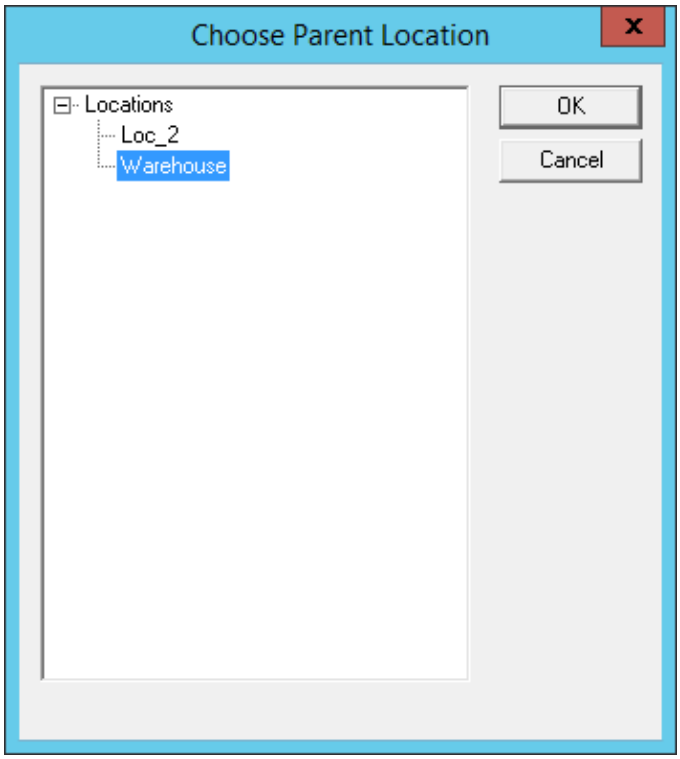
The second method to create a sub-location is to add an existing location to the location.

Launch the **Location Configuration Wizard** by double clicking on a location in the Location branch of the ThinManager tree.



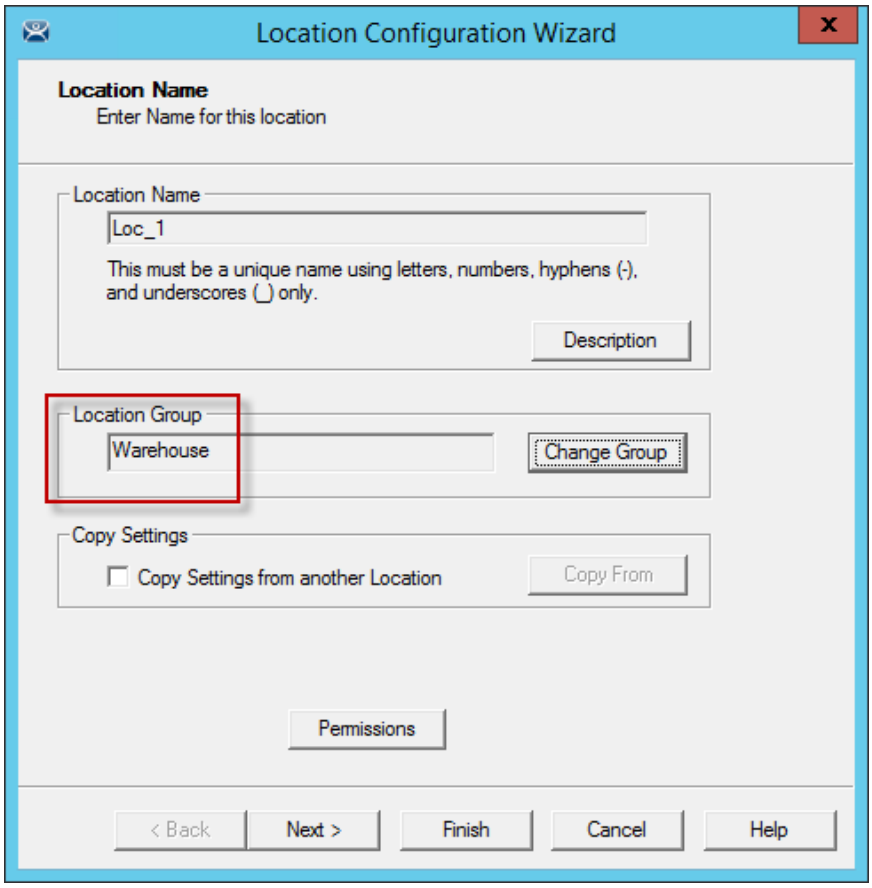
Location Name Page of the Location Configuration Wizard

Select the ***Change Group*** button to launch the **Choose Parent Location** window.



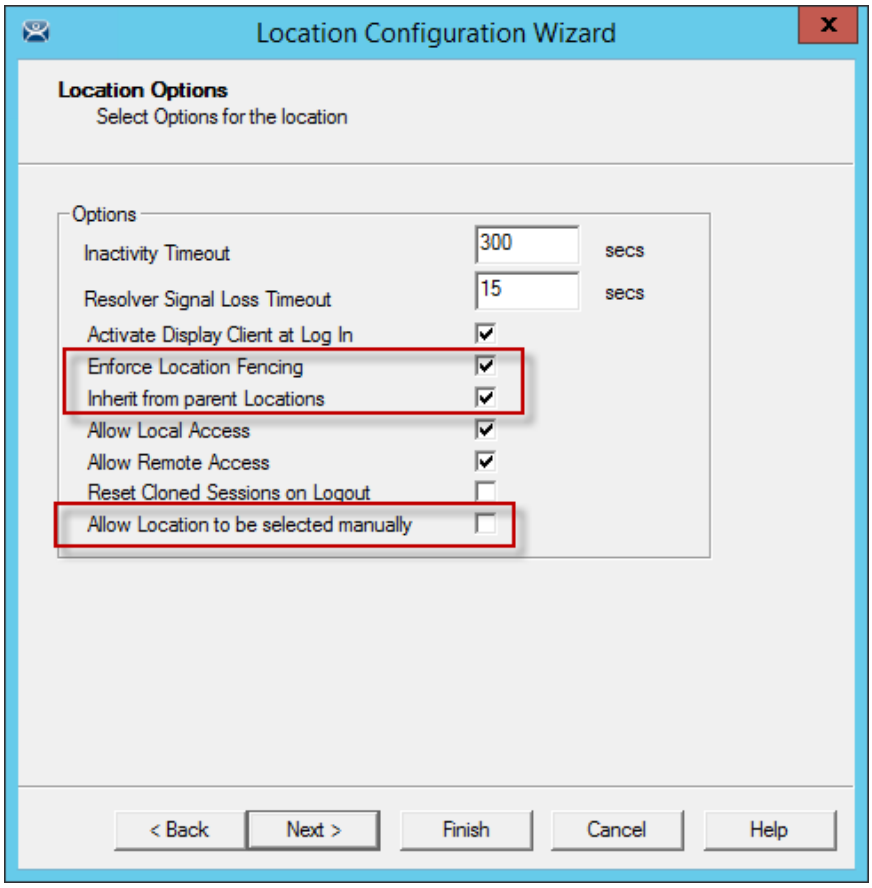
Choose Parent Location Window

Highlight the desired parent location in the **Choose Parent Location** and select the ***OK*** button. The Warehouse location is used in this example.



Location Name Page of the Location Configuration Wizard

The selected parent location will be displayed as the ***Location Group*** and the open location will become a child sub-location once the ***Finish*** button is selected to accept the change.



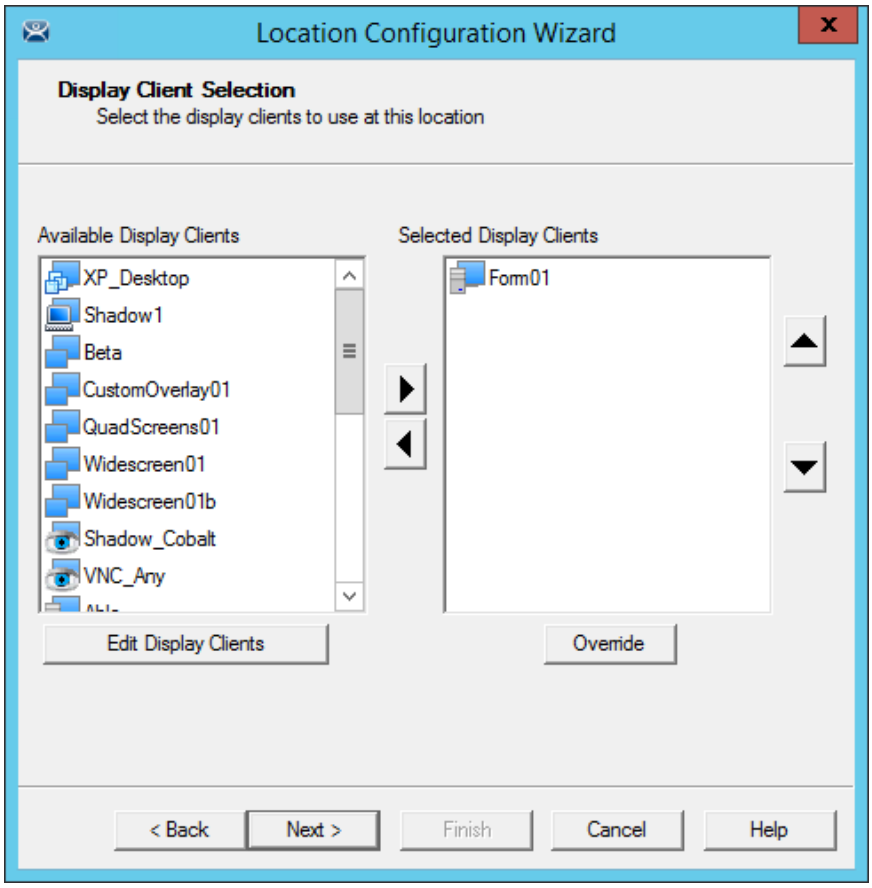
Location Options for Sub- Location

This sub-location is configured to Inherit from parent Location.

If they had sub-locations of their own they could have the ***Enforce Location Fencing*** applied.

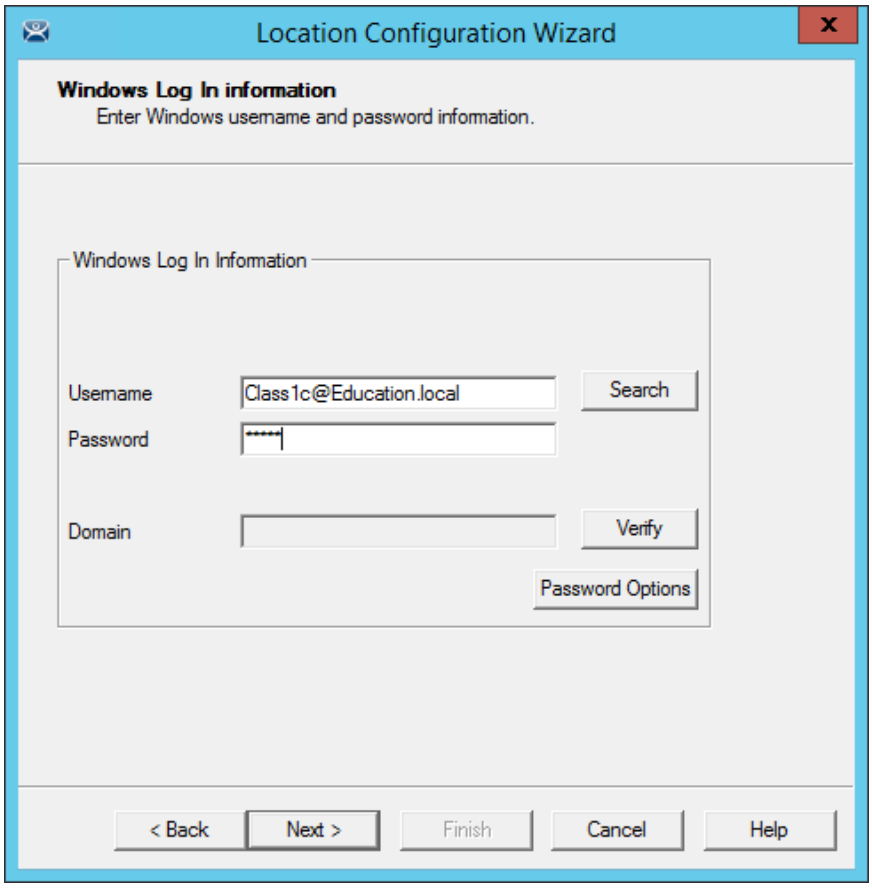
Select the ***Inherit from parent Locations*** to inherit the applications applied to the parent location.

Unselect the ***Allow Location to be selected manually*** to make the user use the resolvers at the location to initiate the application or action.



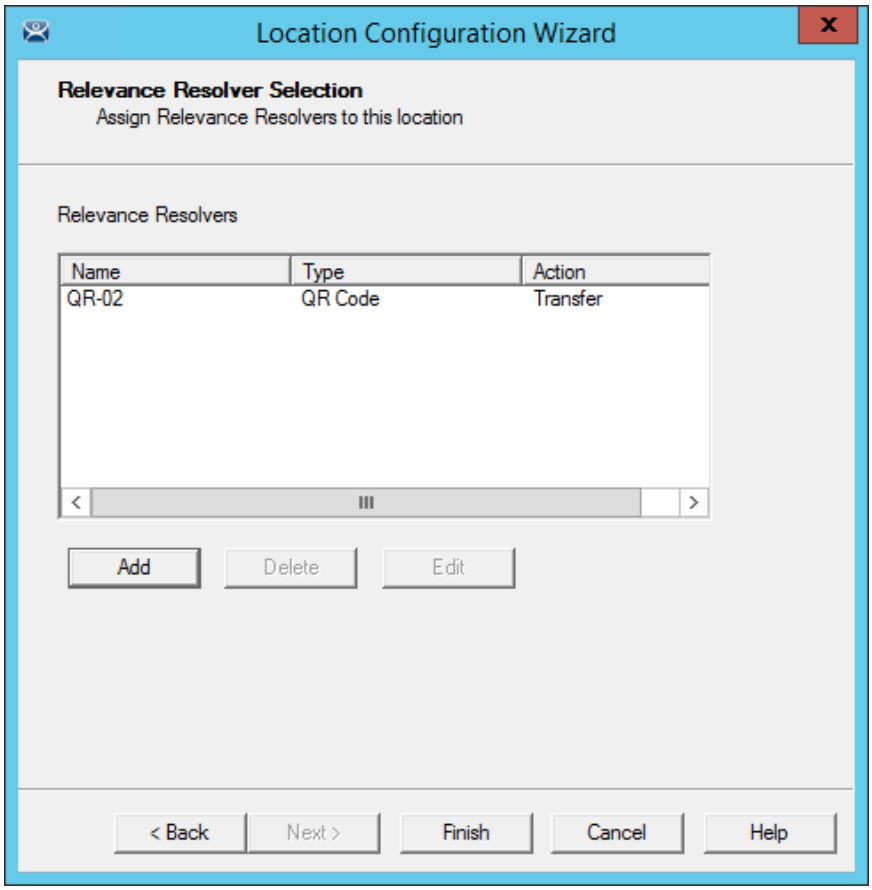
Display Client Selection Page

Add the desired display clients to the sub-location that the user will access when connected.



Windows Log In Information Page

The sub-location will need a user account if it has a display client added. You may use domain accounts or non-domain accounts.



Relevance Resolvers Selection for Sub-Locations

The sub-locations can use any resolver, either QR codes, additional Bluetooth beacons, another Wi-Fi access point, or GPS to allow access to the sub-location. The QR code provides the best way to provide pin point accuracy.

See Adding Actions to Resolver Codes on page 670 for details on adding the Relevance Resolvers to a Location.

44. Relevance User Access

Relevance has Access Groups that can be used to control access to a location or action. This is based on the Relevance permissions in ThinManager.

Relevance has the ability to control access to actions and applications in ThinManager like Relevance does. The steps are:

- Create Access Groups See Relevance Access Group Creation on page 460.
- Apply to Applications or actions. See Add Access Group to a Display Client on page 463.
- Apply to location. See Adding Actions to Resolver Codes on page 670.
- Create Relevance Users. See
- Create the Relevance User using Active Directory on page 484.
- Apply Permissions. See Adding Actions to Resolver Codes on page 670.
- Login to the location to access applications. See Interacting with the Location on page 674.

Access Groups Applied to Display Clients and Users

A Location can have a single resolver, like a QR code, assigned to it. The Location has different Display Clients assigned, each with a different access group.

User Accessing Display Clients Using Permissions

As each person scans the Resolver they get the application that matches their access group.

User Accessing Display Clients Using Permissions

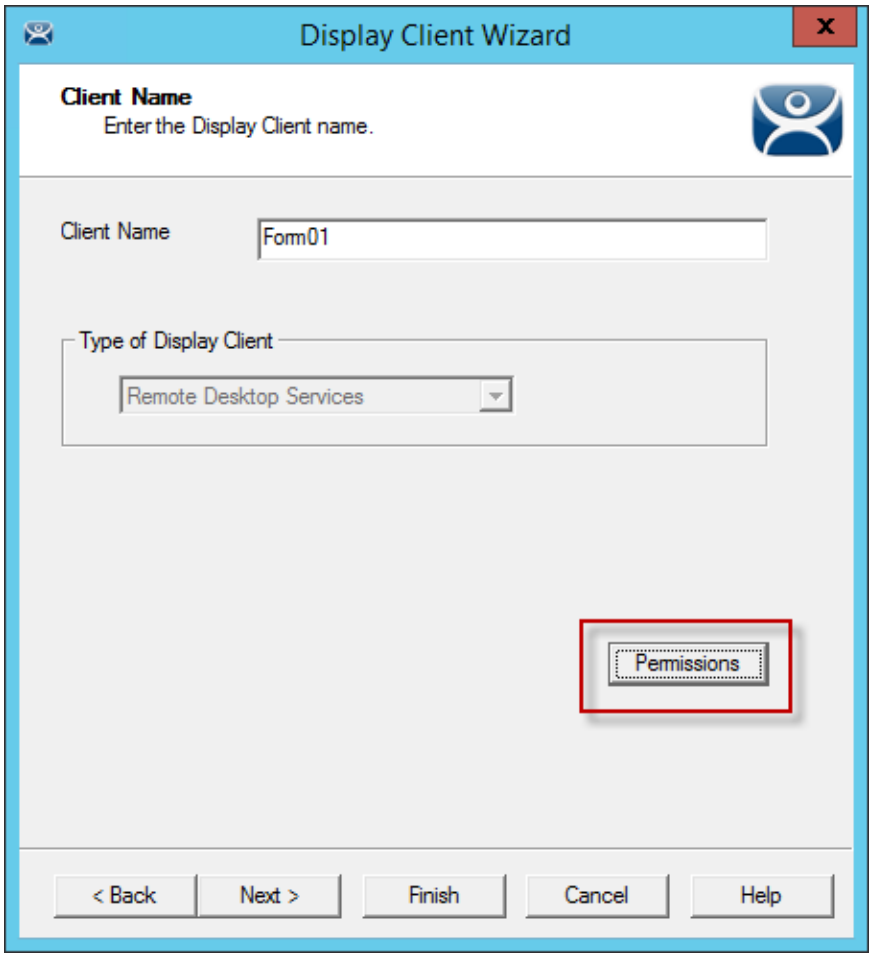
The same Resolver delivers different content, based on Permissions.

44.1. Creating a Location with Restricted Applications

Access Group permissions can be assigned to display clients so that a user has to log on with an account that has permission to access the application. This allows controls application deployment by granting or denying access with permissions.

44.1.1. Using Permission to Restrict an Application

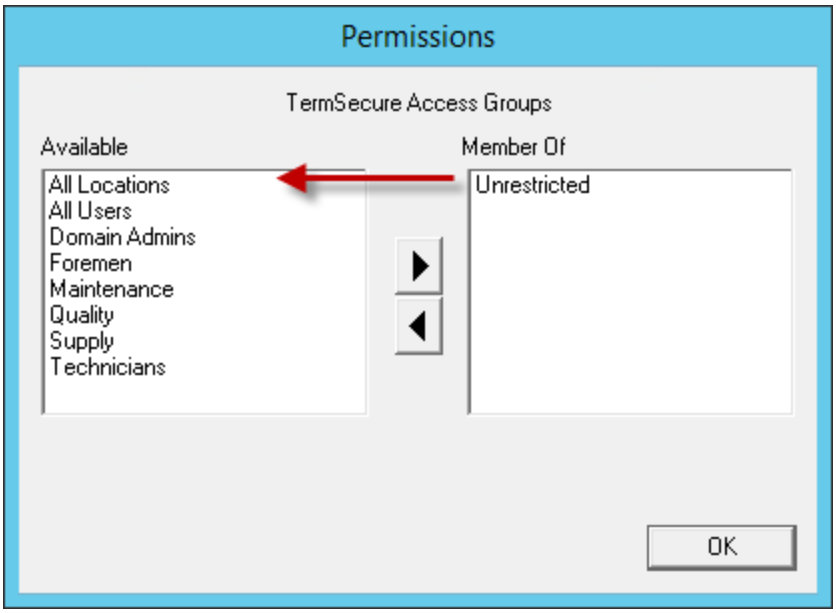
Open the Display Client with the application you want to restrict by double clicking on the display client in the Display Client tree.



Client Name Page of the Display Client Configuration Wizard

Permissions are applied to the display client on the **Client Name Page** of the Display Client Configuration wizard.

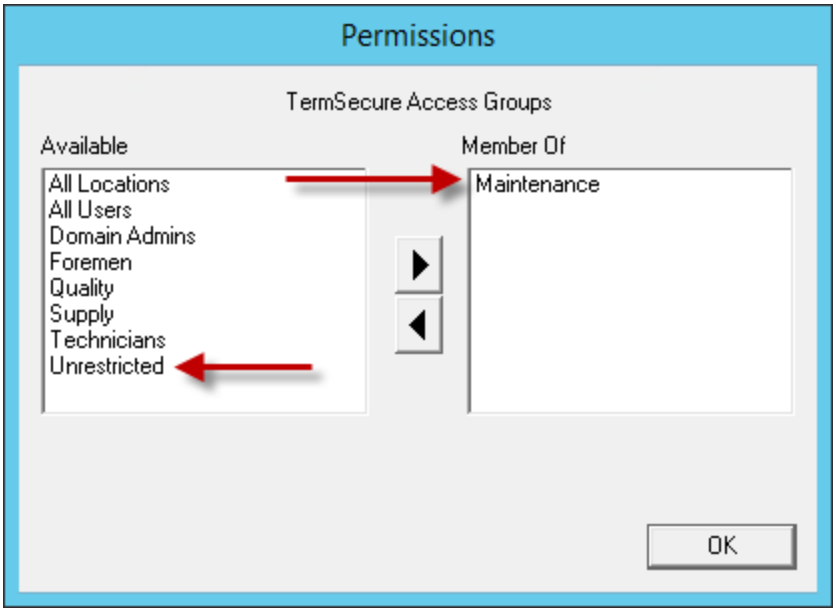
Select the ***Permissions*** button to open the **Permissions** window.



Permissions Window

Remove ***Unrestricted*** from the ***Member of*** list and move the desired Access Group to the ***Member of*** list.

If ***Unrestricted*** isn't removed then anyone can still access it.



Permissions Window

Move the desired Access Group to the ***Member of*** list.

Click ***OK*** to close the window.

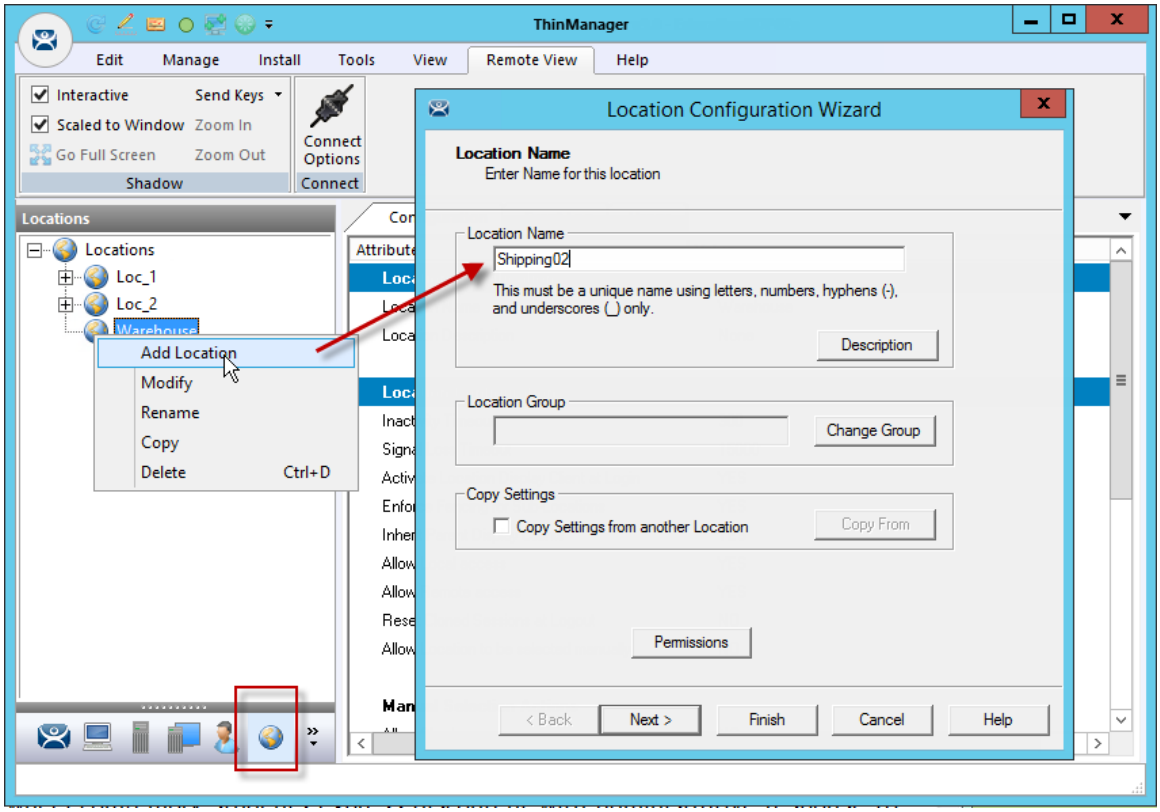
Click the ***Finished*** button on the **Client Name Page** to close the Display Client Configuration wizard.

44.2. Adding a Restricted Application to a Location

You can apply **Relevance User Services** to **Relevance Location Services** and have applications on Locations that are restricted by membership in Access Groups.

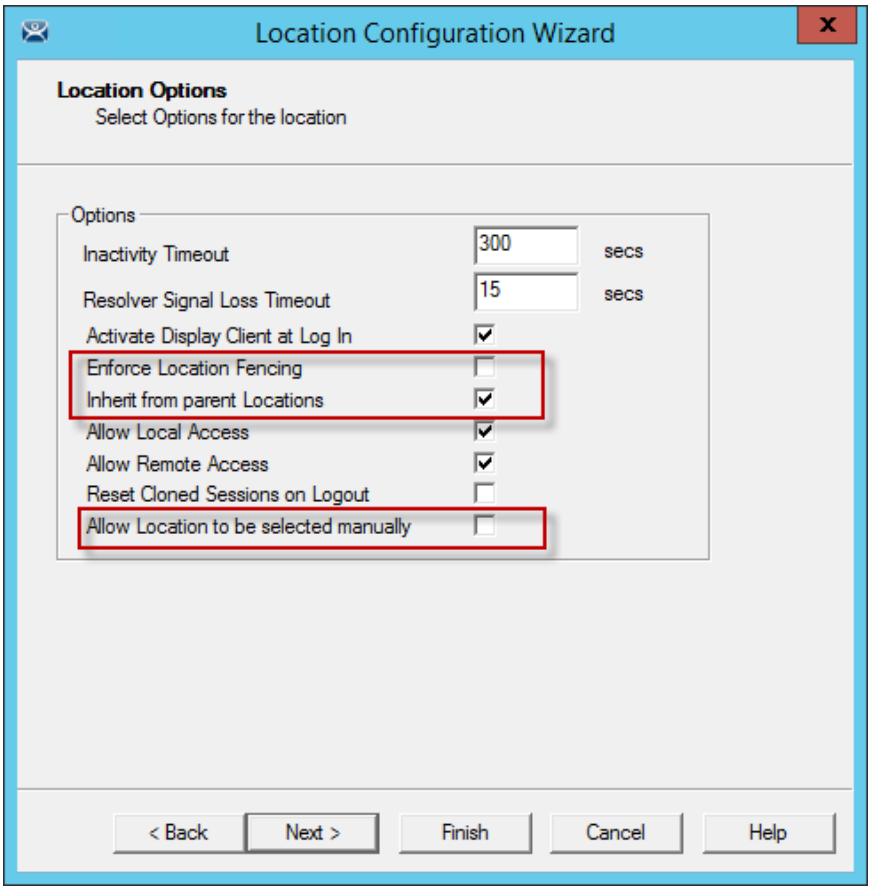
Create a Location with the restricted display client by opening the ***Locations*** tree by selecting the Locations icon on the Tree Selector.

Right click on the ***Locations*** branch and select ***Add Location*** to launch the Location Configuration Wizard.



Location Configuration Wizard

Enter a location name in the ***Location Name*** field and select ***Next***.

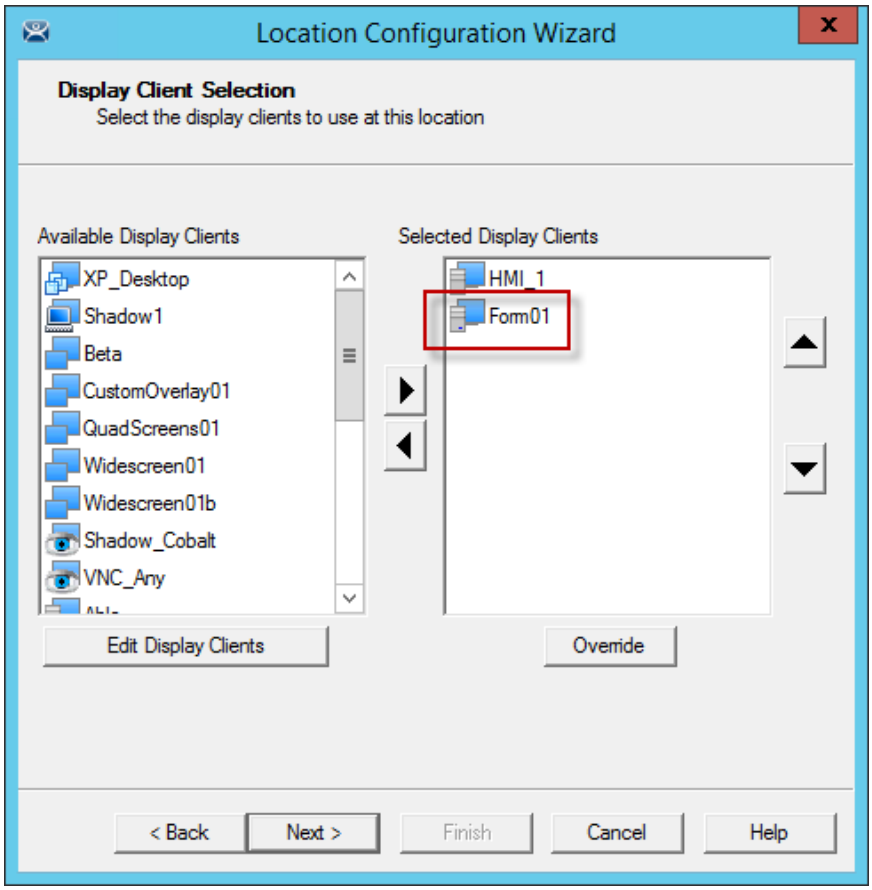


Location Options

Choose your options on the **Location Options** page of the Location Configuration wizard.

Leaving the ***Allow Location to be selected manually*** checkbox unchecked forces the user to use a resolver to access the applications.

Select ***Next*** to continue.

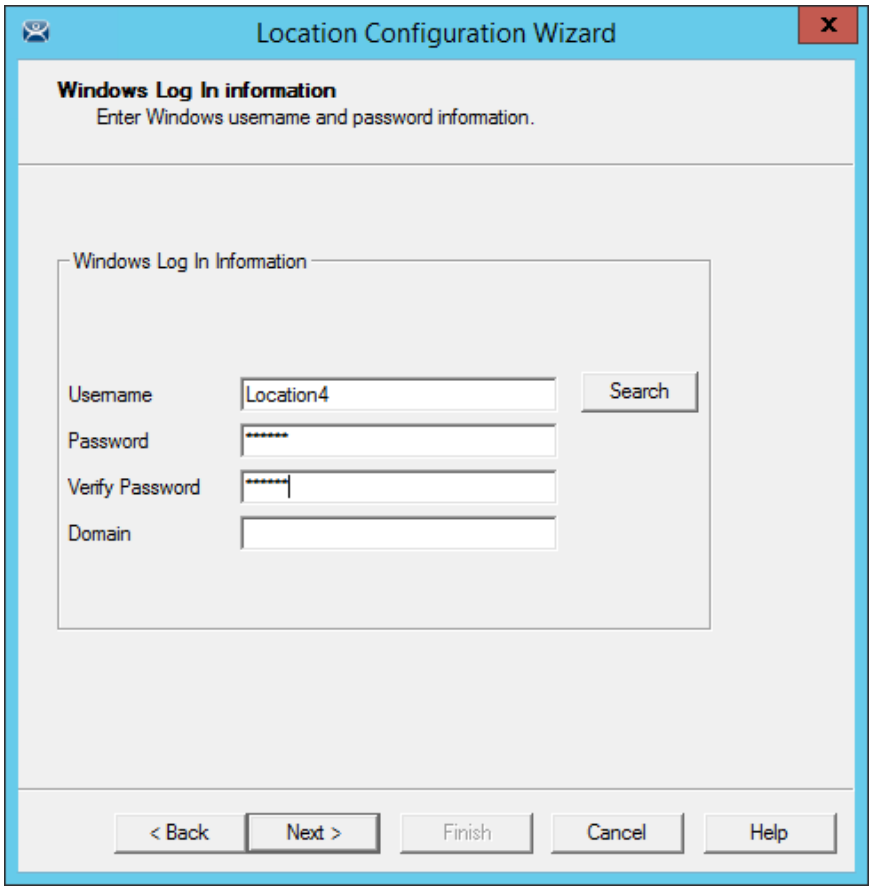


Display Client Selection Page

Add the desired display clients to the ***Selected Display Client*** list on the Display Client Selection page.

In this example the **HMI_1** display client is unrestricted but the **Form01** is restricted to members of the ***Maintenance*** Access Group as shown in Using Permission to Restrict an Application on page 711.

Select ***Next*** to continue.

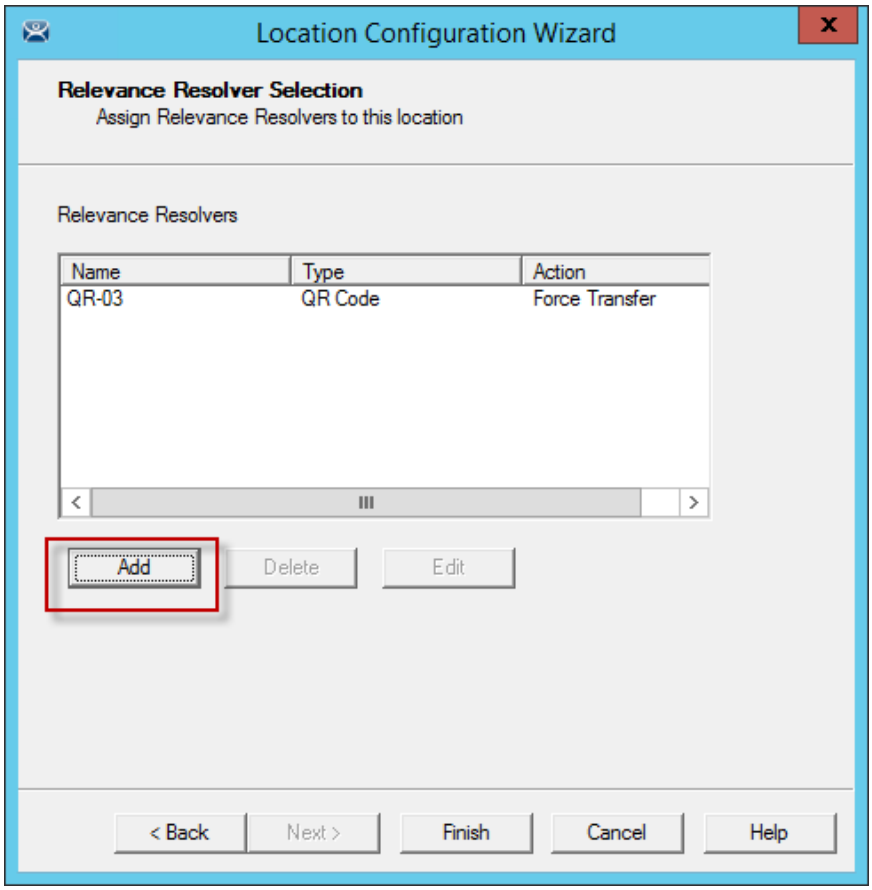


Windows Log In Information Page of the Location Configuration Wizard

A location with display clients requires a valid Windows user account. This may be a domain or non-domain account.

Use the ***Search*** button for a domain account or enter one in the ***Username*** field and add the passwords.

Select ***Next*** to continue.



Relevance Resolver Selection

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

Select your action, ***Forced Transfer*** in this case.

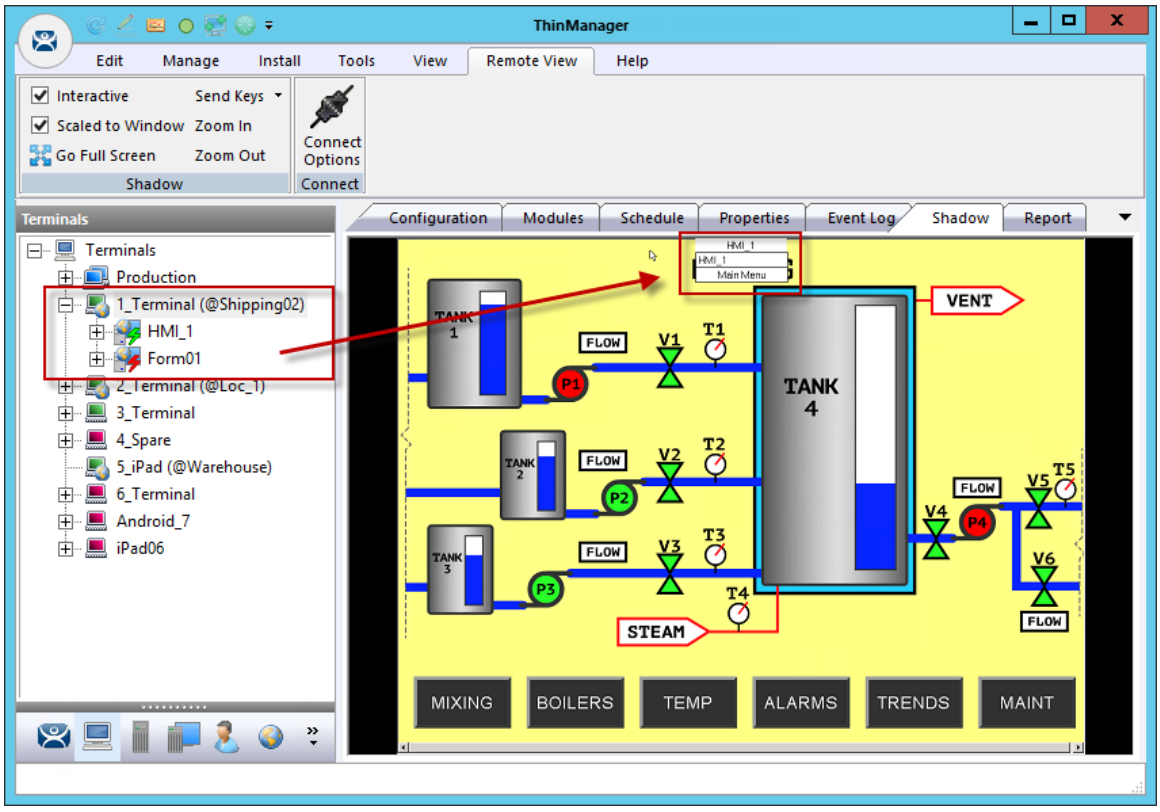
Select ***Finish*** creating the location and closing the wizard.

44.3. Putting It Together

1_Terminal in this example is at the Shipping02 location. It has two display client applications.

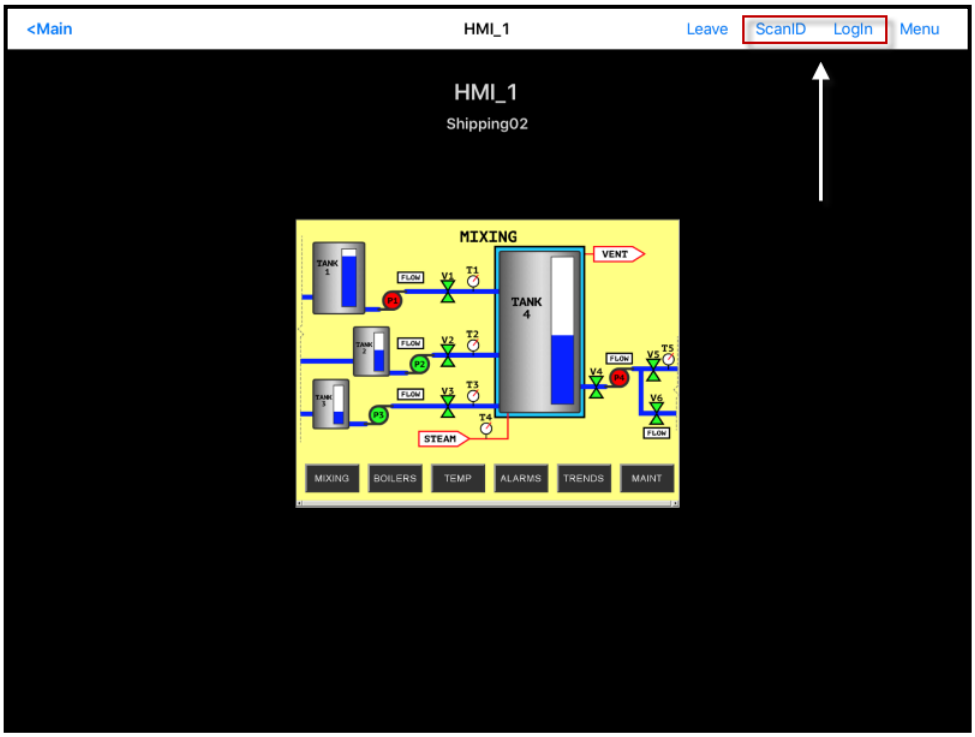
HMI_1 is unrestricted and will be visible for anyone accessing the location.

Form01 is restricted to members of the Maintenance access group.



Shadowed Location

This picture shows the location with the **HMI_1** application running. **Form01** isn't running because no **Maintenance** user is logged in.



Mobile Transfer of the Location

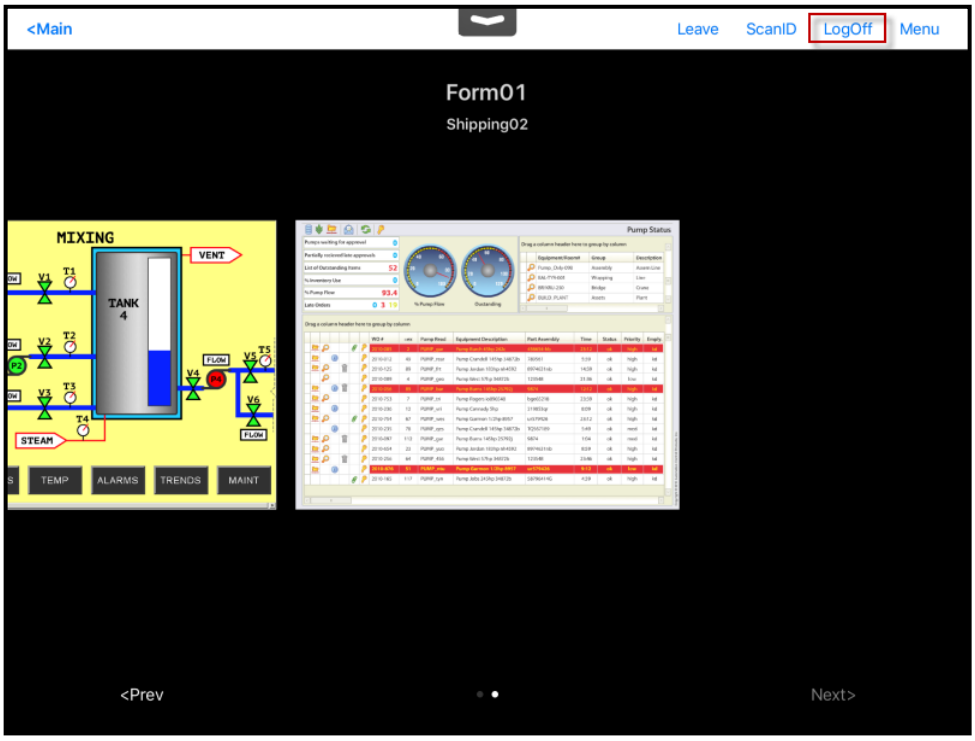
When the mobile user transfers the location they have access to only the unrestricted **HMI_New** application.

Selecting the ***ScanID*** button will allow you to scan a QR code resolver.

Selecting the ***Login*** button in the top right corner will launch a **Login** prompt to allow the Relevance user to login.

Relevance User/Relevance User Login Prompt

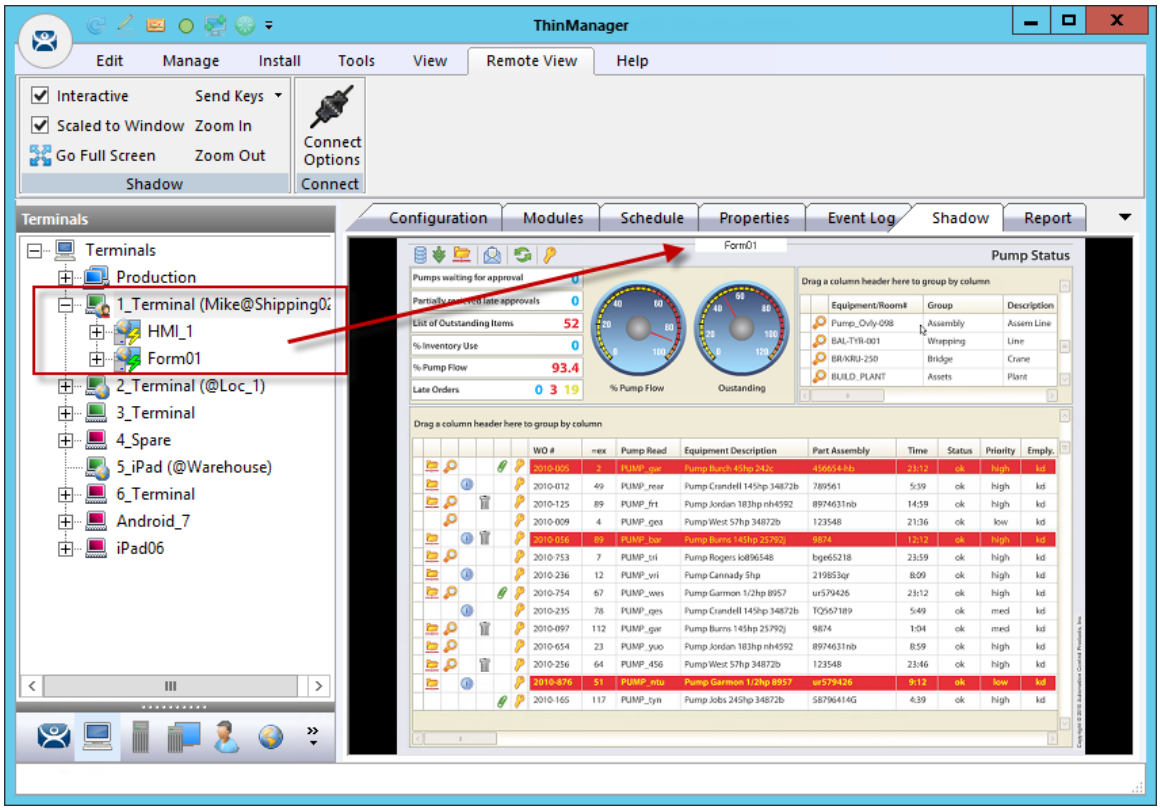
Login with the Relevance User account that is a member of the proper access group.



Relevance User Account Accesses Application

Once the Relevance User logs in, they will have access to the hidden restricted application. This shows both locations on the mobile device.

The user can log off by selecting the ***Logoff*** button in the upper right corner.



ThinManager Tree

Once the Relevance user is logged on with the correct Permissions from the access group membership the hidden application will be revealed.

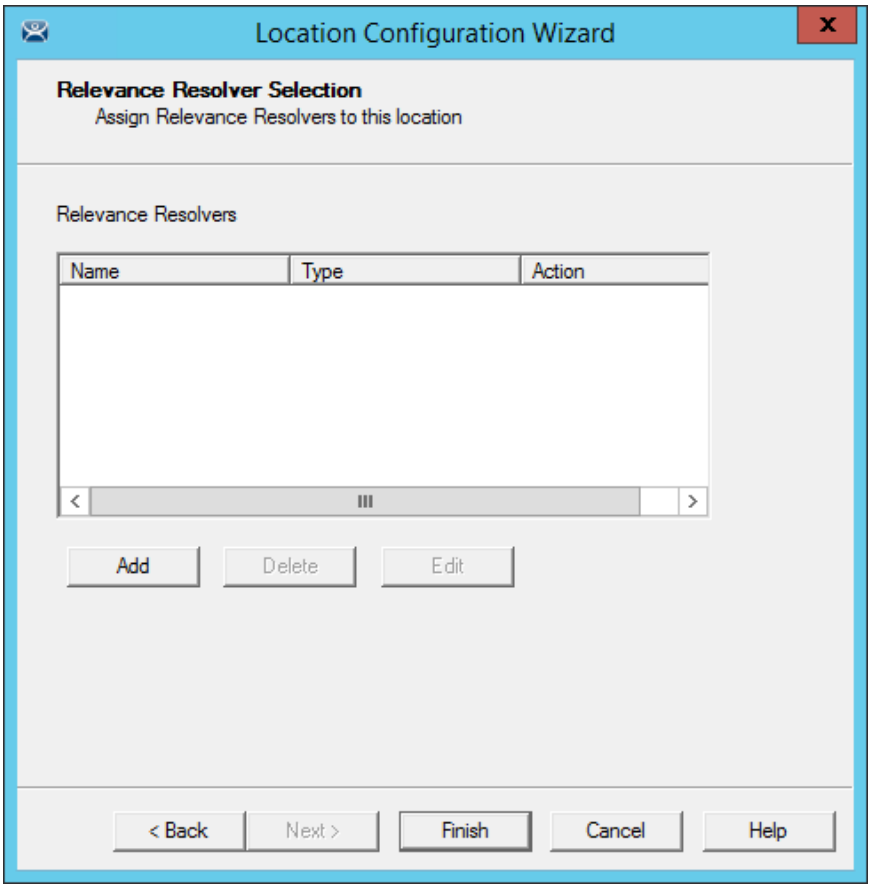
45. One QR Code, Multiple Actions

The last section covered the use of a Relevance Access Group to hide a display client application from the public with use of Access Groups. This section will cover using access groups to provide different actions.

Instead of using a different resolver for every action you can use a single resolver and Access Groups to provide different actions. This example will to use a QR code as the resolver.

Select the **Location** globe icon on the Tree Selector at the bottom of the tree to open the Locations branch.

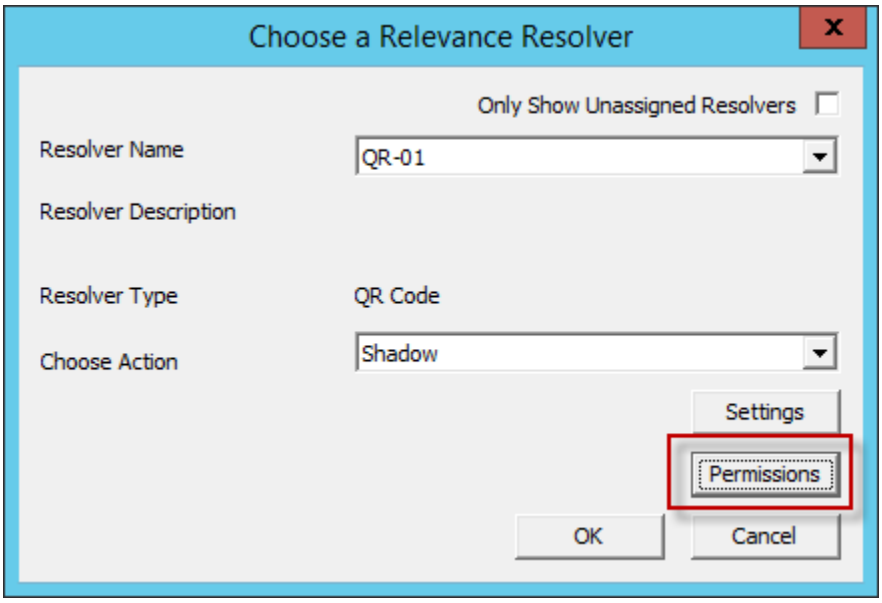
Highlight the Terminal and double click or select ***Modify*** to open the **Location Configuration Wizard**.



Relevance ID Selection Page

Navigate to the **Relevance ID Selection** page.

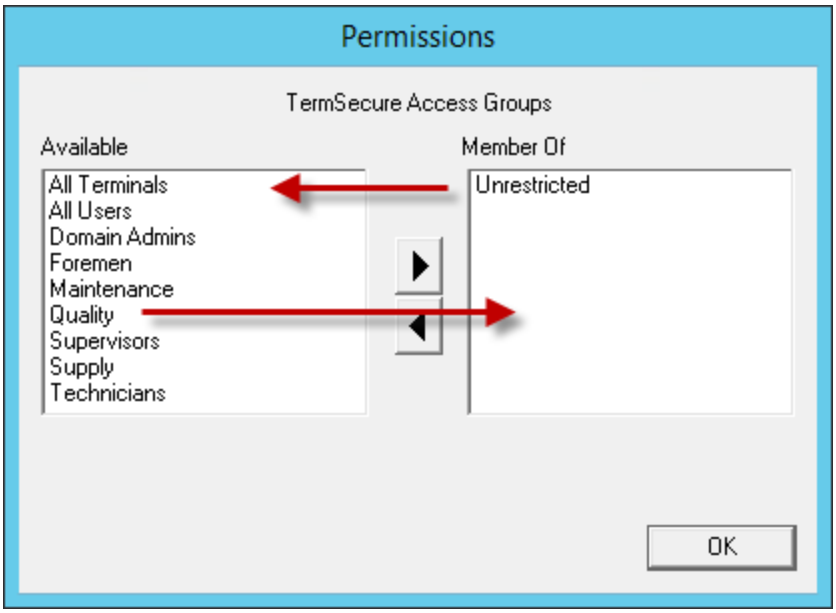
Add the same resolver to the location as many times as you have actions and access groups you want to involve.



Choose a Relevance Resolver Window

Select a different action from the ***Choose Action*** drop-down each time you add it.

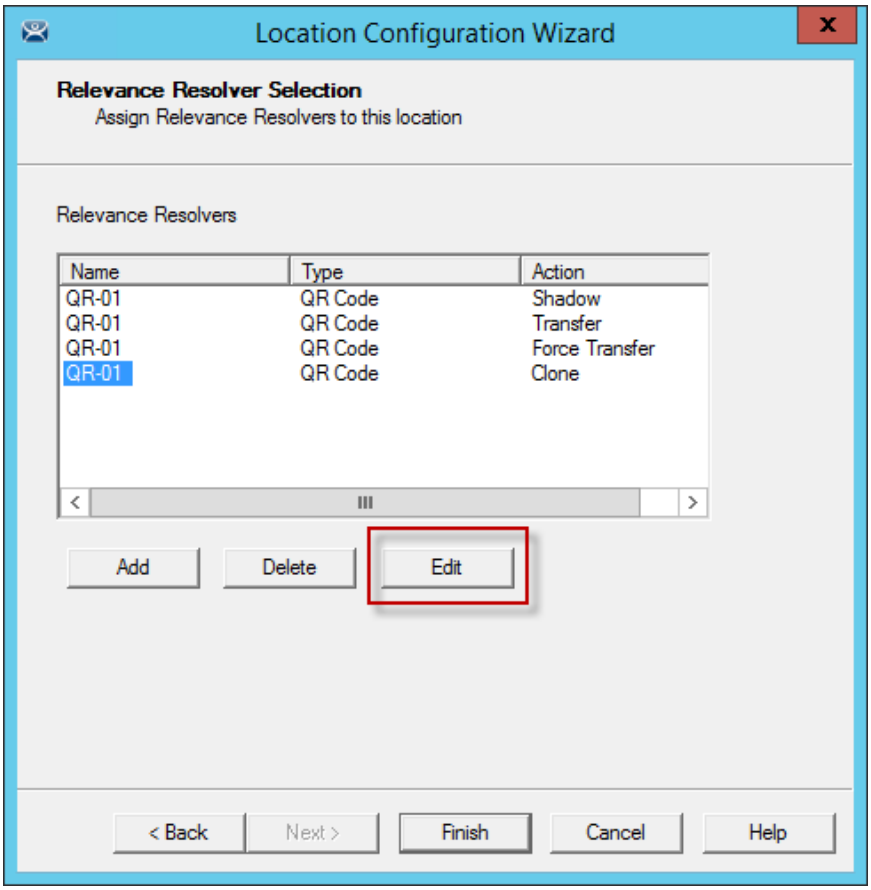
Select the ***Permission*** button to add the Access Group to the action.



Relevance ID Selection Page

Remove the ***Unrestricted*** group and add the desired access group, Quality in this example.

Select the ***OK*** button to finish.



Edit Button on the Relevance Resolver Selection Page

You can also edit the permissions by highlighting a resolver and selecting the ***Edit*** button. This will launch the **Choose a Relevance Resolver** window that has the ***Permissions*** button on it.

This example used the following settings:

Location	Application	Resolver	QR Action	Access Group
Loc_1	HMI_1 Form03	**QR-01**	Shadow	Quality
		QR-01	Transfer	Maintenance
		QR-01	Force Transfer	Foremen
		QR-01	Clone	Supervisor

If a **Quality** member scans the QR-01 code they will be able to shadow the location, leaving control with the operator.

If a **Maintenance** member scans QR-01 they will transfer the application to their mobile device once the operator allows it.

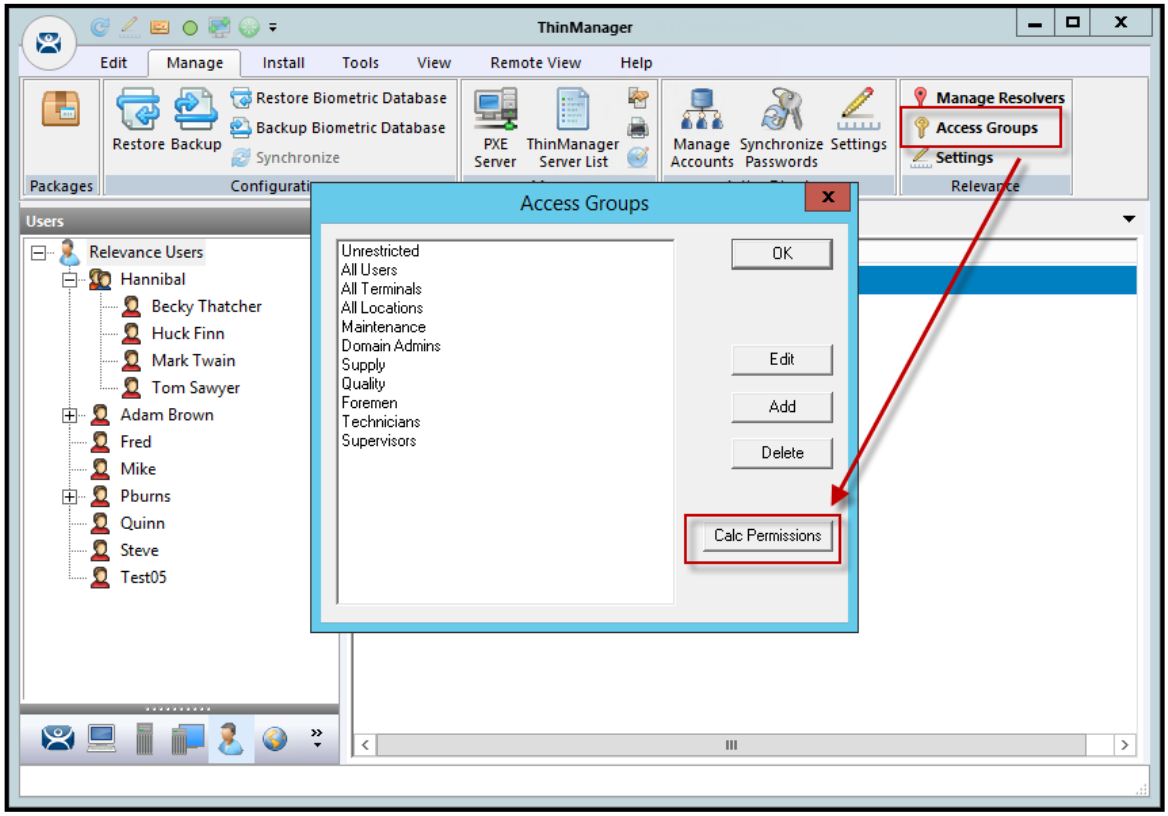
If a **Foreman** scans the QR-01 code they will immediately transfer the display from the location to their mobile device so that they can take their application with them when they roam through their section.

If a **Supervisor** scans QR-01 they will clone the application and run it with their own Windows account.

46. Calculating Permissions

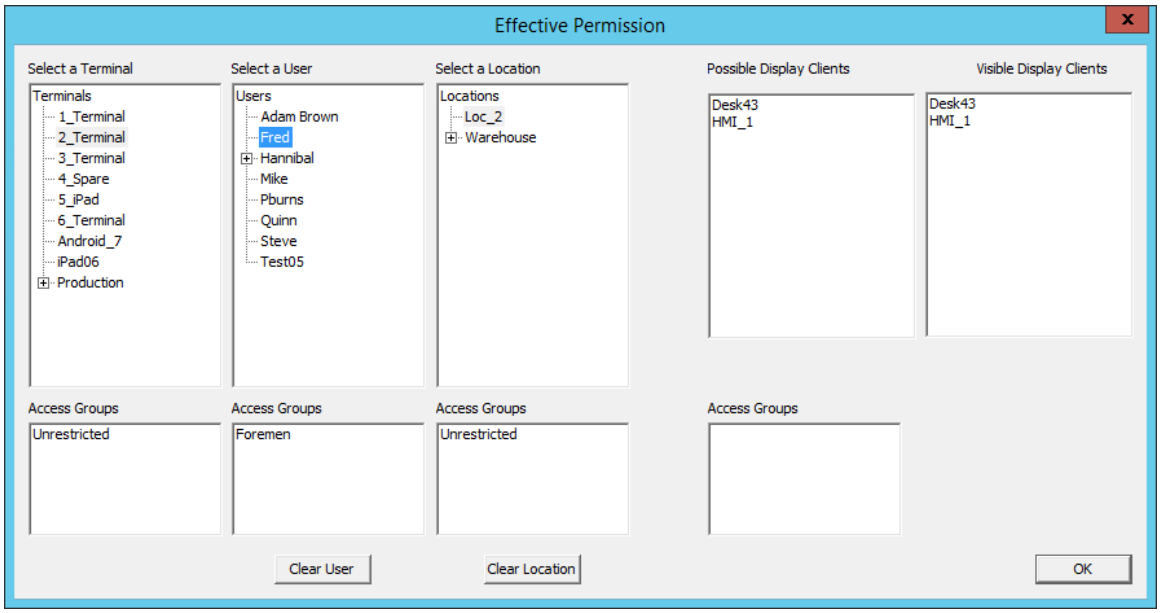
It is easy to lose track of the permissions as your system expands and more functions and features are added. Relevance has a Permission Calculator to help.

Open the **Access Groups** window by selecting ***Manage > Access Groups***.



Access Groups Window

Select the ***Calc Permissions*** button on the **Access Groups** window.



Effective Permission Window

There are four columns, **Select a Terminal**, **Select a User**, **Select a Location**, and **Visible Display Clients**.

Highlighting members of selection lists will show the display clients that will be visible in the **Visible Display Client** column.

The ***Clear User*** and ***Clear Location*** buttons will clear the fields and allow you to test another combination.

The ***OK*** button closes the window.

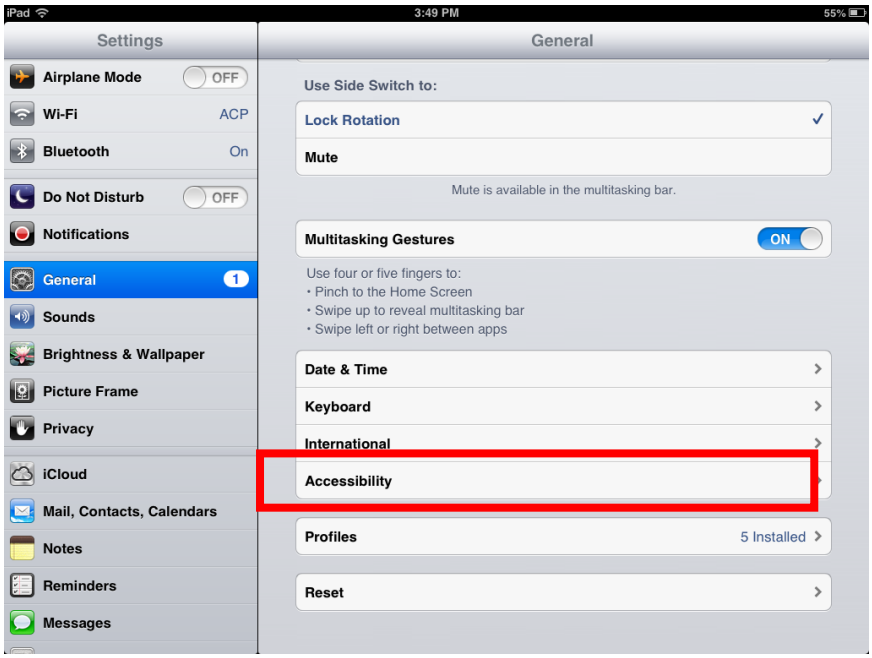
47. Guided Access on the iPad

Guided Access a feature that allows the iPad to be locked to a single application. This can help an administrator control the iPad by limiting users to the iTMC program.

Note: This advice is given as a service to our users. Please see Apple documentation for implementation.

Guided Access is turned on in the General settings of the iPad.

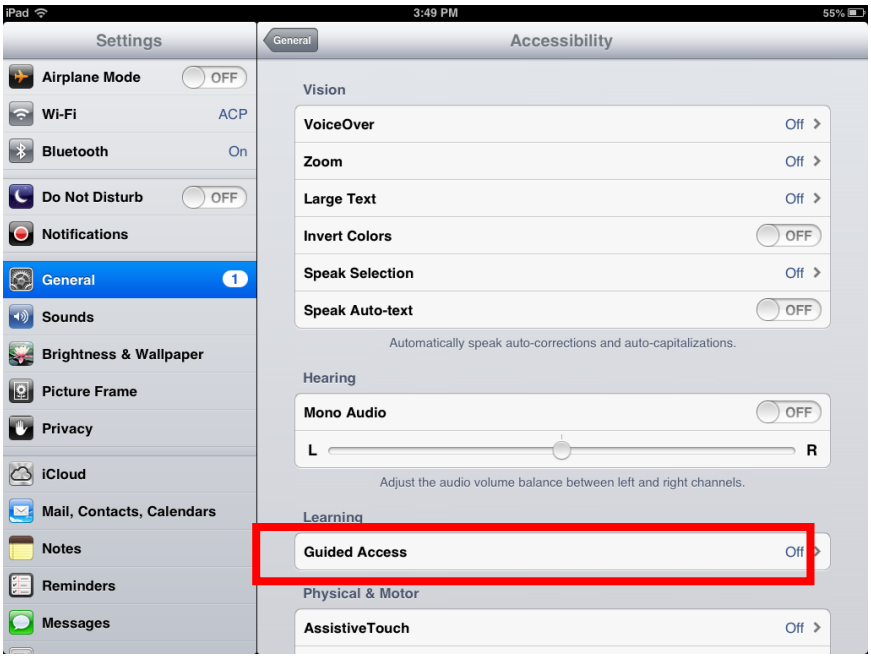
Open the ***Settings*** of the iPad.



Settings Page

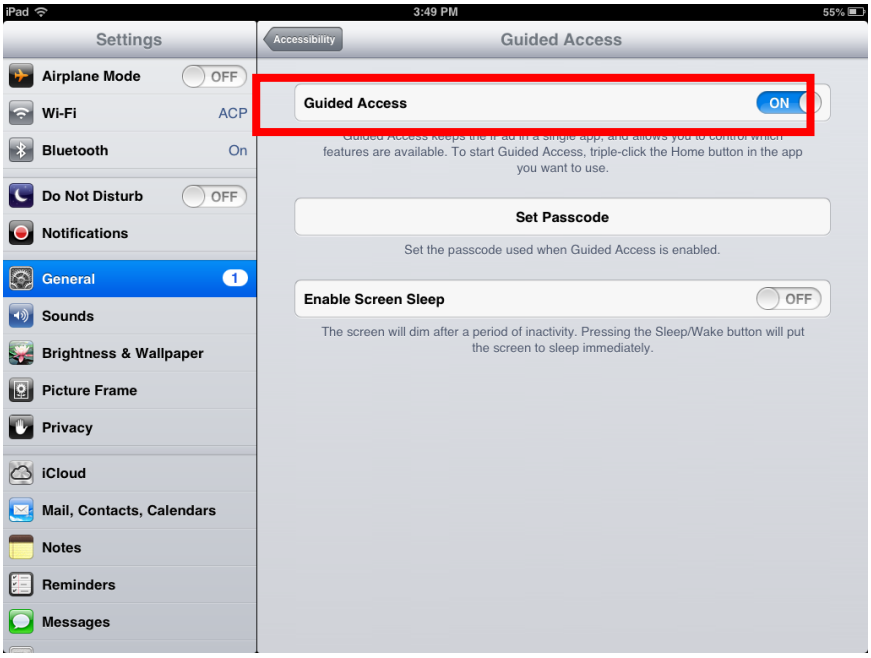
Select the ***General*** setting.

Select ***Accessibility***.



Accessibility Settings

Select the ***Guided Access*** setting.



Guided Access Settings

Turn ***Guided Access*** on.

Select ***Set Passcode***.

Set Passcode

Enter a four digit number as the passcode.

Re-enter the number to confirm.

- ✓ **DO NOT FORGET THIS NUMBER. It will allow you to turn the Guided Access off.**

Close the **Settings** by pressing the **Home** button once.

Guided Access for an Application

Open the application you want to run exclusively, like iTMC.

Click the ***Home*** button three times to open the Guided Access control.

Press the ***Start*** button in the upper right corner.

This will restrict the iPad to that application. The user cannot close the application and is restricted to that app.

Press the ***Home*** button three times to return to the Guided Access control.

Press the ***End*** button in the top left corner to stop Guided Access.

Guided Access will be dormant until re-applied. It can be turned off completely by going into ***Settings > General > Accessibility > Guided Access*** and turning it off.

48. TermMon ActiveX and Relevance

Microsoft Remote Desktop Services lacks the ability to monitor clients and provide much useful information. ThinManager has written an ActiveX component to overcome this shortcoming.

The TermMon (Terminal Monitoring) ActiveX can be embedded into an application that will run on the Remote Desktop Server. When a Terminal starts a session on the server and launches the application with the TermMon ActiveX, the ActiveX will create a socket connection to the Terminal and the session. It is able to pull data from the Terminal into the application using the events, methods, and properties that are provided by TermMon.

This is commonly used by customers that have Automation HMI products, such as Rockwell FactoryTalk View, GE Proficy, or Wonderware InTouch. With this ActiveX, customers can get information about the Terminal, sessions that are running, users that are logged on, and the current Location for Relevance applications. You can create tags for the data and populate them with data from the client via the ActiveX.

There are also methods to control the current Display Client, logged on Users, IP Cameras overlays, and many others.

For Relevance Location Services, the main features are with regard to the Location. Once a mobile device has resolved to a Location a string property is available that has the path and name of the current Location. If you have nested Locations, it provides this information in a path form, such as "***ParentLocation\ChildLocation\ChildLocation***". This can be a very versatile item for customers that are using HMI's and want to control access to pages, security, and other things based on the Location.

One other Relevance feature in the ActiveX is the ability to trigger an Operator to scan a code through the application. This can be used to provide an extra layer of safety and security to an application. It can be tied to any operation in the HMI. For example, it could be added to a button to run a pump. Prior to the command to run going out, an event can be triggered that will prompt the Operator to scan a code. They then scan a QR Code and it provides a result back to the HMI. Then, the code on the button determines if it can go ahead and provide the command to run the pump based on whether it got the expected information from the Location, via the ActiveX.

The ActiveX also contains properties that would allow you to programmatically Logon or Logoff (Enter or Exit) of a Location. This tells the session which Location to login to by passing a string to the appropriate ActiveX property. Selecting the Logoff item is the same as hitting the "Leave" button that is part of the iTMC application.

48.1. Registering the Control

The TermMon ActiveX Control can be found on the ThinManager CD as **`termmon.ocx`**. It is also available in the Download section of www.thinmanager.com.

The Control must be registered before it can be used. Copy the file **`termmon.ocx`** to the computer where you want to use it. Register the OCX by executing **`regsvr32 <path\termmon.ocx>.`**

48.2. Read-Only Properties

The following properties are read only strings. An event will be generated any time one of these properties changes. The Enable method must be invoked prior to reading these properties.

The following properties are read only strings. An event will be generated any time one of these properties changes. The Enable method must be invoked prior to reading these properties.

- **TerminalName** - This is the name of the Terminal.
- **TerminalModel** - This is the Terminal model number.
- **TerminalIP** - This is the Terminal IP address.
- **TerminalMAC** - This is the Terminal MAC Address.
- **TerminalBootLoaderVersion** - This is the Terminal network boot loader version.
- **TerminalFirmwareVersion** - This is the firmware version that the Terminal is running.
- **TerminalWindowsUsername** - This is the Windows Username that is specified in the Terminal's ThinManager configuration.
- **TermSecureUsername** - This is the TermSecure username of the TermSecure user currently logged onto the Terminal. If no TermSecure user is logged on, this value will be blank.
- **TermSecureWindowsUsername** - This is the Windows Username associated with a TermSecure user. This is the Windows Username for all TermSecure user sessions. If no TermSecure user is logged on, this value will be blank.
- **TerminalServerGroupList** - This is a comma-separated list of Display Clients currently running on the Terminal.
- **ConnectionState** - This is the Control's connection state with the Terminal.
- **CurrentTerminalServerGroup** - This is the Display Client that is currently being displayed on the Terminal.
- **CurrentWindowsUsername** - This is the Windows Username of the session where the Control has been executed. This property is not available when the RunInSession property is set to ***False***.
- **TerminalServerName** - This is the name of the Remote Desktop Server where the Control is running. This property is not available when the RunInSession property is set to ***False***.
- **UserID** - This is the identifier associated with a TermSecure user. An example of this would be the badge number of a security badge used by a TermSecure user when scanning the badge. Using this property may require enabling the "Expose ID" setting in the appropriate ThinManager module (i.e. RFIdeas pcProx USB Module).
- **RelevanceLocationName** - This is the complete path and name of the current Relevance Location.
- **ScanResult** – This property will contain the result of the Command Method Scan Code commands.
- **BiometricData** – This property will contain the raw data returned from a biometric scan. The format of this data will be determined by the Biometric module as configured on the Terminal.
- **BiometricLookupResult** – This property will contain the result of the ScanBiometricAndQueryUser command.

  TermMonConst.Success – The lookup was successful.

  TermMonConst.Timeout - The request timed out.

  TermMonConst.Busy - The Control is busy with another request.

TermMonConst.UserNotFound - The scan did not match an enrolled user.

TermMonConst.Fail - The operation failed.

- **BiometricLookupUsername** – This property will contain the TermSecure username when the result of the ScanBiometricAndQueryUser command is successful.

48.3. Read-Write Properties

These properties can be set by the application.

- **RunInSession** - When the RunInSession property is set to True, the Control will be running in the Terminal's Remote Desktop Services session. The Terminal IP address will be determined automatically by the control.
- **OverrideIP** - If the RunInSession property is set to False, the OverrideIP property specifies the IP Address of the Terminal that the Control will connect to.

Note: To use the OverrideIP property, the TermMon ActiveX Control Configuration Module must be added to the Terminal configuration in ThinManager. In the module configuration, ***Allow ActiveX Connections*** must be set to ***YES***, and ***Only Allow Connections from Session*** must be set to ***NO***.

- **WatchdogTime** – This is the number of seconds before the watchdog will reset the Terminal session. Once this property is set to a non-zero value, the property must be updated before the watchdog time reaches zero. To disable the watchdog, set this property to zero. The watchdog is disabled by default.

Note: The ***Enable Method*** does not need to be called for watchdog operation. Watchdog operation is independent of the ***Enable*** and ***Disable Methods***.

- **ActiveScreen** – For MultiMonitor configurations, this is the active screen number. A value of zero (default) will set the active screen to the screen the mouse pointer is on when a method or command is executed. A non-zero value will set the Active Screen to the screen number specified. All methods and commands will be executed on the specified screen.

48.4. Events

When a property value changes, an event will be generated by the Control. When an Event occurs the event code can be used to determine the property that changed. The Enable method must be invoked in order to receive events (except for WatchdogTime). The event code is provided by the Control as follows:

- TermMonEvent.TerminalName
- TermMonEvent.TerminalModel
- TermMonEvent.TerminalIP
- TermMonEvent.TerminalMAC
- TermMonEvent.TerminalBootLoaderVersion
- TermMonEvent.TerminalFirmwareVersion
- TermMonEvent.TerminalWindowsUsername
- TermMonEvent.TermSecureUsername
- TermMonEvent.TermSecureWindowsUsername
- TermMonEvent.TerminalServerGroupList
- TermMonEvent.ConnectionState

- TermMonEvent.CurrentTerminalServerGroup
- TermMonEvent.CurrentWindowsUsername
- TermMonEvent.TerminalServerName
- TermMonEvent.WatchdogTime
- TermMonEvent.RelevanceLocationName
- TermMonEvent.ScanResult
- TermMonEvent.BiometricData
- TermMonEvent.BiometricLookupResult
- TermMonEvent.BiometricLookupUsername

48.5. Methods

- **Enable** - Invoking this method will enable the Control. The Control will attempt to connect to the Terminal and generate events to update the Control Properties. The Control will maintain a connection to the Terminal as long as it is enabled.
- **Disable** - Invoking this method will cause the Control to break the connection with the Terminal. Events will be generated to clear the Control Properties.
- **Command** - The Command method can be used to send Terminal action commands. The Command method requires one parameter which is the Terminal command to be performed. The Enable method must be invoked before these commands can be executed (except for noted exceptions). The supported commands are:
    - **Reboot** - This command will initiate a Terminal reboot.
    - **Restart** - This command will initiate a Terminal restart.
    - **Calibrate** - This command will initiate a touch screen calibration.
    - **GotoMainMenu** - This command will cause the Main Menu to be displayed.
    - **SwitchToNextGroup** - This command will switch to the next Display Client.
    - **SwitchToPrevGroup** - This command will switch to the previous Display Client.
    - **SwitchInstFailover** - This command will switch the instant failover group.
    - **ChangeTermSecureUser** - This command will disconnect any current TermSecure user sessions and then display the TermSecure Log On menu.
    - **LogOffAndChangeTermSecureUser** - This command will log off any current TermSecure user sessions and then display the TermSecure Log On menu.
    - **LogOffTermSecureUser** - This command will log off any current TermSecure user sessions and will return to a Display Client which is assigned to the Terminal. If no Display Clients have been configured on the Terminal, the TermSecure Log On menu will be displayed.
    - **DisconnectTermSecureUser** - This command will disconnect any current TermSecure user sessions and will return to a Display Client which is assigned to the Terminal. If no Display Clients have been configured on the Terminal, the TermSecure Log On menu will be displayed.
    - **DisconnectSession** - This command will disconnect the Remote Desktop Services Session running on the Terminal. This command does not require that the Enable Method be invoked prior to execution.

- **LogOffSession** - This command will log off the Remote Desktop Services Session running on the Terminal. This command does not require that the Enable Method be invoked prior to execution.
- **TileStart** - This command will tile the Display Clients on the current Screen.
- **TileEnd** - This command will untile the Display Clients on the current Screen.
- **ScanCodeReturnData** - This command will prompt the user to scan a QR or Barcode. After the scan is complete, the scan data will be returned in the ScanResult property.
- **ScanCodeAndQueryLocation** - This command will prompt the user to scan a QR or Barcode. After the scan is complete, the location path and name will be returned in the ScanResult property.
- **ScanBiometricAndQueryUser** - This command will send the next Biometric scan to ThinServer and return the associated TermSecure Username. The result of the operation will be returned in the BiometricLookupResult property.Upon a successful result, the TermSecure username is returned in the BiometricLookupUsername property.

The Command Method constants are provided by the Control as follows:

- TermMonCommand.Reboot
- TermMonCommand.Restart
- TermMonCommand.Calibrate
- TermMonCommand.GotoMainMenu
- TermMonCommand.SwitchToNextGroup
- TermMonCommand.SwitchToPrevGroup
- TermMonCommand.SwitchInstFailover
- TermMonCommand.ChangeTermSecureUser
- TermMonCommand.LogOffAndChangeTermSecureUser
- TermMonCommand.LogOffTermSecureUser
- TermMonCommand.DisconnectTermSecureUser
- TermMonCommand.DisconnectSession
- TermMonCommand.LogOffSession
- TermMonCommand.TileStart
- TermMonCommand.TileEnd
- TermMonCommand.ScanCodeReturnData
- TermMonCommand.ScanCodeAndQueryLocation
- TermMonCommand.ScanBiometricAndQueryUser

- **ChangeTerminalServerGroup** - This method can be used to change the Display Client currently displayed on the Terminal. This method requires one parameter which is the name of the Display Client that the Terminal should switch to.
- **TermSecureCheckAccess** - This method can be used to query the access rights of a TermSecure user. This method requires two parameters. The first parameter is the name of the user. The second parameter is the name of the Access Group. This method returns the result of the query as follows:

- **TermMonConst.Timeout** - The request timed out.
- **TermMonConst.Busy** - The Control is busy with another request.
- **TermMonConst.InvalidMember** - The user is not a member of the specified TermSecure Access Group.
- **TermMonConst.ValidMember** - The user is a member of the specified TermSecure Access Group.
- **TermMonConst.UserNotFound** - The TermSecure Username was not found.
- **TermMonConst.GroupNotFound** - The Access Group Name was not found.

- **GetGroupScreen** - This method can be used to determine which screen the specified Display Client is currently on for MultiMonitor configurations. This method requires one parameter which is the name of the Display Client.
- **TermSecureLogonUser** - This method can be used to Log On a specified TermSecure user. This method requires two parameters. The first parameter is the name of the TermSecure user. The second parameter is the password of the TermSecure user. The password will be encrypted before being sent to the Terminal. This method returns a result as follows:
  - **TermMonConst.Success** - The TermSecure user was successfully logged on.
  - **TermMonConst.Timeout** - The request timed out.
  - **TermMonConst.Busy** - The Control is busy with another request.
  - **TermMonConst.UserNotFound** - The TermSecure username was not found.
  - **TermMonConst.BadPassword** - The TermSecure password was invalid.
  - **TermMonConst.NoPermission** - The TermSecure user does not have permission to use the Terminal.
  - **TermMonConst.PasswordChangeReq** - The TermSecure user is required to change his password.
  - **TermMonConst.NoWindowsUsername** - This TermSecure user does not have a Windows Username specified in the TermSecure user configuration. This is only required for Remote Desktop Services Display Clients assigned to the TermSecure User.
  - **TermMonConst.NoWindowsPassword** - This TermSecure user does not have a Windows Password specified in the TermSecure user configuration. This is only required for Remote Desktop Services Display Clients assigned to the TermSecure User.
- **CameraOverlayEnable** - This method is used to enable a camera overlay. This method requires two parameters. The first parameter is the name of the Display Client the overlay is on. The second parameter is the name of the overlay.
- **CameraOverlayDisable** - This method is used to disable a camera overlay. This method requires two parameters. The first parameter is the name of the Display Client the overlay is on. The second parameter is the name of the overlay.
- **CameraOverlayCycleStart** - This method is used to start camera cycling for a camera overlay. This method requires two parameters. The first parameter is the name of the Display Client the overlay is on. The second parameter is the name of the overlay.
- **CameraOverlayCycleStop** - This method is used to stop camera cycling for a camera overlay. This method requires two parameters. The first parameter is the name of the Display Client the overlay is on. The second parameter is the name of the overlay.
- **CameraOverlaySwitchNext** - This method is used to switch to the next camera in a camera overlay list. This method requires two parameters. The first parameter is the name of the Display Client the overlay is on. The second parameter is the name of the overlay.

- **CameraOverlaySwitchPrev** - This method is used to switch to the previous camera in a camera overlay list. This method requires two parameters. The first parameter is the name of the Display Client the overlay is on. The second parameter is the name of the overlay.
- **CameraOverlayFullscreenEnter** - This method is used to make the current camera in a camera overlay enter full screen. This method requires two parameters. The first parameter is the name of the Display Client the overlay is on. The second parameter is the name of the overlay.
- **CameraOverlayFullscreenExit** - This method is used to make the current camera in a camera overlay exit full screen. This method requires two parameters. The first parameter is the name of the Display Client the overlay is on. The second parameter is the name of the overlay.
- **CameraOverlaySwitchByName** - This method is used to change cameras in a camera overlay. This method requires three parameters. The first parameter is the name of the Display Client the overlay is on. The second parameter is the name of the overlay. The third parameter is the name of the camera. The camera name must include the full path if the camera is in a camera group.
- **CameraOverlayMove** - This method is used to change the position of a camera overlay. This method requires four parameters. The first parameter is the name of the Display Client the overlay is on. The second parameter is the name of the overlay. The third parameter is the x location. The forth parameter is the y position.
- **CameraOverlayResize** - This method is used to change the size of a camera overlay. This method requires four parameters. The first parameter is the name of the Display Client the overlay is on. The second parameter is the name of the overlay. The third parameter is the width. The forth parameter is the height.
- **CameraOverlayResizeMove** - This method is used to change the size and position of a camera overlay. This method requires six parameters. The first parameter is the name of the Display Client the overlay is on. The second parameter is the name of the overlay. The third parameter is the x position. The forth parameter is the y position. The fifth parameter is the width. The sixth parameter is the height.
- **RelevanceLocationLogon** – This method is used to log into a relevance location. This method requires two parameters. The first parameter is the complete path and name of the desired location formatted as “top_level_location_name\sub_location_name\location_name”. This string must match the location tree hierarchy in the ThinManager location tree. The second parameter is the action to be performed as defined by the TermMonRelevance action constants.
- **RelevanceLocationLogoff** – This method will log the device out of the current relevance location.
- **GetCustomVariable** - This method can be used to retrieve a custom variable. In ThinManager, custom variables can be added to users, locations, and Terminals. This method requires one parameter. The parameter is the name of the custom variable. This method returns the result of the query as follows:
    - **TermMonConst.Timeout** - The request timed out.
    - **TermMonConst.Busy** - The Control is busy with another request.
    - **TermMonConst.InvalidMember** - The custom variable does not exist.
    - **TermMonConst.Success** - The request completed successfully.

  Upon a successful result, the value of the custom variable can be read from the CustomVariableValue property.

48.6. Control Constants

Constant values provided by the Control are as follows:

TermMonEvent

- TerminalName 1
- TerminalModel 2
- TerminalIP 3
- TerminalMAC 4
- TerminalBootLoaderVersion 5
- TerminalFirmwareVersion 6
- TerminalWindowsUsername 7
- TermSecureUsername 8
- TermSecureWindowsUsername 9
- TerminalServerGroupList 10
- ConnectionState 11
- CurrentTerminalServerGroup 12
- CurrentWindowsUsername 13
- TerminalServerName 14
- WatchdogTime 15
- UserID 16
- RelevanceLocationName 17
- ScanResult 18
- BiometricData 19
- BiometricLookupResult 20
- BiometricLookupUsername 21

TermMonCommand

- Reboot 100
- Restart 101
- Calibrate 102
- GotoMainMenu 103
- SwitchToNextGroup 104
- SwitchToPrevGroup 105
- SwitchInstFailover 106
- ChangeTermSecureUser 107
- LogOffAndChangeTermSecureUser 108
- LogOffTermSecureUser 109

- DisconnectTermSecureUser 110
- DisconnectSession 111
- LogOffSession 112
- TileStart 113
- TileEnd 114
- ScanCodeReturnData 115
- ScanCodeAndQueryLocation 116
- ScanBiometricAndQueryUser 117

TermMonConst

- Success 0
- Fail 1
- Disconnected 2
- Connected 3
- Timeout 4
- Busy 5
- Updating 6
- RequestFailed 7
- InvalidMember 8
- ValidMember 9
- UserNotFound 10
- GroupNotFound 11
- BadPassword 12
- NoPermission 13
- PasswordChangeReq 14
- NoWindowsUsername 15
- NoWindowsPassword 16

TermMonRelevance

- ActionNone 0
- ActionTransfer 1
- ActionClone 2
- ActionShadow 3